ENTRAPASS™
GLOBAL EDITION

High Performance Access Control and Integrated Security System

Инструкция по установке

KANTECH™

DN1316-1003 / Version 4.03

Copyright © 2010 Tyco International Ltd. and its Respective Companies. All Rights Reserved. All specifications were current as of publication date and are subject to change without notice. EntraPass, Kantech and the Kantech logo are trademarks of Tyco International Ltd. and its Respective Companies.

Лицензионное соглашение компании TYCO INTERNATIONAL с конечным пользователем

на программное обеспечение KANTECH, поставляемое отдельно или вместе с другими изделиями или компонентами

ВНИМАНИЕ – НЕОБХОДИМО ВНИМАТЕЛЬНО ПРОЧЕСТЬ!
Программное обеспечение KANTECH, поставляемое отдельно или вместе с изделиями и компонентами, защищено законом об авторском праве и продаётся по условиям настоящего соглашения:

- Данное лицензионное соглашение с конечным пользователем является соглашением между Вами (физическим или юридическим лицом, которое приобрело данное программное обеспечение и сопутствующие аппаратные средства) и компанией KANTECH, являющейся изготовителем интегрированных систем безопасности и создателем программного обеспечения и любых приобретённых Вами сопутствующих аппаратных средств или компонентов (в дальнейшем "Оборудование").
- Если программный продукт KANTECH (в дальнейшем "Программный Продукт"), предназначенный для совместного использования с Оборудованием, НЕ сопровождает новое Оборудование, Вы можете не устанавливать, не копировать и не использовать этот Программный Продукт. Программный Продукт включает в себя компьютерное программное обеспечение и может включать соответствующие носители, печатные материалы и "онлайновую" или электронную документацию.
- Использование любого программного обеспечения, предоставляемого вместе с настоящим Программным Продуктом и имеющего собственное лицензионное соглашение и условия использования, регулируется такими соглашениями и условиями использования, а не данным лицензионным соглашением с конечным пользователем.
- Если Вы устанавливаете, осуществляете доступ, копируете, загружаете, сохраняете настоящий Программный Продукт или используете его каким-либо другим способом, этим Вы подтверждаете свое согласие соблюдать условия данного лицензионного соглашения с конечным пользователем, даже если настоящее соглашение окажется изменённой версией любого ранее составленного соглашения или договора. Если Вы не согласны с условиями данного лицензионного соглашения с конечным пользователем, компания KANTECH отказывает Вам в предоставлении лицензии и в праве использовать данный Программный Продукт.

ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ
Данный Программный Продукт защищён законами об авторском праве и международными соглашениями о защите авторских прав, а также другими законами и соглашениями о защите интеллектуальной собственности. Программный продукт не продается, а предоставляется в пользование по лицензии.

1 **ПРЕДОСТАВЛЕНИЕ ЛИЦЕНЗИИ.** Данное лицензионное соглашение предоставляет Вам следующие права:

a УСТАНОВКА И ИСПОЛЬЗОВАНИЕ. Каждая выданная Вам лицензия даёт Вам право на установку только одной копии Программного Продукта.

b ХРАНЕНИЕ/СЕТЕВОЕ ИСПОЛЬЗОВАНИЕ. Данный Программный Продукт не предназначен для установки, обращения, отображения, запуска, использования коллективно или одновременно на разных компьютерах, в том числе на рабочей станции, терминале или другом цифровом электронном устройстве. Другими словами, для использования Программного Продукта на нескольких компьютерах следует приобрести отдельную лицензию для каждого из них.

c РЕЗЕРВНОЕ КОПИРОВАНИЕ. Вы имеете право создавать резервные копии Программного Продукта, но на каждую лицензию в каждый момент времени должно быть установлено не более одной копии. Вы имеете право использовать резервную копию исключительно для создания архива. За исключением случаев, явно оговоренных в настоящей лицензии, запрещается создавать копии Программного Продукта, а также печатных материалов, сопровождающих данный Программный Продукт.

2 **ДРУГИЕ ПРАВА И ОГРАНИЧЕНИЯ**

a ОГРАНИЧЕНИЯ НА ВСКРЫТИЕ ТЕХНОЛОГИИ, ДЕКОМПИЛЯЦИИЮ И ДИЗАССЕМБЛИРОВАНИЕ. Запрещается вскрывать технологию, декомпилировать или дизассемблировать данный Программный Продукт, за исключением случаев, когда такие действия явно разрешены действующим законодательством, несмотря на наличие в лицензионном соглашении данного ограничения. Запрещается вносить любые изменения и модификации в Программный Продукт, если на это не получено письменного разрешения от представителя компании KANTECH. Запрещается удалять с/из Программного Продукта любые знаки, ярлыки и прочие указания на авторскую принадлежность. Вы обязаны принять необходимые меры для выполнения всех пунктов настоящего соглашения.

b РАЗБИЕНИЕ НА КОМПОНЕНТЫ. Данный Программный Продукт предоставляется в пользование по лицензии как единый продукт. Его компоненты не могут быть разделены для использования на нескольких устройствах.

c ЕДИНЫЙ ИНТЕГРИРОВАННЫЙ ПРОДУКТ. Если Вы приобрели данный Программный Продукт вместе с Оборудованием, то Программный Продукт предоставляется в пользование по лицензии вместе с приобретённым Оборудованием как единый интегрированный продукт. В этом случае Программный Продукт должен быть использован только вместе с Оборудованием, как указано далее в настоящем соглашении.

d ЗАПРЕТ НА ПЕРЕДАЧУ ВО ВРЕМЕННОЕ ПОЛЬЗОВАНИЕ И КОММЕРЧЕСКОЕ ИСПОЛЬЗОВАНИЕ. Запрещается предоставлять Программный Продукт в прокат, в аренду и во временное пользование, а также каким-либо иным образом предоставлять доступ к Программному Продукту третьим лицам, выкладывать на сервер или веб-сайт.

e ПЕРЕДАЧА ПРОГРАММНОГО ПРОДУКТА. Вы имеете право передать все права, предоставляемые настоящим соглашением, только в том случае, если продажа или передача Оборудования осуществляется безвозвратно и при условии, что Вы не оставите себе копии и передадите весь Программный Продукт (включая все компоненты, носители и печатные материалы, обновления и данное лицензионное соглашение). До передачи конечный пользователь, которому будет передан Программный Продукт, должен подтвердить свое согласие со всеми условиями данного лицензионного соглашения. При передаче обновлённой версии Программного Продукта следует передать также и все предыдущие версии.

f РАСТОРЖЕНИЕ СОГЛАШЕНИЯ. Без ущерба для каких-либо других прав компания KANTECH имеет право расторгнуть данное лицензионное соглашение с конечным пользователем в случае нарушения Вами его условий. В этом случае Вы обязаны уничтожить все копии Программного Продукта и всех его компонентов.

g ТОРГОВЫЕ ЗНАКИ. Данное лицензионное соглашение с конечным пользователем не предоставляет Вам никаких прав на товарные знаки и знаки обслуживания компании KANTECH или её поставщиков.

3 ЗАЩИТА АВТОРСКИХ ПРАВ

Все права на интеллектуальную собственность и авторские права, относящиеся к Программному Продукту (в том числе, любые изображения, фотографии и текст, являющиеся частью Программного Продукта), сопроводительной документации и любым копиям Программного Продукта, принадлежат компании KANTECH или её поставщикам. Запрещается копирование сопроводительной печатной документации. Все права на интеллектуальную собственность и иные права на информацию, к которой Вы получаете доступ при использовании настоящего Программного Продукта, являются собственностью владельцев этой информации и защищены соответствующими законами об авторских правах и другими законами и соглашениями о правах на интеллектуальную собственность. Данное лицензионное соглашение с конечным пользователем не предоставляет Вам прав на использование этой информации. Все права, которые не были явно оговорены в настоящем лицензионном соглашении, принадлежат компании KANTECH и её поставщикам.

4 ОГРАНИЧЕНИЯ НА ЭКСПОРТ

Вы соглашаетесь не экспортировать или реэкспортировать Программный Продукт в любую страну, физическому или юридическому лицу, деятельность которого ограничивается законодательством США об экспортных операциях.

5 ЮРИСДИКЦИЯ.

Данное лицензионное соглашение регулируется законодательством штата Нью-Йорк (США).

6 ОГРАНИЧЕННАЯ ГАРАНТИЯ

a ОТКАЗ ОТ ГАРАНТИИ
ПРОГРАММНЫЙ ПРОДУКТ KANTECH ПОСТАВЛЯЕТСЯ НА ОСНОВЕ ПРИНЦИПА "КАК ЕСТЬ" БЕЗ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ. КОМПАНИЯ KANTECH НЕ ГАРАНТИРУЕТ, ЧТО ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ, ИМЕЮЩИЕСЯ В ДАННОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, СООТВЕТСТВУЮТ ВАШИМ ТРЕБОВАНИЯМ, БУДУТ ПОСТОЯННО ДОСТУПНЫ ИЛИ ЯВЛЯЮТСЯ СВОБОДНЫМИ ОТ ОШИБОК.

b ИЗМЕНЕНИЕ ОПЕРАЦИОННОЙ СРЕДЫ
Компания KANTECH не будет нести ответственность за проблемы, связанные с изменением рабочих характеристик Оборудования, или проблемы взаимодействия Программного Продукта с программным и аппаратным обеспечением других изготовителей.

c ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ; РАСПРЕДЕЛЕНИЕ РИСКА
В ЛЮБОМ СЛУЧАЕ, ЕСЛИ КАКОЙ-ЛИБО ЗАКОНОДАТЕЛЬНЫЙ АКТ ПОДРАЗУМЕВАЕТ ВЫПОЛНЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ ИЛИ УСЛОВИЙ, НЕ УКАЗАННЫХ В НАСТОЯЩЕМ ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ КОМПАНИИ KANTECH ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА ПРОГРАММНЫЙ ПРОДУКТ, НО ДОЛЖНА СОСТАВЛЯТЬ НЕ МЕНЕЕ ПЯТИ ДОЛЛАРОВ США (USD$5.00). В НЕКОТОРЫХ СТРАНАХ ДЕЙСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО НЕ ДОПУСКАЕТ В ОПРЕДЕЛЕННЫХ СЛУЧАЯХ ОГРАНИЧЕНИЯ ИЛИ ИСКЛЮЧЕНИЯ СЛУЧАЙНОГО ИЛИ ОПОСРЕДОВАННОГО УЩЕРБА, И, СЛЕДОВАТЕЛЬНО, ПРИ ДАННЫХ ОБСТОЯТЕЛЬСТВАХ УКАЗАННЫЕ ВЫШЕ ОГРАНИЧЕНИЯ НА ВАС НЕ РАСПРОСТРАНЯЮТСЯ.

d ОТКАЗ ОТ ДРУГИХ ГАРАНТИЙ
НАСТОЯЩАЯ ГАРАНТИЯ ПРЕДСТАВЛЯЕТ СОБОЙ ПОЛНЫЙ ПАКЕТ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ И ЗАМЕНЯЕТ СОБОЙ ЛЮБЫЕ ИНЫЕ ГАРАНТИИ, КАК ЯВНЫЕ, ТАК И ПОДРАЗУМЕВАЕМЫЕ, ВКЛЮЧАЯ ВСЕ БЕЗ ИСКЛЮЧЕНИЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ ПРОДАЖИ И СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, А ТАКЖЕ ЛЮБЫЕ ДРУГИЕ ГАРАНТИИ И ОБЯЗАТЕЛЬСТВА СО СТОРОНЫ КОМПАНИИ KANTECH. КОМПАНИЯ KANTECH НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ИНЫХ

ГАРАНТИЙ. KANTECH НЕ ДОПУСКАЕТ И НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ПРАВ КАКИМ-ЛИБО ДРУГИМ ЛИЦАМ, НАМЕРЕВАЮЩИМСЯ САМОСТОЯТЕЛЬНО ПЕРЕДЕЛАТЬ ИЛИ ИЗМЕНИТЬ НАСТОЯЩУЮ ГАРАНТИЮ ИЛИ ЗАМЕНИТЬ ЕЁ ЛЮБОЙ ДРУГОЙ ГАРАНТИЕЙ ИЛИ ОБЯЗАТЕЛЬСТВАМИ В ОТНОШЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА.

e ИСКЛЮЧИТЕЛЬНАЯ КОМПЕНСАЦИЯ И ОГРАНИЧЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ
НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ KANTECH НЕ НЕСЁТ ОТВЕТСТВЕННОСТЬ ЗА КАКОЙ БЫ ТО НИ БЫЛО ОСОБЫЙ, СЛУЧАЙНЫЙ, КОСВЕННЫЙ ИЛИ ОПОСРЕДОВАННЫЙ УЩЕРБ (ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ) СНИЖЕНИЕ ОЖИДАЕМОГО ДОХОДА, УТРАТУ ПРОГРАММНОГО ПРОДУКТА ИЛИ СОПУТСТВУЮЩЕГО ОБОРУДОВАНИЯ, ЗАТРАТЫ НА ПРИВЛЕЧЕНИЕ КАПИТАЛА, ЗАТРАТЫ НА ЗАМЕЩЕНИЕ ИЛИ ЗАМЕНУ ОБОРУДОВАНИЯ, ТЕХНИЧЕСКИХ СРЕДСТВ ИЛИ УСЛУГ, ВРЕМЯ ПРОСТОЯ, ВРЕМЯ НА РАБОТУ С ПОКУПАТЕЛЯМИ, ПРИТЯЗАНИЯ ТРЕТЬИХ ЛИЦ, В ЧАСТНОСТИ, ПОКУПАТЕЛЕЙ, А ТАКЖЕ МАТЕРИАЛЬНЫЙ УЩЕРБ), СВЯЗАННЫЙ С НАРУШЕНИЕМ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ, НЕВЫПОЛНЕНИЕМ УСЛОВИЙ КОНТРАКТА, НЕБРЕЖНОСТЬЮ, ПРЯМОЙ ОТВЕТСТВЕННОСТЬЮ, ИЛИ КАКОЙ-ЛИБО ДРУГОЙ ЗАКОНОДАТЕЛЬНОЙ БАЗОЙ.

ВНИМАНИЕ! Компания KANTECH рекомендует регулярно выполнять полное тестирование всей системы. Однако даже несмотря на частое тестирование, Программный Продукт может функционировать не так, как ожидалось, вследствие (но не только) несанкционированного вмешательства или сбоев в подаче электропитания.

Содержание

Глава 1 •:Введение 1

Основные преимущества EntraPass 3

Руководство и справочная система EntraPass 6

Пользование справочным руководством 6
Обращение к справочной системе 6
Техническая поддержка 7

Системная диаграмма 8

Глава 2 •:Установка программного обеспечения 9

Рекомендуемые системные требования 10

Сервер EntraPass WebStation 10
Рабочая станция и Шлюз с NCC 10
Только NCC8000 или DOS приложения 10
Дополнительные требования 11

Установочный комплект 12

Мастер установки 13

Установка EntraPass (новая установка) 13

Установка системы 14

Регистрация системы 21

Регистрация системы 21
Дополнительные компоненты системы EntraPass 23

Редактирование сведений о компонентах системы 27

Переименование приложений Entra Pass 27

Связь с сервером EntraPass 28

Установление связи с сервером 28

Установка внутреннего Global шлюза (NCC8000) 30

Правка файла Config.sys 30

Установка внешнего Global шлюза (NCC8000) 31

Настройка внешнего Global Шлюз (NCC8000) 32

Переход на другое программное обеспечение SE-CE-GE 32

Обновление системы EntraPass 34

Перед обновлением EntraPass 34
Обновление на новую версию 34

Удаление программного обеспечения EntraPass 38

Глава 3 •:Начало работы 41

Начало и окончание сессии 42

Запуск основного сервера EntraPass 42
Запуск программы Gateway 44
Запуск рабочей станции EntraPass Workstation 45
Получение сведений о статусе рабочей станции 47
Изменение свойств рабочего пространства 48
Восстановление свёрнутых окон на рабочем столе 48

Автоматическая установка (Express Setup) 49

Дополнительные автономные программы EntraPass 50

Панель инструментов EntraPass 51

Основные функции 53

Поиск компонентов 53
Окно расширенного режима поиска (Extended Selection Box) 54
Выбор компонентов 55
Выбор определенной папки 57
Порядок выбора определённого луча или шлюза 57
Вывод на печать списка или отчёта 57
Отображение связей компонентов 58
Плавующие окна 59
Иерхаический режим просмотра 59
Иерхаический режим просмотра из диалога 59
Использование кнопки многоточие (...) 60
Использование дополнительного окна 61

Глава 4 •Системные устройства 63

Панель инструментов устройств 63

Конфигурация приложений EntraPass 64

Настройка конфигурации приложения EntraPass 64
Назначение общих параметров (раздел General) 65
Описание параметров безопасности (раздел Parameters) 65

Назначение рабочего пространства (раздел Workspace) 66
Назначение параметров управления сообщениями 68
Назначение параметров управления тревогами (раздел Alarms) 69
Назначение сетевых тревог (Network Alarms) 70
Назначение параметров электронных отчётов (E-Mail Reports) 70
Настройка конфигурации приложения Шлюз (Gateway) 71
Назначение общих параметров для Шлюза (раздел General) 71
Настройка интерфейса Oracle/MS-SQL (CardGateway) 72
Создание баз данных сервера вручную 74
Настройка конфигурации зеркальной базы данных и резервного сервера 74
Настройка конфигурации приложения типа SmartLink 77
Настройка конфигурации приложения
Видеохранилище EntraPass Video Vault 80
Настройка конфигурации шлюзов EntraPass 85
Настройка конфигурации шлюза Corporate Gateway 86
Настройка Шлюза NCC-8000 90
Настройка Global Шлюза 93
Настройка аппаратного Шлюза KT-NCC 95
Настройка лучей (loops) 102
Настройка времени опроса соединения 103
Настройка прямого соединения лучей через RS-232 103
Настройка конфигурации IP соединений (только для шлюзов Corporate) 104
Настройка конфигурации соединения типа Ethernet опрос 106
Настройка конфигурации соединения типа Dial-Up (RS-232) Modem
(Связь через модем по коммутируемой линии) 107
Настройка конфигурации контроллеров 110
KT-400 4-дверный Ethernet-контроллер 110
Основные преимущества 110
Назначение общих параметров (General) для контроллеров Kantech 111
Настройка контроллера KT-100 114
Настройка контроллера KT-200 115
Назначение модулей расширения контроллеров KT-200 115
Описание дополнительных устройств для контроллера KT-200 115
Настройка контроллеров лифтов KT-2252 116
Программирование контроллеров лифтов REB-8 117
Описание модуля реле REB-8 118
Настройка контроллера KT-300 119
Настройка модулей расширения по шине Combus для KT-300 120
Настройка конфигурации 4-дверного Ethernet-контроллера KT-400 122
Настройка модулей расширения к контроллеру KT-400 124
Настройка активации реле по состоянию (только для шлюза Corporate) . 129
Описание дополнительных функций контроллера 129
Назначение локальных областей для контроллера KT-400 131
Назначение связей с этажами лифта для контроллера KT-400 132
Установление связей шаблонов (Pattern) с дверьми и номерами этажей 132
Сообщения контроллера о переполнении буфера событий 132
Настройка Kantech Telephone Entry System (KTES) 134
Назначение общих параметров для KTES 134
Назначение параметров Kantech Telephone Entry System 136
Назначение языковых параметров для настройки сообщений приветствия 137
Специальные символы 138
Назначение дополнительных параметров 138
Назначение реакций реле на внутренние состояния KTES 139
Назначение опций пейджера 140
Настройка параметров уровня администратора для жильцов 142
Конфигурация дверей 143
Назначение общих параметров дверей (раздел Door) 143
Назначение функций дверной кнопочной панели 145
для контроллеров KT-100 и KT-300 145
Для контроллеров KT-400 145
Назначение функций дверных контактов (герконов) 146
Назначение кнопки REX (Запрос на выход) 147
Назначение взаимной блокировки дверей ("Шлюз") 148
Назначение дверей лифта 149
Назначение дверей под Шлюзом Global/KT-NCC 150
Настройка событий дверей (раздел Door Events)
(Corporate Шлюз только) 152
Назначение Настроек двери для контроллеров
:Анимированные иконкии KTES (Только для Corporate Шлюза) 154
Настройка интерфейсов внешних охранных панелей
(Corporate Gateway Only) 155
Настройка реле 158
Назначение реле 158
Конфигурация входов (раздел Input) 160
Назначение входов 160

Назначение реле и входов 162
Назначение Тампера и проблемы (Tamper and Trouble) 163
Назначение входа для кабины лифта 163
Настройка удалённого оповещения о событиях (Только Шлюз Corporate) .. 164
Назначение входа(input) для группы дверей 164
Конфигурация выходов (выходных устройств) 166
Назначение общих параметров выходов (раздел Output) 166
Установление связей событий дверей с дополнительными выходами 167
Настройка интегрированной панели охранной сигнализации 168
Минимальные требования для просмотра и использования интегрированных кнопок 168
Процес интеграции разделен на три части: 168
Интегрированная настройка компонентов 171

Глава 5 •:Назначения 173

Панель инструментов Definition (Назначения) 173
Назначение расписаний 174
Назначение расписания 175
Создание двухдневного интервала 176
Назначение тревожной системы (Global/KT-NCC/NCC 8000) 177
Способности Тревожной системы 177
Общие входы (inputs) 178
Объемные извещатели и извещатели периметра 178
Процедура постановки на охрану 178
Процедура снятия с охраны 179
Снятие с охраны, когда по расписанию действует режим “No Disarm” 179
Процедура отложения постановки на охрану 180
Чтобы назначить тревожный раздел 181
Назначение областей (Только Global/KT-NCC/NCC 8000 Шлюзы) .. 187
Назначение функции Guard Tour (Только для Шлюзов Global/KT-NCC/NCC 8000) 190
Назначение этажей (Floors) 192
Назначение связки Событие/Реле, (только шлюзы Global/KT-NCC/NCC 8000) 193
Назначение параметра событие/реле (Event Relays) 193
Печатать Событие\Реле (Event Relay) 194
Назначение графических схем 195
Назначение компонентов графических схем (раздел Graphic) 195
Создание фонового изображения для графического окна 198
Создание связей системных компонентов с графическими иконками 199
Печать системных компонентов и графиков 200
Назначение каникул 203
Назначение Task Builder (конструктор команд) 204
Минимальные требования 204
Панель управления конструктора команд (Task Builder) 204
Добавление в задачу Email 207
Вставка в задачу Pager Command (команды на пейджер) 207
Вставка передачи сообщений на serial устроства 208
Вставка серийных устройств для передачи команд 209
Вставка файла 209
Выполнить файл (Executing a File) 209
Параметры выполнения (Executing Parameters) 209
Ввести сетевой Tag (Network Tag) 210
Ввод команд (Entering Commands) 210
Примеры построения команд в Task Builder 212
Построение задачи с Message Value Variable (сообщение о изменении количества) 212
Построение задачи с Trigger Value Variable (запоминаемое изменяемое количество) 214
Построение задачи с использованием различной информации пользователя 216

Глава 6 •Интеграция с системами видеонаблюдения 219

Конфигурация видеосервера 220
Настройка параметров связи видеосервера 220
Повышение уровня защищённости видеосерверов 221
Назначение видеохранилища EntraPass Video Vault 222
Назначение камер 224
Назначение камеры (раздел Camera) 224
Назначение предустановок и маршрутов (preset и pattern) 225

Назначение событий для записи камерой 225
Порядок выбора событий и расписаний для записи камерой 226
Установление связи камеры с иконкой 227
Назначение окон видео VideoView 228
Назначение общих параметров для видеоокон 228
Создание и редактирование видеоокон 231
Изменение видеоокна 231
Video Triggers - События, инициирующие включение-выключение видеозаписи 233
Назначение параметров инициирующих событий для запуска Video Trigger 233
Параметры записи (Recording Parameters) 234
Настройка параметров записи 234
Настройка параметров остановки записи 235
Список событий видео(Video Event List) 237
Порядок работы со списком событий видео (Video Event List) 237
Поиск событий видео 237
Воспроизведение фрагментов видео 241
iПривязка ключевых кадров к видеозаписям 243
Экспортирование видео файлов 243
Защита видеозаписей паролем 244
Воспроизведение файлов видео 246
Просмотр записей видео в окне Video Playback 246
Записи, выполняемые в данный момент (Current Recording) 248
Просмотр текущих записей 248
Рабочий стол видеонаблюдения 249
Вывод на экран окна видеонаблюдения 249
Просмотр экспортированных видеофайлов 251
Просмотр видеохранилища EntraPass Video Vault 252
Просмотр видеофрагментов из архива видеохранилища EntraPass Video Vault 252
Глава 7 •:Управление (Operations) 253
Панель инструментов в окне Operation 253
Панель инструментов в меню Operation 253
Контекстное меню окна Operation 253
Меню состояния компонента 254
Ручное управление Шлюзом 256
Выбор шлюза 256
Обновление физических компонентов 256
Исполнение жесткого сброса Шлюза 256
Повторная загрузка данных шлюза 257
Broadcasting/Посылка широковещательного запроса 257
Принудительная загрузка frimeware 257
Операции с лучами/сайтами при работе в ручном режиме 258
Выполнение операций с лучами/сайтами при работе в ручном режиме 258
Сообщения о состоянии соединения, доступные в списке меню 259
Управление контроллерами при работе в ручном режиме 260
Выбор контроллера 260
Выполнение мягкой перезагрузки контроллера 261
Выполнение жёсткой перезагрузки контроллера 261
Повторная загрузка контроллера в ручном режиме 261
Загрузка прошивки контроллера вручную 261
Разблокировка клавиш считывателя вручную 261
Сброс питания считывателя в ручном режиме 261
Сброс счётчиков карт внутри и вне охраняемой территории или всех карт в локальной зоне контроля 261
Подсчёт числа карт внутри и вне охраняемой территории 262
Сброс счётчиков карт вошедших и вышедших или всех карт в локальной зоне контроля 262
Управление дверями при работе в ручном режиме 263
Выбор двери или группы дверей 264
Блокировка двери вручную 264
Разблокировка двери вручную 264
Временная разблокировка двери 264
Сброс двери в работу по расписанию 265
Разрешить использование считывателя карт на двери 265
Запретить использование считывателя карт на двери 265
Операции с дверями лифтов при работе в ручном режиме 266
Выбор двери лифта 267
Закрытие лифтовых кабин/Блокировка двери лифтовой кабины 267
Разблокировка этажей через двери лифта 267
Временная разблокировка доступа на этажи через двери лифта 268

Сброс расписания лифтовой двери 268
Разрешить доступ на этаж лифта 268
Запретить доступ на этаж из лифта 268
Операции с реле при работе в ручном режиме 269
Выбор реле 269
Деактивация реле вручную 270
Активация реле вручную 270
Временная активация реле 270
Перезагрузка расписания реле/
Возвращения режима работы реле по расписанию 270
Операции с входами/inputs при работе в ручном режиме 271
Операции с входами при работе в ручном режиме 271
Возврат входа в нормальное состояние вручную 271
Установка продолжительного контроля входа 272
Прекращение мониторинга входа 272
Временное прекращение мониторинга входа (шунтирование) 272
Ручное управление над тревожной системой 273
Исполнение ручного управление над тревожной системой 273
Постановка на охрану тревожной системы в ручном режиме 273
Снятие с охраны тревожной системы в ручном режиме 274
Изменение времени отложения постановки
тревожной системы в ручном режиме 274
Ручное управление с Guard Tour 275
Запуск Guard Tour 275
Управление областями в ручном режиме 277
Ручное управление над View Roll Call 279
Ручные управление над интегрированными панелями 280

Глава 8 •Пользователи 283

Панель инструментов Users (Пользователи) 283
Назначение карт (раздел Card) 284
Выпуск новой карты 284
Выпуск новой карты в режиме расширенного
администрирования пользователей 285
Создание новых карт с помощью функции "Сохранить как..." 287
Выпуск карт с помощью функции "Групповая загрузка" (Batch Load) 287
Просмотр и проверка индивидуальных PIN кодов 288
Просмотр карт с одинаковым кодом 288
Работа с идентификационными картами 289
Правка карты 289
Поиск карты 289
Удаление карты 289
Индивидуальная настройка названий
информационных полей идентификационной карты 289
Назначение уровней доступа владельцам карт 291
Назначение уровня доступа для владельца карты 291
Назначение вторичного/дополнительного уровня
доступа только для Global/KT-NCC/NCC 8000) 291
Назначение дополнительных опций карт 293
Добавление комментариев к карте 294
Ограничение числа использований карты 294
Привязка фотографий и подписей к картам 295
Назначение фотографии из файла 295
Получение фотографии с видеокамеры 296
Импортирование подписи из файла 297
Добавление подписи с помощью устройства оцифровки подписей 298
Работа с фотографиями и подписями 298
Извлечение части изображения 299
Редактирование фотографии/подписи 300
Печать электронных пропусков 301
Выбор принтера для печати электронных пропусков 302
Предварительный просмотр и печать электронных пропусков 302
Создание электронных пропусков 304
Создание шаблона электронного пропуска 304
Описание свойств для макета электронных пропусков 304
Редактирование макета пропусков 305
Изменение числа сторон идентификационных карт 305
Изменение цвета фона 306
Добавление объектов в макет пропусков 307
Вставка информационных полей карты 308
Выравнивание объектов в макете шаблона 309
Изменение свойств информационных полей карты 310
Изменение свойств изображений 311

Добавление статических текстовых объектов 311
Добавление штрихкодов 312
Изменение свойств штрихкодов 313
Добавление текущей даты 313
Добавление изображения 315
Добавление других объектов 316
Добавление геометрических форм 317
Проверка уровня доступа карты 317
Печать идентификационных карт 319
Печать карт 319
Отображение последних транзакций с картой 322
Просмотр последних транзакций с картой 322
Назначение уровня доступа для группы карт 324
Назначение уровней доступа 326
Назначение карт посетителей 327
Создание карты посетителя (Visitor card) при создании новой карты 327
Создание карты посетителя (Visitor Card) при помощи шаблона карт 327
Назначение типов карт 328
Создание нового типа карт 328
Назначение разовых пропусков 329
Создание разового пропуска (Day Pass) 329
Создание нового разового пропуска с помощью функции "Сохранить как..." 329
Операции с группами (Batch Operations) 331
Выполнение операций с группой карт 331
Импорт и экспорт файлов CSV 333
Использование уже настроенного шаблона 333
Создание нового шаблона для импорта/экспорта данных 333
Экспорт идентификационных карт 335
Импорт идентификационных карт 337
Исправление ошибок импорта/экспорта 338
Список жильцов 341
Создание нового списка жильцов 341
Добавление новых жильцов в список 341
Импортирования списка жильцов 343
Экспорт списка жильцов 344

Глава 9 •:Группы 347

Создание групп контроллеров 348
Создание группы дверей 349
Создание групп реле 350
Создание групп входов 351
Создание групп уровней доступа 352
Создание групп этажей 353
Создание группы областей 354

Глава 10 •:Состояние системы 355

Список соединений (Connection List) 356
Просмотр списка соединений системы 356
Состояние текста 358
Вывод на экран состояние компонентов 358
Цифровой статус (Numerical Status) 360
Графический статус (Graphic Status) 361
Просмотр состояние контроллера 361
Состояние видеосерверов 363
Просмотр состояния видеосервера 363
Разрешение/запрет создания видеоархивов 363
Состояние баз данных 364
Состояние сервера (Server State) 365

Глава 11 • ..... Рабочие столы EntraPass 367

Панель инструментов DESKTOPS/РАБОЧИЕ СТОЛЫ 367
Индивидуальная настройка рабочего пространства 368
Создание временного рабочего пространства 368
Изменение свойств экрана 369
Индивидуальная настройка специальных рабочих столов 370
Индивидуальная настройка рабочего стола оператором с полным доступом 370
Индивидуальная настройка рабочего стола

для оператора с доступом "только для чтения" 371
Передача индивидуально настроенного рабочего стола 371
Рабочий стол сообщений (Message Desktop) 373
Просмотр и сортировка системных событий 373
Индивидуальная настройка экрана событий для стола сообщений Message 374
Выполнение разных задач с системными сообщениями 376
Рабочий стол фотографий пользоватлей(Picture) 378
Изменение свойств окна Pictures 378
Рабочий стол отфильтрованных собщений (Filtered Messages Desktop) 380
Настройка рабочего стола избранных сообщений (Filtered Messages Desktop) 380
Рабочий стол архивных отчётов (Historical Report Desktop) 381
Настройка рабочего стола архивных отчётов (Historical Report Desktop) .. 381
Создание и редактирование архивных отчётов из рабочего стола 382
Отображение состояния архивного отчёта в реальном времени 382
Воспроизведение архивных видеозаписей
:Анимированные иконкииз списка сообщений на рабочем столе 383
Рабочий стол тревог 384
Назначение рабочего стола тревог (Alarms Desktop) 384
Просмотр тревожных системных сообщений 385
Автоматическое отображение рабочих столов тревог 387
Подтверждение тревог/событий 387
Автоматическое подтверждение 388
Порядок подтверждения тревожных сообщений 388
Подтверждение тревоги в окне рабочего стола тревог 389
Рабочий стол инструкций для оператора (Instruction Desktop) 390
Просмотр инструкции к тревожному сообщению 390
Рабочий стол графических схем (Graphic Desktop) 391
Просмотр графических схем на рабочем столе Graphic Desktop 391
Мониторинг груп областей для Muster отчета 392
Рабочий стол сетевых тревог (Network Alarms Desktop) 395
Просмотр сетевых тревог 395
Рабочий стол видеонаблюдения (Video Desktop) 396
Назначение рабочего стола видеонаблюдения 396
Порядок работы с рабочим столом видеонаблюдения 396
Состояние видеосервера 398
Просмотр полного состояние видеосервера 398
Глава 12 •Системные настройки 401
Панель инструментов System (Системные настройки) 401
Назначение операторов 402
Создание или изменение данных оператора 402
Одновременная авторизация 405
Назначение уровней безопасности 406
Создание/Изменение уровней доступа операторов 406
Назначение регистрационных прав для оператора 407
Как скрыть информационные поля карты 409
Выбор специальных кнопок для управления в режиме видеонаблюдения .. 409
Назначение рабочего пространства 411
Использование фильтров для рабочего пространства 411
Назначение шлюзов и сайтов 412
Назначение контроллеров 413
Назначение дверей 413
Назначение реле 414
Назначение входов 414
Назначение уровней доступа 415
Назначение тревожной системы 415
Назначение областей 416
Назначения Guard Tours 416
Назначение типов идентификационных карт 417
Назначение фильтров карт 417
Назначение групп доступа для идентификационных карт 418
Назначение отчётов 419
Назначение графических схем 419
Назначение рабочего пространства 420
Задание уровней безопасности 420
Назначение видеосерверов 421
Ограничение доступа к отдельным камерам наблюдения 422
Назначение окон видеонаблюдения 423
Назначение задач 423

Назначение охранных панелей 424
Назначение компонентов охранной панели 424
Назначение событий 425
Назначение пункта параметров событий (событие/реакция) 426
Назначение параметров событий 426
Создание связей 428
Просмотр параметров по умолчанию /(Посмотреть связи). 429
Удаление и восстановление связей 429
Вывод на печать параметров событий 430
Назначение инструкций оператору 431
Назначение инструкции 431
Назначение команд SmartLink при использовании конструктора команд Task Builder 431
Назначение фильтров сообщений 432
Назначение события для фильтра сообщений 432
Описание структуры базы данных 435
Просмотр компонентов базы данных 435
Глава 13 •Отчеты 437
Панель инструментов Report (Отчеты) 437
Назначение быстрых отчётов (Quick Report) 438
Назначение быстрого отчёта 438
Назначение архивных отчётов 441
Назначение отчёта по умолчанию "All Events" (Все события) 441
Назначение архивного отчёта с индивидуальными настройками 441
Назначение компонентов для архивного отчёта с индивидуальными настройками 442
Назначение дополнительных функций карт для архивного отчёта с индивидуальными настройками 443
Назначение отчёта об использовании идентификационных карт 444
Настройка расписания автоматических отчётов 446
Дополнительные настройки автоматического отчёта 447
Назначение выходного формата отчёта 448
Выполнение запроса архивных отчётов 450
Запрос отчёта о событиях 452
Отчёты, отправляемые по электронной почте 453
Настройка отчёта для отправки по электронной почте 453
Отправка отчётов на рабочие станции при помощи интерфейса SmartLink 454
Назначение отчётов по учёту рабочего времени 455
Назначение отчётов по учёту рабочего времени 455
Запрос отчёта по учёту рабочего времени 457
Как вручную запросить отчёт по учёту рабочего времени 457
Операции с базой данных по учёту рабочего времени 458
Добавление транзакции в базу данных по учёту рабочего времени 458
Muster Отчеты - Отчеты о сборе людей 460
Muster отчеты для экстренных ситуаций 460
Использование Muster отчета для управлением парковкой 462
Генерация Muster отчета 462
Отчеты Roll Call/ Отчеты о движении людей в течении определенного времени 463
Функциональность 463
Генерация отчета Roll Call 463
Пример отчета Roll Call 464
Состояние отчета 465
Просмотр отчётов 466
Отображение отчёта на экране 466
Предварительный просмотр архивных отчетов 466
Предварительный просмотр отчётов по учёту рабочего времени 467
Глава 14 •Опции системы EntraPass 469
Панель инструментов Опции (Options) 469
Выбор формата карт по умолчанию 470
Назначение формата представления идентификационных карт 470
Смена аутентификационного пароля 472
Порядок изменения аутентификационного пароля 472
Выбор языка интерфейса системы 473
Выбор языков для работы с системой 473
Выбор и настройка принтеров 474
Выбор и настройка принтера журналов (Log Printer) 474

Выбор и настройка принтера отчётов (Report Printer) 475
Выбор и настройка принтера электронных пропусков (Badge Printer) 475
Изменение даты и времени системы 476
Конфигурация мультимедийных устройств 477
Выбор звукового сигнала тревоги 477
Описание параметров оцифровки/захвата изображений 478
Настройка устройства оцифровки подписей 478
Настройка параметров системы 480
Параметры сервера 480
Журналы сервера (Server Logs) 480
Пространство на диске (Disk Space) 480
Резервный сервер (Redundant Server) 481
Завершение сеанса и бездействие (Logout and Idle) 481
Расписание (Schedule) 482
Диагностика (Diagnostic) 483
Сетевая тревога (Network Alarm) 483
Индикация состояния на иконках (Icon Status) 484
Информация по авторизации приложения в качестве службы (Service Login Information) 484
Параметры Шлюза 484
Глобальные преимущества NCC 485
KT-NCC 485
Параметры прошивки (Firmware) 485
KT-100 486
KT-300 486
KT-400 486
KTES 487
Kantech IP Link 487
KT-NCC 488
Параметры изображений (Image) 488
Фотографии и электронные пропуска 489
Графические схемы (Graphic) 490
Параметры отчёта (Report) 490
CSV 490
Пространство на диске (Disk Space) 491
Формат имени пользователя 491
Параметры видеонаблюдения (Video) 492
Параметры (Parameters) 492
Захват изображения (Snap) 493
Параметры времени (Time) 494
Настройки регистрационных данных (Credential parameters) 494
Карты (Card) 494
Рабочая станция и Сервер 495
Кнопки на панели инструментов 495
Интеграция 496
Backup по расписанию 498
Настройка резервного копирования, когда сервер EntraPass работает в режиме службы 498
Настройка расписаний для автоматического создания резервных копий системной базы данных 499
Специальные сообщения (Custom Messages) 502
Настройка специальных сообщений 502
Регистрация системы (System Registration) 503
Проверка баз данных сервера и рабочих станций 504
База данных сервера 504
База данных рабочей станции 504
Глава 15 •Сервер EntraPass 505
Запуск сервера 506
Список соединений сервера (Connection list) 508
Просмотр приложений, подключенных к серверу 508
Резервные копии 509
Панель инструметов Backup 509
Создание резервных копий типа D, A и T 509
Восстановление данных (D, A и T) 511
Просмотр журнала системных событий 512
Просмотр журнала системных ошибок 512
Утилиты сервера 514
Глава 16 •Системные утилиты 515
Утилиты базы данных 516
Запуск приложения Database utility 516
Проверка целостности базы данных 517

Обновление полей базы данных (Update Database Fields) 517
Проверка индекса базы данных (Verify Database Index) 517
Проверка ссылок базы данных (Verify Database Links) 517
Проверка ирархической структуры базы данных (Verify Database Hierarchy) 518
Проверка архивных файлов базы данных (Verify Database Archive Files) 518
Проверка файлов по учёту рабочего времени (Verify Time & Attendance Files) 518
Проверка файлов видеособытий (Verify Video Event Files) 518
Замена описаний (Swap Descriptions) 518
Очистка базы данных (Clean the Database) 519
Восстановление файлов по последней транзакции с картой (Rebuild Card Last Transaction Files) 519
Видеохранилище (EntraPass Video Vault) 520
Установка видеохранилища EntraPass Video Vault 520
Запуск видеохранилища EntraPass Video Vault 520
Работа с архивированными видеофрагментами 521
Редактор языков (Vocabulary Editor) 524
Установка редактора языков (Vocabulary Editor) 524
Перевод словаря системы на другой язык 524
Интегрирование пользовательского языка в систему EntraPass 526
Распространение нового словаря между пользователями 528
Обновление словаря системы 528
Обновление словаря системы 530
Программа быстрой настройки"Express Setup" 531
Настройка луча/сайта NCC 8000/Global при использовании Express Setup . 531
Настройка конфигурации сайта/луча на шлюзе Corporate при помощи программы Express Setup 533
Настройка конфигурации контроллера при помощи программы Express Setup 538
Настройка KTES при использовании системы быстрой настройки Express Setup 539
Порядок назначения реле 540
Порядок назначения входов 540
Порядок назначения дополнительных выходов (зуммер и световой индикатор LED и Buzzer) 541
Quick Viewer - Программы быстрого просмотра отчётов 543
Диагностика по методу "запрос-ответ" (PING Diagnostic) 545
Рабочая станция – APM 546
Программа обновления Global 547
Утилита переноса данных (Migration Utility) 549
Миграция EntraPass Global Edition с версии 1 до версии 3 549
Миграции версии 1 базы данных сервера 549
Интерфейс шлюза 550
Запуск шлюза 550
Перезагрузка Шлюза 550
Интерфейс MS/SQL 552
Установка программы MS/SQL Interface 552
Настройка конфигурации программы CardGateway 552
Запуск программы CardGateway 552
Интерфейс SmartLink 555
Настройка приложения SmartLink 555
Запуск приложения SmartLink 555
Нагрузка на сеть 556
EntraPass Online помощь 557
Получение Online помощи 557
Глава 17 • Анимированные иконки 559
Тревожная система 560
Контроллеры 562
Двери 564
Реле 568
Входы 570
Лучи/Сайты и Шлюзы 573
Луч контроллера: 573
Шлюз: 573
Шлюз (Программный интерфейс Шлюза): 574
Приложения EntraPass 576
Прочее 576

Глава 1 • :Введение

Поздравляем Вас с приобретением пакета программного обеспечения EntraPass – высокоэффективной многопользовательской системы управления доступом, обладающей всеми функциями, которые только могут потребоваться для выполнения большинства задач.Welcome to EntraPass.

Что такое EntraPass? EntraPass представляет собой универсальный, управляемый с помощью меню пакет программного обеспечения управления доступом. EntraPass обладает множеством функций, а именно:

- Возможность дистанционной связи
- Подключение веб-станции EntraPass WebStation для удалённого доступа
- Интерфейс SmartLink для связи с системами оповещения, системами жизнеобеспечения, электронной почтой и пр.
- Резервный сервер для обеспечения дополнительной безопасности (приобретается отдельно)
- Возможность интеграции KT-NCC – сетевого контроллера шлюза
- Возможность подключения KT IP Link
- Совместимость с KT-100, KT-200, KT-300 и KT-400(примечание)

ПРИМЕЧАНИЕ: Вы можете подключать луч (loop) с контроллерами KT-200 на 485 шину контроллера KT-400 если в этой петле нет других контроллеров (Kantech KT-100, KT-300 и KT-400).

- Телефонная система домофонии Kantech (KTES)
- Интеграция с оборудованием других производителей
- Быстрая настройка
- Локальный и глобальный контроль повторного прохода, управление областями, несколько уровней доступа на карту, Guard tour - тур обхода охранником, взаимодействие между контроллерами в рамках шлюза,
- функция DayPass (Разовые пропуска) для временных посетителей
- Управление лифтами
- Встроенная функция изготовления электронных пропусков (бейджей).
- Интерактивные поэтажные планы здания
- Конфигурируемые оператором "рабочие столы"
- Функция Шлюз карт (CardGateway) (опция)
- Возможность использовать считыватели с разными технологиями
- Интеграция с охранными панелями по снятию постановке на охрану при помощи считывателя
- Построение системы тревожной сигнализации
- Учёт рабочего времени (Time and Attendance)
- Отчеты о сборе людей для получения отчетов о нахождении о людей в процессе эвакуации
- Автоматическая отправка отчетов по e-mail
- Визуальная диагностика оборудования
- Интеграция с видеонаблюдением American Dynamics Intellex®
- Просмотр живого и архивного видео, реакция системы видео наблюдения на события доступа
- Архивирование видео через EntraPass Video Vault (опция)
- Встроенный редактор словарей
- Интеграция с тревожной сигнализацией
- Поддержка Windows 7 Pro 32-бита

Что такое система контролядоступа ?. Что такое система контроля доступа? Система контроля доступа представляет собой комплекс совместимых между собой технических средств (считыватели, датчики прохода, детекторы движения и др.), установленных надлежащим образом, и электронный модуль управления. Рабочие станции, входящие в систему, служат для получения сообщений о событиях, оповещения о тревоге, изменения базы данных и пр. Среди поддерживаемых функций системы контроля доступа – тщательное архивирование всех системных событий с последующим быстрым извлечением из архива для проверки.

Основные преимущества EntraPass

***П*рограмма обновления программного беспечения «Kantech Advantage Program» (KAP):** При активации программного обеспечния вы обеспечены бесплатным обновлением в течении 12 месяцев и возможности прохождения online тренингов для конечных пользователей. Для дополнительных деталей, смотрите приложение по новой дополнительной программе «Kantech Advantage Program», DN1874.

SmartLink. EntraPass позволяет организовать интерфейс с такими цифровыми устройствами, какCCTV мультиплексоры, автоматизированные системы рассылки электронных сообщений, системы жизнеобеспечения, ЖК-панели, матричные коммутаторы и др., путём использования RS-232 или сетевого соединения между рабочей станцией EntraPass SmartLink и удаленным устройством. Для углублённой системной интеграции приложение SmartLink обеспечивает двустороннюю связь с такими программными приложениями как система учёта рабочего времени, функция изготовления электронных пропусков, системы управления кадрами, временная регистрация студентов и другие, при помощи TCP/IP, RS-232 или динамически подключаемых библиотек. Это позволяет осуществлять полноценный обмен данными между системами в реальном времени.

Зеркальная база данных и резервный сервер. Приобретаемый отдельно резервный сервер с зеркальной базой данных обеспечивает альтернативный способ дублирования данных на случай отказов или сбоев на основном сервере. На резервном сервере создаётся копия всей базы данных в реальном времени. В случае сбоя основного сервера зеркальная база данных запускает резервный сервер, поддерживающий все возможности и функции основного сервера, за исключением программы CardGateway. При возвращении основного сервера к работе все архивы объединяются, и вся база данных копируется из резервного сервера.

KT-NCC Сетевой контроллер шлюза. Это аппаратный Global шлюз. Система EntraPass совместима с устройствами KT-NCC. KT-NCC это превосходное решение для заказчиков, кто ищет лучшую возможность для построения распределенных систем контроля доступа, без необходимости проведения дополнительных кабелей от каждого удаленного контроллера к серверу. Когда KT-NCC совмещается с мощнейшим программным обеспечением EntraPass Global Edition, в итоге вы получаете эффективную, надежную, распределенную систему контроля доступа с глобальными преимуществами на аппаратном уровне с непревзойденной степенью защиты.

Dual Gateways Option. Опция двойного шлюза. Каждый глобальный шлюз включает также и один Corporate шлюз, при условии, что выбрана опция двойного шлюза (Dual Gateways). Это опция не требует дополнительной лицензии.

Kantech IP Link. Система EntraPass совместима с устройством Kantech IP Link, который обеспечивает защищенное Ethernet-соединение, выступая в качестве опрашивающего устройства, что позволяет контролировать трафик сети, обращаясь к шлюзам Corporate Gateway только при необходимости. Основное назначение модуля Kantech IP Link заключается в том, чтобы передавать информацию между контроллерами и шлюзом.

Контроллеры KT-100, KT-200, KT-300 и KT-400. EntraPass совместима с контроллерами Kantech's KT-100, KT-200, KT-300 и KT-400. (Шлюз NCC-8000 совместим только с KT-200). Это даёт дополнительное преимущество при обновлении объектов, требующих повышения гибкости и улучшения интерфейсов пользователей. Кроме того, есть возможность выбрать тот контроллер, который наиболее соответствует требованиям покупателя и его финансовым возможностям.

KT-400. Контроллер KT-400 – это 4-х дверный контроллер, имеющий порт Etheret с шифрованием данных. Этот контроллер может работать как IP конвертор для удаленных лучей (веток контроллеров).

Модули расширения для KT-400. Контроллер KT-400 позволяет увеличить число входов и выходов (с открытым коллектором и реле) за счёт подключения дополнительных модулей расширения. Использование входных и выходных модулей расширения позволяет подключить к каждому контроллеру KT-400 до 256 входов и до 256 выходов.

- KT-MOD-REL8: релейный модуль расширения, используемый как 8 реле общего назначения или для управления лифтом. Этот модуль поддерживает соединение в цепочку, в которую можно добавлять до 32 модулей KT-MOD-REL8 и, таким образом, увеличить общее число внешних реле до 256 на каждый контроллер KT-400.
- KT-MOD-INP16: модуль расширения входов. Позволяет увеличить число входов до 16 зон для контроллера KT-400. Д Этот модуль поддерживает соединение в цепочку, в которую можно добавлять до 15 модулей KT-MOD-INP16 на каждый контроллер KT-400, то есть до 240 внешних входов. С учётом 16 входов, имеющихся на плате контроллера KT-400, их общее число достигает 256 входов на один контроллер KT-400.
- KT-MOD-OUT16: модуль расширения выходов, 16 выходов 12 В пост. тока, с открытым коллектором. Используется для управления лифтами (при необходимости, может

потребоваться дополнительное оборудование). Допускает подключение в цепочку до 16 модулей KT-MOD-OUT16 на каждый контроллер KT-400, то есть до 256 внешних выходов.

Kantech Telephone Entry System (Домофонная система Kantech) KTES. KTES способна предоставлять доступ в здание своим посетителям, через собственную или общую телефонную сеть. Это устройство может быть также обслужено через встроенный модем или встроенный порт Ethernet. KTES спроектирована для того, чтобы быть автономным прибором, и в тоже время быть совместимой полностью с системой Entra Pass или какой-либо другой системой контроля доступа. Связь с этим устройством организуется через Corporate шлюз для программирования и мониторинга. К KTES можете также подключать контроллеры (KT-100, KT-300 и KT-400). Для получения более подробной информации, касаемо инсталляции и программирования, смотрите инструкцию на KTES, DN1769 и Инструкция на программирование KTES, DN1770.

Автоматическая установка (Express Setup). Программа "Express Setup" позволяет установщикам автоматически описывать и конфигурировать большинство стандартных компонентов системы. Это значительно сокращает время установки и снижает число ошибок при настройке системы. Результатом автоматической установки является полнофункциональная система, готовая к тестированию оборудования и схем соединений. Установщику остаётся лишь внести определенные изменения, необходимые для определённого объекта.

EntraPass WebStation. Программное обеспечение EntraPass WebStation предназначено для управления системой с удаленного рабочего места оператора, подключенного через WEB. Кроме того, EntraPass WebStation позволяет в ручном режиме управлять дверьми, реле, inputs (входами), получать отчеты (в форматах .PDF, CSV, XLS, TXT), а также создаёт визуальное представление системы. Интерфейс программы идеально подходит для предоставления функций управления системой контроля доступа персоналу службы безопасности, секретарям и руководителям и не требует полной загрузки рабочей станции EntraPass. EntraPass WebStation предусматривает возможность авторизации пользователей, которые назначены в программном обеспечении. Для более подробной информации относительно установки и настройки программного обеспечения EntraPass WebStation смотрите инструкцию *Installation Manual,* DN1864 и *User Manual,* DN1709.

Функция управления лифтами. EntraPass позволяет запрограммировать до 64 этажей на каждую лифтовую кабину, используя контроллеры KT-300 с модулями расширения KT-PC4216, или до 16 этажей при использовании контроллеров KT-300 с модулями KT-PC420; или контроллеры KT-400 с модулями KT-MOD-OUT16, KT-MOD-INP16 или KT-MOD-REL8. Эта функция незаменима в тех случаях, когда разные этажи здания сдаются в аренду разным арендодателям, и таким образом, удаётся ограничить доступ идентификационных карт на определённые этажи.

Badging Встроенная функция изготовления электронных пропусков. Система EntraPass оснащена программными средствами для создания и печати электронных пропусков. Данная функция позволяет импортировать фотографии и подписи сотрудников или с помощью соответствующих устройств захватывать изображения и накладывать его на карты для последующей печати.

Интерактивные планы этажей. EntraPass позволяет загружать и отображать графические схемы высокого разрешения, созданные при помощи систем САПР (с конвертацией в формат .jpg or .bmp), то есть позволяет работать с графическим представлением системы. В поэтажные планы можно добавить интерактивные пиктограммы, отображающие статус компонентов системы и позволяющие осуществлять полное управление этими компонентами вручную в режиме реального времени.

Настраиваемые операторами рабочие столы. При работе с системой EntraPass каждый оператор может использовать до 8 настраеваемых рабочих столов. На этих рабочих столах располагаются окна с сообщениями о событиях, фотографиями сотрудников, отфильтрованные события, видео от камер и планы высокого разрешения, а также тревожные сообщения в рамках всей системы. Окна на рабочем столе могут располагаться в любой комбинации.

Установление связи с внешними охранными панелями. Контроллеры KT-100, KT-300 и KT-400 обеспечивают постановку/снятие с охраны внешней сигнализации, и включая задержку на постановку под охрану внутри Corporate Gateway. Это позволяет легко интегрировать EntraPass с внешними охранными панелями.

Partitioning Alarm System. С EntraPass Global Edition, объект может быть разделен на 100 тревожных зон\разделов. Каждая зона может быть настроена с любым количеством считывателей, дверных контактов, детекторов движения, сирен, уровней доступа и расписаний по снятии и постановки на охрану.

Учёт рабочего времени. Функция учёта рабочего времени является низкозатратной альтернативой дорогостоящим специализированным системам. Табели учёта рабочего времени в формате CSV можно выводить на печать или загружать в систему начисления заработной платы.

Muster Report (отчеты в экстренных ситуациях).Управление парковками. Muster report (отчеты о сборе людей) в Entra Pass позволяют формировать отчеты, которые используются в экстренных

ситуациях, где необходимо знать местоположение всех людей, находящихся в областях. Система знает сколько людей находится в определенной области. Muster отчеты автоматически выводятся на печать или по тревожному событию. Иконка области на рабочем столе динамически изменяется, когда область пустая. Данная функция может быть также быть использована. Например, парковка закрывается при достижении определенного количества автомобилей.

Визуальная диагностика. EntraPass обеспечивает графическое отображение компонентов системы на экране в режиме реального времени и оперативно обновляет их статусы, а также позволяет импортировать из других графических программ и выводить на экран планы помещений. Графические схемы высокого разрешения можно дополнить интерактивными пиктограммами, которые будут отображать статус компонентов системы в реальном времени. Такое графическое представление системы в режиме реального времени позволяет выполнять операции ручного управления, используя интерактивную графику.

Улучшенная интеграция с системами видеонаблюдения. В ответ на общую тенденцию возрастания роли видео в системах контроля доступа изготовитель предусмотрел в конфигурациях EntraPass Corporate и EntraPass Global возможность видеонаблюдения в режиме реального времени. Прикладной программный интерфейс (API) обеспечивает интеграцию EntraPass с цифровой системой видеонаблюдения Intellex® производства компании American Dynamics для просмотра "живого видео" и сделанных ранее видеозаписей. В программе предусмотрена возможность привязки видеороликов к "живому видео" или записанным видеофрагментам к событиям контроля доступа. Можно привязать запись видеоизображения к событиям, относящимся к нарушению порядка доступа, и записать изображения, передаваемые с одной или с нескольких камер наблюдения (не более 16 камер), одновременно с разных систем Intellex. Предустановки, последовательности, контроль скоростных купольных камер, просмотр в режимах 1x1, 2x2, 3x3, и 4x4 – это все доступно через программный продукт EntraPass. К каждой камере можно обращаться напрямую щелчком по её пиктограмме на поэтажном плане. Операторы могут настраивать параметры просмотра изображения из интерфейса EntraPass.

Видеохранилище EntraPass Video Vault. Этот инструмент позволяет автоматически

сохранять все видеофрагменты, полученные от тревожных записей Intellex или тревожных событий EntraPass, в файлы формата .AVI (Audio Video Interlaced), .KVI (Kantech Video Intellex), .KVA (Kantech Video Archive) или видеоформата .IMG (формат программы Network Client компании American Dynamic), и при необходимости защищать эти файлы паролем. Каждое видеохранилище EntraPass Video Vault можно подключить ко всем зарегистрированным в системе EntraPass устройствам Intellex. Видеофрагменты можно сохранять на максимум 24 жёстких дисках. Каждый видеофрагмент автоматически сопровождается bmp-изображением, а первый кадр видеофрагмента может быть использован для создания пиктограммы.

Редактор языков. Простая и удобная программа для перевода терминов меню на любой язык по выбору. В заводской поставке система Entrapass доступна на английском, французском, испанском, немецком и итальянском языках. Редактор языков позволяет перевести меню на 99 языков.

Интеграция с охранной сигнализацией. дополнение к ручному управлению охранной сигнализацией. Полный доступ виртуальной панели вложенной в KT-400. Прозрачный механизм на KT-400 связывает управление панели (Panel Manager) шлюза с DLL панели. Режим автоматического детектироания данных от оборудования охранной панели помогает оптимизировать получение данных. Новый параметр событий также добавлен для поддержки многих команд из панели.

Руководство и справочная система EntraPass

Пользование справочным руководством

Справочное руководство предназначено для специалистов по установке, системных администраторов и пользователей системы EntraPass. Доступен печатный экземпляр руководства, а также электронная версия в формате pdf.

Обращение к справочной системе

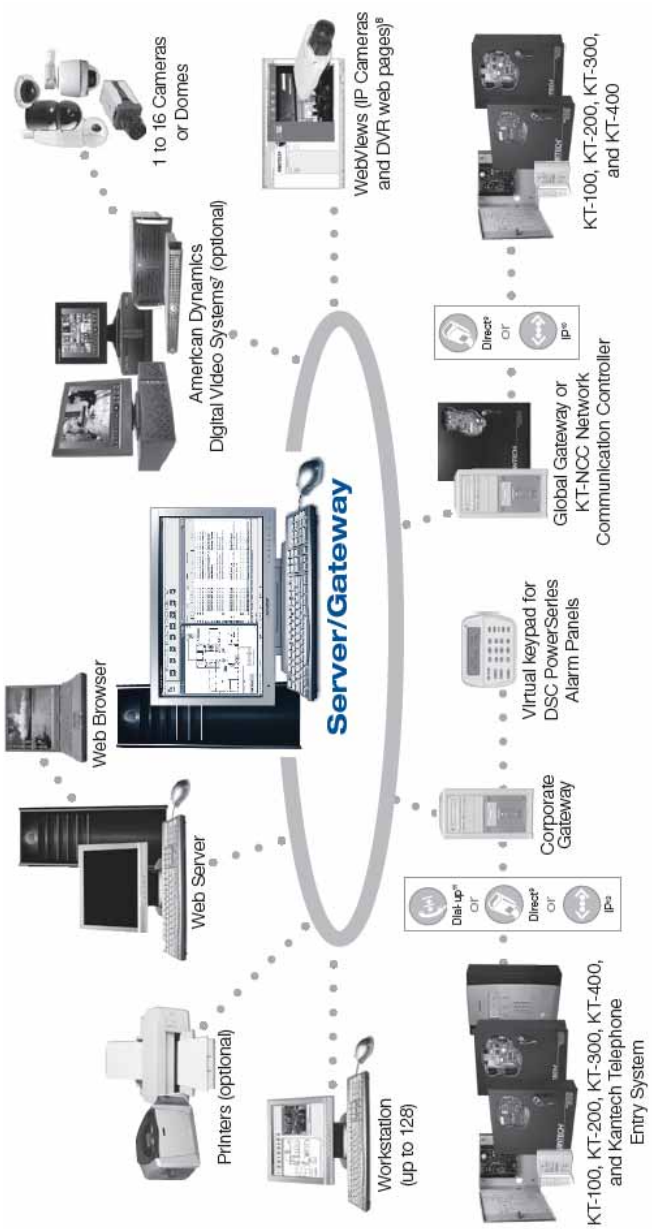
Многоуровневая система подсказок обеспечивает получение мгновенной контекстно-зависимой помощи. Для вызова подсказки, привязанной к активному окну,нажмите на клавиатуре клавишу **[F1]** или выберите в строке меню пункт **Help > Contents.** Для обращения к справочной системе можно воспользоваться клавишей **Help**, доступной во всех окнах программы. Кроме того, при нажатии на правую кнопку мыши на экране появляется всплывающее меню для быстрого вызова команд или файл справки к активному окну.

Техническая поддержка

Если Вы не смогли найти ответ на свой вопрос в этом руководстве или в статьях справочной системы, рекомендуем обратиться к специалистам, устанавливавшим Вашу систему. Хорошо зная конфигурацию Вашей системы, они смогут ответить на любые Ваши вопросы. Для получения дополнительной информации обращайтесь в местную службу технической поддержки по телефонам, указанным ниже в таблице.

Страна/Регион	Контактные телефоны	Часы работы (пн-пт)	Email
бесплатный по Северной Америке 1 888 222 1560 (GMT -05:00)			
US and Canada	+450 444 2030	8:00 to 20:00	kantechsupport@tycoint.com
Europe Toll Free +800 CALL TYCO / +800 2255 8926 (GMT +01:00)			
Бахрейн	+800 04127	8:00 to 18:00	tfsemea.support@tycoint.com
Франция	+33 04 72 79 14 83		
Греция	+00 800 31 22 94 53		
Россия	+8 10 800 2052 1031		
Испания	+900 10 19 45		
Турция	+00 800 31 92 30 37		
Объединённые Арабские Эмираты	+800 0 31 0 7123		
Великобритания	+44 08701 ADT SUP / 44 08701 238 787 : +31 475 352 722		

Системная диаграмма



Глава 2 • :Установка программного обеспечения

Перед любой установкой убедитесь, что компьютеры, на которых будет установлено программное обеспечение, удовлетворяют необходимым требованиям. Для получения информации по оборудованию, устанавливаемому вместе с программным

обеспечением, обращайтесь к сопроводительной документации на это оборудование. В данной главе содержатся сведения по программному обеспечению EntraPass, а именно:

- • Системные требования к компьютеру
- • Установка и обновление программного обеспечения

В зависимости от конфигурации системы, к оборудованию, которое будет использоваться вместе с программным обеспечением EntraPass, предъявляются разные требования.

Рекомендуемые системные требования

Перечисленные ниже требования справедливы для первичного и резервного сервера EntraPass, видеохранилища Video Vault, интерфейса Oracle/MS-SQL (Card Gateway), шлюза Windows Gateway, интерфейса SmartLink и рабочей станции. Убедитесь, что компьютер, на который Вы устанавливаете ПО, удовлетворяет следующим требованиям:• Операционные системы: Windows 2000, XP Pro, Server 2003, Server 2008, Vista и Windows 7 Pro 32-бит с последним Service Packs **(Примечание)**

Примечание: *Поддерживается только 32 битная система..*

- • Процессор: Pentium IV с тактовой частотой 1,8 ГГц
- • Оперативная память (RAM): 1 Гб
- • Минимальное свободное место на диске: 20 Гб
- • Глубина цвета: 24 бита (16 млн. цветов), требуется только для функции интеграции видеосигнала *Video Integration*
- • Разрешение экрана: 1024 x 768
- • AGP или PCI Express графическая карта с памятью 64 Мб и поддержка Direct X 9.0
- • Привод CD-ROM: 48X
- • Сетевая интерфейсная плата: сетевой адаптер 10/100 Base-T

Примечание: *Для использования функции интеграции с видеонаблюдением и операционных систем Vista настоятельно рекомендуется использовать, как минимум, двухядерный процессор с оперативной памятью не менее 2 Гб. В каждом конкретном случае выставляемые требования зависят от используемой операционной системы и конфигурации.*

Сервер EntraPass WebStation

- • Операционные системы: Windows 2000, XP Pro, Server 2003, Server 2008, Vista и Windows 7 Pro 32-бит
- • Установка самых последних пакетов обновления Windows и важных обновлений
- • Процессор: Pentium IV с тактовой частотой 1,8 ГГц
- • Минимальное место на диске: 10 Гб
- • Оперативная память (RAM): 1 Гб
- • Microsoft Internet Information Services (IIS) версии 5.0 или выше с последними
- обновлениями для системы безопасности
- • Microsoft .NET Framework 2.0 с последними обновлениями для системы безопасности
- • На клиентском компьютере должен быть установлен Adobe Flash Player 9.0, если необходим доступ к веб-страницам.
- Более подробные сведения по установке и настройке EntraPass WebStation содержатся в справочном руководстве "*EntraPass WebStation User Manual*, DN1709 и "*Installation Manual*, DN1864.

Рабочая станция и Шлюз с NCC

- Только операционная система Windows® 98 (требуется DOS для программирования NCC) не совместим с другими операционными системами
- Процессор Pentium III 450 MHz (минимум)
- 64 MB RAM (128 MB рекомендуется)
- Жесткий диск 2 GB (минимум)
- 17” монитор с разрешением (1024 x 768 минимальное разрешение)
- Видеокарта 4 MB
- 10/100 MBPS Ethernet TCP/IP

Только NCC8000 или DOS приложения

- Версия DOS 6.22 или выше (требуется DOS для Global Gateway). Не будет запускаться из под Windows
- Процессор Pentium III 450 MHz (минимум)
- 64 MB RAM (128 MB рекомендуется)
- Жесткий диск 2 GB (минимум)
- Требуется память EMS

Дополнительные требования

Для выполнения различных задач может потребоваться следующее оборудование:

- • **Плата для оцифровки изображений -** позволяет оцифровывать фотографии пользователей и использовать их для идентификационных карт
- • **Звуковая карта** - для формирования звуковых сигналов в случае тревоги
- • **Принтер электронных пропусков -** для печати электронных пропусков (Badging)
- • **Устройство оцифровки подписей -** служит для оцифровки подписей (для изготовления электронных пропусков)
- • **Принтер событий -** (матричный или лазерный) для печати событий (сообщений и тревог)
- • Принтер отчётов - (лазерный) для печати отчётов

Установочный комплект

Установочный комплект EntraPass состоит из компакт-диска CD-ROM и справочного руководства DN1316 (*Reference Manual*). Кроме того, в него входит комплект **CBLK-10**, состоящий из 30-метрового кабеля RS-232 с соединителями RJ-12, а также адаптеров DB9F -RJ-12 (740-1023) и DB9M - DB25F (740-1041). Установочный диск позволяет устанавливать основные компоненты системы EntraPass:

- • 1 приложение-сервер (Server)
-
- • 1 рабочая станция APM сервера и 4 Дополнительных рабочих станций APM. (APM – это рабочая станция, Workstation)
-
- • 1 Global шлюз

Примечание: *Каждое приложение Global шлюз также включает в себя один Corporate шлюз, при условии, что включена функция двойного шлюза.*

-
- Интерфейсы SmartLink и SmartLink Network
- • Программа просмотра отчётов (Report Viewer)
- • Редактор языков (Vocabulary Editor)
- Совместимость с KT-NCC
- • Программа обнаружения устройств в сети (KT-Finder)

Установочный компакт-диск может также содержать дополнительные опции. Для них требуется дополнительная лицензия:

- • 8 дополнительных приложений Рабочая станция APM(максимум 128 +1)
-
- • 16 NCC 8000 Gateway, 16 Global Gateway, до 40 приложений Corporate Gateway.
-
- • Приложение Mirror Database and Redundant Server (Зеркальная база данных на резервном сервере)
- • Приложение Видеохранилище (Video Vault)
- • Интерфейс Oracle/MS-SQL для программы MS/SQL
- • Рабочая станция через web (EntraPass WebStation)

Примечание: *Установку дополнительных опций следует выполнять только после регистрации сервера EntraPass Server. Для них требуется дополнительная лицензия.*

Мастер установки

Мастер установки InstallShield Wizard проведёт Вас шаг за шагом через все этапы установки. **Таблица 2-1** отображает различные сценарии установки.

Таблица 2-1: Лист процедур для Entra Pass

Процедуры	Страница
1- Установка EntraPass (новая установка)	**13**
2- Дополнительные компоненты системы EntraPass	**23**
3- Переход на другое программное обеспечение SE-CE-GE	**32**
4- Обновление на новую версию	**34**
5- Удаление программного обеспечения EntraPass	**38**

Установка EntraPass (новая установка)

Для установки и запуска системы необходимо выполнить всего три действия! Для установки требуется:

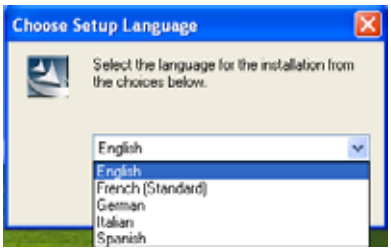
1. Установить программное обеспечение, указав код **System Installation Code** с установочного компакт-диска.
2. Выполнить регистрацию системы с помощью кода **Registration Confirmation Code** (Код подтверждения регистрации), предоставленного службой обслуживания клиентов Kantech (Kantech Technical Support). Установить первые компоненты, входящие в комплект установки (пятьприложений Рабочая станция и 1 шлюз; первая рабочая станция устанавливается автоматически во время установки сервера EntraPass).

Примечание: *Программное обеспечение нормально функционирует даже без регистрации. Однако незарегистрированная версия работает только с десятью идентификационными картами. Кроме того, в случае бездействия системы и неиспользования клавиатуры в течение 1 часа выполняется автоматическая разрегистрация. Если произошла автоматическая разрегистрация, то пользователи должны ввести 20-значный пароль в жёлтом окне, отображаемом в нижней части экрана.*

ПРИМЕЧАНИЕ: *В течение установки Севера EntraPass Global, вам будет предложено установить Глобальный шлюз «Global Gateway» и SmartLink. Все компоненты могут быть установлены на один и тот же компьютер.*

Установка системы

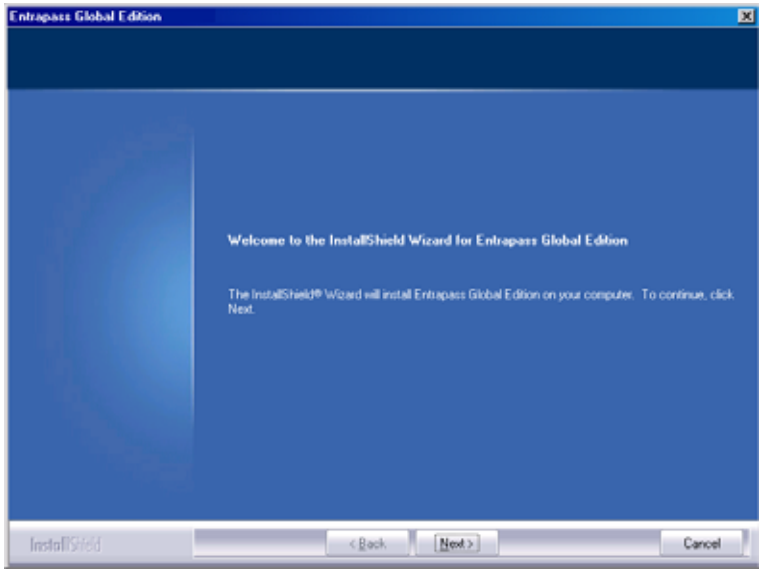
1. Перед началом установки следует убедиться, что ни одно приложение EntraPass не запущено в данный момент времени.
2. Установите компакт-диск в привод CD-ROM компьютера. Если в настройках компьютера разрешён автоматический запуск, программа инсталляции запускается автоматически. Если этого не произошло, следует войти в меню Start > Run и запустить файл D:\Setup.exe (где D: - имя CD-ROM привода).
3. Первым открывается окно **Choose setup language** для выбора языка меню в программе настройки. По умолчанию установлен английский (English)



ПРИМЕЧАНИЕ: *Язык меню в мастере настройки (InstallShield) невозможно будет изменить потом, в частности, при установке обновлений или других компонентов EntraPass. Для того чтобы изменить язык меню в программе настройки, необходимо удалить и заново установить ПО.*

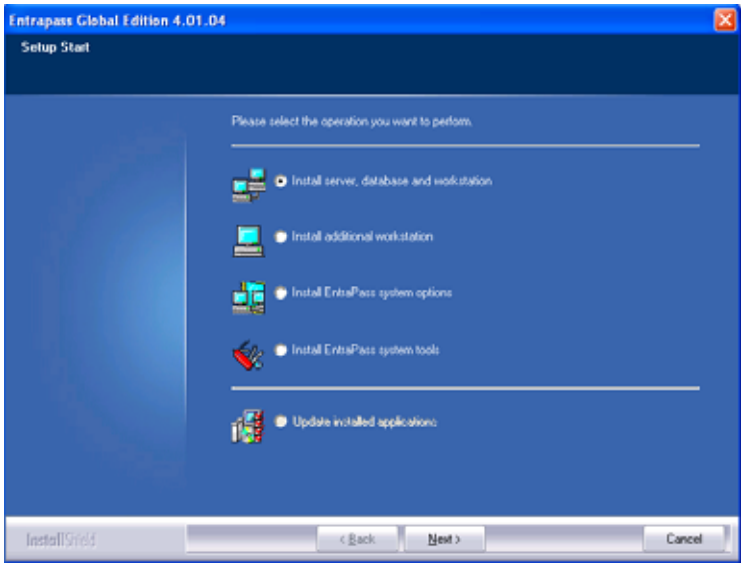
ПРИМЕЧАНИЕ: *Язык, используемый в системе и базах данных, зависит от языка, выбранного при установке ПО. Например, если при установке указан английский (English), он будет использоваться по умолчанию при запуске системы. Для изменения языка системы и базы данных необходимо будет зайти на сервер EntraPass Server и рабочую станцию EntraPass Workstation.*

4. Нажать **OK.** При этом откроется окно приветствия.



- • Все окна в программе инсталляции выглядят аналогично окну приветствия. •
  - В верхнем левом углу отображается версия устанавливаемого программного обеспечения.
  - В центральной части окна появляются указания, которым Вы должны следовать во время установки. При нажатии кнопки **Next** (Далее) инструкции автоматически обновляются.
  - В нижней части окна находятся кнопки **Back** (Назад) и **Next** (Далее), которые служат для перехода от одного шага установки к другому вперёд или назад, чтобы исправить ранее введённый параметр.
  - Кнопка **Cancel** служит для отмены инсталляции программы на любом её этапе.

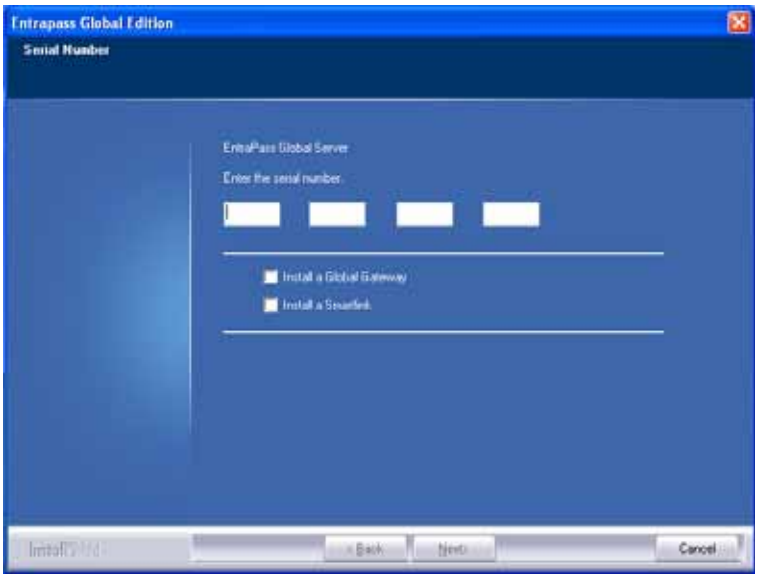
5 Нажать **Next** для продолжения процесса установки ПО. При этом откроется окно Setup Start (Начало установки).



6 Здесь нужно выбрать, какие компоненты системы следует установить. Первые четыре пункта предназначены для установки нового оборудования, а последний (пятый) пункт служит для обновления установленного ПО. Если программа устанавливается впервые, для выбора будет доступна только одна из опций. Рекомендуется указать сначала первый пункт из списка.

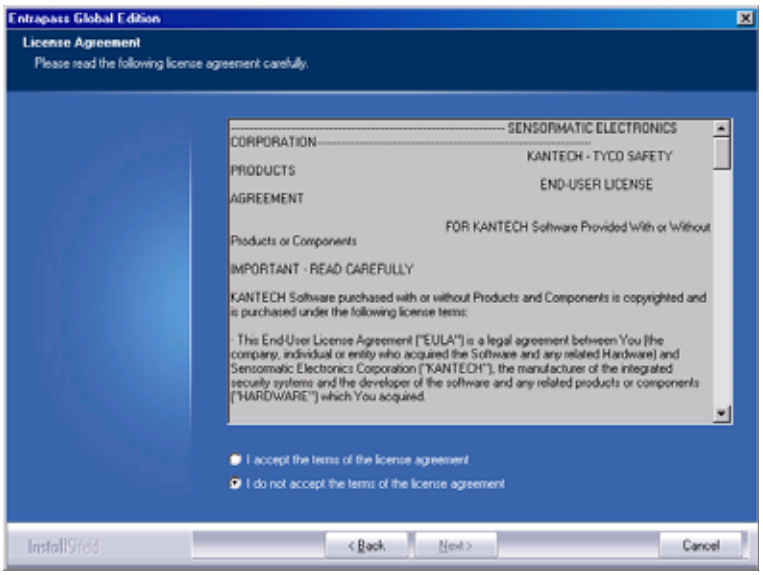
- **Install Server, Database and Workstation** (Установить сервер, базу данных и рабочую станцию)**:** Эта опция будет устанавливать систему EntraPass Global Edition. Этот пункт будет неактивным, если перечисленные компоненты уже установлены.
- **Install Additional Workstation** (Установить дополнительную рабочую станцию). Выберите эту опцию, чтобы установить дополнительную рабочую станцию. Этот пункт будет неактивным, если сервер или рабочая станция уже установлена на этом компьютере.
- • **Install EntraPass System Components** (Установить компоненты системы). Служит для установки опций и дополнительных компонентов Entra Pass, таких как, шлюзов (Gateways), веб-станций (WebStations), интерфейса SmartLink, видеохранилища (Video Vault), интерфейса Oracle/MS-SQL и лицензию резервного сервера (Mirror Database and Redundant Server) и пр. *Этот пункт будет неактивным, если перечисленные компоненты уже установлены на этом компьютере.*
- **Install EntraPass System Tools** (Установить служебные программы). Служит для установки утилит EntraPass: редактора языков (Vocabulary Editor), программу просмотра отчётов (Report Viewer), программу просмотра видеоклипов (Video Viewer), сетевого интерфейса SmartLink и др. Эти пункты будет неактивным, если перечисленные компоненты уже установлены на этом компьютере.
-
- **Update Installed Applications** (Обновить установленные приложения): Этот пункт будет неактивным, если система ещё не установленаю. Для обновления вашей системы Entra Pass , *см. "Обновление системы EntraPass" на стр. 34*.

7 Нажать **Next** для продолжения работы. При этом откроется окно Serial Number (Серийный номер).



8 Указать серийный номер сервера EntraPass Global Server or Software. Эта информация указана на обложке компакт-диска. При вводе цифр будьте внимательны! Кнопка **Next** станет доступной только после правильного ввода серийного номера.

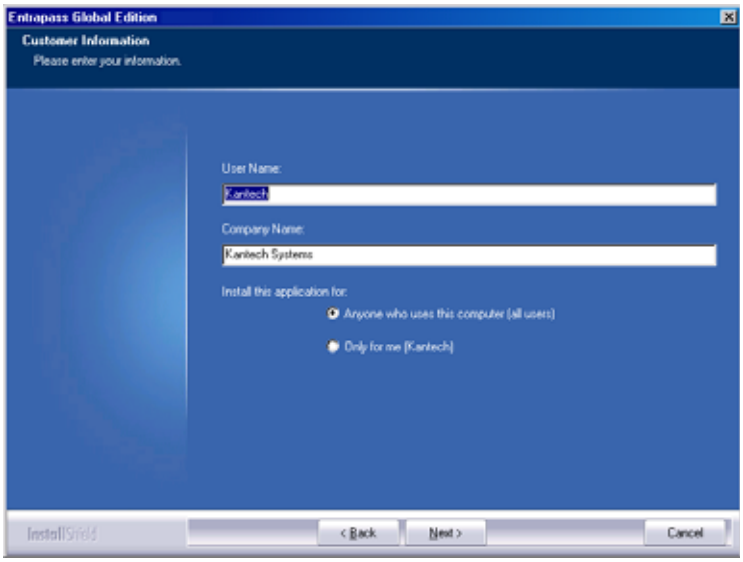
9 Нажать **Next** для продолжения работы. На экране появится Лицензионное соглашение с конечным пользователем ПО.



10 Поставить галочку напротив пункта **I accept...** (Я согласен), чтобы подтвердить свое согласие со всеми пунктами лицензионного соглашения. Или выделить пункт **I do not accept...** (Я не согласен), чтобы отменить установку.

ПРИМЕЧАНИЕ: *В случае несогласия с пунктами лицензионного соглашения завершить установку будет невозможно. Кнопка* **Next** *станет активной только после установки флажка напротив* **I accept..**

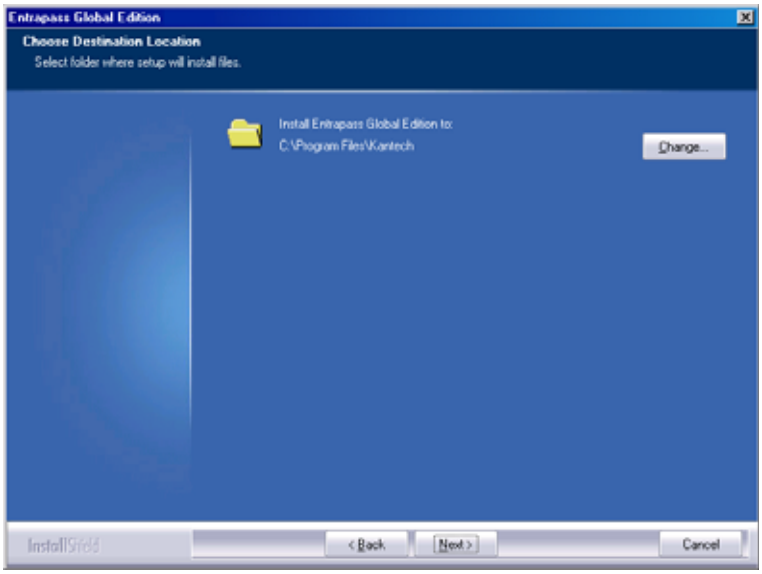
11 Нажать **Next** для продолжения работы. На экране появится окно Customer Information (Сведения о заказчике).



12 Введите имя пользователя в поле "**User name**" и название компании в поле "**Company Name**".

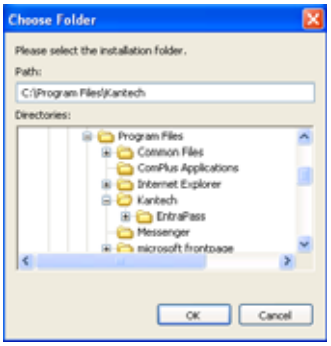
13 Ниже следует указать уровень доступа. Опция "**Anyone** who will use this computer" – доступ любому пользователю данного компьютера. Опция "**Only** for me" – доступ только для того пользователя, который в данный момент зарегистрировался в системе.

14 Нажать **Next** для продолжения работы. При этом откроется окно Choose Destination (Выбрать путь установки).

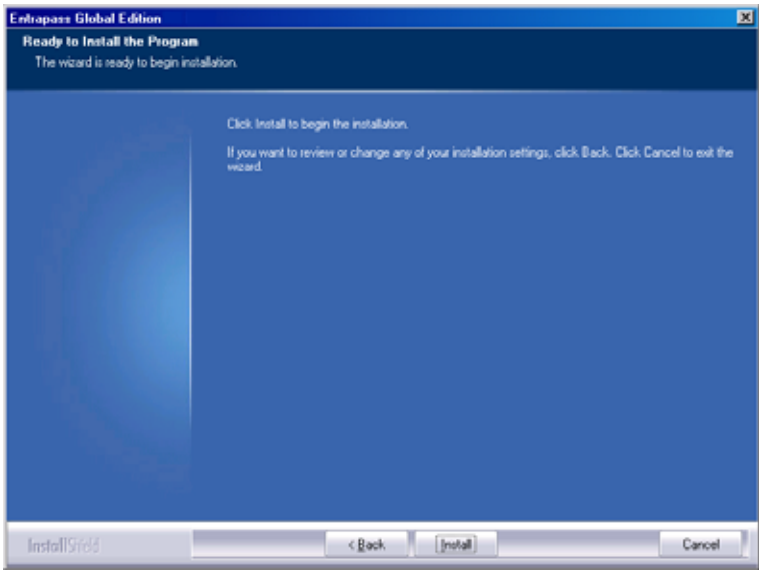


15 Пользователь может выбрать путь по умолчанию и нажать **Next** или указать другой путь.

- Чтобы указать другой путь установки приложения, следует нажать **Change** (Изменить). В таком случае откроется новое окно, в котором нужно указать другой путь установки.
- Для этого можно набрать нужные символы с клавиатуры в верхнем поле или двойным щелчком мыши выбрать нужные каталоги и подкаталоги в нижнем поле. Нажать **Ok**. Указанный путь отобразится в окне Choose Destination Location.

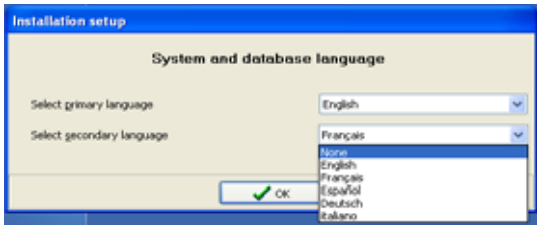


16 Нажать **Next** для продолжения работы. Откроется окно Ready to Install the Program (Готовность к установке программы).



17 Если необходимо изменить какие-то из выбранных ранее параметров, следует нажать **Back**. Если все готово к установке, нажать **Next**. Начинается установка.

18 Во время установки необходимо будет указать два языка в полях **Select primary language** (Основной язык) и **Select secondary languages** (Дополнительный язык). Это меню служит для выбора языка, который используется при построении базы данных, а также языков, используемых при работе с системой EntraPass.



19 Нажать **OK**. Установка продолжается.

20 Во время установки пользователю будет предложено установить: **intellex API,**

- Если необходим Intellex API (программный интерфейс Intellex, нажмите **Yes** и следуйте инструкциям. .•EntraPass WebStation,
  - •Если программа WebStation ещё не установлена, нажмите Yes и следуйте инструкциям.
  - • Если WebStation уже установлена, нажмите No.

ПРИМЕЧАНИЕ: *При процессе обновления WebStation автоматически будет создан backup существующей версии.Папка backup EntraPass WebStation расположена здесь:*

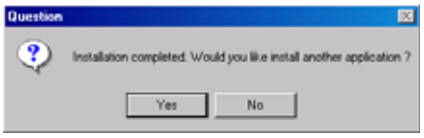
- C:\Inetpub\wwwroot\EntrapassWebStation\Backup\YYYY-M-DD_H-MM\EntraPassWebStation

21 После того как выбранные опции установлены, система предлагает ознакомиться с файлом Read Me. Кроме того, в открывшемся окне можно выбрать установку приложений в режиме службы Windows (Windows service). Приложения, используемые в режиме службы Windows,

автоматически запускаются при загрузке системы, даже если последнее завершение работы было некорректным.

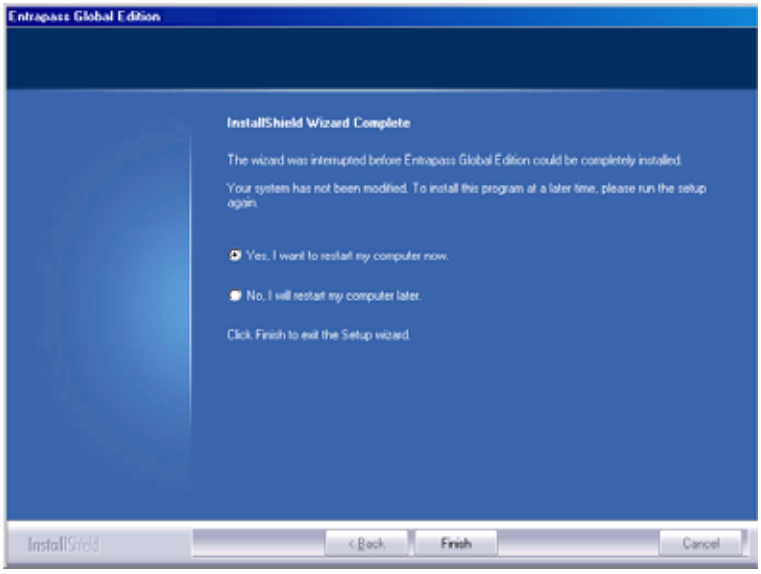
22 Нажать **Next** для продолжения работы. Система проверит, есть ли другие доступные для установки приложения или утилиты. При их обнаружении на экране появится соответствующее сообщение.

- Для того чтобы установить другие приложения, нажмите **Yes** и повторите действия с п.4.



ПРИМЕЧАНИЕ: *Если устанавливаемое приложение требует ввести серийный номер, следует обратиться в службу технической поддержки Kantech и зарегистрировать систему до выполнения любых дальнейших действий : см. "Регистрация системы" на стр. 21.*

- Если установка завершена, и устанавливать другие приложения не требуется, следует нажать **No** (Нет). На экран будет выведено окно завершения работы мастера установки (InstallShield Wizard Completed).



23 Вы можете выбрать Yes, чтобы выполнить перезагрузку компьютера сразу, или No, чтобы сделать это чуть позже.

24 Извлечь компакт-диск из CD-ROM привода.

25 Для завершения установки нажать **Finish.**

ПРИМЕЧАНИЕ: *После завершения установки обязательно нужно перезагрузить компьютер.*

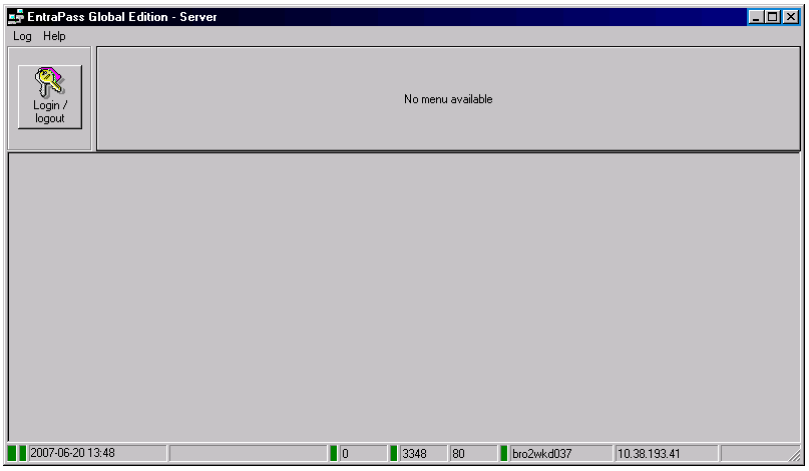
26 Следующим шагом будет обращение в службу технической поддержки Kantech для получения кода регистрации для разных компонентов системы. Следуйте инструкциям в следующем разделе руководства.

Регистрация системы

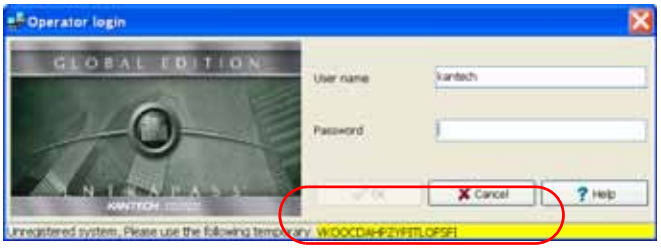
Рекомендуется как можно быстрее зарегистрировать систему, чтобы пользователи получили возможность установить дополнительные опции и работать с программой без ограничений. Фактически система функционирует даже без регистрации, но в усечённом варианте, только с 10-ю идентификационными картами. Кроме того, пока система не зарегистрирована, сеанс работы операторов завершается после каждого часа бездействия, и для возобновления работы им необходимо каждый раз вводить случайно генерируемый 20-символьный пароль.

Регистрация системы

1 Запустить сервер щелчком мыши по ярлыку **Server** на рабочем столе. Или для запуска сервера использовать меню "Пуск" (Start)в среде Windows®: (**Start** > **EntraPass Global Edition > Server > Server)**

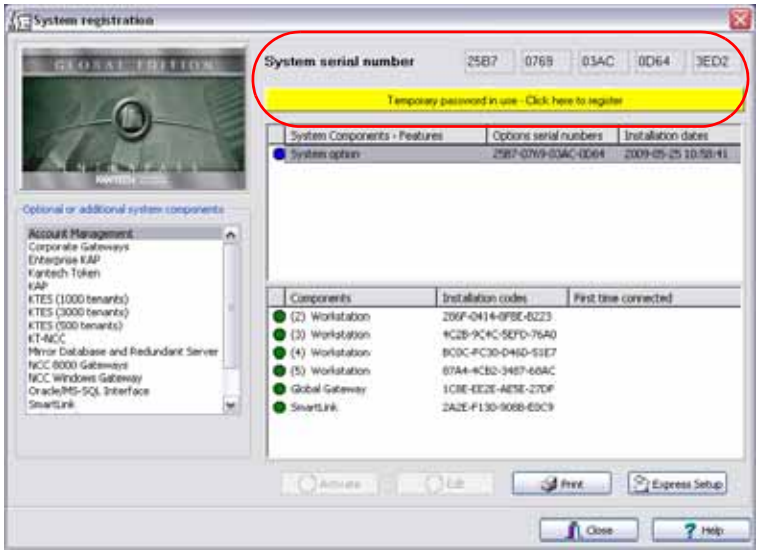


2 Нажать кнопку Login (Регистрация)/ Logout(Завершение сеанса). Открывается окно Operator Login (Регистрация оператора).

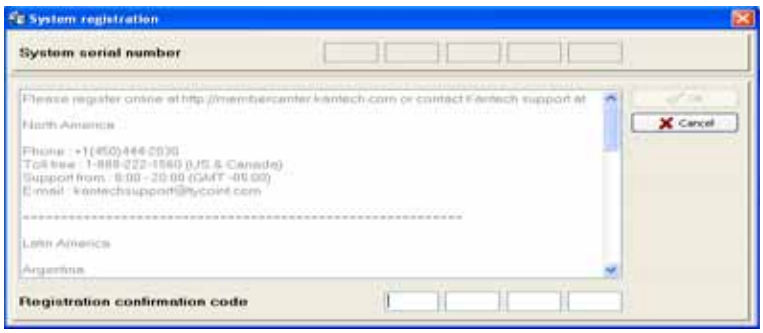


3 В поле **User name** ввести имя Kantech (регистр не учитывается). Ввести временный 20-символьный пароль, отображаемый в нижней части окна (временный пароль отображается лишь

в только что установленных программах и выделяется жёлтым цветом). Открывается окно регистрации System registration.

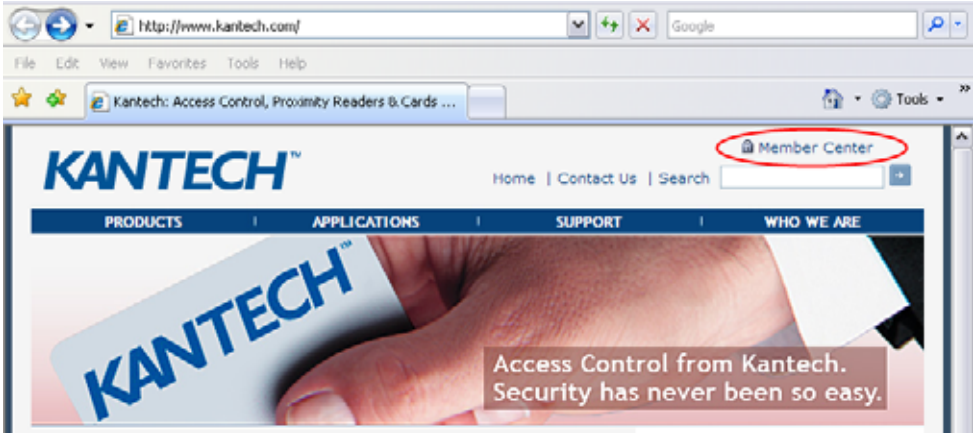


4 Нажать жёлтую кнопку **Temporary password in use (...)(использовать временный пароль),** чтобы зарегистрировать систему. Кнопка отображается лишь в только что установленных программах. Открывается окно регистрации System registration.



ПРИМЕЧАНИЕ: *Существует два способа регистрации новой системы: онлайновая регистрация на сайте www.kantech.com и получение кода регистрации в местной службе технической поддержки Kantech.*

5 Зайти на сайт www.kantech.com и нажать кнопку **Member Center.**



ПРИМЕЧАНИЕ: *Если Вы ещё не являетесь партнёром компании, подтвердите свое желание им стать, и дождитесь электронного письма с подтверждением о включении Вас в список партнёров (1-2 рабочих дня).*

6 Выбрать раздел Kantech Registration.

7 В поле **System Serial Number** ввести серийный номер системы и выполнить дальнейшие указания.

8 Вернуться в раздел **EntraPass System Registration** и указать код регистрации в поле **Registration Confirmation Code**, нажать **OK**. Кнопка **OK** активна только в том случае, если код регистрации введён правильно.

ПРИМЕЧАНИЕ: *В случае выхода из главного окна сервера без регистрации на экране появляется окно Change Authentication Password (Смена аутентификационного пароля). После регистрации системы это окно (Change Authentication Password) больше не отображается.*

Дополнительные компоненты системы EntraPass

После того как регистрация сервера выполнена, появляется возможность установки дополнительных компонентов системы. Это приложения EntraPass и другие утилиты, например, приложение Видеохранилище (EntraPass Video Vault). Перед началом установки компонентов системы необходимо убедиться, что компьютер, на который их устанавливают, удовлетворяет минимальным требованиям. Вам нет необходимости звонить в техническую поддержку для активации первых двух АРМ-ов и первого приложения Шлюза. Эти части уже находятся в базовом пакете.

1 В главном окне **сервера (Server)** открыть меню **Connection** (Соединения) (или в окне приложения типа Рабочая станция войти в меню **Options** (Опции), выбрать пункт **System Registration** (Регистрация системы). Открывается окно регистрации System registration.

ПРИМЕЧАНИЕ: *В комплекте с сервером EntraPass поставляются пять приложений типа Рабочая станция (Workstation) и одно приложение типа Global Шлюз (Global Gateway). Одно приложение типа Рабочая станция устанавливается автоматически во время установки сервера. Оно используется для настройки конфигурации. Оно не отображается на нижней панели, потому что его установка и регистрация выполняется автоматически. Для установки четырёх дополнительных приложений Рабочая станция требуется установочный компакт-диск и коды установки. Убедитесь, что компьютер, на который Вы устанавливаете ПО, удовлетворяет необходимым требованиям.*

2 Чтобы избежать ошибок при вводе кодов установки для рабочих станций и шлюза, не рекомендуется выписывать их на лист бумаги. Вместо этого лучше распечатать коды на принтере, нажав кнопку **Print.**

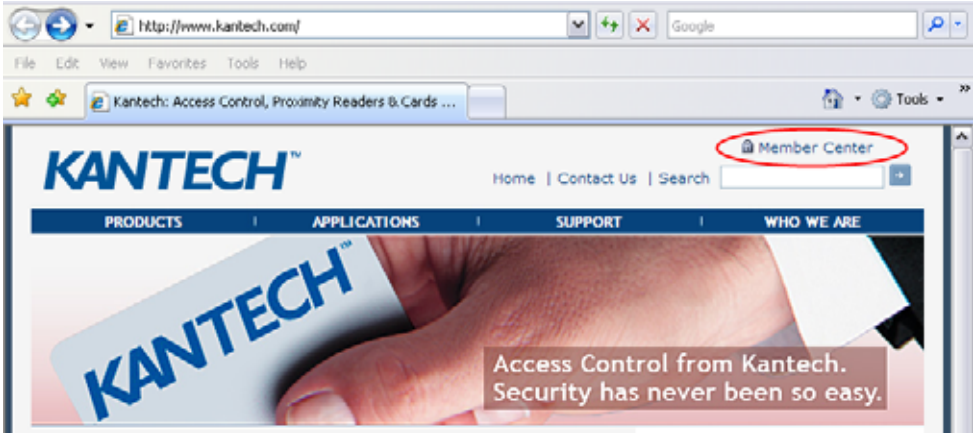
ПРИМЕЧАНИЕ: *При установке дополнительных опций (например, дополнительный шлюз Gateway) объекты при помощи программы автоматической настройки Express Setup.*

3 В окне **System registration** (Регистрация системы) указать, какой компонент будет устанавливаться. Затем на панели слева нажать кнопку **Click here to install component** (Нажмите для установки компонента). Открывается окно Component registration (Регистрация компонента), в скобках указывается название регистрируемого компонента.

4 Введите серийный номер компонента в поле **Option Serial Number** (серийный номер указан в на листке полученной лицензии)

ПРИМЕЧАНИЕ: *Существует два способа регистрации нового компонента: онлайновая регистрация на сайте* ***www.kantech.com*** *и получение кода регистрации в местной службе технической поддержки Kantech.*

5 Зайти на сайт www.kantech.com и нажать кнопку **Member Center** (Обслуживание партнёров).



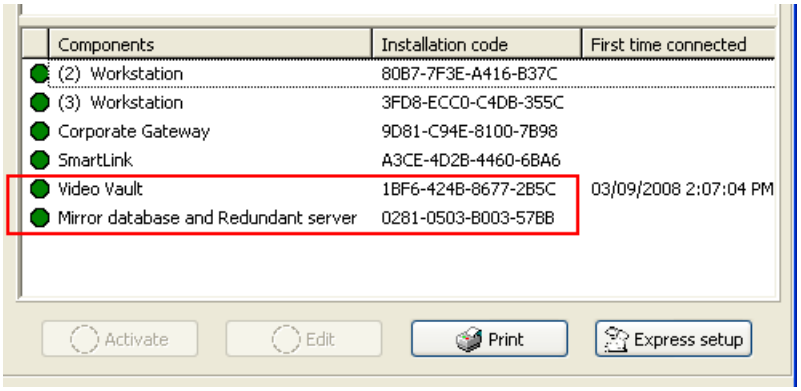
ПРИМЕЧАНИЕ: *Если Вы ещё не являетесь партнёром компании, подтвердите свое желание им стать, и дождитесь электронного письма с подтверждением о включении Вас в список партнёров (1-2 рабочих дня).*

6 Выбрать раздел **Kantech Registration** (Регистрация Kantech).

7 В поле **System Serial Number** ввести серийный номер системы и выполнить дальнейшие указания.

8 Вернуться в раздел **EntraPass Component Registration** (Регистрация компонента EntraPass) и указать код регистрации в поле **Registration Confirmation Code**, нажать **OK**. Кнопка **OK** активна только в том случае, если оба кода регистрации верны

ПРИМЕЧАНИЕ: *После ввода кода регистрации в поле Registration Confirmation Code система генерирует* ***Installation Code*** *(Код установки) в окне* ***System registration*** *(Регистрация системы). Синей меткой помечены уже созданные, но ещё не активированные компоненты. Зелёная метка стоит напротив уже активированных компонентов. Код установки (Installation Code) потребуется, когда Вы будете готовы установить компонент системы с компакт-диска EntraPass CD-ROM.*



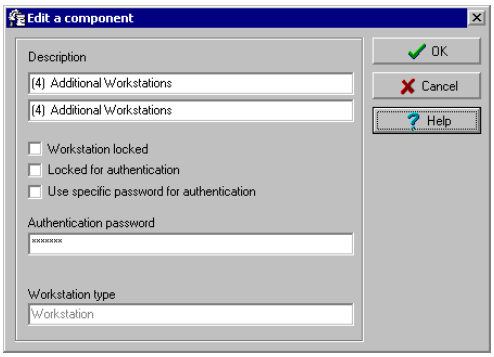
9 Повторите шаги с 3 по 8 для всех компонентов системы.

ПРИМЕЧАНИЕ: *Вам надо установить связь между сервером EntraPass и компьютером, где установлены новые опции\компоненты (если применимо). Исполняйте этот шаг только если вы установили компоненты\опции на другой компьютер, где была установлен АРМ (рабочая станция).*

Редактирование сведений о компонентах системы

EntraPass позволяет пользователю давать названия приложениям по своему желанию, что обеспечивает быструю идентификацию событий в системе. Кроме того, можно изменять названия компонентов в меню описания этих компонентов: **Devices** (Устройства) > **EntraPass Applications** (Приложения EntraPass).

Переименование приложений Entra Pass



1. В окне регистрации выбрать приложение и нажать кнопку **Edit.** При этом открывается окно редактирования (Edit a component).
2. В поле **Description** (Описание) укажите описание для выбранного приложения EntraPass. Если для работы с системой EntraPass используется два языка, рекомендуется создать два имени: одно на основном языке, а другое на дополнительном.
3. Проверить и установить при необходимости флажки напротив следующих опций:
   - **Workstation locked** (Заблокировать рабочую станцию). Выбрать эту опцию, чтобы установить приложение на компьютере и использовать его только для получения системных сообщений.
   - **Locked for authentication** (Блокировать аутентификацию). Выбрать эту опцию, чтобы компьютер, на котором установлено приложение EntraPass, не запрашивал аунтификацию.
   - **Use specific password for authentication** (Использовать особый пароль для аутентификации). Эта опция позволяет назначить особый пароль для данной рабочей станции. В случае выбора этой опции необходимо ввести аутентификационный пароль в поле Authentication password.

ПРИМЕЧАНИЕ: *В поле Application type отображается тип выбранного приложения EntraPass. Например, если выбрано приложение типа Шлюз (Corporate Gateway), то в этом поле отображается надпись "Corporate Gateway". Это же описание отображается в окне описания приложения (**Devices** (Устройства) > **EntraPass application** (Приложения EntraPass).*

Связь с сервером EntraPass

После того как приложение EntraPass установлено на компьютер, необходимо установить связь между этим компьютером и компьютером, который выступает в качестве сервера EntraPass. Изложенные ниже рекомендации помогут правильно настроить и организовать связь между АРМ (рабочей станцией) и сервером EntraPass.

ПРИМЕЧАНИЕ: Перед выполнением приведённых ниже указаний следует убедиться, что сервер подключён к сети. Если это не так, запустите сервер

Установление связи с сервером

1 В меню “Пуск” в операционной среде Windows® войти в меню **Programs > EntraPass Global Edition** > **EntraPass application** (приложения Entra Pass)> **Register to Server** (Зарегистрировать на сервере). Или непосредственно запустить приложение EntraPass, чтобы система автоматически запустила программу регистрации, когда приложение попытается подсоединиться к серверу.

ПРИМЕЧАНИЕ: *Окно регистрации появляется также в случае запуска приложения в момент, когда сервер EntraPass еще не подключён к сети. В такой ситуации следует просто запустить сервер EntraPass.*

2 Далее необходимо выбрать протокол обмена данными для связи сервера EntraPass и используемого приложения EntraPass. .

- **NetBEUI**: Протокол NetBEUI (NetBIOS Enhanced User Interface) использует имя компьютера для связи с другими устройствами. Здесь следует указать имя компьютера, на котором установлено программное обеспечение сервера EntraPass Server (имя чувствительно к регистру!). Имя активного компьютера отображается в строке состояний. Для поиска существующих имён компьютера можно воспользоваться кнопкой **Scan** (Поиск)**.**
- •**TCP/IP**. Введите TCP/IP адрес компьютера, на котором установлен EntraPass Server. TCP/IP адрес севера отображается в строке состояний сервера.
- • **Domain Name** (Имя домена). Здесь следует указать имя компьютера или рабочей группы, в которую входит сервер EntraPass Server.
- • **Local** (Локальный режим). Используется для регистрации компонента, если приложение устанавливается на том же компьютере, где установлен сервер

3 Поставьте флажок напротив пункта **Provide local TCP/IP address (обеспечить локальный TCP/IP адрес),** если рабочая станция EntraPass осуществляет связь с сервером EntraPass по виртуальной частной сети VPN (Virtual Private Network). Здесь необходимо указать IP-адрес, используемый сетью VPN (виртуальная частная сеть). Этот адрес предоставляет приложение

VPN, и чтобы узнать его, обычно достаточно щёлкнуть по свёрнутой пиктограмме VPN в правом нижнем углу экрана рядом с часами (так называемый "трей").

4 В поле **Authentication Password** (Аутентификационный пароль) можно указать особый пароль, которым будут пользоваться операторы для аутентификации АРМ (рабочих станций) на сервере EntraPass Server.

Установка внутреннего Global шлюза (NCC8000)

Под Windows® 98, приложение EntraPass и шлюз могут быть установлены на один компьютер. В этом случае следующие линии отражают файл Config.sys.

Правка файла Config.sys

1. Выберите Windows меню **Пуск/Start**. Выберите **Выполнить/Run**.
2. Введите в командной строке: **Sysedit**.
3. Из отображаемых файлов выберите CONFIG.SYS и введите следующие линии:
   - dos = high,umb
   - break = off
   - device = c:\WINDOWS\himem.sys
   - device = c:\WINDOWS\emm386.exe ram 592
   - files = 20
   - buffers = 20
4. Перезагрузите PC.

Установка внешнего Global шлюза (NCC8000)

Если глобальный шлюз установлен на другой компьютер, на котором нет шлюза, выполните следующие шаги:

1. Используйте различные компьютеры для выполнения этих шагов. Первое. Будьте уверены, что DOS v.6.22 или выше установлен на компьютере, который будет использоваться в качестве Global шлюз.
2. Соедените кабелем RS-232 COM порты двух компьютеров: где установлен шлюз и другой PC, на который будет устанавливаться Global шлюз.

ПРИМЕЧАНИЕ: *COM1 компьютера* ***Шлюзшлюз*** *соеденен с компьютером, на котором есть программное обеспчение. НЕЛЬЗЯ ИСПОЛЬЗОВАТЬ ДРУГИЕ COM ПОРТЫ. В ПРОТИВНОМ СЛУЧАЕ СВЯЗЬ РАБОТАТЬ НЕ БУДЕТ. В противном случае, если порт дефектный, то азамените компьютер.*

3. Создайте загрузочную дискету (под Windows 98). Для создания загрузочной дискеты: вставьте отформатированную дискету в A:\. С рабочегоо стола \Windows® двойным кликом нажмите на иконку **My Computer**. Из окна “Мой компьютер” нажмите правой кнопкой мыши на

, затем выберите “Формат” из выпадающего меню. В опциях Другие настройки “**Other Options”**, выделите **“Copy system files” копировать файлы системы**, затем нажмите кнопку **“Пуск”**.
4. Как только дискета отфарматирована и скопированы файлы системы, вы должны скопировать файлы (см. ниже) на загрузочную дискету.

ПРИМЕЧАНИЕ: *Не забудьте снять атрибут “только для чтения” со всех файлов. Для этого выделите все файлы, нажмите правую кнопку мыши, зайдите в свойства, Снимите поле “только для чтения”.*

5. Для определенных установок может быть необходимо загрузить следующие драйверы. Для того чтобы это сделать вы должны добавить следующие две линии в файл config.sys:
   - DEVICE = C:\DOS\HIMEM.SYS
   - DEVICE = C:\DOS\EMM386.exe

ПРИМЕЧАНИЕ: *HIMEM.SYS и EMM386.EXE это драйверы управления, используемые для свободной памяти - первые 640K памяти компьютера. Эти драйвера позволяют использовать столько памяти сколько им нужно. Это позволяет. Это позволяет использвать Global Шлюз столько памяти сколько ему нужно для необходимой работы. Это может быть необходимо загрузить эти драйвера, в противном случае могут происходить сбои в работе Global Шлюз. Например, это может быть причиной что ПО Global Шлюз не реагирует олжным образом или даже останавливает ответы на каки-либо запросы касаемые активации\деактивации реле. Загружая эти драйверы, вы расширяете область памяти, тем самым обеспечивая полноценную работу Global Шлюз. Даже несмотря на то, что эти проблемы не появяться при инсталяции, это необходимо чтобы предотвратить проблемы в будущем.*

6. Выньте дискету из PC. Выключите PC, где будет устанавливаться Global Шлюз. Вставьте загрузочную дискету. Включите PC. Установка будет происходить автоматически. Когда установка закончится, вы услышите 9 звуковых сигналов.
7. Выньте дискету. Перезагрузите компьютер. Global Remove the diskette, shut down the computer and reboot it. The Global Шлюз будет отображать устройства найденные на PC, на плате COM порт и KLEXP-08 COM порт платы расширения. Начните прокручивать сквозь различные baud rates в поисках Шлюза.

Настройка внешнего Global Шлюз (NCC8000)

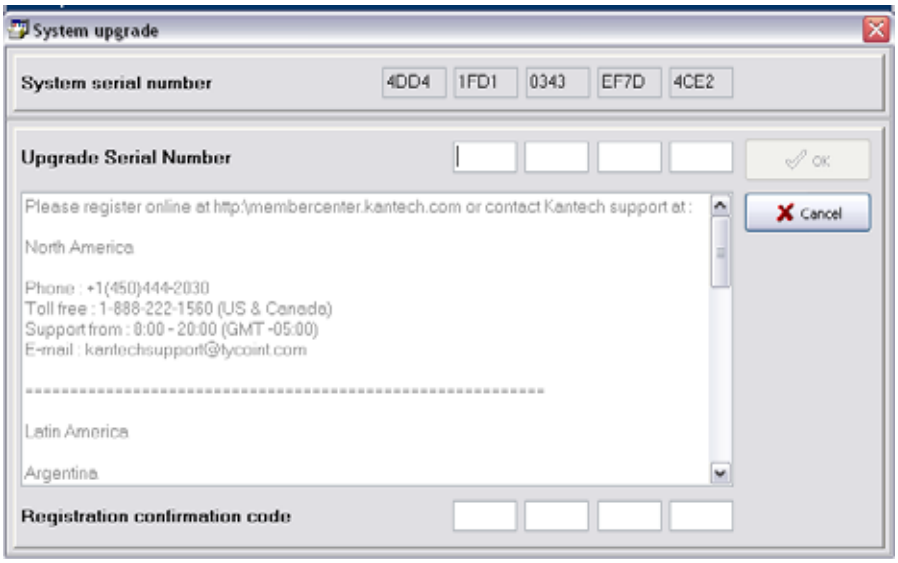
Для настройки/подключения внешнего Global Шлюз для связи с сервером произведите следующие шаги:

1. Запустите приложение EntraPass или **Configuration Program** EntraPass (программа настройки EntraPass**.**
2. В таблице **Device** (Устройства), выберите пункт назначение шлюза **"Gateway Definition**"
3. Из списка выберите Шлюз, который будет использоваться с Global Шлюз.
4. В области **NCC connection** (связь NCC), выберите "RS-232".
5. В области **RS-232 Gateway configuration**укажите **Baud rate**, используемый для связи между Шлюзом и Global Шлюз.
6. Нажите **Save** (сохранить).

Переход на другое программное обеспечение SE-CE-GE

1. До того, как вы начнете установку, будьте уверены, что приложения EntraPass остановлены.
2. Вставить установочный компакт-диск в CD-ROM привод компьютера. Если в настройках компьютера разрешён автоматический запуск, программа инсталляции запускается автоматически. Если этого не произошло, следует войти в меню **Start** (Пуск) > **Run** (Выполнить) и запустить файл d:\Setup.exe (где d: - имя CD-ROM привода). При этом должно открыться окно настройки программы инсталляции.

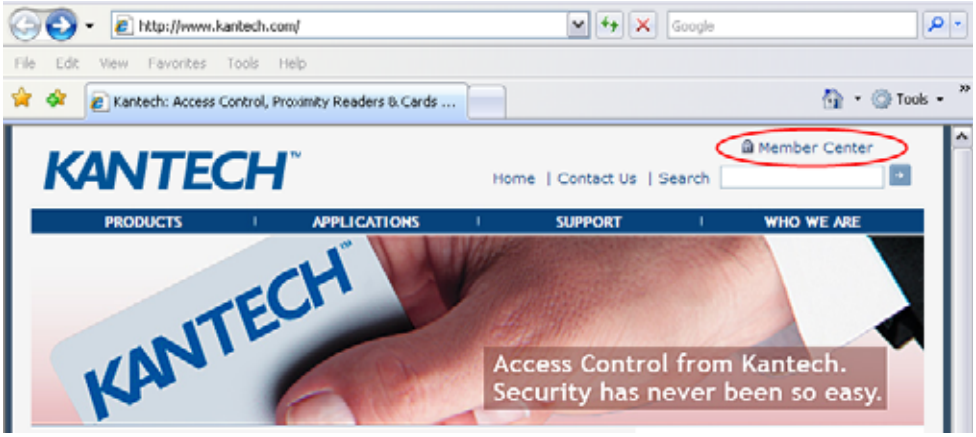
ПРИМЕЧАНИЕ: *Backup базы данных будет автоматически создан в течении процесса обновлений.*



3. Введите **Upgrade Serial Number** (расположенный на полученной лиценции на ПО).

ПРИМЕЧАНИЕ: *Там два пути обновить систему: регистрация на сайте www.kantech.com или контактировать с локальной службой технической поддержки для получения* ***Registration confirmation code****.*

4 Идите на www.kantech.com и нажмите **Member Center**.



ПРИМЕЧАНИЕ: *Если вы еще не авторизированы на metebe r center, пожалуйста оставьте ваш запрос на сайте. Вам обязательно ответят в течении 1-2 рабочихх дней.*

5 Нажмите на **Kantech Registration**.

6 Введите **System Serial Number.** В ответ вы получите Registration Confirmation Code.

7 Вернитесь в режим обновления системы (**System Upgrade)** и введите **Registration Confirmation Code**, затем нажмите **OK**. Копка **OK** будет активна, когда оба кода будут верны.

8 Следующие шаги по updating EntraPass (обновление EntraPass). См. “Обновление на новую версию” на стр. 34.

Обновление системы EntraPass

При обновлении программного обеспечения система автоматически обнаруживает установленные компоненты и обновляет их.

Настоятельно рекомендуем выполнять обновления в то время, когда нагрузка на систему близка к нулю (например, в ночь на субботу).

Перед обновлением EntraPass

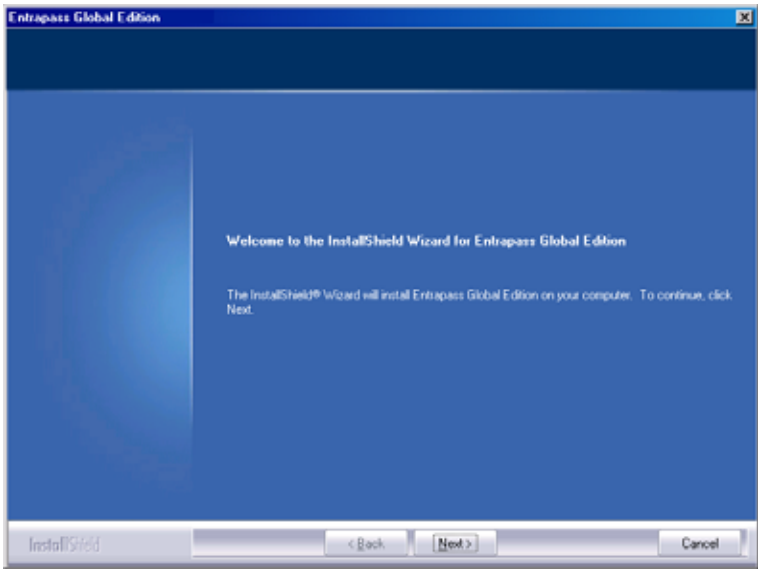
1. Создать **полную резервную копию базы данных системы.** Более подробные сведения по резервному копированию даны *в разделе см. "Backup по расписанию" на стр. 498*.
2. При наличии зеркальной базы данных (Mirror Database) и резервного сервера (Redundant Server) **ОБЯЗАТЕЛЬНО** следует **СНАЧАЛА** выключить резервный сервер.
3. Выключить сервер EntraPass и все другие приложения EntraPass. **До начала обновления системы все приложения, служебные и управляющие программы должны быть закрыты.**

ПРИМЕЧАНИЕ: *Обновление следует выполнять на* ***всех*** *приложениях. До окончания обновления* ***НЕ СЛЕДУЕТ ЗАПУСКАТЬ*** *резервный сервер и зеркальную базу данных. "Mirror Database and Redundant Server".*

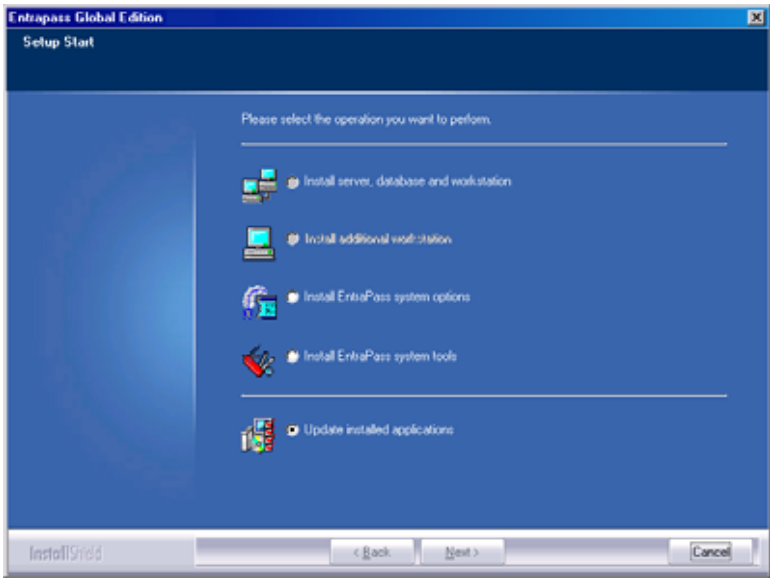
4. Проведите проверку базы данных системы (*см. "Утилиты базы данных" на стр. 516*) чтобы убедиться, что база данных не содержанит ошибок.
5. Только после того как база данных проверена, и не найдено ни одной ошибки, следует запустить EntraPass Server. После запуска и загрузки основного сервера можно запустить зеркальную базу данных и резервный сервер (Mirror Database and Redundant Server). Обратите внимание, что сервер должен быть запущен **до** запуска зеркальной базы данных и резервного сервера.
6. После того как все компоненты обновились, настоятельно рекомендуется перезагрузить шлюзы для гарантированного обновления всех данных и передачи их на контроллеры **(Operations > Gateway reload)**
7. Кроме того, можно использовать пункт меню **View connected List** (Посмотреть список подключенных компонентов) для проверки статусов всех шлюзов системы и приложений EntraPass. Для деталей, *см. "Backup по расписанию" на стр. 498*.

Обновление на новую версию

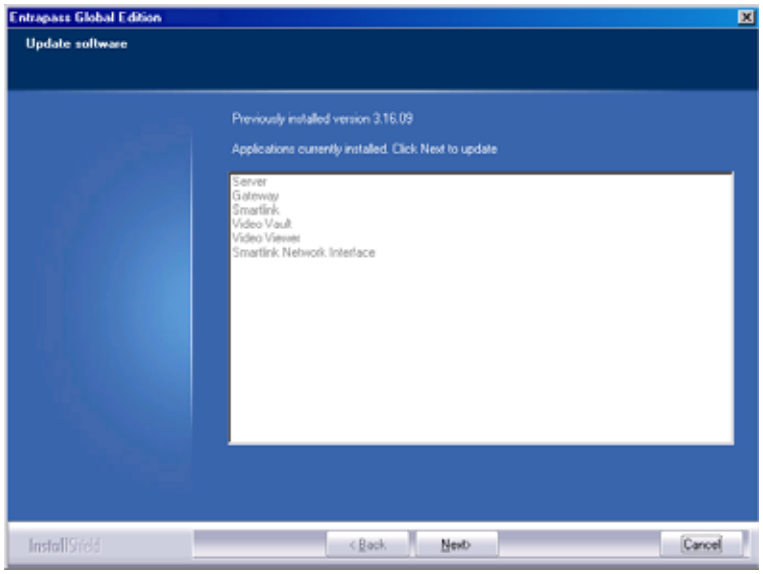
1. Вставить установочный компакт-диск в CD-ROM привод компьютера. Если в настройках компьютера разрешён автоматический запуск, программа инсталляции запускается автоматически. Если этого не произошло, следует войти в меню **Start** (Пуск) > **Run** (Выполнить) и запустить файл d:\Setup.exe (где d: - имя CD-ROM привода). При этом должно открыться окно настройки программы инсталляции.
2. Нажать **Next** для продолжения работы. При этом откроется окно приветствия.



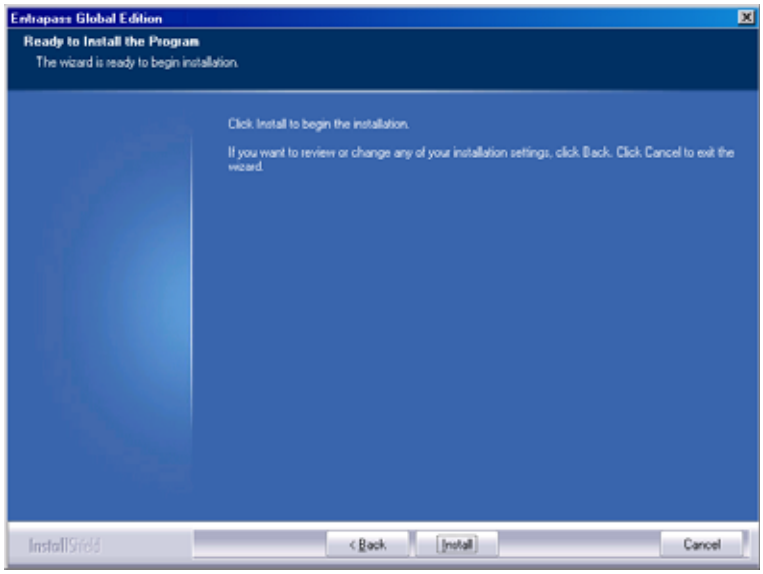
3 Нажать **Next** для продолжения работы. При этом откроется окно Setup Start (Начало установки).



4 Выделить пункт **Update Installed Applications** (Обновить установленные приложения) и нажать **Next**. Открывшееся окно Previous Software будет содержать список всех программ, установленных к данному моменту на этом компьютере.

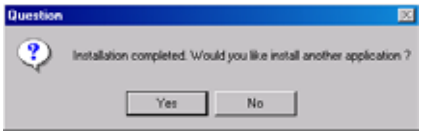


5 Нажать **Next** для продолжения работы. Начинается обновление, и все программы, установленные к данному моменту на этом компьютере, будут обновлены.



6 Чтобы прочитать ознакомительный файл Read-Me, содержащий информацию по выполненным обновлениям для разных приложений, нажать кнопку **View** (Посмотреть). Закрыть файл после прочтения. При этом система автоматически вернётся в окно Setup End (Окончание настройки).

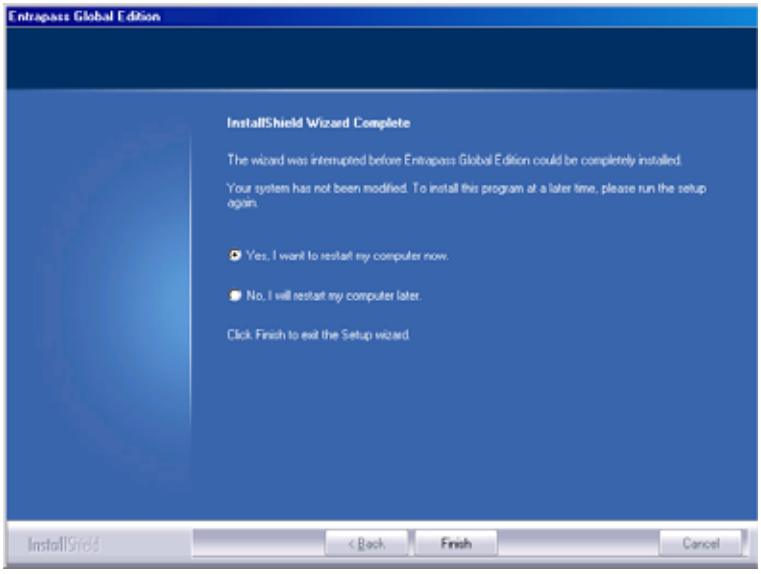
7 Нажать **Next** для продолжения работы. Система проверит, есть ли другие доступные для установки приложения или утилиты. При их обнаружении на экране появится соответствующее сообщение.



- Для того чтобы установить другие приложения, нажмите **Yes** и повторите действия с п.2

ПРИМЕЧАНИЕ: Если устанавливаемое приложение требует ввести серийный номер, следует обратиться в службу технической поддержки Kantech и зарегистрировать систему до выполнения любых дальнейших действий. *см. "Регистрация системы" на стр. 21.*

- Если установка выполнена, нажмите **No**. На экран будет выведено окно завершения работы мастера установки (InstallShield Wizard Completed). :



8 Выбрать **Yes**, чтобы выполнить перезагрузку компьютера сразу, или No, чтобы сделать это чуть позже.

9 Извлечь компакт-диск из CD-ROM привода.

10 Для завершения установки нажать **Finish**.

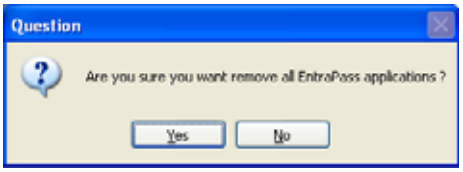
ПРИМЕЧАНИЕ: *После окончания обновления необходимо перезапустить компьютер в той последовательности, которая описана в начале этой главы, см. "Перед обновлением EntraPass" на стр. 34.*

Удаление программного обеспечения EntraPass

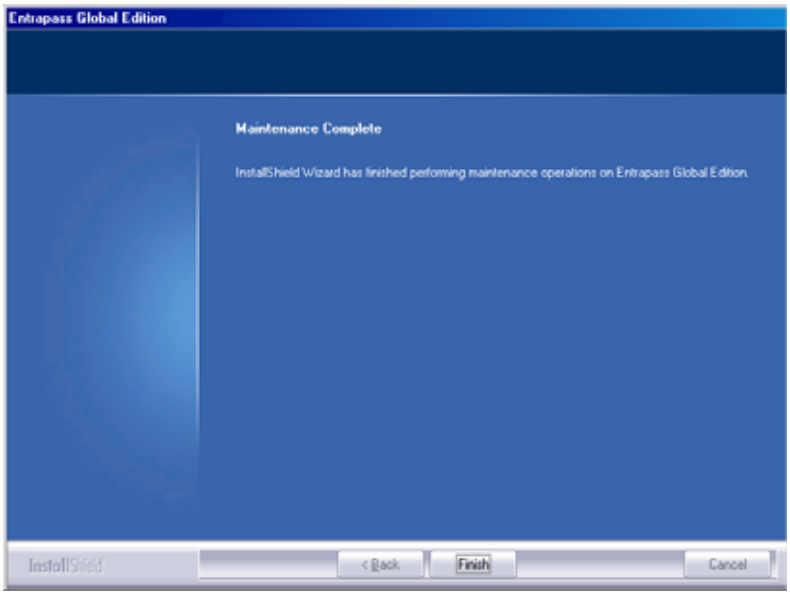
If you need to remove the EntraPass software from the computer, you will use the **Add/Remove Programs** option in the Control Panel.

1. Нажать Start (Пуск) > Settings (Настройки) > Control Panel (Панель управления).
2. В открывшемся окне запустить функцию Add/Remove Programs. При этом откроется диалоговое окно. Select the program you want to delete from the list and click **Remove**. The EntraPass Uninstall program dialog will display on the screen.

3. Выбрать из списка программу, которую необходимо удалить, и нажать Remove. На экране появляется диалоговое окно программы деинсталляции.
4. Нажать **Next**.
5. Чтобы начатый процесс был продолжен, необходимо подтвердить своё желание выполнить его.
   - Нажать **Yes** (Да), чтобы продолжить процесс деинсталляции.
   - Нажать **No** (Нет), чтобы отменить деинсталляцию.



6 После завершения процесса деинсталляции на экране появляется окно Maintenance completed (Техническая операция завершена).



7 Чтобы закрыть окно, нажать **Finish**.

8 Перезагрузить компьютер.

Глава 3 • :Начало работы

Этот раздел знакомит пользователей с графическим интерфейсом пользователя и основными функциями системы EntraPass.

Чтобы начать сессию EntraPass, необходимо запустить сервер EntraPass Server, шлюз EntraPass Gateway и рабочую станцию EntraPass Workstation. Чтобы начать сессию EntraPass, необходимо запустить сервер EntraPass Server, шлюз EntraPass Gateway и рабочую станцию EntraPass Workstation. Сервер представляет собой специализированный компьютер, включённый в сеть, который управляет системой контроля доступом. Сервер получает и отправляет данные через Шлюзы. Шлюзы получают информацию с сайтов\контроллеров и передают её на сервер. Рабочие станции EntraPass Workstations обеспечивают доступ операторов к базе данных и компонентам системы.

ПРИМЕЧАНИЕ: *Резервный сервер с зеркальной базой данных можно настроить для наблюдения за активностью основного сервера, а также для дублирования данных в случае отказа основного сервера. Обращаем внимание, что интерфейс MS-SQL/ORACLE не может быть подключен к резервному серверу и все события будут храниться в буфере, пока соединение с основным сервером не будет восстановлено.*

ПРИМЕЧАНИЕ: *Каждый оператор, авторизованный в системе, должен иметь уникальное, хранящееся в тайне имя и пароль, назначенные системным администратором/ установщиком. Доступ к рабочим станциям EntraPass должны иметь только авторизованные лица – это очень важно!*

Начало и окончание сессии

1 Войти в меню Start (Пуск) Windows® и открыть **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Global Edition** > **Server** / **Workstation** (Сервер/Рабочая станция).. В качестве приложения EntraPass может использоваться приложение Рабочая станция (**Workstation**), Шлюз (**Gateway**) или любая автономная утилита системы. Кроме того, для запуска программы можно воспользоваться ярлыком EntraPass на рабочем столе. Во время запуска приложение пытается установить связь с сервером. Язык меню на экране зависит от настроек оператора, который последним вошел в систему EntraPass. По умолчанию используется английский язык.

2Во время запуска приложение пытается установить связь с сервером. Язык меню на экране зависит от настроек оператора, который последним вошел в систему EntraPass. По умолчанию используется английский язык.

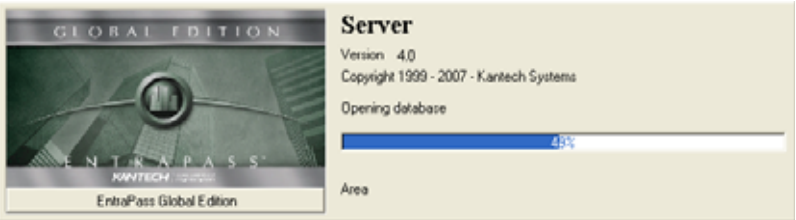
ПРИМЕЧАНИЕ: *Сначала следует запустить сервер EntraPass. Если запустить рабочую станцию раньше сервера, система предложит зарегистрировать рабочую станцию на сервере, даже если она уже была зарегистрирована. Если приложение уже было зарегистрировано, нужно просто запустить сервер.*

Запуск основного сервера EntraPass

Сервер EntraPass используется для следующих целей:

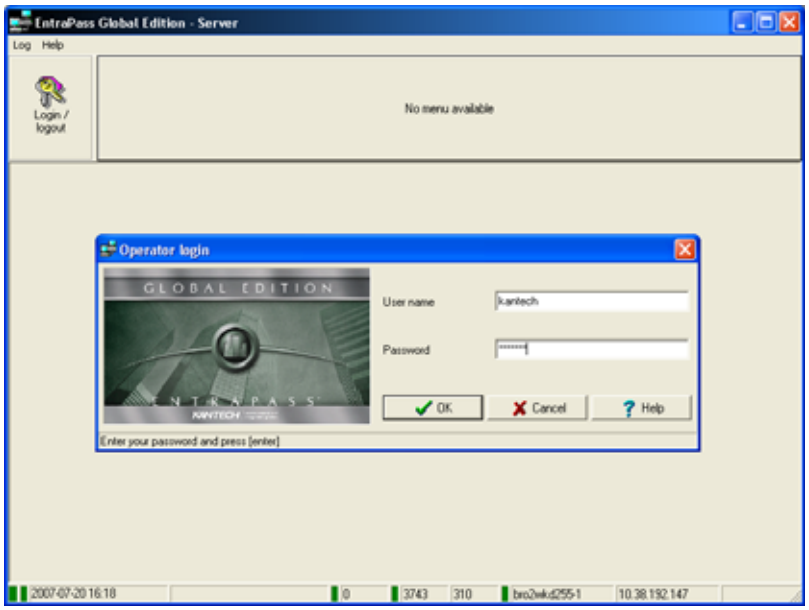
- отображение всех приложений, подключенных к серверу, журналов системных событий и ошибок
- регистрация новых подключений (приложения типа Рабочая станция, Шлюз, клиентские приложения типа интерфейса SmartLink, видеохранилища Video Vault, программы просмотра отчётов Report Viewer и др.)
- создание резервных копий баз данных: системные данные (Data), архивы (Archives), данные по учёту рабочего времени (Time and Attendance)
- восстановление данных: системные данные (Data), архивы (Archives), данные по учёту рабочего времени (Time and Attendance)
- проверка целостности баз данных
- выбор другого языка базы данных

1 **3**апустить сервер (через меню Windows® **Start** (Пуск) или с рабочего стола).



2 В открывшемся окне запуска сервера отображается ход выполнения, а также другие сведения о запуске сервера. После окончания загрузки на экране появляется окно регистрации пользователя.

3 Нажать кнопку **Login/Logout** для открытия окна регистрации оператора.



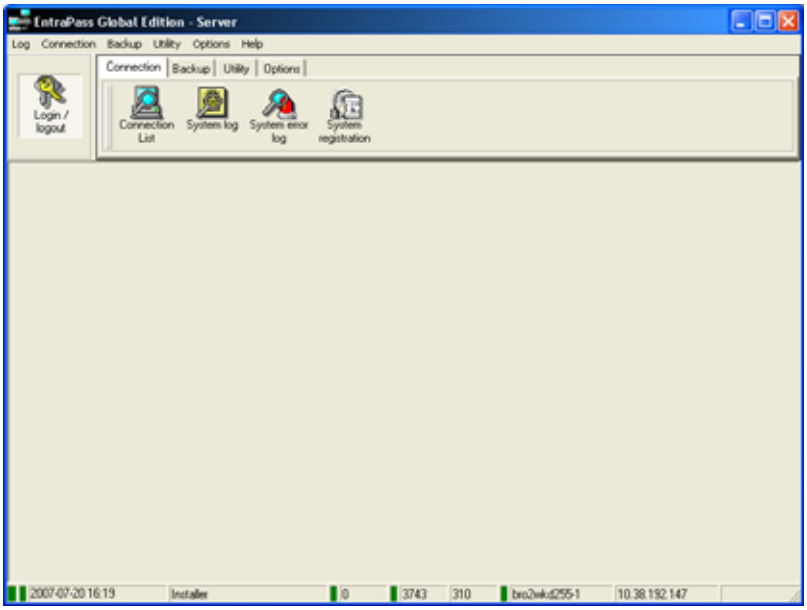
4 В открывшемся окне ввести имя пользователя (**User name**) и пароль (**Password**). По умолчанию в качестве имени пользователя используется "kantech". Имя не чувствительно к регистру. Пароль по умолчанию – kantech (нижний регистр). (Пароли чувствительны к регистру.)

ПРИМЕЧАНИЕ: Чтобы оператор мог регистрироваться на сервере, системный администратор должен установить флажок напротив опции “Allow login on server” (Разрешить регистрацию на сервере) при описании уровня доступа оператора (Operator security level) в меню System (Системные настройки) > Security Level (Уровни безопасности). см. "Назначение уровней безопасности" на странице 406.

ПРИМЕЧАНИЕ: *Система хранит имена последних пяти пользователей, позволяя операторам выбирать своё имя в выпадающем списке имён. Для удаления имени пользователя из этого списка его нужно выделить и нажать кнопку* ***Delete*** *на клавиатуре. По умолчанию опция* ***Display Login List*** *(Показывать регистрационный список) отключена. Чтобы воспользоваться ею, необходимо её активировать в диалоговом меню запущенного приложения (EntraPass Application dialog).*

5 После правильного ввода регистрационных данных на экране появляется главное окно сервера EntraPass Server с активной панелью инструментов. Выберете нужную закладку или войдите в

нужный пункт меню для выполнения необходимых действий или отображения сведений о системе.



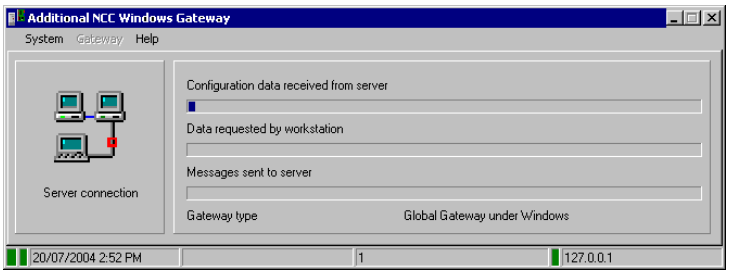
ПРИМЕЧАНИЕ: В строке состояний отображается статус соединения: зелёный означает, что связь в порядке, красный указывает на проблемы со связью.

6 Укажите курсор на флажок статуса (закрашенный прямоугольник) для отображения всплывающей подсказки. Первые два цветных прямоугольника в строке состояний отображают база данных открыта и база данных заблокирована.
- Если первый индикатор состояния окрашен в красный цвет, значит, база данных системы не открывается. Причиной может быть выполнение резервного копирования или проверки базы. Фиолетовый цвет указывает на то, что база данных заблокирована, так как выполняется восстановление данных с резервной копии или копирование в зеркальную базу данных.
- Если второй индикатор состояния окрашен в красный цвет, значит, база данных недоступна. Это происходит при обработке данных сервером или при обновлении базы.
- Зелёный цвет индикатора указывает что база данных доступна.

Запуск программы Gateway

Приложение Gateway (Шлюз) может быть установлено на том же компьютере, что и сервер или на компьютере с рабочей станцией EntraPass Workstation, однако рекомендуется выделять под него отдельный компьютер.

1 Запустить программу шлюза (из меню **Start (Пуск)** Windows® или с рабочего стола). Ввод пароля или имени пользователя не требуется. На экране появляется главное окно программы EntraPass Corporate Edition.



2 Пользователь может вызвать подменю нажатием правой кнопки мыши в любом месте экрана Gateway:
- **Minimize –** свернуть окно Gateway

- **Send to tray –** спрятать окно в правый нижний угол рядом с часами (так называемый "трей")

3 Важную информацию отображают также индикаторы выполнения (расположены внизу); они указывают следующее:
- **Configuration data received from the server** (Параметры конфигурации, полученные от сервера) – данные конфигурации (например, изменения в идентификационных картах), передаваемые на шлюз с сервера.
- **Data requested by workstation** (Данные, запрашиваемые с рабочей станции) – разные запрашиваемые данные, в частности, статус работоспособности.
- **Messages sent to server** (Сообщения, отправляемые на сервер) – сообщения, передаваемые с контроллера на сервер.

ПРИМЕЧАНИЕ: *Поле **Тип Шлюза** (**Gateway type**) показывает, что Шлюх запущен. Это может быть Corporate Шлюз или Global Шлюз.*

4 Раздел меню **System** служит для входа/выхода из системы (**login, logout**), а также для повторной загрузки данных шлюза (**reload**).

5 Меню **Gateway** предназначается для выбора шлюза. Число шлюзов, имеющих в текущий момент связь с сервером, отображается в строке состояний в главном окне Gateway.

ПРИМЕЧАНИЕ: *Индикаторы состояния отображают статус соединения. Первый индикатор состояния показывает текущий статус соединения с сервером. Красный цвет означает, что связи между сервером и шлюзом нет. Эта ситуация возникает, если сервер не подключен (можно запустить его потом). В строке состояний также отображается дата и время системы, число шлюзов и IP-адрес сервера*

ПРИМЕЧАНИЕ: *индикатор выполнения это не является индикатором состояния. Вам нет необходимости ожидать заполнения.*

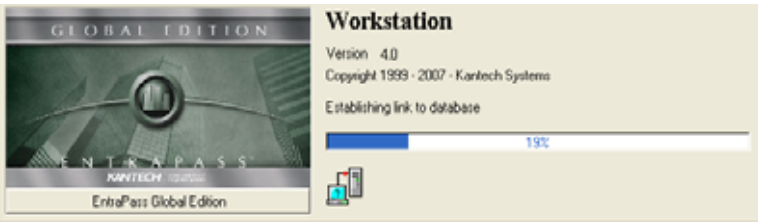
Запуск рабочей станции EntraPass Workstation

Рабочая станция EntraPass представляет собой компьютер, на котором установлено приложение EntraPass, предназначенное для мониторинга системы. С помощью этого приложения операторы получают доступ к базе данных. Операторы могут осуществлять программирование базы данных и компонентов системы.

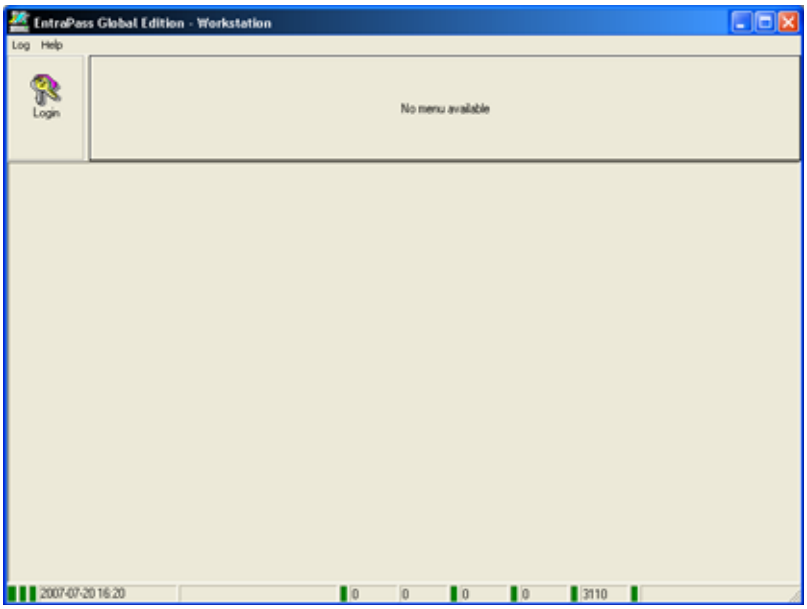
Перед запуском программного обеспечения EntraPass Workstation следует убедиться, что сервер подключен к сети. Во время запуска приложение Workstation обращается к серверу. Язык меню на экране зависит от настроек оператора, который последним зарегистрировался в системе. По умолчанию используется английский язык.

ПРИМЕЧАНИЕ: *Первым следует запустить сервер EntraPass. Если запустить рабочую станцию раньше сервера, система предложит зарегистрировать рабочую станцию на сервере, даже если она уже была зарегистрирована. Если приложение уже было зарегистрировано, нужно просто запустить сервер.*

1 Запустить рабочую станцию EntraPass через меню **Start** (Пуск) Windows® или щелчком по ярлыку на рабочем столе.

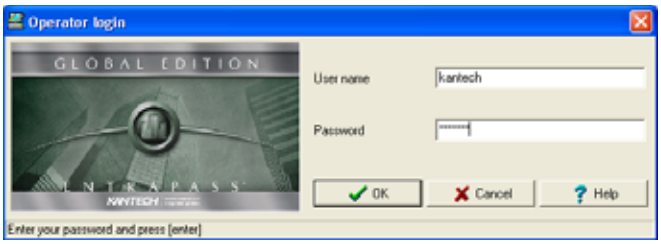


2 На экране появляется главное окно программы EntraPass Workstation.



ПРИМЕЧАНИЕ: *Если сервер не подключен, крайний левый индикатор состояния (все индикаторы состояния представляют собой цветные прямоугольники в строке состояний) окрашен в красный цвет; в это время кнопка Login/Logout недоступна. В таком случае следует запустить сервер, после чего рабочая станция EntraPass возобновит свою работу.*

3 Нажать кнопку **Login**/**Logout** на панели инструментов для открытия окна регистрации оператора.



4 Ввести имя пользователя в поле **User name** и пароль в поле **Password**. Пароль чувствителен к регистру. По умолчанию в качестве **имени пользователя** используется "kantech". Имя не

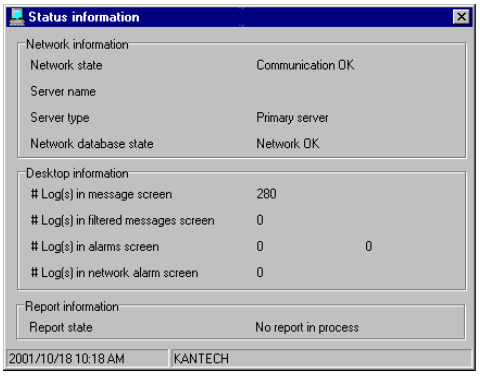
чувствительно к регистру. **Пароль** по умолчанию – kantech (нижний регистр). (Пароли чувствительны к регистру.)

ПРИМЕЧАНИЕ: *Если зарегистрироваться никак не удаётся, следует проверить, не включена ли фиксация регистра прописных букв на клавиатуре (кнопка Caps Lock). Если данные регистрации указаны верно, становятся доступными меню, панель инструментов и строка состояний. Кроме того, зарегистрироваться в системе возможно только при условии, что сервер работает.*

ПРИМЕЧАНИЕ: *По умолчанию, оператор не имеет возможности зарегистрироваться одновременно на нескольких рабочих станциях. Если необходимо, то можно настроить систему таким образом, чтобы оператор мог одновременно под одним паролем зарегестрироваться на нескольких АРМ. Глава 12 'Создание или изменение данных оператора' на стр. 402. Однако у оператора есть возможность одновременно зарегистрироваться на сервере и на рабочей станции.*

Получение сведений о статусе рабочей станции

1. Щёлкнуть по любой закладке для активации панели инструментов или выбрать один из пунктов меню для получения доступа к системному меню. В нижней строке окна цветными прямоугольниками показан статус соединения: зелёный означает, что связь в порядке, красный указывает на проблемы со связью, синий горит во время ожидания ответа.
2. Поместить курсор на цветные прямоугольники для получения подробных сведений о статусе сети, сетевом статусе базы данных и статусе ответа рабочей станции.
3. Поместить курсор на отображаемые цифровые показатели для получения дополнительных сведений. На экран будут выведены дата и время в системе, имя оператора, тревожные события, тревожные сообщения, требующие подтверждения, и др.
4. Щёлкнуть мышью (двойным или одинарным щелчком, в зависимости от выбранных системных настроек) на любом цифровом показателе в строке состояний, чтобы открыть окно Status Information (информация о состоянии).



ПРИМЕЧАНИЕ: Настоятельно рекомендуется выходить из программ EntraPass по кнопке Login/Logout. Это необходимо для корректного завершения работы базы данных.

Изменение свойств рабочего пространства

1 Для вызова окна Properties (Свойства) щёлкнуть правой кнопкой мыши в любом месте главного окна. В этом режиме можно индивидуально настроить кнопки окна, а также цветовой фон.

2 Для изменения размера кнопок на панели инструментов предусмотрены следующие опции:

- **Small buttons** (Малые кнопки) – отображать малые кнопки инструментов под строкой меню
- **Large buttons with images** (Большие кнопки с изображениями) – отображение пиктограмм компонентов на больших кнопках
- **Large buttons without images** (Большие кнопки без изображений) – не отображать пиктограммы на кнопках

3 В разделе меню Miscellaneous (Прочее) выбрать нужную опцию:

- **Display menu** (Показывать меню) – отображать только строку меню. Пиктограммы не отображаются. Для изменения свойств щёлкнуть правой кнопкой мыши в любом месте рабочего экрана.
- **Display toolbar** (Показывать панель инструментов) – отображать строку меню и панель инструментов.

4 Указать цветовой фон рабочего пространства.

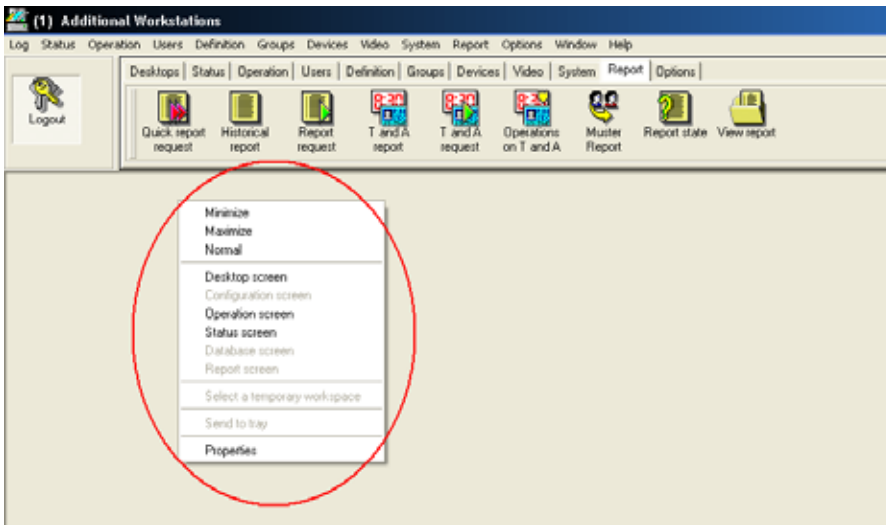
Восстановление свёрнутых окон на рабочем столе

В системе EntraPass допускается держать открытыми на рабочем столе несколько окон. При сворачивании или перемещении окна на задний план оно совсем исчезает с экрана. Для его восстановления на экране рекомендуется воспользоваться контекстным меню рабочей станции.

- Если окно было свёрнуто, специальная команда меню поможет поместить его на передний план, и затем развернуть на весь экран.
- Если окно находилось на заднем плане, то по соответствующей команде меню можно поместить его на передний план.

Данная команда используется для окон рабочего стола, окон настройки конфигурации, окон выполнения различных операций и окон состояний, окон баз данных и окон отчётов.

1 Щёлкнуть правой кнопкой мыши по фону в окне рабочей станции, чтобы вывести на экран контекстное меню.



2 В примере выше окно Status (Статус) находится на заднем плане. Чтобы переместить его вперёд, следует щёлкнуть в контекстном меню по команде **Status screen (дисплей состояния).** После этого дсиплей состояния будет раскрыт перед вами.

Автоматическая установка (Express Setup)

Express Setup позволяет устанавливать конфигурацию компонентов системы, включая сайты/лучи/ветки контроллеров и контроллеры, а также устройства, связанные с этими компонентами (например, двери и входы). Эта утилита сокращает к минимуму процесс программирования, позволяя установщикам тестировать инсталляцию и компоненты системы. Программу можно использовать для настройки сайта/луча/(ветки контроллеров) или для назначения контроллеров, прикреплённых к определённому лучу. Когда вы настраивали луч, это позволяло установщикам сразу присваивать этот луч к определенному Шлюзу. Утилита позволяет быстро настроить луч (ветку контроллеров), используя минимум сведений о конфигурации подключённых к нему контроллеров.

ПРИМЕЧАНИЕ: Для запуска Express Setup из меню Start (Пуск) Windows® следует выбрать: ***Start*** > ***All Programs*** > ***EntraPass Global Edition*** > ***Server*** > ***Express Setup*** или щёлкнуть по пиктограмме **Express Setup** в одном из окон рабочей станции EntraPass Workstation. Там две версии програмы *Express Setup: Express Setup NCC - это для настройки Global шлюзов только, и Express Setup - это для настройки Corporate Шлюзов только.*

Express Setup используется для настройки контроллера. Утилита позволяет операторам назначать значения по умолчанию для контроллера и связанных с ним устройств (реле, входов и выходов). В этом случае её запускают из окна системных сообщений или из меню назначения контроллера.

ПРИМЕЧАНИЕ: *Чтобы запустить программу Express Express Setup, нужно зарегистрироваться на сервере(workstation). Действительно, эта утилита позволяет изменять конфигурацию устройств системы, а перед внесением любых изменений необходимо ввести свои идентификационные данные.*

Более подробные сведения о программе Express Setup изложены *в разделе*, *Глава 16 ‘Программа быстрой настройки"Express Setup"’ на стр. 531*.

Дополнительные автономные программы EntraPass

В систему EntraPass входит ряд автономных приложений, позволяющих выполнять различные задачи, включая проверку баз данных системы и смену языка интерфейса. Перечислим ниже автономные утилиты EntraPass:

- **Database Utility** (Утилита базы данных). Служит для переиндексации архивных файлов, обновления полей базы данных, проверки архивных файлов, проверки целостности базы данных, проверки индекса базы данных, проверки ссылок и иерархии базы данных. Эта утилита может быть запущена, когда сервер отключен.
- **Express Setup** (Автоматическая установка). Программа служит для настройки всех компонентов системы, имеющих отношение к определенному Шлюзу. При помощи Express setup вы можете настроить тип используемых считывателей карт, способ соединения, количество лучей, число контроллеров на каждом луче и др.
- **KT-Finder** (Программа обнаружения устройств). Позволяет локально или удалённо настраивать конфигурацию IP-устройств Kantech, в том числе интерфейса Kantech IP Link, контроллера KT-400, а также сетевого контроллера связи KT-NCC (смотрите ***Примечание***).

ПРИМЕЧАНИЕ: Контроллер сетевой связи KT-NCC доступен только в конфигурации EntraPass Global Edition.

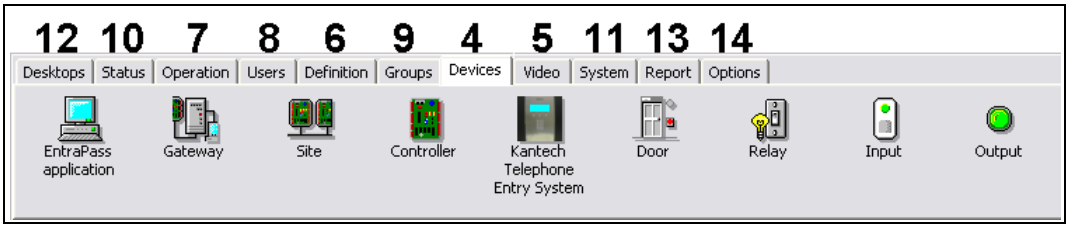
- **PING Diagnostic**: (Тестирование по методу "запрос-ответ"). Программа используется для диагностики проблем сети.
- **System Report Viewer** (Программа просмотра отчётов системы). Позволяет оператору просматривать отчёты, не запуская рабочую станцию. После установки данной утилиты операторы получают возможность просматривать отчёты, отправляемые другими рабочими станциями, по электронной почте.
- **Vocabulary Editor** (Редактор языков). Простая и удобная программа для перевода терминов меню на любой язык по выбору.
- **Workstation** (Программа настройки конфигурации рабочей станции). Эта программа, схожая со стандартным приложением рабочей станции, позволяет администратору системы устанавливать конфигурацию логических и физических компонентов системы.
- **Migration Utility** (Утилита переноса данных). Служит для передачи сведений, касающихся программного обеспечения и баз данных при обновлении системы с версии Special Edition на версию Corporate Edition или с версии Corporate Edition на версию Global Edition.

Перечисленные утилиты можно запускать из меню Start (Пуск) Windows® с любого компьютера, на котором установлено приложение Entrapass Server или EntraPass Workstation. Более подробные сведения по дополнительным автономным программам EntraPass изложены *в* , *Глава 16 ‘Системные утилиты’ на стр. 515*.

Панель инструментов EntraPass

Основной дисплей EntraPass содержит следующие кнопки. Они позволяют быстро получить доступ к системным функциям. Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка.

Каждая панель соотвествует определенной главе, как это показано цифрами на следующем рисунке.



Доступ к панели инструментов открыт из любого диалогового окна EntraPass. В разных окнах доступны разные пиктограммы. Большинство пиктограмм ничем не отличаются от стандартных иконок, используемых в компьютерной отрасли.

Кнопка	Описание
	Кнопка **New** (Создать) служит для ввода новых данных в базу данных системы. Используется при добавлении луча, расписания, контроллера и др.
	Кнопка **Save** (Сохранить) позволяет сохранить все данные, введённые с момента последнего сохранения. Данные сохраняются прямо в системе.
	Кнопка **Save As** (Сохранить как) даёт возможность сохранить всю информацию об уже созданном компоненте под другим именем, не оказывая влияния на исходный компонент. При использовании данной команды в процессе выпуска карты она служит для создания новой карты или сохранения карты под новым номером, без изменения данных исходной карты.
	Кнопка **Delete** (Удалить) предназначена для удаления текущей выделенной записи. Для защиты от случайного удаления нужной информации удаление выполняется только после подтверждения этой операции пользователем. При удалении компонента стираются также и все его связи с другими объектами. Однако записи (архивные) в базе данных остаются даже при удалении объекта.
	Кнопка **Print** (Вывести на печать), в зависимости от активного меню, используется для печати отчётов, списков карт, параметров событий и прочего.
	Кнопка **Parent** (Родительский элемент) позволяет операторам представить поиск в виде иерархической структуры или разделить его на отдельные поиски по шлюзам, лучам и контроллерам (в соответствии с меню). Эта кнопка очень пригодится при работе с большими базами данных, так как позволяет найти определённый объект по его родительскому элементу.
	Кнопка **Link** (Связь) позволяет увидеть все привязки объекта в других меню. Более подробная информация *см. "Отображение связей компонентов" на странице 58*.
	Кнопка **Find** (Поиск) служит для поиска определённого объекта или компонента в базе данных системы с помощью специальной символьной строки. Более подробная информация *см. "Поиск компонентов" на странице 53*.

Кнопка	Описание
	Кнопка **Express Setup** (Автоматическая установка) позволяет установщикам и системным администраторам настраивать устройства, задавая настройки по умолчанию.
	Кнопка **System Tree View** (системное дерево) отображает устройства в иерхаическом формате. Компоненты, выбранные в этом окне могут выбираться
Close	Кнопка **Close** (Закрыть) служит для закрытия меню или подменю. Если перед закрытием не было выполнено сохранение данных, то перед закрытием меню на экране появляется окно с запросом на подтверждение сохранения данных.
Cancel	Кнопка **Cancel** (Отмена) служит для отмены всех изменений, которые были сделаны с момента выполненного сохранения. Система предложит подтвердить выполнение операции.
Help	Кнопка **Help** (Подсказка) служит для получения подсказки на определённую тему.
OK	Кнопка **OK** используется, чтобы сохранить и подтвердить внесение изменений, добавлений или удалений, сделанных в базе данных системы.
	Кнопка **Select all** (Выделить всё) служит для выделения всех объектов или компонентов, отображаемых в списке.
	Кнопка **Unselect all** (Отменить выделение всех) предназначена для отмены выделения всех объектов или компонентов, которые были ранее выделены в списке
	При работе в определённых окнах у операторов есть возможность включить графику и анимацию кнопок. Это особенно полезно, если требуется отобразить статус компонента перед выполнением операции с этим компонентом. Кнопка **Enable graphic** (Разрешить графику) есть, например, в меню Status (Статусы/Состояния) и меню Operations (Операции). Если использование графики разрешено, кнопка показывает изображение, прикреплённое к выделенному компоненту (например, двери) и отображает также связанные с ним компоненты (например, считыватели карт). Для того чтобы компоненты отображались в реальном времени, кнопку **Enable graphic** следует использовать вместе с кнопкой **Enable animation** (Разрешить анимацию).
	Кнопка **Enable animation** (Разрешить анимацию). Если эта кнопка активна (анимация разрешена), то автоматически становится активной и кнопка **Enable graphic** (Разрешить графику). При этом текущий компонент (например, дверь) становится активным, и его статус отображается в реальном времени. Например, если заблокировать дверь, которая до этого была разблокирована, пиктограмма считывателя карт (также видимая) изменится: зелёная метка станет красной.
Right-click	**Правая кнопка мыши** служит для вызова контекстного меню, в котором доступны разные команды в зависимости от активного меню.

Основные функции

Перечислим основные действия, доступные при работе в системе:

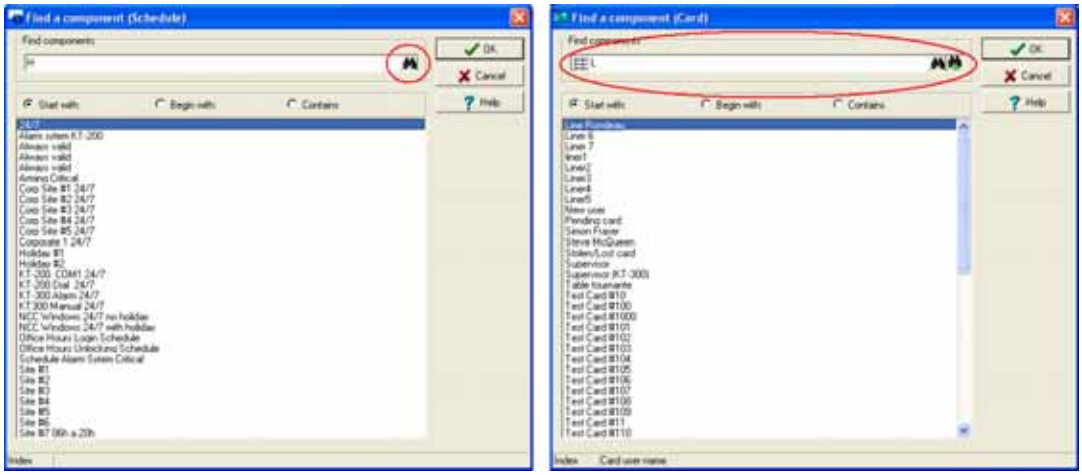
- Поиск компонентов
- **Окно расширенного режима поиска (Extended Selection Box)**
- Выбор компонентов, специфических папок, лучей и шлюзов
- Вывод на печать списков или отчётов
- Просмотр связей между компонентами
- Просмотр системного дерева

Поиск компонентов

Функция Find Components (Поиск компонентов) позволяет найти определённый объект или компонент в базе данных системы с помощью специальной символьной строки.

Существует два типа диалоговых меню поиска компонентов. Одно из них доступно с панели инструментов любого окна EntraPass. Другое открывается во всех меню, связанных с пользователями (это окна Cards (Карты), Visitor Cards (Карты посетителей) и Daypasses (Разовые пропуска)).

1 В обоих случаях для открытия меню поиска компонентов следует нажать на кнопку с изображением бинокля на панели инструментов.



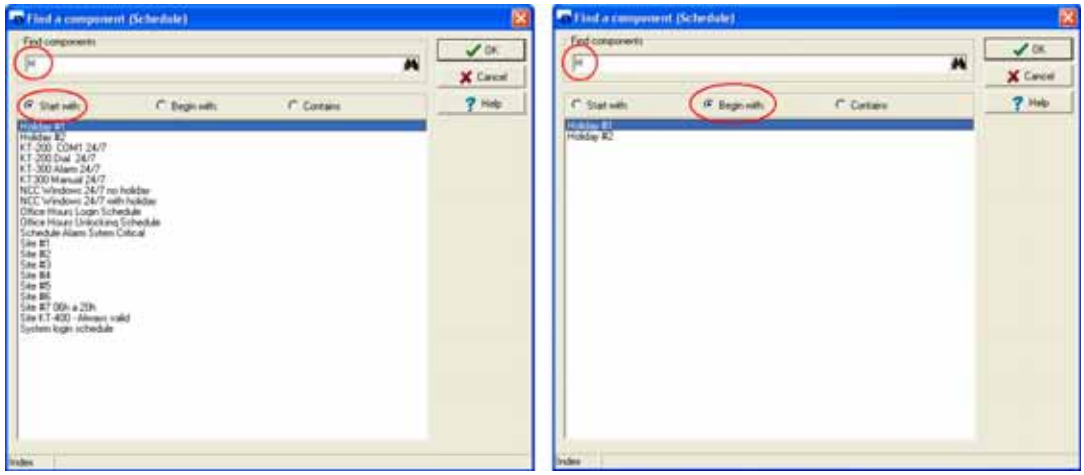
- Слева изображено меню поиска компонентов, справа меню поиска карт.

Кнопки	Описание
	Поиск в базе данных компонентов или карт.
	Поиск в базе данных изображения, соответствующего карте, выбранной из списка.
	Открыть меню, чтобы выбрать параметр, по которому необходимо осуществить поиск карты (номер карты, имя владельца, информационные поля карты и др.).

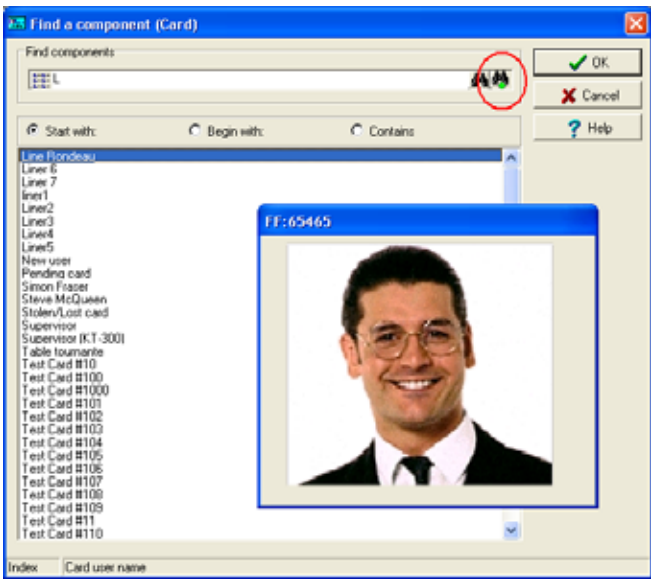
2 Чтобы начать поиск, ввести ключевое слово и нажать кнопку с изображением бинокля (справа). Чтобы сузить поиск, установить флажок в одном из следующих полей:

- **Start with** (Начиная с....). Результаты поиска будут содержать все компоненты, которые начинаются с введённых символов, в алфавитном порядке, а также все остальные компоненты, доступные в базе данных.
- **Begins with** (Начинающиеся с...). Результаты поиска будут содержать только компоненты, имя которых начинается с введённых символов.

- **Contains** (Содержит...). Результаты поиска будут содержать все компоненты, в которых есть введённые символы.



3 Чтобы увидеть изображение, которое соответствует выбранной карте, следует использовать кнопку поиска с изображением бинокля и знаком плюс.



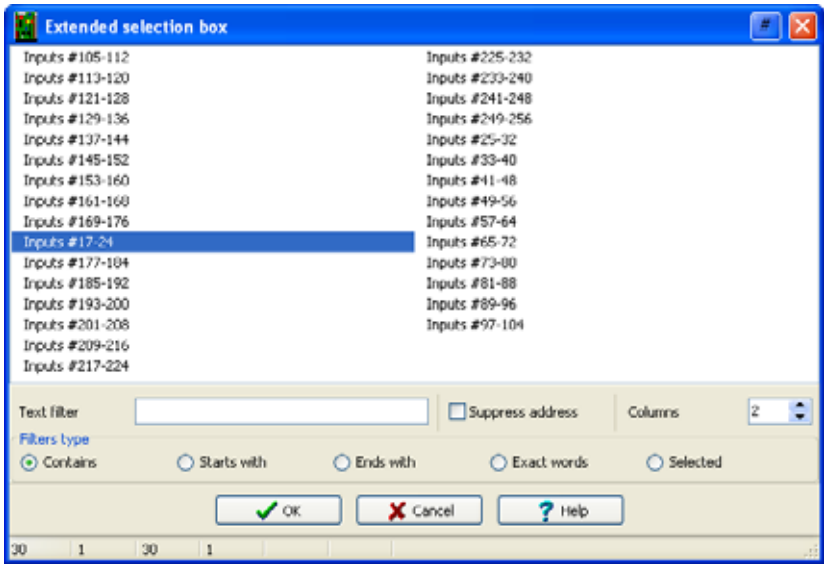
4 Для отмены поиска в процессе выполнения следует нажать кнопку **Cancel** (Отмена).

5 Нажать **OK**. Выделенный в списке компонент появится в окне, из которого был инициирован поиск.

Окно расширенного режима поиска (Extended Selection Box)

Окно расширенного режима поиска позволяет посмотреть все компоненты из выпадающего списка путём нажатия на правую кнопку мыши на этом списке для таких компонентов, как приложения,

контроллеры и двери. Если эта опция доступна, то при помещении курсора на выпадающий список открывается окно-подсказка.



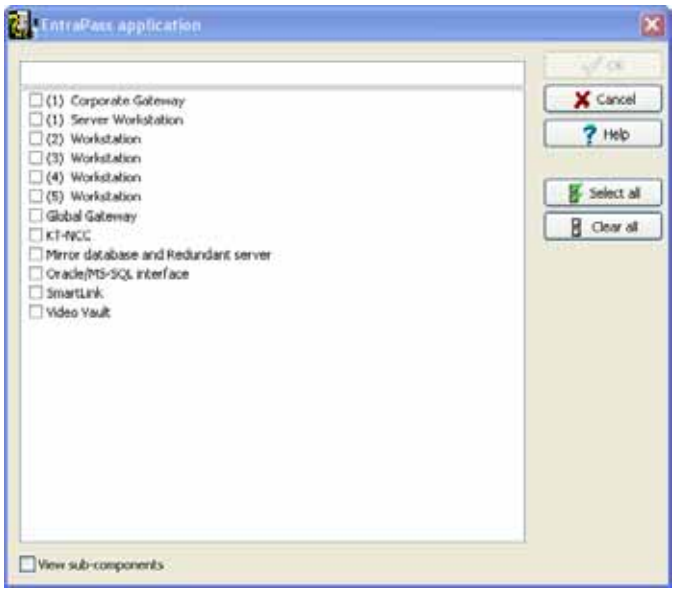
- В окне расширенного поиска предусмотрено использование следующих фильтров (**Filters types**):
  - Contains (Содержит...)
  - Starts with (Начинается с...)
  - Ends with (Оканчивается на...)
  - Exact words (Точное совпадение)
  - Selected (Выделенное)
- В поле **Text filter** (Текстовый фильтр) следует указать, какие слова должен содержать искомый объект.
- Поле **Suppress the address** (Скрыть адреса) можно отметить флажком, чтобы не отображать адреса в результатах поиска.
- Кроме того, в поле **Columns** (Колонки) можно выбрать число колонок на странице результатов.

Выбор компонентов

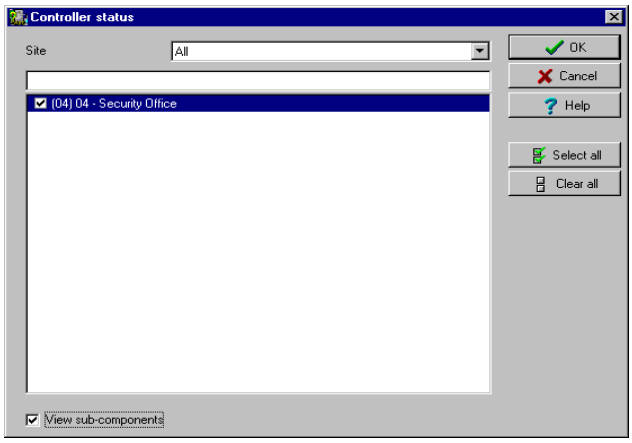
Функция **Select Components** (Выбор компонентов) позволяет выделить один или несколько компонентов системы. В зависимости от ситуации применяется тот или иной способ выделения.

1. В активном окне нажмите кнопку **Select Components**. В открывшемся дополнительном окне можно выбрать необходимые опции.
2. Выделять компоненты можно поштучно, устанавливая флажки напротив каждого объекта, или все сразу, используя кнопку **Select All** (Выделить все), кнопка слева. Кроме того, для просмотра несгруппированных компонентов следует выделить опцию **Single** (Одиночные), а для просмотра групп можно использовать функцию **Group** (Группа).
3. В отображаемом списке выделить компонент/группу, которую необходимо отобразить. При установке флажка в поле **View** (Посмотреть) на экране будут также отображаться компоненты, связанные с выделенными объектами.
4. Где доступно, используйте кнопку **Select all** (Выделить все) чтобы выделить все компоненты. Чтобы снять выделение со всех компонентов, рекомендуется использовать кнопку **Clear all**

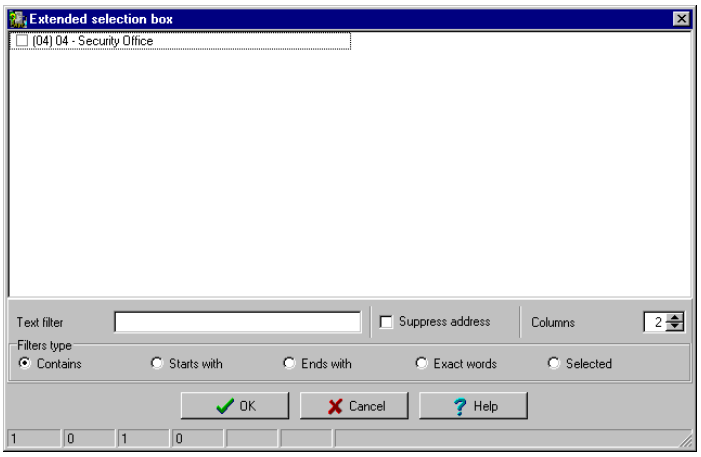
(Очистить все). Для возврата к предыдущему экрану меню без внесения изменений и без выделений следует нажать кнопку **Cancel** (Отмена).



5 Есть ещё один способ выделения, который проиллюстрирован на примере выбора компонентов в окне статусов контроллеров (Controller Status). Он заключается в том, что при нажатии на правую кнопку мыши внутри окна открывается окно расширенного выбора, отображающее компоненты.



6 Установите требуемое количество колонок в **Extended Selection box (**Расширенном режиме выбора**)** для отображения всех запрошенных компонентов. indow to display all components as required. Чтобы сократить список, следует воспользоваться текстовым фильтром (**Text Filter**).



7 Нажать **OK** для дальнейшего использования выделенных компонентов и возврата к предыдущему экрану меню.

Выбор определенной папки

У пользователя может возникнуть необходимость найти в сети или на жёстком диске определённый путь для хранения файлов, например, с резервными копиями.

1 Для этого следует нажать в активном окне кнопку **Select** (стоит с многоточием "..."). В открывшемся дополнительном окне указать нужный путь.

2 Чтобы изменить путь назначения, следует воспользоваться выпадающим списком дисков (в нижней части окна). Для обновления отображаемого списка нажать кнопку **Refresh drive** (Обновить диски).

3 После того как нужный путь будет найден, следует нажать **OK**, чтобы вернуться в активное окно.

Порядок выбора определённого луча или шлюза

Система EntraPass даёт возможность связать определённый компонент с определённым шлюзом/лучом. Например, вы можете назначить праздничные дни для определённого луча или шлюза.

1 В активном окне нажать кнопку **New** (Создать). Система откроет окно Select Gateway/Site (Выбор шлюза/луча).

2 Двойным щелчком мыши выбрать луч/шлюз (Site/Gateway) из появившегося списка и нажать **OK**.

3 Назначить этому компоненту содержательное имя.

4 Следуя указаниям, завершить задачу.

Вывод на печать списка или отчёта

Функция Print (Вывод на печать) используется для следующих целей:

- Вывод на печать списка идентификационных карт
- Вывод на печать параметров событий
- Вывод на печать привязок типа реле-событие
- Настройка отчёта для вывода на печать

1 В любом окне EntraPass нажать кнопку **Print** (Вывод на печать).

2 Выделить компоненты, которые необходимо включить в список. Для включения в список всех отображаемых на экране компонентов выделить их кнопкой **Select All** (Выделить все).

3 Если поставить флажок в поле **Print empty fields** (печатать пустые поля) и/или **Print component reference** (Печатать ссылки компонентов) (если опция доступна), то на печать будут выводиться, то в список будут включены названия даже пустых полей.

4 После выделения всех нужных полей можно перед печатью просмотреть получившийся список. Во время предварительного просмотра доступны следующие операции

- Задание параметров принтера

- Печать отчёта или списка
- Сохранение отчёта или списка для дальнейшего просмотра через программу **Quick Viewer** или загрузка уже созданного отчёта. Более подробная информация об этой программе приведена *в разделе Глава 16 'Quick Viewer - Программы быстрого просмотра отчётов' на стр. 543*.

5 Чтобы изменить какие-либо позиции, следует закрыть окно просмотра, внести изменения, а затем распечатать изменённый список.

6 Чтобы назначить определённый тип и размер шрифта, в программе есть кнопка **Font** (Шрифт).

7 Выбор или изменение шрифта выполняется следующим образом:
- В меню **Font** выбрать тип шрифта. Для предварительного просмотра выделенный текст будет выведен в поле **Sample** (Пример).
- В меню **Font Style** (Стиль шрифта) выбрать атрибуты форматирования (обычный, курсив, жирный или жирный курсив).
- Указать размер шрифта в меню **Size** (Размер) (по умолчанию используется 10 или 11 шрифт). Чем мельче шрифт, тем больше текста умещается на странице.

8 Кроме того, можно выбрать цвет шрифта в меню **Color** (Цвет). По умолчанию используется шрифт чёрного цвета. Внесённые изменения автоматически отображаются в окне предварительного просмотра. Нажать **OK** после внесения всех необходимых изменений. В окне Print нажать кнопку **Preview** (Предварительный просмотр) для проверки текста перед выводом на печать.

ПРИМЕЧАНИЕ: *Если принтер на компьютере не настроен, система выдаёт сообщение об ошибке.*

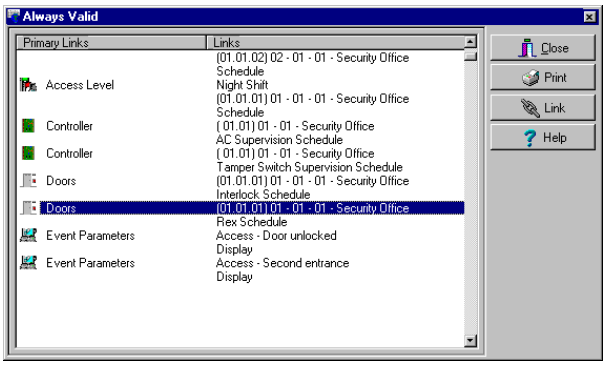
Отображение связей компонентов

Функция **View links** (Посмотреть связи) позволяет увидеть все привязки объекта в других меню. Таким образом, можно изучить все связи объекта с другими объектами.

ПРИМЕЧАНИЕ: *Кнопку **View links** (Посмотреть связи) рекомендуется использовать перед удалением компонента из базы данных, чтобы увидеть, какие меню затронет удаление объекта. Кроме того, связи выделенного компонента можно вывести на печать.*

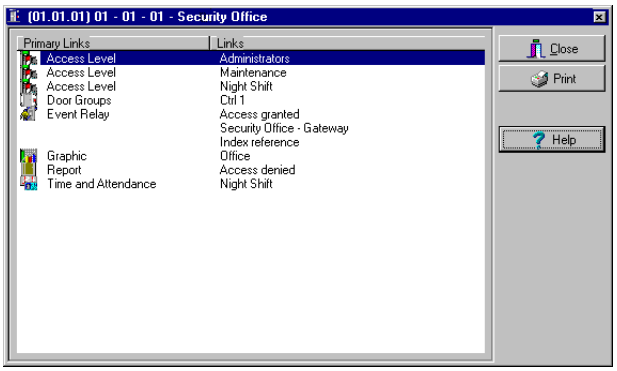
1 В любом окне меню выбрать компонент и нажать кнопку **Link** (Связь). На экране появятся все компоненты, связанные с выделенным объектом.

2 Пиктограммы, расположенные слева от компонентов, указывают их тип. Например, если выделить расписание **Always valid** (Действует всегда) в меню задания расписания и нажать кнопку **Link**, система покажет список всех меню, в которых используется это расписание.



ПРИМЕЧАНИЕ: *В приведённом выше примере расписание **Always valid** используется как расписание кнопки REX (Запрос на выход) в меню описания дверей.* Правой кнопкой мыши можно вызвать контекстное меню для выбора категории. *Например, если нажать на правую кнопку мыши и выбрать в контекстном меню пункт Access levels (Уровни доступа), то система покажет уровни доступа, в которых настроено данное расписание.*

3 Чтобы посмотреть связи какой-либо двери с другими компонентами системы, следует выделить эту дверь и снова нажать кнопку **Link.**:

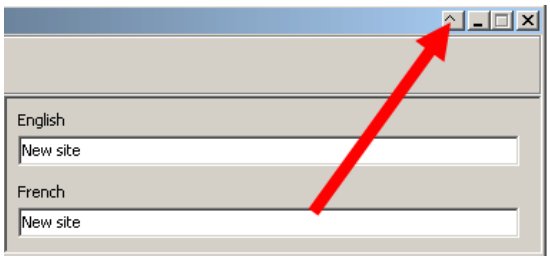


4 На экран будут выведены все компоненты системы, имеющие связь с выбранной дверью. В приведённом примере компонент "Дверь" использует уровень доступа «администратор» (Administrator); пользователям с этим уровнем доступа будет разрешен проход в эту дверь.

5 Для того чтобы вывести на печать информацию, размещённую на экране, следует нажать кнопку **Print** (Вывод на печать).

Плавующие окна

Плавующее окно может быть использовано для перемещения окна снаружи рабочей станции.



Невозможно спрятать окно, когда включен режим плавующего окна. Окно должно быть закрытым и открытым заново. Никакой информации о местоположении окна не сохраняется в системе.

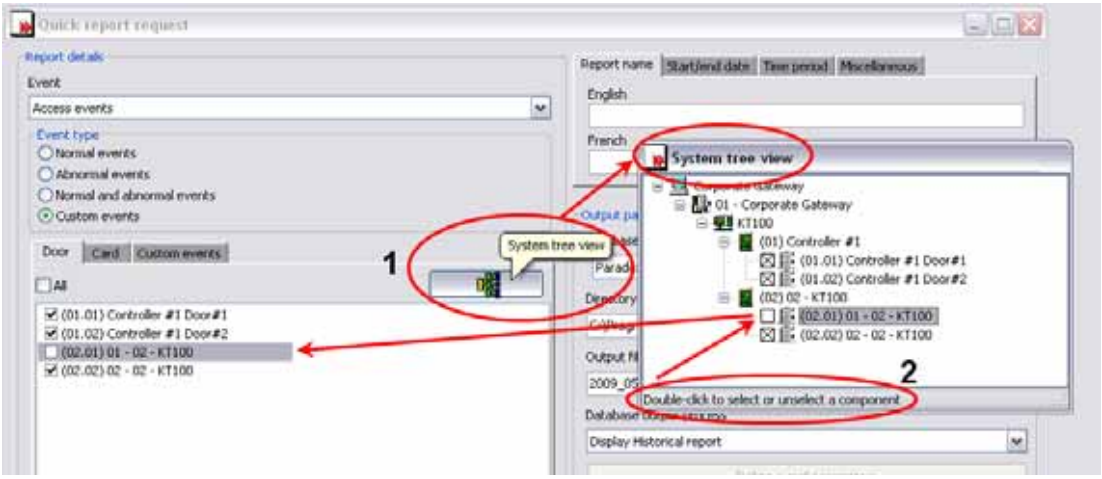
Иерхаический режим просмотра

Кнопка **System Tree View** (Иерхаический режим просмотра) отображает компоненты в иерхаическом формате. Компоненты отображаемые в этом окне могут быть выделены. Вы можете получить доступ к **System Tree View** при помощи различных путей:

Иерхаический режим просмотра из диалога

Когда применимо, кнопка **System Tree View** доступна как в окне **Quick Report Request** (запрос быстрого отчета).

1 Из панели инструментов **Reports(**отчеты**) > Quick Report** (Запрос быстрого отчета). Нажмите на кнопку **System Tree View**.

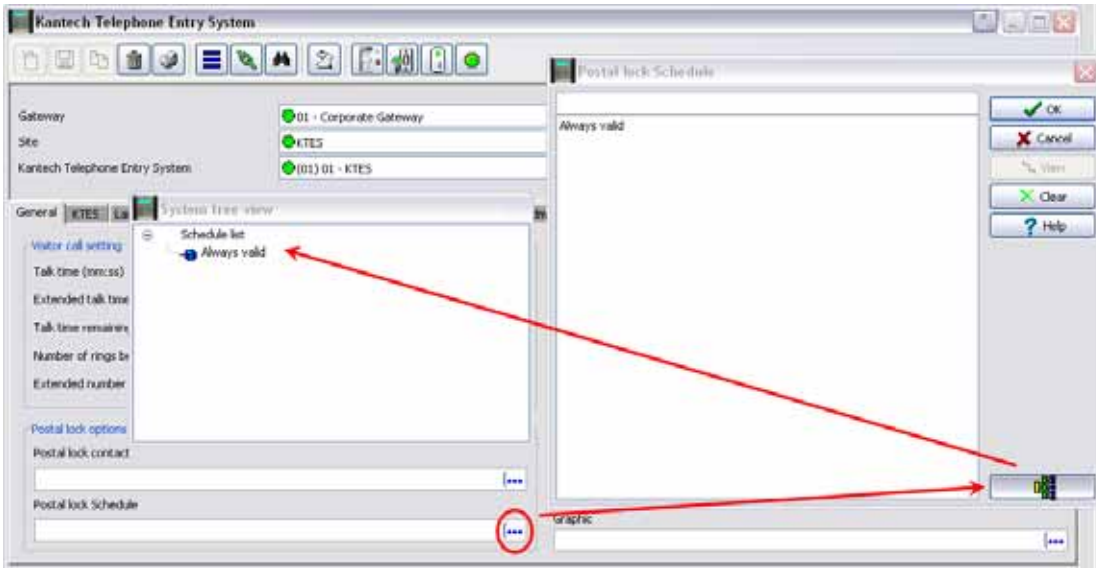


2 Из режима **System Tree View** (Иерхаический режим просмотра), вы можете двойным нажтием выбрать компонент. Изменения вступят в силу автоматически.

3 Нажмите назад на кнопку **System Tree View** (Иерхаический режим просмотра) для закрытия.

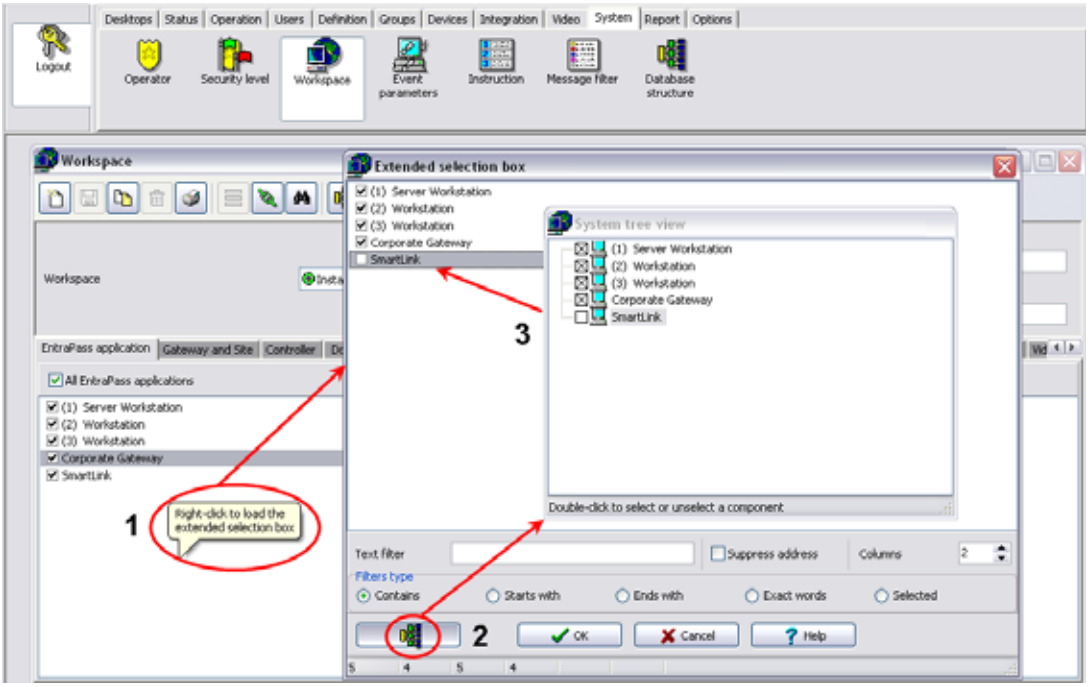
Использование кнопки многоточие (...)

На предоставленном поле данных нажмите кнопку многоточие**(•••)**:



Использование дополнительного окна

1 Из панели инструментов **System** (Система)**> Workspace** (рабочее пространство)**> EntraPass Application** (Їриложения Entra Pass), нажмите правой кнопкой мыши для открытия дополнительного окна (**Extended Selection Box)**:



2 Нажмите на кнопку **System Tree View** (Иерхаический режим просмотра), двойным нажатием на клавишу мыши, вы можете выделять компонент. Обновления произойдут автоматически в расширенном выпадающем окне просмотра.

3 Нажмите назад на кнопке **System Tree View** (Иерхаический режим просмотра) для ее закрытия.

Глава 4 • Системные устройства

Панель инструментов устройств

После установки оборудования и программного обеспечения системы необходимо настроить оборудование. На вкладке **Устройства «Devices»**, которая расположена в панели APM, вы можете получить доступ к настройкам компонентов: приложения EntraPass, шлюзы, интерфейс SmartLink, резервный сервер с базой данных и видеохранилище EntraPass Video Vault, а также физические компоненты (контроллеры,KTES, реле, двери, оборудование третьих компаний).

ПРИМЕЧАНИЕ: *Чтобы сократить время настройки и избежать ошибок при наладке системы рекомендуется воспользоваться программой автоматической установки Express Setup. Кроме того, Express Setup позволяет протестировать оборудование и электрические соединения сразу после установки.*

Воспользуйтесь программой **Express Setup** для первой настройки конфигурации шлюзов, лучей или контроллеров на первое время.

You run the **Express Setup** program when you are configuring gateways, sites or controllers for the first time. Для запуска утилиты Express Setup щёлкните мышью по её пиктограмме в одном из окон EntraPass. Кроме того, для запуска Express Setup можно использовать меню "Пуск" (Start) Windows® или окно System Registration или системную подсказку, появляющуюся при добавлении, например, контроллера.Более подробная информация об использовании программы автоматической установки Express Setup изложена , *в Главе 16 Программа быстрой настройки"Express Setup" на стр. 531*.

ПРИМЕЧАНИЕ: *В случае интеграции с системами видеонаблюдения программное обеспечение EntraPass позволяет все компоненты системы вывести в видеоокно, таким же образом, как это выполняется для интерактивных поэтажных планов (графических схем). Для этого нужно просто выделить видеоокно, где необходимо разместить компонент системы (приложение EntraPass, луч, шлюз, контроллер и др.). Видеоокна настраивают в меню Video (закладка* ***Video*** *>* ***Video*** *views).*

Конфигурация приложений EntraPass

Минимальные требования к конфигурации программного пакета EntraPass включают в себя сервер, приложение типа Рабочая станция APM (приложение для мониторинга) и приложение типа Шлюз. Приложение Шлюз можно интегрировать с рабочей станцией EntraPass и установить на одном компьютере. В программное обеспечение входит несколько приложений, а именно:

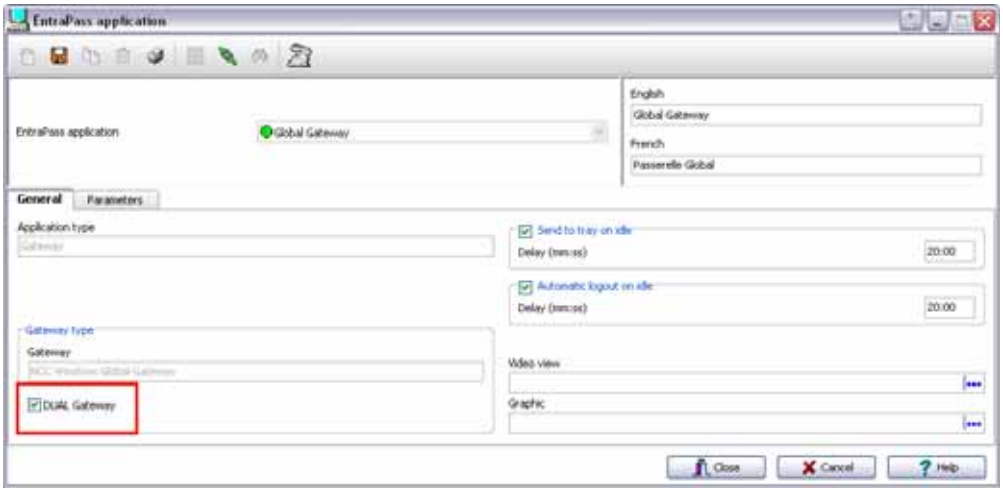
- Приложение Рабочая станция APM
- Приложение Сервер
- Одно приложение Глобальный Шлюз
- Одно приложение Corporate Ш*люз*
- а также ряд утилит, включая редактор языков (Vocabulary Editor), Express Database и др.

Сервер EntraPass рекомендуется установить на отдельном компьютере, чтобы обеспечить устойчивость работы системы. Диалоговые меню приложений EntraPass позволяют операторам настроить компьютеры, на которых установлена система. Сюда входит описание конфигурации компьютеров, на которых установлено следующее программное обеспечение: приложения APM рабочая станция (EntraPass Workstation), Шлюз (Gateways), программы для работы зеркальной базы данных на резервном сервере (Mirror Database and Redundant Server), а также компьютеров, на которых установлен интерфейс SmartLink (если используется). Чтобы настроить конфигурацию приложений EntraPass, следует установить значения следующих параметров:

- Общие параметры, применимые ко всем компьютерам, на которых установлена система EntraPass
- Параметры безопасности (применяемые во всех приложениях EntraPass)
- Фильтры (чтобы указать, какие шлюзы и приложения EntraPass должны отправлять сообщения на настраиваемое приложение типа APM Рабочая станция).
- Элементы управления сообщениями/тревогами

Настройка конфигурации приложения EntraPass

1 В главном окне EntraPass открыть закладку **Devices** (Устройства), нажать кнопку **EntraPass applications** (Приложения EntraPass). После этого открывается главное окно приложений EntraPass.



ПРИМЕЧАНИЕ: *В зависимости от типа выбранного приложения в окне EntraPass Application отображаются разные параметры. Например, если тип приложения – APM рабочая станция (Workstation), то отображаются закладки* ***Workstation*** *(Рабочая станция)****, Gateway*** *(Шлюз) и* ***Site*** *(Луч). Если же выбрано приложение типа Резервный сервер, то появляется закладка* ***Redundant server****.*

2 В выпадающем списке **EntraPass application** выделить приложение, конфигурацию которого необходимо настроить. Этот список содержит все приложения EntraPass, которые были установлены и зарегистрированы. В поле **Application type** (Тип приложения) отображается тип выбранного объекта. Выпадающий список содержит такие позиции, как Workstation (Рабочая станция), Gateway (Шлюз), Mirror Database and Redundant Server (Резервный сервер с зеркальной базой данных) и др.

3 Двойной Шлюз (**Dual Gateways),** включенный под Global шлюзом windows позволяет вам одновременно запускать Global и Corporate Шлюзы одноврмеенно . Это опция добавляет только только один Шлюз Corporate и на это не требуется дополнительной лицензии.

4 Указать имя для выбранного приложения EntraPass. Если программное обеспечение работает на двух языках, например, на английском и на французском, то имя можно указать на английском и на французском языке.

5 Нажать **Save** (Сохранить) для активации нового приложения.

Назначение общих параметров (раздел General)

Под закладкой **General(Общие)** собраны общие параметры, описывающие работу системы в случае бездействия оператора и неиспользования клавиатуры в течение определённого времени.

1 В целях повышения безопасности работы следует выбрать, как должна работать система в том случае, когда оператор не проявляет никакой активности. Это необходимо для защиты от несанкционированного доступа к системе посторонних лиц. По умолчанию установлено время задержки 20 минут. Можно использовать это значение или изменить его.

- Чтобы приложения EntraPass автоматически сворачивались в случае бездействия клавиатуры, следует выделить опцию **Send to tray on idle** (Если не используется, отправлять в трей). В таком случае окно приложения будет свёрнуто и отправлено на панель задач, если ни одна клавиша клавиатуры не нажата в течение указанного времени (укажите время в поле Send to tray on idle).
- Чтобы автоматически прекратить сеанс, если клавиатура не используется определённое время, следует поставить флажок напротив **Automatic Logout on idle** (Если не используется, автоматически закончить сеанс). В этом случае необходимо также указать время, через которое сеанс оператора будет автоматически завершён.

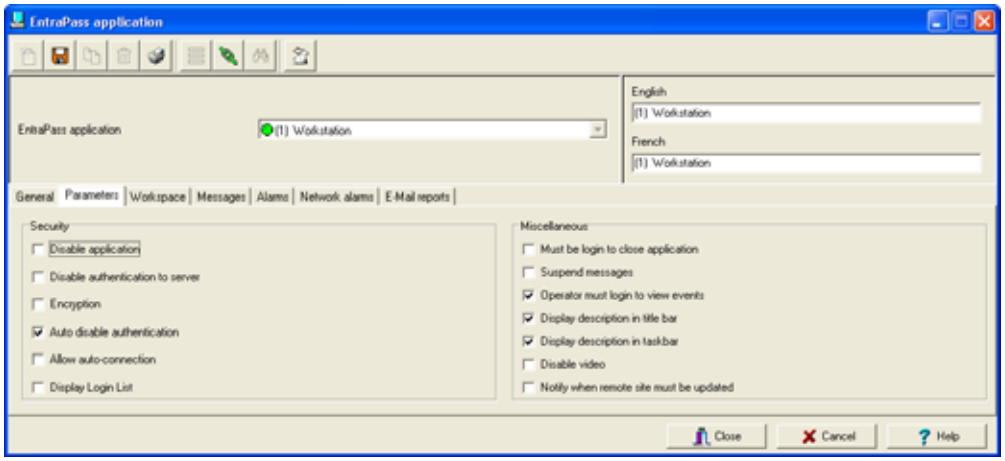
2 Если разрешено видеонаблюдение, то появляется поле **Video view** (Видеовид). В таком случае следует выделить ячейку видеовида, в которой следует отображать описываемый компонент. Подробнее о настройке видеоокон *в Главе 6 Назначение окон видео VideoView на стр. 228*.

3 В списке **Graphic** (Графические схемы) можно выбрать графический план для данного приложения, если необходимо. Подробные сведения об графических схемах *в Главе 5 Назначение графических схем на стр. 195*.

Описание параметров безопасности (раздел Parameters)

Этот раздел применим ко все приложениям EntraPass: рабочим станциям EntraPass Workstations, шлюзам Gateways, интерфейсу SmartLink (если он установлен), резервному серверу с зеркальной базой данных (Mirror Database and Redundant Server) и др.

1 В окне приложений EntraPass applications выбрать тип приложения Workstation (Рабочая станция) и перейти к закладке **Parameters** (Параметры).



2 Установить, где требуется, флажки:

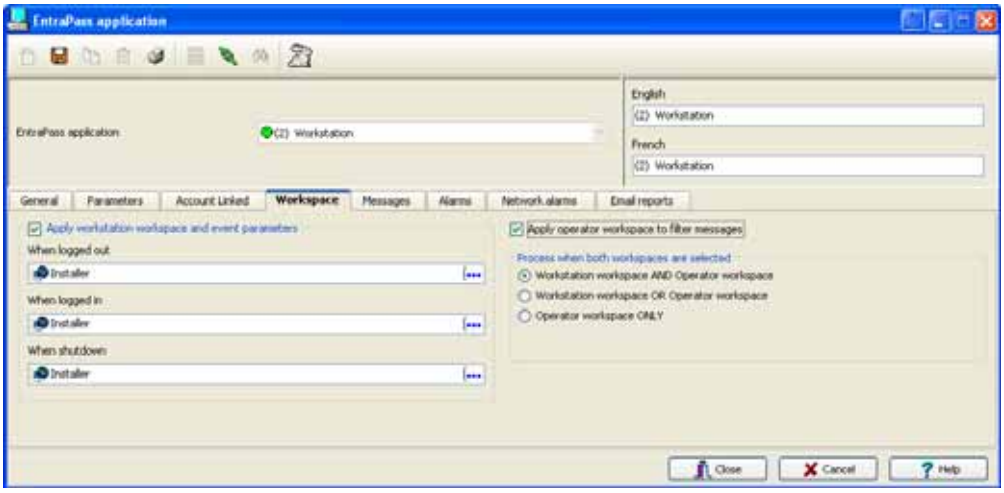
- **Disable application** (Запретить приложение). При выборе этой опции оператор не сможет запустить приложение. Эту опцию следует назначать с осторожностью.
- **Disable authentication to server** (Запретить аутентификацию на сервере). Если поставить флажок, то приложение нельзя будет зарегистрировать на сервере.

- **Encryption** (Кодирование). Выбрать эту опцию, чтобы кодировать все входящие и исходящие сообщения для данного приложения.
- **Auto disable authentication** (Автоматически запретить аутентификацию). При выборе этой опции система автоматически запретит аутентификацию после первой же аутентификации приложения.
- **Allow auto-connection** (Разрешить автоматическое соединение). Если поставить флажок напротив этой опции, рабочая станция будет пытаться автоматически подсоединиться к серверу в случае обрыва связи.
- **Display login list** (Показывать регистрационный список). Позволяет сохранять последние пять имён пользователей, зарегистрировавшихся в системе и отображать их при открытии новых сессий. Это более быстрый способ начать сессию, так как оператору нужно ввести только имя пользователя и пароль. Если оставить эту опцию неактивной (как по умолчанию), то безопасность работы будет выше, так как операторы должны будут перед каждым сеансом вводить достоверные имя пользователя и пароль для доступа в систему EntraPass.
- **Must be login to close application** (Требовать регистрацию для закрытия приложения). Если эта опция активна, операторы должны регистрироваться, чтобы выйти из программы EntraPass.
- **Suspend messages** (Приостановить сообщения). Отключает все входящие сообщения для выбранных приложений EntraPass. Рекомендуется использовать данную опцию в тех случаях, когда рабочая станция EntraPass используется только для настройки компонентов или когда сообщения не нужны.
- **Operator must login at least once to display messages** (Для отображения сообщений требовать регистрацию не менее одного раза). Обязывает операторов зарегистрироваться хотя бы раз с достоверным именем и паролем, чтобы просмотреть **Display description in title bar** (Показывать описание в строке заголовка). Служит для отображения описания приложений EntraPass в строке заголовка (верхняя строка).
- **Display description in taskbar** (Показывать описание на панели задач). Служит для отображения описания приложений EntraPass на панели задач (нижняя строка).
- **Disable video** (Запретить режим видео). Убирает команды для работы с видеоокнами из интерфейса пользователя рабочей станции EntraPass. При установке флажка напротив этой опции список событий видео (Video Events List), просмотр видеозаписей (Video Playback) и рабочий стол видеонаблюдения (Video desktop) станут недоступны. Операторы с соответствующим уровнем доступа смогут настраивать режим видеонаблюдения, но не смогут просматривать видеозаписи или живое видео.
- **Notify when remote sites must be updated** (Уведомлять о необходимости обновления удалённых лучей). При установке флажка напротив этой опции система будет получать уведомление перед обновлением удалённых лучей через модем. Если эта опция выбрана, то операторы будут получать уведомление по модемной связи при каждом изменении данных, имеющих отношение к лучам (например, расписаний, контроллеров и т.п.). При этом у них будет выбор: внести изменения на удалённые сайты (**Yes**) или отклонить внесение изменений (**No**), либо нажать кнопку **Details** (Подробно) и выбрать, на каких сайтах выполнить обновление.

Назначение рабочего пространства (раздел Workspace)

Закладка **Workspace** (Рабочее пространство) служит для выбора конфигурации рабочего пространства и параметров событий, которые будут применяться для конкретной рабочей станции,

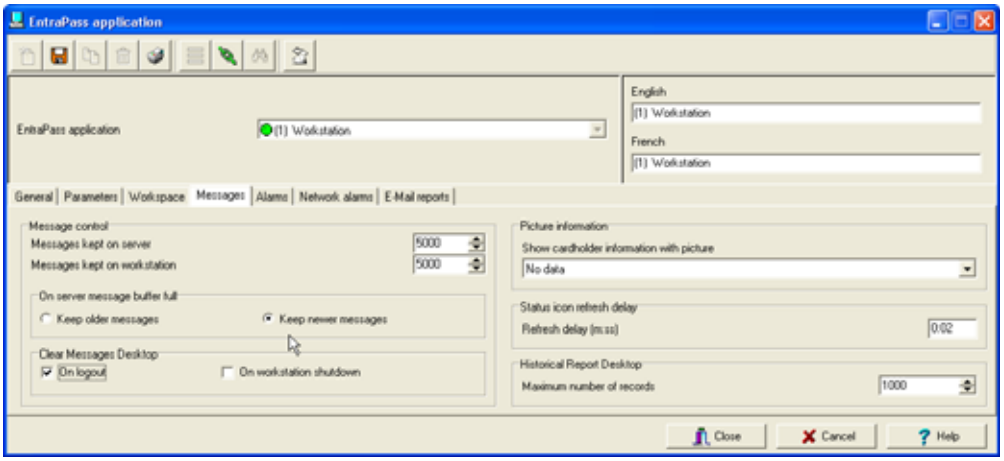
что позволяет создавать географические привязки в системе EntraPass. Эта функция позволяет описать, как должна работать рабочая станция.



- **Apply workstation workspace and event parameters** (Применять рабочее пространство АРМ и параметры событий). Когда вы выделите это, будет разрешаться для рабочей области АРМ назначение назначения опредленных событий.
  - **When logged in** (Во время сеанса). Применить выбранные правила рабочего пространства, когда на рабочей станции зарегистрирован оператор, используя эти правила вместо описания рабочего пространства оператора.
  - **When shutdown** (После выключения). Применить выбранные правила рабочего пространства, когда рабочая станция выключена.
- **Apply operator workspace to filter messages** (Применить правила рабочего пространства оператора для фильтрации сообщений). Когда оператор зарегистрируется в системе, рабочая станция будет применять правила рабочего пространства оператора.
- В поле **Process when both workspaces are selected** (Правила обработки при использовании обоих рабочих пространств) перечислены опции, доступные при установке флажков в обоих полях **Apply workstation workspace and event parameters** и **Apply operator workspace to filter messages**.
  - **Workstation workspace AND Operator workspace** (Рабочее пространство рабочей станции И рабочее пространство оператора). Отбор событий сначала на уровне настроек рабочего пространства рабочей станции, а затем снова, на уровне настроек рабочего пространства оператора, который в данный момент зарегистрирован в системе на этой рабочей станции.
  - **Workstation workspace OR Operator workspace** (Рабочее пространство рабочей станции ИЛИ рабочее пространство оператора). Будет выбираться рабочее пространство, у которого выше уровень в иерархии.
  - **Operator workspace ONLY** (ТОЛЬКО рабочее пространство оператора). Рабочее пространство оператора будет иметь приоритет выше, чем пространство рабочей станции.

Назначение параметров управления сообщениями

1 Нажмите на закладку **Messages** (Сообщения), чтобы определить как сообщения должны обрабатываться/проходить, когда АРМ подключен (или не нет) к серверу.



ПРИМЕЧАНИЕ: *Сообщения, которые поступают на рабочую станцию, следует настроить в меню* ***назначение рабочих столов*** *(Desktop definition menu). Подробнее смотрите смотрите в Главе 11* **Рабочие столы EntraPass** *на стр. 367*

2 В меню **Messages** (сообщения) необходимо выполнить следующие настройки:
- Указать, сколько сообщений должно оставаться на сервере, когда АРМ (рабочая станция EntraPass) работает автономно, то есть не подключена к серверу. В буферной памяти сервера может храниться до 100 000 сообщений на каждую рабочую станцию EntraPass (по умолчанию 5 00).
- Указать, сколько сообщений должно **храниться на рабочей станции (kept on the workstation)**. Каждая рабочая станция EntraPass может хранить максимум 100 000 сообщений. По умолчанию установлено 5 000 сообщений.

ПРИМЕЧАНИЕ: *Рабочая станция EntraPass всегда сохраняет новые события. Для просмотра давних событий следует обратиться к архивным отчётам. Более подробно порядок обращения к отчётам описан* ***в Главе 13 Отчеты на стр. 437***

3 Указать, какие сообщения (старые или новые) следует оставить на сервере после заполнения всех доступных ячеек памяти.
- **Keep older messages** (Сохранять старые сообщения). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет старые сообщения у себя, а новые отправляет в архив к себе.
- **Keep newer messages** (Сохранять новые сообщения). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет новые сообщения у себя, а старые отправляет в архив. Это просходит по правилу: первый пришел, первый ушел.

4 IВ разделе **Clear Message Desktops** (Очищать сообщения с рабочего стола АРМ) указать, когда выполнять удаление сообщений:
- **On logout** (При обычном окончании сеанса оператора)
- **On workstation shutdown** (При полном выключении рабочей станции EntraPass)

5 В разделе **Picture information** (Сведения о фотографии) выбрать, какая информация будет отображаться в поле под фотографией владельца идентификационной карты. Выпадающий список **Show cardholder information with picture** (Показать рядом с фотографией сведения о владельце карты) содержит 10 изменяемых информационных полей (Card information 1, Card information 2 и т.д.).

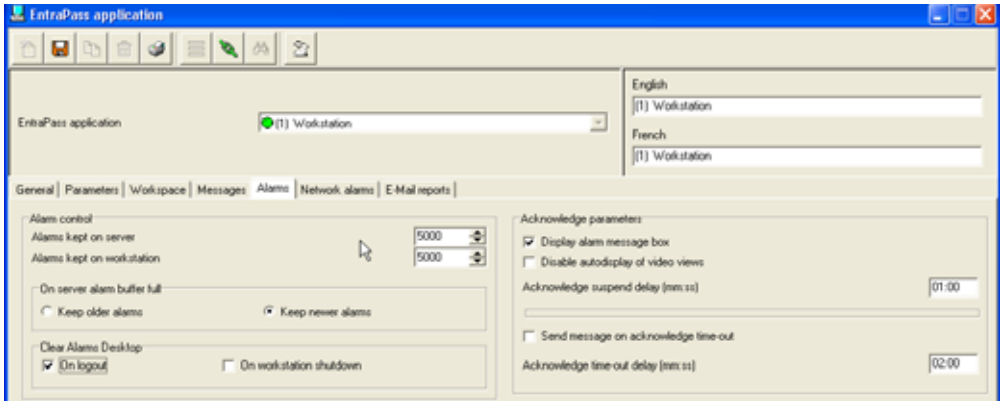
ПРИМЕЧАНИЕ: *По умолчанию в этих полях отображаются надписи “card information #1” ... “card information #10”. Эти надписи можно заменить другими по своему желанию. Более подробная информация об изменении надписей в информационных полях идентификационной карты приведена смотрите в Главе 8* **Индивидуальная настройка названий информационных полей идентификационной карты** *на стр. 289.*

6 В разделе **Status icon refresh delay** (Задержка обновления пиктограммы состояния) указать интервал обновления состояния приложений EntraPass, отображаемого при помощи пиктограммы в строке состояний. Диапазон допустимых значений – от 0,01 до 4,59 сек шагом 0,01 сек.

7 В поле **Maximum Records in Report Desktop** (Максимальное число записей на рабочем столе отчётов) указать, сколько записей извлекать из архива и отображать на экране, при вызове работе с архивными отчетами. Максимальное число 200 000. .

Назначение параметров управления тревогами (раздел Alarms)

1 Под закладкой **Alarms** (Тревоги) находятся параметры, описывающие порядок обработки тревог, если рабочая станция EntraPass подключена (или нет) к серверу.



ПРИМЕЧАНИЕ: *Рабочие столы (Desktops) тревог следует настраивать в меню Рабочие столы EntraPass. Подробнее смотрите в Главе 11 Рабочие столы EntraPass на стр. 367*

2 В меню Alarms (Тревоги) необходимо выполнить следующие настройки:

- Указать, сколько тревог должно **оставаться на сервере**, когда рабочая станция EntraPass работает автономно, то есть не подключена к серверу. В буферной памяти сервера может храниться до 100 000 тревог на каждую рабочую станцию EntraPass (по умолчанию 5 00).
- Указать, сколько тревог должно **храниться на рабочей станции**. Каждая рабочая станция EntraPass может хранить максимум 100 000 тревог. По умолчанию установлено 5 000 тревог.

ПРИМЕЧАНИЕ: *Рабочая станция EntraPass всегда сохраняет новые события. Для просмотра архивных событий следует обратиться к архивным отчётам. Подробнее о получении отчетов в Главе 13 Отчеты на стр. 437*

3 Указать, какие тревоги (старые или новые) следует оставить на сервере в буфере после его заполнения:

- **Keep older alarms** (Сохранять старые тревоги). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер держит старые тревоги в буфере и убирает в архив новые.
- **Keep newer alarms** (Сохранять новые тревоги). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет новые тревоги у себя, а старые отправляет в архив. Это просходит по правилу: первый пришел, первый ушел.

4 В разделе **Clear Alarms Desktops** (Очищать рабочие столы тревог) указать, когда выполнять удаление тревог:

- **On logout** (При обычном окончании сеанса оператора)
- **On workstation shutdown** (При полном выключении рабочей станции EntraPass)

5 Кроме того, можно назначить параметры подтверждения (Acknowledgement parameters). Чтобы окно для подтверждения тревоги (инструкция оператора) появлялось даже если оператор работает на другом АРМ, следует поставить галочку в поле **Display alarm message box** (Показывать окно тревожных сообщений). Когда эта опция включена, вы должны ввести задержку, в течении которой окно тревоги будет ждать подтверждения (Acknowledge suspend delay). По окончании этого времени окно тревожных сообщений снова появится перед оператором, требуя подтверждение.

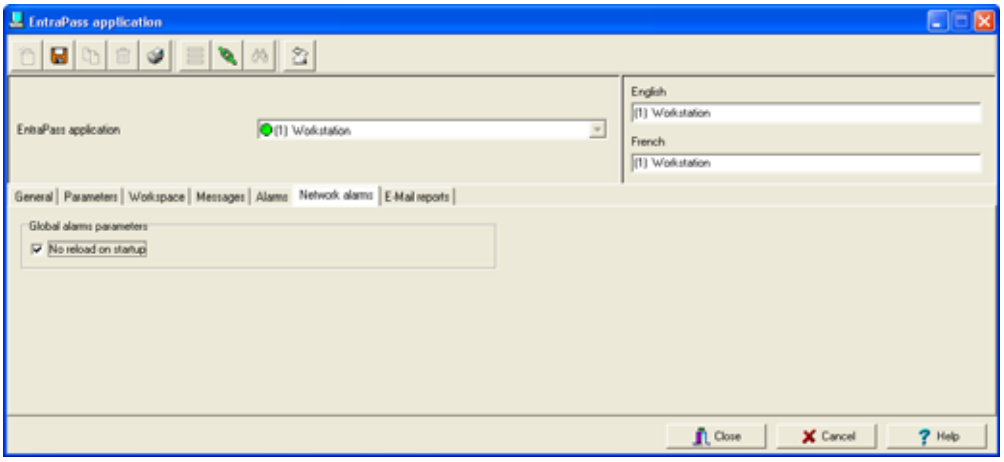
6 Если поставить флажок в поле **Disable auto display of video views** (Запретить автоматическое отображение видеоокон), то эта рабочая станция не будет автоматически показывать видеоокна

на экране. Фактически, видеоокна, определенные как тревожные и прикреплённые к компонентам системы, автоматически отображаются на экране при получении сигнала тревоги.

7 Если выделить опцию **Send message on acknowledge time-out** (Посылать сообщение, если по истечении времени отсутствует подтверждение тревоги), то во всех случаях, когда от оператора не было получено подтверждение в течении определенного времени, то будет формироваться сообщение “Acknowledge time-out” (Истекло время для подтверждения, указанное в строке **Acknowledge time-out delay**). Это сообщение будет отправлено на рабочий стол сообщений (Message) и рабочий стол тревог (Alarms). Более подробная информация приведена *в Главе 11 Рабочие столы EntraPass на стр. 367*.

Назначение сетевых тревог (Network Alarms)

Закладка **Networks alarms** (Сетевые тревоги) появляется только в том случае, если опция **Use network alarm** (Использовать сетевые тревоги) выделена в меню System parameters (Системные параметры), под закладкой **Networks alarms** в разделе **Server** (Серверы).



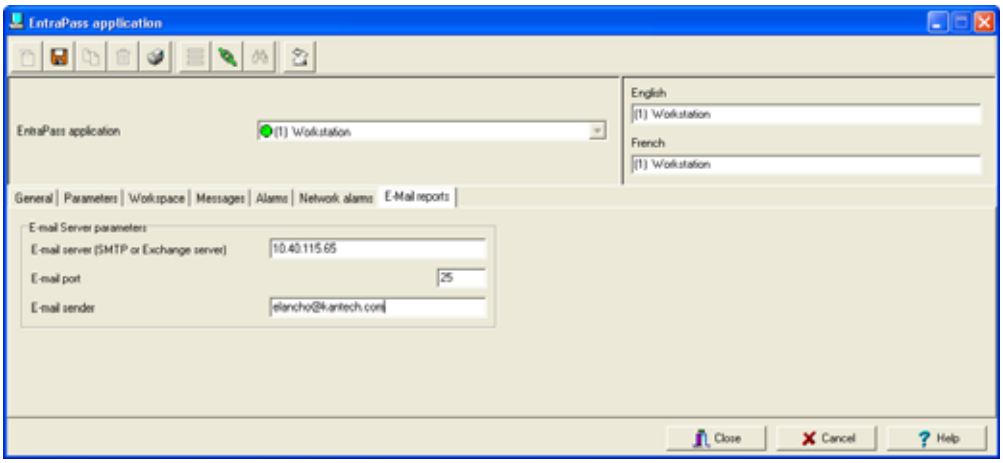
1 Здесь необходимо выбрать, требуется ли при запуске АРМ повторно загружать все системные (сетевые) тревоги. Системные тревоги хранятся в базе данных сервера. Если в поле **No reload on startup** (Не загружать повторно при запуске) поставить флажок, то повторную загрузку системных тревог операторам придётся выполнять вручную.

ПРИМЕЧАНИЕ: *Повторную загрузку системных тревог выполняют на рабочем столе через Network Alarms (Сетевые тревоги). Для этого следует открыть рабочий стол, правой кнопкой мыши щёлкнуть на одном из пунктов, чтобы вызвать контекстное меню, и выбрать в меню пункт **Refresh** (Обновить). Эту опцию можно использовать для быстрого запуска; она пригодится при медленном соединении.*

Назначение параметров электронных отчётов (E-Mail Reports)

Система EntraPass и EntraPass WebStation может самостоятельно автоматически отправлять отчёты по электронной почте.

1 Открыть закладку **E-mail** в главном окне приложения EntraPass.



2 В поле **E-mail server (SMTP or Exchange server)** указать IP-адрес почтового сервера, который будет использоваться для отправки электронных писем.

3 В поле **E-mail Port** (Почтовый порт) указать имя порта, который будет использоваться для отправки электронной почты (обычно 25).

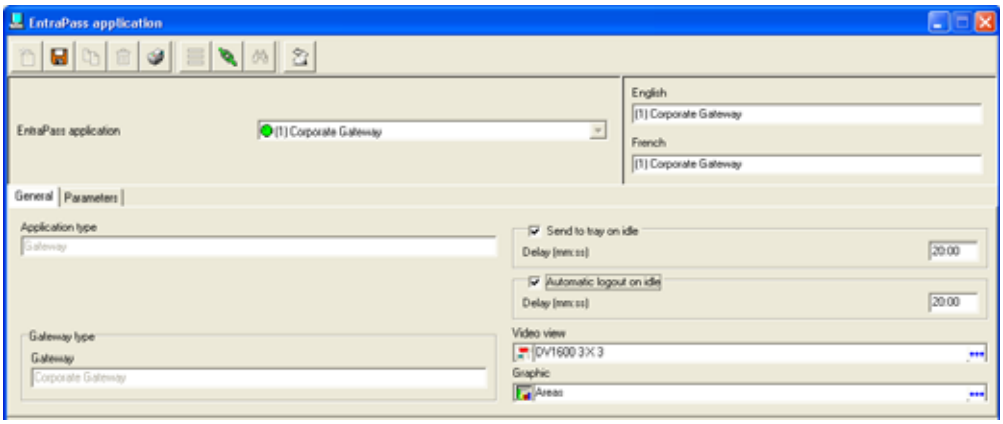
4 В поле **E-mail sender** (Отправитель) указать достоверный электронный адрес отправителя. Этот адрес будет использоваться для идентификации почтового сервера.

Настройка конфигурации приложения Шлюз (Gateway)

Шлюз EntraPass преобразует информацию, полученную с контроллера или луча, и передаёт преобразованные данные на сервер. Сервер отправляет их определённому приложению EntraPass. Шлюз преобразует данные, полученные с АРМ (рабочей станции EntraPass), и передаёт их контроллерам. Таким образом, шлюз взаимодействует с лучами и с приложением EntraPass. Приложение типа Шлюз позволяет мониторить лучи контроллеров, подключенные к шлюзу. EntraPass Global Edition включает в себя в базовом пакете один Global Шлюз. Шлюзы Global , NCC-8000, Corporate и KT-NCC могут быть использованы в EntraPass Global Edition. При этом в системе может быть до 40 Corporate Шлюзов , 128 Global Шлюзов и 128 KT-NCC Шлюзов.

Назначение общих параметров для Шлюза (раздел General)

1 В строке **EntraPass application** (Приложение EntraPass) необходимо выбрать приложение Шлюз, которое требуется настроить. Если в строке EntraPass application выбран тип приложения Gateway (Шлюз), то под закладкой **General** (Общие) в поле **Application type** (Тип приложения) отображается надпись “Gateway”.



2 Более подробные сведения по настройке параметров системы в режиме бездействия (on idle) *см. "Конфигурация приложений EntraPass" на стр. 64*.

3 Для назначения параметров безопасности для шлюзов *см. "Описание параметров безопасности (раздел Parameters)" на стр. 65*.

Настройка интерфейса Oracle/MS-SQL (CardGateway)

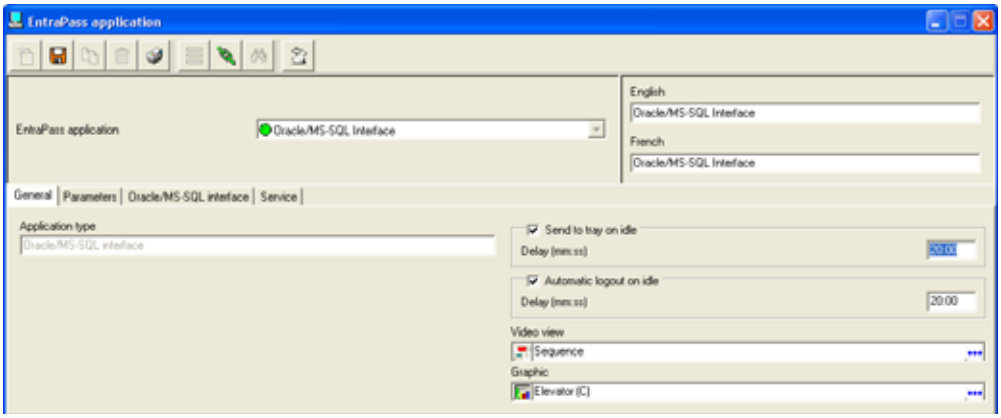
Интерфейс Oracle/MS-SQL создаёт в реальном времени зеркальную копию баз данных EntraPass по картам (таблицу карт, таблицу групп карт, таблицу типов карт и таблицу бейджей) в базе данных MS-SQL или Oracle. В дополнение, это позволяет операторам взаимодействовать с системной базой данных карт с помощью своих программ MS-SQL или Oracle. Таким образом, можно добавлять, изменять и удалять карты или получать сведения о картах из базы данных EntraPass. Данные по картам обновляются во всех базах данных, независимо от того, для каких целей используется программа (для изменения или для обновления базы данных). Интерфейс MS-SQL гарантирует что все изменения произведены для отправки данных на сервер и потом на рабочие станции.

ПРИМЕЧАНИЕ: *Для использования интерфейса Oracle/MS-SQL требуется дополнительная лицензия.*

Будьте уверены, что клиентское обеспечение MS-SQL или Oracle установлено на том же компьютере, что и лицензия EntraPass Oracle/MS-SQL. Интерфейс Oracle/MS-SQL рекомендуется ставить на отдельном компьютере, на котором установлена система EntraPass. При установке двух приложений на одном компьютере могут возникнуть проблемы при обмене данными между системой EntraPass и сервером Oracle или MS-SQL. Чтобы настроить конфигурацию интерфейса базы данных Oracle/MS-SQL, следует указать параметры:

- Общие параметры (General), применимые к интерфейсу баз данных Oracle/MS-SQL, включая параметры безопасности приложения EntraPass
- Параметры базы данных (Database), включая права доступа к базе данных

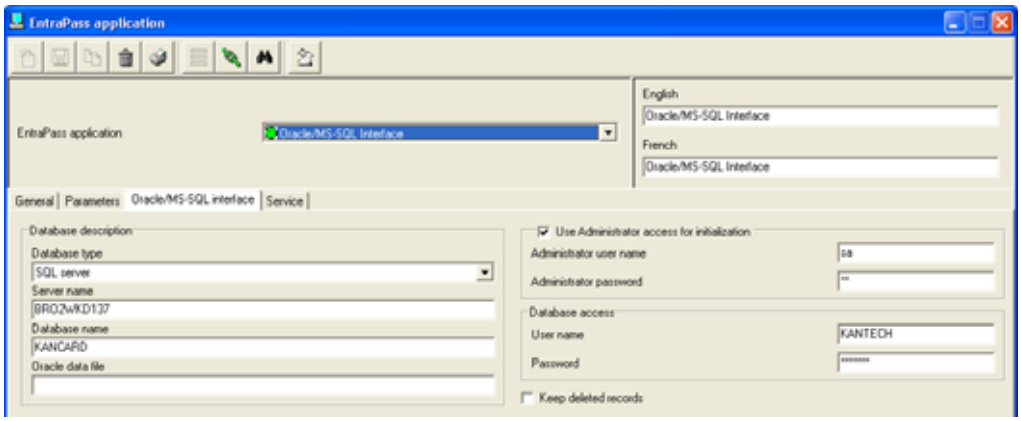
1 В строке **EntraPass application** в выпадающем списке выделить приложение Oracle/MS-SQL Interface.



2 Настроить приложение, на которое вы установили интерфейс Oracle/MS-SQL. Более подробные сведения по настройке *см. "Конфигурация приложений EntraPass" на стр. 64*.

3 Настроить параметры безопасности для интерфейса Oracle/MS-SQL под закладкой **Parameters** (Параметры). Подробнее *см. "Описание параметров безопасности (раздел Parameters)" на стр. 65*.

4 Открыть закладку **ORACLE/MS-SQL Interface,** указать параметры связи между программным обеспечением EntraPass и клиентской базой данных и настроить права доступа к базе данных.



5 В выпадающем списке **Database type** (Тип базы данных) выбрать сервер базы данных: сервер Oracle 8.0, сервер Oracle 7.3 или сервер SQL. База данных имеет разную конфигурацию для разных версий сервера, поэтому очень важно правильно указать версию сервера.

ПРИМЕЧАНИЕ: *Если версия сервера указана неверно, интерфейс Oracle/MS-SQL не будет работать, и связи с сервером не будет.*

6 Указать имя сервера базы данных в строке **Server name**.

7 Указать имя базы данных Oracle или SQL в строке **Database Name**.

8 Если используется сервер типа Oracle, указать в строке **Oracle data file** имя файла данных, доступ к которым необходимо получить.

ПРИМЕЧАНИЕ: *Серверы Oracle и SQL могут содержать больше одной базы данных. Для доступа к базе данных SQL необходимо указать её имя, а для доступа к базе данных Oracle необходимо указать её имя и имя особого файла данных. Параметры баз данных для каждого конкретного случая следует узнавать у системного администратора.*

9 Если необходимо, поставить флажок в поле **Use administrator Access for Initialization** (Для инициализации использовать уровень доступа администратора). Эта опция позволяет вам ввести имя и пароль администратора.

ПРИМЕЧАНИЕ: *Настоятельно рекомендуется отметить флажком эту опцию. В противном случае придётся вручную создавать базу данных, имя и пароль пользователя на сервере баз данных.*

10 Введите имя пользователя в поле "**Administrator user name**" и пароль в поле "**Administrator password**". Программа автоматически создаст базу данных, имя и пароль пользователя на сервере баз данных.

11 IB области **Database access** (Доступ к базе данных) указать имя пользователя (Username) и пароль (Password), которые будут использованы программой CardGateway для соединения с базой данных Oracle/SQL

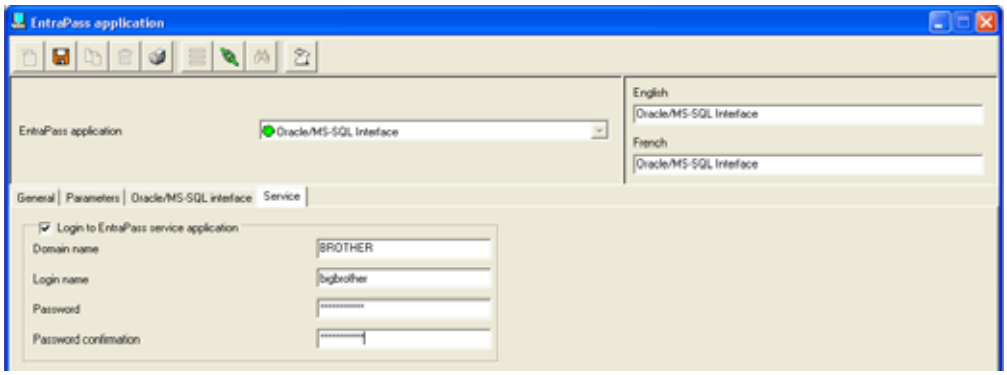
ПРИМЕЧАНИЕ: *Процедура доступа к базе данных не позволяет с помощью программы CardGateway создавать или изменять действующий профиль пользователя на сервере Oracle/SQL.*

12 Отметить галочкой опцию **Keep deleted records** (Хранить удалённые записи), чтобы сохранять запись карты даже после её удаления из базы данных EntraPass. Запись будет храниться в базе данных интерфейса Oracle/MS-SQL.

ПРИМЕЧАНИЕ: *Если вы не выделите эту опцию, то удалённые записи навсегда стираются из базы Oracle/MS-SQL.*

ПРИМЕЧАНИЕ: *При автоматическом создании базы данных идентификационных карт на сервере SQL или Oracle её максимальный размер составляет **50 Мб**. Если необходимо увеличить размер базы данных, её следует создавать вручную. Более подробные указания изложены в следующем разделе "Создание баз данных сервера вручную".*

13 Под закладкой **Service** (Служба) собраны параметры, необходимые для входа в систему при использовании интерфейса Oracle/MS/SQL в режиме службы и для необходимости печати MUSTER отчета.



- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле Login to EntraPass service application (Регистрационные данные для работы приложения в режиме службы).

- Для интерфейса Oracle/MS-SQL ввести имя домена в поле Domain name и имя пользователя в поле Login name.
- Указать пароль в поле **Password** и повторить его ввод в поле **Password confirmation**.

Создание баз данных сервера вручную

Чтобы интегрировать базу данных с системой EntraPass, необходимо создать базу данных и затем создать в этой базе оператора Kantech. В случае использования сервера MS-SQL необходимо выполнить следующие действия:

Создание оператора вручную на сервере ORACLE/MS-SQL

Чтобы интегрировать ORACLE/MS-SQL с системой EntraPass, необходимо, прежде всего, создать базу данных, которая будет затем использоваться.

1. Правой кнопкой мыши вызвать контекстное меню, щёлкнув по папке Database (База данных), и выбрать пункт **New Database** (Новая база данных).
2. Указать имя базы данных в поле **Database name**.
3. Нажать **OK** после ввода имени базы

Создание оператора KANTECH для сервера MS-SQL

Теперь необходимо создать оператора, который будет использоваться интерфейсом Oracle/MS-SQL для входа на сервер MS-SQL.

1. Щёлкнуть правой кнопкой мыши в поле **Logins** (Входы в систему) и выбрать пункт **New Login** (Новый вход).
2. Ввести имя **kantech** (в нижнем регистре) в поле **Name** (Имя).
3. Убедиться, что в поле **SQL Server Authentication** (Аутентификация сервера SQL) поставлен флажок.
4. Ввести имя **kantech** (в нижнем регистре) в поле **Password** (Пароль).
5. Открыть закладку **Database Access** (Доступ к базе данных).
6. Выделить имя базы данных, созданное в п. 2. Если выделена эта опция, то в нижней части окна отображается надпись “Database Roles - Permit in database role” (Задачи базы данных – Разрешить использовать как базу данных).
7. Чтобы иметь возможность вносить изменения в базу данных, следует установить флажок напротив опции **Public and db_owner** и нажать **OK** для сохранения и выхода. Откроется окно для ввода пароля.
8. Ввести имя kantech (в нижнем регистре) и нажать **OK**, чтобы выйти.

Создание оператора KANTECH для сервера Oracle

1. Войти на сервер ORACLE под именем администратора. По умолчанию может быть использовано имя “**kantech**”.
2. Создать базу данных. По умолчанию можеь быть использовано имя базы “**KanCard**”.
3. Создать профиль пользователя. По умолчанию может быть использовано имя и пароль “**kantech**”.
4. Назначить для оператора kantech права доступа “**Owner**” (Владелец).

ПРИМЕЧАНИЕ: *Чтобы использовать свои настройки, вместо указанных здесь по умолчанию, то необходимо правильно указать в базе данных и в программе EntraPass имя базы данных (Database name), имя пользователя (User name) и пароль (Password).*

Настройка конфигурации зеркальной базы данных и резервного сервера

Зеркальная база данных (Mirror Database) проверяет наличие связи себя с основным сервером. Она создаётся в реальном режиме времени и представляет собой копию базы данных системы и элементов реестра системы Windows, за исключением базы данных карт Oracle/MS-SQL.

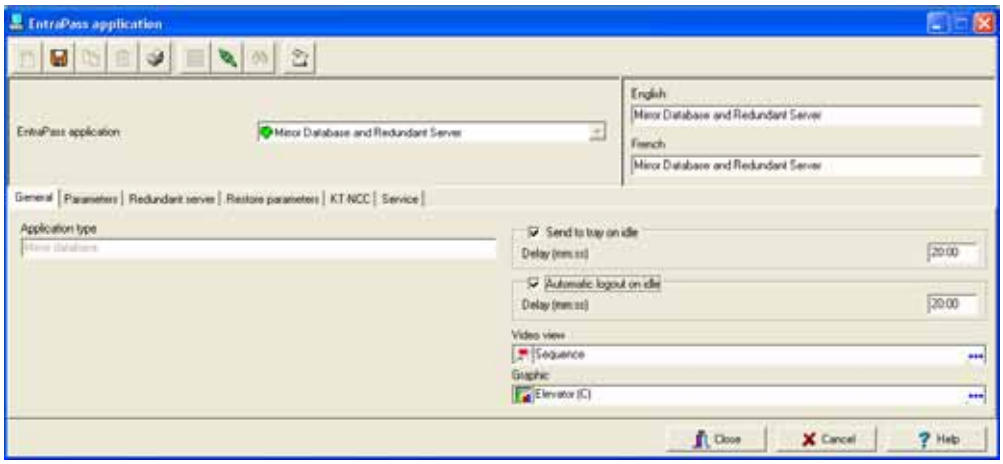
Если связь между зеркальной базой данных и основным сервером потеряна, резервная\зеркальная база данных автоматически запускает резервный сервер взамен основного после окончания определённой временной задержки. Программное обеспечение резервного сервера зеркальной базой данных нельзя поставить на компьютер, на котором установлен сервер Entrapass. Это ПО должно быть установлено на отдельном компьютере.

ПРИМЕЧАНИЕ: *При желании можно создать в системе несколько резервных серверов с зеркальными базами данных. Для использования зеркальной базы данных и резервного сервера требуется дополнительная лицензия.*

Чтобы настроить АРМ рабочую станцию на работу с зеркальной базой и резервным сервером, необходимо задать следующие параметры:

- Общие параметры (General), применимые к зеркальной базе данных и резервному серверу (Mirror Database and Redundant Server), включая параметры безопасности
- Параметры резервного сервера (Redundant Server)
- Параметры восстановления (Restore parameters)
- Параметры безопасности (Security parameters)
- Параметры KT-NCC

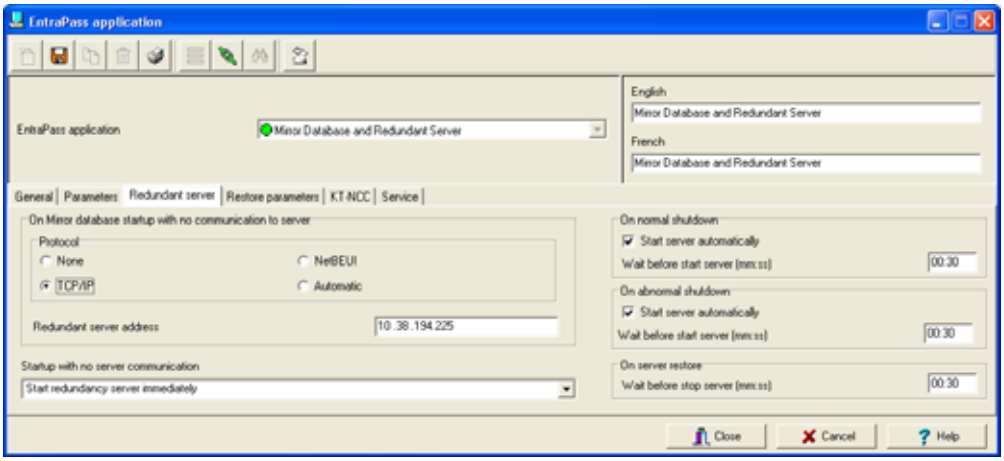
1 В выпадающем списке приложений **EntraPass application** выделить приложение "Mirror Database and Redundant Server" (Зеркальная база данных и резервный сервер).



2 Настроить параметры под закладкой **General** (Общее). Более подробно *см. "Назначение общих параметров (раздел General)" на стр. 65.*

3 Открыть закладку **Parameters** (Параметры) и настроить параметры безопасности для зеркальной базы данных и резервного сервера. Подробнее *см. "Описание параметров безопасности (раздел Parameters)" на стр. 65*

4 Открыть закладку **Redundant Server** (Резервный сервер) и настроить параметры связи для зеркальной базы данных и резервного сервера.



5 Выделить протокол, который используется для связи с компьютером, на котором стоит зеркальная база данных: **None** (не использовать), **TCP/IP** (сетевой сервер), **NetBEUI** (имя компьютера) или **Automatic** (автоматический).

ПРИМЕЧАНИЕ: *Если выбран протокол TCP/IP, на экране появляется поле* ***Redundant server address*** *(Адрес резервного сервера), в котором нужно указать TCP/IP-адрес компьютера, на котором установлена зеркальная база и резервный сервер. Это поле появляется также при использовании протокола NetBeui.*

ПРИМЕЧАНИЕ: *Если выбран протокол* ***Automatic****, то IP-адрес компьютера, на котором установлена зеркальная база и резервный сервер, будет отправлен на сервер для пересылки на все рабочие станции сети. Эта опция особенно полезна, если IP-адрес этого компьютера неизвестен, а также при использовании динамической адресации или если компьютер подключен к DHCP серверу.*

6 Указать IP-адрес резервного сервера.

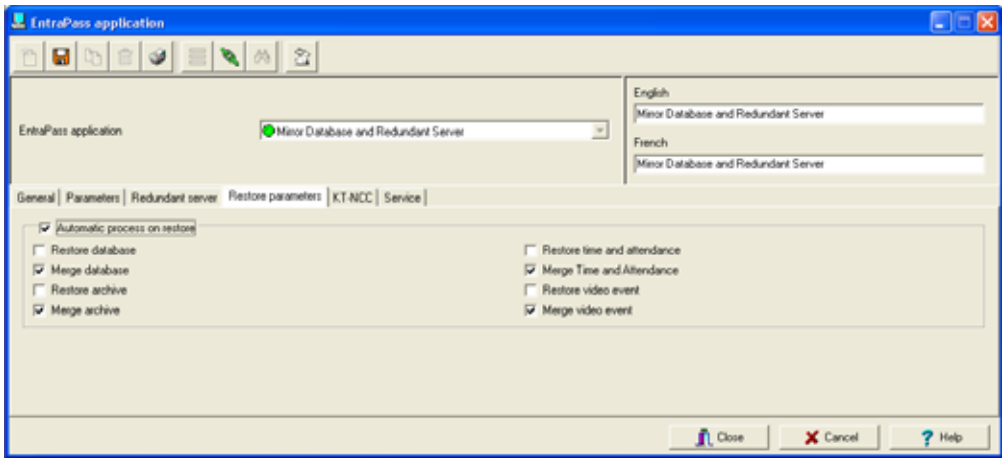
7 Выбрать действия, которые должны быть выполнены с резервным сервером в том случае, когда при запуске отсутствует связь с основным сервером (Startup with no server communication).

8 Указать параметры запуска резервного сервера в случае выключения основного сервера: это может быть автоматический запуск при стандартном выключении (когда сервер EntraPass выключает оператор) или при аварийном выключении. Зеркальная база данных запускает резервный сервер после окончания задержки, указанной в поле **Wait before start server** (Ожидание перед запуском сервера).

ПРИМЕЧАНИЕ: *Если в поле* **Start server automatically** *(Запускать сервер автоматически) не поставлен флажок, резервный сервер* ***не будет*** *запущен при обычном выключении основного сервера (то есть когда сервер выключает оператор).. Таким образом, его будет необходимо запускать вручную.*

9 Указать действия в случае возобновления нормальной работы основного сервера (**On server restore**): указать задержку, после окончания которой, резервный сервер будет остановлен когда основной сервер вернетсья к нормальному функционированию. Всё это время резервный сервер будет продолжать преобладать (не более 59:59 минут).

10 Открыть закладку **Restore Parameters** (Параметры восстановления) чтобы назначить необходимые действия резервного сервера после возобновления нормальной работы основного сервера после выключечния.

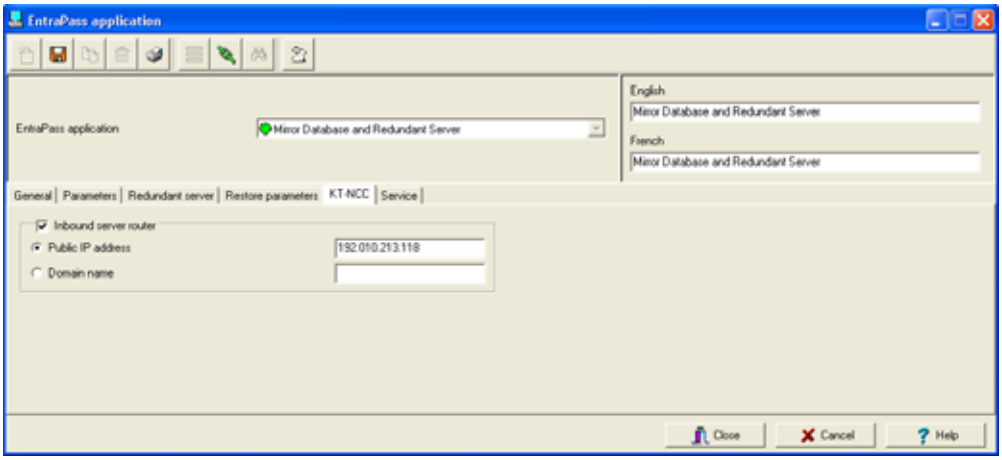


- Для того чтобы автоматизировать процесс восстановления данных с резервного сервера, поставьте флажок в поле **Automatic process on restore** (Автоматический процесс восстановления). После этого станут доступными остальные опции.
- Отметить флажками нужные опции, в зависимости от того, какие функции установлены и какие действия восстановления необходимо выполнить:
  - **Restore -** перенос всей базы данных, которая содержит все транзакции, с резервного сервера на основной сервер и переписывание поверх данных, хранящихся на основном сервере.
  - **Merge** - перенос с резервного на основной сервер тех данных, которые на основном сервере отсутствуют/не могут быть найдены.

ПРИМЕЧАНИЕ: *Вы можете выбрать* **Restore** *или* **Merge**.

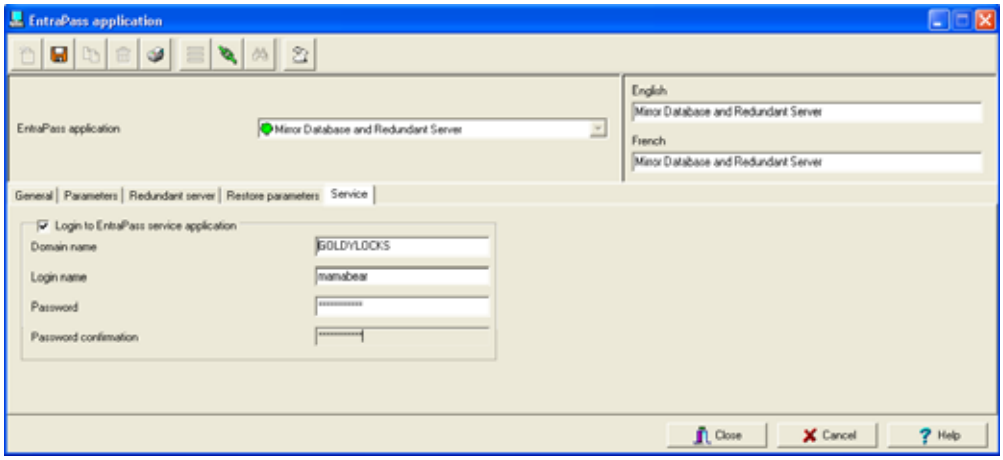
ПРИМЕЧАНИЕ: *При использовании функции* **Merge** *данные не передаются на основной сервер в тех случаях, когда, например, карта была изменена одновременно и на резервном сервере и на основном, в то время пока основной сервер был отключен.*

11 Двиньтесь на вкладку **KT-NCC** для назначения public IP адреса для KT-NCC, когда необходимо.



- Если вы хотите активировать адрес маршрутизатора **Inbound Server Router**, то поставьте флажок.
- Вы можете ввести адрес **Public IP или имя домена**.

12 Нажмите на вккладку Service (службы) для назначения авторизации, когда зеркальная база данных и резервный сервер запущены в качестве сервиса и необходимо напечатать Muster отчет.



- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login to EntraPass service application** (Регистрационные данные для работы приложения в режиме службы).
- Указать имя домена в поле **Domain name** и имя пользователя в поле **Login name** для зеркальной базы данных и резервного сервера.
- Указать пароль в поле **Password** и повторить его ввод в поле **Password confirmation**.

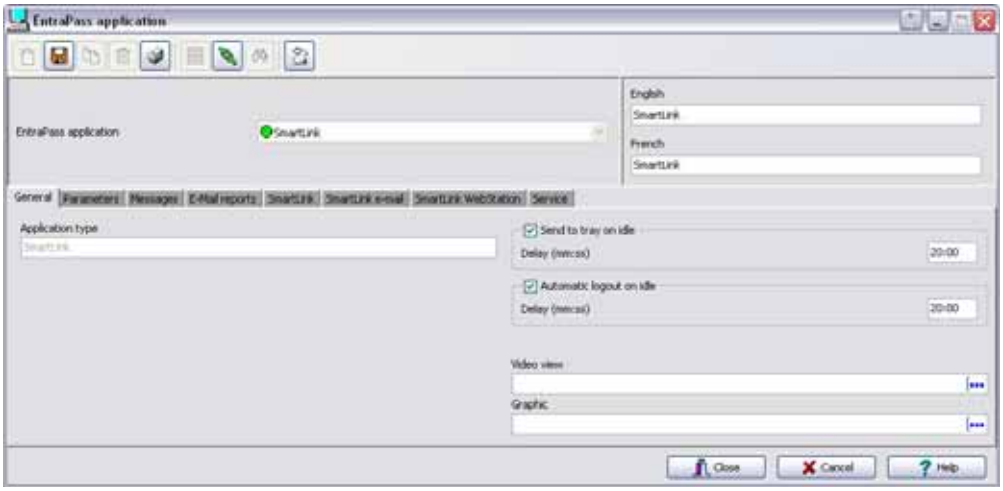
Настройка конфигурации приложения типа SmartLink

Приложение SmarkLink позволяет операторам обеспечивать взаимосвязь системы управления доступом EntraPass с любым интеллектуальным устройством, включая матричные коммутаторы, системы персонального вызова (пейджеры), системы рассылки электронных сообщений и др., путём использования соединения RS-232 между одной из рабочих станций EntraPass и внешним устройством. Интеграция с другими системами может быть также выполнена при помощи программного обеспечения DLL. SmartLink может быть использован для связи с другим компьютером для обмена данными и автоматического обновления их в режиме реального времени. Кроме того, с помощью этого интерфейса система EntraPass получает и отправляет сообщения, отчёты или команды и осуществляет связь с клиентскими приложениями.

ПРИМЕЧАНИЕ: *Для использования приложения SmartLink дополнительная лицензия не требуется.*

Система EntraPass позволяет настроить режим связи с использованием приложения SmartLink. Подробные сведения о работе SmartLink изложены в *SmartLink Reference Manual, DN1327*.

1 В выпадающем списке **EntraPass application** выберете приложение **SmartLink**.



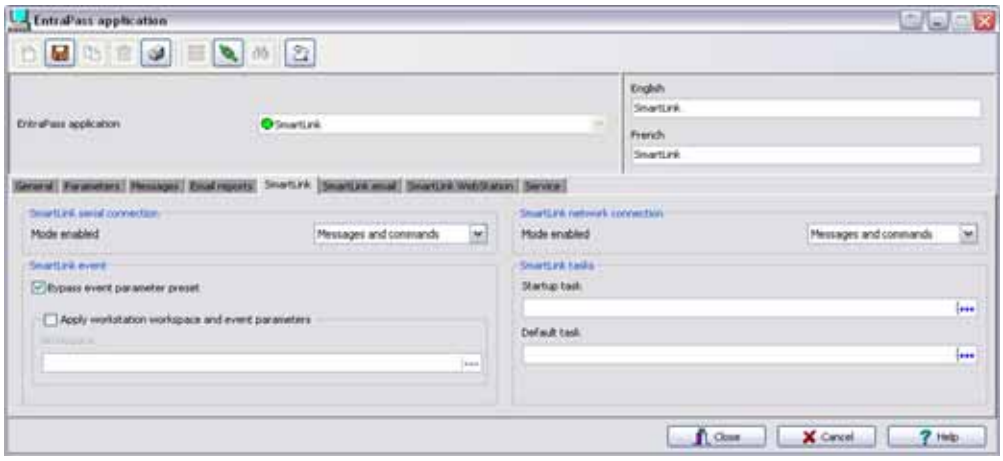
2 Настроить АРМ, на котором установлен интерфейс SmartLink. Подробнее *см. "Назначение общих параметров (раздел General)" на стр. 65*.

3 Настроить параметры безопасности рабочей станции SmartLink. Подробнее *см. "Описание параметров безопасности (раздел Parameters)" на стр. 65*.

4 Настроить сообщения поступаемые на АРМ SmartLink (Workstation Smartlink). Подробнее *см. "Назначение параметров управления сообщениями" на стр. 68*.

5 Настройте электронные отчеты для АРМ SmartLink. Подробнее *см. "Назначение параметров электронных отчётов (E-Mail Reports)" на стр. 70*.

6 Нажмите вкладку **SmartLink** для просмотра и настройки параметров связи SmartLink.



7 В выпадающем списке **Mode enabled** (Разрешённый режим) в разделе **SmartLink serial connection** (Последовательное соединение SmartLink) и в разделе **SmartLink network connection** (Сетевое соединение SmartLink) указать режим передачи:

- **Messages only** (Только сообщения). SmartLink служит только для получения сообщений.
- **Commands only** (Только команды). SmartLink служит только для выполнения команд (инструкций).
- **Messages and commands** (Сообщения и команды). SmartLink служит только для получения сообщений и выполнения команд.

ПРИМЕЧАНИЕ: При запуске приложения SmartLink параметры последовательного порта и сетевого соединения считываются с сервера EntraPass. Если режим сетевого соединения SmartLink указан отличным от “none”, то приложение SmartLink будет запускаться, позволяя клиентским приложениям соединяться, использоваться для выполнения команд или для получения сообщений, отправленных по сети, либо для выполнения этих двух процессов одновременно.

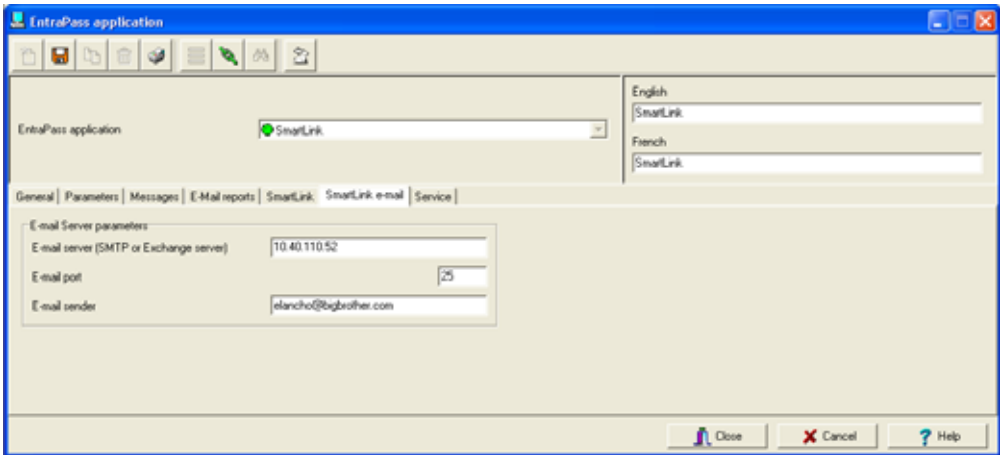
8 Отметить флажком опцию **Bypass event parameter preset** (Пренебречь предварительными установками параметров событий), чтобы игнорировать все установки по умолчанию, указанные в меню **Event Parameter** (Параметры событий) (закладка **System > Event Parameters**). По

умолчанию запланировано отправлять все события на все рабочие станции (включая рабочую станцию SmartLink). Выделение этой опции позволяет избежать получения ненужных команд и сообщений о событиях, не предназначенных для приложения SmartLink.

ПРИМЕЧАНИЕ: *Необходимо "вручную" создать связи для событий и команд в меню назначение параметров событий (Event Parameter). Например, можно выбрать событие “Door forced open” (Дверь взломана) и отправить в приложение SmartLink только специальную команду, чтобы в этом случае было отправлено сообщение по электронной почте.*

9 В разделе **SmarLink tasks** (Команды SmarLink) можно настроить команды для **Startup** (Запуск) или **Default** (По умолчанию). Выбранная команда будет автоматически выполнена при запуске приложения **SmartLink.** Более подробные сведения по настройке команд SmartLink и других системных команд *смотрите в Главе 5 Панель управления конструктора команд (Task Builder) на стр. 204*

10 Открыть закладку **SmartLink e-Mail** (Электронная почта SmartLink) для просмотра и настройки параметров соединения SmartLink.



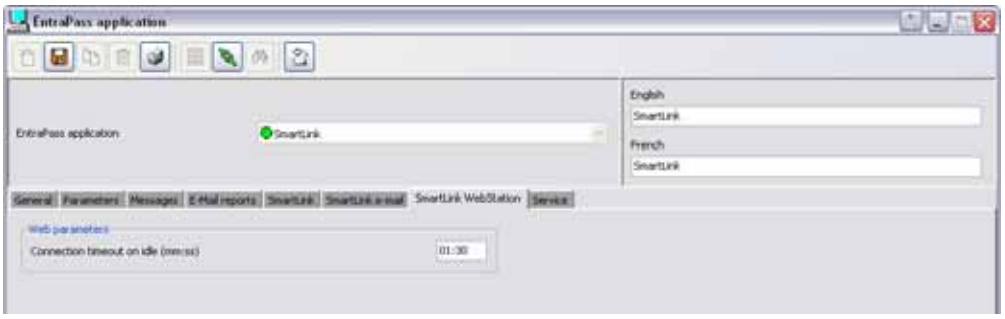
- Чтобы использовать приложение SmartLink с электронной почтой, необходимо указать имя почтового сервера в поле **E-mail server name,** номер порта в поле **E-mail port** и адрес отправителя в поле **E-mail sender**.

ПРИМЕЧАНИЕ: *По умолчанию используется порт номер 25. При необходимости можно выбрать другой номер порта (от 0 до 65 535). За сведениями по настройке почтового сервера следует обращаться к системному администратору.*

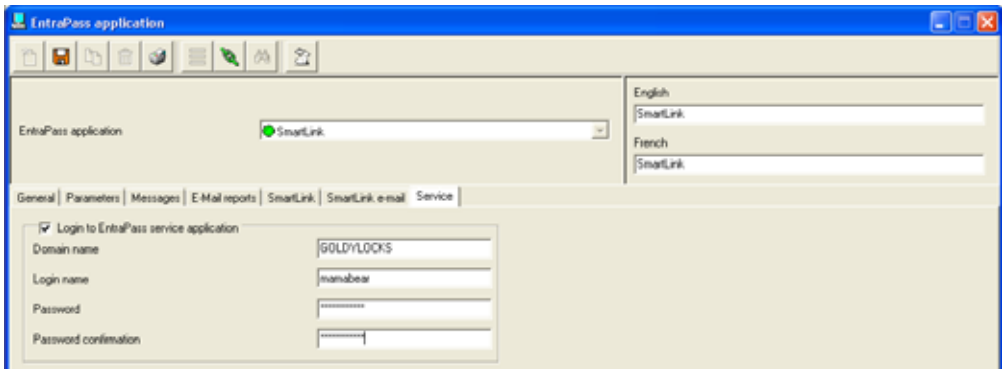
11 Нажмите на вкладку **SmartLink WebStation** чтобы назначить параметры WebStation.

12 Введите timeout соединения **(мин:сек)** (**Connection timeout on idle)** : Когда время ожидания будет достигнуто указанному, оператору будет необходимо вновь авторизоваться для продолжения работы. Все изменения, после последнего сохранения будут потеряны. По умолчанию, timeout соединения составляет 5:00 мин. Время может быть изменено от 00:30 до 20:00 мин.

ПРИМЕЧАНИЕ: *Если вы обновили систему EntraPass, timeout соединения не может быть изменен автоматически. Значение останется как было. Будьте уверены для изменения этого пункта.*



13 Откройте закладку **Service** (Служба) и настройте параметры, необходимые для входа в систему при использовании сервера SmartLink в режиме службы и необходимых muster отчетов для печати.



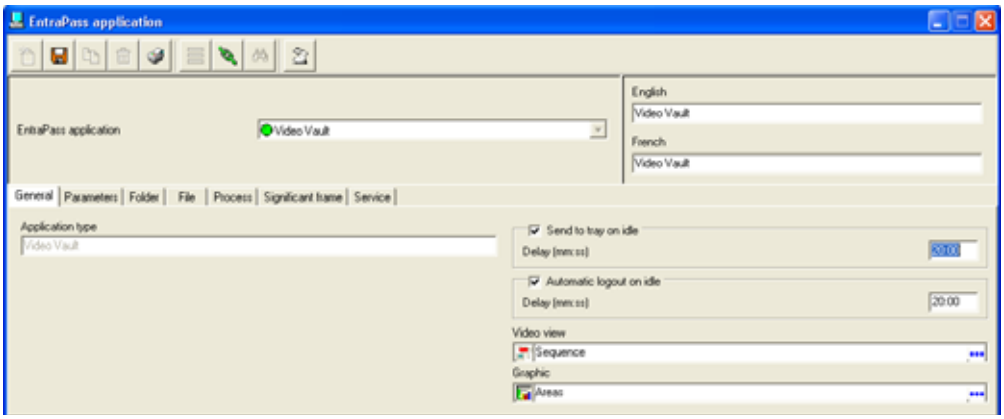
- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login to EntraPass service application** (Регистрационные данные для работы приложения в режиме службы).
- Для интерфейса SmartLink ввести имя домена в поле **Domain name** и имя пользователя в поле **Login name**.
- Указать пароль в поле **Password** и повторить его ввод в поле **Password confirmation**.

Настройка конфигурации приложения Видеохранилище EntraPass Video Vault

Видеохранилище EntraPass Video Vault предназначено для удовлетворения потребностей пользователей в удобном архивировании видеоинформации. Это приложение извлекает видеофрагменты с видеосерверов, подключённых к системе EntraPass, и сохраняет их для дальнейшего использования. На видеосервере данные могут храниться строго ограниченное время. Этот период зависит от того, какую ёмкость имеет жёсткий диск сервера, и от того, какие выбраны настройки для его работы. Для того чтобы в полной мере использовать все возможности интеграции с системами видеонаблюдения пользователи программного обеспечения EntraPass, работающие с программами видеомониторинга, должны воспользоваться приложением EntraPass Video Vault для работы с базами данных видеозаписей

После установки и регистрации видеохранилища EntraPass Video Vault следует настроить его параметры в других приложениях EntraPass. Более подробные сведения по регистрации EntraPass Video Vault, *в Главе 2 Дополнительные компоненты системы EntraPass на стр. 23*. Детали работы с приложением EntraPass Video Vault смотрите *в Главе 16 Видеохранилище (EntraPass Video Vault) на стр. 520*.

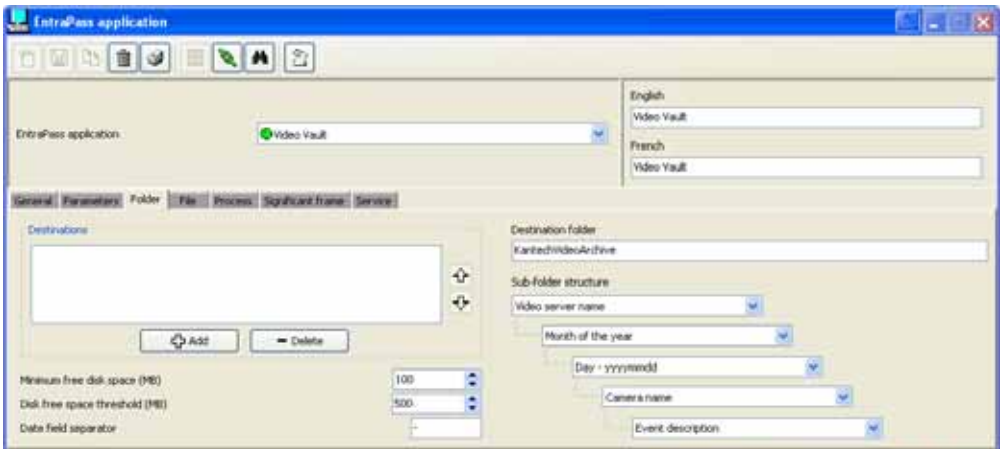
1 В выпадающем списке **EntraPass Application** выделить приложение EntraPass Video Vault.



2 Настройку общих параметров приложения EntraPass Video Vault выполнить, как описано в разделе *см. "Назначение общих параметров (раздел General)" на стр. 65*.

3 Настройку параметров безопасности приложения EntraPass Video Vaul выполнить, как описано в разделе, *см. "Описание параметров безопасности (раздел Parameters)" на стр. 65*.

4 Открыть закладку **Folder** (Папка) и указать путь видеофайла и структуру имени. Настройки, указываемые в этом окне, отражают, каким образом должны отображаться видеофайлы в окне Browse Video Vault (**Video** > **Browse Video Vault**).



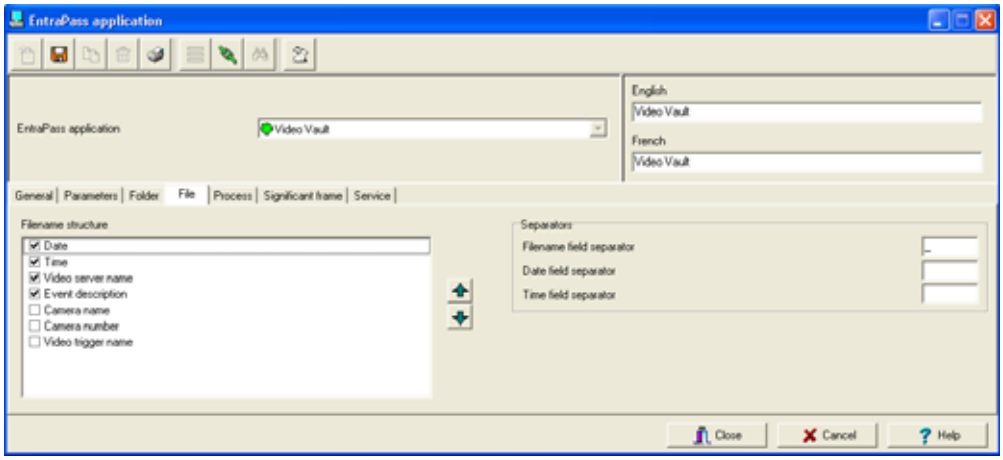
- **Destination drive(s)**(Назначение дисков): Список дисков, на которых будут храниться видеозаписи. Видеофрагменты будут записываться, в зависимости от доступного места на дисках, на всех выбранных дисках по порядку.

ПРИМЕЧАНИЕ: *Назначенные диски, отображаемые в поле* ***Destination drives****, соответствуют подключённым сетевым дискам на используемом компьютере.* Для каждого компьютера список дисков будет индивидуальным.

ПРИМЕЧАНИЕ: *По умолчанию диски в списке стоят в алфавитном порядке. Однако при желании можно изменить этот порядок, руководствуясь, например, доступным местом на каждом диске. Зелёные стрелочки "вверх/вниз" позволяют изменить последовательность дисков, предназначенных для архивирования.*

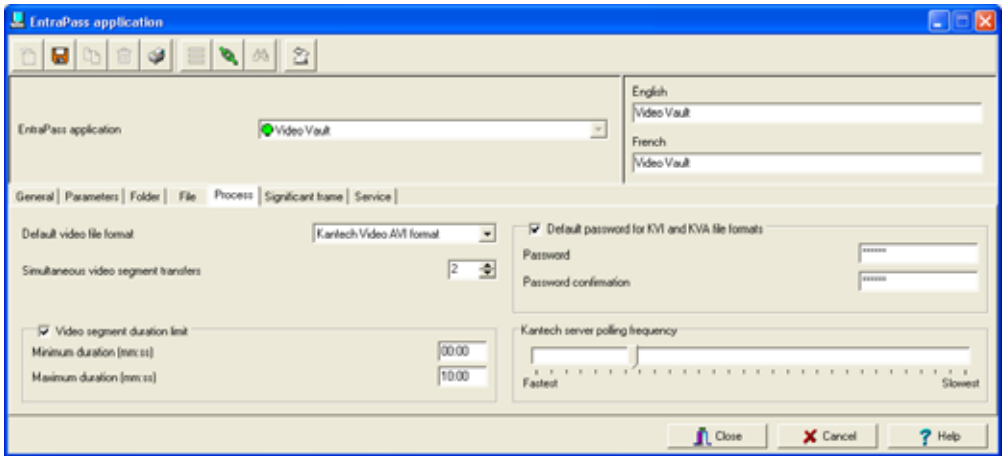
- **Minimum free disk space, MB** (Минимальное свободное место на диске, Мб). Система выдаёт сообщение о нехватке места на диске, как только свободного пространства на диске остаётся меньше указанного значения. Значение может быть до 99,999 Мб.
- **Disk free space threshold, MB** (Граница свободного пространства, Мб). Максимальное занятое файлами пространство на диске, по достижении которого система посылает сообщение, что видеохранилище заполнено. Система будет продолжать архивировать видео до наступления **minimum free disk space.** Значение может быть до 99,999 Мб.
- **Date field separator** (Разделитель полей даты). Вы можете назначить разделитель полей даты, отображаемый в директории видеоархива.
- **Destination folder** (Путь для записи файлов). Папка, в которой будут храниться файлы видеоархива. Если путь не будет указан, система не сможет выполнить архивирование файлов. По умолчанию видеофрагменты архивируются в папке C:\KantechVideoArchive.
- **Sub-folder structure** (Структура вложенных папок). В каждом поле со списком предлагаются критерии, по которым в архиве будут создаваться вложенные папки. Например, при выборе опции Video Server Name (Имя видеосервера) система создаст вложенные папки для каждого видеосервера и сгруппирует в них все видеофрагменты по этому признаку. Если, например, в следующем уровне выбрать опцию Day-yyyy-mm-dd, то в каждой папке Video Server Name будут созданы вложенные папки с наименованием даты сохранения видеофайлов ежедневно. Всего предусмотрено 5 уровней вложенных папок.

5 Открыть закладку **File** (Файл) для выбора способа присвоения имён файлов.



- **Filename structure** (Структура имени файла). Отметить галочками, какие данные должны содержаться в именах файлов.
- **Separators** (Разделители). В этом разделе следует выбрать, какие разделители должны быть использованы в имени файла (Filename field separator), а также в полях даты (Data field separator) и времени (Time field separator).

6 Открыть закладку **Process** (Обработка) и указать, как должны быть обработаны архивируемые видеофрагменты.



- **Default Video file format for your video archives** (Формат по умолчанию архивируемых видеофайлов). Для архивирования видеофрагментов используются форматы KVI, KVA, AVI и IMG.
  - **KVI** – сокращённое название формата Kantech Video Intellex. Файл KVI содержит пиктограмму и собственно видеоинформацию с водяными знаками (информацией о подлинности), установленными на вложенных изображениях формата embedded.img. Для просмотра необходима программа Intellex Video Player, которая использует прикладной программный интерфейс API компании American Dynamic. Таким образом, интерфейс API обязательно должен быть установлен на клиентском компьютере.
  - **KVA** – сокращённое название формата Kantech Video AVI. Файл KVA содержит пиктограмму и собственно видеоинформацию без нанесённых водяных знаков на вложенное видео формата embedded.avi. Видеофайлы можно просматривать с помощью Windows Media Player или любой другой программы для просмотра файлов AVI.
  - **AVI** – сокращённое название формата Audio Video Interlaced. Видеофайлы AVI можно просматривать при помощи Windows Media Player.
  - **IMG** – собственный формат Intellex. Видеоданные хранятся в формате Intellex (.img), а для их просмотра можно использовать программу Intellex Video Player.

ПРИМЕЧАНИЕ: *Форматы KVI и KVA позволяют пользователям защитить видеофайлы паролем и указать ключевые кадры для любого выделенного видеособытия. Ключевые кадры обеспечивают быстрый поиск видеофрагментов путём просмотра отдельных кадров формата .bmp, выбранных в качестве наиболее представительных из всех кадров видеофрагмента.*

- **Simultaneous video segment transfers** (Одновременные пересылки видеофрагментов). В этом поле следует указать допустимое число одновременных закачек. Одновременно допускается извлечение не более одного видеофрагмента с каждого видеосервера. Однако разрешается одновременное извлечение нескольких видеофрагментов с разных видеосерверов. Диапазон допустимых значений – от 1 до 8.

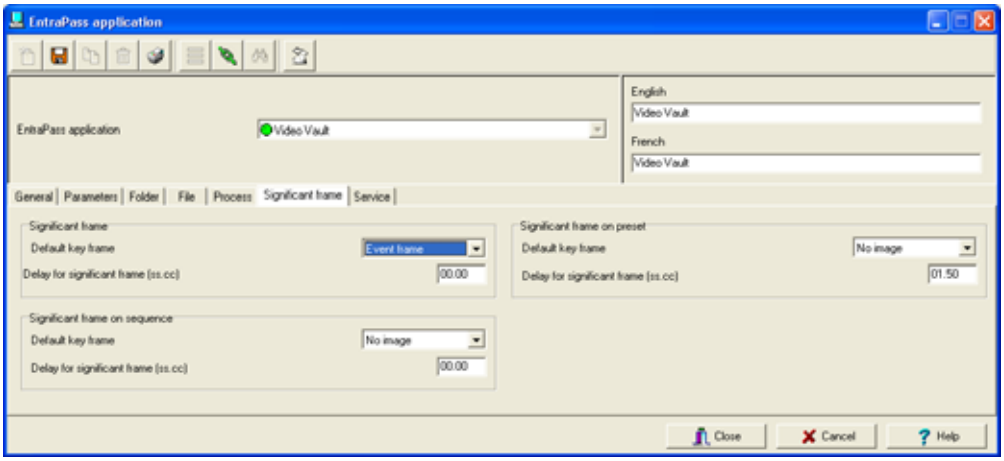
ПРИМЕЧАНИЕ: *Чем больше число одновременно извлекаемых файлов, тем больше должна быть пропускная способность сети. Поскольку при передаче видеоданных затрачивается значительная часть сетевых ресурсов, рекомендуется обратиться к администратору сети для оптимизации этих настроек.*

- **Video segment duration limit** (Ограничение длительности видеофрагмента). Необходимо задать допустимую минимальную и максимальную длительность архивируемых видеофрагментов. максимальная продолжительность сотоавляет 59 мин. 59 сек. После установки флажка в данном поле на экране становятся активными поля ввода минимальной (Minimum) и максимальной (Maximum) длительности видеоданных. Данная функция может оказаться полезной, если вы хотите ограничить число архивируемых видеофрагментов. Например, может быть установлено ограничение по размеру видеозаписи. Пользователь, может, например, сказать системе игнорировать все видеозаписи длительностью менее 10 секунд.
- **Default password for KVI and KVA file formats** (Пароль по умолчанию для файлов формата KVI и KVA). В целях повышения безопасности можно защитить архивируемые видеофрагменты паролем, если поставить флажок напротив этой опции. Форматы KVI и KVA позволяют устанавливать пароль на видеоданные. Обращаем внимание, что записи в полях **Password** (Пароль) и **Password Confirmation** (Повторный ввод пароля) должны быть идентичными. Операторы, имеющие необходимые полномочия для просмотра архивных видеофрагментов, получат доступ к видеоданным только после ввода достоверного пароля.
- **Kantech server polling frequency, m:ss** (Частота опроса сервера Kantech, мин:сек). Перемещением скользящего регулятора указать частоту, с которой видеохранилище EntraPass Video Vault будет опрашивать сервер EntraPass.

ПРИМЕЧАНИЕ: *Следует помнить, что нагрузка сети зависит от частоты опроса между сервером EntraPass, рабочими станциями, шлюзами и видеосерверами. Чем чаще опросы, тем выше нагрузка на сеть.*

7 Открыть закладку **Significant Frame** (Ключевой кадр) и указать ключевые кадры, которые будут использоваться, как пиктограммы для предварительного просмотра видеофрагментов в директориях.

- В этом окне необходимо выбрать тип настройки:

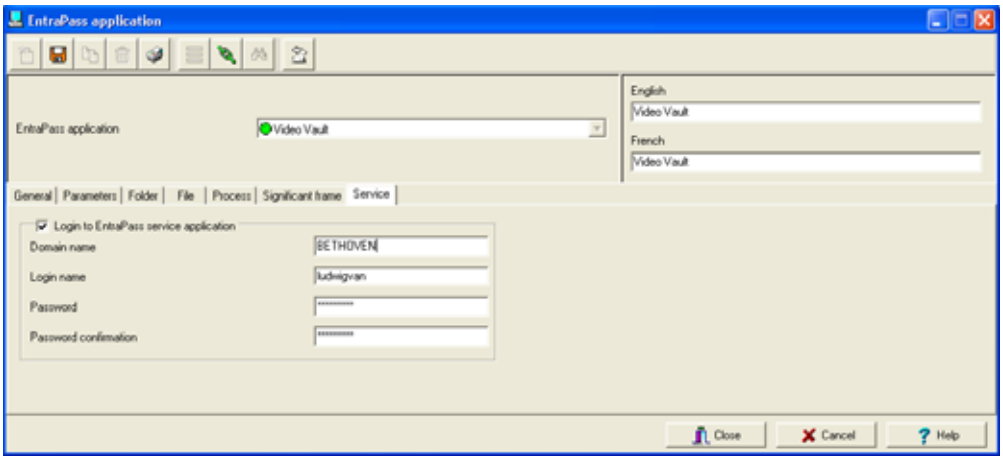


- **Significant Frame** (Ключевой кадр). Наиболее представительный неподвижный кадр видеофрагмента. Ключевой кадр служит обобщением видеофрагмента. Его можно использовать как пиктограмму, например, при поиске определённой видеозаписи.

- **Significant Frame on Sequence** (Ключевой кадр при использовании последовательности/тура обхода для speed dome). Эта функция используется только с купольными камерами, которые настроены на определённый маршрут движения по препозициям или автотур, для которого необходимо выбрать наиболее представительный из всех кадров видеофрагмента внутри тура.
- **Significant Frame on Preset** (Ключевой кадр при использовании предустановок). Эта функция используется только с купольными камерами, которые настроены на выполнение предустановок. При выборе самого представительного кадра видеофрагмента принимают во внимание, что для перемещения камеры с первого кадра на следующую предустановленную позицию нужно определённое время.

- Для каждого типа настройки ключевого кадра следует выбрать один из типов **Default Key Frame** (Ключевой кадр по умолчанию):
  - **No image** (Не использовать). Не выбирать пиктограмму для этого видеофрагмента.
  - **First frame** (Первый кадр). Ключевым кадром видеофрагмента будет кадр предтревожной записи. При выборе этой опции автоматически становится активным параметр **Delay for Significant Frame, ss:cc** (Задержка до ключевого кадра, сек), который представляет собой время с первого кадра до кадра, выбираемого в качестве ключевого. После установки курсора в этом поле на экране становятся активными поля ввода минимальной и максимальной задержки.
  - **Event Frame** (Тревожный кадр). Ключевым кадром видеофрагмента будет кадр, снятый в момент возникновения тревоги.

8 Открыть закладку **Service** (Служба) и настроить параметры, необходимые для входа в систему при использовании сервера видеохранилища Entrapass Video Vault в режиме службы и для выдачи результатов пользователю.



- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login to EntraPass service application** (Регистрационные данные для работы приложения в режиме службы).
- Для видеохранилища EntraPass Video Vault ввести имя домена в поле **Domain name** и имя пользователя в поле **Login name**.
- Указать пароль в поле **Password** и повторить его ввод в поле **Password confirmation**.

Настройка конфигурации шлюзов EntraPass

Entrapass Gateways convert the information received from a controller or a site and transmit 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.Шлюзы EntraPass преобразуют информацию, полученную с контроллера или луча, и передают преобразованные данные на сервер. Кроме того, шлюзы также преобразуют данные, полученные с сервера, и передают их контроллерам. Приложение шлюза можно установить на отдельном компьютере или интегрировать его с другой рабочей станцией EntraPass.

EntraPass Global Edition поддерживает три типа Шлюзов: Corporate, NCC-8000 и Global. Global Edition также поддерживаает KT-NCC. Все шлюзы взаимодействуют с лучами и сервером. Исключая KT-NCC, все шлюзы могут быть установленны на отдельные компьютеры или могут быть установлены на АРМ (рабочую станцию).

ПРИМЕЧАНИЕ 1: *EntraPass Global Edition идет в комплекте с Global Шлюз и Шлюзом KT-NCC. Одиночный Corporate Шлюз может быть добавлен через двойной Шлюз (Dual Gateway) без необходимости приобретения дополнительной лицензии.*

ПРИМЕЧАНИЕ 2: *Допоолнительные Шлюзы (Corporate, NCC-8000 и Global) требуют приобретения дополнительных лицензий.*

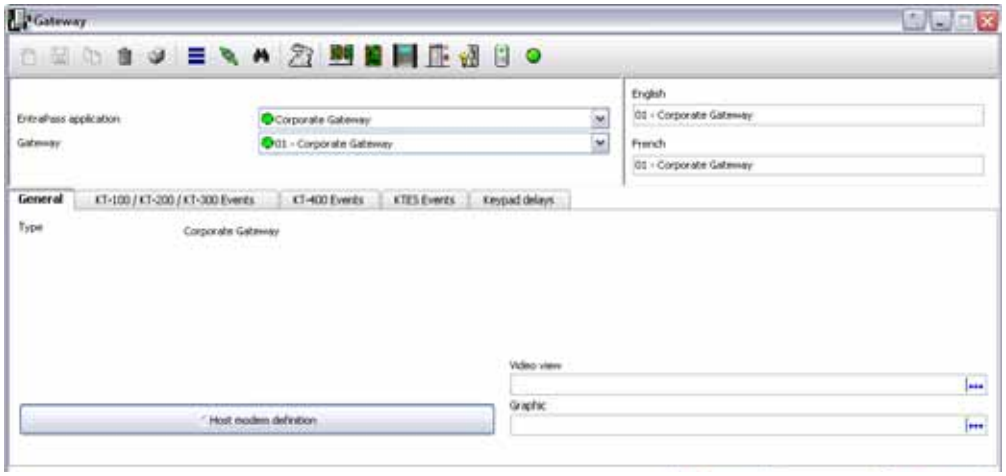
Ниже в таблице приведены сравниваются функционал Шлюзов, которые могут быть использованы в EntraPass Global Edition:

Capacities	Corporate Шлюз	NCC-8000 Шлюз	Global Шлюз	KT-NCC
Число шлюзов	40	128	128	128
Локальные лучи	32 луча с последовательными портами и USB	8 (лучей)	32	2 x RS-485 1 x RS-232
On-Line удалённые лучи	512 лучей с интерфейсом Kantech IP Link* 32 луча с Lantronix	нет	32	4 x TCP/IP (UDP)
Модемы на хост-сайте для передачи по коммутируемой линии	по 32 на каждом шлюзе	нет	нет	нет
Удалённые лучи со связью по телефонному модему	по 512 на каждом шлюзе	нет	нет	нет
Число контроллеров на каждый шлюз	17,408 всего (32 KT на луч)	128 всего (16 на луч KT-200 только)	1,024 на Global Шлюз (32 KT на луч)	128 на KT-NCC (32/COM Port x 3, 8 TCP/IP / луч x4)
Число считывателей на каждый шлюз	34,816	256	2,048	256

* Системные требования могут различаться в зависимости от размеров сайтов и числа событий, генерируемых за день.

Настройка конфигурации шлюза Corporate Gateway

1 Открыть закладку **Devices** (Устройства) и нажать иконку **Gateway** (Шлюз).

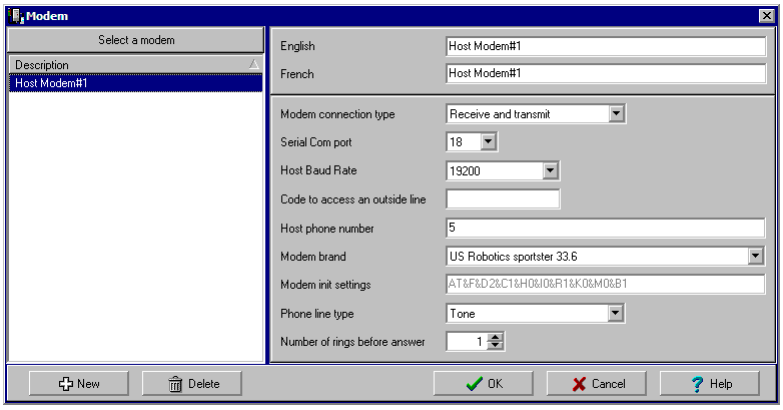


2 В выпадающем списке **Gateway** указать, какой шлюз необходимо настроить.

ПРИМЕЧАНИЕ: *Если опция "**Dual Gateway**" была разрешена в приложении Global Шлюз, тогда **Corporate Шлюз** будет отображен. Для большей информации см. "Настройка конфигурации приложения EntraPass" на стр. 64.*

3 Под закладкой **General** (Общие параметры) выполнить следующие настройки:

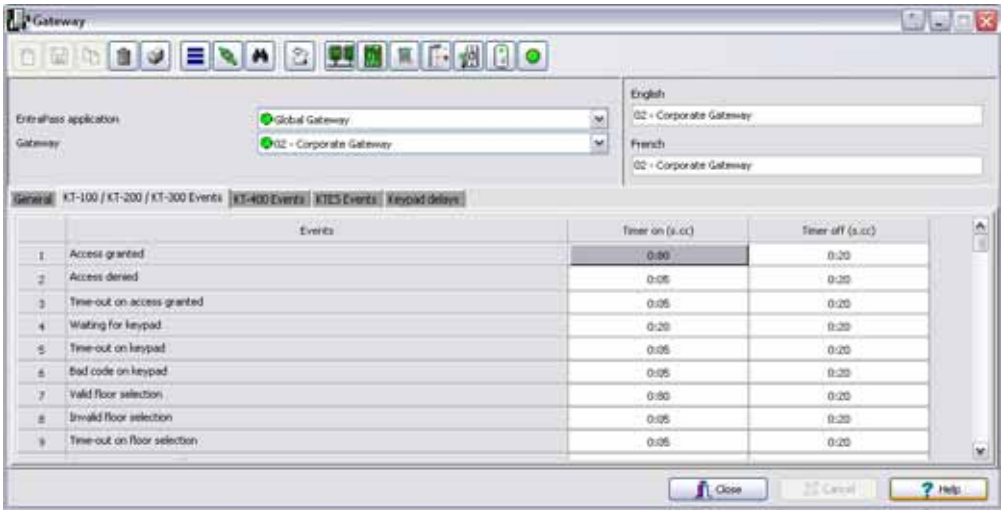
- Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которым прикреплён шлюз. Выбор видеоокна будет доступным только в том случае, если в системе EntraPass разрешено использовать функцию видеонаблюдения.
- Если шлюз Corporate подсоединён к первому контроллеру удалённого сайта через модем, то необходимо нажать кнопку описания модема **Host Modem** и настроить параметры связи для модема.



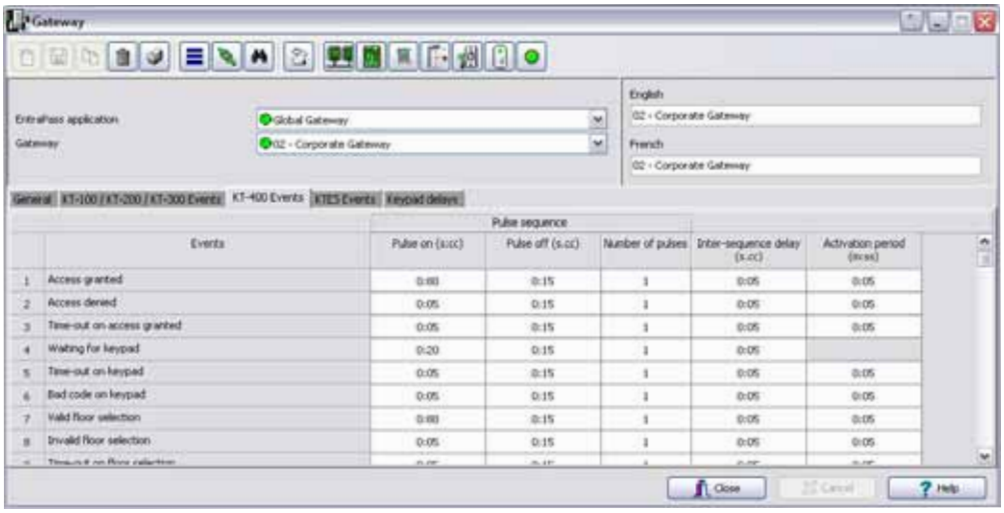
- Для того чтобы добавить модем в общий список, следует нажать кнопку **New** (Создать).
- Указать все необходимые значения параметров, как на иллюстрации выше, и нажать **OK** для возврата в меню **Device** (Устройство).

ПРИМЕЧАНИЕ: *В целях обеспечения высокой надёжности и идеальной совместимости всех устройств компания Kantech к настоящему моменту обеспечила поддержку внешних модемов только серии US Robotics Sportster. Кромк того, тип соединения через модем в поле **Modem connection type** должен быть установлен на получение и передачу (**Receive and transmit**), а **все остальные настройки модема** должны быть оставлены неизменными. При возникновении вопросов по поводу тех или иных настроек модема следует обращаться к системному администратору, обслуживающему данное оборудование.*

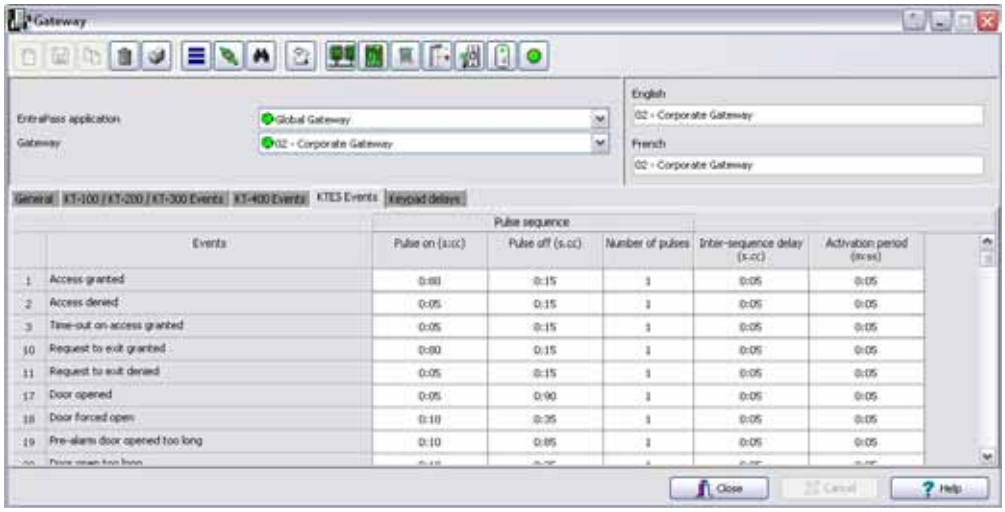
4 Открыть закладку **KT-100/KT-200/KT-300 Events** (События KT-100/KT-200/KT-300) и настроить включение (**Timer on**) и выключение (**Timer off**) таймера светодиода для каждого события. Версия Corporate Gateway позволяет настроить таким образом до 30 событий.



5 Открыть закладку **KT-400 Events** (События KT-400) и настроить включение (**Pulse on**) и выключение (**Pulse off**) пульсации светодиода для каждого события. Версия Corporate Gateway позволяет настроить таким образом связанные события.



6 Во вкладке **KTES Events** (события **KTES**), настройте включение (**Pulse on**) и выключение (**Pulse off**) пульсации светодиода для каждого события.



ПРИМЕЧАНИЕ: *Приложение Corporate Gateway поддерживает до 41 шлюза.*

Ниже в таблице приведены все события, допустимые в версии Corporate Gateway:

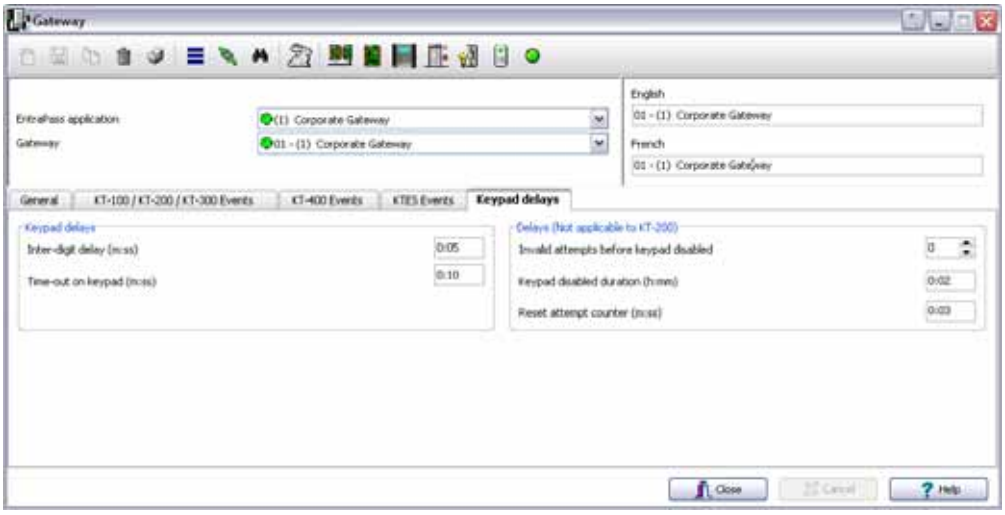
Access granted (Доступ разрешён)	Arming request denied (Запрос для постановки на охрану запрещён)	Time-out on waiting for a second card (Таймаут ожидания второй карты)
Access denied (Доступ запрещён)	Postpone granted (Отсрочка разрешена)	Access denied - Waiting for a second card (Доступ запрещён - Ожидание второй карты)
Time-out on access granted (Таймаут на разрешение доступа) d	Postpone denied (Отсрочка запрещена)	Access denied - Reader locked (Доступ запрещён – Считыватель заблокирован)
Waiting for keypad (Ожидание нажатия клавиши) – *прим. 1*	Door opened (Дверь открыта)	Exit delay (Задержка на выход)
Time-out on keypad (Таймаут нажатия клавиши)	Door forced open (Дверь силой открыта)	Entry delay (Задержка на вход)
Bad code on keypad (Неверный код клавиши)	Pre-alarm door opened too long (Предтревожное состояние двери при слишком долгом открытии)	Access granted by tenant/(доступ предоставлен жильцом) (*Примечание 3*)
Valid floor selection (Достоверный выбор этажа)	Door open too long (Дверь открыта слишком долго)	Access denied by tenant/(доступ запрещен жильцом) (*Примечание 3*)
Invalid floor selection (Недостоверный выбор этажа)	Door alarm on relock (Сигнализация двери при выполнении блокировки)	Auxiliary relay activated by tenant/ (Внешнее реле ктивиовано жильцом) (*Примечание 3*)
Time-out on floor selection (Таймаут выбора этажа)	Door unlocked (Дверь разблокирована)	Postal lock request granted /(Запрос на открытие замка для почты предоставлен)(*Примечание 3*)
Request to exit granted (Запрос на выход разрешён)	Reader disabled (Считыватель отключён)	Postal lock request denied/(Запрос на открытие замка для почты отклонен)(*Примечание 3*)
Request to exit denied (Запрос на выход запрещён)	Door armed (Дверь поставлена на охрану)	
Arming request granted (Запрос для постановки на охрану разрешён)	Waiting for a second card (Ожидание второй карты) – *прим. 2*	

ПРИМЕЧАНИЕ 1: Чтобы задать время активации кода на клавиатуре считывателя **Waiting for keypad** (Ожидание нажатия клавиши) смотрите **в пункте 7**).

ПРИМЕЧАНИЕ 2: Чтобы настроить время активации события **Waiting for a second card** (Ожидание второй карты), следует выполнить указания, описанные в разделе “Настройка конфигурации 4-дверного Ethernet-контроллера KT-400” на стр. 122

ПРИМЕЧАНИЕ 3: Эти события только для домофонного устройства KTES.

7 Под закладкой **Keypad delays** (Задержки нажатия клавиш) выполнить настройку клавиатуры считывателя:



- В разделе **Keypad delays** указать значение параметра **Inter-digit delay** (Задержка между двумя последовательными нажатиями клавиш, мин:сек). Это максимально допустимое время задержки перед каждым последующим выбором клавиши пользователем.
- Указать время задержки в строке **Time-out on keypad** (Таймаут нажатия клавиши, мин:сек). Значение этого параметра задаётся в секундах. Это максимальное время, отведённое пользователям, для того чтобы начать ввод кода на кнопочной панели считывателя.

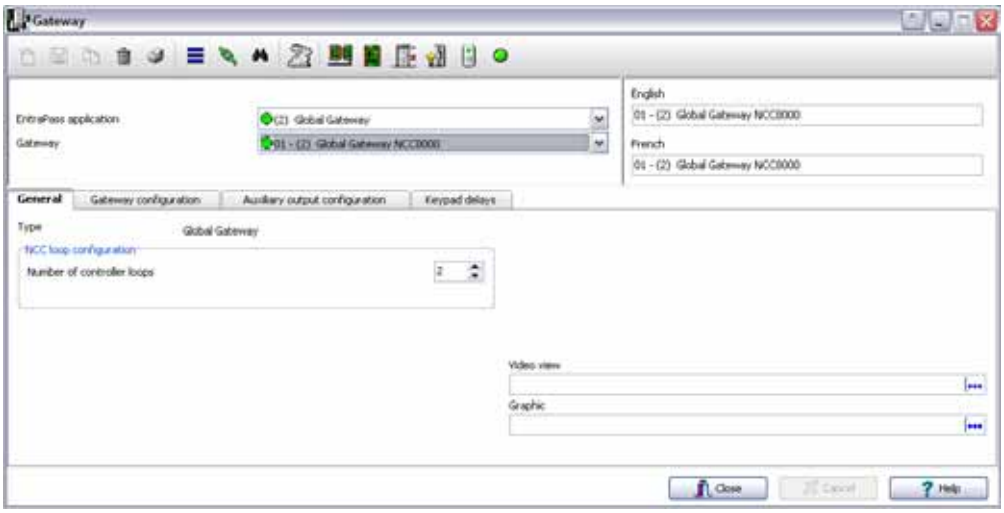
ПРИМЕЧАНИЕ: *Максимальное время задержки, допустимое между нажатием двух клавиш (Inter-digit delay), а также для таймаута (Time-out on keypad) составляет 2 минуты 7 секунд. Значения этих же параметров для контроллера KT-400 составляют 4 минуты 15 секунд.*

- При помощи клавиш со стрелками вверх/вниз в разделе настройки задержек **Delays (не совместимо с KT-200)** указать **число неверных попыток, после которых кнопочная панель считывателя блокируется**. Максимально возможное число неудачных попыток пользователей, после которых выполняется автоматическая блокировка клавиш, составляет 255 попыток.
- Указать длительность блокировки кнопочной панели в строке **Keypad disabled duration** (час:мин). Максимальная допустимая длительность составляет 4 часа 15 минут. После того как показания счётчика достигнут максимального значения, кнопочная панель будет заблокирована для всех карт. Время, в течение которого клавиши будут заблокированы, указывается в поле **Keypad disabled duration** (Длительность блокировки клавиш). .
- Указать время задержки в поле **Reset attempt counter** (Сброс счётчика попыток, мин:сек). После окончания времени, указанного в поле **Reset attempt counter**, система обнулит показания счётчика попыток. Максимальное время задержки составляет 4 минуты 15 секунд. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное значение.

Настройка Шлюза NCC-8000

Шлюз NCC-8000будет работать на определенном компьютере с DOS 6.2 или Windows 98 с оболочкой DOS.

1 Из списка Шлюзов (Gateway) выберите Шлюз NCC-8000, который вы хотите настроить.



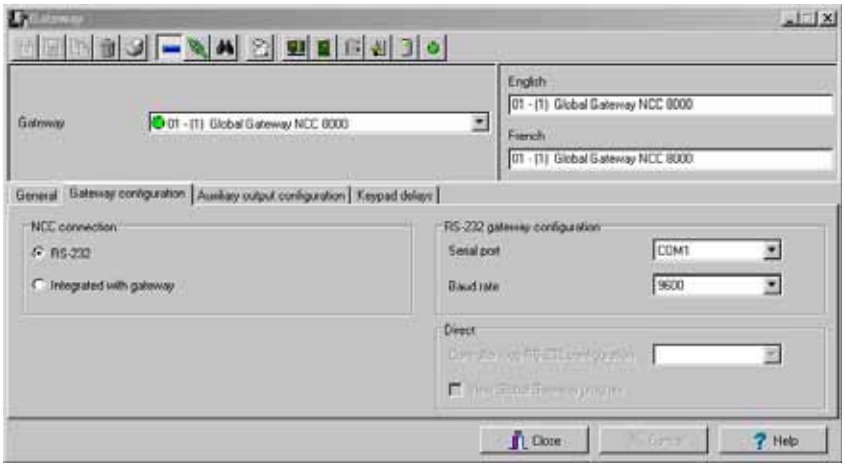
2 Под вкладкой **General** (общие):

- Используйте клавиши вниз/верх, чтобы указать количество лучей, которые подулючены к этому компьютеру (максимум 8).

ПРИМЕЧАНИЕ: *Под Шлюзом NCC-8000, на луче может быть подключено до 16 кон троллеров и до 8 лучей на NCC-8000. Только КТ-200 с ПЗУ EP-8002 может быть подключена к Шлюзу NCC-8000.*

- Выберите **Graphic view** (графический вид) для которого назначен шлюз, если позволено. Функция **Video View** (видео окно) будет активирована, если функция Video включена в EntraPass.

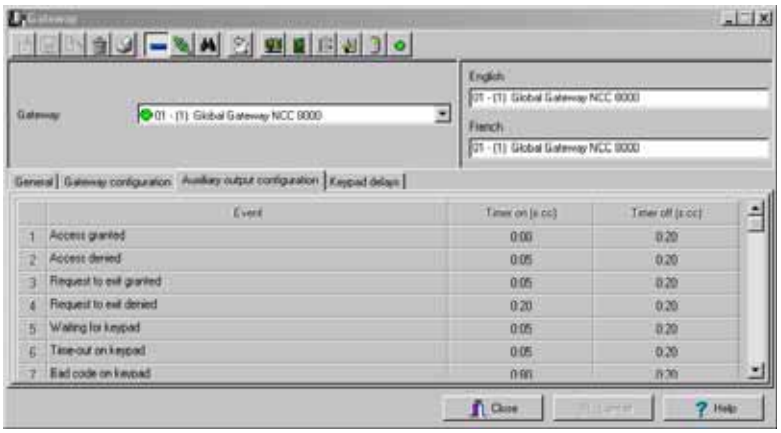
3 Двигайтесь на вкладку **Gateway Configuration** (настройка Шлюза).



- Укажите тип соединения между Шлюзом и NCC-8000 (этот же PC или отдельный).
  - **RS-232**—если Шлюз NCC-8000 установлен на отдельном PC, тогда связь между NCC-8000 и Шлюзом установлена через определнный выбранный порт RS-232. В этом случае вы должны также указать бит рейт, используемый для связи с Шлюзом NCC-8000.
  - **Integrated with Gateway** (встроенный в Шлюз)—если NCC-8000/Global Шлюз и программное обеспечение установленное на одном и том же компьютере, укажите какой порт использован для лучей.
- Если NCC-8000 соединен через RS-232, назначьте параметры RS-232 в **Gateway Configuration** (Настройка Шлюза):
  - **Serial Port (Серийный порт)—**Выберите серийный порт связи, используемый на компьютере, где установлен Шлюз с внешним Шлюзом NCC-8000/Global.
  - **Baud Rate (Скорость передачи)**—Выберите скорость передачи между PC, где установлен Шлюз, и другим PC, на котором установлен Шлюз NCC-8000/Global.

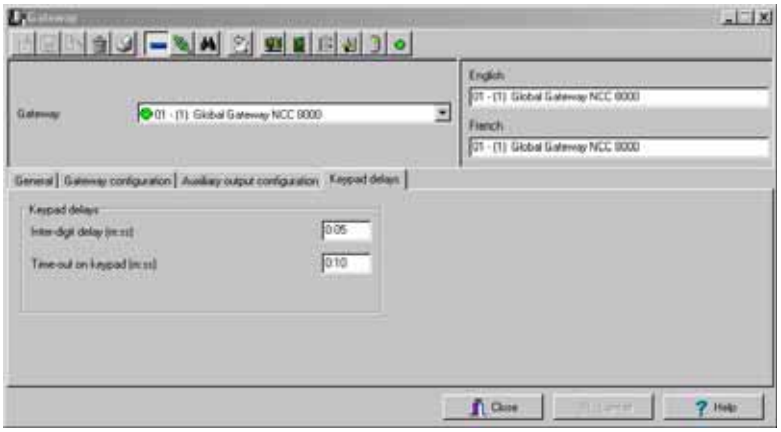
- Если NCC-8000 встроен в Шлюз (NCC-800 установлен на том же PC, на котором стоит другой Шлюз), то вы должны назначить конфигурации луча, чтобы определить COM порт, к которому подключен луч. Если вы выберите пункт **Integrated with gateway** (встроен в Шлюз), то настройте следующие пункты:
  - **Controller loop RS-232 configuration (Настройка луча контроллера RS232):** Выберите COM порт, используемый для связи. Для инфорамции отосительно COM портов используемых в Шлюзе NCC-8000/Global контактирйте с вашим системным администратором.
  - Выбериите **View Global Gateway program (Видеть программу Global Шлюз)** если вы хотите увидеть Global Шлюз как программу, запускаемую под Windows. Оставьте эту опцию невыбранной, чтобы иметь Global Шлюз, запускаемый на заднем фоне Windows.

4 Двигайтесь к вкладке **Auxiliary output configuration** (настройка дополнительных выходов).



- Установите **Timer on** (таймер вкл.) и**Timer off** (таймер выкл.) для каждого события. Шлюз NCC-8000 настроен для управления 16 событиями.

5 Двигайтесь к вкладке **Keypad delay** (задержка на кодонаборнике).



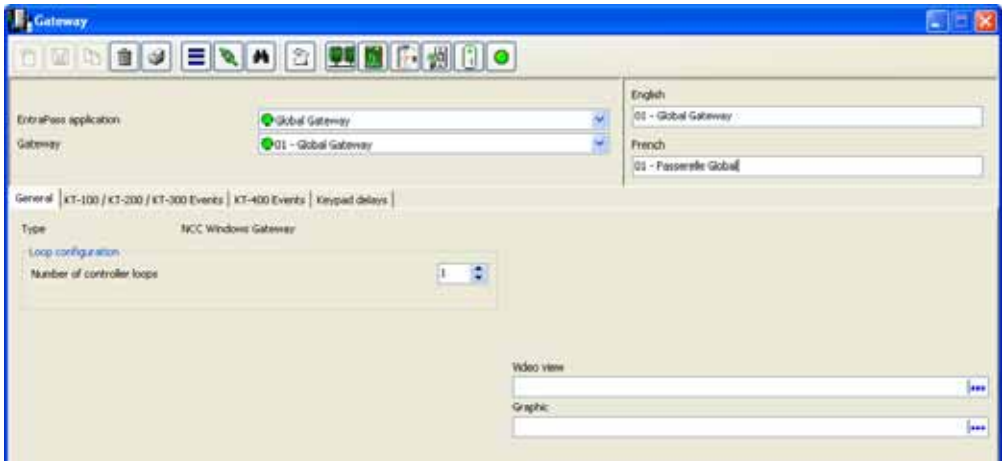
- В разделе **Keypad delays** указать значение параметра **Inter-digit delay** (Задержка между двумя последовательными нажатиями клавиш, мин:сек). Это максимально допустимое время задержки перед каждым последующим выбором клавиши пользователем.
- Указать время задержки в строке **Time-out on keypad** (Таймаут нажатия клавиши, мин:сек). Значение этого параметра задаётся в секундах. Это максимальное время, отведённое пользователям, для того чтобы начать ввод кода на кнопочной панели считывателя.

ПРИМЕЧАНИЕ: *Максимальное время задержки, допустимое между нажатием двух клавиш (Inter-digit delay), а также для таймаута (Time-out on keypad) составляют 4 минуты 15 секунд.*

Настройка Global Шлюза

1 Из вкладки **Devices** (Устройства), нажмите на иконку **Gateway** (Шлюз).

2 Из списка **Gateway** (Шлюз), Выберите пункт Global Gateway (Global Шлюз) для его настройки.



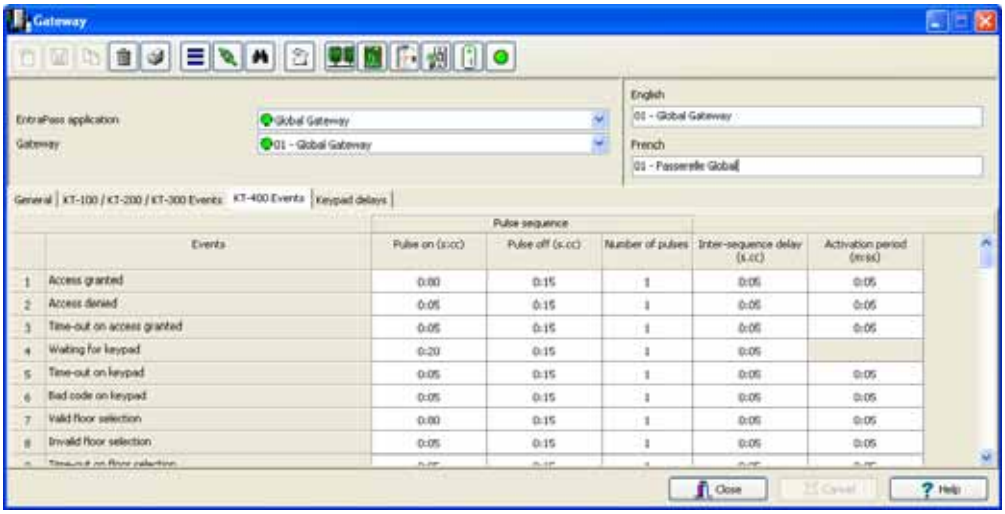
3 Под вкладкой **General** (устройства):

- Используйте клвиши вверх/вниз для выбора **Number of controller loops (**количества лучей с контролелрами). Global Шлюз поддерживает до 32 лучей с контроллерами.
- Выберите **Graphic** (График) и **Video view** (Вид Видео) для которого назначен этот Шлюз, если применимо. Режим **Video View** (Вид Видео) будет назначен, если он разрешен в EntraPass.

4 Двигайтесь на вкладку **KT-100/KT-200/KT-300 Events** (события KT-100/KT-200/KT-300):

- Установите **Timer on** (таймер вкл.) и **Timer off** (таймер выкл.) для каждого события. Global Шлюз настроен для управления связанными событиями KT-100, KT-200 или KT-300.

5 Двигайтесь на вкладку **KT-400 Events** (События KT-400):



- Настроить включение (**Pulse on**) и выключение (**Pulse off**) пульсации светодиода для каждого события. Global Шлюз позволяет настроить таким образом связанные события для KT-400.

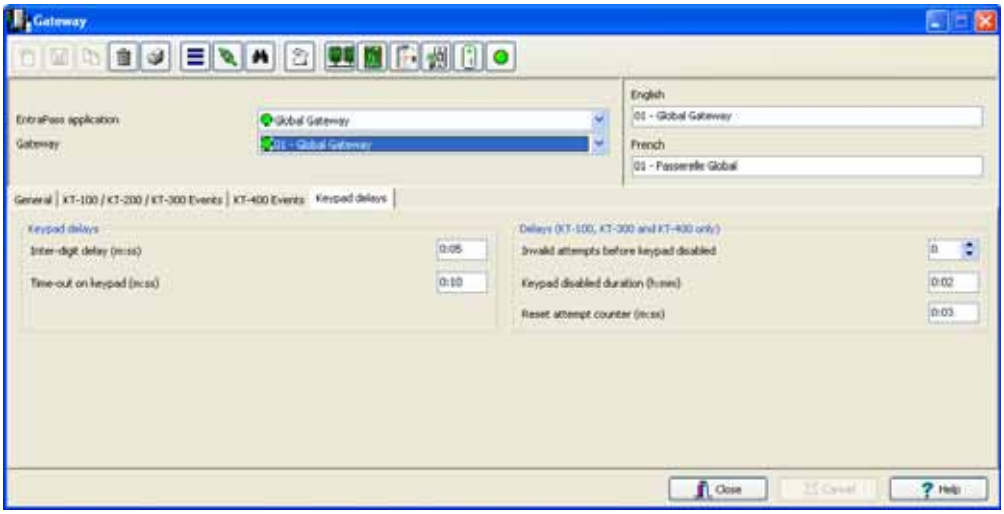
Следущая таблица отображает все события, доступные в Global Шлюзе:

Access granted (Доступ разрешён)	Time-out on floor selection (Таймаут выбора этажа)	Door unlocked (Дверь разблокирована)
Access denied (Доступ запрещён)	Request to exit granted (Запрос на выход разрешён)	Reader disabled (Считыватель отключён)
Time-out on access granted (Таймаут на разрешение доступа)	Request to exit denied (Запрос на выход запрещён)	Waiting for a second card (Ожидание второй карты) – *прим. 2*
Waiting for keypad (Ожидание нажатия клавиши) – *прим. 1*	Door opened (Дверь открыта)	Time-out on waiting for a second card (Таймаут ожидания второй карты)
Time-out on keypad (Таймаут нажатия клавиши)	Door forced open (Дверь силой открыта)	Access denied - Waiting for a second card (Доступ запрещён - Ожидание второй карты)
Bad code on keypad (Неверный код клавиши)	Pre-alarm door opened too long (Предтревожное состояние двери при слишком долгом открытии)	Access denied - Reader locked (Доступ запрещён – Считыватель заблокирован)
Valid floor selection (Достоверный выбор этажа)	Door open too long (Дверь открыта слишком долго)	
Invalid floor selection (Недостоверный выбор этажа)	Door alarm on relock (Сигнализация двери при выполнении блокировки)	

ПРИМЕЧАНИЕ 1: *Чтобы задать время активации события* ***Waiting for keypad*** *(Ожидание нажатия клавиши), следует открыть закладку* ***Keypad delays*** *(Задержки нажатия клавиш), как описано* ***пункт 6****.*

ПРИМЕЧАНИЕ 2: *Чтобы настроить время активации события* ***Waiting for a second card*** *(Ожидание второй карты), следует выполнить указания, описанные* ***в Главе 4 Настройка конфигурации 4-дверного Ethernet-контроллера KT-400 на стр. 122****.*

6 Под закладкой **Keypad delays** (Задержки нажатия клавиш) выполнить настройку клавиатуры считывателя:



- В разделе **Keypad delays** указать значение параметра **Inter-digit delay** (Задержка между двумя последовательными нажатиями клавиш, мин:сек). Это максимально допустимое время задержки перед каждым последующим выбором клавиши пользователем.
- Указать время задержки в строке **Time-out on keypad** (Таймаут нажатия клавиши, мин:сек). Значение этого параметра задаётся в секундах. Это максимальное время, отведённое пользователям, для того чтобы начать ввод кода на кнопочной панели считывателя.

ПРИМЕЧАНИЕ: *Максимальное время задержки, допустимое между нажатием двух клавиш (Inter-digit delay), а также для таймаута (Time-out on keypad) составляет 2 минуты 7 секунд. Значения этих же параметров для контроллера KT-400 составляют 4 минуты 15 секунд.*

- При помощи клавиш со стрелками вверх/вниз в разделе настройки задержек **Delays (KT-100, KT-300, KT-400)** указать **число неверных попыток, после которых кнопочная панель считывателя блокируется**. Максимально возможное число неудачных попыток пользователей, после которых выполняется автоматическая блокировка клавиш, составляет 255 попыток.
- Указать длительность блокировки кнопочной панели в строке **Keypad disabled duration** (час:мин). Максимальная допустимая длительность составляет 4 часа 15 минут. После того как показания счётчика достигнут максимального значения, кнопочная панель будет заблокирована для всех карт. Время, в течение которого клавиши будут заблокированы, указывается в поле **Keypad disabled duration** (Длительность блокировки клавиш).
- Указать время задержки в поле **Reset attempt counter** (Сброс счётчика попыток, мин:сек). После окончания времени, указанного в поле **Reset attempt counter**, система обнулит показания счётчика попыток. Максимальное время задержки составляет 4 минуты 15 секунд. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное значение.

Настройка аппаратного Шлюза KT-NCC

До того как вы начнете настраивать Шлюз KT-NCC, будьте уверены в присвоении сетевых настроек или проконсультируйтесь с сетевым администратором для получение верного IP адреса, для того чтобы избежать конфликтов в сети. Для полной информации на KT-NCC, пожалйста изучите *KT-NCC Installation Manual*, DN1611 и KT-*NCC Quick Configuration Guide*, DN1656. Там возможны три типа сетевого соединения, которые вы можете определить и назначить. Эти настройки необходимо применять в соответствии с вашей сетевой архитектурой.

DHCP with Enterprise Server IP Address (DHCP IP адрес от сервера предприятия):

- Используйте этот тип настройки, когда сервер компании сам назначет IP адреса для связи между севрером и KT-NCC.

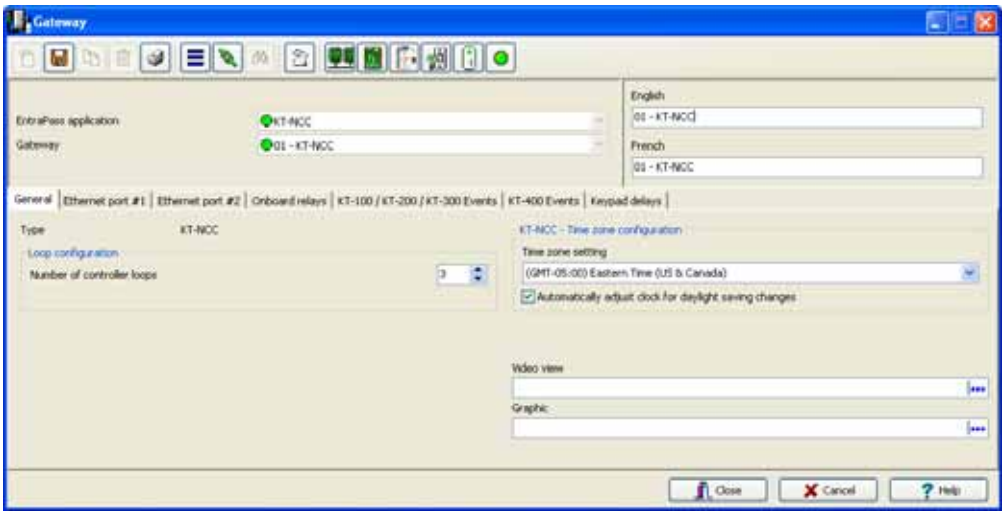
Static IP address (Статический IP адрес)**:**

- Используйте этот тип настройки, когда вы имеете определенный IP адрес для связи между сервером EntraPass и KT-NCC.

ПРИМЕЧАНИЕ: *Изначальная конфигурация будет сделана через web страницу. Пожалуйста изучите KT-NCC Installation Manual*, DN1611 и KT-*NCC Quick Configuration Guide*, DN1656.

WAN: Используйте этот тип соединения в окружении удаленных объектов. Когда связь с KT-NCC защищена роутерами и происходит через Internet.

1 В основном меню EntraPass Workstation, нажмите на вкладку **Devices** (устройства) и выберите **Gateway (Шлюз)**.



2 На вкладке **General** (Общие):

- Нажмите на выпадающее окно Gateway (Шлюз) и выберите ваш Шлюз KT-NCC. Шлюз KT-NCC будет появляться один с номером с правой стороны.
- Укажите **Number of controller loops** (количество лучей контроллеров) в окне под **Loop Configuration** (конфигурация луча). KT-NCC может физически поддерживать 7 лучей с контроллерами.
- В области **KT-NCC Time Zone configuration** (настройка временной зоны), вы должны выбрать подходящую временную зону в графе **Time zone setting** (настройка временной зоны)**.**
- Выделите пункт ниже **Automatically adjust the clock for daylight saving changes**, если вы хотите чтобы система автоматически осуществляла переход на летнее время и обратно.
- Выберите **Graphic** (график) и **Video view** (Вид видео) в который назначен Шлюз, если это приемлемо. Функция **Video View** (Вид видео) будет активная, если это функция разрешена в системе EntraPass.

3 Двигайтесь на вкладку **Ethernet #1** для настрйоки сетевого соединения KT-NCC.

- Введите **MAC адрес** устройства KT-NCC . Первые 6 цифр MAC адреса (00-50-F9 в примере выше) не могут быть изменены.

ПРИМЕЧАНИЕ: *MAC адрес может быть найдет на плате KT-NCC, под портом Ethernet #1. Это 12-ти цифровой 16-ти ричный код, где каждые две цифры разделены чертой. (xx-xx-xx-xx-xx).*

- Следующая таблица показывает какие параметры необходимо указать в зависимости от вашего сетевого окружения.

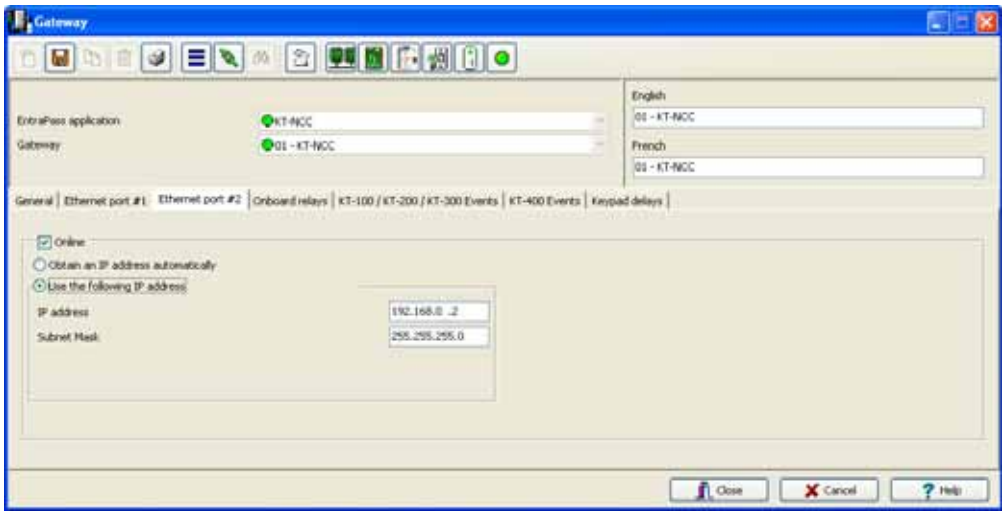
Параметр	DHCP сервер	Статический IP	WAN
Ethernet Port #1	отмечено	отмечено	отмечено
Obtain an IP Address Automatically/(получить IP адрес автматически)	Указать	нет	Указать
Use the Following IP Address/ (использовать следующий IP адрес)	нет	Указать	нет
IP address/(IP адрес)	оставить пустым	KT-NCC IP адрес	оставить как есть
Маска подсети	оставить пустым	KT-NCC Маска подсети	оставить как есть
Шлюз (Роутер)	оставить пустым	KT-NCC Gateway Address	оставить как есть
Порт	18710	18710	18710
Разрешить broadcast assignation	отмечено	отмечено	отмечено
Локальный IP адрес LAN	оставить пустым	оставить пустым	оставить пустым
Public IP адрес (LAN/WAN)	оставить пустым	оставить пустым	Выбрать и ввести public IP адрес от сервера, панель Parameters (параметры).
Имя домена(LAN/WAN)	оставить пустым	оставить пустым	оставить пустым
Use inbound server router	оставить пустым	оставить пустым	отмечено

ПРИМЕЧАНИЕ: *Мы убедительно советуем вам оставить порт по умолчанию* **18710**.

- **Network Response Time** (Сетевое время отклика) это установлено по умолчанию. Вы можете изменять время опроса между сервером EntraPass и KT-NCC.

Параметр	Communication Timing/ Время связи
Очень быстро	время ожидания: макс. 300 ms
Быстро	время ожидания: макс. 800 ms
Средний	время ожидания: макс. 1500 ms
Медленно	время ожидания: макс. 2500 ms
Очень медленно	время ожидания: макс. 4000 ms
Опасно медленно	время ожидания: макс. 6000 ms

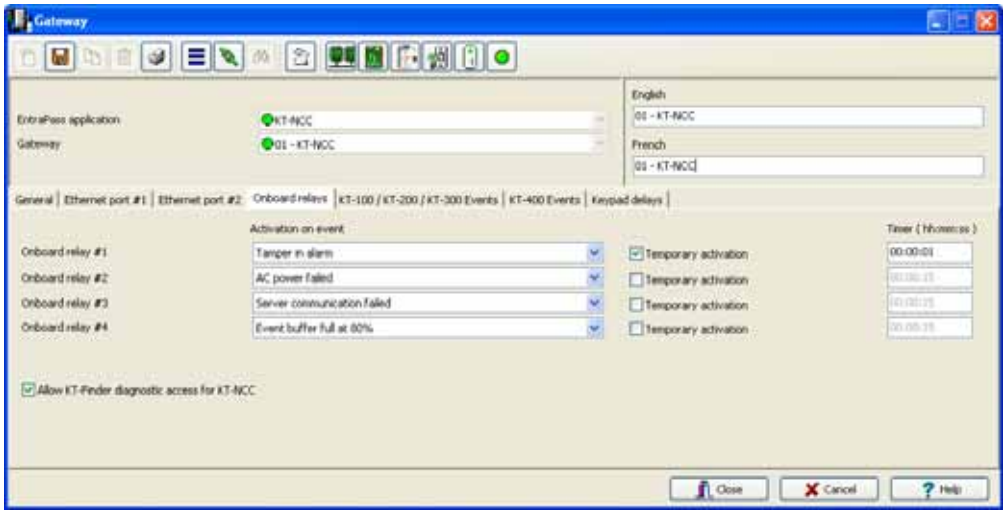
4 Двигайтесь на вкладку **Ethernet #2** когда вам необходимо настроить Ethernet port для работы с IP лучами.



- Выберите **Obtain an IP address automatically** (получить IP адрес автоматически), когда сервер назнает IP адрес.
- Выбирете **Use the following IP address** (использовать следующий IP адрес), когда вы хотите самостоятельно установить **IP адрес и маску подсети**.

5 Двигайтесь далее на вкладку **Onboard Relays** (реле на плате) чтобы назначить условия активации этих реле и длительность сработки этих реле на плате KT-NCC.

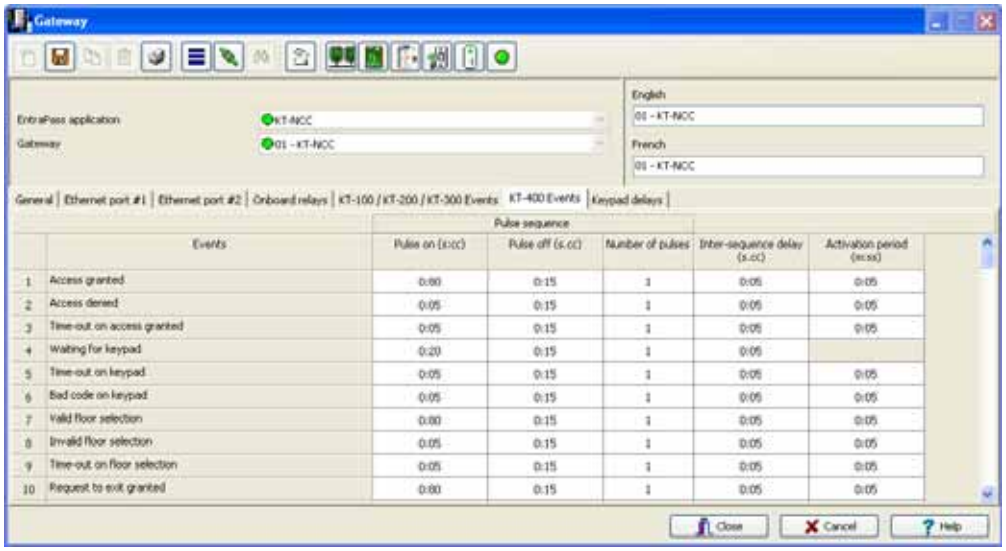
6 Будьте уверены, что пункт выбран пункт: **Allow KT-Finder diagnostic access for KT-NCC** (позволять диагностировать KT-NCC при помощи сервиса KT-Finder).



- Выберите условие активации каждого локального реле на плате в пункте **Activation on event**.
- Если вы хотите только временно активироватьт реле, тогда выделите пункт **Temporary activation** (временная активация).
- Введите время активации в поле **Timer**.

7 Двигайтесь к вкладке **KT-100/KT-200/KT-300 Events** (События KT-100/KT-200/KT-300). Установите **Timer on** и **Timer off** для каждого события. Шлюз KT-NCC позволяет вам управлять событиями KT-100/KT-200/KT-300.

8 Открыть закладку **KT-400 Events** (События KT-400) и настроить включение (**Pulse on**) и выключение (**Pulse off**) пульсации светодиода для каждого события. KT-NCC Шлюз позволяет настроить таким образом связанные события.



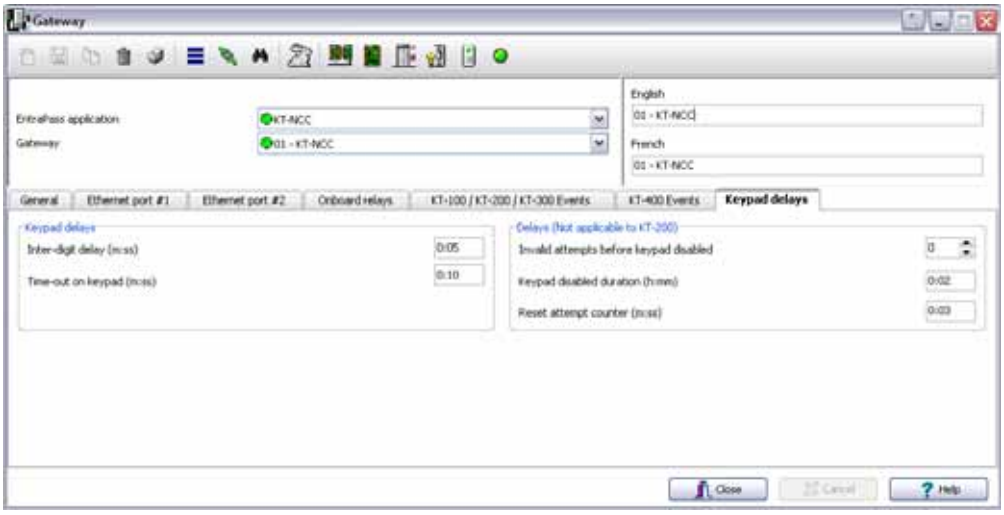
Следующая таблица отображает список всех событий, доступных в Шлюзе KT-NCC:

Access granted (Доступ разрешён)	Time-out on floor selection (Таймаут выбора этажа)	Door unlocked (Дверь разблокирована)
Access denied (Доступ запрещён)	Request to exit granted (Запрос на выход разрешён)	Reader disabled (Считыватель отключён)
Time-out on access granted (Таймаут на разрешение доступа)	Request to exit denied (Запрос на выход запрещён)	Waiting for a second card (Ожидание второй карты) – *прим. 2*
Waiting for keypad (Ожидание нажатия клавиши) – *прим. 1*	Door opened (Дверь открыта)	Time-out on waiting for a second card (Таймаут ожидания второй карты)
Time-out on keypad (Таймаут нажатия клавиши)	Door forced open (Дверь силой открыта)	Access denied - Waiting for a second card (Доступ запрещён - Ожидание второй карты)
Bad code on keypad (Неверный код клавиши)	Pre-alarm door opened too long (Предтревожное состояние двери при слишком долгом открытии)	Access denied - Waiting for a second card (Доступ запрещён - Ожидание второй карты)
Valid floor selection (Достоверный выбор этажа)	Door open too long (Дверь открыта слишком долго)	
Invalid floor selection (Недостоверный выбор этажа)	Door alarm on relock (Сигнализация двери при выполнении блокировки)	

ПРИМЕЧАНИЕ 1: *Чтобы задать время активации события* ***Waiting for keypad*** *(Ожидание нажатия клавиши), следует открыть закладку* ***Keypad delays*** *(Задержки нажатия клавиш), как описано* ***пункт 9****.*

ПРИМЕЧАНИЕ 2: *Чтобы настроить время активации события* ***Waiting for a second card*** *(Ожидание второй карты), следует выполнить указания, описанные* ***в Главе 4 Настройка конфигурации 4-дверного Ethernet-контроллера KT-400 на стр. 122****.*

9 Под закладкой **Keypad delays** (Задержки нажатия клавиш) выполнить настройку клавиатуры считывателя:



- В разделе **Keypad delays** указать значение параметра **Inter-digit delay** (Задержка между двумя последовательными нажатиями клавиш, мин:сек). Это максимально допустимое время задержки перед каждым последующим выбором клавиши пользователем.
- Указать время задержки в строке **Time-out on keypad** (Таймаут нажатия клавиши, мин:сек). Значение этого параметра задаётся в секундах. Это максимальное время, отведённое пользователям, для того чтобы начать ввод кода на кнопочной панели считывателя.

ПРИМЕЧАНИЕ: *Максимальное время задержки, допустимое между нажатием двух клавиш (Inter-digit delay), а также для таймаута (Time-out on keypad) составляет 2 минуты 7 секунд. Значения этих же параметров для контроллера KT-400 составляют 4 минуты 15 секунд.*

- При помощи клавиш со стрелками вверх/вниз в разделе настройки задержек **Delays (KT-100, KT-300, KT-400)** указать **число неверных попыток, после которых кнопочная панель считывателя блокируется**. Максимально возможное число неудачных попыток пользователей, после которых выполняется автоматическая блокировка клавиш, составляет 255 попыток.
- Указать длительность блокировки кнопочной панели в строке **Keypad disabled duration** (час:мин). Максимальная допустимая длительность составляет 4 часа 15 минут. После того как показания счётчика достигнут максимального значения, кнопочная панель будет заблокирована для всех карт. Время, в течение которого клавиши будут заблокированы, указывается в поле **Keypad disabled duration** (Длительность блокировки клавиш).
- Указать время задержки в поле **Reset attempt counter** (Сброс счётчика попыток, мин:сек). После окончания времени, указанного в поле **Reset attempt counter**, система обнулит показания счётчика попыток. Максимальное время задержки составляет 4 минуты 15 секунд. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное значение.

Настройка лучей (loops)

Луч состоит из контроллеров, подключённых к одному и тому же последовательному порту. Данная система может управлять до 32 локальных лучей на Corporate Шлюз, 8 лучей на NCC-8000 Шлюз, 3 физических прямых луча на на KT-NCC Шлюз, и 32 луча на Global Шлюз. EntraPass также позволяет пользователям добовлять до 512 удаленных соединений на Corporate Шлюз. Лучи Corporate и Global Шлюза состоят из контроллеров KT-100, KT-200, KT-300 и KT-400. Не рекомендуется использовать контроллеры KT-100, KT-200, KT-300 и KT-400 в одном луче.

Предметы отображаются в EntraPass в окне EntraPass Site/Loop window , отличаясь типом соединения. Например, если выбран тип соединения RS-232, то вкладка **RS-232** будет отображена для настройки серийного порта и скорости передачи. Если тип соединения это dial-up, то там три дополнительные таблицы будут отображены для конфигурации.

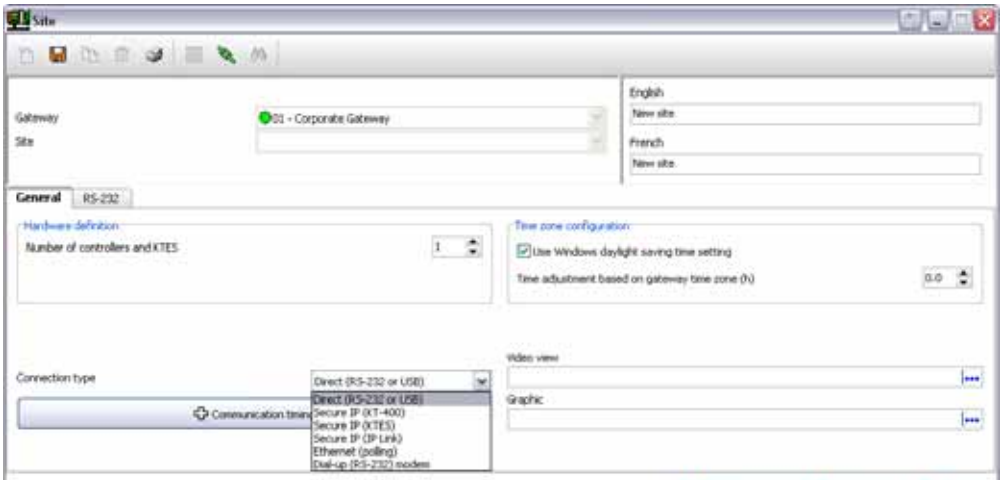
Всего предусмотрено шесть типов соединения: прямое "Direct (RS-232 / USB)", Sucure IP (KT-400), Secure IP (KTES), Secure IP (Kantech IP Link)", опрос "Ethernet (polling)" и по коммутируемой линии через модем "Dial-Up (RS-232) modem". Проверьте следующую таблицу по типу подсоединения к Шлюзу..

Тип соединения	Corporate Шлюз (*Їрим.1*)	Global Шлюз (*Прим.2*)	KT-NCC (*Прим. 2*)
Прямое(RS-232 или USB)	Да	Да	Да
Ethernet (опрос)	Да	Да	ms
Secure IP (KT-400)	Да	Нет	
Secure IP (KTES)	Да		
Secure IP (IP Link)	Да		
Dial-up (RS-232) модем	Да		

ПРИМЕЧАНИЕ 1: *Corporate Шлюз доступен во всех версиях EntraPass. Даже несмотря на то, что об этом не заявляется в Special Edition, Special Edition включает функции Corporate Gateway.*

ПРИМЕЧАНИЕ 2: *KT-NCC и Global Шлюз доступны только с EntraPass Global Edition.*

1 В окне **Devices** (Устройства) нажать иконку **Site** (Луч).



2 Выбрать шлюз в поле **Gateway**, который будет использоваться для подключения луча.

3 При настройке нового луча, его имя следует добавить в поле **Site** (луч) и сохранить кнопкой **Save** (Сохранить). Кружочек рядом с именем сайта станет зелёным.

ПРИМЕЧАНИЕ: *Под Шлюзами Global, NCC-8000 и KT-NCC, луи назначаются через Шлюз.*

4 Под закладкой **General** (Общие параметры) выполнить следующие настройки:

- В разделе **Hardware definition and KTES** (Описание оборудования и KTES) указать число контроллеров на луче. На каждом луче может быть подключено до 32 контроллеров. При вводе значения, превышающего максимально допустимую величину, система будет использовать число 32. t

ПРИМЕЧАНИЕ: *Когда вы указываете тип соединения как* ***Secure IP (KTES)*** *(Надежное IP KTES), количество KTES автоматически ограничивается одним на KTES на луч.*

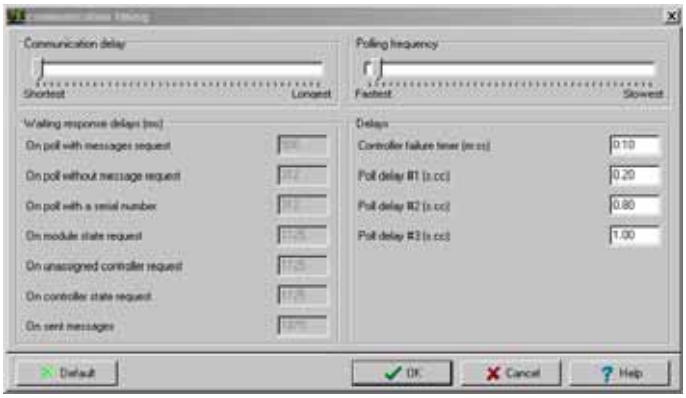
- В разделе **Daylight saving time options** (Настройки летнего времени) поставить флажок в поле **Use Windows daylight saving time setting** (Использовать настройки летнего времени Windows), чтобы автоматически переключаться на летнее время согласно стандартным настройкам операционной системы Windows. Или не ставить флажок в этом поле, чтобы производить эту настройку вручную.
- Если связь с удалённым лучом осуществляется по модему, необходимо указать разницу во времени между географическим местом расположения шлюза и сервера EntraPass в поле **Time adjustment based on Gateway timezone, в часах.** Таким образом, события, происходящие на удалённом сайте, будут отображаться на рабочих станциях EntraPass, расположенных в разных часовых поясах, в соответствии с местным временем шлюза.
- Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплён шлюз. Выбор видеоокна будет доступным только в том случае, если в системе EntraPass разрешено использовать функцию видеонаблюдения. Выбор видеоокна будет доступным только в том случае, если в системе EntraPass разрешено использовать функцию видеонаблюдения.
- В списке **Connection type** (Тип соединения) выбрать способ соединения между компьютером и шлюзом . От этого зависит, какие закладки отображаются в окне настройки.

ПРИМЕЧАНИЕ: *Эта опция недоступна в Шлюзе NCC-8000.*

Настройка времени опроса соединения

ОСТОРОЖНО! Ни в коем случае не следует самостоятельно изменять значения параметров в разделе **Communication timing!** Если необходимо настроить в линии связи задержку и частоту опроса, следует обратиться в службу технической поддержки Kantech. Ненадлежащее изменение настроек может вызвать серьёзные проблемы в работе системы!

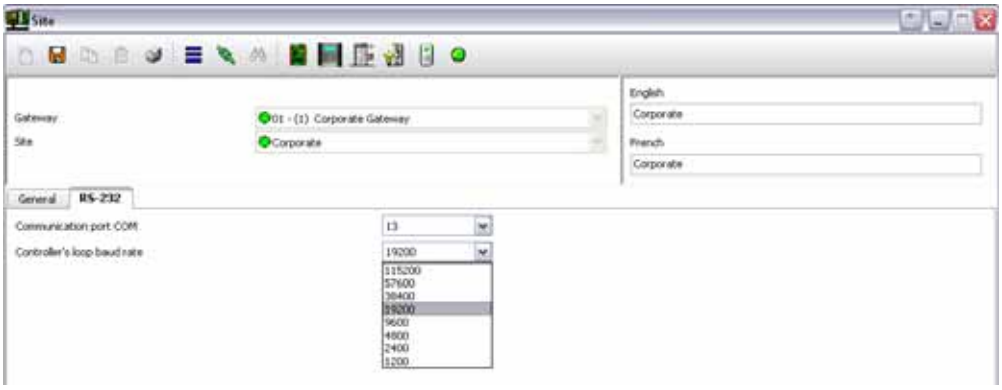
Окно Communication timing отображает значения параметров по умолчанию. Эти значения должны оставаться неизменными, если только иное не указано изготовителем (Kantech).



Настройка прямого соединения лучей через RS-232

Этот тип соединения используется в системах EntraPass версии EntraPass Global Edition для Global и Corporate шлюзов, также в KT-NCC для связи через RS-232 с лучами.

1 При выборе опции **Direct RS-232 connection type** под закладкой **General** (Общие параметры) появляется дополнительная закладка **RS-232**.



- В поле Communication Port COM указать номер порта.
- Выбрать скорость передачи данных в ветви контроллеров. По умолчанию используется 19200 бит/с.

Настройка конфигурации IP соединений (только для шлюзов Corporate)

Этот тип соединения используется в системах EntraPass Global Edition с Corporate Шлюзом для соединения через модуль Kantech IP Link или через 4-дверный Ethernet-контроллер KT-400 или KTES.

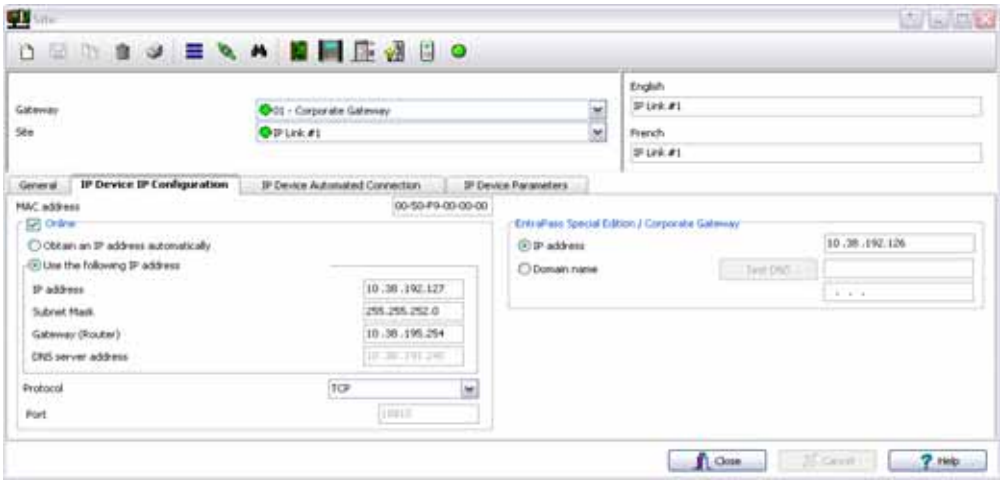
ПРИМЕЧАНИЕ 1: *Для получения самых полных сведений по конфигурации модуля Kantech IP Link рекомендуем изучить руководство по установке модуля Kantech IP Link (DN1670).*

ПРИМЕЧАНИЕ 2: *Чтобы получить наиболее полные сведения о 4-дверном Ethernet-контроллере KT-400, следует обратиться к соответствующему руководству по установке (DN1726).*

ПРИМЕЧАНИЕ 3: *Если выбран тип соединения Secure (IP KT-400), то главным контроллером должен быть KT-400.*

ПРИМЕЧАНИЕ 4: *Для KTES, контроллером в луче должен быть KTES. Для более подробной информации по установке KTES, пожалуйста изучите уснструкцию по установке KTES Installation Manual, DN1769.*

1 Выберите один из пунктов в **Connection type** под закладкой **General** указан тип соединения Secure IP (IP Link) или Secure IP (KT-400). Появляются три дополнительных закладки: **IP Device IP configuration**, **IP Device Automated Connection** and **IP Device Parameters**.
   - **IP Device IP configuration** - Настройка IP устройства
   - **IP Device Automated Connection** - Автоматическое соединение IP устройства
   - **IP Device Parameters-** Параметры IP устройства



- **MAC Address** (MAC-адрес). В этом поле необходимо указать MAC-адрес устройства. Первые 6 знаков в поле MAC-адреса (00-50-F9) должны остаться неизменными
- Поставить флажок в поле **Online** (Подключить).

- **Obtain IP address automatically** (Получить IP-адрес автоматически). Эту опцию следует использовать при настройке устройства с зарезервированнымс предоставлемым IP-адресом в конфигурации DHCP.
- **Use the following IP address** (Использовать следующий IP-адрес). Эта опция позволяет назначить статический IP-адрес для данного устройства. При выделении этой опции появляются три дополнительных параметра:
  - **IP Address** (IP-адрес). Статический IP-адрес назначается системным администратором.
  - **Subnet Mask** (Маска подсети). Этот адрес назначается системным администратором.
  - **Gateway/Router** (Шлюз/Роутер). Этот адрес назначается системным администратором.
  - **DNS Server Address** (Адрес DNS сервера). Этот адрес назначается системным администратором.
- **Протокол:** Используемый для опредления протокола связви **UDP** или **TCP**.
- По умолчанию для данного устройства автоматически назначается порт **18810.** Его не следует изменять, за исключением случаев, когда IP-устройство подключено удалённо, например, через WAN.

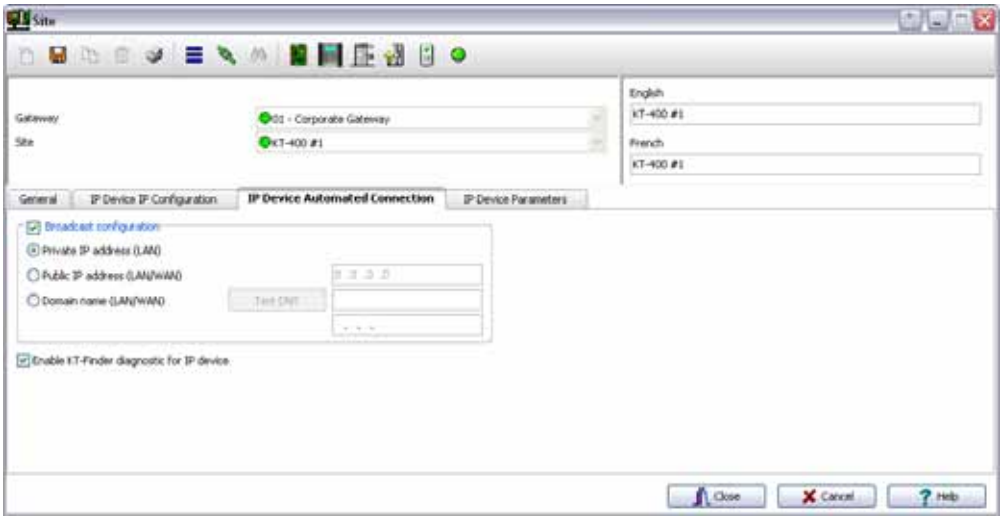
ПРИМЕЧАНИЕ: *Порт 18802 должен быть использован с KT-400 или IPLink.*

- **EntraPass Special Edition / Corporate Шлюз IP адрес** будет использоваться.
  - **IP address:** Вы будете вводить IP адрес компьютера Шлюза.
  - **Domain name:** Если вы не имеете IP адрес шлюза, вы можете ввести имя домена, выданное вам системным администратором (только для Kantech IP Link и KT-400).

ПРИМЕЧАНИЕ: *Здесь следует указать либо IP-адрес, либо доменное имя. Вводить данные в оба поля не требуется.* (Только для Kantech IP Link и KT-400).

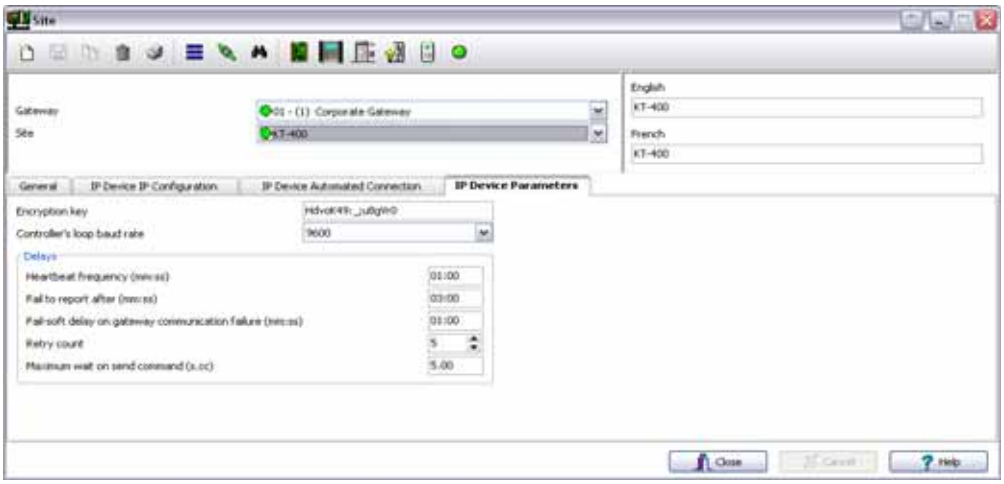
- **Test DNS** (Тест **DNS**). После ввода доменного имени следует нажать кнопку **Test DNS.** При этом в поле **IP address** должен отобразиться соответствующий IP-адрес. (Только для Kantech IP Link и KT-400)

2 Если используется подключение через WAN, следует перейти к закладке **IP Device automated connection** (Автоматическое соединение IP устройств).



- В поле **Broadcast configuration** (Конфигурация широковещательного запроса) обязательно должна стоять галочка!
  - **Private IP Address (LAN):** Будет назначен IP адрес автоматически.
  - **Public IP Address** (Публичный IP-адрес), **WAN**. Этот IP-адрес предоставляется провайдером Интернет-услуг. Соответствует IP-адресу удалённого луча.
  - **Domain Name** (Доменное имя), **WAN.** Эта информация должна быть предоставлена системным администратором. Соответствует IP-адресу удалённого луча.
- **Enable KT-Finder diagnostic for IP device** (Сделать доступным мастер обнаружения устройств KT-Finder). Выделите эту опцию, если вы хотите использовать KT-Finder в качестве инструмента для настройки и отладки.

3 Двигайтесь в раздел **IP Device Parameters** (Параметры IP устройств) для настройки параметров безопасности и параметров связи.



- **Encryption key** (Шифр-ключ). В этом поле следует ввести 16-значный шестнадцатеричный код для защиты луча.
- **Controller's loop baud rate** (Скорость передачи данных в луче контроллера). Выбрать скорость передачи данных из выпадающего списка.

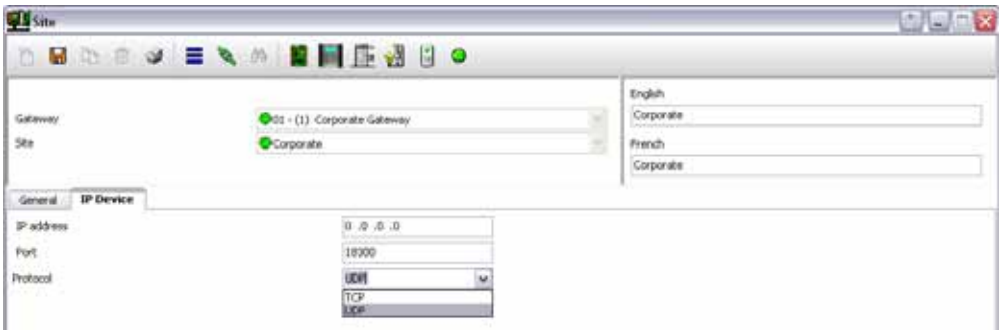
ПРИМЕЧАНИЕ: *Для контроллеров KT-200 максимальная скорость передачи данных составляет 19200. .*

- В меню **Delay** (Задержки) необходимо выполнить следующие настройки:
  - **Heartbeat frequency (мин:сек)** (Частота контрольных сообщений). В этом поле следует указать частоту, с которой IP устройство должно отправлять на шлюз сигнал для проверки связи (от 00:15 до 10:00).
  - **Fail to report after (мин:сек)**: Введите задержку на подтверждение об ошибке связи (01:30 до 59:59).
- **Fail-soft delay on gateway communication failure, мин:сек** (Задержка включения безопасного режима при потере соединения со шлюзом, мин:сек). В этом поле следует указать время задержки, по окончании которого IP устройство будет считать, что связь с контроллером потеряна и контроллер работает в автономном режиме.
- **Retry Count** (Число повторов). Число попыток (от 1 до 15) Шлюза установить связь между IP модулем Kantech с указанным выше интервалом задержки, по истечении которых связь будет считаться потерянной.
- **Maximum wait on send command (Максимальное время ожидания на отправку команды) (s.cc)**: Когда необходимо, введите максимальное время задержки, которое шлюз будет предоставлять IP устройству для того чтобы подтвердить получение команды от APM Workstation EntraPass (1.00 до 9.99).

Настройка конфигурации соединения типа Ethernet опрос

Этот тип соединения может быть настроен между лучем через Lantronix и EntraPass Global Edition Corporate/Global Шлюз.

1 Если под закладкой **General** (Общие параметры) выбран тип соединения **Ethernet (Polling)**, появляется дополнительная закладка **IP device** (IP устройство).



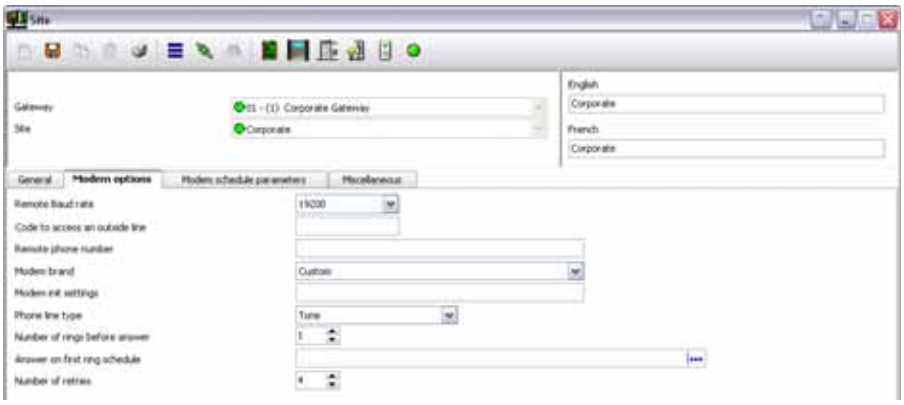
- В полях **IP address** и **Port** следует указать IP-адрес и порт.
- В поле **Protocol** необходимо выбрать протокол связи:
  - **TCP,** если луч осуществляет связь со шлюзом через терминальный сервер при помощи протокола TCP. В этом случае необходимо выбрать конфигурацию терминального сервера. Для этого необходимо выполнить указания изготовителя или инструкции, изложенные в руководстве по эксплуатации терминального сервера.
  - **UDP** (протокол пользовательских дейтаграмм), использует IP-протокол для отправки дейтаграмм из одного Internet-приложения в другое. Является протоколом "без установки соединения", так как не требует организации прямого соединения для обмена данными. Если настраиваемый луч использует этот протокол, следует отметить флажком это поле.

Настройка конфигурации соединения типа Dial-Up (RS-232) Modem (Связь через модем по коммутируемой линии)

Если в меню **General** (Общие параметры) в выпадающем списке **Connection type** (Тип соединения) выбрана опция **Dial-up (RS-232) modem**, на экране появляются три дополнительные закладки: Modem options (Настройки модема), Modem schedule parameters (Параметры расписания модема) и Miscellaneous (Прочее).

ПРИМЕЧАНИЕ: *Опция связи по коммутируемой линии через модем доступна только при выборе приложения шлюза (Corporate Gateway).*

1 Открыть закладку **Modem Options** (Настройки модема) и настроить характеристики исходящего вызова модема.



ПРИМЕЧАНИЕ: *Параметр **Remote Baud rate** (Скорость обмена данными с удалённым лучом) должен оставаться неизменным. При возникновении вопросов по поводу тех или иных настроек модема следует обращаться к системному администратору, обслуживающему данное оборудование.*

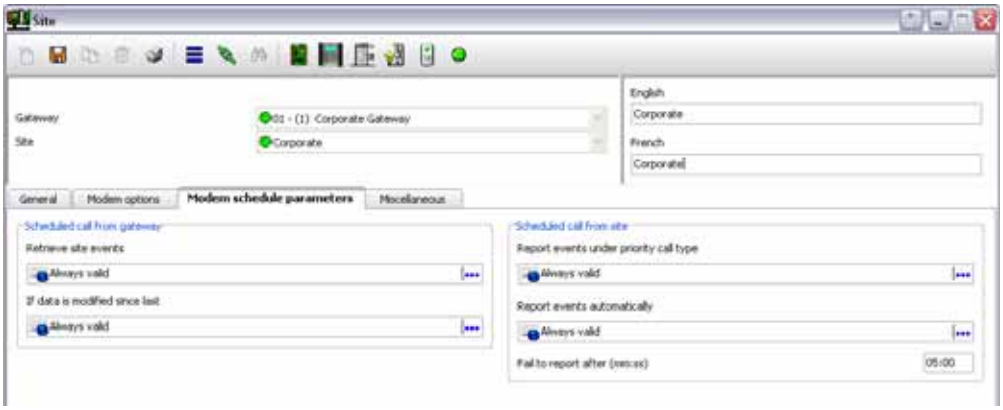
- В поле **Code to access an outside line** указать код для доступа к внешней линии (если используется).
- Введите телефонный номер удалённого луча в поле **Remote phone number**.

ПРИМЕЧАНИЕ: *В целях обеспечения высокой надёжности и идеальной совместимости всех устройств компания Kantech к настоящему моменту обеспечила поддержку внешних модемов только серии US Robotics Sportster.*

ПРИМЕЧАНИЕ: *Параметр **Modem init settings** (Начальные настройки модема) должен оставаться неизменным.*

- В поле **Phone line type** указать тип телефонной линии: Tone (тоновый) или Pulse (пульсация).
- В поле **Number of rings before answer** указать число гудков, предшествующих ответу модема. Эта опция действует во всех случаях, когда расписания звонков не используются.
- Настроить опцию **Answer on first ring schedule** (Расписание ответа на первый звонок), то есть временной интервал, в течение которого модему сайта разрешено отвечать на первый гудок.
- Указать число попыток в поле **Number of retries**. Это число вызовов, которые предпринимает модем, прежде чем положить трубку.

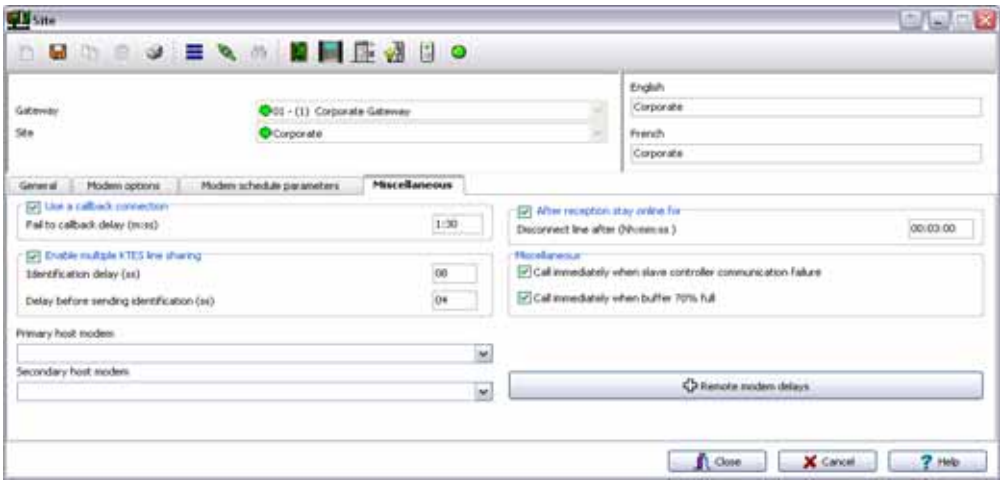
2 Перейти к закладке **Modem Schedule parameters** (Параметры расписания модема) для настройки временных интервалов подключения шлюза к удалённым лучам (или лучей к шлюзу) через модем с целью выполнения определённых задач.



- Нажать кнопку **Retrieve site events** (Извлечь события луча), чтобы открыть окно выбора расписания. Выбрать расписание, наиболее соответствующее требованиям поставленной задачи. Речь идет о временном интервале, когда будут запрошены события от удаленного луча. Более подробные сведения о задании расписаний изложены *в Главе 5 Назначение расписаний на стр. 174*
- Повторить те же действия для пунктов **If data is modified since last** (Если данные изменились с момента последнего ...), **Report events under priority call type** (Сообщать о событиях по типу приоритетного вызова) и **Report events automatically** (Сообщать о событиях автоматически).
- В поле **Fail to report after, mm:ss** (Не удалось сообщить, мин:сек) указать задержку, по окончании которой система выдаст сообщение о невозможности запроса событий.

ПРИМЕЧАНИЕ: *Чтобы составить план оповещения о событиях по типу приоритетных вызовов, сначала необходимо указать типы приоритетных вызовов в разделе* ***Priority call types*** *(Типы приоритетных вызовов) для таких объектов, как двери, входы и контроллеры.*

3 Открыть закладку **Miscellaneous** (Прочее) и указать, как модемы должны обрабатывать исходящие и входящие звонки сайтов.



- Поставить флажок в поле **Use a callback connection** (Использовать функцию перезвонить), чтобы заставить модем шлюза разъединять связь после первого соединения с модемом удалённого сайта и ожидать ответного вызова с удалённого модема. Кроме того, можно по своему желанию изменить длительность задержки для выполнения обратного вызова в поле **Fail to callback delay.** По умолчанию установлено 1:30 (1 мин. 30 сек.).
- Это опция предлагается только для KTES. Поставьте галочку **Enable multiple KTES line sharing** (Разрешить несколько KTES на одну линию) для возможности изменения **Identification delay** (время идентификации) **(ss)** между каждым KTES. Возможность регулировки времени от 00 and 20 seconds.

- Указать данные в выпадающем списке **Primary host modem** (Основной хост-модем). Если необходимо, указать резервный модем в поле **Secondary host modem** (Дополнительный хост-модем)**.** Эта настройка пригодится, если основной модем занят или не может принять вызов.
- Поставить флажок в поле **After reception stay online for** (После приёма вызова оставаться на линии в течение ...), чтобы ограничить длительность поступающего вызова до любой величины в диапазоне от 00.03.00 до 23.59.59.
- Отметить флажком опцию **Call immediately when slave controller communication failure** (Немедленно звонить в случае потери связи с ведомым контроллером), чтобы получить уведомление в случае, когда ведомому контроллеру не удаётся отправить данные на главный контроллер (к которому подключен модем).
- Выделить опцию **Call immediately when buffer 70% full** (Немедленно звонить в случае заполнения буфера на 70%), чтобы загружать события, хранящиеся в буфере контроллера сайта, как только ёмкость буфера будет заполнена на 70%.

ПРИМЕЧАНИЕ: *Кнопку* ***Remote modem delays*** *(Задержки удалённого модема) нажимать не следует! Все указанные в этом пункте меню значения параметров настроены на заводе-изготовителе, чтобы обеспечить оптимальную работу системы с модемами типа US Robotics. Эти настройки* **НЕ СЛЕДУЕТ** *изменять, если только иное не рекомендовано специалистами компании Kantech.*

Настройка конфигурации контроллеров

Контроллеры обеспечивают визуальную и звуковую обратную связь с пользователями, информируя их о разрешении/отказе доступа. Как правило, красный/зелёный светодиодный индикатор на считывателе информирует владельца электронной карты, что дверь разблокирована или доступ закрыт. Для звукового предупреждения на дверь может быть установлена локальная сигнализация, предупреждающая о взломе двери или незакрытии её после входа посетителя.

Параметры конфигурации контроллера сообщают системе, как этот контроллер используется и какие устройства к нему подключены (двери, входы, реле и выходы). Контроллеры могут быть назначены в течении настройки шлюза или луча; а также меню назначения контроллера, вызываемое нажатием на пиктограмму контроллера (**Devices > Controller**), или через программу автоматической установки Express Setup. Система EntraPass поддерживает четыре типа контроллеров: KT-100, KT-200, KT-300 и KT-400. Эти четыре типа контроллеров удовлетворяют потребностям системы по использованию локальных функций, выполняемых контроллерами. Число устройств, связанных с контроллером, зависит от его типа. Основные компоненты, связанные с каждым типом контроллеров Kantech, перечислены в таблице:

Тип	Кол-во дверей	Кол-во реле	Кол-во входов	Доп. выходы
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4
KT-400	4	4	16	16

ПРИМЕЧАНИЕ: *Шлюз NCC-8000 поддерживает только KT-200. Шлюзы Corporate и Global поддерживают все контроллеры Kantech (KT-100, KT-200, KT-300 и KT-400). Под шлюзом NCC-8000, система позволяет вам максимум подключить 16 контроллеров на луч, и 8 лучей на NCC-8000. Только KT-200 с ПЗУ EP-8002 EPROM может быть свзязана с Шлюзом NCC-8000. Под Global, KT-200 должна быть использована с ПЗУ EP-Entra3 EPROM.*

KT-400 4-дверный Ethernet-контроллер

KT-400 – это 4-дверный Ethernet-контроллер, который представляет верное решение для любой компании, стремящейся обеспечить максимальный уровень безопасности. Его можно интегрировать в уже действующие системы EntraPass с версии 4.01, а также использовать вместе с другими контроллерами Kantech или в качестве основы при создании новых систем безопасности. В Северной Америке (UL) и Европе (EU) контроллеры KT-400 стоят на пороге открытия новых восхитительных возможностей.

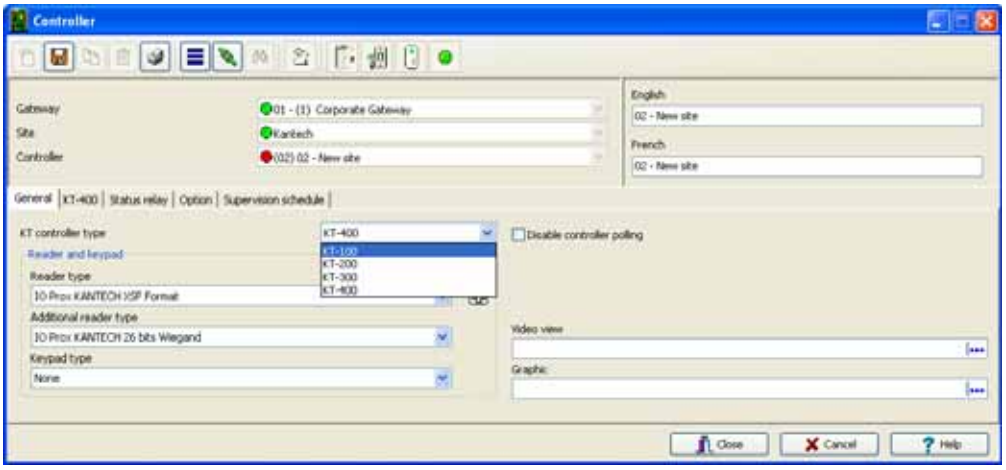
Основные преимущества

- До 256 входов (16 входов уже на плате контроллера, с возможностью использования схемы с двойным оконечным резистором)
- До 256 выходов
- Четыре реле формы «C» на плате контроллера
- 16 выходов считывателя на плате контроллера типа открытый коллектор
- Встроенное 128-битное шифрование по стандарту AES (улучшенный стандарт шифрования) обеспечивает высокую степень безопасности сети
- Съёмные клеммные колодки
- Встроенный порт Ethernet обеспечивает быстрое подключение к сети (WAN\LAN), без необходимости использования внешних Ethernet-устройств
- Автоматическое обнаружение порта
- Для считывателей, замков и других устройств предусмотрен встроенный блок питания с аккумулятором, что обеспечивает беспрерывную работу и сокращает время и материальные затраты на установку, так как отпадает необходимость использования внешнего источника питаниия.
- Совместимость с контроллерами Kantech KT-100, KT-300 и (KT-200 на отдельном луче)

- Отдельный вход тампер (Tamper Input)
- Возможность организации дополнительного питания на замки с платы контроллера
- Четыре конфигурируемых выхода на каждый считыватель типа открытый коллектор
- Встроенный Web browser для настройки устройства.
- Возможность связи по нескольким портам (IP, RS-485 и RS-232)
- Низкая нагрузка на пропускную способность сети
- Визуальные индикаторы статуса (светодиоды)
- Возможность мониторинга большего количества состояний контроллера
- Контроль локальной области внутри контроллера с локальным контролем повторного прохода.
- 100 000 идентификационных карт на каждый контроллер и 20 000 сохранённых событий при работе в автономном режиме
- Активации по времени на определенные действия и события

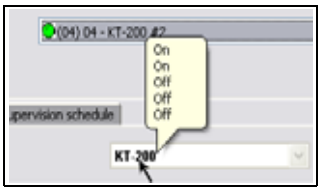
Назначение общих параметров (General) для контроллеров Kantech

1. В меню **Devices** (Устройства) **> Controller** (Контроллер) выбрать шлюз, связанный с лучом/сайтом контроллеров.
2. В выпадающем списке **Site** (луч) указать луч, на котором расположен настраиваемый контроллер.
3. В выпадающем списке **Controller** (Контролер) выделить контроллер, конфигурацию которого необходимо настроить. После выделения появляется меню для выбора имени на используемых языках. В этом разделе можно переименовать выбранный контроллер.
4. В выпадающем списке **General** (Общие параметры) выделить тип контроллера в поле **KT Controller type.**



- В разделе выбора имени на используемых языках (в проиллюстрированном примере это английский (English) и французский (French) языки) назначить этому контроллеру содержательное имя и сохранить его кнопкой **Save** (Сохранить). После сохранения данных выпадающий список **Controller type** (Тип контроллера) становится недоступным.

ПРИМЕЧАНИЕ: *Если выбран тип контроллера KT-200, то рядом с выпадающим списком появляется номер. При установке курсора на этот номер появляется всплывающая подсказка, указывающая параметры настройки для этого контроллера KT-200. .*



- Система должна предложить воспользоваться программой автоматической установки Express Setup. Нажать **Yes** (Да) для продолжения работы. в случае выбора **No** (Нет) пользователь должен вручную установить конфигурацию этих устройств через соответствующие меню описания (двери, реле, входы и дополнительные выходы).

ПРИМЕЧАНИЕ: *Система EntraPass даёт возможность установить два типа считывателей на одном контроллере (основной и дополнительный). Оба считывателя должны быть построены на одной и той же технологии (Wiegand или ABA). Эта функция доступна с контроллерами KT-100, KT-300, KT-400 под Шлюзами Global и Corporate.*

- После настройки конфигурации компонентов, связанных с контроллером, необходимо выбрать считыватель и кнопочную панель, установленную на данном контроллере, из выпадающего списка **Reader** (Считыватель) и **Keypad type** (Тип кнопочной панели). Смотрите **в пункте 4-1** описание типов считывателей и **в пункте 4-2** описание типов кодонаборника.

Таблица 4-1: Типы считывателей

Типы считывателей	KT-100	KT-200	KT-300	KT-400
ABA с картами CNPID	Да	Да	Да	
BC-201 - CF100	Да	Да	Да	
BC-201 Barcode с картами Polaris	Да	Да	Да	Да
CARDKEY	Да	Да	Да	
CASI-RUSCO 26/28-Bit Wiegand	Да	Да	Да	
CHECKPOINT Sielox Format	Да	Да	Да	
CHUBB	Да	Да	Да	
DORADO ABA clock and data	Да	Да	Да	
DORADO ABA Wiegand	Да	Да	Да	
DORADO EMPI 26-Bit	Да	Да	Да	
DORADO EMPI 34-Bit	Да	Да	Да	
FIPS 201 75-bit no expiry date				Да
FIPS 201 75-bit with expiry date				Да
H10302, 37-Bit	Да	Да	Да	Да
HID CORPORATE 1000 Generic	Да	Да	Да	Да
HID iClass 37-Bit No Party				Да
HID KSF (Kantech Secure Format)	Да	Да	Да	Да
HUGHES 36-Bit - CF104	Да	Да	Да	
INDALA old 27-Bit Format	Да	Да	Да	
INTERCON	Да	Да	Да	
ioProx Dual Driver (26-Bit and XSF)	Да	Да	Да	Да
ioProx Kantech 26-Bit Wiegand	Да	Да	Да	Да
ioProx Kantech XSF Format	Да	Да	Да	Да
ioProx UK 31-Bit Wiegand				Да
Карта KRONOS со считывателями штрих кода	Да	Да	Да	
Mifare 32-Bit CSN	Да	Да	Да	Да
Mifare 34-Bit AID 517A	Да	Да	Да	
Mirage 135	Да	Да	Да	
NCS	Да	Да	Да	
Northern 32-Bit с NR1 Reader	Да	Да	Да	
Northern 34-Bit с Hughes Reader	Да	Да	Да	

Типы считывателей	KT-100	KT-200	KT-300	KT-400
Paramount Farm 32-Bit Wiegand	Да	Да	Да	Да
Polaris 1 - CF101	Да	Да	Да	
Polaris 1 с 10-Digit Cards	Да	Да	Да	
Polaris 1 с 16-Digit Cards	Да	Да	Да	
Polaris 1 с Polaris Cards	Да	Да	Да	Да
Polaris 2 ABA с 10-Digit Cards	Да	Да	Да	
Polaris 2 ABA with 16-Digit Cards	Да	Да	Да	
Polaris 2 ABA with Polaris Cards	Yes	Yes	Yes	Yes
Polaris 2KP ABA with 10-Digit Cards	Yes	Yes	Yes	
Polaris 2KP ABA with 16-Digit Cards	Yes	Yes	Yes	
Polaris 2KP ABA with Polaris Cards	Yes	Yes	Yes	Yes
Polaris 32/35/37 CHRS - CF103	Yes	Yes	Yes	
RBH 50-Bit Card Driver				Yes
SCHLAGE 1030 and 1040 Card Format	Yes	Yes	Yes	
Sensor 26-Bit Wiegand Standard	Yes	Yes	Yes	Yes
Sensor 34-Bit Wiegand	Yes	Yes	Yes	Yes
SFT-R50 26-Bit	Yes	Yes	Yes	
Shadow PROX	Yes	Yes	Yes	Yes
Siteguard Format	Yes	Yes	Yes	
Wiegand 26/28-Bit - CF102	Yes	Yes	Yes	
WLS Wireless 26-Bit	Yes	Yes	Yes	
WLS Wireless Shadow Prox and HID	Yes	Yes	Yes	

Таблица 4-2: Типы клавиатур

Типы клавиатур	KT-100	KT-200	KT-300	KT-400
KP-1003H	Yes	Yes	Yes	
KP-500, KP-2000, KP-2500, KP-3000	Yes	Yes	Yes	
ioProxc интегрированной клавиатурой (8-Bit Burst)	Yes	Yes	Yes	Yes
POL-2KP - 5-цифровая интегрированная клавиатура	Yes	Yes	Yes	Yes

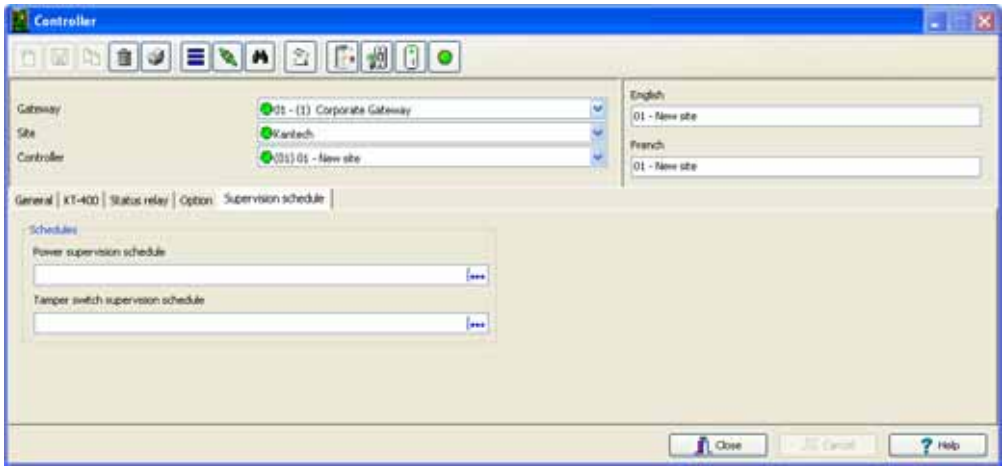
ПРИМЕЧАНИЕ: *Иконка* **New reader driver** *(Новый драйвер считывателя) позволяет пользователю установить свой драйвер для определённого контроллера. Помимо этого, данная кнопка служит для добавления драйвера в таблицу Reader+ Driver, из которой его можно будет использовать и в следующий раз при добавлении нового контроллера.*

- Чтобы запретить работу контроллера, следует отметить флажком опцию **Disable controller polling** (Запретить опрос контроллера). В этом режиме контроллер не будет опрашиваться системой ни при каких условиях, и на все запросы статуса от этого контроллера система будет отправлять сообщение, что этот контроллер отключён.

ПРИМЕЧАНИЕ: *Данную опцию полезно использовать при необходимости физически отсоединить контроллер, не удаляя его из системы (например, для ремонта). Кроме того, она позволяет операторам легко настраивать программное обеспечение до завершения физического монтажа системы.*

- Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплён шлюз. Выбор видеоокна будет доступным только в том случае, если в системе EntraPass разрешено использовать функцию видеонаблюдения.

5 Чтобы настроить расписания работы нового контроллера, следует перейти к закладке **Supervision Schedule** (Расписание контроля).



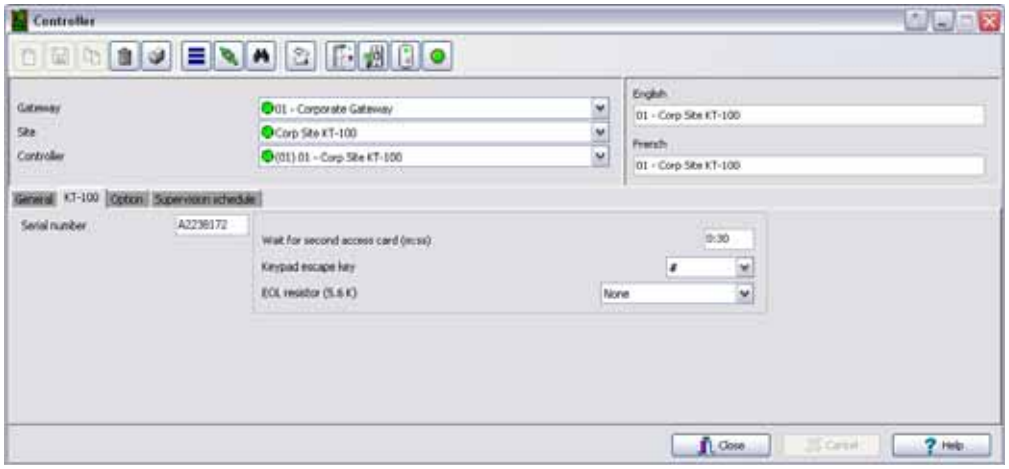
- Выбрать наиболее удобные расписания в разделе **Schedules** для нового контроллера:
  - Для контроллеров KT-100 или KT-300 доступен только список **Power supervision schedule** (Расписание контроля подачи питания).
  - Для контроллеров KT-200 или KT-400 доступно два списка **Power supervision schedule** (Расписание контроля подачи питания) и **Tamper switch supervision schedule** (Расписание контроля работы тампера).

6 Нажать кнопку **Save** (Сохранить).

Настройка контроллера KT-100

После того как общие параметры настроены, появляется закладка **Controller type** (Тип контроллера) для выбора типа контроллера.

1 В окне **Controller** (Контроллер) перейти к закладке **KT-100**..



2 В поле **Serial Number** ввести серийный номер контроллера. Как правило, серийный номер указан на шильдике контроллера. В этом поле должны быть указаны только цифры, за исключением первого символа, который может быть буквой a или A. Если первый символ указан строчной буквой, то система всё равно преобразует его в прописную букву.

3 Указать задержку **Wait for second access card** (Ожидать вторую карту доступа). Максимальное время задержки составляет 2 минуты 07 секунд. Эта функция используется в зонах повышенной

безопасности, где для получения доступа требуется предъявить две карты. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное значение.

4 IB выпадающем списке **Keypad escape key** (Клавиша ESC) указать, какая клавиша на кнопочной панели будет использоваться как ESC. Эта функция полезна при вводе PIN-кодов. Если пользователь ошибочно нажал не ту клавишу, он может нажать клавишу ESC и ввести PIN-код заново, при этом доступное число попыток останется прежним.

5 В выпадающем списке **EOL resistor (5.6K)** (оконечный резистор) выбрать, какой тип резистора используется в данной системе. По умолчанию установлено **None** (без резистора). Эта функция используется как устройство для мониторинга всех входов. Если эта опция активна, то в случае отсоединения входа система формирует тревожное сообщение и отправляет его на рабочий стол тревог (или на любой другой рабочий стол, настроенный на приём таких сообщений).

ПРИМЕЧАНИЕ: *Подробные сведения по настройке контроллеров KT-100 см. "Описание дополнительных функций контроллера" на стр. 129.*

Настройка контроллера KT-200

Каждый контроллер KT-200 может в режиме реального времени выполнять мониторинг статуса 16-ти точек входа, включая магнитные контакты, детекторы движения, датчики температуры и пр. К таким же входам могут быть подключены контактные датчики открытия дверей (отслеживающие состояние дверей) и кнопка запроса на выход REX (предупреждающие систему, что пользователь выходит из охраняемой зоны).

KT-200 оснащён двумя реле. Эти реле могут работать по разным расписаниям, описанным событиям или комбинации разных логических условий. Систему можно расширить до 16 реле с помощью релейных модулей REB-8. REB-8 используются как реле или как контроллеры лифтов. KT-2252 используются только в качестве контроллеров лифтов.

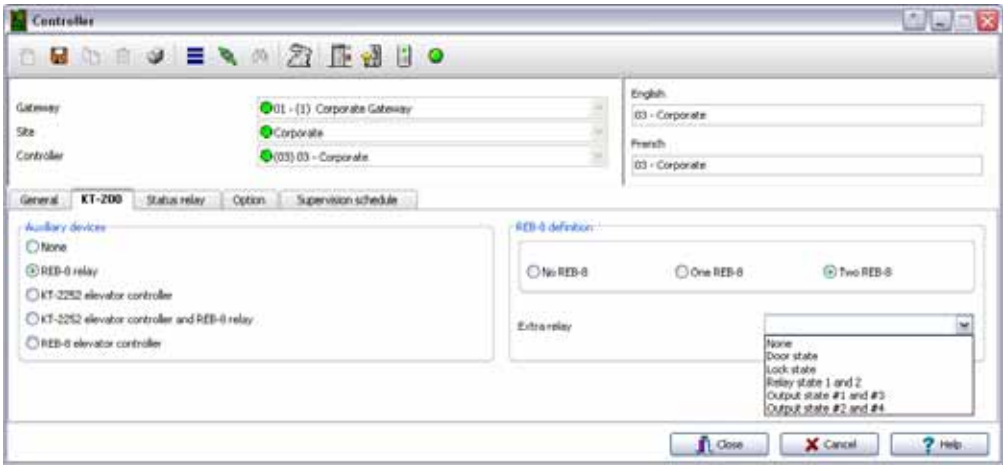
ПРИМЕЧАНИЕ: *Модель KT-2252 больше не выпускается.*

Назначение модулей расширения контроллеров KT-200

Контроллеры лифтов KT-2252 обеспечивают низковольтный интерфейс для контроля до 32 этажей. К одному контроллеру KT-200 можно подключить до 4 устройств KT-2252 для обслуживания до 64 этажей на одну лифтовую кабину. Кроме того, можно использовать один контроллер KT-2252 на 2 лифтовых кабины, по 16 этажей на каждую кабину (с одной общей кнопкой вызова для обеих кабин). При опускании идентификационной карты посетителя в считыватель, установленный в лифтовой кабине, контроллер KT-200 проверяет, на какие этажи открыт доступ этому посетителю, и посылает список разрешённых этажей в интерфейс KT-2252. KT-2252 замыкает электронные прерыватели, отвечающие за выбор этажей (копки выбора этажа).

Описание дополнительных устройств для контроллера KT-200

1 В окне назначения контроллера **Controller** открыть закладку **KT-200**.



2 В разделе **Auxiliary devices** (Дополнительные устройства) выбрать тип устройств, которые будут использоваться вместе с контроллером KT-200.

- Отметить флажком пункт **REB-8 relay** (Реле REB-8), если модули расширения REB-8 используются как реле. Всего может быть настроено только 16 реле. Если добавлено два модуля REB-8, то два последних реле (17-е и 18-е) можно использовать для выполнения различных действий. Дополнительные действия для этих двух реле следует выбрать в выпадающем списке **Extra relay** (Дополнительные реле).
- Check the **KT-2252 elevator controller and REB-8 relay** option if KT-2252 are used as elevator controllers and REB-8 are used as relays on the same door controller. A maximum of four KT-2252 can be connected to the controller.
- Отметить опцию **REB-8 Elevator Controller** (Контроллер лифта REB-8), если модули REB-8 используются для управления лифтами. Для этой цели можно использовать максимум четыре REB-8.

ПРИМЕЧАНИЕ: *Если в настройках отмечено использовать контроллер для управления лифтами, то за закладкой KT-200 появляется закладка Elevator (Лифт).*

В следующем разделе объясняется как настроить устройства управления лифтами при помощи модулей REB-8 и контроллеров лифтов KT-2252.

Настройка контроллеров лифтов KT-2252

Закладка **Elevator** (Лифты) служит для настройки и описания дополнительных устройств, используемых с контроллером KT-200 для управления лифтами. В зависимости от установленной платы расширения и отмеченных флажком опций в окне Elevator отображается раздел **REB-8 Installed** или **KT-2252 Installed**.

1. В окне описания контроллера **Controller** открыть закладку **KT-200**.
2. В разделе **Auxiliary devices** (Дополнительные устройства) выделить пункт **KT-2252 elevator controller** (Контроллер лифтов KT-2252) или **KT-2252 elevator controller and REB-8 relay** (Контроллер лифтов KT-2252 и реле REB-8). После этого рядом с закладкой KT-200 появляется закладка **Elevator** (Лифт).
3. Открыть закладку **Elevator,** чтобы настроить контроллеры лифтов. Если используются контроллеры лифтов типа KT-2252, то в меню становится доступным раздел **Elevator mode** (Режим лифта).

4. В разделе **Elevator mode** следует отметить число этажей, обслуживаемых лифтом. Это число этажей, контролируемых устройством KT-2252.
   - Выбрать 16 этажей, если один контроллер KT-2252 используется для управления двумя кабинами, обслуживающими одни и те же этажи.
   - Выбрать 32 этажа, если на одну кабину используется один контроллер KT-2252.

ПРИМЕЧАНИЕ: *В колонке Inputs (Входы) указаны терминалы KT-2252. Если описание этажей уже выполнено (в меню* **Floor***), то в колонке* **Floors** *отображаются этажи, связанные с входами.*

5. В разделе **KT-2252 installed** указать число установленных контроллеров KT-2252. Эти опции суммируются. Если, например, отмечена опция KT-2252 #3, то опции KT-2252 #1 и 2 должны быть

тоже отмечены. Различные варианты применения контроллеров лифтов типа KT-2252 представлены ниже в таблице:

Число лифтовых кабин	Число этажей	Число контроллеров KT-2252
1	8	1
1	16	1
1	32	1
1	64	2
2	8	1
2	16	1
2	32	2
2	64	4

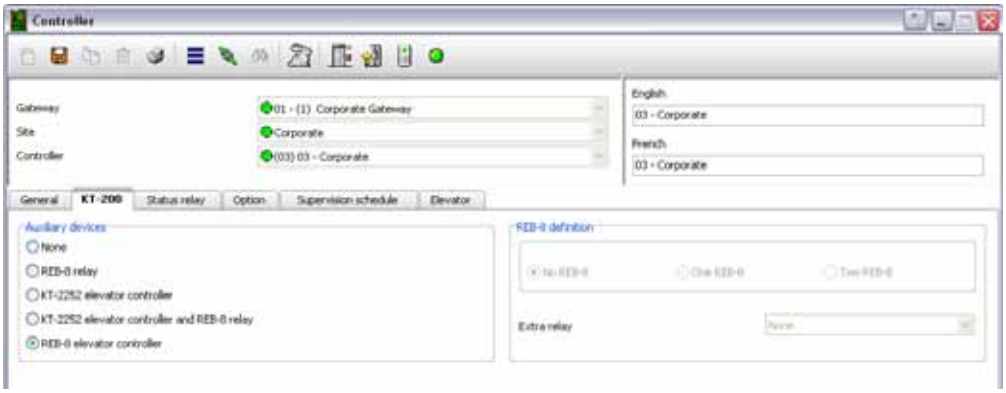
6 В колонке **Floors** (Этажи) указать число этажей, связанных с терминалами контроллера KT-2252.

ПРИМЕЧАНИЕ: *В колонке Inputs (Входы) указаны терминалы KT-2252. Если назначение этажей уже выполнено (в меню **Floor**), то в колонке Floors отображаются этажи, связанные с входами.*

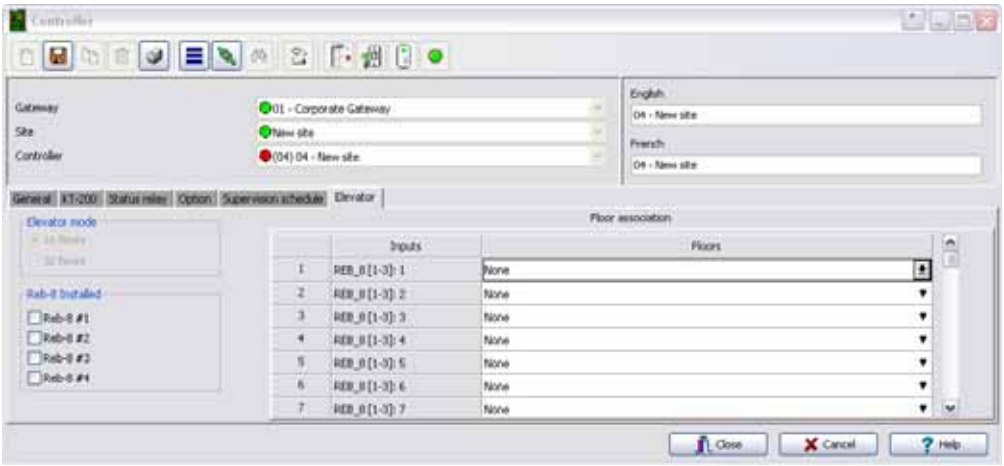
Программирование контроллеров лифтов REB-8

Релейные модули расширения REB-8 можно использовать в качестве бюджетного альтернативного устройства управления лифтами. При оснащении контроллера KT-200 модулем расширения REB-8 программа может управлять двумя лифтовыми кабинами на каждый контроллер.

1 В окне описания контроллера **KT-200** выделить опцию **REB-8 elevator controller** (Контроллер лифтов REB-8). После этого рядом с закладкой **KT-200** появляется закладка **Elevator** (Лифты). Раздел описания модуля REB-8 активен только при условии, что REB-8 используются в качестве реле.



2 Открыть закладку **Elevator (Лифт)**, чтобы настроить контроллеры лифтов REB-8. Система поддерживает до четырёх модулей REB-8.



3 Указать, сколько модулей REB-8 установлено на контроллере. Эти опции суммируются. Если, например, установлено четыре модуля REB-8, то первые три строки должны быть тоже отмечены флажком. Различные варианты применения модулей REB-8 представлены ниже в таблице: .

Число контроллеров REB-8	Число этажей	Число лифтовых кабин
1	1 до 8	Каб. 1
2	9 до 16	Каб. 1
3	1 до 8	Каб. 2
4	9 до 16	Каб. 2

ПРИМЕЧАНИЕ: *В колонке **Inputs** (Входы) указаны терминалы REB-8. Если назначение этажей уже выполнено (в меню **Floor**), то в колонке **Floors** отображаются этажи, связанные с входами.*

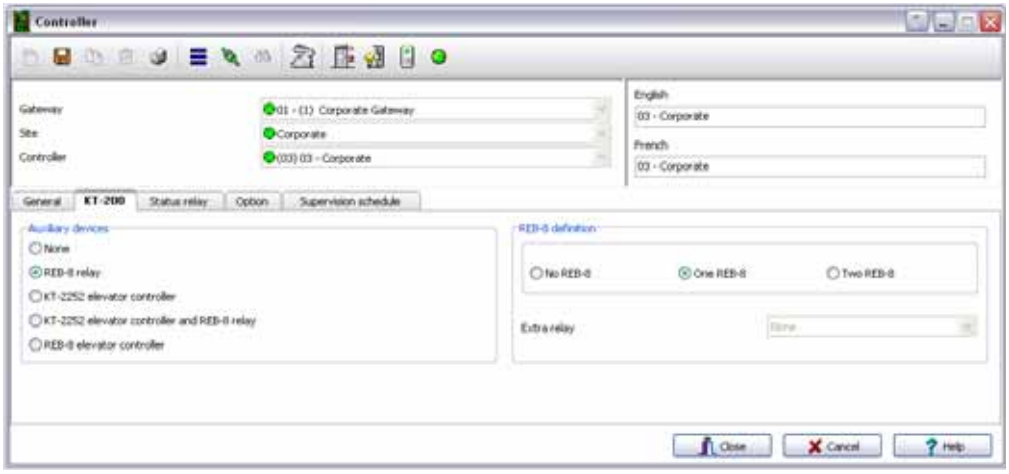
4 В колонке **Floors** (Этажи) указать число этажей, связанных с терминалами контроллера REB-8. Подробные сведения по назначению этажей и групп дверей*см. "Конфигурация дверей" на стр. 143*.

ПРИМЕЧАНИЕ: *Если модуль REB-8 используется в качестве контроллера лифтов, то функция подтверждения работы по этажам не выполняется.*

Описание модуля реле REB-8

Если модули REB-8 используются в качестве реле, необходимо указать, сколько модулей REB-8 установлено на контроллере KT-200. Один контроллер может обслуживать до 16 доступных реле и уже оснащён двумя встроенными реле.

1 Открыть закладку **KT-200** и выделить опцию **REB-8 relay** (Реле REB-8), чтобы назначить эти модули в качестве реле.



2 При использовании вместе с контроллером лифтов KT-2252 следует выделить опцию **KT-2252 elevator controller and REB8 relay** (Контроллер лифтов KT-2252 и реле REB8). В обоих случаях появляется окно назначения **REB-8 definition**.

3 В разделе **REB-8 Definition** выбрать нужную опцию: No REB-8 (Без модулей REB-8), One REB-8 (Один модуль REB-8) или Two REB-8 (Два модуля REB-8).

4 Если добавлено два модуля REB-8 (с общим числом реле 18), то последние два реле можно использовать для выполнения различных действий, которые необходимо указать в выпадающем списке в поле **Extra relay** (Дополнительные реле).

ПРИМЕЧАНИЕ: *Для получения дополнительных деталей по настройке других опций на контроллере \KT-200, см. "Описание дополнительных функций контроллера" на стр. 129.*

5 Открыть закладку **Status relay** (состояние реле), чтобы запрограммировать реле (одно или группу) на срабатывание при возникновении определённого события:

- Power failure – сбой питания
- Battery trouble – разряжен аккумулятор
- Tamper in alarm – противовзломное реле в состоянии тревоги
- Buffer 70% full – буфер памяти заполнен на 70%
- Lock power trouble – сбой питания замка
- Slave controller communication failure – обрыв связи с ведомым контроллером

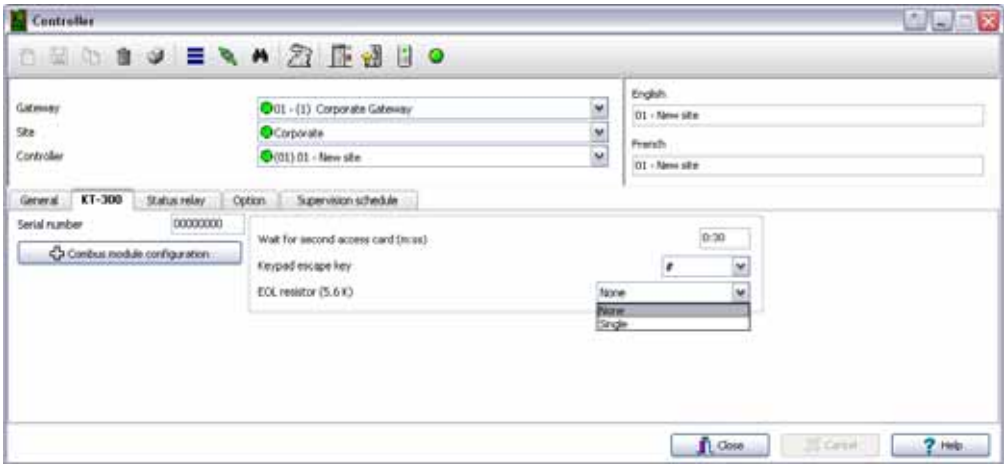
ПРИМЕЧАНИЕ: *Для получения дополнительной информации по назначению опций для контроллера на KT-200, см. "Описание дополнительных функций контроллера" на стр. 129.*

Настройка контроллера KT-300

KT-300 постоянно отслеживает состояние аккумуляторного модуля питания и сообщает о низком заряде / отсутствии аккумуляторной батареи. Кроме того, этот контроллер следит за короткими замыканиями и обрывами в цепях запирающих устройств для своевременного обнаружения неисправностей замков.

Контроллеры KT-300 совместимы с модулями Combus. Combus представляет собой 4-жильный шинный кабель, который служит для параллельного подключения нескольких модулей расширения, позволяющих добавлять входы, выходы, реле и ЖК-панели для отображения даты и времени.

1 В меню **Site** (Луч) нажать иконку **Controller** (Контроллер), выбрать закладку **KT-300**.



2 В поле **Serial Number** ввести серийный номер контроллера. Как правило, серийный номер указан на шильдике контроллера. В этом поле должны быть указаны только цифры, за исключением первого символа, который может быть буквой a или A. Если первый символ указан строчной буквой, то система всё равно преобразует его в прописную букву.

3 Указать задержку **Wait for second access card** (Ожидать вторую карту доступа). Максимальное время задержки составляет 2 минуты 07 секунд. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное значение. Эта функция используется в зонах повышенной безопасности, где для получения доступа требуется предъявить две карты.

4 В выпадающем списке **Keypad escape key** (Клавиша ESC) указать, какая клавиша на кнопочной панели будет использоваться как ESC. Эта функция связана с вводом PIN-кодов. Если пользователь ошибочно нажал не ту клавишу, он может нажать клавишу ESC и ввести PIN-код заново, при этом доступное число попыток останется прежним.

5 В выпадающем списке **EOL resistor (5.6K)** (оконечный резистор) выбрать, какой тип резистора используется в данной системе. По умолчанию установлено **None** (без резистора). Эта функция используется как устройство для мониторинга всех входов. Если эта опция активна, то в случае отсоединения входа система формирует тревожное сообщение и отправляет его на рабочий стол тревог (или на любой другой рабочий стол, настроенный на приём таких сообщений).

Настройка модулей расширения по шине Combus для KT-300

К контроллеру a KT-300 можно подсоединить пять различных модулей Combus:

- KT-PC4108 (8-зонный входной модуль расширения). Имеет вход тампер (tamper contact).
- KT-PC4116 (16-зонный входной модуль расширения). Имеет вход тампер (tamper contact).
- KT-PC4204 (4-релейный модуль расширения/требующий внешнего питания 16VA). Имеет вход тампер (tamper contact) и, также, встроенный блок питания на 12 В пост., 1 А.
- KT-PC4216 (16-зонный выходной модуль расширения). Используется для управления лифтами. Несмотря на это, может потребоваться дополнительное оборудование).
- KT-LCD3 (32-символьный ЖК-дисплей Kantech). Отображается *зелёным* (норма), *красным* (сбой в подаче питания) или *жёлтым* (неисправность).

1 Если на контроллер KT-300 установлен один из дополнительных модулей Combus, следует нажать кнопку **Combus module configuration** (Конфигурация модуля Combus). Ненастроенные

терминалы Combus обозначаются красными флажками/метками. После настройки модуля флажок становится зелёным

2 Чтобы настроить модуль, следует выделить его и нажать кнопку **Define (Назначить)** (в нижней части экрана). На экране появляется сообщение **Enter Combus module serial number** (Введите серийный номер модуля Combus).

3 Указать серийный номер модуля и нажать **OK**.

ПРИМЕЧАНИЕ: *Для получения этого номера необходимо активировать тампер контакт (Tamper switch) или нажать любую клавишу на кнопочной панели. Серийный номер модуля Combus будет выведен в виде сообщения на рабочий стол.*

4 Назначить имена модулей в соответствующих полях для каждого применяемого языка.

5 Отметить опции, связанные с настраиваемым модулем (если они отображаются в этом окне).

ПРИМЕЧАНИЕ: *В зависимости от того, какой модуль Combus выбран для настройки, пользователю будут представлены разные варианты его назначения. Например, при установке KT3-LCD и отметке флажками опций* ***Combus low power*** *(Низкое питание линии Combus) и* ***Display date and time*** *(Отображение даты и времени) контроллер KT-300 будет сообщать о недостаточном питании линии Cambus, а также отображать дату и время на KT3-LCD.*

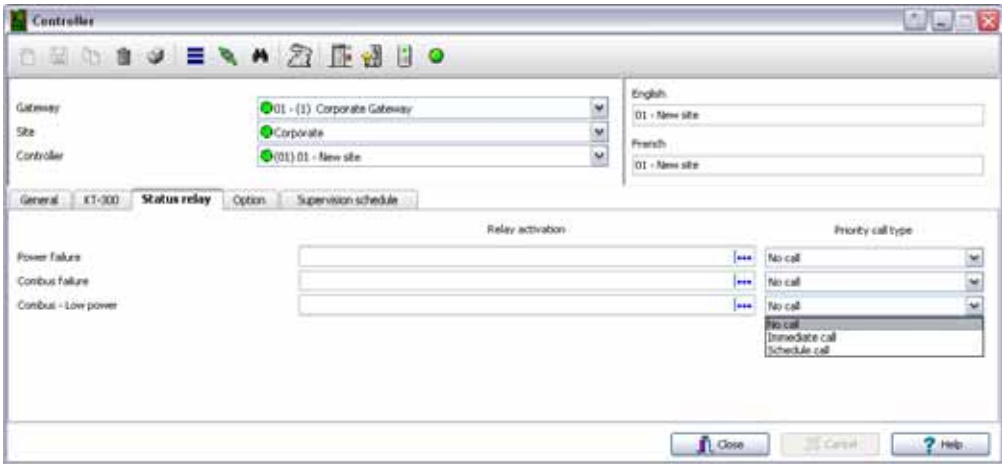
Ниже в таблице представлены функции, доступные для каждого модуля:

Тип модуля Combus	Функции	Дополнительные функции
KT3-LCD	Низкое питание линии Combus, отображение даты и времени	Нет дополнительных функций
KT-PC4108	Тревога по тамперу, Низкое питание линии Combus	модуль на 8 входов
KT-PC4116	Тревога по тамперу, Низкое питание линии Combus	модуль на 16 входов
KT-PC4204	Тревога по тамперу, Низкое питание линии Combus, разряженные аккумуляторы, сбой в подаче питания, низкая выходная нагрузка	Используется как реле (1-4)
KT-PC4216	Тревога по тамперу, Низкое питание линии Combus	Используется в качестве выходов типа открытый колллектор

6 Отметить флажком опцию **Combus low power** (низкое питание линии Cambus), чтобы контроллер KT-300 сообщал о низком питании линии Cambus.

7 Выделить опцию **Display date and time** (Показывать дату и время), чтобы на ЖК-экране KT3-LCD отображались дата и время.

8 После завершения настройки модуля Combus следует нажать **Ok** чтобы вернуться в раздел KT-300 status relay (состояние реле).



9 Назначьте локальную активацию реле, срабатывающие в ответ на сбой питания (**Power failure**), неисправность модуля Combus (**Combus failure**) и низкое питание в линии Cambus (**Combus low power**) (Corporate Шлюз только). Чтобы назначить определённое реле, следует нажать кнопку с многоточием и выбрать реле (одно или группу).

ПРИМЕЧАНИЕ: *Чтобы настроить активацию локального реле, следует настроить реле в разделе (**Devices** > **Relays**), и затем выделить локальные реле.*

10 В разделе **Priority call type** (Тип приоритетного вызова) указать тип вызова, который больше всего подходит для сообщения о сбоях и неисправностях (Corporate Шлюз только). Чтобы опция **Priority call type** стала доступной, в поле Site connection type (Тип соединения луча) должен быть указан Modem (Модем).

ПРИМЕЧАНИЕ: *Более подробная информация по назначению опций для контроллера KT-300, см. "Описание дополнительных функций контроллера" на стр. 129.*

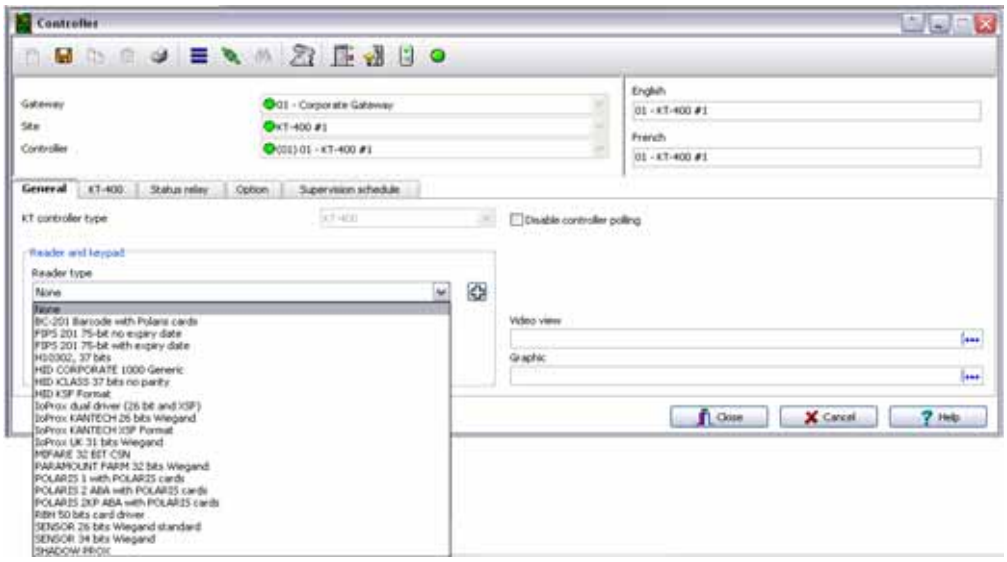
ПРИМЕЧАНИЕ: *Для большей информации, см. "Настройка лучей (loops)" на стр. 102.*

Настройка конфигурации 4-дверного Ethernet-контроллера KT-400

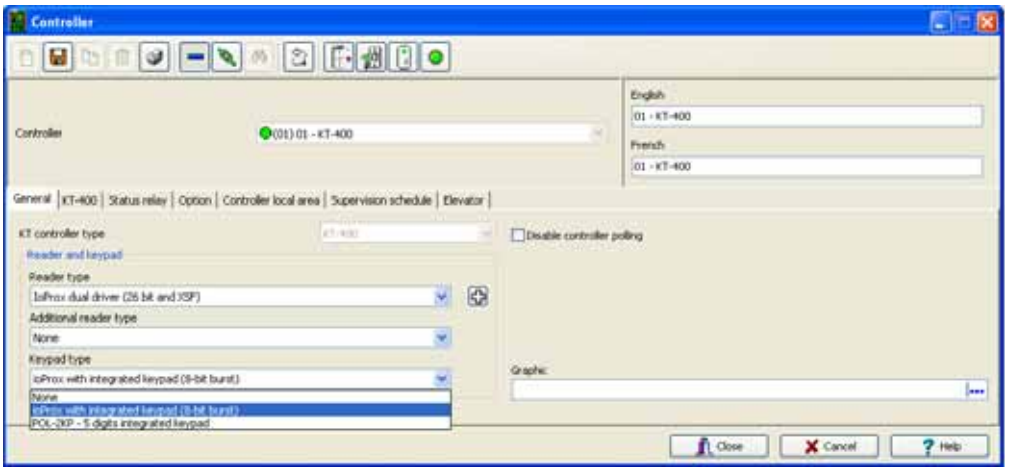
Контроллер KT-400 постоянно отслеживает статус сетевого питания переменного тока и состояние аккумулятора и передаёт в систему EntraPass сообщения: “AC Power Failure” (Сбой подачи питания переменного тока), “Normal Battery” (Аккумулятор в норме), “Low Battery” (Низкий заряд аккумулятора), “Battery Critical” (Аккумулятор в критическом состоянии), “No Battery” (Без аккумулятора) или “Battery Brown Out” (Аккумулятор неисправен). Выходы питания имеют электронную защиту от коротких замыканий и бросков напряжения. Цепи для замков также оснащены системой защиты от коротких замыканий и от разрыва цепи.

ПРИМЕЧАНИЕ: *Чтобы получить наиболее полные сведения о 4-дверном Ethernet-контроллере KT-400, следует обратиться к соответствующему руководству по установке (DN1726).*

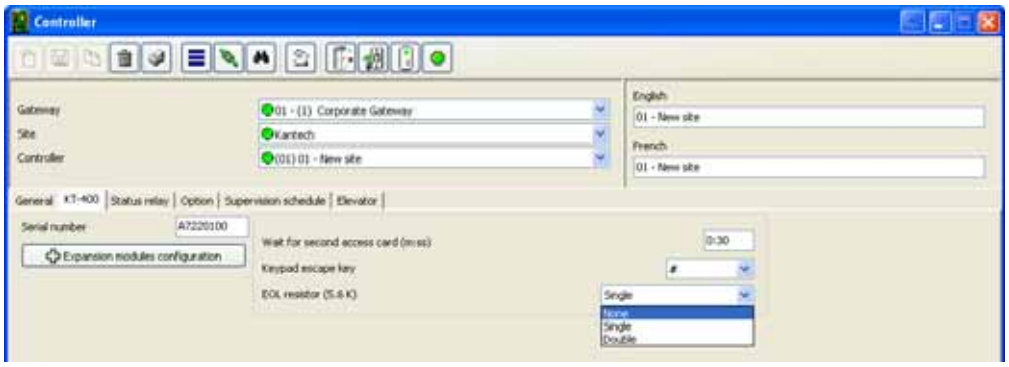
1 В меню **Devices** (Устройства) > **Controller** (Контроллер) открыть закладку **General** (Общие параметры) и выбрать тип считывателя в поле **Reader type(s)**.



2 Указать тип кнопочной панели в поле **Keypad type** (при её наличии).



3 Открыть закладку **KT-400.** В поле **Serial Number** ввести серийный номер контроллера. Этот номер указан на шильдике контроллера рядом с кнопкой восстановления (reset). В этом поле должны быть указаны только цифры, за исключением первого символа, который может быть буквой a или A. Если первый символ указан строчной буквой, то система всё равно преобразует его в прописную букву.



4 Указать задержку **Wait for second access card** (Ожидать вторую карту доступа). Максимальное время задержки составляет 2 минуты 7 секунд. При вводе значения, превышающего максимально допустимую величину, система будет использовать предыдущее правильное

значение. Эта функция используется в зонах повышенной безопасности, где для получения доступа требуется предъявить две карты.

5 В выпадающем списке **Keypad escape key** (Клавиша ESC) указать, какая клавиша на кнопочной панели будет использоваться как ESC. Эта функция связана с вводом PIN-кодов. Если пользователь ошибочно нажал не ту клавишу, он может нажать клавишу ESC и ввести PIN-код заново, при этом доступное число попыток останется прежним.

6 В выпадающем списке **EOL Resistor (5.6 K)** выделить тип резистора. По умолчанию установлено **Single resistor** (Один резистор). В случае возникновения длинного звукового сигнала на считывателе/кнопочной панели, следует проверить число резисторов, установленных в системе.

Настройка модулей расширения к контроллеру KT-400

Контроллер KT-400 поддерживает модули расширения, которые подключаются к расширительному порту SPI. Порт SPI представляет собой 6-жильный шинный кабель для подключения модулей расширения типа входов, выходов и реле по принципу последовательного соединения.

Warning: *Порт SPI контроллера KT-400 допускает максимальный ток 500 мА при условии неиспользования терминалов AUX (12 В). Если суммарный ток превышает 500 мА, следует подключать модули расширения к дополнительному блоку питания (12 В пост., 2 А). Более подробные сведения смотрите в руководстве по установке 4-дверного Ethernet-контроллера KT-400 (DN1726).*

Доступны три модуля расширения:

- **KT-MOD-INP16**: модуль расширения входов. Позволяет добавить 240 зон на один контроллер KT-400. К одному устройству KT-400 может быть подключено до 15 входных модулей (16 входных модулей используется в схеме управления лифтом), то есть общее число внешних входов может достигать 240. С учётом 16 входов, имеющихся на плате контроллера, их общее число достигает 256 входов на один контроллер KT-400. Подробные сведения изложены *в брошюре по установке* KT-MOD-INP16 (DN1776).
- **KT-MOD-OUT16:** модуль расширения на 16 выходов. Используется для управления лифтами с применением другого дополнительного оборудования. К контроллеру KT-400 можно подсоединить до 16 выходных модулей, то есть общее число выходов может достигать 256. Подробные сведения изложены в брошюре по установке KT-MOD-OUT16 (DN1781).
- **KT-MOD-REL8:** релейный модуль расширения на 8 выходов, используемых как реле общего назначения или для управления лифтами. К контроллеру KT-400 можно подсоединить до 32 релейных модулей, то есть общее число реле может достигать 256. Подробные сведения изложены в брошюре по установке KT-MOD-REL8 (DN1786).

Ниже в таблице представлены функции, доступные для каждого модуля::

Модуль расширения	Функции
KT-MOD-INP16	Входы контроллера (до 256) и/или входы лифта (до 64 на одну дверь лифта)
KT-MOD-OUT16	Выходные реле (до 256) и/или выходы лифта (до 64 на одну дверь лифта)
KT-MOD-REL8 (***Note***)	Реле (до 256) и/или выходы лифта (до 64 на одну дверь лифта)

ПРИМЕЧАНИЕ: *К настоящему моменту контроллеры KT-400 выпускаются с 4 реле. Рекомендуется заранее рассчитать, сколько реле потребуется, чтобы часть из них не оказались лишними (если только они не запланированы в качестве резервных).*

ПРИМЕЧАНИЕ: *Конфигурация реле 9-16 установлена по умолчанию.*

1 Если на контроллер KT-400 установлен(ы) модуль(и) расширения, следует нажать кнопку **Expansion module configuration** (Конфигурация модуля расширения). При этом открывается окно настройки модулей расширения **Expansion modules setup**. .

Если необходимо	то следует перейти к:
настроить входной модуль KT-MOD-INP16	**пункт 2**.
настроить выходной модуль KT-MOD-OUT16	**пункт 5**.
настроить релейный модуль KT-MOD-REL8	**пункт 6**.
изменить конфигурацию уже установленного модуля расширения	**пункт 7**.

2 Чтобы добавить модуль KT-MOD-INP16, следует открыть закладку **Input Module** (входной модуль) и нажать кнопку **Add**. Если в списке найдено более одного входного модуля, то необходимо тщательно проверить, что вы выбрали правильный модуль, который будет подвергнут изменениям. Назначить имена модулей в соответствующих полях для каждого применяемого языка и выделить необходимые опции.

3 Выберите **DEOL: Double end-of-line resistor JP4 On** (Двойной оконечный резистор), чтобы назначить DEQL на модуле KT-MOD-INP16.

ПРИМЕЧАНИЕ: *Целая плата расширения использована для обеспечения 8 входов с DEOL. Эти 8 входов добавлены в следующую группу на 8 входов. Например, если входа № 33-40 имеют режим DEOL, то входа № 33-40 и № 41-48 не будут доступны для других модулей. Эти номера будут уже заняты. При подключении новых модулей вам будет необходимо присваивать другие номера.*

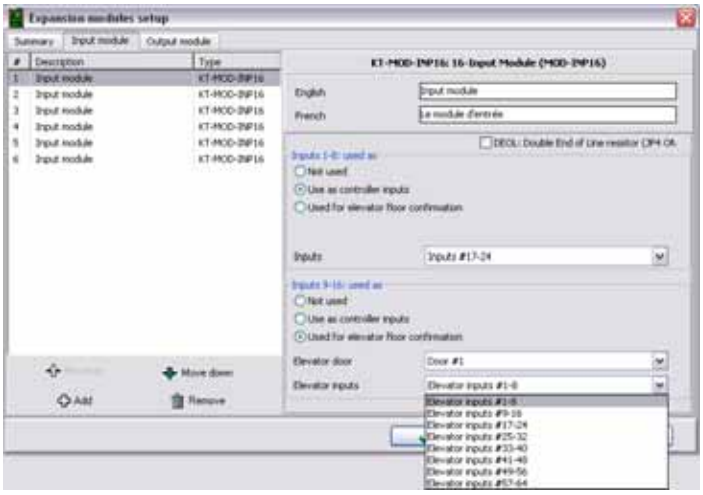
ПРИМЕЧАНИЕ: *Входы контроллера 1-16 зарезервированы для входов на KT-400.*

Пример с входами 1-8, которые назначены как input контроллера

4 Для выбора номеров входов можно использовать два способа: выпадающий список меню и окно расширенного режима поиска **Extended selection box**. Чтобы загрузить окно **Extended selection**

box, следует щёлкнуть на изображении правой кнопкой мыши. Более подробная информация см. "Окно расширенного режима поиска (Extended Selection Box)" на стр. 54.

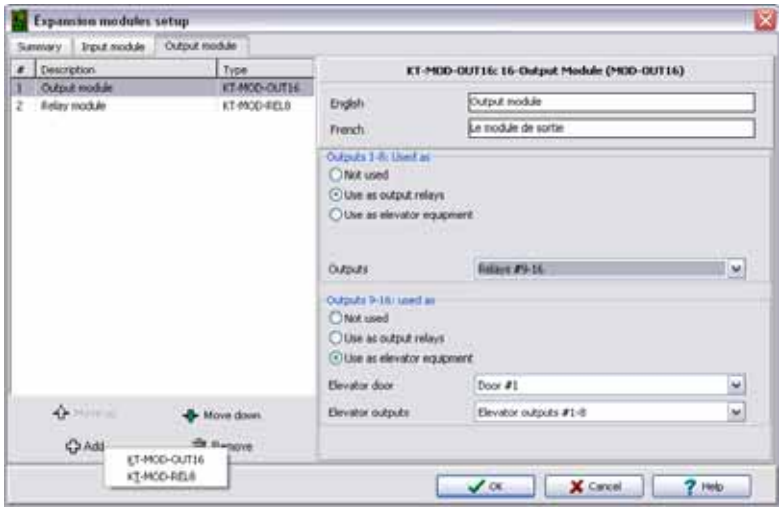
Пример назначения входов 9-16 в качестве входов лифта (Elevator Inputs)



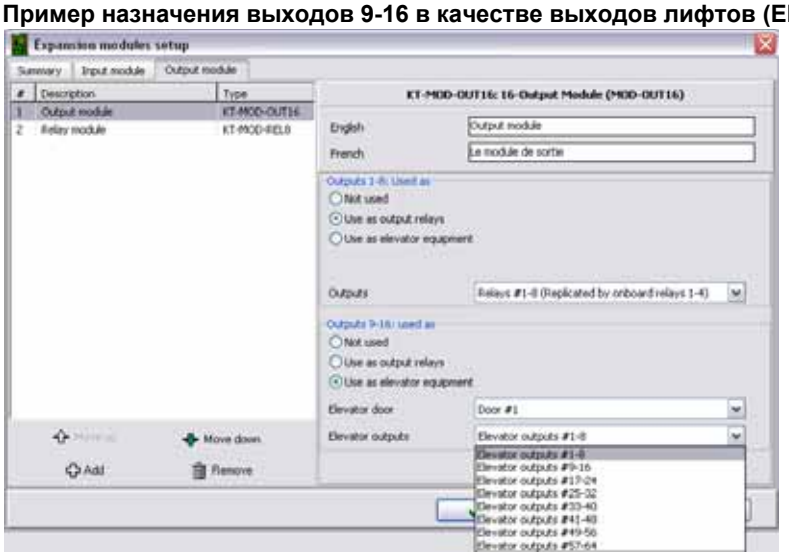
ПРИМЕЧАНИЕ: *Эти списки взаимоисключают друг друга. Нельзя выбрать один и тот же вход в меню* ***Inputs*** *и в меню* ***Elevator inputs****, так как получится дублирование, которое система не поддерживает. Например, входы 17-24 (****Inputs # 17-24****) нельзя выбрать дважды. С другой стороны, эта концепция станет понятнее, если принять во внимание тот факт, что в меню* ***Elevator inputs*** *тот же пункт из списка не будет доступен для одной и той же двери. Такая же концепция применяется и для меню* ***Elevator outputs*** *(Выходы лифтов).*

5 Чтобы добавить модуль KT-MOD-OUT16, выберите закладку **Output Module** (Выходной модуль) и нажать кнопку **Add** (Добавить). После этого на экране открывается новое меню, в котором можно выбрать, какой выходной модуль добавить. Назначить имена модулей в соответствующих полях для каждого применяемого языка и выделить необходимые опции.

Пример назначения выходов 1-8 в качестве выходных реле (Output Relays)

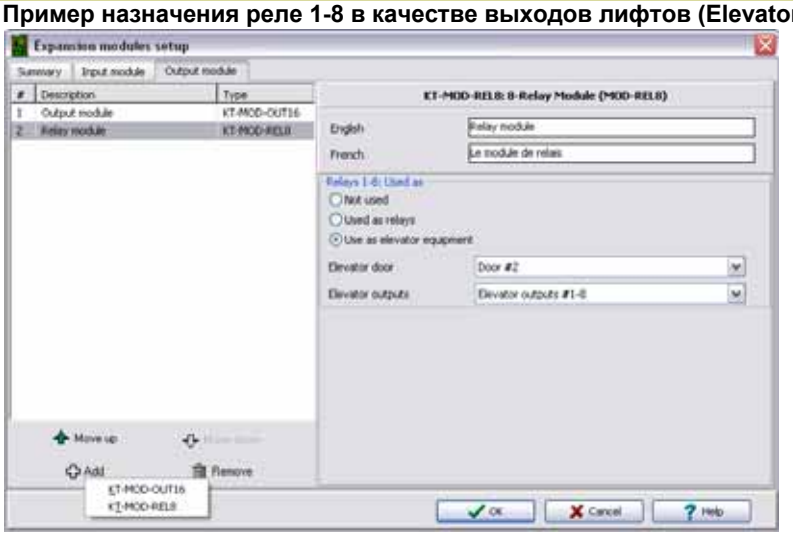


Пример назначения выходов 9-16 в качестве выходов лифтов (Elevator Outputs)

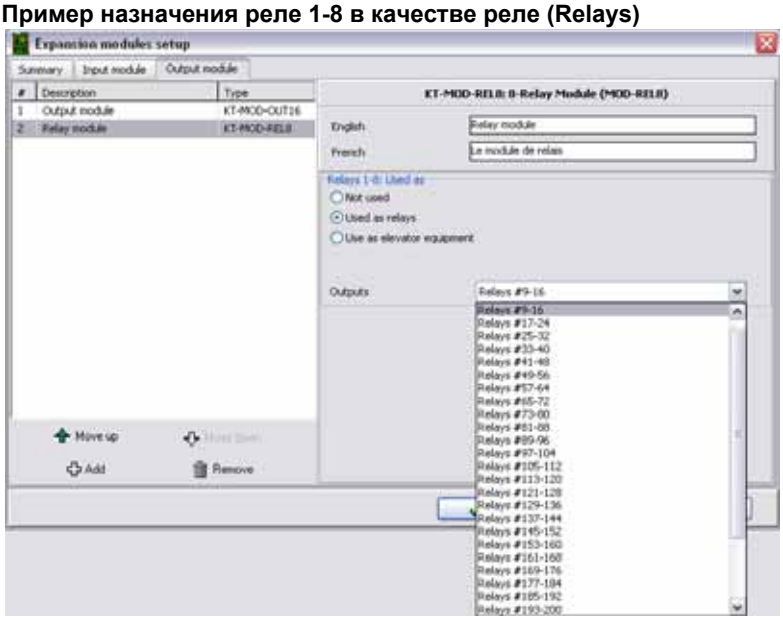


6 Чтобы добавить модуль KT-MOD-REL8, необходимо выбрать закладку **Output Module** (Выходной модуль) и нажать кнопку **Add** (Добавить). После этого на экране открывается новое меню, в котором можно выбрать, какой выходной модуль добавить. Назначить имена модулей в соответствующих полях для каждого применяемого языка и выделить необходимые опции.

Пример назначения реле 1-8 в качестве выходов лифтов (Elevator Outputs)



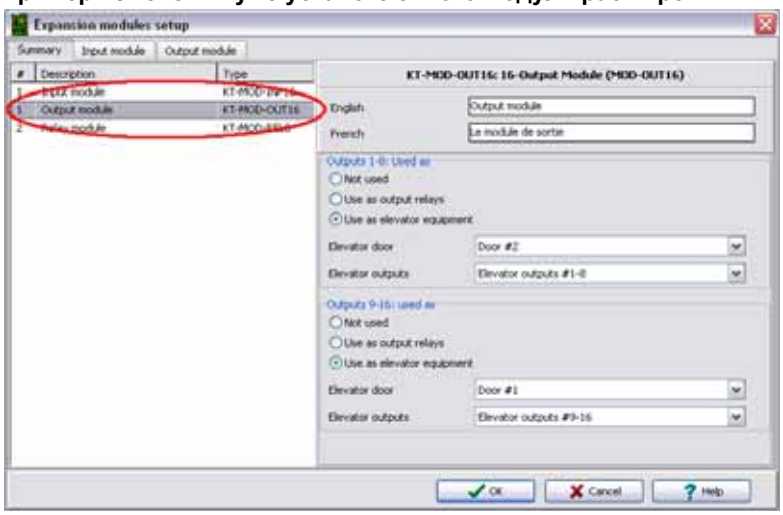
Пример назначения реле 1-8 в качестве реле (Relays)



ВНИМАНИЕ! К настоящему моменту контроллеры KT-400 выпускаются с 4 реле. Рекомендуется заранее рассчитать, сколько реле потребуется, чтобы часть из них не оказались лишними (если только они не запланированы в качестве резервных).

7 Открыть закладку **Summary** (Общее), которая позволяет изменять любые параметры модулей. Выделить модуль, который необходимо изменить, в левой колонке и изменить его параметры в правой части окна.

Пример изменения уже установленного модуля расширения

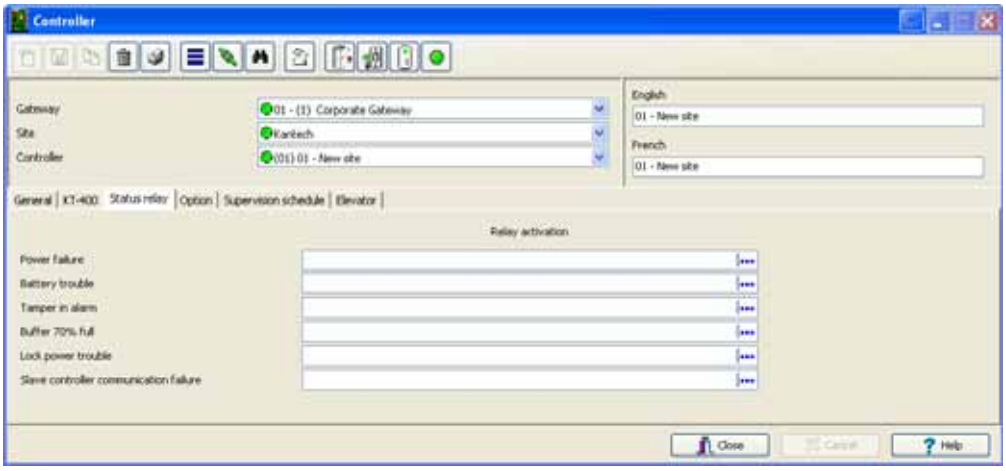


8 После окончания настройки модулей расширения нажать кнопку **OK** для возврата в меню настройки KT-400.

ПРИМЕЧАНИЕ: *За более подробной информацией, см. "Настройка лучей (loops)" на стр. 102.*

Настройка активации реле по состоянию (только для шлюза Corporate)

1 Открыть закладку **Status relay** (состояние реле), чтобы запрограммировать реле (одно или группу) на срабатывание при возникновении определённого события.
- Power failure – сбой питания
- Battery trouble – разряжен аккумулятор
- Tamper in alarm – противовзломное реле в состоянии тревоги
- Buffer 70% full – буфер памяти заполнен на 70%
- Lock power trouble – сбой питания замка
- Slave controller communication failure – обрыв связи с ведомым контроллером



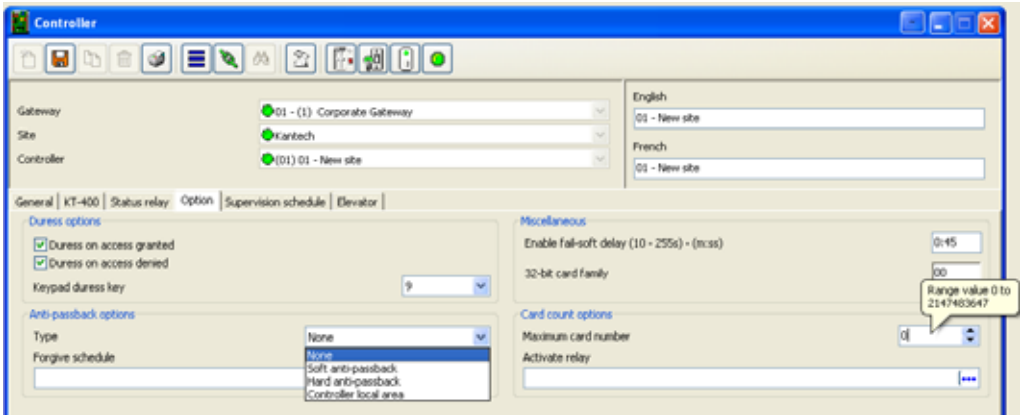
Описание дополнительных функций контроллера

Под закладкой **Option** (Опции) находятся следующие функции контроллера:
- Anti-passback – запрет повторного прохода (для синхронизации считывателей входа/выхода)
- Duress function – функция "принуждение" (для использования для назначения тревожной кнопки)

- Card count options – функции подсчета идентификационных карт (для учёта карт в определённой зоне) и др.

ПРИМЕЧАНИЕ: *Функция запрета повторного прохода используется со считывателями входа/выхода. Она помогает администраторам службы безопасности отслеживать число владельцев карт в определённой зоне. Эта функция действует локально для каждого контроллера, в зависимости от установленных считывателей входа/выхода. Реле может срабатывать, когда счётчик зарегистрирует указанное число карт в обслуживаемой зоне, восстановление реле будет происходить после того, как число карт в этой зоне опустится ниже указанной величины.*

1 В окне **Controller** (Контроллер) открыть закладку **Option** (Опции) и настроить функции Anti-passback (Запрет повторного прохода), Duress (Принуждение) и Card count (Счётчики карт).



2 Выбрать опции для функции "Принуждение" (**Duress options**). В случае использования функции "Принуждение" следует назначить клавишу, которая будет выполнять роль кнопки паники (тихая тревога).
   - **Duress on access granted** (Принуждение, доступ разрешён) – при использовании кода принуждения, доступ будет разрешён.
   - **Duress on access granted** (Принуждение, доступ запрещён) – при использовании кода принуждения, доступ будет запрещён.

3 Выбрать в выпадающем списке **Keypad duress key**, какая клавиша будет использоваться в качестве кнопки паники.

ПРИМЕЧАНИЕ: *Для дополнительного повышения безопасности в этом меню можно выделить обе опции. Кнопка паники доступна на обоих Шлюзах Corporate и Global. Функция запрета повторного прохода доступна только для конфигурации Corporate Gateway.*

4 Функция **Anti-passback options** (Опции запрета повторного прохода) только для конфигурации Corporate Gateway. В этом разделе следует выбрать тип запрета в выпадающем списке **Type** (Тип). Функция Anti-passback может работать таким образом, что использовать карту для выхода через какую-либо дверь можно будет только в том случае, если она была предъявлена для входа через эту же дверь.
   - **None** – не использовать функцию Anti-passback.
   - **Soft anti-passback** (Мягкий запрет повторного прохода) – владелец карты может воспользоваться считывателем карт на входе/выходе более одного раза, не пользуясь соответствующим считывателем до этого на выходе/входе. При этом на АРМ (рабочий стол сообщений) будет отправлено сообщение **"Access granted - Passback bad location"** (Доступ разрешён – повторный проход не в том месте).
   - **Hard anti-passback** (Жёсткий запрет повторного прохода) – карту нельзя будет использовать для повторного входа через один и тот же считыватель на входе, пока она не будет предъявлена для выхода через соответствующий считыватель на выходе. При этом на рабочий стол сообщений будет отправлено только сообщение **"Access denied - Passback bad location"** (Доступ запрещён – повторный проход не в том месте).
   - **Controller local area** (Локальная зона контроля) – при выборе этой опции появляется новая закладка **Controller local area**. Эта функция применяется только для контроллеров типа KT-400; закладка **Controller Local Area** появляется только в том случае, если используется контроллер KT-400.

5 В разделе **Forgive schedule** (Расписание сброса нарушений) нажать кнопку с многоточием, чтобы настроить расписание сброса функции запрета повторного прохода на всех остальных картах. Указать время, когда когда антипасбек не будет работать.

ПРИМЕЧАНИЕ: *Раздел* ***Forgive Schedule*** *доступен только при условии выделения одного из пунктов: Soft anti-passback или Hard anti-passback.*

6 В разделе **Miscellaneous** (Прочее) указать задержку в поле **Enable fail-soft delay, 10-255 s** (Разрешить задержку при пропадании связи, по истечении которой контроллер будет переведен в автономный режим, 10-255 сек). В безопасном режиме контроллер работает автономно, когда пропадает связь с другими устройствами.

7 В поле **32-bit card family** (Семейство 32-битных карт) ввести код (опция). Этот шестнадцатеричный код указан на идентификационной карте.

8 В разделе **Card count options** (Опции счётчика карт) выбрать максимальное число карт (Maximum card number) стрелками вверх-вниз. Максимально допустимое значение для параметра "**maximum card number**" – 2 147 483 647. Система отслеживает число контролируемых карт на контролируемой территории и активирует реле по достижении указанного числа. Когда пользователи покидают контролируемую территорию, счётчик уменьшает значение, и реле в конечном счёте восстанавливается, как только значение счётчика становится меньше, чем указанное значение.

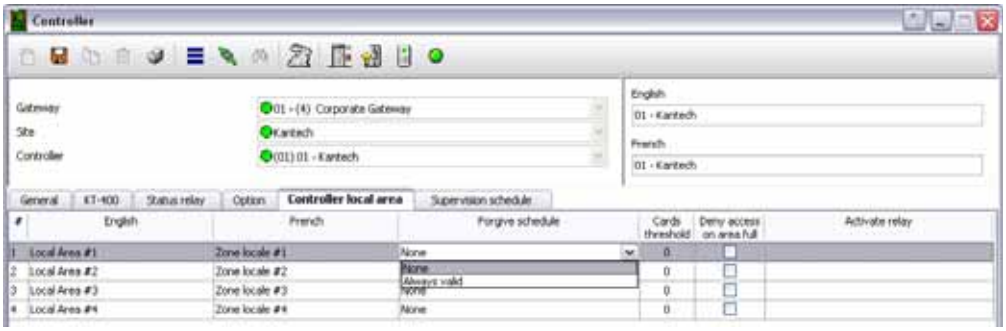
9 Систему можно настроить таким образом, что при достижении максимально допустимого числа карт будет срабатывать одно реле (**Activate a single relay**) или группа (**Group of relays**). Чтобы выбрать одно или группу реле, следует нажать кнопку с многоточием.

ПРИМЕЧАНИЕ: *Раздел* **Activate relay** *доступен только при условии выделения одного из пунктов: Soft anti-passback (Мягкий запрет повторного прохода) или Hard anti-passback (Жёсткий запрет повторного прохода).*

Назначение локальных областей для контроллера KT-400

ПРИМЕЧАНИЕ: *Функция* ***Controller local area*** *(локальная область контроллера) доступна только в конфигурации KT-400 на Corporate шлюзе. См. предыдущую секцию вкладку* **Controller local area** (локальная область контроллера).

1 В окне **Controller** (Контроллер) открыть закладку **Controller local area** (Локальные зоны контроля), чтобы указать до 4 локальных зон.



2 Назначить имя для первой локальной зоны (на обоих языках).

3 В выпадающем списке **Forgive schedule** (Расписание сброса нарушений) выбрать нужное расписание.

4 Указать максимальное разрешённое число карт в поле **Cards threshold** (Пороговое число карт).

5 Поставить флажок напротив **Deny access on area full** (Запретить доступ в зону при переполнении), чтобы после достижении установленного порога по числу карт запретить доступ посетителей в контролируемую зону.

6 Нажав на кнопку с многоточием, выбрать одно или группу реле, которые должны срабатывать после достижения порогового значения по числу карт.

7 Повторить действия в **пп. 2 ... 6** для каждой локальной зоны контроля.

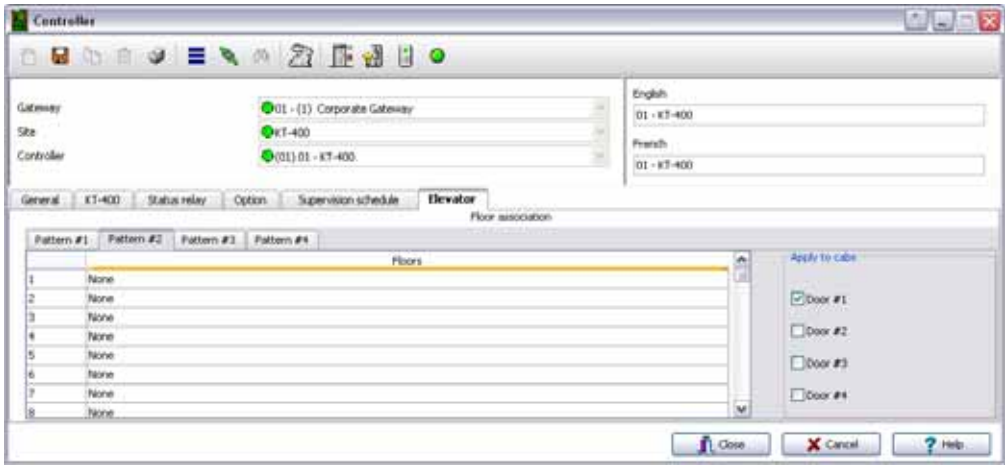
Назначение связей с этажами лифта для контроллера KT-400

ПРИМЕЧАНИЕ: *Закладка **Elevator** (Лифт) отображается только в том случае, когда в закладке **KT-400** модули расширения настроены как входы или выходы для лифтов. Для более подробной информации смотрите в Главе 4 Настройка модулей расширения к контроллеру KT-400 на стр. 124.*

Установление связей шаблонов (Pattern) с дверьми и номерами этажей

Только в контроллерах KT-400 предусмотрена возможность выбора четырёх шаблонов для настройки дверей и номеров этажей, которые будут привязаны к каждому шаблону. По умолчанию шаблон №1 описывает все номера дверей.

1 В окне **Controller** (Контроллер) открыть закладку **Elevator** (Лифты), чтобы назначить привязки по этажам.



2 В закладке **Elevator** нажать **Pattern #2**, и выделить флажком необходимые номера дверей (**Door**).

3 В выпадающем списке **Floors** (Этажи) выделить соответствующий пункт или номер этажа для привязки номера двери к номеру шаблона.

4 Повторить **пп. 2** и **3** для каждого шаблона.

5 Нажать **Save** (Сохранить).

Сообщения контроллера о переполнении буфера событий

Если контроллер не имеет связи с сервером, то сообщения контроллера заносятся в буфер памяти. После заполнения буфера старые сообщения переносятся во вспомогательный буфер (от 50 до 100 байт), в который всегда помещается 50 событий. После восстановления соединения с сервером система начинает отправлять сообщения на рабочий стол сообщений (показан на иллюстрации ниже), чтобы указать, что буфер заполнен и что сообщения удаляются из буфера.

- Удаление сообщений контроллер осуществляет в порядке их поступления. Таким образом, самое старое сообщение будет удалено в первую очередь.
- После того как связь с сервером восстановлена, все сообщения контроллера сразу отправляются в список сообщений на столе сообщений, в следующем порядке: сначала идут сообщения из вспомогательного буфера событий, затем одно сообщение "Event Buffer

Overflow" (Переполнение буфера событий), а за ним список событий, возникших во время отсутствия связи контроллера с сервером.

- В проиллюстрированном выше примере выделенное сообщение об ошибке “*Event buffer overflow*” является 50-м по счёту из самых старых событий контроллера, отправленных в список событий на АРМ.

Настройка Kantech Telephone Entry System (KTES)

Kantech™ Telephone Entry System (KTES) - это телефонная система, которая подходит для малых и больших приложений, где также требуется система контроля доступа или где вам необходимо иметь только телефонную систему. Данная система обеспечивает контроль визита посетителей на различных объектах: многоквартирный дом, офисные здания, фабрики, и промышленные объекты. Посетители используют KTES для прямой связи с жильцом при помощи встроенного телефона. Жилец может предоставить доступ или запретить доступ посетителя с обычного или сотового телефона.

Спроектированный как атономное устройство, система контролирует одну дверь, внешенее реле и поддерживает открытие двери почтальону. Для больших коммерческих инсталляций KTES интегрируется в систему EntraPass через Corporate Шлюз и с контроллерами KT для обеспечения полнофункциональной системы контроля доступа. Все настройки системы могут быть сделаны с приборной панели KTES или удаленно через ПК с помощью модема, Ethernet или RS-485.

Система передает все события прямо в систему EntraPass, где вы можете получить детализированный log событий. Дополнительно, программированные тревоги могут быть отправлены на бумагу и/или в систему EntraPass через встроенный модем. Для детальной информации на KTES, смотрите документ *KTES Installation Manual, DN1769* и *KTES Programming Manual, DN1770*.

Назначение общих параметров для KTES

1 Во вкладке **Devices** (Устройства), выберите иконку **KTES**.

ПРИМЕЧАНИЕ: *Вы должны выбрать Corporate шлюз, когда настраиваете KTES.*

ПРИМЕЧАНИЕ: *Как показано на картинке выше, использование* ***KTES Setup Wizard*** *(помощника установки) будет помогать вам настраивать Kantech Telephone Entry System (KTES) при помощи нескольких быстрах простых шагов. Более подробную информацию смотри в Главе 16 Системные утилиты на стр. 515.*

2 в окне KTES, выберите подходящий Шлюз чтобы отобразить луч контроллера, затем выберите луч/сайт(из выпадающего списка под **Site** (луч)) и укажите KTES, который вы хотите назначить. Новые пункты будут обозначены при помощи красных кнопок. Когда вы назначите новое устройство KTES, тогда пункт поменяет свое изображение на зеленый.

ПРИМЕЧАНИЕ: *Для большей информации см. "Настройка лучей (loops)" на стр. 102.*

3 В закладке **General** (общее), укажите **visitor call settings** (настройки звонка посетителя):

- **Talk time (Время разговора):** Это максимальная продолжительность времени разговора в секундах для нормальеного звонка между посетителем и жильцом (от 10 secs до 59 мин:59 сек). По умолчанию стоит 40 сек.
- **Extended talk time (Расширенное время разговора):** Это максимальное продолжительность разговра для расширенного звонка между посетителем и жильцом (от 10 сек. до 59 мин.:59 сек.). По умолчанию установлено 60 сек.
- **Talk time remaining warning** (предупреждение об окончании времени разговра): Система посылает предупреждающий сигнал (биип), определенной длительности для того чтобы предупредить о скором окончании разговора. Вы молжете изменять показатель (от 1 сек до 59 мин:59 сек). ПО умолчанию установлено 10 сек.
- **Number of rings before answer (количество гудков для ответа жильцом)**: Это максимальное количество гудков, которое дается жильцу для ответа. По истечении этого количество гудков будет дан отбой. Количество может изменяться (4 до 16). По умолчанию 5.
- **Extended number of rings before answer (расширенное количество гудков для ответа жильцом)**: Это максимальное количество гудков, которое дается жильцу для ответа при расширенном режиме. По истечении этого количество гудков будет дан отбой. Количество может изменяться (4 до 16). По умолчанию 10.

4 Укажите **Postal Lock options** (Опции замка для почтальона):

- **Postal lock contact (контакт почтового замка):** Это вход, который связан с открытием замка для почтальона (0 до 4). Выберите вход и нажмите OK:

ПРИМЕЧАНИЕ: *Для большей информации см. "Конфигурация входов (раздел Input)" на стр. 160.*

- **Postal lock Schedule (Расписание работы почтового замка)**: Это расписание внутри которого вход, который связан с замком для почтальона, генерирует верный запрос на вход для почтальона, когда данный вход находится в тревоге.

ПРИМЕЧАНИЕ: *Для большей информации смотрите в Главе 5* **Назначение расписаний** *на стр. 174.*

5 Опция **Disable KTES polling** (запрещение опроса KTES): выберите эту функцию когда вы хотите отключить KTES. В отулюяенном режиме, KTES не будет отвечать на запросы. По умолчанию это опция выбрана.

6 Укажите опции **Tenants list** (список жильцов):

- **Tenants list capacity** (максимально возможное количество жильцов): По умолчанию, количество установлено на 125 жильцов. Но вы можете приобрести дополнительную лицензию для расширения этого количества до 500, 1000 или 3000 жильцов.

ПРИМЕЧАНИЕ: *Помните, что вы ограничены этой опцией в самом программном обеспечении. Если вы зарегестрировали много опций на KTES для дополнительных расширений, то будьте уверены в назначении KTES на определенный луч/сайт.*

- **Tenants list** (список жильцов): Выберите tenants list (список жильцов). По умолчанию он пустой.

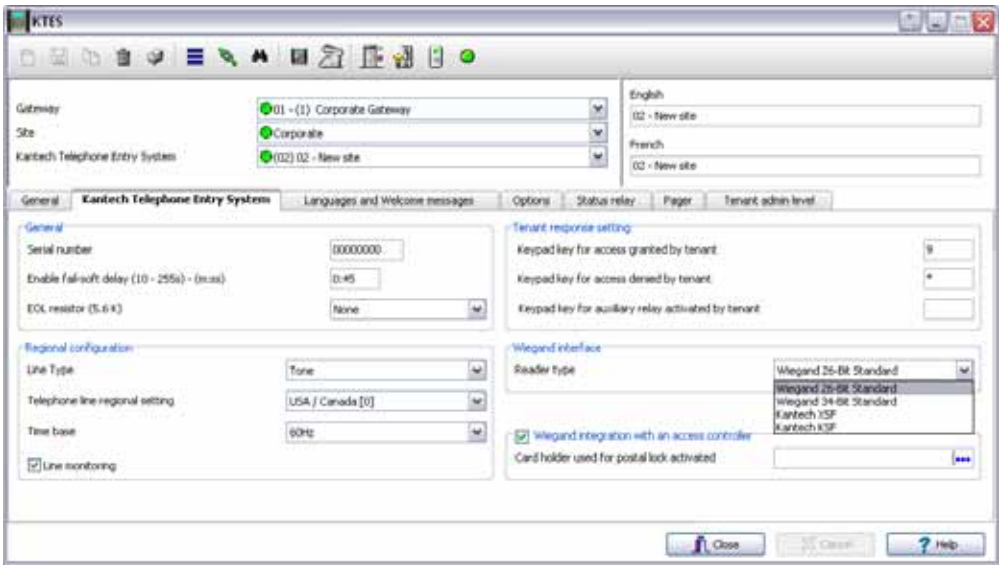
ПРИМЕЧАНИЕ: *Для большей информации смотрите в Главе 8* **Список жильцов** *на стр. 341.*

- **Use all tenants from list** (использовать всех жильцов из списка): выберите этот пункт чтобы включить всех жильцов в этот список. В противном случае, оставьте этот пункт пустым и нажмите на кнопку **Customize** (частичное). Выберите количество жильцов для включения или\и отображения их на LCD/ GJ умолчанию выбран этот пункт.
- Используйте клавишу **Print** (печать) чтобы отправить список жильцов на принтер по вашему выбору. Отсортируйте по имени или по коду. Также можете сделать предпросмотр (**preview)** перед печатью.
- Выберите График и Видеовид чтобы определить к какому шлюзу назначено, если это возможно.

Назначение параметров Kantech Telephone Entry System

1 Из окна **KTES**, выберите вкладку **Kantech Telephone Entry System**.

2 Укажите общие настройки в разделе **General** (общие):



- **Серийный номер**. Серийный номер является уникальным для каждого **KTES**. Это необходимо для связи между **KTES** и EntraPass. По умолчанию 00000000.
- **Enable fail-soft delay** (Установка задержки обрыва связи): Введите задержку связи, до того как EntraPass введет режим автономной работы и будет считать, что KTES потерян. Значение может быть от 10 сек. до 4 мин:15 сек. Значение по умолчанию 45 сек.
- **EOL resistor (оконечный резистор)**: Этот параметр может быть определен как: **None** не использоватть EOL резистор (сухой контакт), **Single** для одиночного EOL резистора (5.6K) или **Double** для режима двойного оконечного резистора (2 * 5.6K). Значение по умолчанию None.

3 Назнчение региональных параметров:

- **Line Type** (Тип линии): Установить параметр, чтобы выбрать тип телефонной линии, используемый системой. Возможные значения **Tone** или **Pulse**. По умолчанию стоит Tone.

ПРИМЕЧАНИЕ: *Для Новой Зеландии, pulse не не может быть использован.*

- **Telephone line regional setting** (региональные настройки телефонной линии): Региональные настройки телефонной линии должны быть указаны в соответствии с региональными кодами в KTES. Значение по умолчанию для USA/Canada (0). Нажмите на выпадающее меню, чтобы выбрать подходящую страну:
- **Time base** (База времени/синхронизация времени): В основном, время синхронизируется от частоты входного питания (**50 Hz** или **60 Hz**). Синхронизация времени будет автоматически переключена на **Xtal** (внутренний генератор) в случае пропадения входного питания 220 В. Синхронизация времени будет принудительна переведена на внутренний синхронизатор **Xtal,** когда присутствует только DC питание либо проблемы с основным питанием. Значение по умолчанию 60Hz.
- **Line monitoring** (мониторинг линии): Если вы выберите этот пункт, то телефонная линия будет мониторится, когда она занята или отсоединена. По умолчанию выбран этот пункт.

4 Укажите настройки для ответов жильцами **Tenant response setting**:

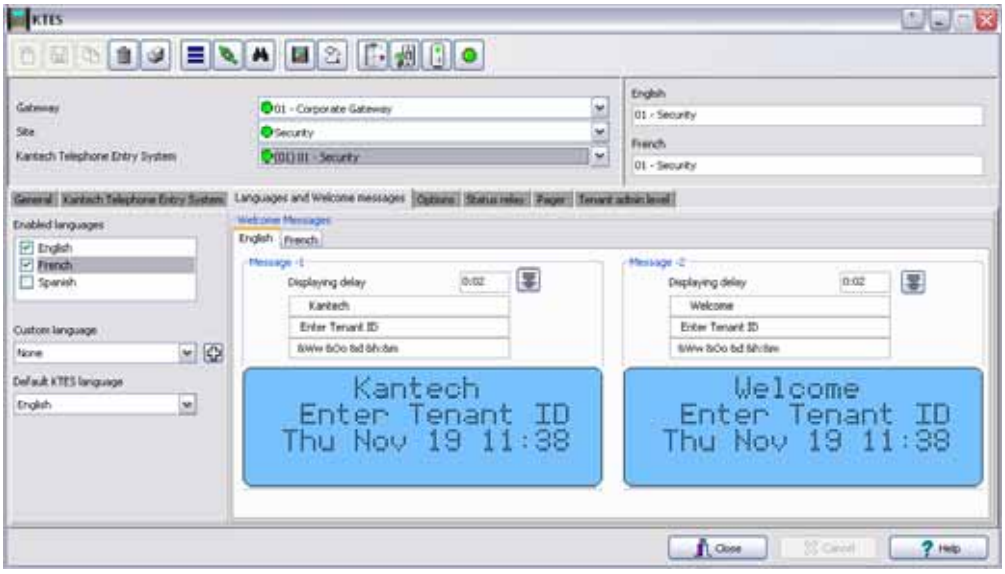
- **Keypad key for access granted by tenant** (Клавиша для предоставления доступа жильцом): Эта телефонная клавиша будет использована жильцом для предоставления доступа посетителю. По умолчанию, это значение 9.
- **Keypad key for access denied by tenant**: (Клавиша для запрещения доступа жильцом): Эта телефонная клавиша будет использована жильцом для запрещения доступа посетителю. По умолчанию, это значение *.

- **Keypad key for auxiliary relay activated by tenant** (Клавиша, которая активирует дополнительное реле при помощи жильца): Это клавиша будет использоваться для предоставления доступа на территорию посетителя, если используется второй вход. Значение по умолчанию пусто.

5 Укажите настройки **Wiegand interface** (Интерфейса Wigand):
- **Reader type** (Тип считывателя): Это интерфейс, который установлен для считывателей. Возможны 4 режима: **Kantech XSF, Kantech KSF, Wiegand 26-bit** и **Wiegand 34-bit**. Значение по умолчанию **Kantech XSF**.
- **Wiegand integration with an access controller** (интеграция Wigand с контролем доступа): Выберите эту опцию, чтобы показать что KTES подключен к контроллеру (KTES работает как контроллер доступа также). В противном случае KTES будет находиться в автономном режиме .
- **Card holder used for postal activated** (Код карты используемый для активации почтовой службы): Это номер карты, используемый KTES для генерации виртуального кода Wigand, когда происходит активация почтовго замка. Значение по умолчанию - пусто.

Назначение языковых параметров для настройки сообщений приветствия

1 Из окна **KTES**, выберите вкладку **Languages and Welcome messages**.



2 Укажите **Enabled languages** (разрешенный языки): Выберите языки, которые будут отображаться на LCD дисплее KTES. По умолчанию данный параметр не выделен.

3 Укажите **Custom language** (частные языки): Выберите частный язык доступный на LCD дсиплее KTES, выбранный заказчиком (в дополнение к уже разрешенным языкам выше). Используйте кнопку **+** чтобы добавить другие языки. По умолчанию **None** (нет).

ПРИМЕЧАНИЕ: *смотрите в Главе 16* **Редактор языков (Vocabulary Editor)** *на стр. 524 для назначение других частных языков. При помощи этого редактора словаря вы можете загрузить в KTES русский язык.*

4 Укахите **Default KTES language** (язык по умолчанию в KTES): Выберите язык по умолчанию, используемый в **KTES**. По умолчанию этот параметр None (нет).

5 Назначьте сообщения привествия **Welcome Messages**:
- Введите сообщения которое будет отображаться на панели LCD для каждого разрешенного языка. Это поле пустое по умолчанию. Используйте следующую клавишу, чтобы отобразить задержку текстового окна.
- Введите время отображения в сек. (0 сек до 4 мин:15 сек). По умолчанию установлено 2 сек.
- Повторите оба шага для второго сообщения.

6 Нажмите кнопку **Save**.

Специальные символы

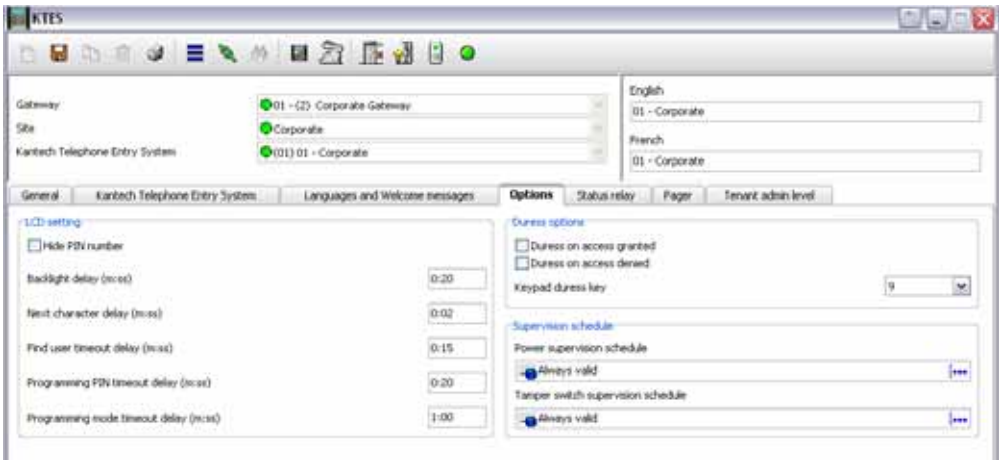
При помощи комбинации команд, отраженных в следующей таблице, вы можете выводить а дисплей LCD текущее время и дату в различных форматах:

- Дата в международном формате: &yyy/&o/&d = 2007/01/18
- Дата в американском формате: &o/&d/&y = 01/18/07
- Время в 24 часовом формате: &h:&m:&s = 14:50:55
- Время в формате am/pm: &h:&m:&s&a = 02:50:55pm
- Текущий день в трех символьном формате: &ww = mon
- Текущий день в десяти символьном формате: &wwwwwwwww = wednesday
- Текущий месяц в трех символьном формате: &oo = jan
- Текущий месяц в девяти символьном формате: &Ooooooo = January
- Полная дата в буквенном и численном формате: &ww &oo &d &yyy = thu jan 18 2007

Дисплей	Формат/код
Часы отображаются 24 часовом формате	&h
Часы отображаются 12 часовом формате	&h&a
Минуты	&m
Секунды	&s
Год из десятка	&y
Год	&yyy
Месяц	&o
Дата	&d
День недели	&ww to &wwwwwwwww
Текущий месяц в тектовом формате	&oo to &ooooooooo

Назначение дополнительных параметров

1 Из окна KTES выберите вкладку **Options** (опции).



2 Укажите настройки **LCD (LCD setting)**:

- **Hide PIN number** (скрыть PIN): Выберите этот пункт, чтобы скрыть PIN код жильца на LCD. По умолчанию это опция не выделена.
- **Backlight delay**: **Backlight Delay** (задержка отключения дисплея) это максимальная задержка, по истечении которой дисплей гаснет(0 сек до 4 мин:15 сек). По умолчанию 20 сек.

- **Next character delay**: **Next Character Delay** (Задержка ввода символов) - это максимальная задержка, которая дается на ввод следующей цифры при наборе кода. (0 сек до4 мин:15 сек). По умолчанию 2 сек.
- **Find user timeout delay** (задержка таймаута поиска жильца): После нажатия дополнительной клавиши **Find** (искать), **Find user timeout delay** - это максимальное время после последнего нажатия клавиши, после которого будет производится поиск жильца с указанным кодом. (5 сек до 4 мин:15 сек). Значение по умолчанию 15 сек.
- **Programming PIN timeout delay**: **Programming PIN timeout delay** (Таймаут на ввод PIN кода при программировании)- это максимальная задержка на ввод PIN кода для входа в режим програмирования. (5 сек до 4 мин:15 сек). По умолчанию 20 сек.
- **Programming mode timeout delay**: **Programming mode timeout delay** (таймаут на автоматический выход из режима программирования)- это максимальная задержка между последним нажатием клавиши и автоматическим выходом из режима программирования (5 сек до 9ч:59 мин). Установка по умолчанию 60 сек.

3 Указать настройки **Duress** (входа под принуждением). Эта клавиша используется если работник или житель пытается подать сигнал тревоги:

- **Duress on access granted** (вход под принуждением, доступ предоставить): Позволяет жителю войти в здание, как после верного PIN кода. Тревога вход под принуждением будет отправлена на АРМ. Значение по умолчанию, не выбрано.
- **Duress on access denied** (вход под принуждением, доступ запретить): Позволяет жителю запретить доступ, как после НЕверного PIN кода. Тревога вход под принуждением будет отправлена на АРМ. Значение по умолчанию, не выбрано.
- **Keypad duress key** (Клавиша входа под принуждением): Установите этот параметр для назначения клавиши входа под принуждением. (0 до 9, # и *). По умолчанию 9.

4 Указать **Supervision Schedule** (Расписание контроля):

- **Power supervision schedule** (Расписание контроля питания): Для назначения расписания контроля питания KTES. Выберите расписание из списка и затем нажмите ок. Значение по умолчанию “пусто”.
- **Tamper switch supervision schedule** (Расспиание контроля тампер контакта): Для назначения расписания контроля тампера KTES. Выберите расписание из списка и затем нажмите ок. Значение по умолчанию “пусто”.

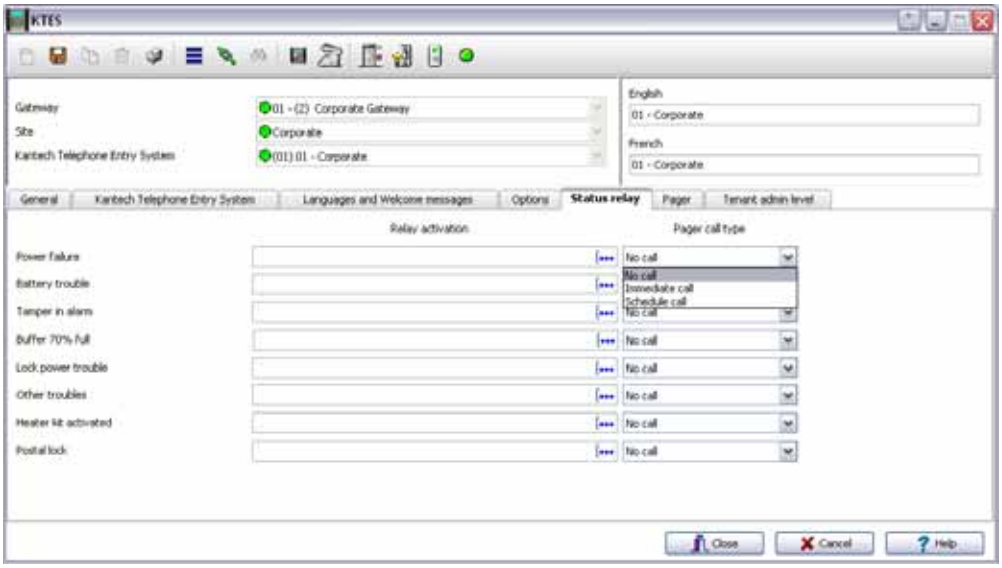
5 Нажмите на кнопку сохранить.

ПРИМЕЧАНИЕ: *Для большей информации смотрите в Главе 5* **Назначение расписаний** *на стр. 174.*

Назначение реакций реле на внутренние состояния KTES

1 Из окна **KTES**, выберите вкладку **Status relay** (состояния реле).

ПРИМЕЧАНИЕ: *Для большей информации смотрите в Главе 4* **Настройка реле** *на стр. 158.*



2 Выберите необходимые параметры **Relay activation** (активации реле):

- **Power failure** (сбой питания): Это реле может быть активировано, когда появляется ошибка входного AC питания KTES. По умолчанию установлено нет.
- **Battery trouble** (Проблема аккумулятора): Реле может быть активировано, если аккумулятор 12 В отсоединен или приходит напряжение меньше чем 11.5 В DC. По умолчанию установлено нет.
- **Tamper in alarm** (тампер контакт в тревоге): Это реле, которое может быть активировано, когда появляется тревога тампер контакта KTES. По умолчанию установлено нет.
- **Buffer 70% full** (Буфер заполнен на 70%): Реле будет активировано, если буфер событий для EntraPass будет заполнен на 70%. По умолчанию установлено нет.
- **Lock power trouble** (проблема питания замка): Этот параметр предназначен для активации реле, если проблемы с дверным замком (замок отсоединен, короткое замыкание). По умолчанию установлено нет.
- **Other troubles** (Другие проблемы): Реле будет активировано в случае если будут появляться какие-либо другие проблемы. По умолчанию установлено нет.
- **Heater kit activated** (Активация нагревателя): Реле будет активировано, если темпереатура в корпусе упала ниже -5 C. По умолчанию установлено нет.
- **Postal lock** (Почтовый замок): Реле будет активировано с входным запросом от передней двери почтового замка. По умолчанию установлено нет.

3 Укажите **Pager call type (тип вызова на пейджер)**:

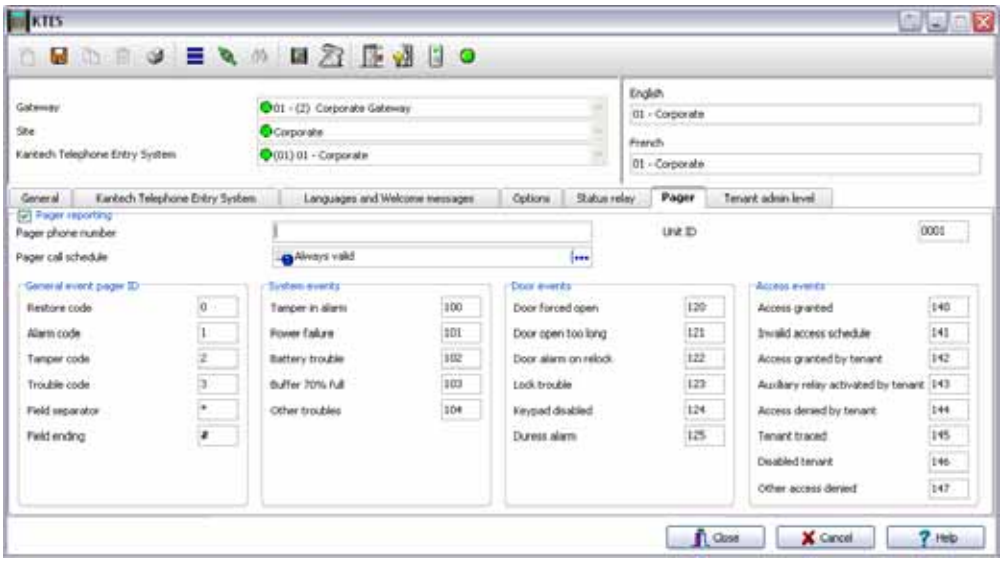
Для каждого события вы можете настраивать pager call type (тип вызова на пейджер). вы можете выбрать **No call (не звонить)** (активация реле не будет послано на пейджер), **Immediate call (звонить немедленно)** (активация реле на определенное событие будет послано незамедлительно на пейджер) или **Schedule call** (вызовы по расписанию) (активация реле на определенные события будут посланы в соответствии с указанным расписанием. Значение по умолчнию **No call (не звонить)**. см. "Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для APM, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт." на стр. 174.

ПРИМЕЧАНИЕ: *Для получения более полной информации по вызовам на пейджер по определенным событиям, то должна быть включена функция Pager reporting function (функция отправки отчетов на пейджер). см. "Назначение опций пейджера" на стр. 140*

Назначение опций пейджера

1 Из окна **KTES**, выберитие вкладку **Pager** (пейджер).

ПРИМЕЧАНИЕ: *Для новой Зеландии это о борудование не может быть установлено для автоматических звонков в службы спасения.*



2 Укажите настройки **Pager Reporting** (отчеты на пейджер):

- **Pager phone number** (номер телефона пейджера): Номер телефона пейджера на который будут отправляться события (24 символа максимум). Эта опция пустая по умолчанию.
- **Pager call schedule** (расписание звонков на пейджер): Укажите расписание когда события могут быть отпралвены на пейджер. Выберите расписание и нажмите OK.

ПРИМЕЧАНИЕ: *Для большей информации смотрите в Главе 5* **Назначение расписаний** *на стр. 174.*

- **Unit ID**: Номер устройства **KTES,** который будет послан (0001 до 9999). Значение по умолчанию 0001.
- **Restore code**: **Restore code** (код восстановления) это код, который будет ставится перед событиями, обозначенные как восстановленные (0 до 999). По умолчанию 0.
- **Alarm code**: **Alarm code** (код тревоги) - это код, который будет ставиться перед кодами , обозначенными как тревожные события (0 до 999). По умолчанию 1.
- **Tamper code** (код тампера): Этот код будет ставиться перед событиями, обозначенными как тревоги тампера, которые относятся к тамперу (0 до 999). По умолчанию 2.
- **Trouble code** (код проблемы): Код который будет ставится перед событиями, обозначенными как проблеммные (0 до 999). По умолчанию 3.
- **Field separator**: **Field separator** (разделитель поля) - это символ, который будет использоваться как разделитель поля(*, # или ,). По умолчанию это *.
- **Field ending**: **Field ending** (поле окончания) используется для обозначения окончания звонка. Помните, что вы можете ввести любой знак в качестве символа окончания (*, # или ,). По умолчанию #.

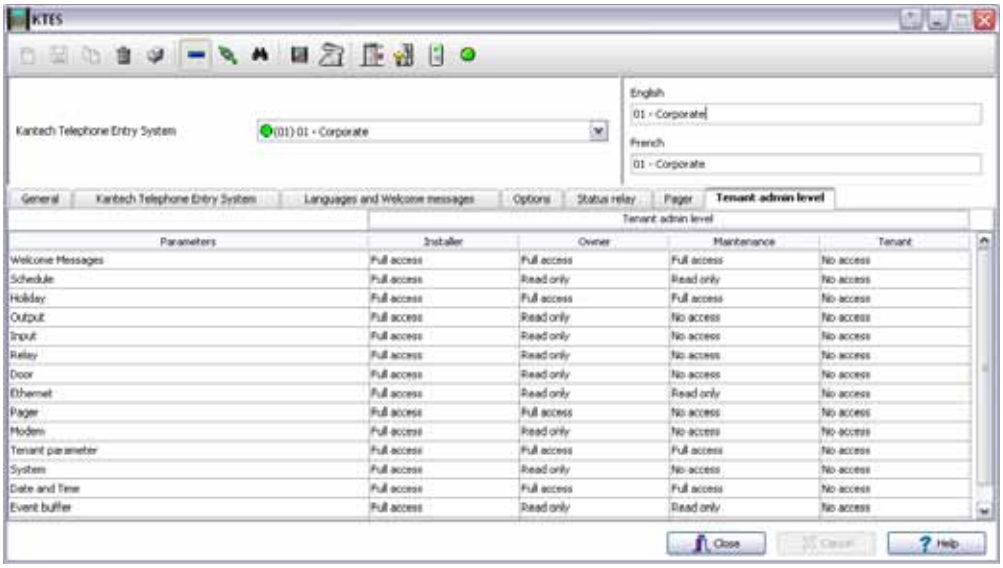
3 Укажите коды для пейджера на вкладке **General event** (общие события):

- **Tamper in alarm** (Тампер в тревоге): Код, который будет передан на пейджер при тревоге по тамперу (0 до 999). По умолчанию 100.
- **Power failure** (Сбой питания): Код, который будет передан на пейджер при сбое по основному AC питанию (0 до 999). По умолчанию 101.
- **Battery trouble** (проблема с аккумулятором): Код, который будет передан на пейджер при тревоге, связанный с аккумулятором (0 до 999). По умолчанию 102.
- **Buffer 70% full** (заполнение буфера на 70%): Код, который будет передан на пейджер при заполнении буфера событий KTES на 70% (0 до 999). По умолчанию 103
- **Other troubles** (другие проблемы): Код, который будет передан на пейджер при появлении других проблем (0 до 999). По умолчанию 104.
- **Door forced open** (Дверь принудительно открыта): Код, который будет передан на пейджер при тревоге по принудительно открытой двери (0 до 999). По умолчанию 120.
- **Door open too long** (дверь открыта слишком долго): Код, который будет передан на пейджер при тревоге “дверь открыта слишком долго” (0 до 999). По умолчанию 121.
- **Door alarm on relock** (Сигнал тревоги двери замкнут): Код, который будет передан на пейджер при тревоге “дверь оставлена открытой” (0 до 999). По умолчанию 122.

- **Lock trouble** (проблема с замком): Код, который будет передан на пейджер при тревоге “проблема с замком обрыв/КЗ” (0 до 999). По умолчанию 123.
- **Keypad disabled** (Клавиатура заблокирована): код, который будет передан на пейджер при тревоге “клавиатура заблокирована” (если эта функция включена) (0 до 999). По умолчанию 124.
- **Duress alarm** (тревога, вход под принуждением): Код, который будет передан на пейджер при тревоге “вход под принуждением” (0 до 999). По умолчанию 125.
- **Access granted** (доступ предоставлен): код, который будет передан на пейджер при событии “доступ предоставлен” (0 до 999). Событие “доступ предоставлен” отправляется на пейджер, когда житель ввел верный PIN код. По умолчанию 126.
- **Invalid access schedule** (доступ запрещен расписание): код, который будет передан на пейджер при событии “доступ запрещен”. Данный код может быть отправлен, если житель ввел неверный PIN код для доступа (0 до 999). По умолчанию 141.
- **Access granted by tenant** (доступ предоставлен посетителю жильцом): Код, который будет передан на пейджер при событии “доступ предоставлен жильцом” (0 до 999). По умолчанию 142.
- **Auxiliary relay activated by tenant** (дополнительное реле активировано жителем): код, который будет передан на пейджер при событии “дополнительное реле активировано жителем” для входа в дополнительный вход. Различно от основного входа используемые посетителем или жильцом(0 до 999). По умолчанию 143.
- **Access denied by tenant** (доступ запрещен жильцом): код, который будет передан на пейджер при событии “доступ запрещен жильцом” при запрещении доступа для посетителя жильцом (0 до 999). По умолчанию 144.
- **Tenant traced** (Жилец вошел): код, который будет передан на пейджер при предоставлении доступа жильцу (0 до 999). По умолчанию 145.
- **Disabled tenant** (Жилец запрещен): код, который будет передан на пейджер при попытке входа жильца с неверным статусом (0 до 999). По умолчанию 146.
- **Other access denied**: код, который будет передан на пейджер при предоставлении попытки входа жильцу в неверное расписание (0 до 999). т.е. жилец пришел домой в то время, когда он не должен приходить в соответствии с выданным ему расписанием. По умолчанию 147.

Настройка параметров уровня администратора для жильцов

1 Из окна **KTES**, выберите вкладку **Tenant administration level** (уровень администратора жильцов).



2 Укажите верные параметры доступа: используйте scroll чтобы установить уровень администратора для четырех видов жильцов (Full access(полный доступ), Read only (только чтение) или No access (нет доступа)).

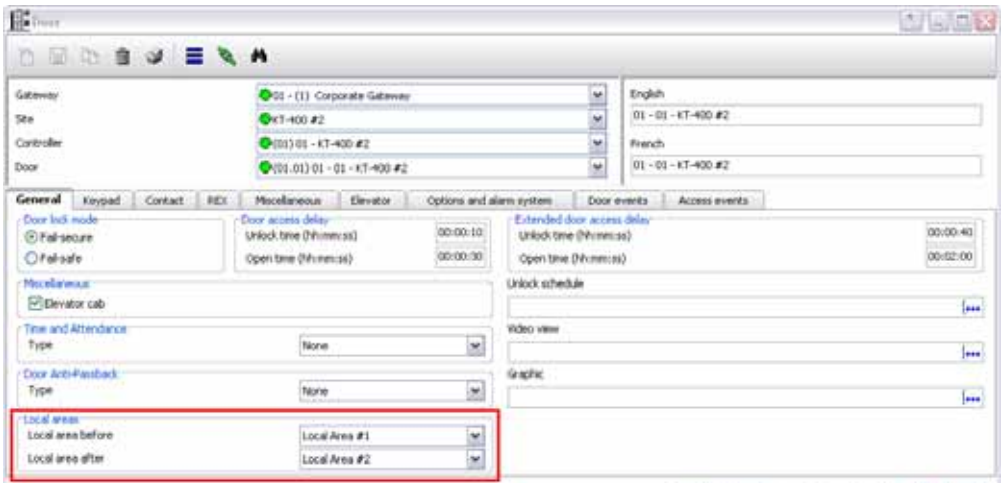
Конфигурация дверей

Это меню служит для назначения параметров дверей, на которых установлены считыватели идентификационных карт и/или кнопочные панели. Любая дверь может представлять собой дверь лифта, дверь учёта рабочего времени, входную дверь с запретом повторного прохода, ответную выходную дверь с запретом повторного прохода или служебную дверь. Это зависит от настроек программного обеспечения. Контролируемая дверь может быть всегда заперта или открыта в определённое время (по расписанию). Традиционными запирающими устройствами служат электрические защёлки и электромагнитные замки. Дверь может быть оснащена одним или двумя считывателями карт, по одному считывателю с каждой стороны. В дверях с двумя считывателями считыватель, установленный снаружи, считается "входным", а считыватель на выходе называется "выходным".

Назначение общих параметров дверей (раздел Door)

ПРИМЕЧАНИЕ: *При использовании системы с контроллерами типа KT-300 время указывается в формате ч:мм:сс и диапазон может быть настроен от 00:00:01 до 9:06:07. При использовании системы KT-400 время указывается в формате чч:мм:сс, а диапазон может быть настроен от 00:00:01 до 04:15 (255 сек) для KT-100, KT-200 и KT-300, или до 18:12:15 (65535 секунд) для KT-400. Это следует принимать во внимание при настройке.*

1 На панели устройств (**Devices**) выбрать иконку **Door** (Двери).



ПРИМЕЧАНИЕ: *Опции **local areas** (локальные области) доступна для контроллера KT-400 на Corporate шлюзе с включенной функцией **Controller local area** (локальная область контроллера)* (см. "Назначение локальных областей для контроллера KT-400" на стр. 131

ПРИМЕЧАНИЕ: *Функции **Miscellaneous** (Дополнительные), **Time and Attendance** (Учета рабочего времени), и **Door Anti-Passback** (запрет повторного прохода)**НЕ РАБОТАЮТ НА дверях KTES**.*

2 В окне **Door** выделить шлюз (**Gateway**) для просмотра лучей с контроллерами, прикреплённых к определённому шлюзу, затем выделить луч/сайт (из выпадающего списка сайтов **Site**/луч) и контроллер (**Controller**), связанный с дверью, которую необходимо настроить.

3 В выпадающем списке **Door** (Двери) выбрать дверь, конфигурацию которой необходимо настроить или изменить. Новые объекты отмечены красной меткой. После настройки и сохранения параметров эта метка становится зелёной.

4 В закладке **General** (Общие параметры) указать режим запирания двери в поле **Door lock mode**: в зависимости от используемого запирающего устройства переход в заблокированное состояние может осуществляться посредством подачи на замок напряжения питания или напротив, обесточивания цепи.

- **Fail-secure:** замок запирается при обесточивании (электромеханические дверные замки, защёлки).
- **Fail-safe:** для запирания замка необходимо подать напряжение (электромагнитные замки).

5 Если это дверь принадлежит **KTES** тогда идите на **Пункт 13.**

6 Отметить флажком опцию **Elevator cab** (Кабина лифта), если дверь используется в системе управления лифтом. Если напротив этой опции поставлен флажок, то появляется закладка **Elevator** (Лифт) для настройки расписания разблокировки двери. По умолчанию данная позиция не выделена.

7 В поле **Time and Attendance type** указать тип учёта рабочего времени (по умолчанию не использовать):
- **None** (Не использовать): считыватель используется для обслуживания служебной двери. Такое устройство выдаёт только сообщения типа “Access granted/Access denied” (Доступ разрешён/запрещён).
- **Entry** (На входе): входная дверь используется как входной пункт. Для того чтобы система выполнила запись о входе посетителя, дверь должна быть открыта после разрешения доступа (если эта дверь оснащена контактным датчиком открытия герконом).
- **Exit** (На выходе): выходная дверь используется в качестве пункта выхода. Чтобы система выполнила запись о выходе посетителя, он должен открыть дверь после разрешения на проход (если установлен контактный датчик открытия двери геркон).

8 Если включены **Controller Local Areas** (локальные области контроллера), тогда отправляйтесь на **Пункт 11.**

9 Указать тип функции запрета повторного прохода (**Door Anti-Passback**):
- **Access** (Доступ): считыватель используется для обслуживания служебной двери. Функция **Anti-Passback** не используется для служебных дверей. Такое устройство выдаёт только сообщения типа “Access granted/Access denied” (Доступ разрешён/запрещён).
- **Entry** (На входе): входная дверь используется как входной пункт. Для того чтобы система выполнила запись о входе посетителя, дверь должна быть открыта после разрешения (если эта дверь оснащена контактным датчиком открытия: герконом).
- **Exit** (На выходе): выходная дверь используется в качестве пункта выхода. Чтобы система выполнила запись о выходе посетителя, он должен открыть дверь после разрешения на проход (если установлен контактный датчик открытия двери, геркон).

10 Идите на **Пункт 13**.

***ПРИМЕЧАНИЕ: Опции None**, **Soft anti-passback** и **Hard anti-passback** доступны только для контроллеров **KT-400** с выделенной функцией **Controller Local Area** (Локальные область контроллера).*

11 Указать тип функции запрета повторного прохода (**Door Anti-Passback**):
- **None** – не использовать функцию Anti-passback.
- **Soft anti-passback** (Мягкий запрет повторного прохода) – запретить доступ, если в зоне доступа действует функция Deny Access on area full (Запретить доступ в зону при переполнении). Если, например, пользовать предъявляет свою идентификационную карту в какой-то локальной зоне, система разрешает ему пройти в другую локальную зону, даже если он не был зарегистрирован в предыдущей локальной зоне (**Local area before**). При этом только генерируется сообщение “Access granted - Passback bad location” (Доступ разрешён – повторный проход не в том месте).
- **Hard anti-passback** (Жёсткий запрет повторного прохода) – запретить доступ, если в зоне доступа действует функция Deny Access on area full (Запретить доступ в зону при переполнении). Карту, использованную для входа, нельзя будет использовать для повторного входа через этот же считыватель, пока карта не будет предъявлена для выхода через соответствующий считыватель на выходе. При этом системе генерирует сообщение “**Access denied - Passback bad location**” (Доступ запрещён – повторный проход не в том месте).

12 Описать области **Local area before** (Предыдущая локальная область) и **Local area after** (Следующая локальная область). Эти пункты меню доступны только в случае использования функции **Controller Local Area** (Локальная область контроллера).

13 Указать задержку на доступ через дверь **Extended door access delay**
- **Unlock time (hh:mm:ss)** – длительность разблокировки (чч:мм:сс). Это время, в течение которого дверь остаётся незапертой после считывания верной карты или верного запроса на выход (если кнопка запроса на выход (REX) настроена на разблокировку двери). Время указывается в диапазоне от 00:00:01 до 04:15 (255 сек) для KT-100, KT-200 и KT-300; или до 18:12:15 (65535 секунд) для KT-400. Если это дверь лифта и нажимная кнопка (вход) служит для выбора этажа, то указанное время – интервал, в течение которого разрешён выбор этажа. Как правило, это время должно быть достаточно большим, чтобы у посетителей была возможность спокойно выбрать этаж. Более подробная информация, *см. "Назначение входа для кабины лифта" на стр. 163*

- **Open time (hh:mm:ss)** – длительность открытия (чч:мм:сс). Это время, в течение которого дверь может оставаться открытой после верного считывания карты или удачного запроса на выход. Данная функция применима только к дверям, оснащённым контактными датчиками открытия. Время указывается в диапазоне от 00:00:01 до 04:15 (255 сек) для KT-100, KT-200 и KT-300; или до 18:12:15 (65535 секунд) для KT-400. После окончания указанной задержки система генерирует событие “Door open too long” (Дверь открыта слишком долго) и дверь издаёт предупредительный сигнал, побуждающий посетителя закрыть её. При желании можно настроить включение предупредительного сигнала по прошествии половины времени, допустимого для открытия двери. Для этого следует выделить опцию "Pre-alarm on door open too long" (Предтревожное состояние двери при слишком долгом открытии) под закладкой **Contact** (Контакты), окно **Door** (Двери). Сигнал будет раздаваться до тех пор, пока дверь не закроется. По умолчанию 30 сек.

14 Опция **Extended door access delay (hh:mm:ss)** – Расширенная задержка на вход, чч:мм:сс – позволяет оставлять дверь открытой более длительное время без срабатывания тревоги для прохода людей с ограниченными возможностями (назначается в картах). Для использования данной опции должны быть указаны интервалы для разблокировки и открытия двери **Unlock time** (время разблокировки, по умолчанию 40 сек) и **Open time** (время открытия, 2 мин. Время для обоих параметров указывается в диапазоне от 00:00:01 до 04:15 (255 сек) для KT-100, KT-200 и KT-300; или до 18:12:15 (65535 секунд) для KT-400.

15 **Unlock Schedule** (Расписание разблокировки двери) позволяет отпирать дверь в определённое, заранее указанное время, которое вы выберите.

16 Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплён шлюз. Выбор видеоокна будет доступным только в том случае, если в системе EntraPass разрешено использовать функцию видеонаблюдения.

ПРИМЕЧАНИЕ: *Под Corporate и Global Шлюзами, Система EntraPass позволяет назначить увеличенное время доступа и особые интервалы для разблокировки и открытия двери для людей с ограниченными возможностями. Помимо настройки этих параметров в данном разделе программы, необходимо соответствующим образом запрограммировать карту пользователя. Эта функция доступна только для контроллеров типа KT-100, KT-300 и KT-400.*

Назначение функций дверной кнопочной панели

для контроллеров KT-100 и KT-300

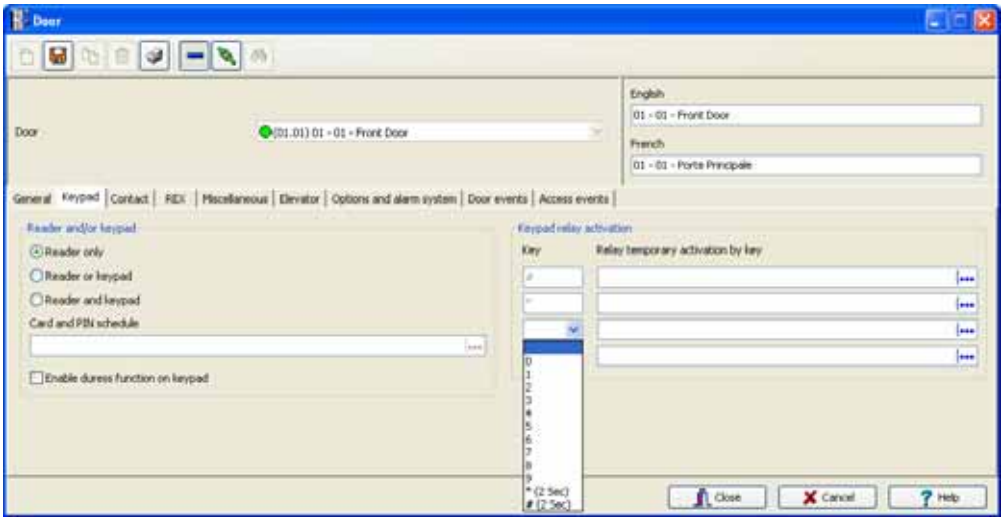
Предусмотрена возможность настройки срабатывания реле при нажатии клавиш * или # на кнопочной панели двери. Эта опция доступна только для контроллеров типа KT-100 (с прошивкой версии 1.04 и выше) и KT-300 (с прошивкой версии 1.16 и выше).

Для контроллеров KT-400

Предусмотрена возможность настройки срабатывания одного или группы реле при нажатии определённой клавиши на кнопочной панели (кейпеде) двери.

ПРИМЕЧАНИЕ: *Закладка **Keypad** (кодонаборник) доступна только при условии настройки типа кнопочной панели в поле **Keypad type** (Тип кнопочной панели) при настройке связей контроллера с дверями, см. "Указать тип кнопочной панели в поле Keypad type (при её наличии)." на стр. 123. Предусмотрено 4 клавиши. Первые две клавиши используются всегда: # и *. Они выполняют ту же роль, что и в системе контроллера KT-300. Другие две клавиши (Key 3 и Key 4) можно назначить по желанию пользователя.*

1 В окне **Door** (Двери) открыть закладку **Keypad** (кодонаборник).



2 Указать способ управления дверью (по умолчанию **reader only**):
- **Reader only** (Только считыватель) – для доступа к двери используется только считыватель. Это наиболее распространённый случай.
- **Reader or keypad** (Считыватель или клавиши) – для доступа к двери используется считыватель или клавиши кнопочной панели. Установка только кнопочной панели считается **опасным** способом защиты двери, так как пользователь может назвать свой код доступа другому лицу и не сможет предотвратить использование этого кода посторонними в дальнейшем (в отличие от карты, которую он может потребовать назад).

ПРИМЕЧАНИЕ: *Эта опция может быть разрешена на считывателе со встроенной клавиатурой, если пользователь намеревается, например, использовать только клавиатуру.*

- **Reader and keypad** (Считыватель и клавиши) – для доступа к двери требуется и считыватель, и кнопочная панель. Клавиши используются только, когда расписание “Keypad schedule” назначено. Использование клавиш в дополнение к считывателю существенно повышает уровень безопасности системы. Систему можно настроить таким образом, что идентификационный код (PIN code) будет требоваться для доступа, например, только во внеурочное время, чтобы не замедлять проход в часы пик.

3 В меню **Card and PIN schedule** (Расписание карты и кода) указать расписание, согласно которому владельцы карт должны будут, помимо предъявления действительной карты, ввести свой идентификационный код. Допустимый интервал между считыванием верной карты и вводом кода необходимо указать в меню описания шлюза (опция **Time-out on keypad** – таймаут нажатия клавиши).

4 Выделить опцию **Enable duress function on keypad** (Разрешить использование функции "Принуждение" на кнопочной панели), если необходимо. По умолчанию данная функция не выбрана.(Только для дверей на Corporate/Global/KT-NCC)

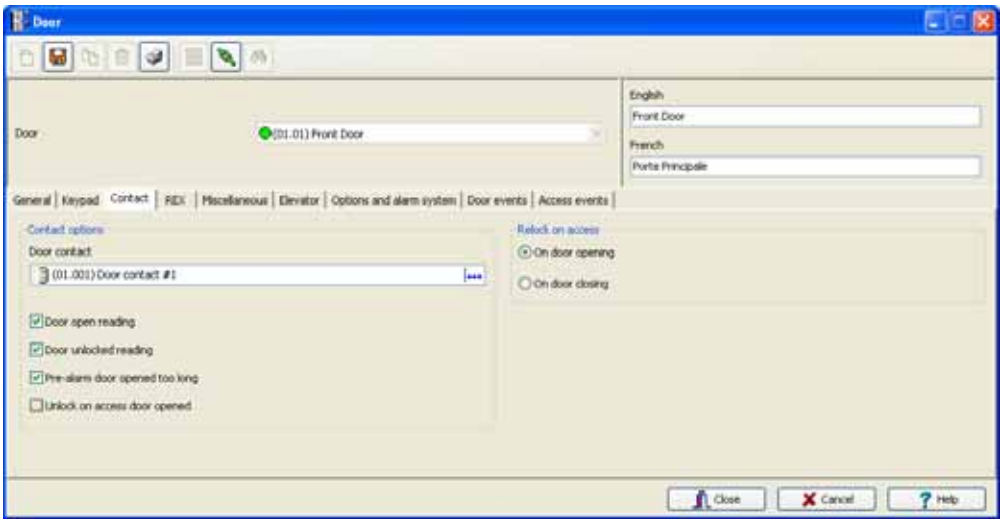
5 Выбрать клавишу(и) активации реле (**Keypad relay activation**):
- **Для контроллеров KT-100 и KT-300**: в дверях, оснащённых кнопочной панелью или считывателем с кнопочной панелью, предусмотрена возможность настройки срабатывания реле при нажатии клавиш * или #. Если эта функция активна, пользователи могут активировать реле простым нажатием определённой клавиши.
- **Для контроллеров KT-400**: в дверях, оснащённых кнопочной панелью или считывателем с кнопочной панелью, предусмотрена возможность настройки срабатывания реле или группы реле при нажатии клавиш * или # или любой другой указанной клавиши. Если эта функция активна, пользователи могут активировать одно или группу реле простым нажатием определённой клавиши.

Назначение функций дверных контактов (герконов)

В большинстве случаев дешёвый контактный датчик открытия двери является единственным контрольным элементом, от которого зависит эффективность вложения средств в дорогостоящую систему контроля доступа двери. Дверной замок и считывающее устройство (или кнопочная панель) обеспечивают безопасность и защищают от несанкционированного доступа только при условии, что дверь закрыта и заперта. Простой контактный датчик позволяет отслеживать различные состояния

двери, например: взлом двери, слишком длительное оставление двери в открытом состоянии, функции взаимной блокировки дверей ("Шлюз") и др.

1 В окне **Door** (Двери) открыть закладку **Contact** (Контакты).



2 Выбрать датчик двери (геркон) из списка **Door contact.**

ПРИМЕЧАНИЕ: *В контроллерах KT-200 вход №1 (дверной контакт) и №2 (кнопка запроса на выход) оптимизирован для двери №1 контроллера , в то время как входы №9 (дверной контакт) и №10 (кнопка запроса на выход) оптимизированы для двери №2 того же контроллера. Вход, используемый для дверного контакта или для кнопки запроса на выход (REX), НЕ ДОЛЖЕН иметь расписание "мониторинга", которое настраивают в меню "Описание входов".*

3 Отметить флажком опции считывания карт:

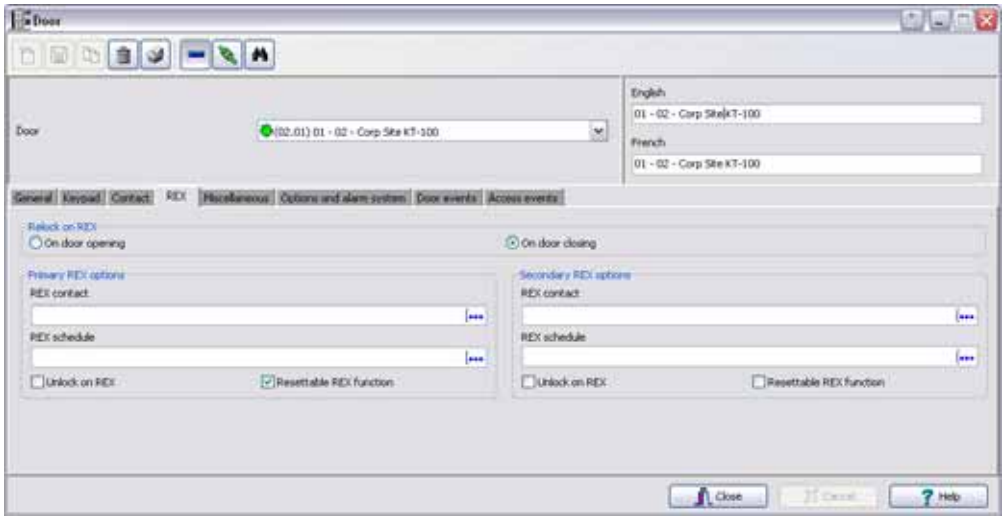
- **Door open reading** (Считывание карт при открытой двери) – позволяет считывать карты, пока дверь открыта. Однако система не разблокирует запертую дверь. При выборе этой опции система будет генерировать сообщения типа “Access granted” (Доступ разрешён). В противном случае, вы будете получать сообщения “Access granted - Door open” (Доступ разрешён – дверь открыта). По умолчанию, данная функция выбрана.
- **Door unlocked reading** (Считывание при незапертой двери) – позволяет считывать карты, если дверь отперта/разблокирована вручную оператором или по расписанию разблокировки дверей. При выборе этой опции система выдаёт сообщения типа “Access granted - Door unlocked” (Доступ разрешён – дверь отперта) в случае разрешения доступа. Чтобы не получать все сообщения о доступе при незапертой двери, эту опцию следует оставить без выделения флажком. По умолчанию, опция выделена.
- **Pre-alarm door opened too long** (Предтревожное состояние двери при слишком долгом открытии) – при выделении этой опции система будет генерировать соответствующее сообщение и включать предупредительный звуковой сигнал по прошествии половины времени, допустимого для открытия двери (**Open time**). Сигнал будет раздаваться до тех пор, пока дверь не закроется. По умолчанию, опция не выбрана.
- **Unlock on access door opened** (Отпирать во время доступа при открытой двери) – позволяет системе отпирать замок при обращении к открытой двери. По умолчанию, опция не выбрана.

4 Выбрать соответствующую опцию "Запирать(перевзять) во время доступа" в поле **Relock on access**. Предусмотрена возможность запирания/перевзятия при открытии двери (**On door opening**) или при её закрытии (**On door closing**). По умолчанию, выделена опция **On door opening.**

Назначение кнопки REX (Запрос на выход)

Сигнал "Запрос на выход" (REX) указывает, что посетитель хочет покинуть охраняемую территорию через контролируемую дверь. Сигнал REX могут генерировать такие устройства как детекторы движения или нажимные кнопки. Система EntraPass позволяет настроить двери таким образом, чтобы обнулять таймер отсчёта времени, в течение которого дверь отперта, каждый раз при срабатывании основного или дополнительного устройства "Запрос на выход". Эта опция доступна только в контроллерах типа KT-100 (с прошивкой версии 1.04) и KT-300 (с прошивкой версии 1.16).

1 В окне Door (Двери) открыть закладку **REX** (Устройства запроса на выход) и в разделе **Relock on Rex** (Запирать по сигналу REX...) выбрать необходимые функции блокировки:
- **On door opening** (при открытии двери) – чтобы система включила замок после открытия двери правильным путем.
- **On door closing** (при закрытии двери) – чтобы система закрыла замок после закрытия двери.



2 В разделах **Rex options** (основная кнопка на выход) и **Secondary Rex options** (дополнительная кнопка на выход) указать параметры для основного и дополнительного устройства "Запрос на выход":
- В поле **REX contact** (Контакт REX) указать вход, к которому будет подсоединено устройство "Запрос на выход". Этот вход должен быть местным; это должен быть один из входов на контроллере, управляющем дверью.
- Выбрать расписание в поле **Rex schedule.** Когда расписание станет достоверным, контроллер будет отслеживать и обрабатывать сигналы запроса на выход, поступающие на соответствующий контакт. Эта опция действует только для дверей, оснащённых контактами REX.
- **Unlock on REX** (Отпирать дверь по сигналу запроса на выход) – отпирать дверь по сигналу контроллера после получения им запроса на выход. Эта опция пригодится для выходных дверей, в том числе внутренних дверей, дверей для погрузочно-разгрузочных работ и других распашных дверей, через которые проходят люди с грузом. Система разрешит выход посетителя и сформирует сообщение “Request to exit granted” (Запрос на выход – выход разрешён) вместо сообщения “Door forced open” (Дверь принудительно открыта).
- **Resettable REX function** (обнулить функцию "запрос на выход") – время разблокировки двери сбрасывается при нажатии кнопки запроса на выход. Время открытия и время разблокировки двери указываются в меню назначения двери (**Devices (устройства)**> **Door (Дверь)**> **General (Общие)**). Эта опция рекомендуется для дверей в проходах с интенсивным движением, в частности, в производственных цехах, где регулярно весь персонал быстро покидает помещение (например, после окончания рабочей смены), иначе система будет выдавать сообщения типа "Door open too long" (Дверь открыта слишком долго) или "Door forced open" (Дверь принудительно открыта). Вместо сигналов "Door forced open" и "Door open too long", вы будете получать сигнал “Request to exit granted”.

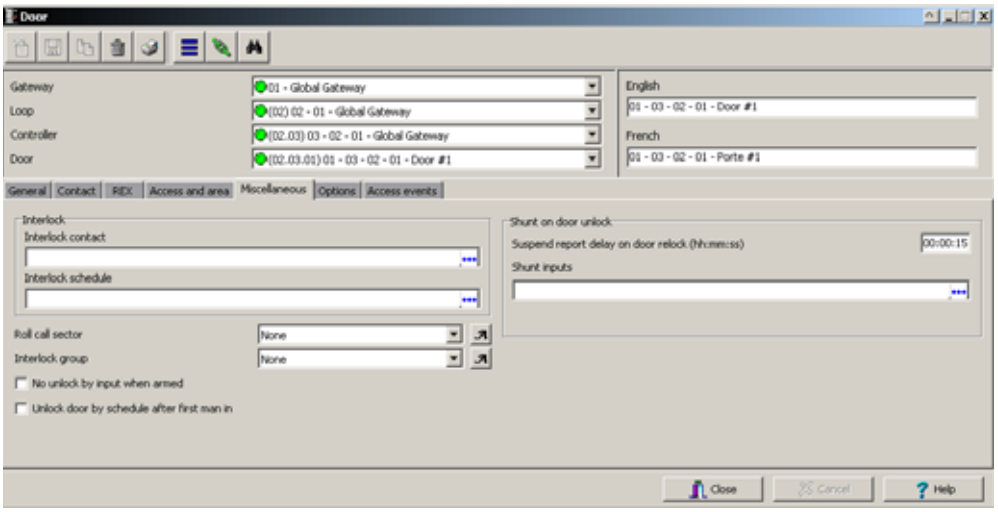
ПРИМЕЧАНИЕ: *Рекомендуется выбрать только одну из опций **Unlock on REX** (Отпирать по сигналу запроса на выход) или **Resettable REX function** (Сбрасываемая функция "запрос на выход"). Если выбрать обе опции, дверь будет оставаться незапертой длительное время. Кроме того, эти опции не следует использовать, если не настроены параметры дверного контакта.*

Назначение взаимной блокировки дверей ("Шлюз")

iПрограмма позволяет настроить параметры взаимной блокировки ("Шлюз") между двумя дверями для синхронизации времени открытия/закрытия этих дверей. Функция взаимной блокировки дверей называется также "Шлюз". Это означает, что после того как посетитель получил доступ к первой двери, эта дверь должна быть закрыта и заперта, чтобы он получил доступ ко второй двери. Обеими дверями должен управлять один и тот же контроллер.

ПРИМЕЧАНИЕ: *Опция “Шлюз” не применима к дверям KTES.*

1 В окне **Door** Двери) открыть закладку **Miscellaneous** (Прочее).



2 В выпадающем списке **Door** (Двери) выбрать первую дверь, которая будет использоваться в системе взаимной блокировки дверей (Шлюз).

3 В списке **Interlock contact** (Контакты блокировки) выбрать первый вход/input для системы взаимной блокировки (Шлюз). Выбранный вход/input должен быть *дверным контактом второй двери*.

4 Вернуться к выпадающему списку **Door** (Двери) и выбрать вторую дверь с функциями взаимной блокировки (Шлюз); затем указать контакт блокировки для этой двери. Им должен быть дверной контакт первой двери.

5 Выбрать расписание работы шлюза в поле **Interlock schedule**: обе двери должны иметь одно и то же расписание блокировки. Это расписание, согласно которому контроллер проверяет блокировку перед предоставлением доступа посетителям.

ПРИМЕЧАНИЕ: *Функции взаимной блокировки ("Шлюз") не поддерживаются контроллером типа KT-100.*

6 Выделите пункт опцию **No unlock by input when armed** (не разблокировать дверь по input, когда дверь поставлена на охрану), если необходимо. По умолчанию опция не выделена.

7 Выделить опцию **Unlock door by schedule after first man in** (Отпирать дверь по расписанию после входа первого посетителя), чтобы система автоматически отпирала дверь после успешного предъявления карты первым посетителем. По умолчанию не выделена.

8 В поле **Suspend report delay on door relock, hh:mm:ss** (отложить отчет на незапертую дверь, чч:мм:сс) должно быть указано время, в течение которого мониторинг выбранных входов не будет выполняться, если дверь отперта в течении определенного времени. Система будет автоматически шунтировать дверной контакт. Возможные значения от 00:00:01 до 18:12:15. По умолчанию 15 сек.

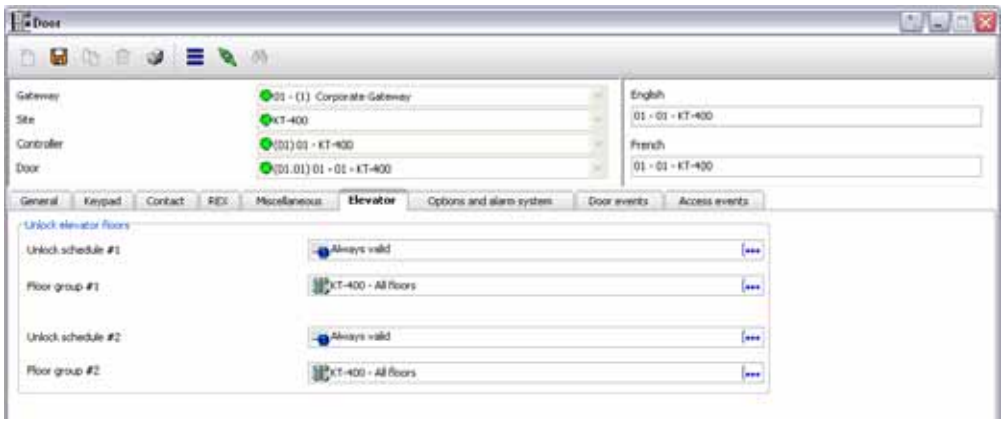
9 В списке **Shunt inputs** (Шунтируемые входы) выделить входы, мониторинг которых будет прекращаться на время разблокировки двери. Выбранные входы или группа входов будет оставаться без мониторинга в течение времени, указанного в поле **Shunt delay.**

ПРИМЕЧАНИЕ: *Меню Shunt input (Шунтируемые входы) отображается по-разному, в зависимости от того, какая система используется: KT-300 или KT-400.*

Назначение дверей лифта

При описании дверей в окне **Door**, закладка **General**, указывают тип двери: обычная или лифтовая кабина. Если дверь используется в лифтовой кабине (Elevator cab), то в меню описания двери **Door** появляется закладка **Elevator** (Лифт). Этот раздел меню используется для настройки расписания автоматической разблокировки дверей для определённых групп этажей.

1 В окне **Door** (Двери) открыть закладку **Elevator** (Лифты).



2 Выбрать расписание разблокировки двери в списке **Unlock schedule #1**. По умолчанию установлено расписание Always valid (Достоверно всегда). Помимо этого, можно составить новое расписание (меню **Definition (Назначение), Schedules (Расписание**

3 В списке **Floor group #1** (Группа этажей №1) выбрать группу этажей, прикреплённую к расписанию **Unlock schedule #1**. После того как расписание **Unlock schedule #1** станет достоверным, только этажи с настроенным в разделе Floor Group расписанием будут доступны для выбора посетителями или "открыты" для посещения.

4 Выбрать для второй группы этажей расписание разблокировки двери в списке **Unlock schedule #2**.

5 В списке **Floor group #2 (Группа этажей №2)** выбрать соответствующую группу этажей. После того как расписание **Unlock schedule #2** станет достоверным, только этажи с настроенным в разделе Floor Group расписанием будут доступны для выбора посетителями или "открыты" для посещения.

Важные примечания:

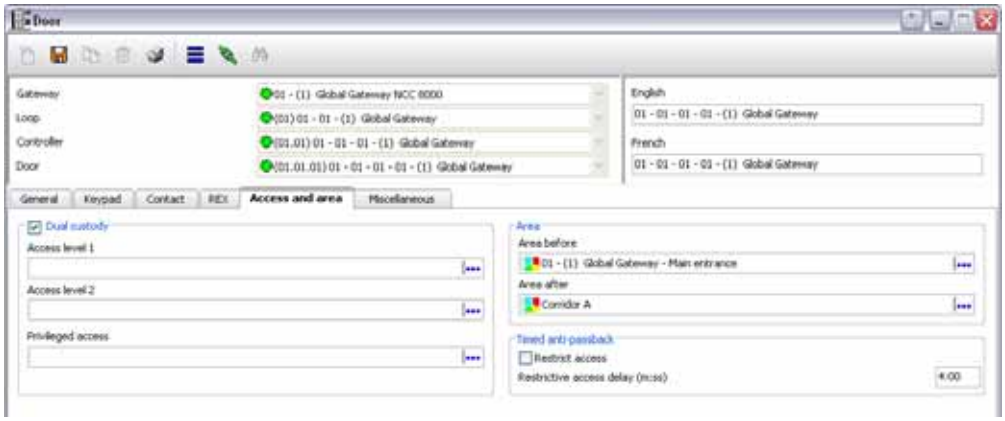
- *Расписание разблокировки двери **Unlock schedule,** настраиваемое в меню описаний дверей **Door** (закладка **General**) будет ПЕРЕКРЫВАТЬ эти расписания, даже если они будут достоверными.*
- *В каждый момент времени действует только одно достоверное расписание **Unlock schedule.** Например, если первое расписание (Unlock schedule #1) действует с 6:00 до 9:00, а второе (Unlock schedule #2) с 7:00 до 9:00, то второе расписание ВООБЩЕ не будет применяться, так как уже применяется расписание №1.*
- *Накладки расписаний недопустимы! Например, если первое расписание действует с 8:00 до 17:00, а второе с 16:00 до 21:00, то в интервале с 16:00 до 17:00 система управления лифтом будет работать с ошибками.*
- *После того как расписания Unlock schedule начнут действовать, только этажи с достоверным расписанием, описанным в разделе Floor Group, будут доступны для выбора посетителями или "открыты" для посещения.*

ПРИМЕЧАНИЕ: *Более подробные сведения по настройке системы управления лифтами с помощью реле REB-8, см. "Назначение модулей расширения контроллеров KT-200" на стр. 115.*

Назначение дверей под Шлюзом Global/KT-NCC

Эта опция доступна только года вы работаете с Global Шлюз или KT-NCC в Шлобальном Шлюзе.

1 Используйте вкладку **Access and Area** (Доступ и области) для того чтобы определить вход по двум картам, область до/после и ограничения для назначенных дверей.



2 Выделите пункт **Dual Custody** (проход по двум картам), чтобы включить эту функцию. Dual custody используется для добавления повышенных мер безопасности, требуя прикладывания двух карт для доступ в охраняемое помещение.

3 Назначьте необходимые уровни доступа для обоих держателей карт:
- Выберите **Access Level 1** (Уровень доступа №1), первый уровень доступа, необходимый для входа в эту дверь.
- Выберите **Access Level 2** (Уровень доступа №2), второй первый уровень доступа, необходимый для входа в эту дверь.
- Выберите **Privileged access**. Это уровень доступа предназначен для перекрытия запроса входа по двум картам на эту дверь.

ПРИМЕЧАНИЕ: *С функцией **Проход по двум картам** карты должны предъявляться в соответственными уровнями доступа, которые были заданы выше. Имеется виду, что сначала должны быть поднесена карта с уровнем досутпа №1, затем №2.*

4 Назначьте Области для функции Anti-Passback и отчетов muster:
- **Area before** — Выберите область, которая будет рассматриваться как *“область до”, когда картодержатель подносит карту к двери*. Для отчетов muster, всегда выбирайте Неизвестную область (Unknown area). Если вам не нужны функцииanti-passback на эту дверь, то оставьте это поле пустым.
- **Area after**— Выберите область, которая будет рассматриваться как *“область после”, когда картодержатель подносит карту к двери*. Если вам не нужны функцииanti-passback на эту дверь, то оставьте это поле пустым.

ПРИМЕЧАНИЕ: *Обычно, двери (или считыватели) являются связующим звеном между областями. Имеется в виду, благодаря этому, вы всегда можете определить где, в какой области, находится человек. Вы можете сказать, что откуда человек вышел (область до) и куда человек попал (область после).*

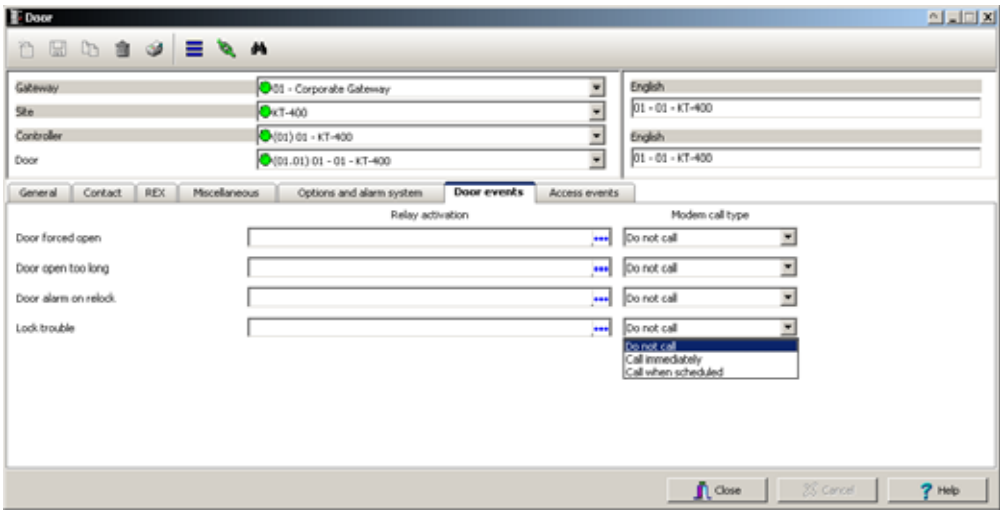
Например, картодержатель хочет попасть из Неизвестной области в Область “A”:
- Картодержатель прикладывает свою карту и запрашивает доступ в область “A”.
- Система определяет его текущее местоположение (чтобы определить текущее местоположение картодержателя см. Инструкцию на меню управление областями).
- Система затем смотрит в меню назначения двери, куда картодержатель прислонил свою карту, чтобы посмотреть какая область определена ***“область до”*** и ***“область после”*** для выбранного считывателя.
- Если область отмечена как *“Неизвестная”* (*“Unknown”*) как “область до” и “область A” установлена как “область после” и текущее местоположение картодержателя будет область “Неизвестная”, тогда доступ будет предоставлен.
- Если этот картодержатель в этот момент находился в “области B”, тогда доступ в запрашиваемую область был бы отклонен/запрещен, потому что считыватель был назначен для “области до” как область “Неизвестная”.

5 Назначьте временное ограничение на Anti-Passback. Для этого вам необходимо выделить пункт **Restrict Access** (ограничить доступ) и ввести время задержки, в течении которой будет действовать ограничение на **Anti-Passback**(мин:сек).

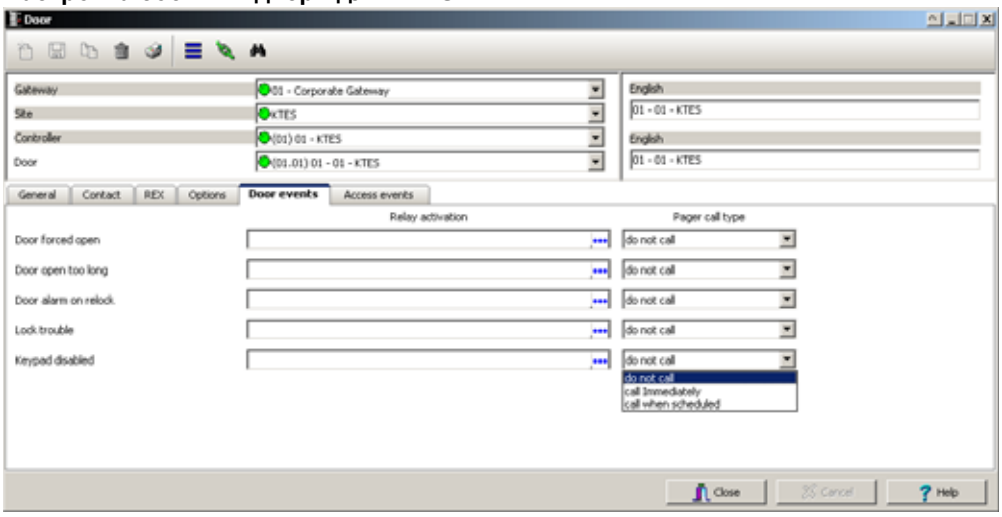
ПРИМЕЧАНИЕ: *Когда картодержатель подносит свои карты на эту дверь, картодержатель не имеет возможности подносить свои карты к другим считывателям/дверям пока не истечет указанная временная задержка.*

Настройка событий дверей (раздел Door Events) (Corporate Шлюз только)

1 В окне **Door** (Двери) открыть закладку **Door events** (События дверей). Это меню служит для настройки реле (или групп реле) на срабатывание при определённых событиях. Однако при использовании любых контроллеров, кроме KT-400 эта закладка позволяет настроить только отдельные реле.



Настройка событий двери для KTES



2 Указать реле, которые будут срабатывать локально при таких событиях, как **Door forced open** (Дверь принудительно открыта), **Door open too long** (Дверь слишком долго открыта), **Door alarm on relock** (Сигнализация двери при запирании) или **Lock Trouble** (Проблемы при запирании).

3 **Pager call type** (Тип вызова на пейджер,а применимо только для **KTES**): Вы можете выбрать **Do not call** (не звонить, активация реле на событие не будет посылаться на пейджер), **Call immediately** (звонить немендленно, активация реле на эти события, будет незамедлительно инициировать звонок на пейджер) или **Call when scheduled** (звонить по расспсианию. Активация реле будет будет вызывать звонок на пейдер при условии действия действительного расписания в этот момент). см. "Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для APM, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет

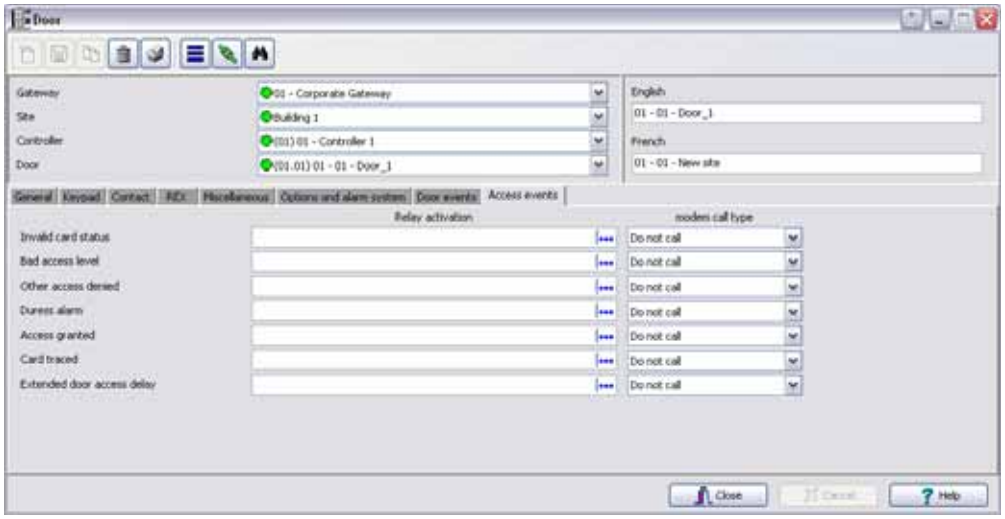
две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт." на стр. 174. По умолчанию установлено Не звонить (**Do not call**).

ПРИМЕЧАНИЕ: *Для того чтобы назначить тип вызова для каждого события, то должна быть включена функция **Pager reporting** (Отчеты на пейджер). см. "Назначение опций пейджера" на стр. 140.*

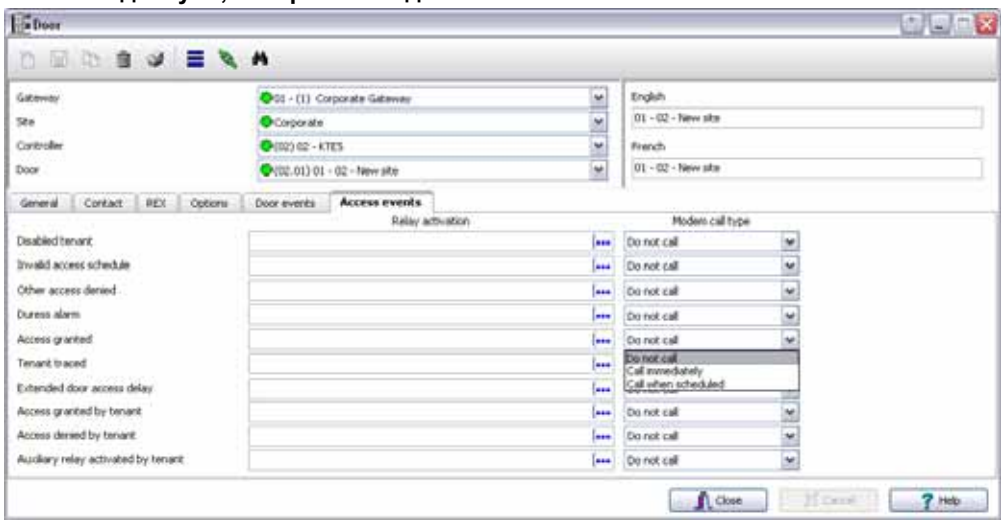
4 Под **modem call type** (тип вызова модема), назначьте такой тип вызова, который больше всего вам подходит для отчета по событиям.

ПРИМЕЧАНИЕ: *Для досутпа к функции **modem call type** (тип вызовного модема), вам необходимо в настрйоках соединения с лучом/сайтом установить режим Модем. Для большей инфорамции, см. "Настройка лучей (loops)" на стр. 102. Функция работы через модем **modem call type** поддерживается только Corporate Шлюзом.*

5 Как только вы настроили все события дверей, выберите Once all door event features have been set, select the



События доступа, настроенные для KTES



ПРИМЕЧАНИЕ: *EntraPass предлагает возможность назначения реле, которое может быть активирвоано если используется функция **Extended delay** (расширенная задержка). Карта также должна быть назнаяена для работы с этой функцией. Только на контроллерах KT-100, KT-300, KT-400 и KTES может быть настроена функция **Extended door access delay** (расширенная задержка на вход). Это преимущество доступно только на Шлюзах Corporate и Global.*

6 Выберите реле, которое которое будет активировано локально или группу реле (если вы используете KT-400) для каждого события.

7 **Pager call type** (Тип вызова пейджера, применим только для **KTES**): Вы можете выбрать **Do not call** (не звонить, активация локального реле не будет провоцировать отправку звонка на пейджер), **Call immediately** (Звонить незамедлительно. Активация локального реле будет провоцировать немедленный звонок на пейджер) или **Call when scheduled** (Звонить когда расписание. Активация локального реле будет провоцировать отправку звонка на пейджер при условии установки действующего расписания на это время). см. "Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для АРМ, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт." на стр. 174. По умолчанию установлено **Do not call** (не звонить).

ПРИМЕЧАНИЕ: *Для определения типов звонка на пейджер по каждому событию, функция **Pager reporting** (отчеты на пейджер) должна быть включена. см. "Назначение опций пейджера" на стр. 140*

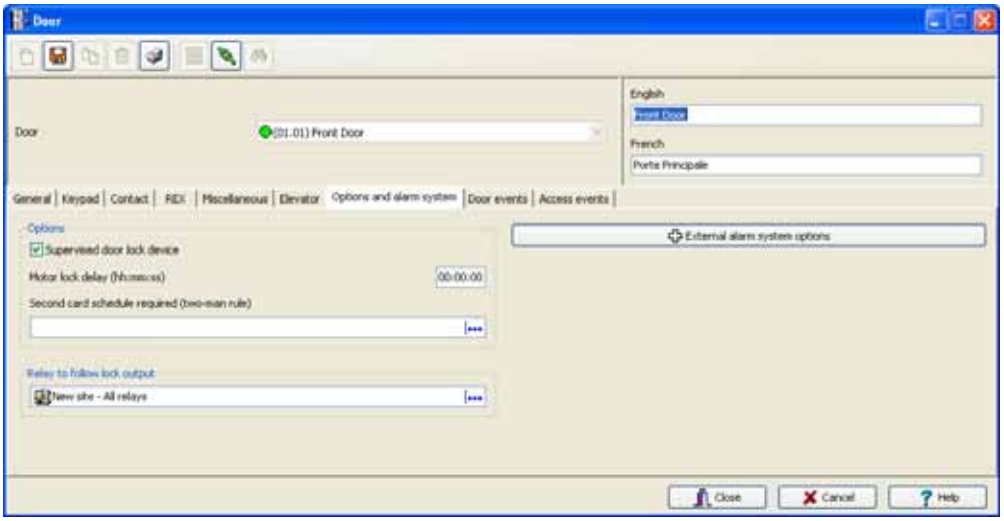
8 Под **modem call type** (тип вызывного модема), назначьте лучший тип вызова, кторый наиболее полновам подходит для функций отчета.

ПРИМЕЧАНИЕ: *Для возможности установки функции **modem call type** (тип вызывного модема), в типе соединения луча/сайта, должно стоять Модем. Для бльшей информации, см. "Настройка конфигурации соединения типа Dial-Up (RS-232) Modem (Связь через модем по коммутируемой линии)" на стр. 107.*

Назначение Настроек двери для контроллеров :Анимированные иконкии KTES (Только для Corporate Шлюза)

Описанный ниже раздел отображается только в конфигурации контроллеров KT-100, KT-300, KT-400 и KTES со шлюзами Corporate gateway.

1 Открыть закладку **Options and alarm system** (Опции и охранные панели) (или **Options** для KTES).



- **Supervised door lock device** (Контролировать запирающее устройство двери) – эта функция предназначена для выполнения особых задач, например, в банковских хранилищах для компенсации замедленного движения двигателя замка. Эта дополнительная задержка предотвращает ложное срабатывание сигнализации о взломе двери, если пользователь начинает открывать дверь до завершения длительности разблокировки. При необходимости использовать эту функцию следует отметить её флажком.
- **Motor lock delay** (Задержка запирания двигателя замка, не применима для KTES) – временной интервал (чч:мм:сс), по окончании которого дверь считается запертой. По умолчанию установлено 0:00, то есть опция не используется. Например, если это время установить равным 5 секунд, а длительность разблокировки равной 20 с. После разрешения

доступа, выход замка будет активирован (замок будет включен, 5 сек необходимо на закрытие замка) через 15 с, а дверь будет открыта в течение 5 последних секунд, сообщение о взломе формироваться не будет.

- Если для доступа требуется вторая карта, следует выбрать расписание, когда будет необходимо использовать вторую карту, из списка **Second card schedule required, two-man rule** (Расписание для второй карты, доступ по двум картам). (не применим к KTES)
- **Relay to follow lock output** (Only available for KT-400 and KTES): The relay follows the lock output status.
- **Enable duress function on keypad** (KTES only): Set this parameter to enable the duress function on the door controller keypad. A duress alarm is used by employees or tenants to signal for help. Duress function must be previously enabled to operate. Default is unchecked. см. "Назначение дополнительных параметров" на стр. 138 for more information.

ПРИМЕЧАНИЕ: *When KT-100, KT-300 and KT-400 are installed in a Corporate Gateway, the system offers the ability to interface an external alarm system.*

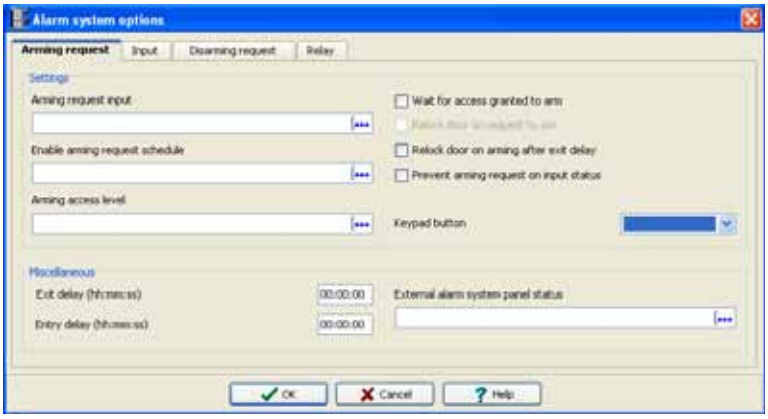
Настройка интерфейсов внешних охранных панелей (Corporate Gateway Only)

Описанный ниже раздел меню доступен только в конфигурации контроллеров KT-100, KT-300 или KT-400 со шлюзами Corporate gateway. При добавлении этих контроллеров Kantech к действующей охранной системе, владельцы карт получают возможность ставить (снимать) систему на охрану путем простого предъявления действительной идентификационной карты у входной/выходной двери. (не применимо к дверям KTES) Применение кнопочной панели повышает защищённость системы, поскольку в этом случае помимо предъявления карты требуется ввести идентификационный код. Существует два способа постановки/снятия с охраны внешней охранной панели, включая постановку на охрану с задержкой:

- По действительной карте, считываемой устройством постановки на охрану и с запоминанием срабатывания входа;
- По специальному коду, набранному на кнопочной панели и с запоминанием срабатывания входа;

Может использоваться комбинация перечисленных способов. Например, для снятия с охраны может требоваться правильный ввод кода доступа в указанном временном интервале (по достоверному расписанию) после предъявления действительной идентификационной карты.

1 В окне **Door** (Двери) открыть закладку **Options and Alarm System** (Опции и охранные панели) и нажать кнопку **External alarm system options** (Настройки внешней охранной панели). На экране появляется диалоговое окно настройки параметров охранной панели.



2 Под закладкой **Arming request** (Запрос о постановке на охрану) выбрать **Arming request input** (тревожный вход запроса на постановку). Этот вход активируется при поступлении запроса о постановке на охрану на внешнюю охранную панель.

3 После выбора входа запроса необходимо утвердить расписание в разделе **Enable arming request schedule**, по которому будет действовать запрос.

4 Если необходимо, указать уровень доступа для постановки на охрану в поле **Arming access level.**

.

- **Group** (Группа) позволяет использовать все уровни доступа.
- **Single** (Один уровень) позволяет выделить определённый уровень доступа.

- Если необходимого уровня доступа нет в списке, то его можно создать нажатием на правую кнопку мыши в поле **Arming access level** (Уровни доступа для постановки на охрану). После этого вы сможете ставить на охрану внешнюю охранную панель.

5 Чтобы повысить степень защищённости охранной панели, предусмотрены следующие опции:

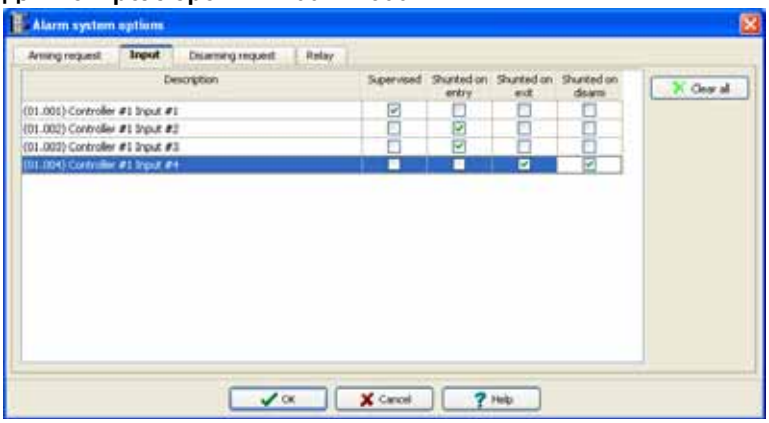
- **Wait for access granted to arm** (Ожидать разрешения для постановки на охрану) – пользователь должен предъявить действительную карту перед нажатием определённой клавиши на кнопочной панели, выбранной в меню **Keypad button**.
- **Relock door on request to arm** (Запирать дверь по запросу о постановке на охрану) – используется вместе с предыдущей опцией (**Wait for access granted to arm**), чтобы игнорировать/перекрывать расписание.
- **Relock door on arming after exit delay** (Запирать дверь при постановке на охрану после задержки на выход) – запирает дверь и ставит систему на охрану после указанной задержки, необходимой для выхода владельцев.
- **Prevent arming request on input status** (Не допускать постановку на охрану по состоянию входа) – предотвращает постановку на охрану при тревожном состоянии определённого входа.

6 Указать время задержки для входа и выхода (чч:мм:сс) в разделе **Exit delay and Entry delay (hh:mm:ss)**. **Entry delay** (Задержка входа) – это время с момента разрешения доступа, в течение которого охранная система маскирует зоны (не воспринимает сигналы тревог). **Exit delay** (Задержка выхода) – время до постановки системы на охрану. Максимальные значения для обоих параметров составляют 18:12:15. В случае использования контроллеров KT-300 максимальные значения будут равными 9:06:07. Как правило, время задержки входа короче времени задержки выхода.

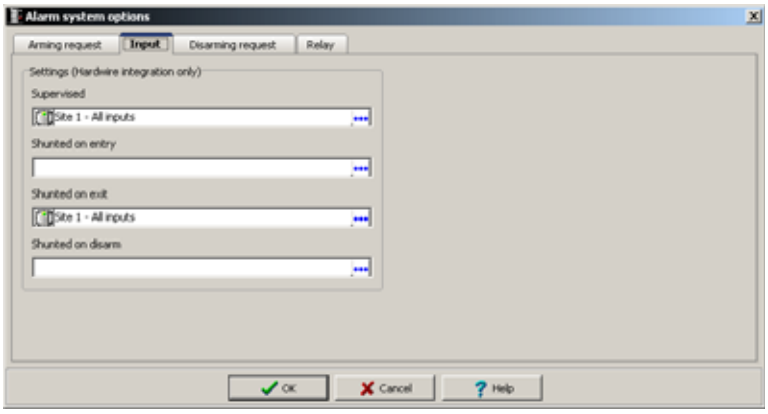
7 Указать охранный вход Kantech, который будет использоваться для указания состояния внешней охранной панели **External alarm system panel status**. Когда этот вход имеет статус "норма" (normal), охранная панель считается поставленной на охрану.

8 Открыть закладку **Input** (Входы) и указать входные устройства, которые должны находиться под наблюдением или шунтироваться (становиться неконтролируемыми), пока система стоит на охране. В списки входов включены все входы, описанные в системе.

Для контроллеров KT-100/KT-300



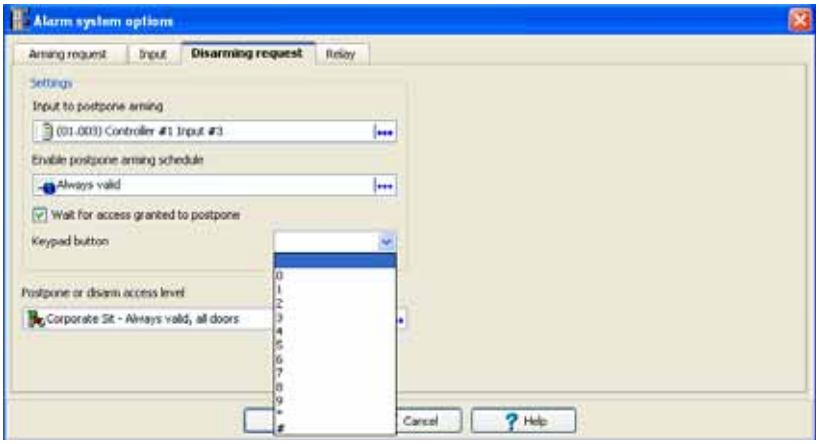
Для контроллеров KT-400



- В поле "Supervised" выбрать вход(ы), предназначенный(е) для мониторинга внешней охранной панелью; в остальных трёх полях указать входы, которые не должны

контролироваться при следующих условиях: во время входа (on entry), во время выхода (on exit) и когда система снята с охраны (on disarm).

9 В закладке **Disarming request** (запрос на снятие с охраны) вход для отложенной постановки на охрану в поле **Input to postpone arming**

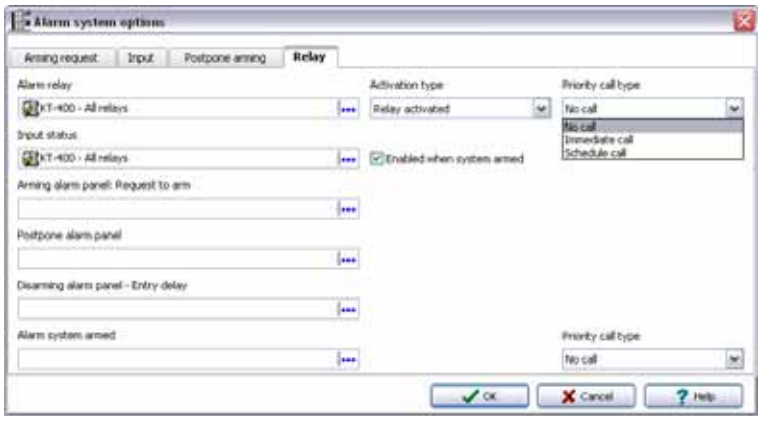


10 Указать расписание в поле **Enable postpone arming schedule** (Включить расписание режима отложение постановки на охрану).

11 При необходимости поставить флажок в поле **Wait for access granted to postpone** (Ожидать разрешения/доступа для отложенной постановки на охрану). В случае выделения этой опции режим отложенной постановки на охрану будет включён только после предъявления действительной карты и нажатия клавиши, указанной в меню **Keypad button.**

12 Выбрать уровень доступа для отложения/снятия с охраны из списка **Postpone or disarm access level.**

13 Открыть закладку **Relay** (Реле), чтобы выбрать одно или группу реле (группа доступна только для контроллеров KT-400), а также указать состояние входа для реле внешней сигнализации.



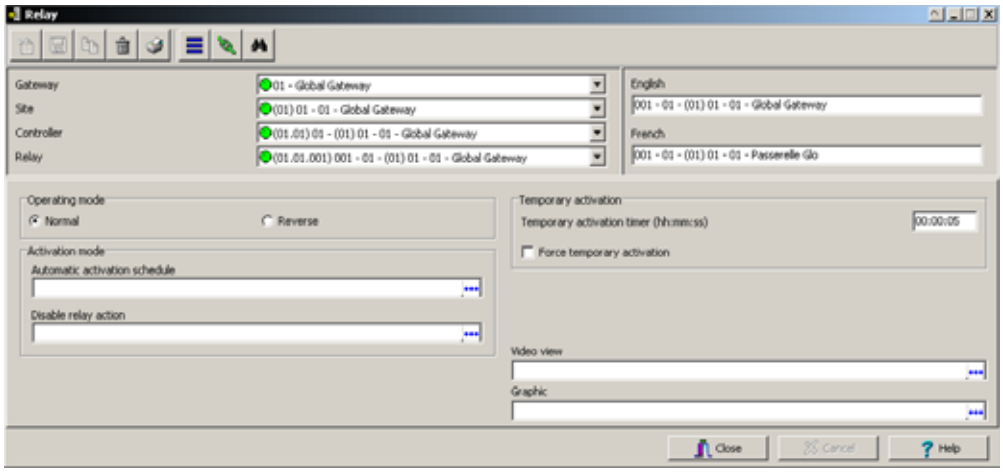
ПРИМЕЧАНИЕ: *После выбора тревожных реле в поле* ***Alarm relay*** *появляется доступ к полю* ***Activation type,*** *где можно указать тип активации реле. Они могут быть активированы постоянно или временно.*

Настройка реле

Выходные управляющие реле, которыми оснащён каждый контроллер KT-100, KT-200, KT-300 и KT-400, могут использоваться для активации сигнализаций и других устройств, включая регуляторы освещённости, системы вентиляции и кондиционирования воздуха. Эти реле активируются по расписанию или по событиям, зарегистрированным системой. Кроме того, они могут срабатывать при определённом статусе охранной панели или при комбинации различных логических условий.

Назначение реле

1 Открыть закладку **Devices** (Устройства) и нажать иконку **Relay** (Реле).



2 Указать в поле **Gateway** шлюз, в поле **Site** сайт/луч и в поле **Controller** контроллер, а также выбрать реле, которое необходимо настроить, в поле **Relay**.

3 Указать режим работы реле в поле **Operating mode** (Рабочий режим):
- **Normal** (Стандартный) – реле нормально разомкнуто (деактивировано) и замыкается (срабатывает) по команде оператора, при возникновении события или по расписанию системы.
- **Reverse** (Обратный) – реле нормально замкнуто (активировано) и размыкается (оказывается не под напряжением) по команде оператора, при возникновении события или по расписанию системы.

4 В поле **Automatic activation schedule** (Расписание автоматического срабатывания) выбрать расписание, в соответствии с которым реле будет срабатывать (замыкаться или размыкаться, в зависимости от выбранного режима работы).

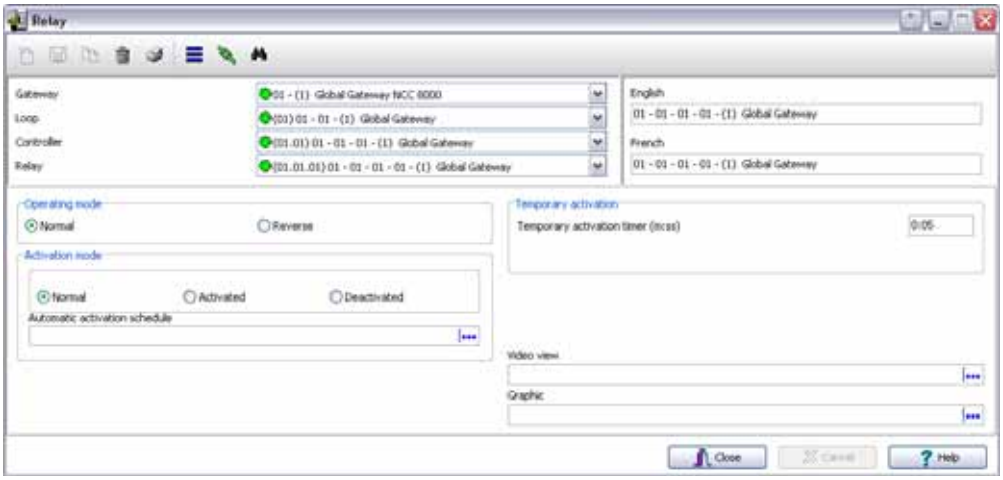
5 В поле **Disable relay action** (Запретить работу реле) выбрать расписание, во время действия которого реле будет деактивироваться (или активироваться) в соответствии с выбранным режимом работы. (только Corporate/Global Шлюз)

ПРИМЕЧАНИЕ: *Под Шлюзы NCC-8000 и Global, EntraPass предлагает пользователям возможность принудительной временной активации. В EntraPass Global Edition, появляется возможность принудительной активации реле в поле* ***Force temporary activation*** *в окне (****Devices*** *>* ***Relays****). Например, реле, которое было активировано, остается в этом состоянии пока оно не будет принудительно деактивировано. Когда выбрана эта опция, реле будет деактвировано по тревожному событию,системному событию или по расписанию.*

6 В поле **Temporary activation timer** (Таймер временной активации реле) указать задержку, во время которой реле будет временно активироваться в соответствии с режимом временной активации.

ПРИМЕЧАНИЕ: *Если таймер установлен равным нулю, то по умолчанию задержка срабатывания реле будет составлять пять секунд. Максимальное время задержки составляет 9:06:07 (9 часов 6 минут 7 секунд). При использовании контроллера KT-400 максимальное время задержки составляет 18:12:15 (18 часов 12 минут 15 секунд).*

7 Под Шлюзом NCC-8000, вы должны назначить действие на реле в режиме типа активации **Activation Mode**.



- **Normal**—На реле не оказывается влияние при помощи пункта “activation schedule” расписание активации. Будет запомнено состояние реле, когда необходимо (ручное управление, событие, тревожная система, итд.).
- **Activated**—(активировано)Реле временно активировано на время, которое указано во времени активации “activation schedule”. В этом случае, события или другие системные функции не могут оказывать влияние на реле. Оно будет оставаться активировано. Когда “activation schedule” станет неверным, активированное реле перейдет в нормальный режим.
- **Deactivated**—(деактивировано). Реле временно деактивировано на время, которое указано во времени активации “activation schedule”. В этом случае, события или другие системные функции не могут оказывать влияние на реле. Оно будет оставаться деактивировано. Когда “activation schedule” станет неверным, недеактивированное реле перейдет в нормальный режим.

8 Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплено реле.

Конфигурация входов (раздел Input)

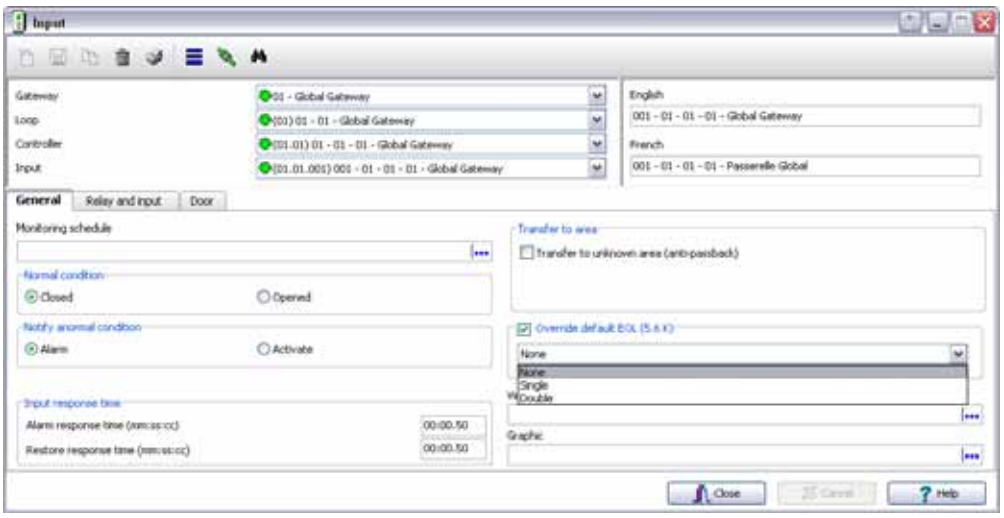
Контроллеры дверей контролируют сотояние входов/Input, в том числе контактные датчики открытия дверей, замки, детекторы движения, датчики температуры, различные устройства запроса на выход (REX), а также другие устройства с сухими контактами. Число контролируемых входов зависит от типа контроллера: 4 входов у KT-100, 16 у KT-200, 8 входов на плате (возможность расширения до 16) у KT-300.

- **Только для модели KT-200.** Входы представляют собой нормально замкнутые или нормально разомкнутые сухие контакты, последовательно соединённые с одним резистором. Если сухой контакт соединён последовательно с зелёным резистором, то вход имеет нечётный номер. Если сухой контакт соединён последовательно с красным резистором, то вход имеет чётный номер.
- **Вход №1** (дверной контакт) и **№2** (кнопка запроса на выход) оптимизирован для двери №1 контроллера, в то время как входы №9 (дверной контакт) и №10 (кнопка запроса на выход) оптимизированы для двери №2 того же контроллера. Вход, используемый для дверного контакта или для кнопки запроса на выход (REX), НЕ ДОЛЖЕН иметь расписание "мониторинга" в меню "Описание входов".
- **Для контроллеров KT-100.** Вход №1 предназначен для дверного контакта, а вход №2 для кнопки запроса на выход.
- **Для контроллеров KT-300.** Вход №1 служит для подсоединения датчика двери №1, а вход №2 для кнопки запроса на выход на двери №1 того же контроллера. Вход №3 используется для контактного датчика на двери №2, а вход №4 для кнопки запроса на выход на двери №2 того же контроллера.
- **Для контроллеров KT-400.** Вход №1 используется для датчика двери на двери №1, а вход №2 для кнопки запроса на выход на двери №1 (REX Door #1) того же контроллера. Вход №5 служит для датчика двери на двери №2, а вход №6 для кнопки запроса на выход на двери №2 контроллера. Вход №9 предназначен для датчика двери на двери №3, а вход №10 для кнопки запроса на выход для двери №3 контроллера. Вход №13 используется для датчика двери на двери №4, а вход №6 для кнопки запроса на выход для двери №4 контроллера.

Назначение входов

Входа/inputs можно настроить через кнопку **Input** (Вход) на вкладке меню **Devices** (Устройства). Вы можете также назначить входа (inputs) при назначении контроллера в Express Setup (*в Главе 16 Программа быстрой настройки"Express Setup" на стр. 531*).

1 Открыть закладку **Devices** (Устройства) и нажать иконку **Input** (Входы).



2 Указать шлюз в поле **Gateway**, сайт/луч в поле **Site** и контроллер в поле **Controller**.

3 В выпадающем списке **Input** (Входы) выделить вход, конфигурацию которого необходимо настроить.

4 Назначить для указанного входа расписание мониторинга в меню **Monitoring schedule** (это расписание, по которому система будет отслеживать статус входа). Если расписание действует, при изменении статуса входа будет сформировано событие типа “Input in alarm” (Вход переведён в статус тревоги) или “Input restore” (Статус входа восстановлен).

ПРИМЕЧАНИЕ: *Вход, используемый для датчика двери или для кнопки запроса на выход (REX), НЕ ДОЛЖЕН иметь расписание "мониторинга".*

5 Указать в поле **Normal condition** нормальное состояние входа: замкнутое (**Closed**) или разомкнутое (**Opened**).

ПРИМЕЧАНИЕ: *Когда используете одинарный или двойной оконечный резистор, установите режим входа **Normal Condition** (нормальное условие) чтобы **Closed** (закрыть).*

6 Укажите для входа “извещение о ненормальном условии входа” **Notify abnormal condition**: это может быть **Alarm** (тревога) или **Activate** (активация).

ПРИМЕЧАНИЕ: *Когда вы настраиваете пункт события/реакция (event parameters) с **Input in alarm** (вход в тревоге) или **Input activated** (вход активирован) в качестве выбранного события, то вам отображаются только входы только с этими критериями. в Главе 12 Назначение пункта параметров событий (событие/ реакция) на стр. 426 for more information.*

7 По óмолчанию, EntraPass не выбирает **Suspend status update when not monitored** (Приостановить состояние обновления когда не контроллируется). Это уменьшает трафик до минимума. Тем не менее, эта опция может быть включена при необходимости.

8 Указать время для отклика входа в поле **Input response time** (Время отклика входа). Это задержка, в течение которой статус входа должен оставаться прежним, перед тем как будет обнаружено изменение статуса. Эта задержка указывается в минутах (формат мм:сс:дд, где дд – доли секунды). Время для обоих параметров, alarm response и alarm restore, составляет от 10 сек до 10:55:35. I Например, сработал вход, система увидела, что вход сработал через 10 сек.

- **Alarm response time, mm:ss:cc** (Время отклика при переходе в статус тревоги) – задержка, после окончания которой система формирует событие об изменении статуса входа на тревожный. Например, вход сработал, лампочка зажглась через 10 сек.
- **Restore response time, mm:ss:cc** (Время отклика при возвращении прежнего статуса) – задержка, после окончания которой система формирует событие о возвращении прежнего статуса Corporate и Global Шлюзы). По умолчанию 50 сек.

ПРИМЕЧАНИЕ: *Указание времени отклика входа позволяет исключить из рассмотрения то время, в которое контакт изменяет своё положение, и помогает генерировать только одно событие для каждого переключения, если это время дольше, чем время переключения контакта. Например, при указании задержки 01:00:00 контакт должен оставаться в новом положении не менее одной минуты, чтобы система сформировала сообщение об этом.*

9 Укажите опции **Kantech Telephone Entry System** options (применимо только для KTES).

ПРИМЕЧАНИЕ: *Пункт **modem call type** (тип вызова модема), соединение с лучем должно быть установлено через модем. Для получения дополнительной информации, см. "Настройка лучей (loops)" на стр. 102. Пункт **modem call type** (тип вызова модема) поддерживается только Corporate Шлюзом.*

- **Pager call type** (Тип вызова на пейджер): Вы можете выбрать **Do not call** (Не звонить) (активация реле не будет инициировать отправку сообщения на пейджер), **Call immediately** (Незамедлительно звонить)(активация реле будет инициировать отправку сообщения на пейджер незамедлительно) или **Call when scheduled** (активация реле будет провоцировать отправку сообщения на пейджер, в соответствии расписанием звонков на пейджер). см. "Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для APM, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт." на стр. 174. Значение по умолчанию **Do not call** (Не звонить).
- Под вкладкой **modem call type** (Типа вызова модема), назначьте опцию типа вызова, что наиболее лучше подходит для отчета по событиям. Значение по умолчанию **Do not call** (Не производить вызов).
- **Input pager ID** (ID входа для пейджера): Введите код пейджера, сввязанного с выбранным входом. Возможные значения 201, 202, 203 и 204.

ПРИМЕЧАНИЕ: *Для указания типа вызова для пейджера для каждого события, должна быть включена функция отсылки отчета на пейджер. см. "Назначение опций пейджера" на стр. 140*

10 Только для Global шлюза: Выделите пункт **Transfer to Unknown Area (anti-passback)** (перместить в неизвестную область (антипасбек)). Это необходимо для назначения сухого контакта (специальной кнопки), которая может быть использована менеджерами всех карт всех зон и секторов в “Unknown area” (неизвестную область), если контроль повторного прохода назначен в системе. Это также может быnm использовано, когда весь персонал должен покинуть здание из-за пожара. Это опция будет сбрасывать все карты, вместо использования ручной операции, на которую может потребоваться значительное время.

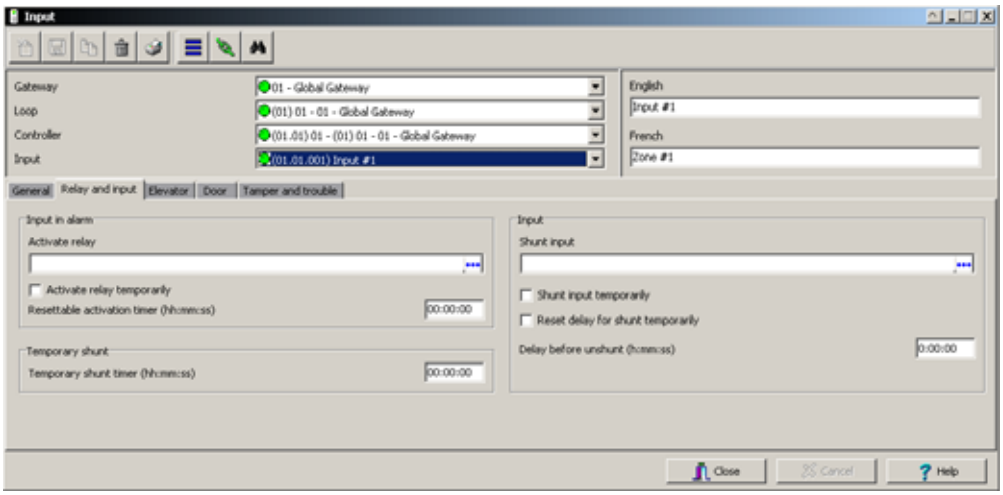
ПРИМЕЧАНИЕ: *Расписание контроля входа, должно быть достоверным.*

11 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.

12 Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплён вход.

Назначение реле и входов

1 Открыть закладку **Relay and input** (Реле и входы), чтобы указать реле и вход(ы), которые будут активироваться или шунтироваться при активировании настраиваемого входа.



2 В поле **Activate relay** (Активировать реле) указать одно или группу реле, которые будут срабатывать при тревоге по входу.

3 При установке флажка в поле **Activate relay temporarily** (Активировать реле временно) реле будет активировано в соответствии с параметрами временной активации (**Temporary activation**), указанными в меню Relay. По умолчанию, не выбрано.

4 В поле **Temporary Shunt Timer, h:mm:ss** (Таймер временного шунтирования, ч:мм:сс) указать время, в течение которого мониторинг входа отключён. При установке таймера на ноль (0:00:00) реле точно отслеживает статус входа. Максимальное значение задержки Shunt delay составляет 18:12:00 (при использовании контроллера типа KT-400 или KTES). Шлюзы только Corporate или Global. Значение по умолчанию 0.

ПРИМЕЧАНИЕ: *Под Global шлюзом, пользователи имеют возможность назначать задержку до шунтирования.*

ПРИМЕЧАНИЕ: *Для того чтобы система правильно обрабатывала задержку возврата при временном шунтировании/маскировании, опция **Temporary Shunt Timer** (Таймер временного шунтирования) должна быть настроена в меню назначения входа, который будет сбрасывать эту задержку. Например, если вход 1 временно шунтирует вход 2, то таймер **Temporary Shunt Timer** должен быть также указан в назначении входа 2.*

5 В списке **Shunt input** (Шунтируемые входы) выбрать вход, мониторинг которого не будет выполняться, пока указанный вход активирован.

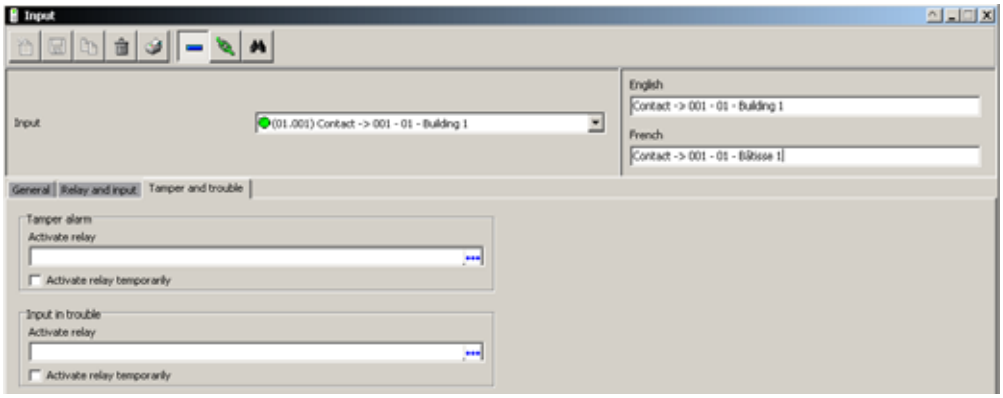
6 Если преминимо, то выделите пункт **Shunt input temporarily** (временно шунтировать вход) и Reset delay (задержка сброс) для опций временно шунтируемых входов. По умолчанию, данные опции не выделены.

7 **Delay before unshunt**:(Задержка до сброса шунтирования) Значение могут быть от 1 сек. до 18 ч:12мин:15 сек.

ПРИМЕЧАНИЕ: *В случае восстановления входа или возвращения его в нормальное состояние шунтируемый вход так же вернётся в нормальное состояние. Система сформирует событие “Input shunted by input” (Вход шунтируется по входу). Когда вход вернётся в нормальное состояние, будет сгенерировано событие “Input unshunted by input” (Вход перестал шунтироваться по входу).*

Назначение Тампера и проблемы (Tamper and Trouble)

1 Выберите вкладку **Tamper and trouble** (Тампер и проблема) для связи реле или группы реле для активации в случае проблемы по входу (input in trouble) или тревоги по тамперу. Эта таблица только для **DEOL** (Двойной оконечный резистор).



2 В поле **Activate relay** (тревога по тамперу) указать одно или группу реле, которые будут срабатывать при тревоге по входу тампер.

3 При установке флажка в поле **Activate relay temporarily** (Активировать реле временно) реле будет активировано в соответствии с параметрами временной активации (**Temporary activation**), указанными в меню Relay. По умолчанию, не выбрано.

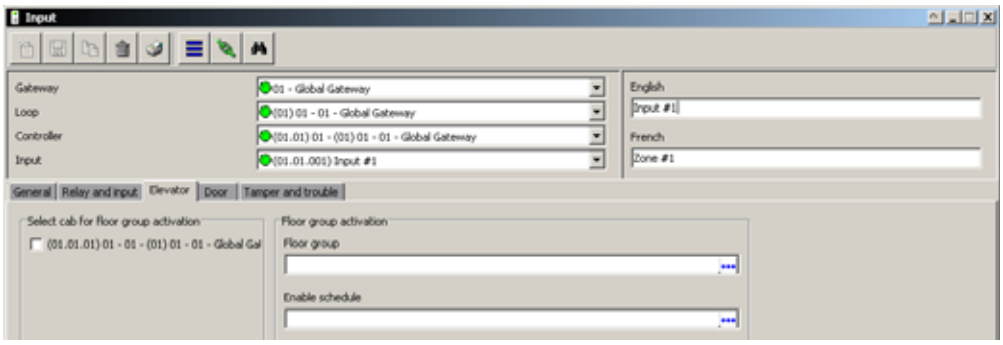
4 В поле **Activate relay** (тревога по входу) указать одно или группу реле, которые будут срабатывать при тревоге по входу.

5 При установке флажка в поле **Activate relay temporarily** (Активировать реле временно) реле будет активировано в соответствии с параметрами временной активации (**Temporary activation**), указанными в меню Relay. По умолчанию, не выбрано.

Назначение входа для кабины лифта

Если настраиваемый вход предназначен для управления лифтом, в окне описания входов (Input) отображается закладка **Elevator** (Лифты). Вход можно привязать к нажимной кнопке. В таком случае им могут воспользоваться охранник или секретарь в приёмной для временной активации этажей, описанных в разделе активации группы этажей (Floor group).

1 В окне описания входов **Input** открыть закладку **Elevator** (Лифты).



ПРИМЕЧАНИЕ: *Для выбора будут доступны только те этажи, которые отмечены (X) флажком в меню Floor group (Группы этажей), колонка* **State** (Статус). *Временный доступ к этажам будет предоставляться в соответствии с задержкой, указанной в меню* ***Door*** *(Двери), Unlock time (Время разблокировки). Для того чтобы активировать эту опцию, необходимо указать в списке Enable schedule list подходящее достоверное расписание. Данная закладка доступна только при условии, что в настройках двери указан тип "лифтовая кабина".*

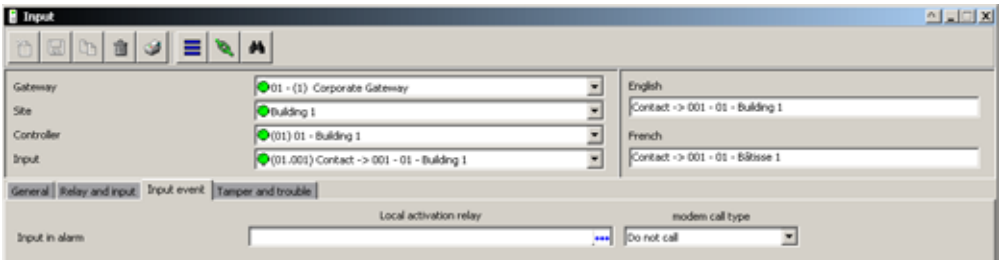
2 В разделе **Select cab for floor group activation** (Выбрать кабину для активации группы этажей) указать кабину, прикреплённую к данному входу.

3 Выбрать группу этажей (**Floor group**), прикреплённую к указанной кабине, которые будут активироваться при срабатывании настраиваемого входа.

4 Выбрать расписание, по которому настраиваемый вход будет выполнять эту команду.

Настройка удалённого оповещения о событиях (Только Шлюз Corporate)

1 Открыть закладку **Input event** (События входа).



2 В списке **Local activation relay** (Активация локального реле) выбрать одно или группу реле, которые будут срабатывать при переключении этого входа в состояние тревоги (при активировании входа).

ПРИМЕЧАНИЕ: *Группы реле доступны только при использовании контроллеров KT-400.*

3 В разделе **Modem call type** (Тип вызова модема) указать тип вызова, наиболее полно отвечающий сообщению о событии, активирующем настраиваемый вход.

ПРИМЕЧАНИЕ: *Чтобы опция* ***Modem call type*** *стала доступной, в поле* ***Site connection type*** *(Тип соединения луча/сайта) должен быть указан* ***Modem*** *(Модем). Более подробная информация см. "Настройка лучей (loops)" на стр. 102. Опция* ***Modem call type*** *поддерживается только Corporate Шлюзом только.*

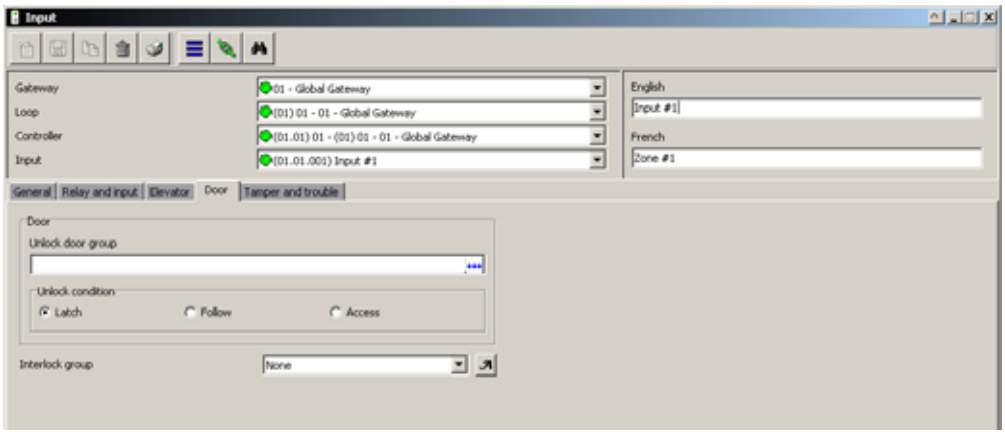
Назначение входа(input) для группы дверей

Это преимущество позволяет операторам вход(input), который будет разблокировать группу дверей по трвеоге на входе. Это преимущество модет быть установлено для группы дверей.

ПРИМЕЧАНИЕ: *Если вы имеете одну дверь, которую вы хотите разблокировать по тревоге на входе, создайте группу дверей, которая содержит всего одну дверь.Для того, чтобы создать групппу, см в Главе 9 Создание группы дверей на стр. 349.*

Когда вход/input будет назначен/исправлен используемый для дверного контакта, вкладка **Door** оторазится в окне назначения входов/Input.

1 На вкладке назначения входа, выберите вкладку **Door** (Дверь).



2 Выберите группу дверей, которая будет разблокироваться по тревоге на входе/input.

3 Выберите действие, которое последует после разблокировки дверей

- **Latch** (защелка) будет удерживать двери разблокированными до тех пор, пока оператор в ручном режиме их не заблокирует, при условии нормального состояния входа/input.
- **Follow** (следящий) двери будут удерживатьсся разблокированными до тех пор, пока кто-то не вернет состояние входа/input в нормальный режим. Эта опция является наиболее подходящей для ручного открытия дверей и необходимости после этого сбрасывать тревогу в ручном режиме.
  - Пример: для двери, являющееся частью групы, соответствующего расписания. Когда тревога по входу восстановится в нормальный режим, тогда двери будут вновь заблокированы/закрыты в соответствии с действующим расписанием работы этих дверей.
- **Access** (Доступ) Двери будут разблокированы на указанное время, даже если input вернулся в нормальные условия.

ПРИМЕЧАНИЕ: *Это преимущество не будет работать, если произошел обрыв связи между контроллерами и Global Шлюз.*

Конфигурация выходов (выходных устройств)

Выходы, как правило, управляют светодиодным индикатором и зуммером на считывателях. Контроллеры типа KT-200, KT-300 имеют по четыре выхода (по 2 на одну дверь), контроллеры KT-400 имеют по 16 выходов (по 4 на одну дверь). KT-100 отслеживает статус двух выходов.

Электрические выходы имеют конфигурацию с открытым коллектором. В деактивированном состоянии они создают разомкнутый контур (не подсоединены к заземлению), а в активированном состоянии соединены на землю. Выходные устройства можно настроить через меню Controller (Контроллер) или меню Gateway (Шлюзы).

Назначение общих параметров выходов (раздел Output)

1 В окне Devices (Устройства) нажать иконку **Output** (Выходы).

ПРИМЕЧАНИЕ: *В случае использования системы KT-400 раздел Miscellaneous (Прочее) не показывается, так как его параметры уже описаны в разделе Gateway (Шлюзы), закладка KT-400 events (События KT-400).*

2 Указать, какие физические компоненты связаны с выходами для выхода: шлюз, сайт/луч, контроллер.

3 В выпадающем списке **Output** (Выходы) выделить выход, конфигурацию которого необходимо настроить.

4 Указать режим работы выходного устройства в поле **Operating mode** (Рабочий режим) (по умолчанию установлен режим Normal):
- **Normal** (Стандартный) – выход заземляется при активации.
- **Inverse** (Обратный) – выход размыкается (не заземляется) при активации.

5 IB разделе **Selected doors** (Выбранные двери) указать, какая дверь будет оказывать влияние на выход/output, который вы настраиваете.
- **First door** (Первая дверь) – только порт первой двери будет отслеживать статус, указанный для этих событий.
- **Second door** (Вторая дверь) – только порт второй двери будет отслеживать статус, указанный для этих событий.

ПРИМЕЧАНИЕ: *Эта функция недоступна для контроллеров типа KT-100 и KTES.*

6 Указать задержку на период активации в поле **Activation period (m:ss) delay**. Это время активации в секундах, в течение которого выход остаётся активным, если он запрограммирован на временную активацию. При выборе значения "e" выход будет всегда оставаться активным, независимо от типа активации. Значение от 1 сек. до 4 мин. 15 сек. по умолчанию 5 сек.

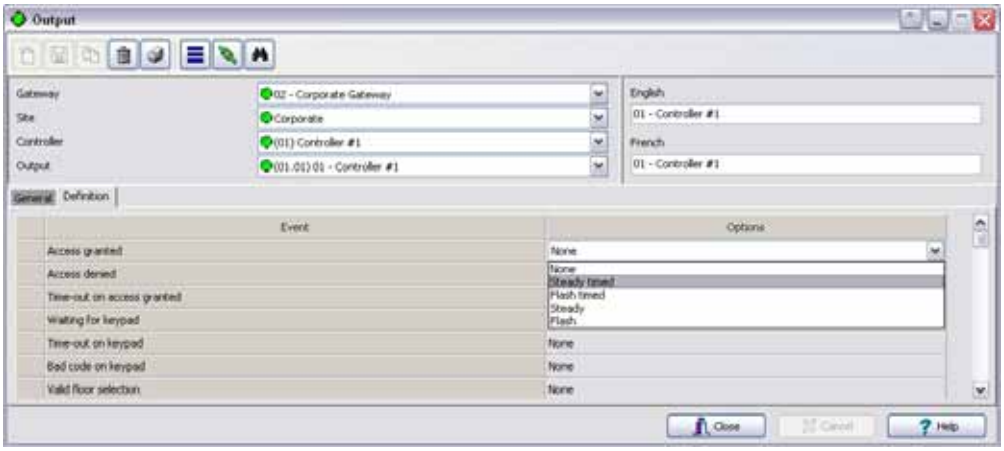
ПРИМЕЧАНИЕ: *Эта опция недоступна для контроллеров KT-400 и KTES.*

ПРИМЕЧАНИЕ: *В случае интеграции с системами видеонаблюдения (функция Video Integration) программное обеспечение EntraPass позволяет назначить все компоненты системы вывести на видеоокно, таким же образом, как это выполняется для интерактивных поэтажных планов (графических схем). Для этого нужно просто выделить видеоокно, где необходимо разместить компонент системы (рабочая станция, сайт/луч, шлюз, контроллер и др.).*

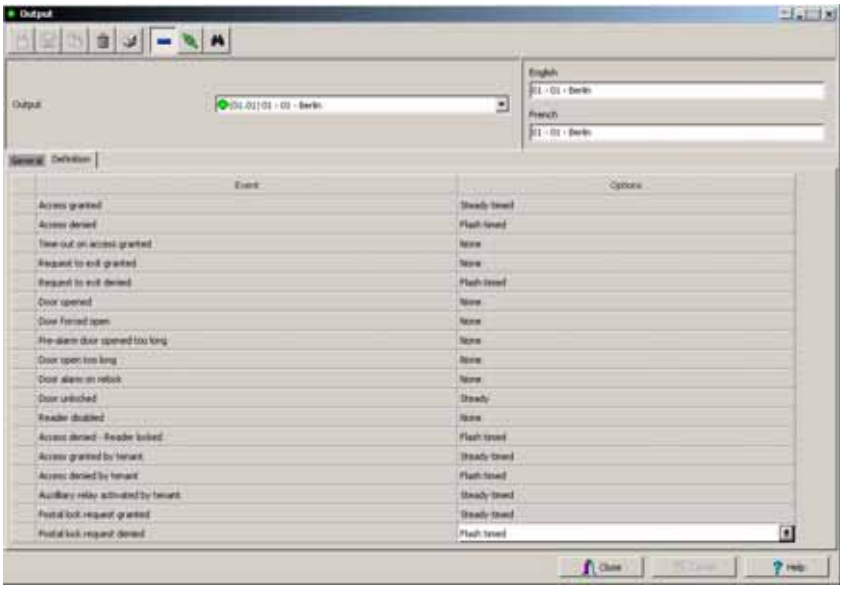
Установление связей событий дверей с дополнительными выходами

Системные события могут вызывать срабатывание дополнительных выходов. Для этого необходимо указать, каким образом каждое событие должно вызывать срабатывание настраиваемого выхода.

1 Открыть закладку **Definition** (Назначения), чтобы установить связь события двери с дополнительным выходом.



Назначение выходов для KTES



2 В колонке **Options** (Опции) привязать событие к состоянию выхода. По умолчанию **HET/None.**

- **Steady timed** (Ровная работа, ограниченное время) – настраиваемый выход не будет мигать; он будет оставаться активным в течение определённого времени активации и вернётся в нормальное состояние после окончания этого времени.
- **Flash timed** (Мигание, ограниченное время) – настраиваемый выход будет мигать; он будет оставаться активным в течение определённого времени активации и вернётся в нормальное состояние после окончания этого времени.
- **Steady** (Ровная работа) – настраиваемый выход не будет мигать, он будет оставаться активным, пока не input вернётся в нормальное состояние.
- **Flash** (Мигание) – настраиваемый выход будет мигать, он будет оставаться активным, пока input не вернётся в нормальное состояние.

ПРИМЕЧАНИЕ: *Задержки включения-выключения для выходов указывают при назначении шлюза. Подробнее, см. "Настройка конфигурации шлюзов EntraPass" на стр. 85. События для включения-выключения таймера зависят от типа выбранного шлюза. Шлюз NCC-8000 поддерживает до 16 событий, Corporate Шлюз поддерживает до 34 событий и Global шлюз поддерживает до 22 событий.*

Настройка интегрированной панели охранной сигнализации

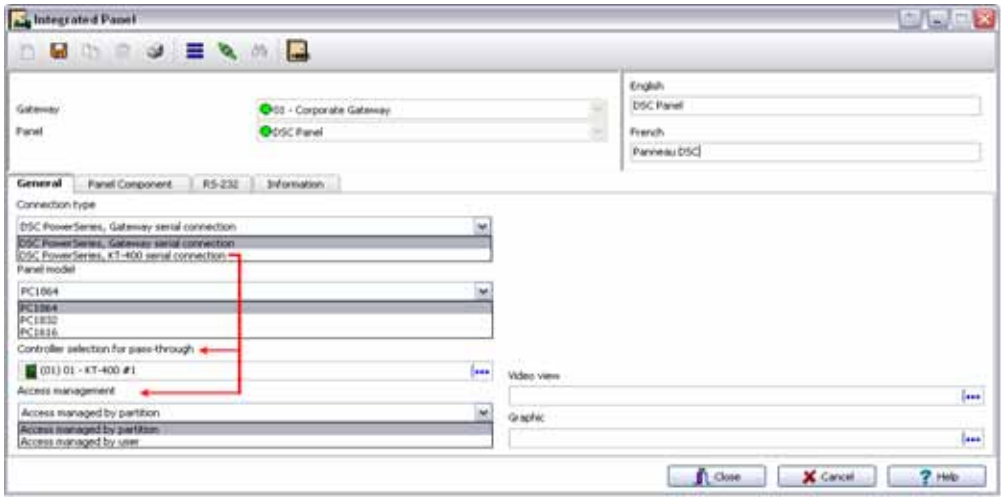
Минимальные требования для просмотра и использования интегрированных кнопок

- DLL для интеграции должна быть загружена на **EntraPass Server**. Если панель инструментов не отображает две кнопки, см. в Главе 14 Интеграция на стр. 496.
- Оборудование третьих компаний должно быть подсоеденено на serial порт **Corporate Шлюза** или к serial порту через контроллера KT-400.
- Оборудование третьих компаний должно быть включено (**powered up)**.

Процес интеграции разделен на три части:

- С панели инструментов **Devices (Устройства)> Integrated Panel (Интегрированная панель)**— Назначить **connection type** (Тип соединения), **panel model** (режим панели), **communication port** (порт связи), **virtual keypad** (виртуальный пульт) и partition\s (разделы/Зоны) долэжны быть назначены.
- С панели инструментов **Devices** (Устройства) **> Integrated Component** (Интегрированный компонент)— Типы компонентов назначены.
- Из панели инстурументов **Operations** (Работа) **> Integrated Panel** (Интегрированная панель)— в Главе 7 Ручные управление над интегрированными панелями на стр. 280.
  - Устройство настроенное через Virtual Keypad (Виртуальный пульт).
  - Раздел/зона может быть:
    - Arm away -
    - Arm stay -
    - Arm no entry delay - поставить на охрану без задержки на вход
    - Arm with code - поставить зону на охрану с кодом
    - Disarm partition - снять зону с охраны

1 Из панели инструментов **Devices** (устройства), выберите иконку **Integrated Panel** (интегрированная панель).



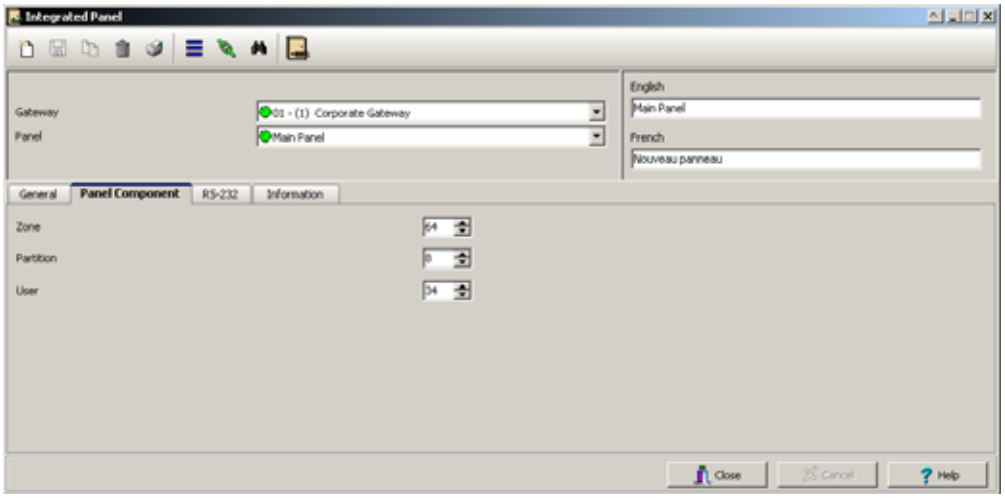
2 Нажмите на кнопку **New** и назначьте имя на обоих языках.
3 По умолчанию, Шлюз это **Corporate Шлюз**. Выберите тип панели из выпадающего списка.
4 Выберите тип соединения (**Connection type)**: **Gateway/Шлюз** или **KT-400**.
5 Выберите режим панели (**Panel model**).
6 Если вы имеете ранее выбранную **DSC PowerSeries, KT-400 serial selection** (прямое соединение через KT400) из **connection type** (тип соединения), то вы должны сейчас выбрать через какой именно контроллер данное подключение будет происходить.
7 Если вы ранее выбрали **DSC PowerSeries, KT-400 serial selection** для **connection type**, вы должны сейчас выбрать **access management** (управление доступом).

ПРИМЕЧАНИЕ: *Когда выбираете* ***Access managed by user*** *(управление доступом от пользователя), то панель, названная* ***Intrusion*** *(охранная), будет становится доступной панели* ***Users*** (Пользователи) ***> Card (Карта).***

8 Если вам доступна интеграция с видео, появится поле **Video view** (Вид видео). В этом случае, выберите Video view в который вы хотите чтобы появился выбранный компонент. Для деталей см, *в Главе 6 Назначение окон видео VideoView на стр. 228*.

9 Из списка **Graphic,** вы можете выбрать график, в который назначено приложение EntraPAss. Для детелей см, *в Главе 5 Graphics Definition на стр. 199*.

10 Выберите пункт **компоненты панели** (**Panel Component**).



- **Auto-detection** (автоматическая детекция): раздел и название зон автоматически появится на панели.

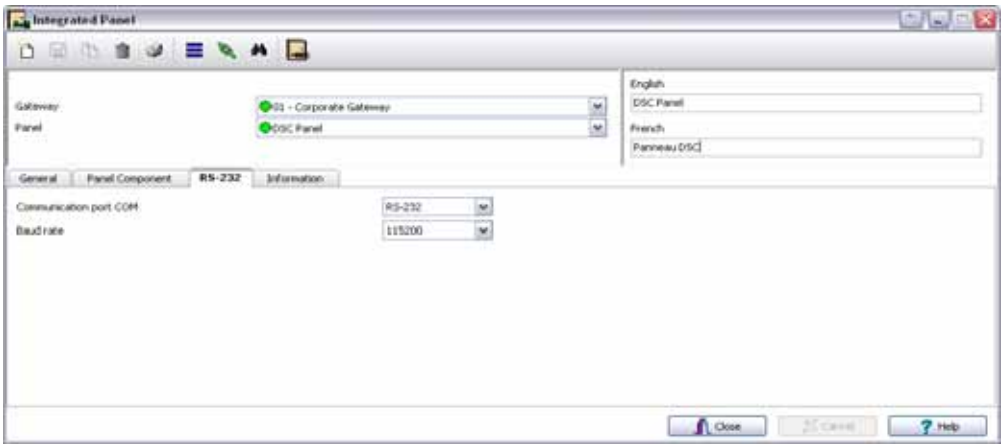
ПРИМЕЧАНИЕ: *Это преимущество зависит от типа охранной панели. Устройство, должно быть создано в EntraPass, DLL должна быть загружена в соотвествующий Шлюз или KT-400. После загрузки, автоматическая детекция станет активна.*

11 Назначение **Zone**, **Partition** и **User**. (Назначение зон, разделов и пользоватлей).

- Эти параметры имеют следующие максимальные значения:

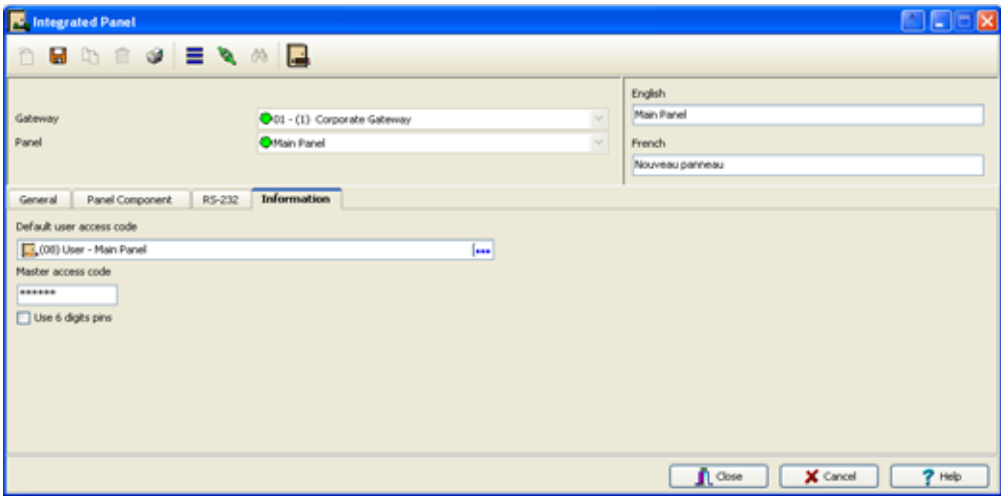
Параметр	PC1616	PC1832	PC1864
Кол-во зон	32	32	64
Разделы	2	4	8
Пользовател и	48	72	95

12 Выберите вкладку **RS-232**.



13 Выберите **Communication port COM** (com порт связи) и **Baud rate** (скорость передачи) из выпадающего списка.

14 Выберите вкладку **Information** (информация).



15 Выберите пункт **Default user access code** (код доступа по умолчанию). Этот код, используемый оператором Kantech для снятия/постановки на охрану из дисплея оператора. Этот код обеспечивает полный доступ для всех функций.

ПРИМЕЧАНИЕ: *Это не может быть сделано, когда вы создаете новую систему. Это должно быть сохранено, после настройки самой панели DSC.*

16 Введите **Master access code** (Master код). Этот код используется для загрузки информации от панели в систему EntraPass.

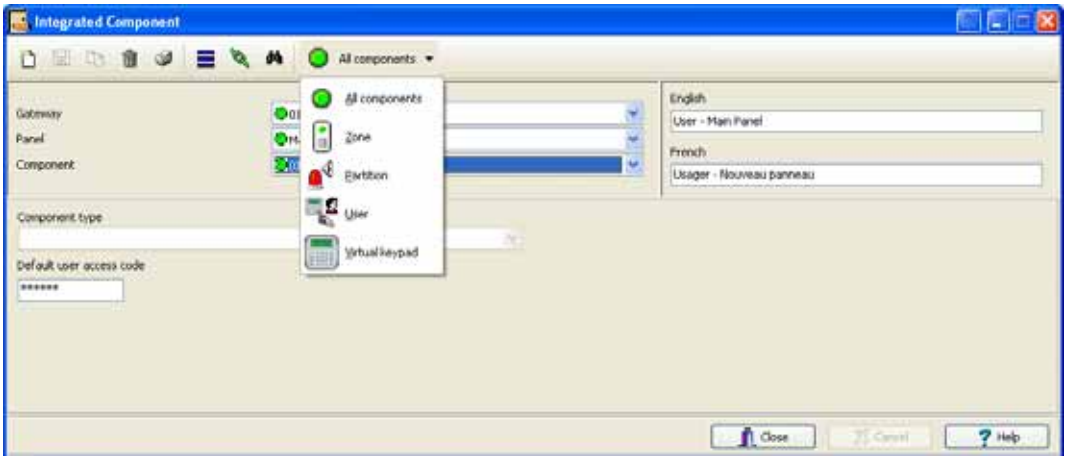
17 Выберите **Use 6 digits pins** (использовать 6-ти цифровые клавиши) для введения Master access code (Master кода).

18 Нажмите **Save/сохранить**.

Интегрированная настройка компонентов

На вкладке **Integrated Component** (интегрированный компонент) вы можете увидеть любой из компонентов панели (раздел, зона, итд), предварительно выбрав тип панели (охранная, контроль температуры,...итд).

1 Из панели инструментов **Devices** (устройства), выберите иконку **Integrated Component** (интегрированные компоненты).



2 Выберите **Panel** (Панель) из выпадающего списка, затем выберите **Component** (компонент).

ПРИМЕЧАНИЕ: *Вы можете использовать выпадающее меню, чтобы выделить необходимый компонент.*

3 Выберите **Component type** - тип компонента.

4 Введите **User access code** (код доступ пользователя) (используемый для типов компонентов пользователя). Этот PIN код используется для снятия/постановки раздела.

5 Если доступна Интеграция Video, появляется окно **Video view**. В этом случае, выберите Video view в который вы хотите определить компонент. Для деталей по назначению Видов видео смотрите, *в Главе 6 Назначение окон видео VideoView на стр. 228*.

6 Из списка **Graphic** (График), вы можете выбрать график, в который назначено приложения EntraPass. Для деталей, см. *в Главе 5 Назначение графических схем на стр. 195*.

7 Нажмите **Save/сохранить**.

8 Для более полной информации смотрите в Главе 7 Ручные управление над интегрированными панелями на стр. 280.

Глава 5 • :Назначения

Панель инструментов Definition (Назначения)

В панели инструментов **Definition** (Назначения), операторы могут назначать логические компоненты системы, такие как:

- Расписания
- Тревожная система (Alarm systems)
- Области
- Тур обхода охранником - Guard tours
- Этажи
- Раздел События/Действия (Event relays)
- Графические схемы
- Праздничные дни
- Task Builder - сервис построения команды действия для SmartLink
- Event Trigger - Реакция действий на событие

Назначение расписаний

Расписание указывает системе, когда выполнять определённые операции, включая автоматическую разблокировку дверей, предоставление доступа посетителям, создание автоматических отчётов, мониторинг входов и др. Кроме того, от расписания зависит, когда высылаются уведомления о событиях или когда активируются реле, выполняющие различные функции (освещение, обогрев и т.п.). Одно и то же расписание может использоваться в разных меню, но рекомендуется создавать отдельное расписание для каждого приложения, потому что таким образом проще изменить одно из расписаний, не затрагивая остальные приложения.

Каждое расписание состоит из четырёх интервалов. Каждый интервал имеет время начала и время окончания. Каждый интервал можно выбрать индивидуально для каждого из семи дней недели и для четырёх праздничных дней. Система EntraPass позволяет запрограммировать 99 расписаний на Шлюз и неограниченное число системных расписаний. Для этого следует активировать опцию **Upgrade to advanced schedule capability** (Обновить до улучшенных характеристик расписания) в окне **System parameters** (Системные параметры), меню **Option** (Опции).

ПРИМЕЧАНИЕ: *Более подробная информация см. в Главе 14 'Настройка параметров системы' на странице 480.*

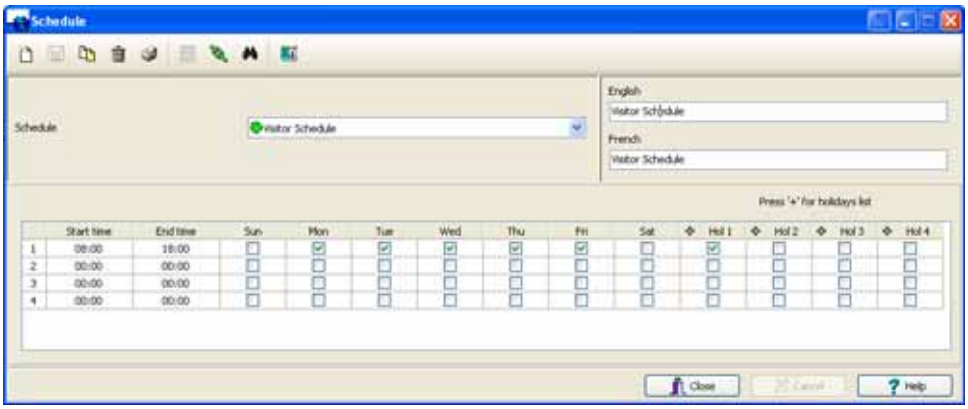
Система EntraPass поддерживает три группы расписаний одну группу расписаний:

- **System schedules** (Системные расписания) – выполняют глобальные функции, например, параметры событий, расписания регистрации операторов и события, инициирующие включение-выключение видеозаписи. Эти расписания не загружаются в контроллеры.
- **Global schedules** (Глобальные расписания): Глобальные расписания сгруппированы по Шлюзу. Они определяются на глобальный Шлюз. Вы можете назначить до 99: реле, вторичный уровень доступа, тревожные системы, области, тур обхода охранников guard tours и контроль лифта.
- **Corporate site schedules** (Corporate расписание для луча/сайта) – отдельные расписания для каждого сайта/луча. Для каждого сайта/луча в версии Corporate можно создать до 99 расписаний следующего назначения: расписание контроля подачи питания (на контроллеры), расписание разблокировки (дверей), расписание кнопок запроса на выход REX (двери), режим активации (реле), расписание мониторинга (за входами).

Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для APM, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт.

Назначение расписания

1 В главном окне EntraPass открыть закладку **Definition** (Назначение). На панели инструментов **Definition** (Назначение) нажать кнопку **Schedules** (Расписания).



ПРИМЕЧАНИЕ: *Если был поставлен флажок напротив опции* ***Upgrade to advanced schedule capability*** *(Обновить до улучшенных характеристик расписания) в меню* ***System parameters*** *>* ***Server*** *>* ***Schedule****, то появляется выпадающий список* ***Gateway/Site*** *(Шлюз/Сайт(Луч)). В списке* ***Gateway/site (Шлюз/луч)****, выбрать* ***Gateway*** *(Gobal луч) или, выберите* ***Site*** *(Corporate site/луч) или* ***System schedule*** *(Системное расписание), , (применимое к системным компонентам типа параметров событий, реакция на события видео, регистрация операторов).*

2 В выпадающем списке **Schedule** (Расписания) выбрать расписание, которое необходимо изменить или указать расписание для выбранной перед этим категории или нажать кнопку **New** (Создать), чтобы создать новое расписание.

3 Назначить для этого расписания имя (или изменить уже созданное). Рекомендуется подобрать подходящее по смыслу имя.

4 Нажать иконку **Holiday** (Праздничные дни) на панели инструментов, чтобы просмотреть список праздничных дней, заданных в системе.

ПРИМЕЧАНИЕ: *Система EntraPass поддерживает четыре типа праздничных дней.*

5 Указать начальное время в поле **Start time** – это запланированное время, когда интервал становится достоверным. Интервал перестанет быть достоверным после наступления времени окончания.

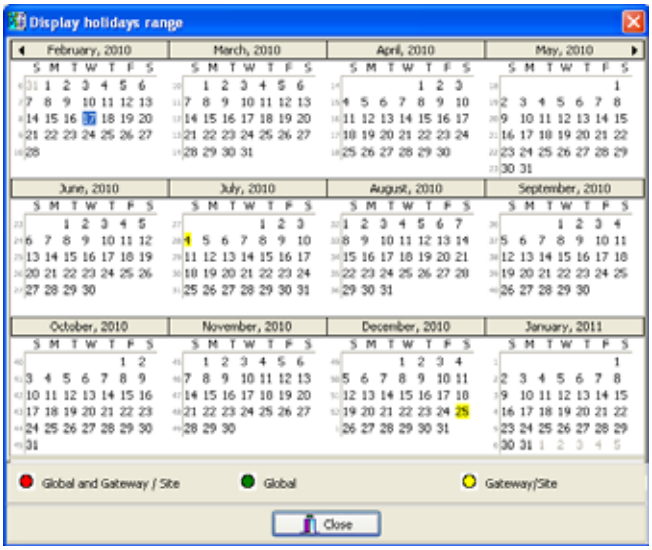
6 Указать время окончания в поле " **End time** – это запланированное время, когда интервал прекращает быть достоверным.

ПРИМЕЧАНИЕ: *Время начала и время окончания указываются в 24-часовом формате, то есть от 00:00 до 24:00. Для любого интервала время окончания должно быть больше, чем время начала.*

7 Указать, в какие дни недели это расписание будет достоверным. Для этого поставить галочку в поле под каждым днём недели.

8 Отметить тип праздничных дней (**Hol1, Hol2** и т.д.), если в меню описания праздников (Holiday definition) уже определены четыре типа праздников, и данный интервал расписания должен быть достоверным в праздничные дни. Вы можете также нажать на +sign (назначить) чтобы отобразить

календарь в течении следующих 12 месяцев. Данный календарь показывает каникулы при помощи трех цветов, определяющих ссылку.

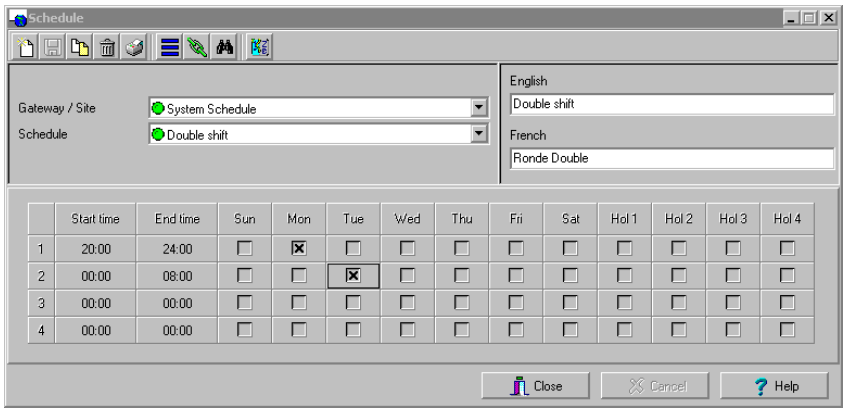


ПРИМЕЧАНИЕ: *Ссылка (legend) - это различие для назначения праздничных дней. Для большей информации смотрите "Назначение каникул" на странице 203.*

Создание двухдневного интервала

Чтобы создать интервал с понедельника, 20:00 по вторник, 08:00, необходимо разделить расписание на два интервала:

1 Первый интервал должен быть в понедельник с 20:00 по 24:00;



2 Второй интервал будет во вторник, с 00:00 до 08:00. Система будет рассматривать эти два интервала как единый интервал.

Назначение тревожной системы (Global/KT-NCC/NCC 8000)

Тревожный раздел (alarm partition) - это сборка устройств и оборудования, предназначенного для сигнализирования и определения присутствия в охраняемой зоне. Данная реакция предполагает незамедлительное привлечение вниманиет оператора или запрос на подтверждение тревоги со стороны оператора. Система предлагает до 100 виртуальных тревожных разделов на шлюз. Виртуальный тревожный раздел - тревожный раздел, который полностью контролируется шлюзом, вместо использования дополнительного оборудования для использования этой функции. В зависимости от тогоТртр как виртуальные тревожные раделы запрограммированы, они могут вызывать различные реакции реле/выходов.

Пример тревожного раздела

Система будет способна собирать в раздел различные области здания в 100VASP (Virtual Alarm System Partition)(Виртуальный тревожный системный раздел). Каждый раздел VASP может быть установлен с использованием любого количества считывателей, дверных контактов, детекторов движения, сирен и прав достпа пользоватлей. Контролируемые входы могут быть использованы одновременно в нескольких разделах.

Operation - работа

Каждая область может быть разделена при помощи дверей, оборудованных считывателями и дверными контактами. Двери с одним считывателем могут быть также оборудованы устройством запроса выхода (T-REX) для обеспечения hands-free выхода. Как необходимо для службы безопаснсоти область разделяется, VASP будет контролировать в сумме все эти устройства: считыватели, дверные контакты, детекторы движения, контроль температуры в помещении, предупреждение о задержке на выход и дверные замки.

Постановка/Снятие с охраны, Отсрочка постановка на охрану

Каждый VASP может быть настроен с расписанием автоматической постановки на охрану на каждый день недели, включая каникулы. В запрограммированное время постановки на охрану, предупреждение о задержки на выход будет предупреждать звуком в течении минимум 4 минут. Любой работник в области, кому не позволительно находится в области более чем время постановки, должен покинуть эту область. В конце задержки на выход область будет ставится на охрану и область будет контролироваться для охраны и на различные изменения самих датчиков. В течении задержки на выход, если авторизованный работник хочет оставаться в защащаемой области более чем время постановки на охрану, то работник может использвать карту. Карта может быть приложена к любому считывателю в области, назначенному как считыватель для отложения режима постановки на охрану. Этот режим будет инизиализировать режим отложения постановки на охрану в системе. Задержка на отложение по постановке на охрану (postponement delay) может быть запрограммирована для каждой области в отдельности и составлять до 18 часов 12 минут. После режима **отложение постановки на охрану** система будет предпринимать попытку поставить снова систему на охрану. Будет вновь звучать сигнал запуска задержки на выход. Такой же сценарий отложения по постановке на охрану может быть примененен снова, если не превышен лимит количеств отложений постановок на охрану и до тех пор пока не включилось расписание “no disarm” **не ставить на охрану**. Каждая карта в системе может быть запрограммирована, что позволять или ограничивать использовать данную функцию.

Когда область находится на охране, она может быть снята с охраны авторизированным картодержателем (кто имеет права снимать данный раздел с охраны), при помощи прикладывания своей карты к назначенному считывателю, предназначенному для снятия с охраны. Если картодержатель авторизовался в этой области в течении назначенного времени, дверь будет разблокироватся и раздел будет снят с охраны после того как картодержатель откроет дверь. Если произошло снятие с охраны в течении времени, когда по расписанию необходимо произвести автоматическую постановку на охрану, то система будет пытаться автоматически перевзять на охрану после истечения времени отложения при постановке на охрану. В дополнение к тем задачам, которые выполнены картодержателем, авторизированный оператор (такой как охранник) может в ручном режиме управлять разделами с рабочего АРМ (снимать/ставить на охрану, изменять время отложения при постановке на охрану).

Способности Тревожной системы

- До 100 независимых тревожных разделов может быть запрограммировано на шлюз.

- Каждый тревожный разделможет контролировать любое количество входов или дверей в системе.
- Когда назначаете тревожные разделы, элементы такие как: двери, считыватели, входные зоны и реле, которые могут быть назначены в группы и в отдельности.
- Каждый тревожный раздел может включать входы/inputs или двери, контролируемые одним или несколькими разделами как общие элементы.

ПРИМЕЧАНИЕ: *Если один и тот же вход определен сразу в два раздела, и только один раздел поставлен на охрану, то тревога по этому входу не будет провоцировать общую тревогу по разделу. Должны быть поставлены на охрану оба раздела, тогда тревога по входу появится в отчете.*

Общие входы (inputs)

Входные зоны или двери, которые настроены для использования с несколькими тревожными разделами, используют следующие праивла:

- Тревожный раздел будет производить тревогу от входа (input), двери на другие разделы, если все тревожные разделы, содержащие даный input/дверь, поставлены на охрану. Входы или двери - которые являются частью “Alarm level 1 и 2” могут быть назначены различными путями в раздел, но быть частью одной группы.
- Alarm level 1 и 2 (Группы входов **input groups**) рассматриваются системой как одна большая группа для целей определния состояния входа. Данные входы могут также быть включены в другой раздел.
- Общие двери, которые обозначеннные как “Door to be locked on arming” (Дверь запирается при постановке на охрану) или “Door disabled on arming” (Дверь отключена при постановке на охрану) в двух тревожных разделах, то двери будут возвращаться в нормальное состояние если один или более из этих тревожных разделов снят с охраны.

Объемные извещатели и извещатели периметра

Устройства тревожной системы сгруппированы в две категории: извещатели периметра и объемные извещатели.

Perimeter (извещатели периметра) (Alarm Level Inputs - уровень тревожных входов)

Извещатели периметра отражают детектирования сигнала вторжения в охраняемую зону при помощи физических барьеров: дверные контакты, детекторы разбития стекла, дверные контакты на неохраняемых дверях.

Обычно, входы, назначенные как “perimeter” (датчики разбития стекла, гаражные двери, пожарные двери, дополнительные двери необорудованные ACCESS итд) группируются и назначаются как “alarm level #1 inputs” (входы, уровень №1). Когда один из этих входов активируется, тогда будет активировано “alarm relay #1” (тревожное реле №1). Данное реле может быть подключено тревожной панели, которая будет посылать сообщение о событии вторжения. Детекция на периметре рассматривается более важной областью с большим приоритетом по сравнению с внутренней контролируемой областью. Для контролируемых дверей (считыватель, T.REX, дверной контакт), вы можете использовать поле **“Supervised door”** (контролировать дверь), когда группа дверей будет ставится на охрану. При срабатывании будет также активироваться “alarm relay #1”, когда дверь будет принудительно открыта или “door open too long” (дверь открыта слишком долго). Например, главные двери входа/выхода могут быть также включены в это поле.

Volumetric (Объемные извещатели)(Alarm Level # 2 Inputs)(Тревожные входы, уровень №2)

Объемные извещатели показывают сработку внутри охраняемого помещения, такого как целая комната или часть комнаты. В основном, это такие извещатели как: объемные детекторы движения, контроллируемые двери внутри охраняемой области (считыватели итд). Данные извещатели группируются и обозначаются “alarm level # 2 inputs” (тревожные входы, уровень №2). Когда активируется один из этих входов, то будет активировано реле “alarm relay #2”, которое может быть соеденено к “alarm panel” (тревожной панели), которая будет посылать сообщения на центральную станцию о сработке объемных извещателей.

Процедура постановки на охрану

Существует три метода постановки на охрану:

1. **Manual arming** (Ручная постановка на охрану): Это обычно делается с окна APM авторизированным оператором. Тревожная система встанет на охрану после истечения задержки на выход.
2. **Automatic arming** (автоматическая постановка на охрану по расписанию): Тревожный раздел будет инициировать задержку на выход, когда наступит соответствующее время по расписанию. Раздел будет поставлен на охрану после истечения этой задержки.
3. **Arming at a door reader** (Постановка на охрану при помощи считывателя с/без использования дополнительной кнопки): Возможны три варианта:
   - **With a card** (При помощи карты)—Необходимо поднести соответствующую карту к считывателю, назначенному как “arming reader” (считыватель для постановки на охрану). Когда истечет задержка на выход, то раздел будет поставлен на охрану.
   - **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.
   - **Только с использованием “arming request input”** (кнопка запроса на постановку на охрану)— “arm request input (button)” должна быть нажата для инициирования процеса постановки на охрану. После того как вы нажмете кнопку запроса на постановку на охрану, включится режим задержки на выход, по истечении которой раздел будет поставлен на охрану. Если вы используете “arming request input”, нет необходимости использовать считыватель для постановки на охрану.

ПРИМЕЧАНИЕ: *Процес постановки на охрану представляет из себя прикладывание карты к определенному считывателю (или ввод код на клавиатуре/keypad), назначенному в качестве “arming reader” (считыватель постановки на охрану) в меню назначения тревожной системы. Постановка на охрану через считыватель предназначена только для соответствующего уровня доступа.*

Процедура снятия с охраны

Эта команда снимает тревожную систему с охраны. Возможны несколько вариантов снятие системы с охраны.

- **Manual disarming** (Ручное снятие с охраны): Это может быть сделано в ручном режиме с APM авторизированным оператором. Будет произведено сразу снятие с охраны, если в данный момент не запущено расписание “no disarm” (не снимать с охраны). Эта команда будет инициализировать задержку “postpone” (отложить).
- **Disarming at a door reader** (снятие с охраны при использовании карты): Снятие с охраны произойдет, если пользователь приложит свою карту к назначенному считывателю/клавиатуре, назначенному в системе как “disarming reader” (считыватель для снятия с охраны).

Общие правила:

- Снятие с охраны выполняется при помощи прикладывания карты к считывателю (или вводом кода на клавиатуре) на считывателе, назначенным как “disarming reader” в меню назначения тревожной системы.
- Ручное снятие с охраны разрешено при помощи карты с назначенным соответствующим уровнем доступа (disarming access level). Данная карта должна иметь доступ к этому считывателю.
- Если там дверной контакт, назначенный для этой двери, тогда дверь должна быть открыта для того чтобы произошло снятие с охраны. Если вы приложили карту, а дверь не открыли, тогда снятия с охраны не произойдет.
- Считыватель для снятия с охраны должен быть назначен в качестве “disarming reader”, необходимо будет открыть дверь, чтобы снять систему с охраны. С другой стороны, если действует расписание “no disarm” (не снимать с охраны), то тогда будет включен режим откладывания постановки на охрану “postpone”, по истечении этого режима включится задержка на выход.

Снятие с охраны, когда по расписанию действует режим “No Disarm”

Если действует расписание “no disarm” (не снимать с охраны) и пользователь снял систему с охраны, тогда будет включен режим “postpone delay” (задержка по отложению на постановку). По истечении данной задержки, система включит задержку на вход, по истечении которой система сама встанет на охрану, если расписание “no disarm” все еще действуее. В случае ограничения количества отложений на постановку “postpone”, это оказывает влияние только после начала задержки. Постановка на охрану тревожного раздела может быть отложена на

предустановленный период (максимум 16.5 часов) после которого система будет автоматически ставится на охрану, только если не включено расписание “no disarm”.

Процедура отложения постановки на охрану

Режим отложения постанови на охрану может быть активирован в двух случаях, зависимо от обстановки:

1. В течении задержки на выход (когда система находится в режиме постановки на охрану, в ручном или по расписанию).
2. Система стоит на охране, и действует расписание “no disarm”. При снятии системы с охраны автоматически будет включаться режим отложения постановки на охрану. Количество отложений (postpone) не должно быть выше чем назначенное количество.

Примечание:

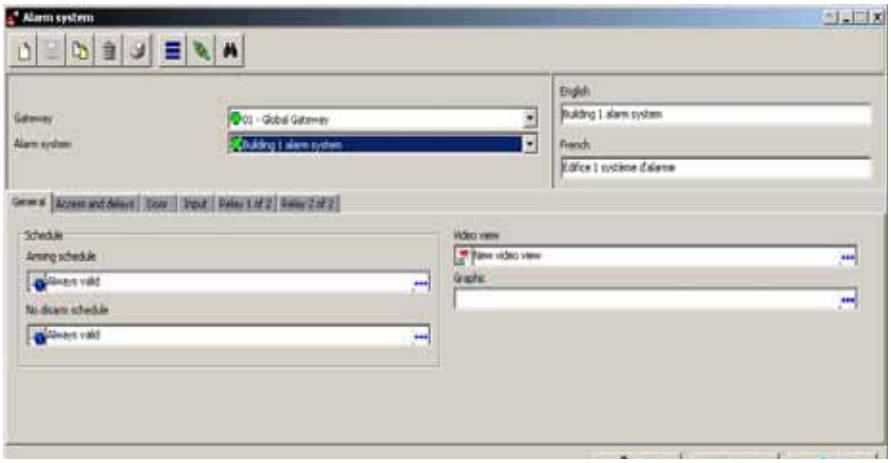
- В обоих случах, система будет автоматически ставить на о храну саму себя в конце режима задержки отложения (когда задержка отложения истечет, включится задержка на выход), только если расписание “no disarm” не действует в настоящее время.
- Отложенная постановка на охрану может быть активирована дверным считывателем, назначенным как “arming reader” (считыватель постановки на охрану) или как “postponing reader” (считыватель отложения постановки на охрану).
- Для считывателя двери, назначенного как “postponing reader”, вы можете включить режим отложения в течении действия задержки на выход.
- Для считывателя двери, назначенного как “disarming reader”(считыватель для снятия с охраны), вы можетете включить режим отложения “postpone” в течении задержки на выход или когда система поставлена на охрану и не действует расписание “no disarm”.
- Режим отложения постановки на охрану может быть активирован с картой имеющей статус “disarming access level” (уровень доступа для снятия), который должен иметь доступ к двери, с которой это будет активироавно.
- Режим отложения постановки на охрану может быть активирован в течении задержки на выход когда система находится в режиме постановки на охрану, также в течении действия режима отложения или когда система уже стоит на охране при действующем расписании “no disarm”.
- Если сделан запрос на отложения режима постановки на охрану, когда данный режим находится в процессе, то данная задержка будет сброшена и счетчик будет включен заново (если не достигнуто максимальное количество попыток отложения). Количество попыток отложения (0-15).

Внимание: Введение “0” в поле “postpone count field” (количество попыток режима отложения) будет являться причиной включения режима неограниченного количества разрешенных попыток.

- Должен считыватель быть назначен как BOTH (оба режима) для одновременной постановки и снятии с охраны для тревожного раздела, функция отложения может быть также включена на этом считывателе. Например, режим отложения будет включен незамедлительно на предоставленную карту.

Чтобы назначить тревожный раздел

1 Из выпадающего списка **Gateway**, выберите Шлюз, который относится к вашему тревожному разделу.

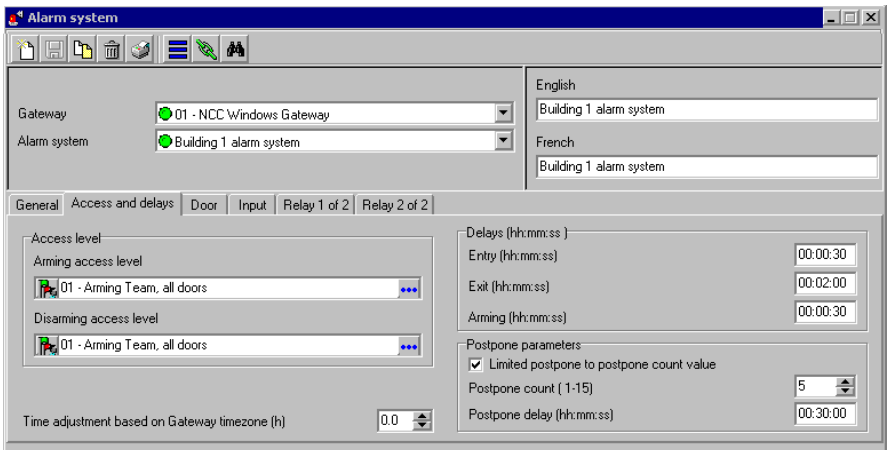


2 Из выпадающего списка **Alarm System** (тревожная система), выберите существующую тревожную систему или нажмите **New** для создания новой тревожной системы.

3 Из поля **Arming Schedule** (расписание постановки на охрану), выберите соотвествующее расписание в соотвествии с которым тревожный раздел будет автоматически ставится на охрану в течении указанного в расписании времени. Задержка на выход будет инициироваться до указанного времени постанвоки на охрану. Это расписание используется только для постановки систему на охрану. Не устанавливайте расписание “All valid” (можно всегда). Когда расписание станет неверным (закончится), система не будет сниматься с охраны. Система будет оставаться на охране до тех пор, пока верная карта не будет приложена к считывателю, предназначенному для снятия с охраны. вы можете нажать правой кнопкой мыши там. У вас появится возможность создать новое/другое расписание для постановки на охрану.

4 Из поля **No Disarm Schedule** (расписание не снимать с охраны), выберите расписание, в течении которого все попытки на снятие системы с охраны будут включать режим отложения на новую постановку на охрану этого тревожного раздела. После того, как задержка отложения на постановку закончится, система будет автоматически включать задержку на выход и ставить систему автоматически на охрану при ее истечении.

5 Выберите вкладку **Access and delays** (доступ и задержки), чтобы назначить опции уровней доступа:



- **Arming Access Level** (Уровень доступа для постановки на охрану): выберите требуемый уровень доступа для постановки на охрану тревожного раздела. Постановка системы на охрану требует соответствующего уровня доступа и предоставление данного уровня доступа на считыватель/и.
- **Disarming Access Level** (Уровень доступа для снятия с охраны): выберите требуемый уровень доступа для снятия с охраны тревожного раздела. Снятие системы с охраны

требует соответствующего уровня доступа и предоставление данного уровня доступа на считыватель/и.

6 В разделе **Delays (hh:mm:ss) (Задержки)**, укажите задержки на вход и на выход:

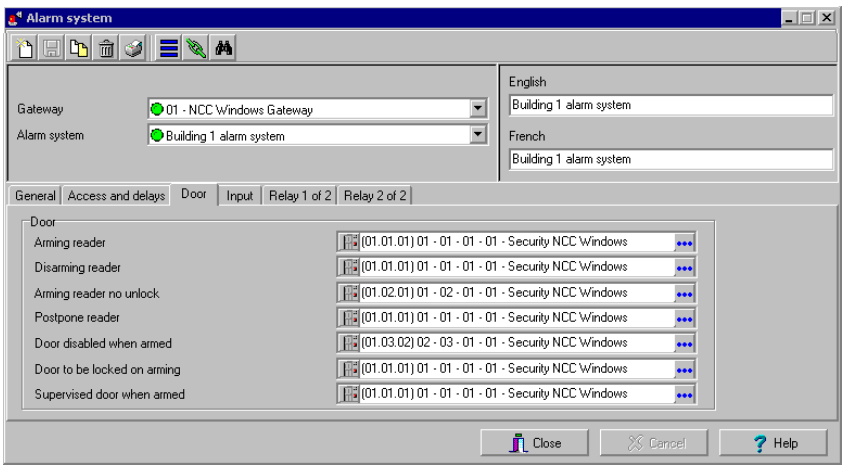
- **Entry delay** (Задержка на вход): укажите задержку на вход, в течении которой пользователь может попасть в контролируемую область для снятия системы с охраны.
- **Exit Delay** (Задержка на выход)— Введите задержку на выход. Задержка на выход используется чтобы поторопить работников покинуть помещение в течении указанного времени. По истечении этого времени система будет поставлена на охрану. Система попадает в режим задержки на выход в следующих режимах:
  - запрос на постановку на охрану,
  - или когда “postpone delay”(задержка отложения) заканчивается и расписание “no disarm” все еще действует.
- **Arming Delay**—Введите задержку на постановку на охрану. Это задержка, которая обеспечивается системой между моментом когда подносится карта для постановки на охрану и нажатием кнопки “arming request button” для подтверждения постановки на охрану.
- **Postpone Delay**—Введите задержку отложения постановки на охрану. Задержка отложения - это период в течении которого тревожный раздел снят с охраны.
  - Если действует расписание “no disarm”, система будет включать “exit delay” (задержку на выход) затем система встанет на охрану.
  - Если будет включена функция отложения или снятие с охраны в режиме действия задержки на выход, то система будет включать режим отложения постановки на охрану.
  - Если расписание “no disarm” недействительно, то система будет автоматически снимать с охраныв конце окончания задержки отложения.
  - Задержка отложения может быть изменена в ручном режиме через раздел: ручное управление системой.

ПРИМЕЧАНИЕ: *Возможно назначить связи с реле, которые будут включаться когда идет процесс постановки/снятия с охраны или включен режим отложения. Это помогает обеспечить вам обратную связь на панель состояния о текущем состоянии системы или для визуального подтверждения!.*

- **Postpone Count** (счетчик попыток режима отложения постановки)—Эта опция указывает максимальное количество попыток по отложению постановки). Когда достигается указанное значение, система будет включать режим задержки на выход и по истечению будет произведена автоматическая постановка на охрану (если не включено расписание “no disarm“) или снятие с охраны если действует нормальное расписание постановки на охрану.

ПРИМЕЧАНИЕ: *Если установлено значение “0”, то раздел может может быть отложен неограниченное количество раз.*

7 Выберите вкладку **Door** (Дверь) для назначения считывателей для снятия и постановки на охрану, и включение режима отложения:



- **Arming reader** (Считыватель для постановки на охрану)— Выберите дверь или дверную группу, которая будет использоваться для постановки на тревожного раздела на охрану.

Постановка на охрану будет работать только с **arming reader.** Для постановки на охрану требуется уровень доступа для постановки на охрану и доступ к этим считывателям.

ПРИМЕЧАНИЕ: *Обычно, считыватели для постановки на охрану используют считыватели вблизи выходных дверей.*

ПРИМЕЧАНИЕ: *Если вам необходимо ставить на охрану с одного считывателя более чем один раздел, используйте дополнительный вход “arming request input” для подтверждения.*

- **Disarming reader** (Считыватель для снятия с охраны)—Выберите дверь или дверную группу для снятия с охраны тревожного раздела. Режим снятия с охраны будет работать только со считывателями, предназначенными для снятия с охраны. Для снятия с охраны необходимо иметь соответствующий уровень доступа и доступ к этому считывателю.

ПРИМЕЧАНИЕ: *Обычно, считыватель, который предназначен для снятия с охраны, установлен внутри защищенной зоны. Например, считыватель для снятия с охраны может быть расположен перед дверью, где установлена камера.*

- **Arming reader no unlock** (Считыватель для постановки на охрану без разблокировки двери) — Выберите дверь или группу дверей, которая будет использоваться для постановки на охрану без необходимости разблокировать дверь.
- **Postpone reader** (Считыватель для режима отложения)—выберите дверь или группу дверей, которая будет использоваться для режима отложения постановки для тревожного раздела. Для включения режима отложения “postpone” необходим уровень доступа “снимающего с охраны”, который прикладывает карточку к считывателю, определенному как считыватель “postpone”(отложения). Считыватель для режима отложения может быть использован в течении задержки на выход.

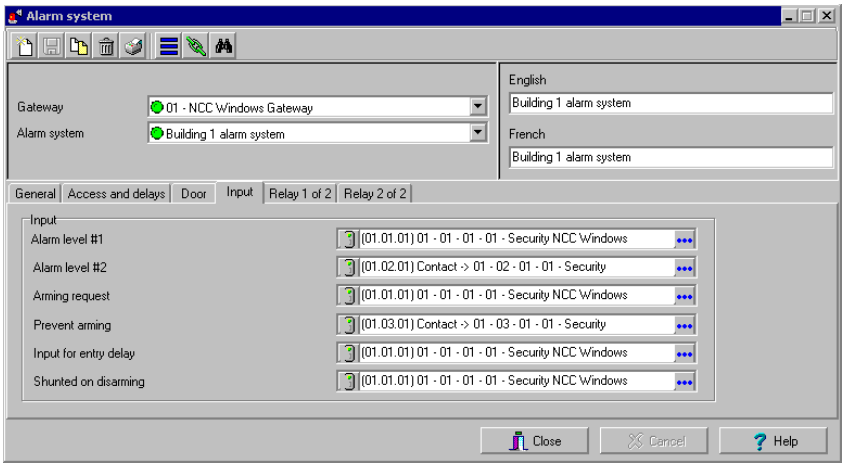
ПРИМЕЧАНИЕ: *Обычно, считыватель для режима отложения находится внутри защищаемой области, чтобы иметь возможность работникам отложить процес постановки на охрану.*

- **Door disabled when armed** (блокирование двери при постановке на охрану)—выберите дверь или группу дверей, которые будут блокироваться, когда раздел поставлен на охрану. Доступ в эти области запрещен даже тем людям, у которых уровень доступа для снятия с охраны.

ПРИМЕЧАНИЕ: *Например, это поле может быть использовано для выбора задней двери, чтобы посетители использовали переднюю дверь для снятия с охраны.*

- **Door to be lock on arming** (Закрытие дверей при постановке на охрану)—Выберите дверь или группу дверей, которые будут закрываться когда тревожный раздел поставлен на охрану. Эта функция будет перекрывать расписание разблокировки дверей. Также будет перекрыт режим ручного открытия двери.
- **Supervised door when armed** (Контроль двери когда система поставлена на охрану)—Выберите дверь или группу дверей, которая будет генерировать “Тревога уровень №1” (периметр) и включать реле выбранное в разделе **Alarm # 1 Relay State** (**Relay 2 of 2** вкладка). Если будут происходить события “door forced open”(дверь принудительно открыта) или “door open too long”(дверь открыта слишком долго), то будут генерироваться тревоги .

8 Выберите вкладку **Input** для назначения входа для постановки/снятия:



- **Alarm level #1 input** (Тревога, уровень№1)—Выберите один вход или группу входов, которые будут автоматически активировать выбранное реле **Alarm # 1 Relay State(реле тревога 1)** (**Relay 2 of 2** вкладка). Срабатывание реле произойдет, если система поставлена на охрану и сработает один из входов.
- **Alarm level #2 input**(Тревога, уровень№2)—Выберите один вход или группу входов, которые будут автоматически активировать выбранное реле **Alarm # 2 Relay State(реле тревога 2)** (**Relay 2 of 2** вкладка). Срабатывание реле произойдет, если система поставлена на охрану и сработает один из входов.
- **Arming request input** (дополнительный вход для постановки на охрану)—Выберите один вход или группу, активация которого будет подтверждать постановку на охрану раздела. Данный вход необходимо использовать, когда с одного считывателя ставите на охрану более чем один раздел. Обычно используется кнопка, как кнопка запроса постановки на охрану. После поднесения карты, включается задержка “arming delay” для нажатия кнопки. По истечении этого времени раздел встает на охрану.

ПРИМЕЧАНИЕ: *Это возможно связать реле, которое будет включаться приактивации режима “**arming delay**” (задержка на постановку). Это может являтся вам примером визуальной обратной связи на панель состояния. Это говорит о том, что система ожидает подтверждения.*

- **Prevent arming input** (Вход прерывания постановки на охрану)—Выберите один или группу контактов. Если один из этих контактов в тревоге, когда система пытается встать на охрану, тогда процесс постановки прервется. Обычно входа “Alarm Level 1 & 2” группируются вместе как одна группа и выбираются. Это правило работает при условии, что сделан запрос на постановку на охрану с сработкой дополнительного контакта “arming request input”.

ПРИМЕЧАНИЕ: *Если тревожный раздел ставится на охрану автоматически по распсианию, то данный пункт игнорируется. Постановка на охрану происходит в любом случае.*

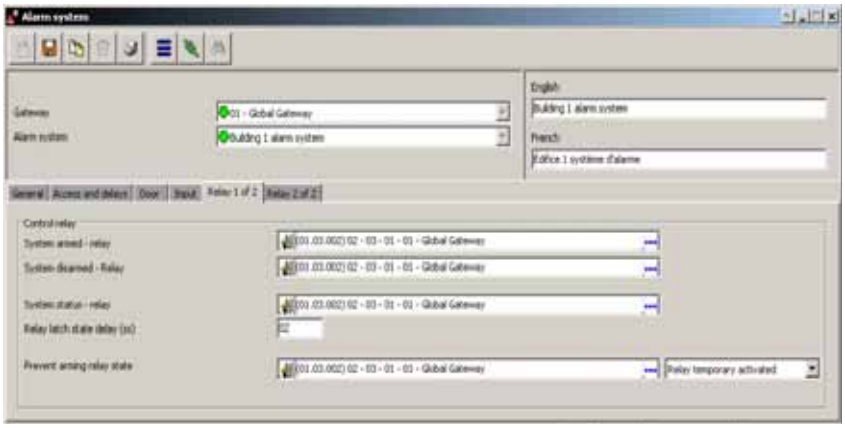
ПРИМЕЧАНИЕ: *Это возможно назначить связи с реле, которое будет включаться, когда произошло прекращение режима постановки на охрану.*

- **Entry input**(контакт на вход)—Выберите один или группу контактов, которые используются для включения задержки на вход. Если один из входов в тревоге, и когда система на охране, то будет включаться задержка на вход и входы/контакты в поле “Shunted on Disarming” будут шунтироваться на период действия задержки на вход.
- **Shunted on disarming** (шунтирование при снятии с охраны)—Выберите один или группу контактов, которые будут шунтироваться (маскироваться/не мониториться) когда сработает “Entry Input” (контакт на вход). Эти входа будут шунтированы в течении времени, указанному в графе “entry delay” задержка на вход.

9 Выберите вкладку **Relay 1 of 2** (реле 1 из 2) для назначения реле, которые будут использоваться для индикации и отображения различных состояний назначенной тревожной системы. Для каждого реле, это возможно определить когда реле будет возвращаться в норамльные условия. Там возможно назначение двух условий:

- **Temporary**(временная): Реле будет временно активированным в течении запрограммированного времени в разделе relay definition (назначение реле). Будте внимательны, если время активации реле установлено в 0 в меню назначения реле, то реле будет включаться на период действия входа.

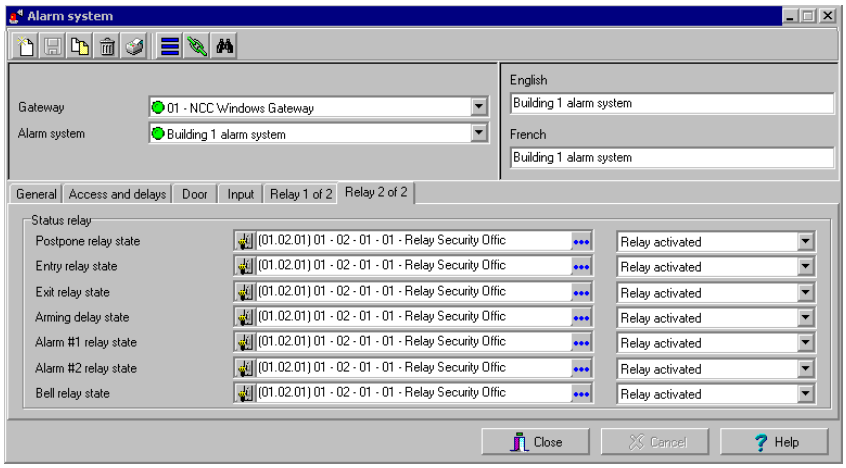
- **Follow** (Следящий): Реле будет оставаться активированным до тех пор, пока вход/input не изменит свое состояние.



ПРИМЕЧАНИЕ: Когда реле активировано/деактивировано из тревожной системы, то события не будут происходить.

- **System Armed—Relay** (система на охране - реле)—Это реле будет включаться когда раздел поставлен на охрану.
- **System Disarmed—Relay** (система снята с охраны - реле)—Реле будет включено когда система снята с охраны.
- **System Status Relay** (состояние системы-реле)—Реле будет отражать состояние входов “Alarm Level #1 и #2” также хорошо как в поле “Door supervised when armed” (контроль двери, когда система на охране).
- **Prevent arming Relay State**—(Состояние реле для прерывания постановки на охрану)Выберите реле, которое будет активироваться, когда процесс постановки на охрану прерван из-за тревоги по входу, кототрая пришла в процесе постановки систему на охрану. Выберите из выпадающего меню, активацию реле.

10 Выберите вкладку **Relay 2 of 2** (реле 2 из 2) для того чтобы назначить реле, которые будут отражат различные состояния определенной тревожной системы.



ПРИМЕЧАНИЕ: Когда реле активируются/деактивируются из тревожной системы, события не будут отправляться.

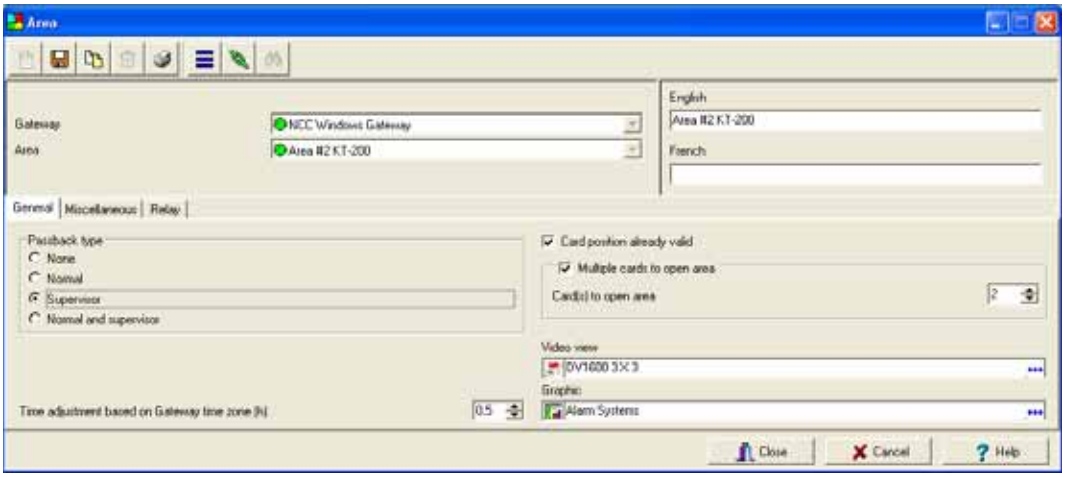
- **Postpone Relay(реле отложения)**—Выберите реле, которое будет активироваться, когда тревожный раздел находиться в режиме отсрочки.
- **Entry Relay** (задержка на вход - реле)—Выберите реле, которое будет активироваться, когда включится задержка на вход.
- **Exit Relay State**—(задержка на выход реле)Выберите реле, которое будет активироваться, когда включена задержка на выход.
- **Arming Delay State** (состояние задержки при постановке на охрану)—Выберите реле, которое будет активироваться, когда включен режим “arming delay” (ожидание включения дополнительного условия включения режима постановки на охрану).

- **Alarm #1 Relay State** (Реле - состояние Alarm#1)—Выберите реле, которое будет активировано, когда тревожный раздел детектирует тревогу по входу, от одного или группы входов, определенных в поле “Alarm Level #1” или от одной или более дверей (например, door forced open or door open too long), назначеннных в поле **Supervised door when armed** (контроллировать двери когда под охраной).
- **Alarm #2 Relay State** (реле - состояние Alarm#2)—Выберите реле, которое будет активировано, когда тревожный раздел детектирует тревогу по входу, от одного или группы входов, определенных в поле “Alarm Level #2
- **Bell-Relay state**(состояние звонок реле)—Выберите реле, которое будет активировано когда тревожный раздел детектирут тревогу по входу от одного или более входов, определенных к полю **Alarm Level #1** или от одной или более дверей (например, door forced open(дверь принудительно открыта) или door open too long(дверь долго открыта)) . Данные двери должны быть назначены **Supervised door when armed** (контролировать когда на охране). Обычно на это реле подключается звуковой оповещатель.

Назначение областей (Только Global/KT-NCC/NCC 8000 Шлюзы)

Области - это базовый пункт для использования режима Anti-passback. Области назначаются чтобы контролировать активность людей в области, внутри контроллируемых дверей. Под шлюзами Global, KT-NCC, NCC 8000 функция anti-passback целиком контроллируется шлюзом.

1 Выберите **Gateway** связанный с областью, которую вы хотите назначить. Затем выберите **Area** (Область) для изменения или для создания новой.



ПРИМЕЧАНИЕ: *Когда вы создали список карт, то карты будут автоматически перемещены в “unknown area” (неизвестную область).*

2 Назначить тип контроля повторного прохода **Passback type,** применимо к назначаемой области:

- **None** (Нет)—Функция anti-passback выключена, область назначена для доступа в область. Если вы хотите запретить функцию passback в течении какого-либо времени, используйте поле **Disable passback schedule** (расписание запрета действия запрета повторного прохода) на вкладке **Miscellaneous** (прочее).
- **Normal (hard/жесткий anti-passback)—**Это рассматривается как жесткий **anti-passback.** Это значит что доступ предоставляется и контролируется. Обычно, двери (считыватели) связывают области между собой. Имеется ввиду, что есть область до и область после этой двери. Посетитель прикладывает карту и попадает из одной области в другую.
- **Supervisor** (Ревизор/Руководитель)—Supervisor passback (контроль повторного прохода с режимом контроля), это называется “controlled passback”. Там есть различные функции ограничения и контроля, которые могут быть запрограммированы в этом типе passback. Например, вы можете наблюдать, чтобы не менее 2-х контроллеров находилось всегда в области, после этого посетители могут получить доступ в эту область.

ПРИМЕЧАНИЕ: *Уровень доступа supervisor (контроллер) программируется в разделе Карты.*

- **Normal and supervisor**—(нормальный и режим контроля **anti-passback**) оба режима нормальный и контроля будут работать в этой области.

3 Выберите опцию **Card position already valid** (местоположение карты уже верно), если применимо. Когда вы выбрали эту опцию, вы не будете видеть сообщение “Card location in bad area” (местоположение карты в неверной области) если пользователю не разрешено находится в области, т.к. его расписание (уровень доступа) недействительны/истекли.

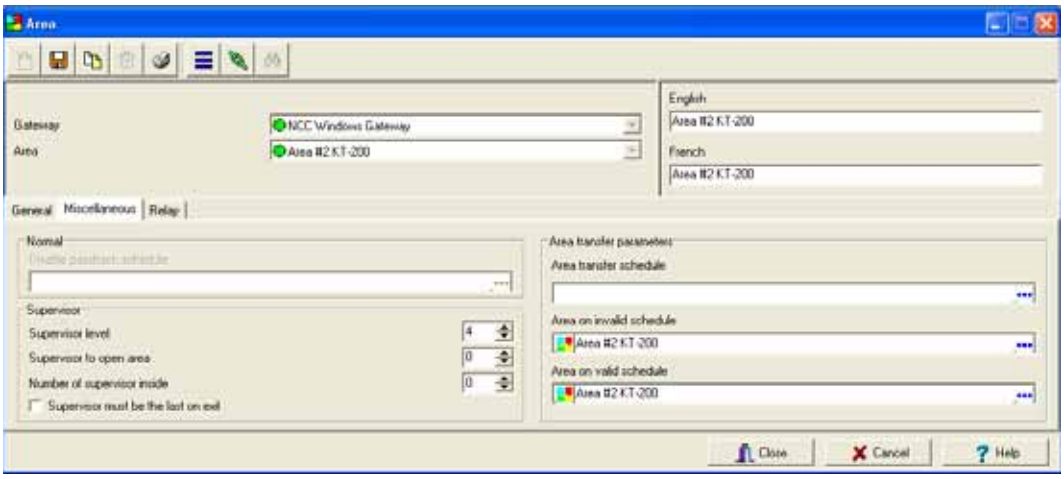
4 Укажите в поле **Card(s) to open area** (Карты в открытую область), количество карт требуемых для получения события **область открыта.** Это поле будет решать количество верных предъявленных карт для назначения этой области в статус “Область открыта” (область переходит в состояние “закрыта” или “пусто”, когда все посетители ушли; область переходит в состояние “открыта” когда в области более одного картодержателя). По умолчанию, установлено 0, это значит, что если область пустая, то система будет создавать сообщение “Область открыта”.

ПРИМЕЧАНИЕ: *Если вы указываете значение более чем 1 карта (например 2 или более), каждый картодержатель должен приложить свою карту к считывателю один за другим.Сначала один, потом другой.*

5 Если у вас возможна функция видео, то у вас появится поле **Video view** (окно видео). Выберите вид видео, в который вы хотите назначить компонент для появления. Для более подробной информации *см. в Главе 12 'Назначение окон видеонаблюдения' на странице 423*.

6 Из списка **Graphic** (График), вы можете выбрать график, в который приложения EntraPass назначены, если применимо. *Для деталей смотрите "Назначение графических схем" на странице 195*.

7 Двигайтесь на вкладку **Miscellaneous** (Прочее) для установки расписания перемещения для настраиваемой области.



- **Disable passback schedule** (Расписание запрета повторного прохода)—Эта опция устанавливает расписание, в течении которого отключается функция запрета повторного прохода (для всех типов passback). Когда данное расписание верное, passback будет отключен.
- **Supervisor(Ревизор):**
  - **Supervisor level** (Уровень ревизора)— Введите уровень контроллера, необходимый для вскрытия области. Это поле должно быть использовано совместно с полем "supervisor to open area" (необходимость ревизора для вскрытия области).
  - **Supervisor to open area** (необходимость ревизора для вскрытия области)— Введите количество требуемых людей/контроллеров для открытия данной области. Имейте ввиду, что внутри должно находится указанное количество людей/контроллеров, соответствующего уровня доступа (это назначается в поле supervisor level)после чего область откроется. После этого картодержатель или человек-контролер меньшего ранга чем указан может попасть в зону после ее открытия. Например, 2 человека ревизора, которые имеют уровень 9, могут попасть внутрь до основного открытия области для доступа картодержателей или ревизоров с уровнем меньше чем 9. Вы должны указать уровень ревизора, требуемый в поле "supervisor level".
  - **Number of supervisor inside** (количество ревизоров внутри области)—Введите количество ревизоров, которые должны оставаться внутри области (имеющие назначенные уровни ревизора) все время. Это поле используется когда вам необходимо иметь ревизора внутри охраняемого помещения в течении всего времени. Когда другой ревизор приходит в область (имеющий соотвествующий уровень ревизора), тогда предыдущий ревизор может покинуть область.

ПРИМЕЧАНИЕ: *Вы не можете использовать это поле, есл вы используте поле* **Supervisor must be last on exit** *(ревизор должен уходить последним). Эта функкция выключена, когда установлена в 0.*

- **Supervisor must be last on exit** (Ревизор должен уходить последним)—Когда эта функция выбрана, то ревизору (имея соответствующий уровень ревизора) не будет позволено покинуть область до тех пор пока там находятся картодержатели.

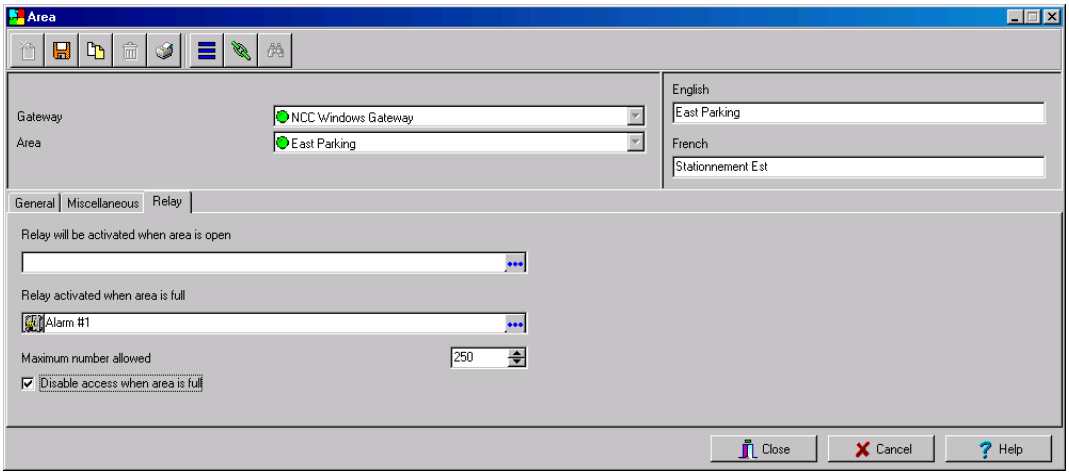
ПРИМЕЧАНИЕ: *Вы не можете использовать \поле* ***"Number of supervisors inside field"*** оличество ревизоров внутри области *если вы используете поле* ***"Supervisor must be last on exit"***(Ревизор должен уходить последним).

8 Define the Area transfer parameters (Назначение параметров перемещения области):
- **Area transfer schedule (расписание перемещения области)—**Это расписание используется для перемещения картодержателей из одной области в другую область,

чтобы избежать сообщения типа “Access denied - Passback bad location” (доступ отклонен, плохое местоположение) или “Card in bad location” (карта в плохом месте). Когда расписание перемещения станет действительным (или недействительным), вы можете указать область куда карты будут перермещены. Вы можете также в ручном режиме изменять местоположение карт используя ручной режим в меню **Области**.

- **Area on invalid schedule (Область на неверное расписание)—**Эта область будет получать всех картодержателей этой области, когда расписание перемещения станет неверным.
- **Area on valid schedule (Область на верное расписание)—**Эта область будет получать всех картодержателей этой области, когда расписание перемещения станет верным.

9 Двигайтесь на вкладку **Relay** для назначения параметров активации реле.



10 Из поле **Relay will be activated when area is open** f(активировать реле когда область открыта), выберите реле или группу реле, которые будут активироваться когда область открыта (событие Area Open). Реле будет оставаться открытым до тех пор, пока область не будет закрыта (событие Area Closed).

- Из пункта **Relay activated when area is full** (активация реле когда область полная), выберите реле или группу реле, которые будут активированы когда область полная (событие Area Full) и будет оставаться активированным пока область не будет пустая.
- Вы можете назначить **Maximum number allowed** (максимальное количество в области) для области, чтобы контролировать количество людей внутри области. Эта функция может быть использована для функции парковки, чтобы контролировать количество мест на парковке.
- Вы можете выделить пункт **Disable access when area is full** (запретить вход в область, когда она полная). Если вы хотите ограничить доступ в область которая полная. Если вы укажете количество в предыдущем параметре, то дверь/двери будут оставаться закрытыми до тех пор, пока кто-то не покинет область. Эта функция также может быть удобна в решениях с парковками.

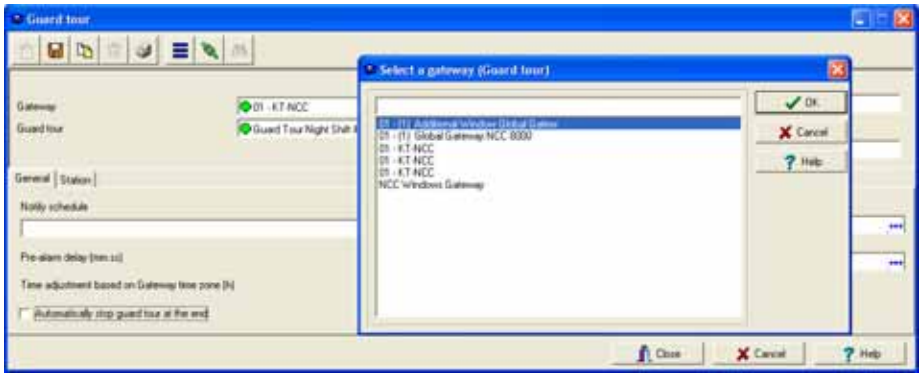
Назначение функции Guard Tour (Только для Шлюзов Global/KT-NCC/NCC 8000)

Guard tour (тур обхода охранником) содержит колоичество остановок/пунктов или дверей, которые должны быть физически верифицированы в соответствии с предписанным расписанием. Остановками могут также быть считыватели или входа/inputs. Задержка между остановками может быть назначена. Система будет создавать тревогу, если охранник не подошел в указанное время к определенной остановке/пункту.

ПРИМЕЧАНИЕ: *Guard tour может быть запущен и остановлен только оператором в ручном режиме (***Operations** > **Guard tours***).*

1 Из панели инструментов Definition (Назначения), выберите иконку **Guard tour**.

- Если вы хотите создать новый guard tour, нажмите на кнопку **New** на панели инструментов. Выберите Шлюз в появившемся окне (Guard tour).



- Выберите шлюз, где guard tour будет иметь место быть, затем нажмите **OK** чтобы закрыть окно.
- В окне Guard tour, введите имя для нового **Guard tour** и нажмите кнопку **Save**.
- Если вы хотите изменить существующий guard tour, выберите тип **Guard tour** из списка.

2 Выберите расписание из списка **Notify schedule** (расписание извещений) нажимая на кнопку **Select a component** (выбрать компонент). Если расписание станет верным, система выдаст сообщение “Guard tour scheduled” (По расписанию Guard tour). Это известит оператора о необходимости запуска Guard tour. После этого оператор будет в ручном режиме запускать этот Guard tour. Затем охраннику будет необходимо проделать действия запрограммированные в этом Guard tour (приложить карту, открыть определенные двери итд).

3 Укажите **Pre-alarm delay** (предтревожная задержка). После этой задержки, система будет создавать событие “Guard tour ТРЕВОГА”.

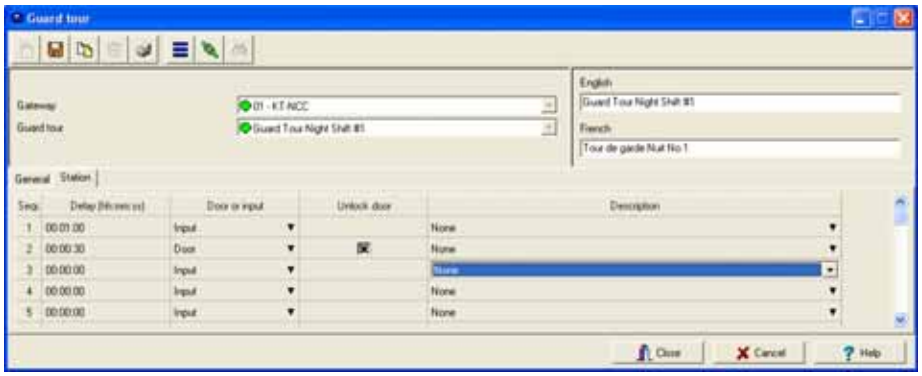
ПРИМЕЧАНИЕ: *Если время до следующего пункта вышло, тогда бует запускаться предтревожная задержка.Например, охранник имеет 1:00 минуту чтобы дойти до следующей остановки. Проходит одна минута, охранника нет. После этого появляется сообщение “Guard tour station late” (*Guard Tour *опоздание). После этого будет запускаться “pre-alarm delay” (предтревожная задержка). Событие “Guard tour alarm” (тревога* Guard Tour*) будет появляться после истечения предтревожной задержки.*

4 Когда необходимо, введите **Time adjustment based on Gateway time zone** (настройка временной зоны между сервером и Шлюзом). Если например, вы имеете временные расхождения 1 час 30 минут, тогда введите 1,5.

5 Вы можете выделить функцию **Automatically stop guard tour at the end** (Автоматическая остановка guard tour в конце), если вам не требуется останавливать Guard tour в ручном режиме после того, как Guard tour закончен.

6 Выберите **Video view** (если применимо) аи **Graphic view** (Вид графика) там, где назначен Guard Tour.

7 Выберите вкладку **Station** (шаги/пункты/остановки) для назначения пунктов для Guard Tour.

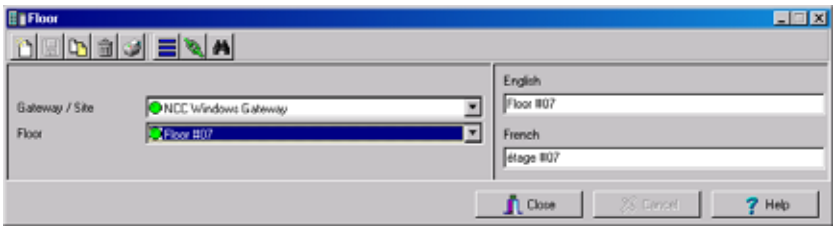


- **Sequence** (Последовательность)— Показывает шаги Guard Tour. Эти шаги должны быть назначены таким образом, что бы охраннику было просто идти от одной станции к другой. Например, последовательность должна быть запрограммирована в соответствии с пунктами, которые встречаются охраннику на пути.
- **Delay** (Задержка)—Эта задержка указывает период (ч:м:с) для достижения следующей остановки. Если задержка истекает до того как охранник достигает следующего пункта, то система делает сообщение *(*Guard Tour *опоздание до остановки)*. Если охранник не достигает остановки остановки в течении следующей задержки, тогда система создает событие “ТРЕВОГА Guard tour”.
- **Door/Input** (Дверь/вход)—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** (Разблокировать дверь)—Когда вы выбираете дверь как станцию/пункт, то возможно указать должен ли охранник открывать дверь в процессе Guard Tour. Если укажите, то дверь будет разблокироваться и ее необходимо будет открыть.
- **Description** (Описание)—Выберите дверь или вход (в соотвествии с колонкой “door or input” - это будет использоваться как остановка для охранника.

Назначение этажей (Floors)

Меню Floor служит для создания и редактирования этажей для лифтов. После создания этажей их группируют и привязывают к расписанию, от которого зависит доступ к тому или иному этажу.

1 На панели инструментов **Definition** (Назначения) нажать кнопку **Floor** (Этажи).



2 В выпадающем списке **Site** (луч) выделить луч, для которого необходимо выполнить описание этажей. Это позволяет сократить список компонентов, описываемых в системе.

3 Выделить этаж или нажать иконку **New** (Создать), чтобы создать новую группу этажей.

4 Назначить этому компоненту содержательное имя. Нажать кнопку **Close** (Закрыть). Система сделает запрос на сохранение данных.

Назначение связки Событие/Реле, (только шлюзы Global/KT-NCC/NCC 8000)

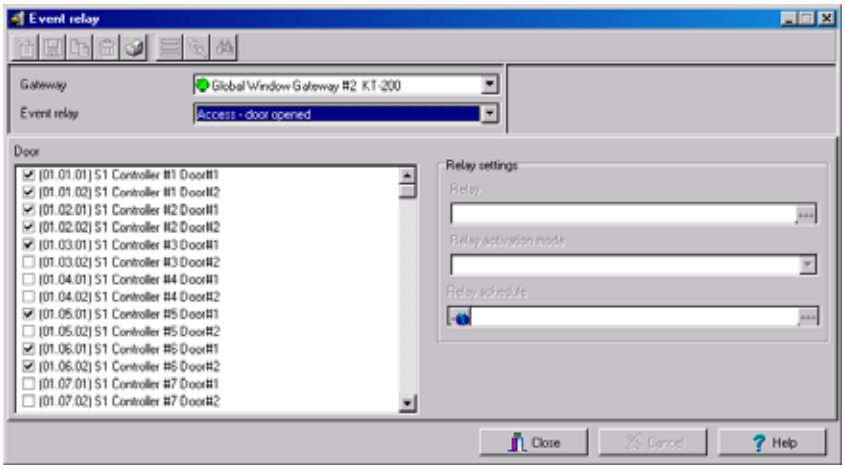
Это меню предназначено для связи событий, которые будут активировать реле. Вы также можете назначить, что реле будет активировано в течении определенного расписания. Реле может быть активировано, деактивировано или активировано на время. Например, вы можете активировать реле, когда система поставлена на охрану. Это реле может быть назначено, например, для выключения света в здании.
События могут быть сделаны для различных причин. Они могут быть созданы для отчета по этим событиям:

- Unauthorized access - неавторизированный доступ
- Intrusion - вторжение
- Defective components - плохой компонент
- Modified components - иземененные компоненты
- Состояние Guard tour (например, охранник не достиг следущей точки обхода), итд.

Назначение параметра событие/реле (Event Relays)

1 Из панели инструментов Definition (Назначение), нажмите кнопку **Event relay** (событие\реле).

,



2 Из списка **Gateway**, выберите Шлюз, затем выберите **Event** (событие), которое вы хотите связать с реле. Слева на экране будет от ображаться тип выбранного события, применимого к вашей системе.

3 Выберите компонент, связанный с этим событием. Затем выберите реле, которое вы хотите активировать, когда данное событие произойдет.

4 Для выбранного реле или группы реле выберите тип активацвии реле (**Relay activation mode**):
   - **Temporarily activated** (временно активировать)—Реле будет временно активирвано на время назначенное в поле **Temporary activation timer** (время активации). Данное поле находится в меню назначения реле. Если время активации реле установлено (**Temporary activation timer**) в “0”, тогда время активации реле будет соответствовать времени активации события.
   - **Activated** (активировать)—Реле будет активированным до тех пор, пока не придет команда на отключение.
   - **Deactivated** (деактивировать) - Реле будет деактивированным до тех пор, пока не придет команда на активирование.

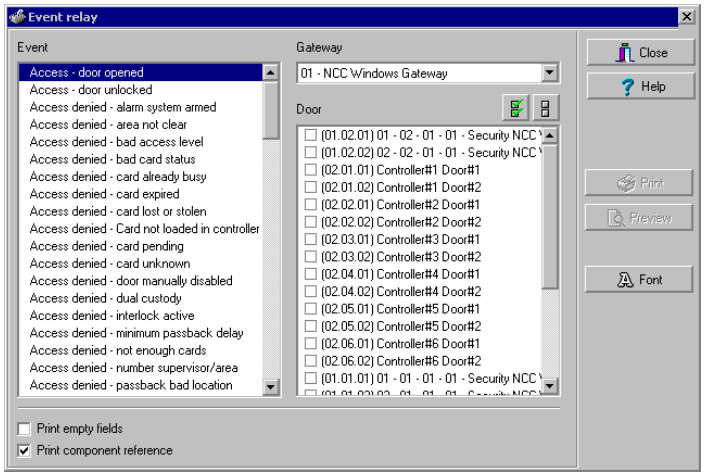
5 Выбрать расписание активации в разделе **Activation schedule**: Реле будет активирвоаться только при условии верного расписания. Другими словами, когда происходит событие и расписание верное, тогда реле будет активироваться. Если расписание не верно, тогда активации не будет.

ПРИМЕЧАНИЕ: *Когда выбрана группа реле, тогда каждое реле в этой групе будет активироваться на время, описанное в настройках каждого реле (поле activation timer). Например, одно реле может быть установлено на активацию 10 сек., а второе реле может быть установлено в “0” (следовать з асобытием).*

Печатать Событие\Реле (Event Relay)

Это меню используется чтобы напечатать для определенного события.

1 Из окна **Event relay (событие-реле)**, нажмите на кнопку **Printer**.



2 Из панели **Event Relay** (событие-реле), выберите **Event** (событие) для которого вы хотите напечатать связанные параметры.

3 Из выпадающего списка **Gateway**, выберите Шлюз, для которого вы хотите напечатать параметры события.

4 Выберите компоненты, связанные с выбранными событиями: События обычно связываются с систменым компонентом: дверь, контроллер, тревожный раздел, АРМ итд. Например, если вы хотите выбрать событие “тревога по входу”, то вам будет предложено выбрать компонент из всех input/входов назначенных в вашей системе. Выберите вход, который вы хотите напечатать (вы можете выбрать все компоненты, используйте кнопку “check mark” (отметить все)).

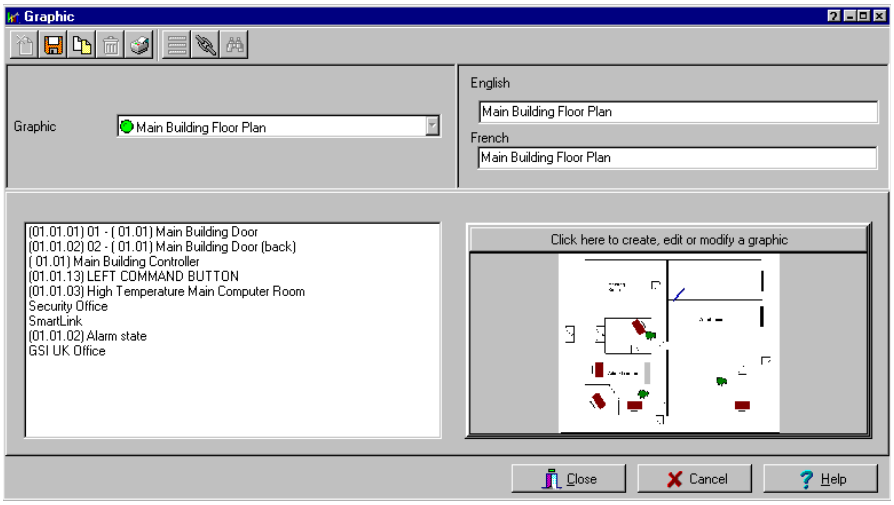
Назначение графических схем

Графическая схема соответствует охраняемой территории объекта, на которой расположены компоненты (приложения EntraPass, контроллеры, входы, реле и др.). С помощью графических схем операторы могут легко определить точное место расположение компонента на объекте или увидеть состояние компонентов и устройств, в том числе дверей, контактов, детекторов движения, контроллеров и панелей, прикреплённых к графическому плану системы. Операторы в ручном режиме могут напрямую управлять отображенным компонентом (например, отпирать-запирать двери). Операторы могут выполнять операции с или без подтверждения. Число графических планов в системе может быть любым. Каждый план может содержать до 250 компонентов, включая отображение живого видео на заднем фоне. Кроме того, предусмотрено импортирование графических схем в формате BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF или PCD из других программ.

ПРИМЕЧАНИЕ: *Система Entrapass содержит четыре поэтажных плана-образца. При желании можно изменить их в соответствии со своей схемой системы. Эти планы хранятся в папке C:\Program Files\Kantech\Server_GE\ Generaldata\Demobmp folder.*

Назначение компонентов графических схем (раздел Graphic)

1 На панели инструментов Definition (Назначения) нажать кнопку **Graphics** (Графические схемы).

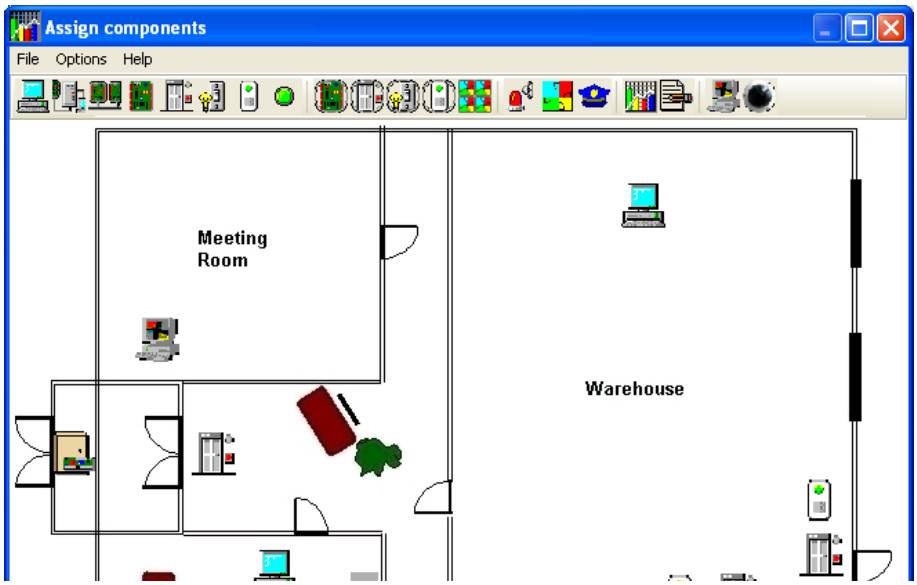


2 В выпадающем списке **Graphic** выбрать графическую схему, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой.

3 Назначить для этой схемы новое имя (или изменить уже созданное). .

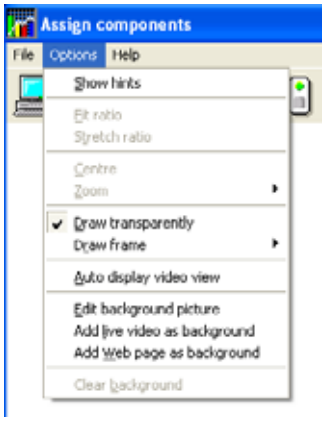
ПРИМЕЧАНИЕ: *При работе с уже созданной схемой и при создании новой все компоненты, прикреплённые к этой схеме, отображаются в левой части окна. В правой половине будет выведена сама графическая схема.*

4 В окне **Graphic** нажать кнопку **Click here to create, edit or modify a graphic** (Нажмите для создания, редактирования или изменения схемы), чтобы открыть окно **Assign Components** (Назначить компоненты).



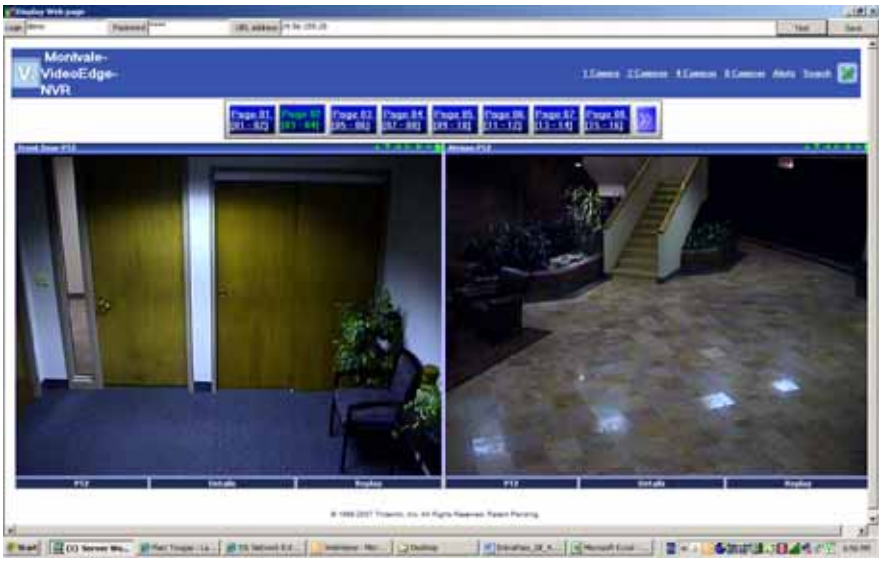
ПРИМЕЧАНИЕ: Если в системе разрешено использование видеонаблюдения, то в меню Graphics добавляются видеокомпоненты. К этим видеокомпонентам есть доступ прямо со схемы. Если на графическую схему поместить иконку, то её статус будет отображаться при щелчке по иконке видеонаблюдения. Помимо стандартных функций, предусмотрены следующие опции для определения состояние видеокомпонентов: статус подключения видеосервера, параметры видеосервера, состояние камер наблюдения.

5 Открыть меню **Options** (Опции) для выбора функций рисования. Активная функция отмечена флажком. .



- **Show hints** (Выдавать подсказки) – отображать данные компонента (имя и адрес) при наведении курсора мыши поверх изображения этого компонента.
- **Draw transparently** (Нарисовать прозрачный объект) – поместить прозрачную иконку поверх фонового изображения для получения смешанного эфекта.
- **Draw frame** (Нарисовать рамку) – обвести компонент в рамку. **Frame color** (Цвет рамки) – отображает текущий цвет рамки и позволяет выбрать другой цвет
- **Auto display video view** (Автоматически отображать видеоокно) – позволяет добавить видеоокно.
- Выделить опцию **Edit background picture** (Редактировать фоновое изображение), чтобы изменить фоновое изображение для выбранной графической схемы. В этом окне можно изменить цвет рамки и фона схемы, а также добавить комментарии.

- Выделить опцию **Add live video as background** (Добавить живое видео, как фон), чтобы добавить на задний план живое видео.

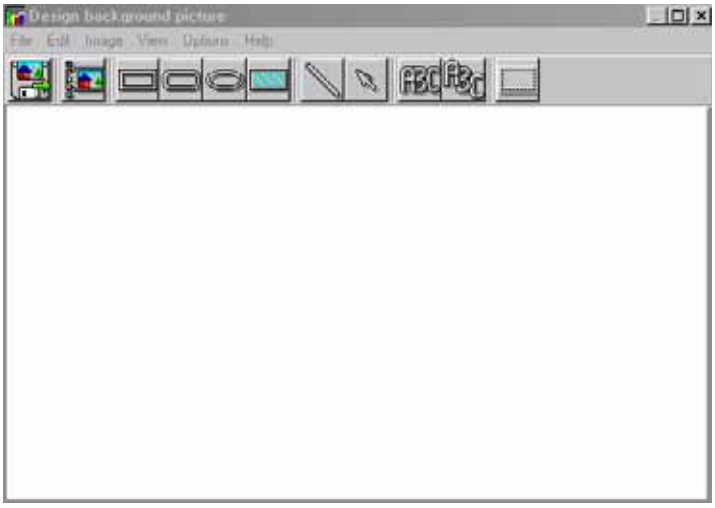


- Выделить опцию **Add Web page as background** (Добавить веб-страницу, как фон), чтобы добавить на задний план веб-страницу. Для этого в поле **URL address** следует ввести адрес веб-сайта и нажать **Enter** (Ввод) на клавиатуре или нажать **Test** (Проверить). Если для доступа к веб-странице не требуется ввод регистрационных данных и пароля, то поля **Login** и **Password** можно оставить пустыми. Нажать **Test** (Проверить) и убедиться, что веб-страница загружается правильно. Затем нажать **Save** (Сохранить).

- Выделить флажком опцию **Clear background** (Очистить фон), чтобы удалить фоновое изображение с графической схемы и оставить только изображения компонентов. Эту функцию можно использовать для того, чтобы вставить новую схему, оставив те же компоненты.

Создание фонового изображения для графического окна

1 Дважды щёлкнуть мышью в любом месте на фоновом изображении в окне Assign components (Назначить компоненты), чтобы открыть окно **Design background picture** (Дизайн фонового изображение).



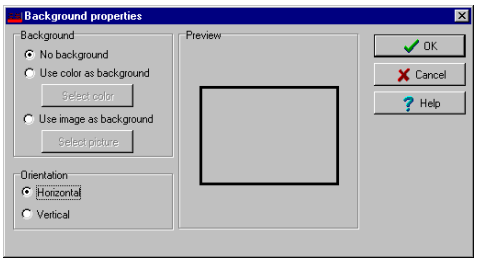
2 Использовать это окно для импортирования изображения, которое было создано в другом приложении или создать свой собственный фон при помощи инструментов для рисования.

•Чтобы импортировать созданную графическую схему, следует щёлкнуть по иконке дискеты, затем перетащить дискету в рабочую область. После того компонент будет установлен на нужное место, следует отпустить кнопку мыши, и на экране появится диалоговое меню настройки свойств изображения (Image properties). При этом должно открыться окно **Open** (Открыть). Выбрав изображение, которое необходимо импортировать, следует нажать кнопку **Open.** Изображение будет помещено в графическую область меню.

•Чтобы импортировать собственную иконку в качестве фонового изображения, следует нажать на панели инструментов кнопку **Custom images** (Собственные изображения). На экране откроется окно Select an image (Выбрать изображение). Выбрав нужную иконку, нажать **OK**, чтобы закрыть окно и импортировать изображение в окно редактирования схемы.

- Чтобы вставить в фоновое изображение готовые геометрические фигуры и текст, следует просто выделить нужную фигуру (прямоугольник, круг, эллипс и пр.) на панели инструментов и перетащить её в фоновое изображение.

- Чтобы изменить фигуру, уже помещённую в редактируемое окно, следует щёлкнуть по ней правой кнопкой мыши, чтобы открыть меню Properties (Свойства), и внести необходимые изменения (цвет, расположение и пр.).



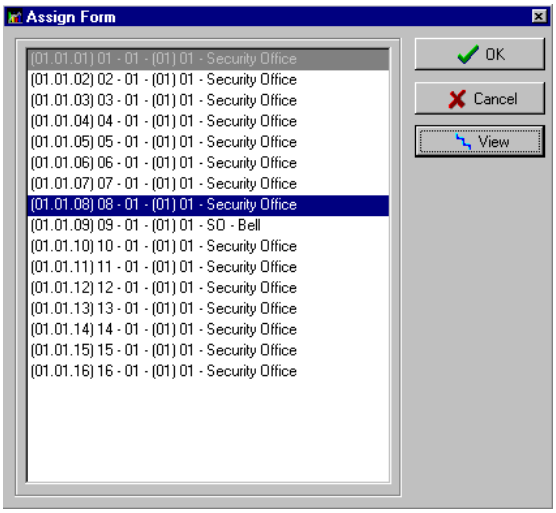
- Система может быть настроена таким образом, что меню Properties будет появляться сразу при перетаскивании фигуры в окно редактирования схемы. Для этого следует выделить опцию **Show properties on Drop** (Показывать свойства при перетаскивании) в меню **Options** (Опции).
- Чтобы найти фигуры, которые ранее были сохранены на диск, следует вызвать функцию **Load annotations** (Загрузить комментарии) в меню **Image** (Изображение). При добавлении геометрических фигур в схему в таком случае у пользователя будет возможность сохранить их как комментарии в отдельный файл, чтобы потом извлечь их из этого файла.
- Чтобы сохранить комментарии со схемы в отдельный файл, следует вызвать функцию **Save annotations** (Сохранить комментарии) в меню **Image** (Изображение). Теперь пользователь сможет извлечь их для дальнейшего использования.
- Чтобы удалить фигуры, необходимо вызвать функцию **Clear annotation** (Удалить комментарии) в меню **Image** (Изображение). В случае сохранения графической схемы вместе с геометрическими фигурами эти фигуры становятся прозрачными.

- В меню **View** (Вид) указать, как будет отображаться графическая схема.

ПРИМЕЧАНИЕ: *Манипуляторы размера (крестики по краям изображения для регулировки его размеров) указывают но то, что этот объект выделен*

Создание связей системных компонентов с графическими иконками

1 На панели инструментов Assign Components (Назначить компоненты) перетащить выделенный компонент в нужное положение. Чтобы перетащить объект из одного места в другое, следует выделить этот объект мышью и, не отпуская кнопки мыши, перетащить его в нужное место на схеме.



2 После того компонент будет установлен на нужное место, следует отпустить кнопку мыши, и на экране появится диалоговое меню настройки Assign Form (Назначить форму).

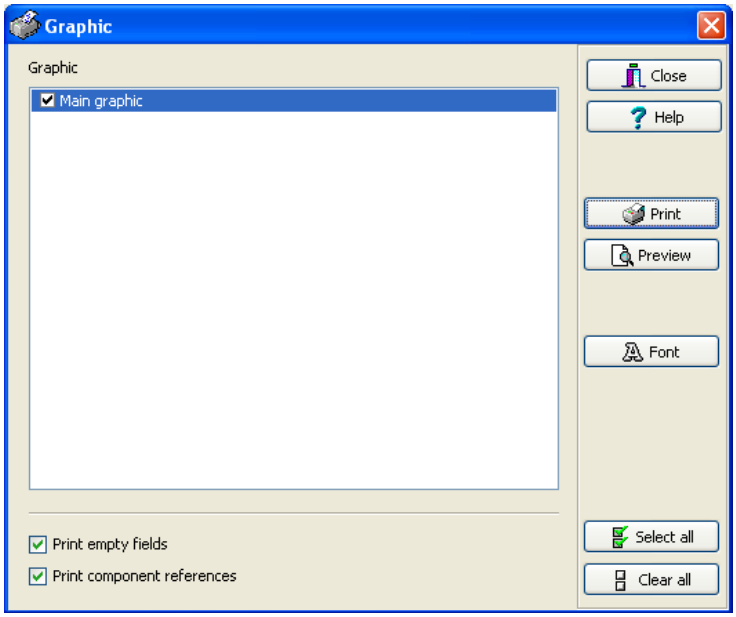
3 Выделить компонент системы, который должен быть прикреплён к иконке на экране.

4 Нажать **OK**, чтобы вернуться в предыдущее окно.

ПРИМЕЧАНИЕ: *Если иконка не будет привязана к какому-либо компоненту системы, то она не будет сохранена на схеме. Для выбора будут доступны только те компоненты, которые не были выбраны для использования на схеме.*

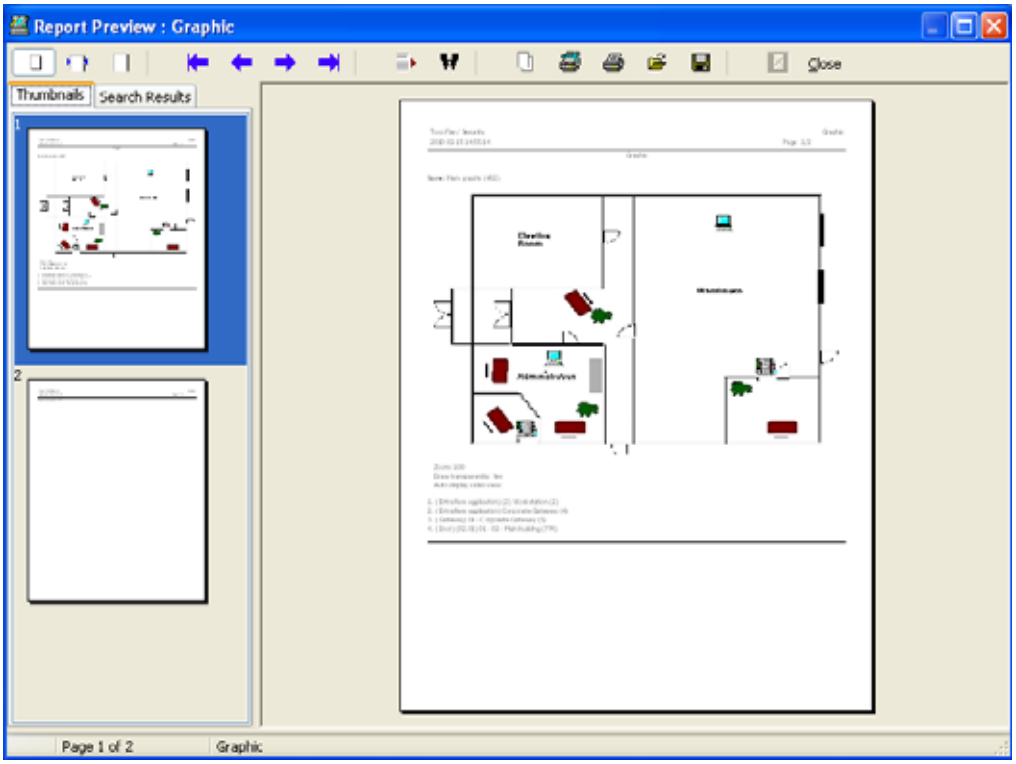
Печать системных компонентов и графиков

1. Из панели инструментов **Definition** (Назначение), нажмите на иконку **Graphic** и выберите график из выпадающего окна.
2. Нажмите кнопку **Print** из окна **Graphic**

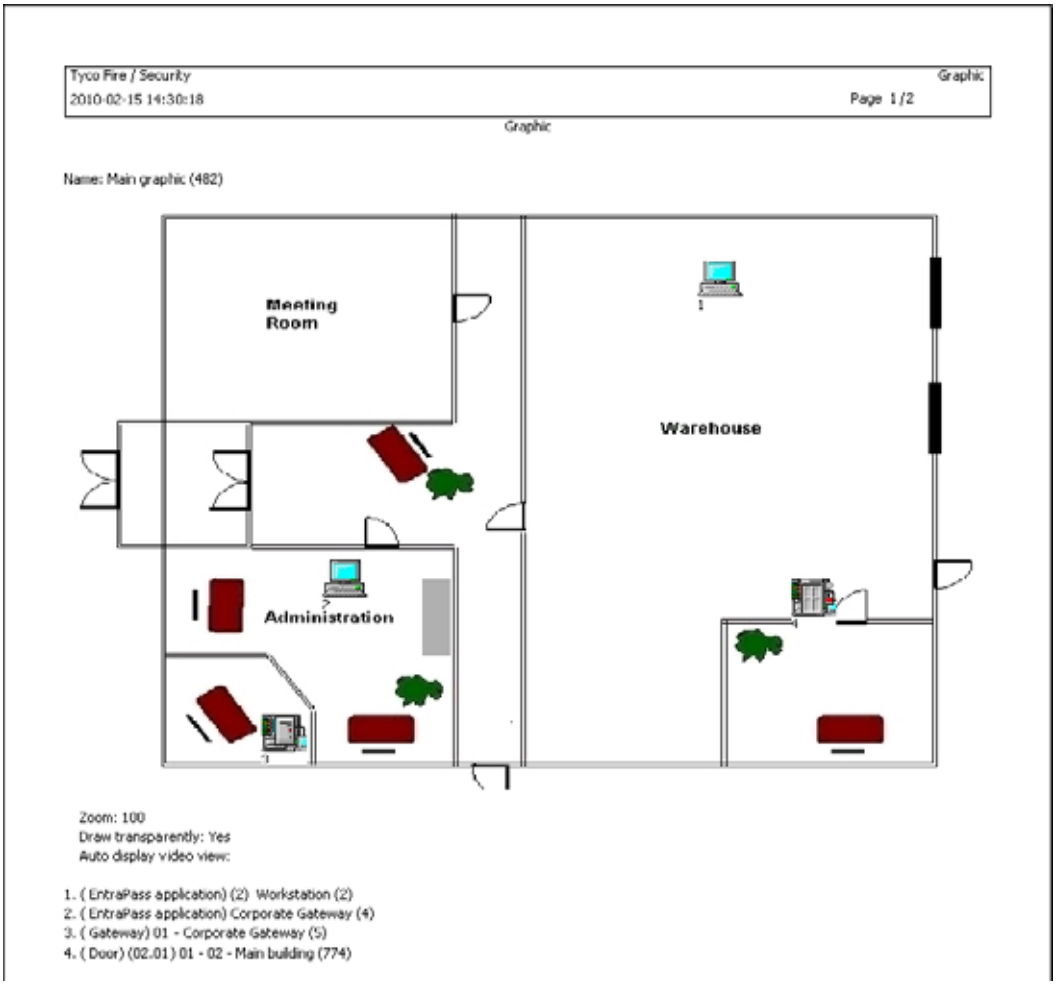


- Выберите графики, которые должны быть напечатаны, используя окна выбора. Вы можете также назначить кнопки **выбрать все** (**Select all)** или **Clear all** (очистить все).
- Укажите **Print empty fields** (печатать пустые поля), чтобы включить титры полей, даже если они пустые.
- Укажите пункт **Print component references** () чтобы вывести на печать описания/reference компонентов.
- Используйте кнопку **Font** (шрифт), чтобы отобразить стандартный шрифт Windows или изменить атрибуты шрифта.

- Нажмите на кнопку **Preview** (предварительный обзор) для отображения общего вида печатаемого материала.



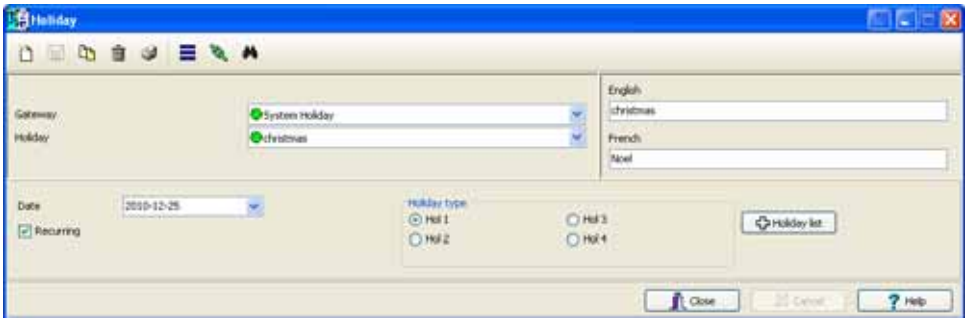
3 Нажмите **Print** (печать) для отправки графической схемы на принтер.



Назначение каникул

Праздники обрабатываются не так, как остальные дни. Рекомендуется планировать праздники в начале года; это помогает заранее настроить праздники с плавающей датой (Пасха, День благодарения и др.). Каникулы могут быть назначены специфическим типом (Hol 1, 2, 3, 4). Один и тот же день может быть назначен как праздник на одном объекте и как рабочий день на другом объекте. Каникулы могут также быть назначены как глобальные каникулы или назначаться отдельно на Шлюз.

1 Чтобы создать новый праздник, нажать кнопку **New** (Создать).



2 Чтобы создать новый праздник, нажать кнопку **New** (Создать).

3 Для создания глобального праздника, продолжайте с пункта holiday definition (назначение каникул). Чтобы создать праздник для определённого шлюза/луча, следует указать этот шлюз/сайт в выпадающем списке.

4 Назначить имя празднику.

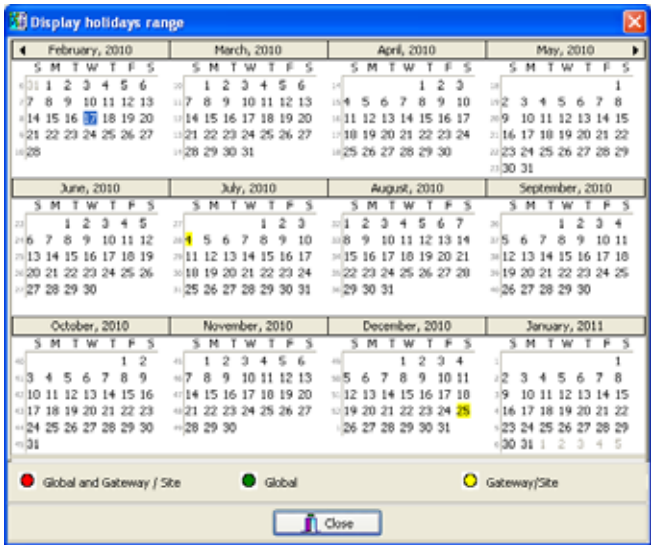
5 В меню **Date** (Дата) указать календарную дату праздника.

6 Отметить флажком опцию **Recurring** (Повторяющийся), если праздник повторяется ежегодно.

ПРИМЕЧАНИЕ: *Если праздник не повторяется из года в год, следует перенастроить его на следующий год. Таким образом, можно запланировать праздники на много лет вперёд; однако рекомендуется обновлять информацию о праздниках ежегодно.*

7 В разделе Holiday type (Тип праздника) указать тип описываемого праздника. Деление праздников на несколько типов повышает гибкость системы. Например, день благодарения можно назначить выходным днём для одной группы пользователей и рабочим днём для другой группы.

8 Нажмите на кнопку **+ Holiday list** (список праздников) чтобы отобразить календарь на 12 месяцев, при этом показываяя вам одним из трех цветов легенду.



ПРИМЕЧАНИЕ: *legend - это тип прикрепления выбранного праздника к разделу. Для большей информации смотрите "Назначение расписаний" на странице 174 for more information.*

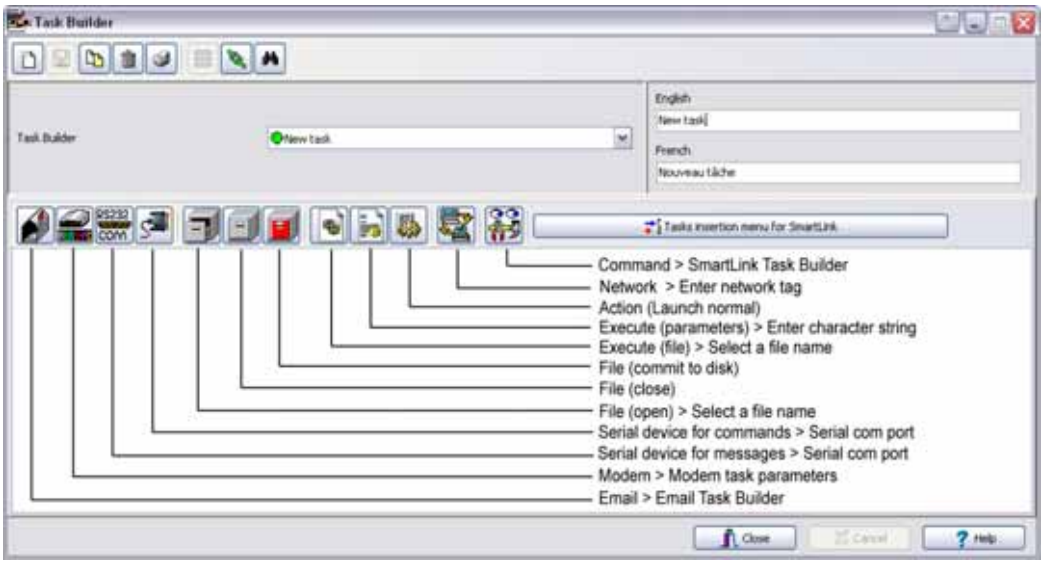
Назначение Task Builder (конструктор команд)

Минимальные требования

Иконки **Task Builder** (конструктор команд) и **Event Trigger** (триггер событий) будут отображаться при условии, если компонент SmartLink был установлен на APM и зарегестрирован на сервере EntraPass.

Панель управления конструктора команд (Task Builder)

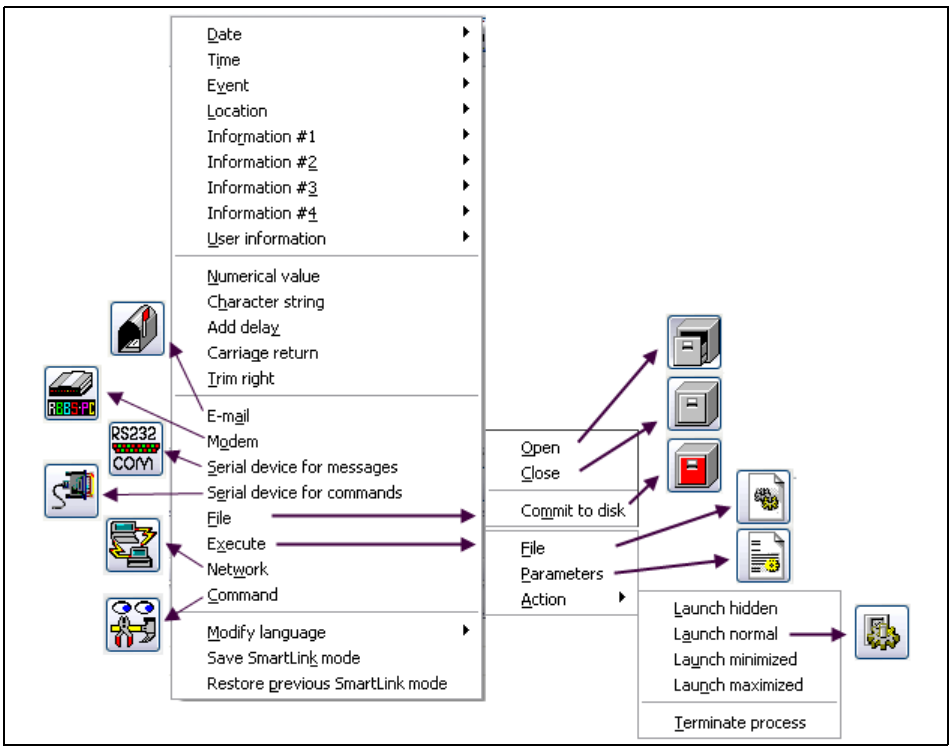
1 Из панели управления **Definition** (назначения), выбрать иконку **Task Builder** (конструктор команд).



Меню **Task Builder** позволяют вам создать задачи для SmartLink. Когда вы имеете установленное приложение, меню вставки задач является активным. Это позволяет операторам сконструированные команды в приложение SmartLink.

ПРИМЕЧАНИЕ: *Была добавлена новая команда в SmartLink (BATCHMODIFY), позволяющая производить изменения на группу карт. Сейчас возможно изменить параметры для группы карт. Будут изменяться только данные, в поле которых вы произвели изменения. Для бльшей информации по командам* **Task Builder***, обращайтесь к SmartLink Reference Manual DN1327.*

1 Нажмите на кнопку **Task insertion menu for SmartLink** (Меню вставки задачи для SmartLink)/ Меню отобразится на экране. Вы также можете использовать **icons** (иконки), которые связывают большинство обших вставок.



ПРИМЕЧАНИЕ: *При создании задач SmartLink, воспринимаются только верные команды, написанные на основном языке. Для большей информации, смотрите SmartLink Reference Manual, DN1327.*

Следующая таблица описывает опции, которые вы сможете найти в меню.

Параметр	Описание
Date	**Вставляет дату в задачу. Опции: год, месяц, день, YYYY/MM/DD или MM/DD/YYYY**
Time	**Вставляет время в задачу. Опции: час, минуты, секунды, HH:MM:SS или HH:MM.**
Event	**Вставить описания события в задачу. Вы можете выбрать отображать имя события или его номер.**
Location	**Вставить местоположение, где задача будет происходить. Опции: Приложение EntraPass, Gateway/Шлюз или Site/луч.**
Information #1 to 4	**Вставить информацию о событии. Опции в базе данных: Index Number (индекс номера), Index Text (индекс текста), Component ID и Component Text (ID компонента и текст компонента).**
User Information	**Вставить информацию о карте в задачу. Опции: номер карты, имя пользователя, информация о карте №1-№10 или комментарии.**
Numerical Value	**Вставить число в задачу.**
Character String	**Вставить текст в задачу (свободный текст).**
Add Delay	**Вставить задержку в 1/10 секундах в задачу.**
Carriage Return	**Вставить carriage return (Enter) в задачу.**

Параметр	Описание
Trim Right	Будет удалять последний символ с права в задаче.
Email	Вставить email в задачу, на который будет автоматичсеки посылаться, когда событие происходит.
Modem	Вставить сообщение в задачу, которое будет посылаться автоматичсеки на пейджер когда событие происходит.
Serial Device for Messages	Выбрать серийный порт и скорость передачи для отправки сообщения.
Serial Device for Commands	Выбрать серийный порт и скорость передачи для отправки команды.
File	Откроется выбранный файл (или создать новый), где вся информация о событиях будет записываться, если случаются события. Close - будет закрывать этот файл. Commit to disk - будет происходить сохранение файла на диск. Эта команда не может закрывать файл.
Execute	Откроется файл выбранного имени, который позволит вам напечатать текстовый поток, который будет добавлен в задачу. Action - позволит вам назначить как вы хотите запускаит задачу (Launch Hidden(запуск скрыто), Launch Normal(запуск нормально), Launch Minimized(запуск минимально), Launch Maximized(максимальный запуск) или Terminate process(завершить процесс)).
Network	Вставить значок сеть (Network Tag).
Command	Вставить значок команда (Command Tag).
Modify Language	Вы можете изменить язык команды на английский или французский.
Save SmartLink Mode	Вставить в команду SmartLink чтобы взаимодействовать и положить текущий режим SmartLink в задний фон (например, отправка email). Эта команда должна всегда быть использована с режимом Restore Previous SmartLink (восстановить предыдущий режим SmartLink).
Restore Previous SmartLink Mode	Вставить в команду SmartLink чтобы восстановить предыдущий режим SmartLink. Эта команда должна быть использована совместно с режимом Save SmartLink (Сохранить SmartLink).

Добавление в задачу Email

1 После того как вы создали новую задачу или выбрали существующую задачу, нажмите на иконку **Mailbox**. Окно **Email Task Builder** будет отображаться на экране.

2 Введите ваш email адрес в поле **From...** (От).

3 Введите email адрес/а, кому вы хотите отправить письмо в поле **To...** (Кому). Каждый адрес должен быть разделен точкой с запятой (;).

4 Если вы желаете отправить копию этого письма другому человеку, тогда введите в поле **CC...** e-mail адрес.

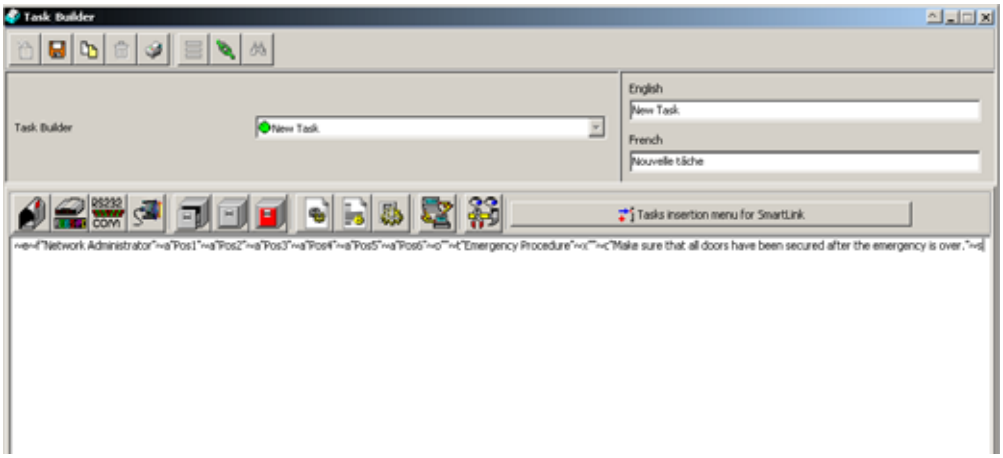
5 Введите данные в поле **Subject** (Тема).

6 Если вы хотите вложить файл к этому письму, введите путь к файлу в поле **Attachment**. Каждое поле должно быть разделено точкой с запятой (;).

7 Введите сообщение в текст письма.

ПРИМЕЧАНИЕ: *Различные значение могут быть добавлены в тему письма и в тело письма.*

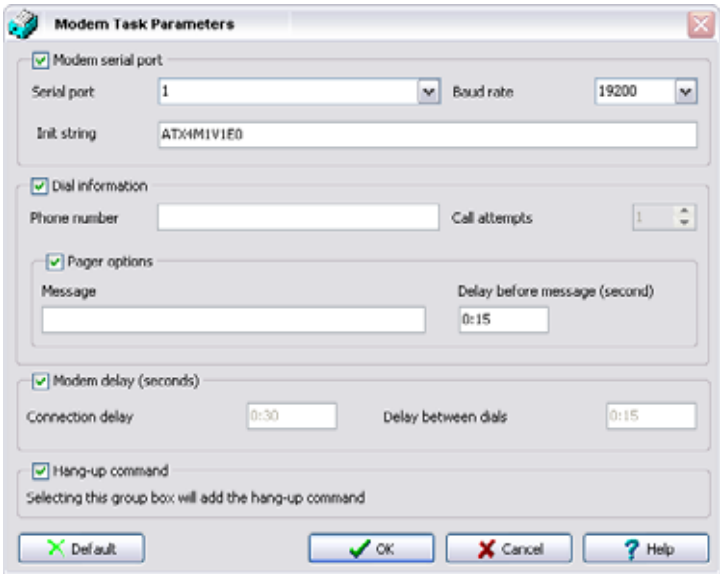
8 Нажмите **OK,** чтобы прикрепить email к задаче SmartLink. Ваше сообщение будет появляться в этом окне в вид кода.



Вставка в задачу Pager Command (команды на пейджер)

Когда вы используете SmartLink, EntraPass позволяет вам отправлять команды на пейджинговые станции.

1 Нажмите иконку **Modem**. На экране будет отображаться **Modem task parameters** (параметры задачи для модема).

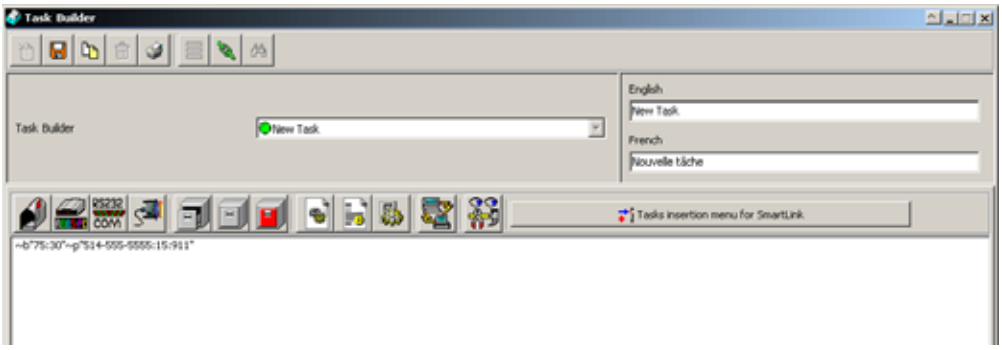


2 Должен быть уже установлен параметр **Modem serial port** (серийный порт модема).

3 Введите в раздел **Dial information** (информация о звонке) номер телефона в раздел **Phone number.**

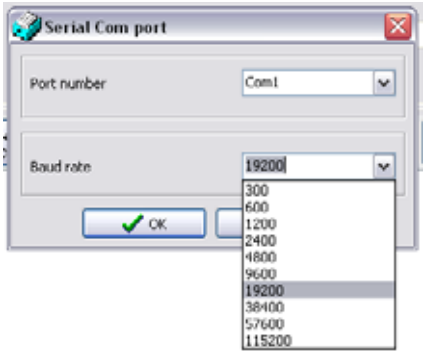
4 Выделите пункт **Pager options** (опции пейджера) и введите сообщение в поле **Message**. Данное сообщение будет появляться на пейджере (если пейджер имеет опции отображать) после истечения задержки в разделе **Delay before message (seconds)**. Значения от 00:00 до 09:59 мин.

5 Нажмите **OK**. Данное сообщение и телефонный номер появяться в окне Task Builder.



Вставка передачи сообщений на serial устроства

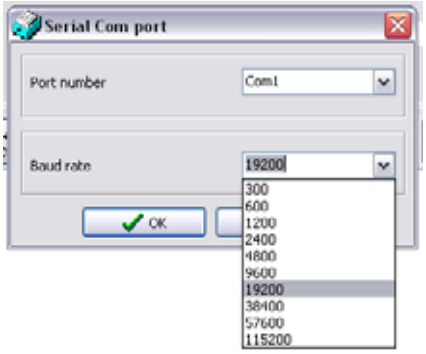
1 Нажмите иконку **Serial device for messages** (серийное устройство для передачи сообщений). Окно **Serial com port** будет отображаться на дисплее.



2 Выберите номер порта и скорость передачи в разделе **Port Number** и **Baud rate**.
3 Нажмите **OK**.

Вставка серийных устройств для передачи команд

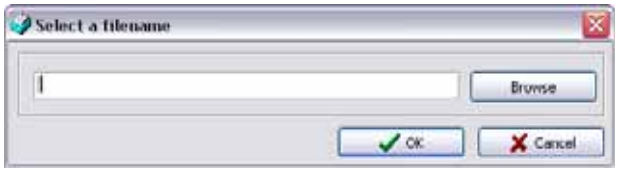
1 Нажмите вкладку **Serial device for commands** (сериные устройства для команд). Окно выбора com порта отобразится на экране в разделе **Serial com port**.



2 Выберите номер порта и скорость передачи в разделе **Port Number** и **Baud rate**.
3 Нажмите **OK**.

Вставка файла

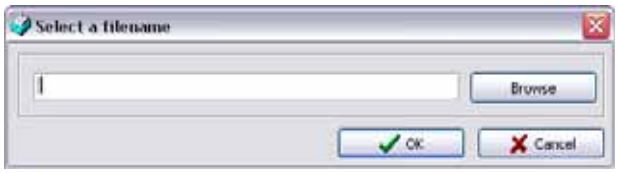
1 Нажмите на иконку **File (Open)** (открыть файл). Окно **Select a file name** будет отображено на экране.



2 Введите имя файла и путь к нему.
3 Нажмите **OK**.

Выполнить файл (Executing a File)

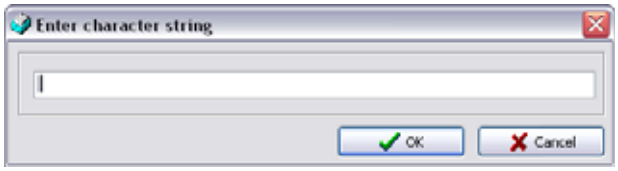
1 Нажмите на иконку **Execute (File)** (выполнить файл). Окно **Select a file name** появится на экране.



2 Введите имя файла и путь к нему.
3 Нажмите **OK**.

Параметры выполнения (Executing Parameters)

1 Нажмите на иконку **Execute (Parameters)** (Параметры выполнения). Окно **Enter character string** (введите текстовый поток) появится на экране.



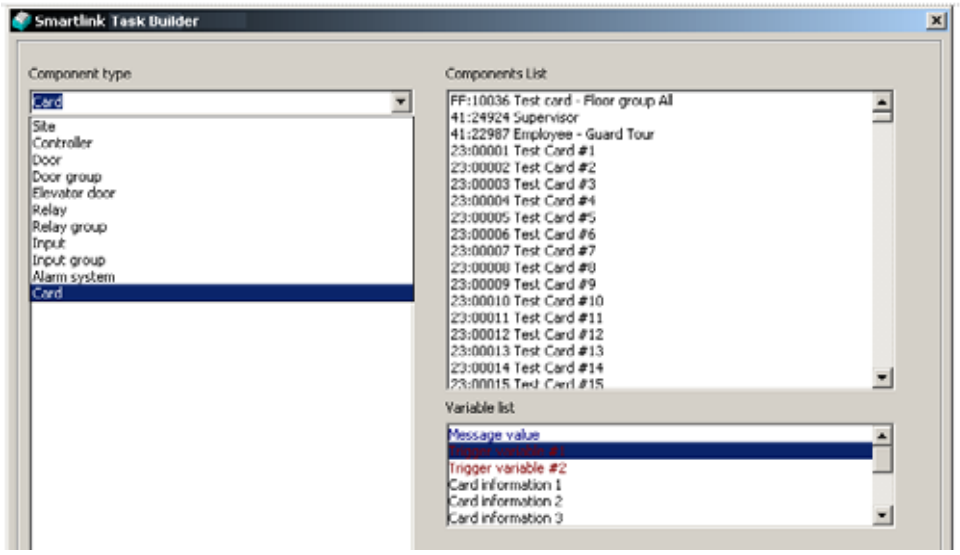
Ввести сетевой Tag (Network Tag)

1 Нажмите на иконку **Network**. Окно **Enter network tag** (введите сетевой tag) появится на экране.

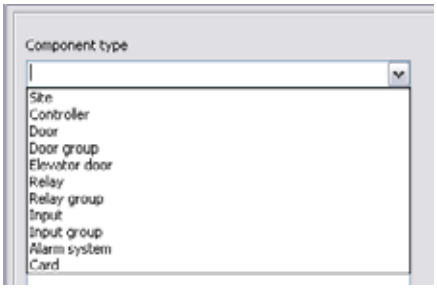
2 Введите сетевой tag (**network tag**). Значение от 0 до 999,999.
3 Нажмите **OK**.

Ввод команд (Entering Commands)

1 Нажмите на иконку **Command** (команда). Диалог **SmartLink Task Builder** будет отображаться на экране.

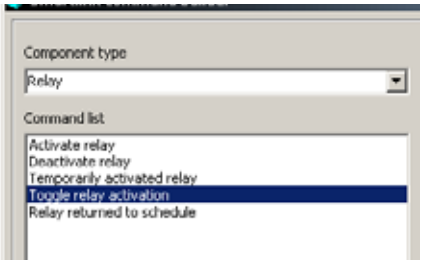


2 Выберите тип компонента из списка **Component type** (список компонентов).



3 Выберите команду из списка команд.

ПРИМЕЧАНИЕ: *Команда **toggle** (переключить) доступна только с некоторыми компонентами, такими как: дверь, вход, реле.*



4 Выберите пункт variable (изменяемые) из списка **Variables list**. Там есть три категории variable, которые могут быть связаны с компонентом и командой.

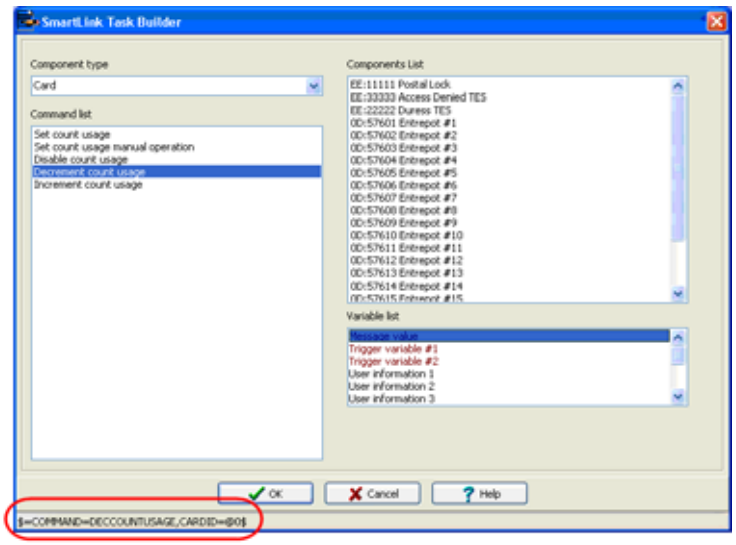
- Message Value - сообщить количество
- Trigger - триггер (включить)
- Card Information 1 to 10 - информация о карте 1-10

Примеры построения команд в Task Builder

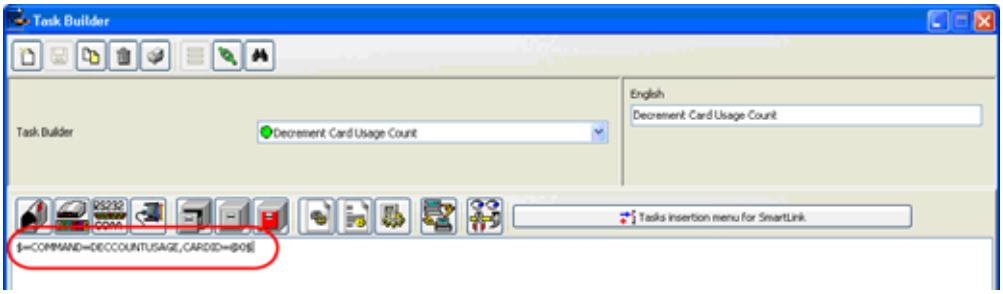
Следующая процедура будет раскрывать каждый из пунктов variables (изменяемый/различный), который может бытьс вязан с типом компонента или командой.

Построение задачи с Message Value Variable
(сообщение о изменении количества)

1. Из панели инструментов **Definition** (Назначение), выберите иконку **Task Builder**.
2. Нажмите **New** и введите имя **Decrement Card Usage Count** (понижение количества обращений карт) в имени задачи.
3. Нажмите на кнопку **Command** (команда).
4. Из окна **SmartLink Task Builder**, выберите пункт **Card** из выпадающего окна **Component type** (Тип компонента).

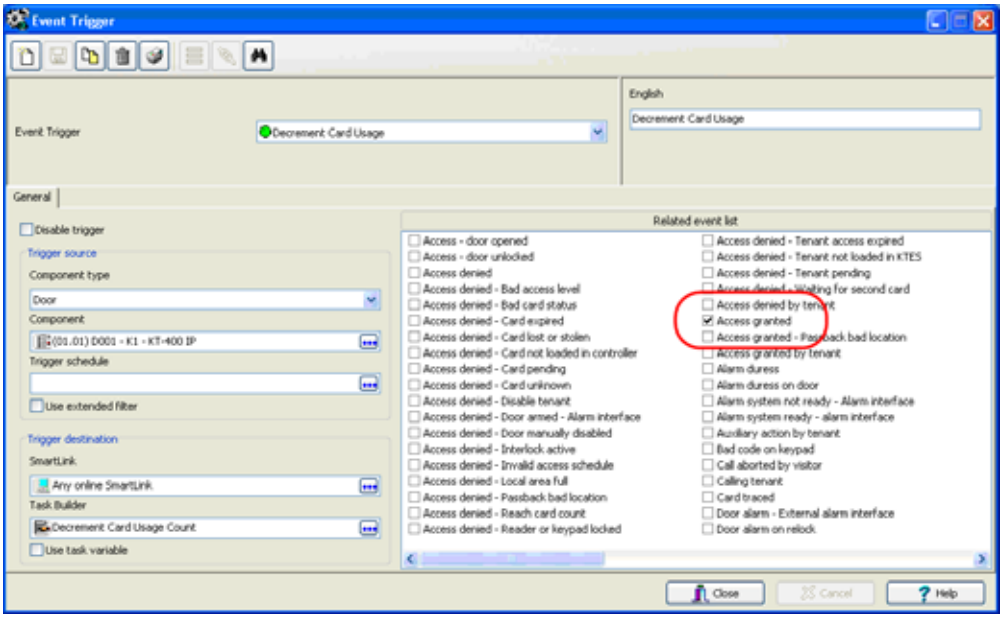


5. Выберите **Decrement count usage** (понижение количества использования) из списка **Command** (команды).
6. Выберите пункт **Message Value** (сообщение о количестве) из списка **Variable** (переменные). Задача будет отображаться в нижнем окне. Нажмите **OK**.



7. Задача SmartLink сейчас отображается в текстовом поле.
8. Нажмите **Save** (сохранить) и закройте окно **Task Builder**.
9. Нажмите из панели инструментов **Definition** (назначение), выберите пункт иконку **Event Trigger (**реакция на событие).
10. Нажмите **New** (новый) и введите **Decrement Card Usage** (понижение количества использования) в качестве имени event trigger(реакция на событие).

11 В разделе **Trigger source**, выберите **Door** из списка компонентов.



12 Нажмите многоточие, чтобы выбрать компонент.

13 В разделе **Trigger destination** (назначение триггера), нажмите на многоточие, чтобы выбрать **SmartLink**.

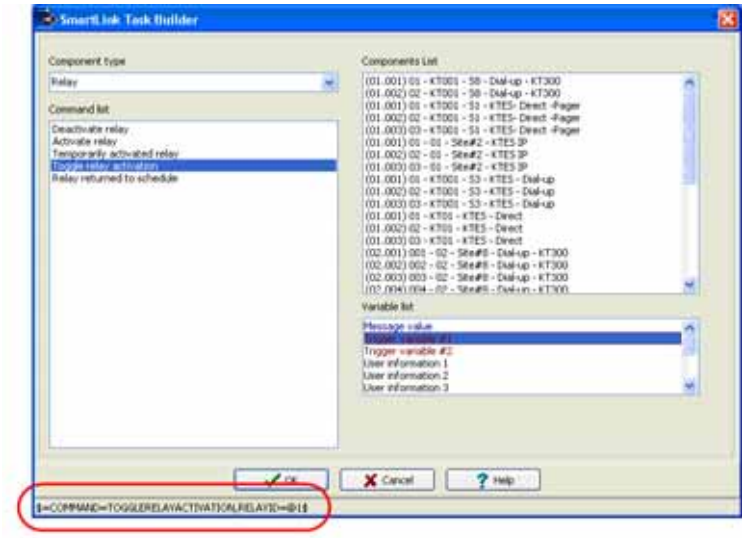
14 Нажмите на многоточие, чтобы выбрать пункт (который вы самостоятельно ранее создали в task builder) **Decrement Card Usage Count** как задачу.

15 Из списка **Related event list** (связанный список событий), выберите событие **Access granted**.

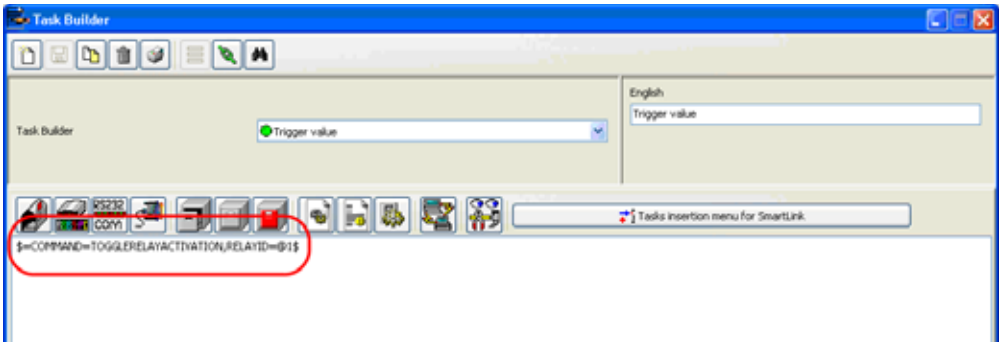
16 Нажмите сохранить и закрыть.

Построение задачи с Trigger Value Variable
(запоминаемое изменяемое количество)

1. Нажмите на вкладку **Definition** (назначение), выберите иконку **Task Builder**.
2. Нажмите **New** (новый) и введите **Trigger value** (запомнить колчество) в названии задачи.
3. Нажмите на кнопку **Command** (команда).
4. Из окна **SmartLink Task Builder**, выберите реле **Relay** из выпадающего списка и укажите **Component type** (Тип компонента).

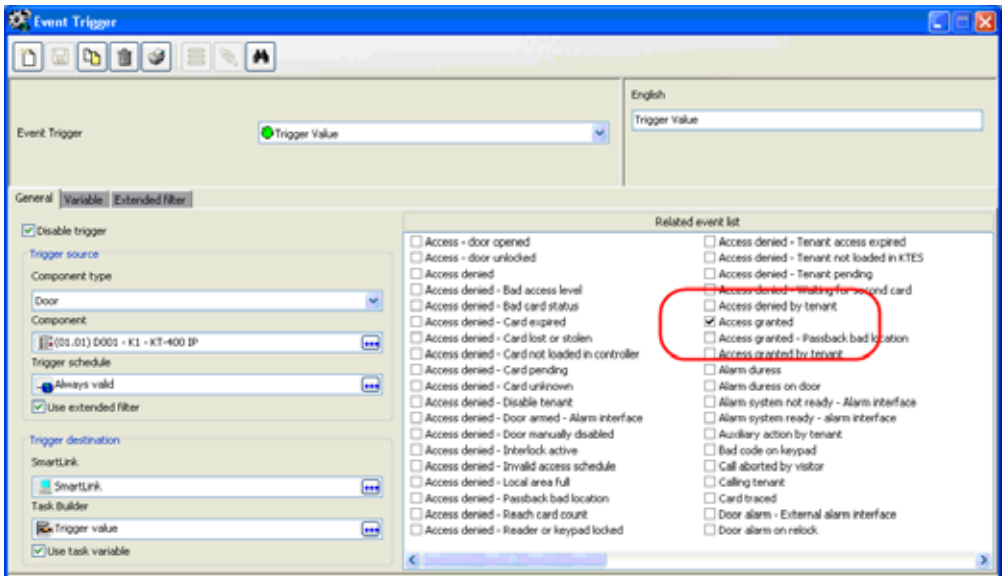


5. Выберите **Toggle relay activation** (переключение реле) из списка команд **Command list**.
6. Выберите пункт **Trigger variable #1** из списка **Variable list** (список изменяемых величин). Текст надачи будет отображаться внизу вашего окна. Затем нажмите **OK**.



7. Сейчас текст задачи SmartLink отображается в этом поле.
8. Нажмите **Save** (сохранить) и закройте окно **Task Builder**.
9. Из панели инструментов выберите вкладку **Definition** (назначение), затем выберите иконку **Event Trigger** (триггер событий/реакция на событие).
10. Нажмите **New** и введите имя триггера **Trigger value** (триггер количества).

11 В разделе **Trigger source** (ресурс триггера), укажите **Door** из списка компонентов .



12 Нажмите многоточие и выберите компонент.

13 Нажмите многоточие и выберите компонентт **Always valid** (верно всегда) в качестве расписания действия триггера в поле **Trigger schedule**.

14 Выделите опцию **Use extended filter** (использовать продлевающееся фильтр).

15 В разделе **Trigger destination** (назначение триггера), нажмите на многоточие и выберите **SmartLink**.

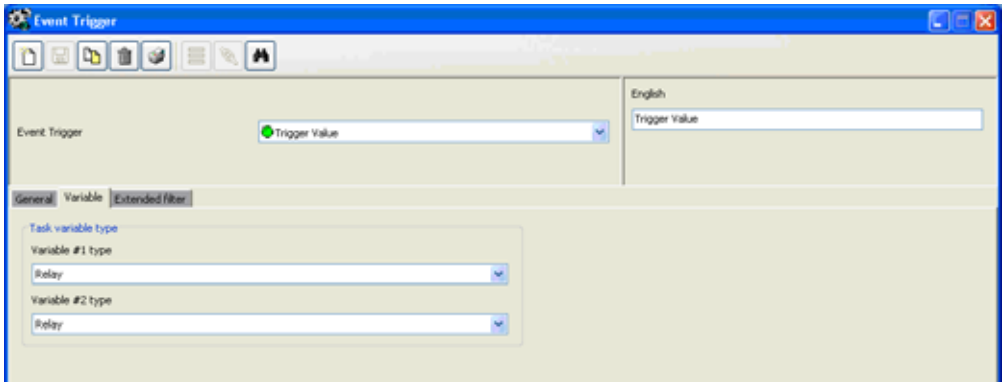
16 Нажмите многоточие и выберите в качестве задачи **Trigger value**.

17 Поставьте галочку на пункте **Use task variable**.

18 Из списка **Related event list** (связанный список событий),выберите событие **Access granted** (доступ предоставлен).

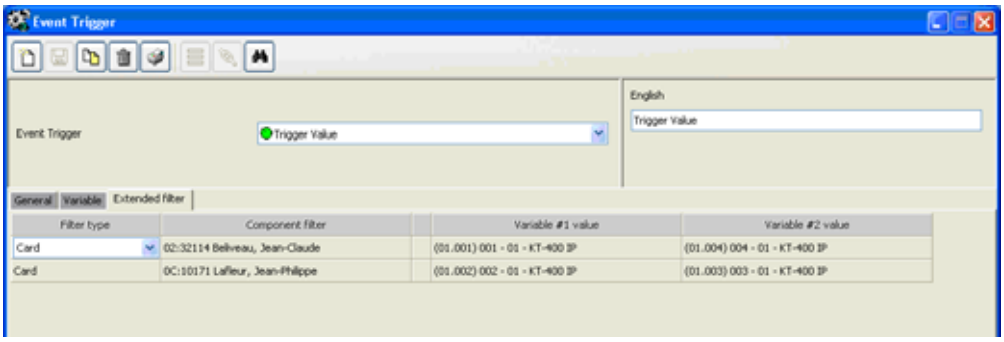
19 Нажмите сохранить **Save**.

20 Нажмите на вкладку **Variable** (изменяемые).



21 Выберите **Relay** для обоих типов.

22 Нажмите на вкладку **Extended filter** (расширенный фильтр).



23 Выберите **Card** в пункте **Filter type.** Затем выберите **component filter** (фильр компонента) для обоих **variables**.

24 Повторите шаги с шаг 23 для других карт, если требуется.

25 Нажмите сохранить и закрыть.

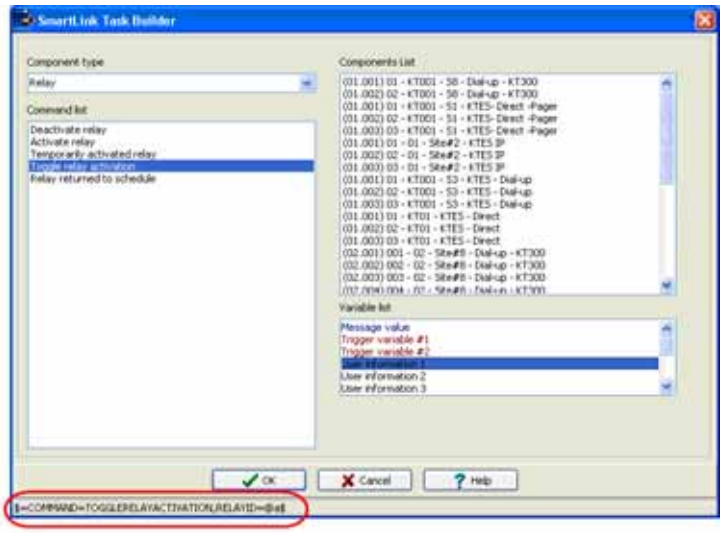
Построение задачи с использованием различной информации пользователя

1 С панели инструментов выберите вкладку **Definition** (назначение), выберите затем иконку **Task Builder**.

2 Нажмите **New** (новый) и введите имя в качестве имени для задачи **Toggle Relay via User Information** (переключить реле через информацию пользователя).

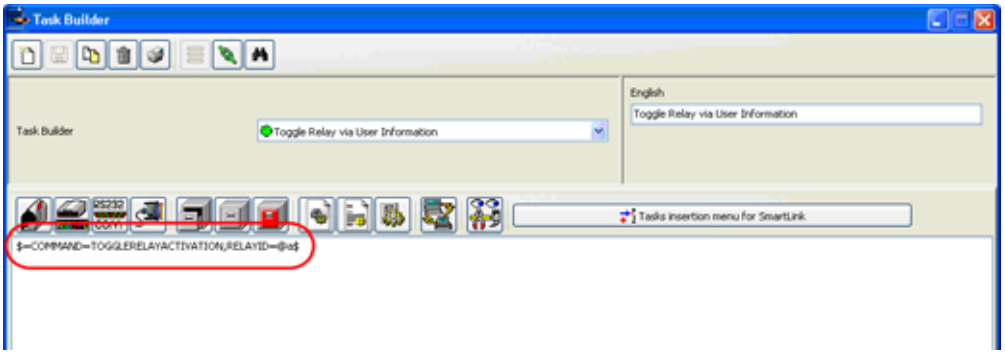
3 Нажмите кнопку **Command** (команда).

4 Из окна **SmartLink Task Builder**, выберите **Relay** из выпадающего пункта **Component type** (тип компонента).



5 Выберите из списка команд слева **Toggle relay activation** (переключить реле).

6 Выберите из списка **Variable list** (изменяемый список) **User Information 1** (информация о пользователе 1). Текст задачи отображается внизу окна. Нажмите **OK**.



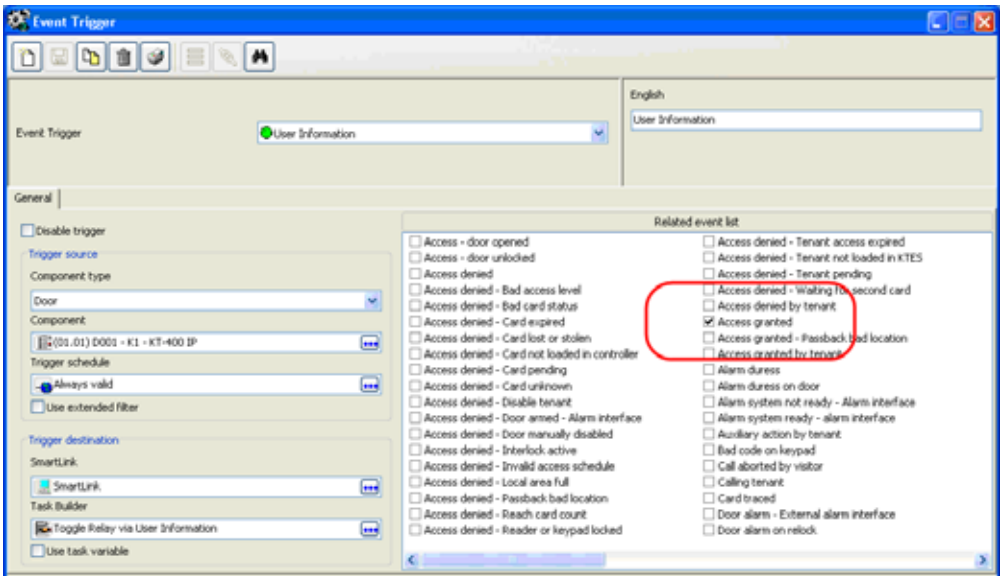
7 Задача SmartLink сейчас отображается в текстовом поле.

8 Нажмите **Save** и закройте **Task Builder**.

9 Из панели инструментов, вкладка **Definition** (назначения), выберите иконку **Event Trigger** (событие триггера).

10 Нажмите **New** (Новый) и введите **User Information** в название триггера.

11 В разделе **Trigger source** (ресурс триггера), выберите тип **Door** (Дверь)из **component type** (список компонентов).



12 Нажмите на многоточие, чтобы выбрать компонент.

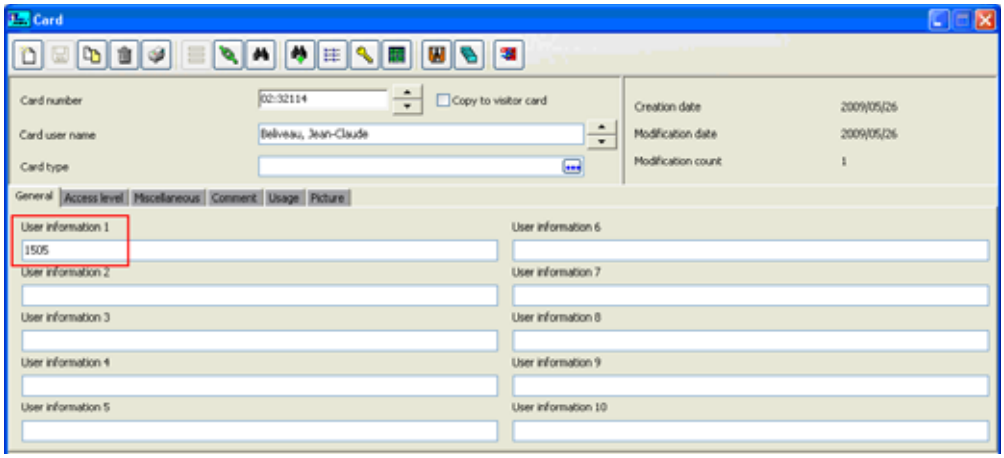
13 Нажмите на многоточие, чтобы выбрать расписание для триггера **Always valid** (действует всегда).

14 В разделе **Trigger destination** (назначение триггера), нажмите многоточие, чтобы указать **SmartLink**.

15 Нажмите многоточие, чтобы выбрать в качестве задачи **Toggle Relay via User Information** (эту задачу мы создавали самостоятельно).

16 Из списка **Related event list** (лист связанных событий), выберите событие **Access granted** (доступ предоставлен).

ПРИМЕЧАНИЕ: *Будьте уверены, что в поле **User Information** введена верная информация. Вы можете для примера ввести в поле **User information** 1505. Это поле вы можете найти **Users**(пользователи) > **Card**(Карта) > **General** (Общие). Это значит, что выбранное реле будет переключаться, когда картодержатель с информации в поле 1505 прошел через дверь.*

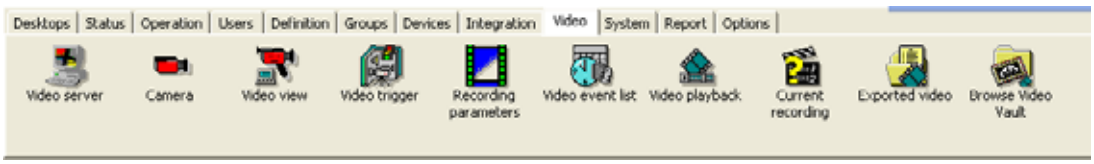


17 Нажмите **Save** (сохранить) и Close (закрыть).

Глава 6 • Интеграция с системами видеонаблюдения

Панель инструментов Video

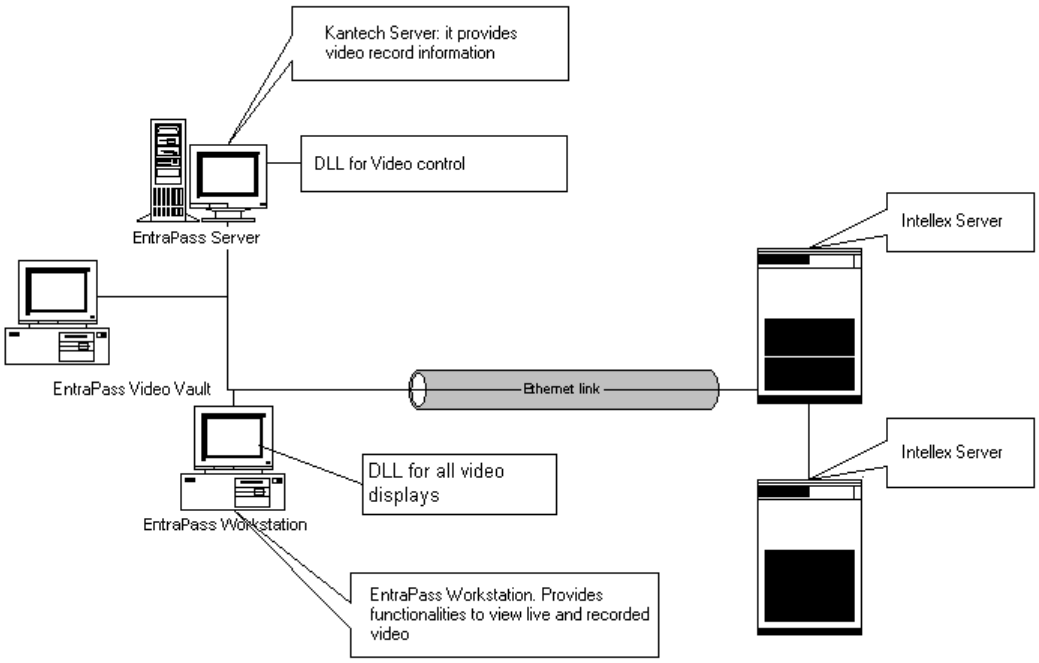
В ответ на общую тенденцию возрастания роли видео в системах контроля доступа в конфигурации EntraPass Global Edition предусмотрена возможность видеонаблюдения в режиме реального времени. Функция видеонаблюдения (Video) позволяет операторам настроить параметры видеонаблюдения и воспользоваться разными возможностями интерфейсов пользователя EntraPass. Администраторы системы EntraPass должны настроить конфигурацию системы видеонаблюдения и параметры просмотра видео, а именно:



- видеосерверы для использования в системе EntraPass (выбор источника видеоданных и описание подключённых к нему камер наблюдения)
- видеоокна на рабочих столах EntraPass для видеонаблюдения
- события, инициирующие включение-выключение видеозаписи
- параметры записи
- видеохранилище EntraPass Video Vault и др.

ПРИМЕЧАНИЕ: *Установка и использование функций видеонаблюдения требуют значительных сетевых ресурсов (LAN или WAN) (пропускной способности сети). Для оптимизации работы сети рекомендуется обратиться к администратору сети.*

Ниже показана схема организации видеонаблюдения в системе EntraPass. Видеохранилище EntraPass Video Vault может быть установлено на одном компьютере вместе с любым другим приложением EntraPass или на специально выделенном компьютере.



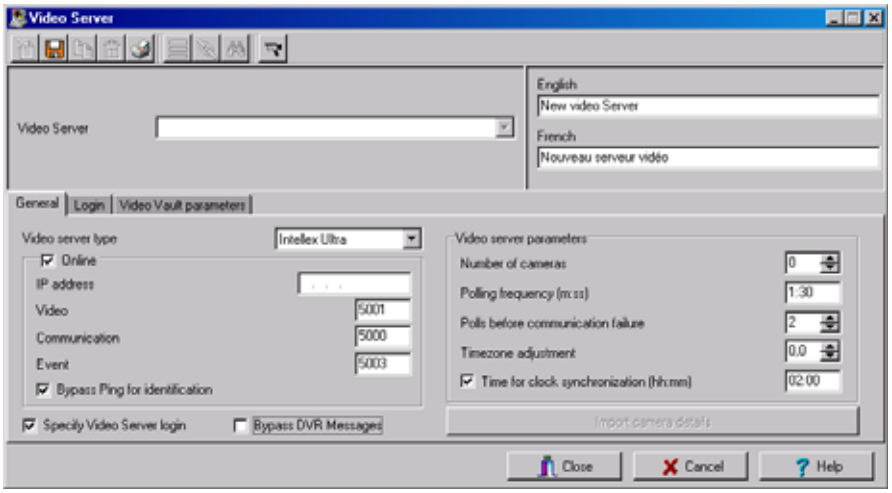
Конфигурация видеосервера

Видеосервер подключается к системе EntraPass через IP-адрес. Видеосервер собирает, хранит и раздаёт видеоданные на рабочие столы EntraPass для видеоконтроля и наблюдения. Доступ к видеоданным может осуществляться с любой рабочей станции EntraPass (с соответствующими правами доступа) по сети. Для того чтобы воспользоваться функциями видеонаблюдения в системе EntraPass, видеосервер должен быть настроен на работу с EntraPass. Для этого необходимо выполнить следующие действия:

- Настроить параметры связи видеосервера
- Указать параметры видеонаблюдения, в частности, число камер наблюдения, подключённых к видеосерверу
- Указать задержки соединения
- Настроить параметры, необходимые для использования видеохранилища и др.

Настройка параметров связи видеосервера

1 В главном окне EntraPass открыть закладку **Video** (Видеонаблюдение), нажать на иконку **Video server** (Видеосерверы) в окне инструментов Video. На экране должно открыться окно Video server с открытой закладкой **General** (Общие параметры).



2 В выпадающем списке **Video server** (Видеосерверы) выбрать сервер, который необходимо настроить (или нажать кнопку **New** (Создать), чтобы создать новый видеосервер). Назначить для этого сервера описательное имя на используемых языках. Если для работы с системой EntraPass используется два языка, рекомендуется создать два имени: одно на основном языке, а другое на дополнительном.

3 В выпадающем списке **Video Server type** (Тип видеосервера) указать тип видеорегистратора.

ПРИМЕЧАНИЕ: *Используемая в настоящий момент версия программного обеспечения интегрируется с системами видеонаблюдения Intellex®, компании American Dynamics. EntraPass поддерживает все версии систем Intellex: DVMS8000 и DVMS16000, Intellex IP (до 16 сетевых видеопотоков), Intellex Ultra (16 каналов) и Intellex LT. Последняя версия работает с ограниченным числом камер (4, 8 или 16) в зависимости от выбранной модели (LT-4, LT-8 или LT-16).*

4 Отметить флажком опцию **On-line**, если видеосервер оперативно доступен..

ПРИМЕЧАНИЕ: *Рекомендуется удалять флажок из поля **On-line**, если сервер длительное время отключён от сети, например, при проведении ремонта. Если этого не сделать, то система EntraPass будет продолжать опрашивать видеосервер, что может привести к её зависанию.*

5 В поле **IP address** указать статический IP-адрес видеосервера. Видеосервер обязательно должен иметь статический IP-адрес. Для получения подробной информации об адресе видеосервера рекомендуется связаться с администратором сети.

6 Указать номера портов для **Video** (Видео), **Communication** (Связь) и **Event** (События). Убедиться, что именно эти порты используются видеорегистратором.

ПРИМЕЧАНИЕ: *Связь видеоприложения с системой EntraPass осуществляется по протоколу TCP (Transmission Control Protocol). Опции, отображаемые в разделе TCP port (Порт TCP), зависят от типа настраиваемого устройства. Подробнее о настройках портов можно узнать у администратора сети или в документации, прилагаемой к видеорегистратору.*

7 Отметить флажком опцию **Bypass Ping for identification** (Пропускать команду PING для идентификации), чтобы снизить нагрузку на сеть. Если эту опцию не выделить, рабочая станция будет постоянно выполнять опрос для идентификации статуса сервера.

8 Выделить опцию **Specify video server login** (Указать видеосерверу логин/пароль), если необходимо, чтобы пользователи вводили свои регистрационные данные, прежде чем получить доступ к видеосерверу. Если эта опция отмечена флажком, то в окне Video Server появляется закладка **Login** (Регистрационные данные).

9 Отметить флажком опцию **Bypass DVR Messages** (Пропускать сообщения видеорегистратора), чтобы пропускать все сообщения, поступающие с модулей Intellex на АРМ.

10 В разделе **Video server parameters** (Параметры видеосервера) выполнить следующие действия:

- Указать в поле **Number of cameras** число камер наблюдения, подключённых к видеосерверу (можно использовать клавиши со стрелками вверх-вниз) или нажать кнопку **Import camera details** (Импортировать данные камер), чтобы получить эту информацию с видеосервера. Кнопка **Import camera details** позволяет быстро настроить камеры, подключённые к видеосерверу. Фактически, при нажатии этой кнопки система EntraPass подсоединяется к видеосерверу и получает с него информацию о количестве и именах по умолчанию для всех камер, подсоединённых к видеорегистратору.
- В поле **Polling frequency (mm:ss)** указать частоту опроса в формате мм:сс. Частота опроса зависит от задержки между двумя опросами, посылаемыми сервером Kantech на видеосервер. Эта операция выполняется при помощи интерфейса видеосервера Kantech.
- Указать в поле **Polls before Communication failure** число неудачных опросов, после которых сервер EntraPass сообщит о потере связи с сервером Intellex. Например, если для этого параметра указано число "4", то EntraPass сделает 4 попытки соединиться с видеосервером, и в случае неудачи объявит о потере связи с сервером.
- Выбрать часовой пояс в поле **Time zone adjustment.** Часовой пояс следует указать при помощи стрелок вверх-вниз в том случае, если он разный для сервера EntraPass и сервера Intellex. Этот параметр зависит от разницы часовых поясов между сервером Intellex и сервером EntraPass. Благодаря настройке временных поясов рабочие станции осуществляют поиск событий, сгенерированных сервером Intellex, по времени, установленному на сервере EntraPass.
- Поставить флажок в поле **Time for clock synchronization** (Часы сверки времени). В соседнем окне следует указать часы, когда видеосервер будет синхронизировать своё время и дату с сервером Kantech. Эта операция выполняется при помощи интерфейса видеосервера Kantech.

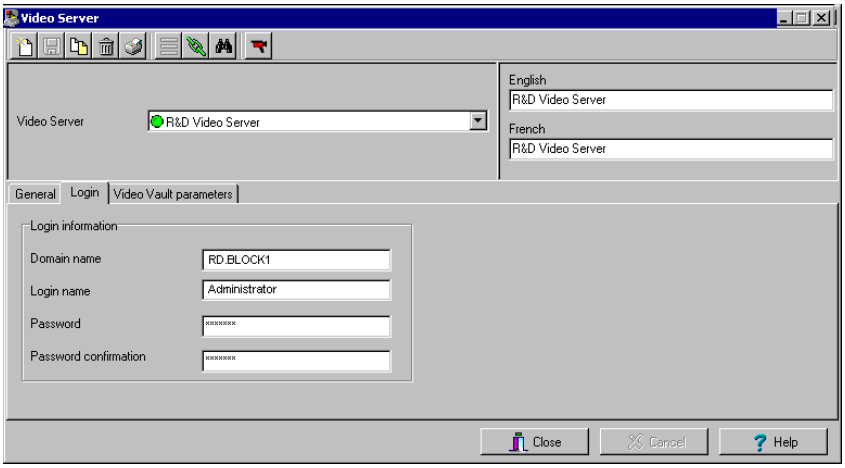
ПРИМЕЧАНИЕ: *Сервер EntraPass служит эталоном времени. Сервер Intellex будет устанавливать время по времени сервера EntraPass. Например, если на сервере EntraPass установлено время 3:00, а на сервере Intellex 2:00, то для правильного отображения информации о событии на сервере Intellex необходимо скорректировать время на -1 (это число должно быть указано в поле Timezone adjustment).*

Повышение уровня защищённости видеосерверов

1 Если для защиты видеосервера Intellex используется Policy Manager, то для доступа к видеосерверу операторам EntraPass будет нужно вводить имя домена, данные регистрации и пароль. В этом случае необходимо поставить флажок в поле **Specify Video server login** (Сообщать видеосерверу регистрационные данные) под закладкой **General** (Общие параметры).

ПРИМЕЧАНИЕ: *Для получения подробной информации о установленных параметрах безопасности на вашем видеосеврере, рекомендуется связаться с сетевым администратором.*

2 Если опция **Specify video server login** отмечена флажком, то появляется новая закладка **Login** (Регистрационные данные). Открыть закладку, чтобы указать данные регистрации.



3 Указать следующие данные:

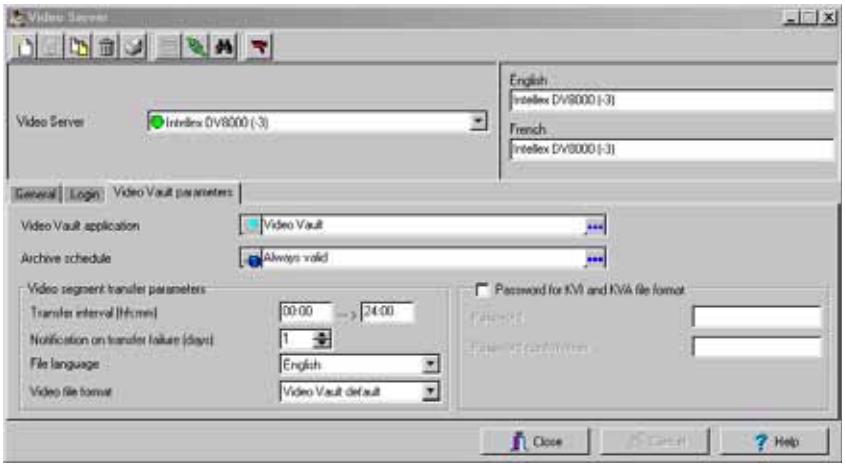
- **Domain Name** (Имя домена). Указать имя домена, используемое видеосервером Intellex.
- **Login name** (Регистрационное имя). Указать регистрационное имя, используемое для доступа к серверу Intellex.
- **Password** (Пароль). Указать пароль для домен домен контроллера.
- **Password confirmation** (Подтверждение пароля). Пароль, указанный в этом поле, должен быть идентичен паролю, введённому строкой выше. В случае получения сообщения об ошибке следует убедиться, что верхний регистр не включен.

Назначение видеохранилища EntraPass Video Vault

Закладка **Video Vault parameters** (Параметры видеохранилища) содержит такие настройки, как расписание для создания архива на video vault и частота передачи данных для видеохранилища (если это приложение активировано в системе EntraPass и настроено на совместное использование с другими приложениями EntraPass).

- Для большей подробной информации об EntraPass Video Vault, *смотрите в Главе 2 'Дополнительные компоненты системы EntraPass' на странице 23*.
- Для большей подробной информации по настройке приложения EntraPass Video Vault, *смотрите в Главе 4 'Настройка конфигурации приложения Видеохранилище EntraPass Video Vault' на странице 80*.
- Для большей подробной информации по использованию приложения EntraPass Video Vault, *смотрите в Главе 16 'Видеохранилище (EntraPass Video Vault)' на странице 520*.

1 В окне **Video server** (Видеосерверы) открыть закладку **Video Vault parameters** (Параметры видеохранилища).



2 Указать данные приложения EntraPass Video Vault:
   - **Video Vault application** – имя приложения видеохранилища EntraPass Video Vault, связанное с выбранным видеосервером.
   - **Archive schedule** – расписание для создания архива. Выбранное расписание указывает время, в течение которого будет выполняться сохранение видеофрагментов. Пока это расписание будет действовать, будет выполняться архивирование всех видеофрагментов, запись которых инициирована указанными пользователем событиями, инициирующими командами видеосервера или в ручном режиме.

3 Настроить параметры передачи видеофрагментов в разделе **Video segment transfer parameters**:
   - **Transfer interval, hh:mm** (Интервал передачи, чч:мм). Это интервал, в течение которого видеофрагменты извлекаются с видеосервера. Эта функция ограничивает время извлечения данных и доступность видеосервера в течение указанного временного интервала.

ПРИМЕЧАНИЕ: *Система Intellex позволяет единовременно извлекать только одну видеозапись. Например, если указан период с 02:00 до 04:00, извлечение видеофрагментов будет выполняться по два часа в день. Если же указан период с 18:00 до 06:00, то будет использоваться интервал времени с шести часов вечера до шести часов утра (двенадцать часов).*

   - **Notify on transfer failure (days)** (Сообщать о неудачной передаче, дни). В этом поле следует указать число дней, выделенных для скачивания видеоданных. Если в течение указанного времени видеофрагмент не удалось извлечь для архивирования, то он считается невосстанавливаемым для архивирования в Video Vault, и приложение EntraPass Video Vault сообщит оператору об ошибке.
   - **File language** (Язык файла). Эта опция доступна только в форматах KVI и KVA. Пользователи могут выбрать, какой язык (английский или французский) использовать для описания архивных данных.
   - **Video file format**: Выбрать формат видеофайлов, которые будут извлечены из видеосервера:
     - **Video Vault default** (Настройки видеохранилища по умолчанию). Это формат, выбранный для настраиваемого видеохранилища: **Devices** (Устройства) > **EntraPass Applications** (Приложения EntraPass)> (Выбрать приложение **Video Vault application**) > закладка **Video Vault Process**).
     - **KVI (Kantech Intellex Video) Format** (Формат KVI). Файл KVI содержит пиктограмму и собственно видеоинформацию с водяными знаками (информацией о подлинности), установленными на вложенных изображениях формата embedded.img. Для просмотра необходима программа Intellex Video Player, которая использует прикладной программный интерфейс API компании American Dynamic. Таким образом, интерфейс API обязательно должен быть установлен на клиентском компьютере.
     - **KVA (Kantech Video AVI) Format** (Формат KVA). Файл KVA содержит пиктограмму и собственно видеоинформацию без нанесённых водяных знаков на вложенное видео формата embedded.avi. Видеофайлы можно просматривать с помощью Windows Media Player или любой другой программы для просмотра файлов AVI.
     - **AVI (Audio Video Interlaced) Format** (Формат AVI). Стандартный формат AVI, без водяных знаков. Видеофайлы можно просматривать с помощью Windows Media Player или любой другой программы для просмотра файлов AVI.
     - **IMG Intellex Format** (Формат **IMG Intellex).** Размещает на видеокадрах водяные знаки. Для просмотра необходима программа Intellex Video Player, которая использует прикладной программный интерфейс API компании American Dynamic. Таким образом, интерфейс API обязательно должен быть установлен на клиентском компьютере.

4 Для повышения уровня безопасности отметить флажком опцию **Use a password for KVI and KVA file formats** (Использовать пароль для файлов формата KVI и KVA). Обращаем внимание, что записи в полях **Password** (Пароль) и **Password Confirmation** (Повторный ввод пароля) должны быть идентичными. В таком случае для просмотра архивных видеофрагментов, хранящихся в данном хранилище, операторы должны ввести этот пароль. Архивные файлы можно просматривать в окне Browse Video Vault.

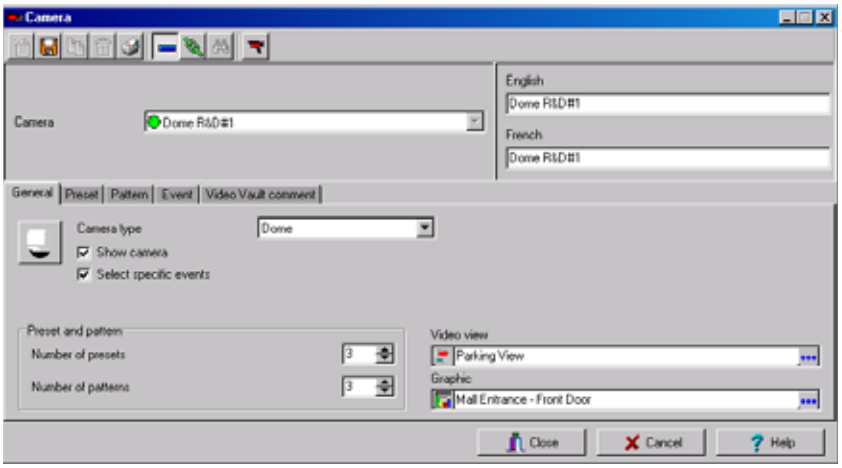
Назначение камер

- В системе EntraPass предусмотрена возможность назначения имён камерам, предустановкам (preset) и маршрутам движения камер (pattern) для облегчения идентификации объектов на рабочем столе видеонаблюдения (Video) и при поиске видеособытий. При описании камеры наблюдения указываются следующие параметры:
- Тип (неповоротная или купольная)
- Предустановки (preset) (для купольных камер)
- Маршруты (pattern) (для купольных камер)

Имя камеры отображается при просмотре видеозаписей и при видеонаблюдении в реальном времени. По умолчанию камерам присваиваются имена *Camera1 ... Camera n (где n – последний номер камеры).*

Назначение камеры (раздел Camera)

1 В инструментах окна Video нажать кнопку **Camera** (Камеры наблюдения). Открывается окно Camera.



2 В выпадающем списке Camera выбрать камеру наблюдения, которую необходимо настроить и назначить для неё описательное имя на используемых языках. Если для работы с системой EntraPass используется два языка, рекомендуется создать два имени: одно на основном языке, а другое на дополнительном.

3 В выпадающем списке **Camera type** выбрать тип камеры:
- **Fixed camera** (Неповоротная камера) – не имеет предустановок/маршрутов, не предусмотрена возможность управления камерой.
- **Dome** (Купольная камера) – может работать по предустановкам/маршрутам, операторы имеют возможность управления камерой. В случае выбора этой опции следует указать описательные имена для предустановок камеры.

4 Чтобы камера была доступной для выбора и отображения на рабочем столе видеонаблюдения, следует отметить флажком поле **Show camera** (Показывать камеру). Эта опция обязательно должна быть выделена, чтобы камера была доступной в системе EntraPass. Камеры, не отмеченные флажком (так называемые "скрытые" камеры), будут доступны для наблюдения только операторам с особыми полномочиями. Для назначения оператору особых полномочий следует перейти в меню **System** (Системные настройки) > **Operator definition** (Назначения операторов) > **Privileges** (Особые права).

ПРИМЕЧАНИЕ: *Если опция **Show camera** (Показывать камеру) не выделена, камера не будет отображаться в списке компонентов, доступных для вывода в видеоокно (**Video view** (Видеоокно) > **Modify video view components** (Изменить компоненты видеоокна)) и, соответственно, её нельзя будет вывести на рабочий стол для видеонаблюдения. Такой режим позволяет скрыть камеру ото всех. Операторы, не имеющие особых полномочий, не смогут выполнять просмотр, поиск, экспортирование данных и любые другие действия с этой камерой. Однако все ссылки и связи с этой камерой будут сохраняться. В этом отличие данной функции от функции удаления камеры: при удалении камеры все ссылки и связи также удаляются.*

5 Выделить поле **Select specific events** (Выделить особые события), если необходимо, чтобы камера записывала особые события. По умолчанию все события камеры отображаются в списке видеособытий EntraPass (Video Events List). Однако, эта опция позволяет выбрать, какие события будут записываться этой конкретной камерой. При выделении этой опции появляется закладка **Event** (События). Здесь следует указать, какие события будут записываться настраиваемой камерой.

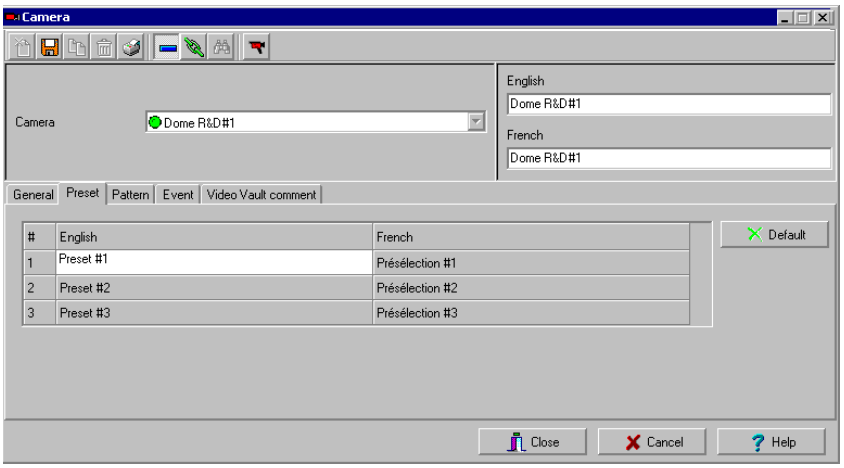
6 С помощью кнопок вверх/вниз определить количество предустановок и маршрутов движения (pattern) выбранной камеры (если она купольная). После этого в окне **Camera** появятся закладки **Preset** (Предустановки) или **Pattern** (Маршруты).

7 Указать, в каком формате выводить изображение при возникновении тревоги.

- **Video View** (Видео) – при переключении камеры в тревожный режим на экране будет отображаться видеоизображение в выбранном видеоокне.
- **Graphic View** (Графические схемы) – при переключении камеры в тревожный режим на экран будет выведено выбранное графическое изображение.

Назначение предустановок и маршрутов (preset и pattern)

1 В окне Video server (Видеосерверы) открыть закладку **Preset** (Предустановки) или **Pattern** (Маршруты) для назначения каждой предустановке подходящего имени.



2 Выбрать нужную ячейку в таблице и заменить имя по умолчанию на другое, более подходящее имя. Если для работы с системой используется два языка, следует указать два имени: одно на основном языке, а другое на дополнительном. Затем нажать кнопку **Close** (Закрыть), чтобы закрыть окно предустановок (маршрутов).

ПРИМЕЧАНИЕ: *Если выделить предустановку/маршрут движения камеры и нажать кнопку* ***Default*** *(Настройки по умолчанию), то имя выделенной предустановки/маршрута будет заменено на имя по умолчанию.*

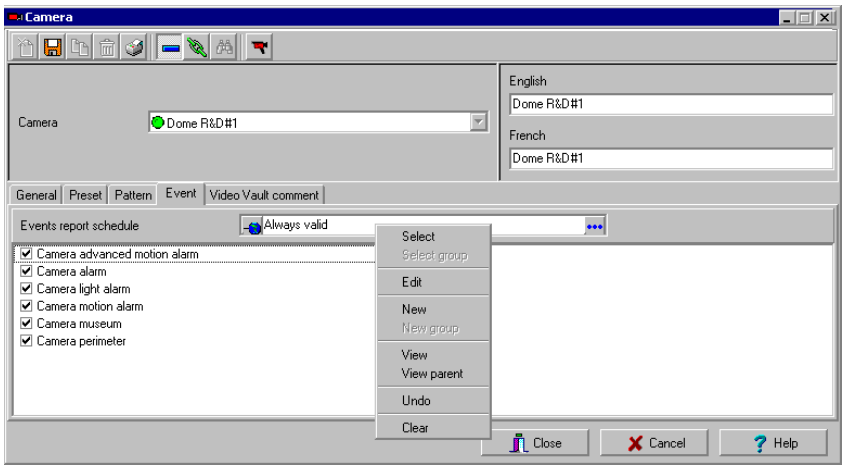
Назначение событий для записи камерой

После выделения опции **Select specific events** (Выделить особые события) под закладкой **General** (Общие параметры) следует выполнить следующие действия:

- Выбрать события, которые будут записываться настраиваемой камерой и затем будут отправлены на сервер EntraPass. **Эта опция недоступна, если камера подключена к видеорегистратору типа Intellex LT.**
- Выбрать или создать новое расписание, по которому выбранные события будут передаваться с видеосервера на сервер EntraPass. Это расписание выполняет роль фильтра, так как позволяет ограничить количество сообщений, передаваемых видеосервером на сервер EntraPass. Например, при выборе расписания "Always valid" (Достоверно всегда) на сервер EntraPass будут передаваться всегда выбранные события. А при указании ограниченного временного интервала будут передаваться события, которые случились в этом указанном интервале.

Порядок выбора событий и расписаний для записи камерой

1 В окне Camera (Камеры наблюдения) открыть закладку **Event** (События). Открывшийся список будет содержать все типовые события камеры. Список событий зависит от того, какой видеорегистратор выбран.



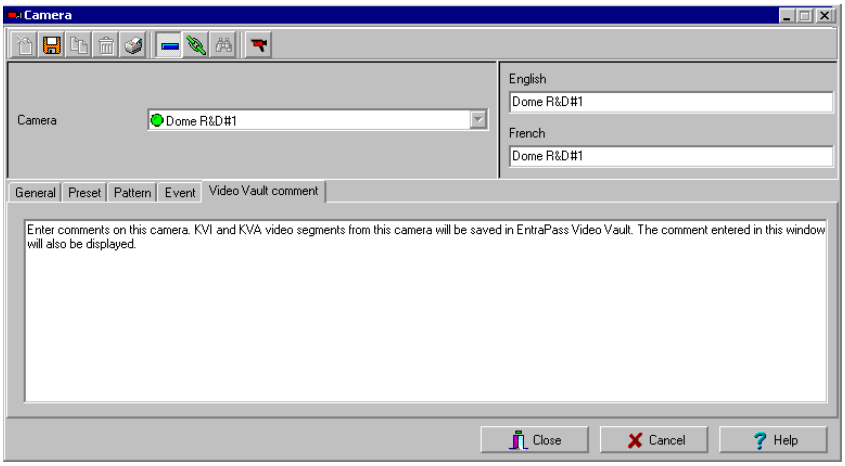
2 Выбрать расписание для передачи сообщений о событиях камеры. На сервер EntraPass будут отправляться только те события, которые будут записаны в указанный интервал времени. При нажатии на правую кнопку мыши в окне выбора расписания всплывает контекстное меню, позволяющее оператору создать новое расписание или выбрать одно из уже созданных. *Если вы назначаете расписания, будьте уверены, что вы выбираете правильную категорию этого расписания. Например, если вы назначаете системное расписание (для АРМ, оператора, параметров соыбытий,видео триггеров), то это расписание будет доступно для выбора этой категории. Если вы выбраете для физических компонентов (контроллеры, двери, входы), то эти расписания будут сгруппированы по шлюзу если вы используйте Global Шлюз и по лучу(сайту) если вы используйте Corporate шлюз. Если вы назнаяили 2 луча/сайта в вашей системе, то там будет две различные группы расписаний для каждого луча/сайта. Вы можете назначить до 99 расписаний на каждый луч/сайт. на странице 174*.

3 Выбрать те события камеры, которые необходимо отправлять на сервер EntraPass. Создание более точного списка событий, отправляемых на сервер Intellex, позволяет снизить трафик видеоданных и уменьшить нагрузку на сеть. Список событий зависит от типа видеосервера. Ниже приведён список событий, доступных на серверах Intellex:

- **Camera advanced motion alarm** (Усиленная сигнализация о движении). Камера будет посылать все события, связанные с тревогой по детектору движения на данной камере.
- **Camera alarm** (Сигнализация камеры). Камера будет посылать любое событие, связанное с тревогой в охраняемой области.
- **Camera motion alarm** (Сигнализация о движении). Камера будет отправлять серверу EntraPass события, о любом движении на контролируемой территории. Имеется в виду, что если в настройках камеры на Intellex вы выделили детектор движения в виде области, то движение в этой области вызовет тревогу.
- **Camera museum** (Режим музея).
- **Camera perimeter** (Сигнализация о движении по периметру). Камера сообщает серверу EntraPass о любом пересечении границ контролируемой территории. Имеется в виду, что если в настройках камеры на Intellex вы выделили детектор движения на камере в виде периметра, то пересечение этой области вызовет тревогу.

4 Открыть закладку **Video Vault Comment** (Комментарий для видеохранилища), чтобы добавить комментарий для настраиваемой камеры. Файлы, полученные с этой камеры и отправленные в

видеохранилище в формате KVI и KVA, будут отображаться с комментарием, который введён в этом окне.

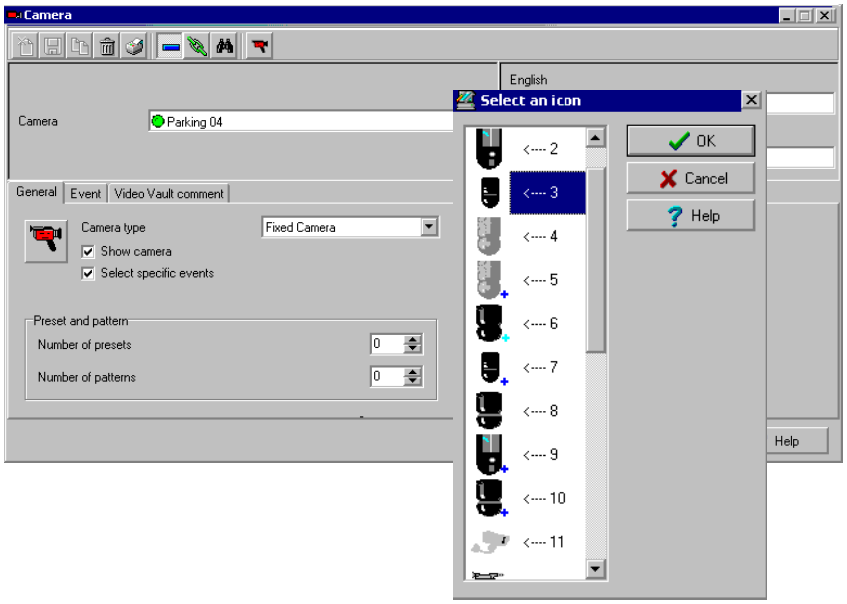


5 Введите комментарий к настраиваемой камере наблюдения. Нажмите кнопку сохранить и затем закройте окно.

Установление связи камеры с иконкой

В системе EntraPass предусмотрена возможность назначения для камеры определённой иконки для облегчения идентификации объектов на рабочем столе видеонаблюдения (Video) и на графических планах системы (Graphic).

1 В окне Camera (Камеры) указать камеру наблюдения, для которой необходимо назначить иконку, затем щёлкнуть мышью один раз или дважды по кнопке рядом с надписью "Camera type" (Тип камеры). При этом открывается окно **Select an icon** (Выбрать иконку).



2 Выбрать иконку для настраиваемой камеры и дважды щёлкнуть по ней, чтобы закрыть окно. После этого между камерой и иконкой устанавливается связь по номеру иконки.

ПРИМЕЧАНИЕ: *Иконка камеры, расположенная в окне Camera на панели инструментов, позволяет добавлять свои иконки в список доступных иконок. Кнопки* **Add** *(Добавить) и* **Delete** *(Удалить) позволяет добавлять другие иконки, а также удалять иконки, отображаемые в списке. Список иконок отображается при нажатии иконки Camera (Камера) на панели инструментов.*

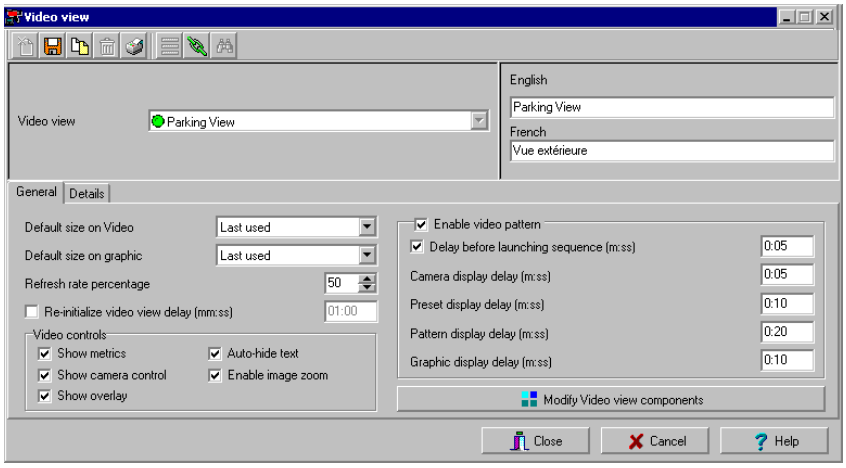
Назначение окон видео VideoView

После настройки видеосервера и назначения камер, операторы получают возможность настраивать видеоокна, отображаемые на рабочем столе видеонаблюдения для целей мониторинга и просмотра. После этого операторы EntraPass могут вызывать уже настроенные предустановки и маршруты движения. Число предустановок, которые можно описать в системе, не ограничено.

Между устройствами EntraPass (рабочие станции APM, шлюзы, лучи/сайты, контроллеры и др.) и видеоокнами можно установить связь. Позже, в меню описания компонентов можно назначить видеоокно, которое будет использоваться для отображения конкретного компонента в окне видео.

Назначение общих параметров для видеоокон

1 На панели инструментов в окне Video нажать кнопку **Video view** (Видеоокна). На экране должно открыться окно Video View с открытой закладкой **General** (Общие параметры).



2 В выпадающем списке **Video view** выбрать уже существующее видеоокно (или нажать кнопку **New** (Создать), чтобы создать новое видеоокно). Назначить для этого видеоокна описательное имя на используемых языках. Если для работы с системой EntraPass используется два языка, рекомендуется создать два имени: одно на основном языке, а другое на дополнительном.

3 В выпадающем списке **Default size on video** (Размеры по умолчанию) указать размеры отображаемого окна: если помимо окна видеонаблюдения на экран будет выведено другое окно, рекомендуется выбирать меньший размер.

- **Large** (Большой) 1024x768
- **Medium** (Средний) 800x600
- **Small** (Малый) 640x480
- **Tiny** (Миниатюрный) 400x300
- **Last used** (Последний использованный) размер, который был использован на рабочем столе Video в предыдущий раз.

4 В выпадающем списке **Default size on graphic** (Размер по умолчанию для изображений) указать размер кадра, который будет отображаться на графических схемах системы (Large, Medium, Small, Tiny, Last used).

5 В поле **Refresh rate percentage** указать частоту обновления в процентах, используя кнопки со стрелками вверх/вниз.

ПРИМЕЧАНИЕ: *Частота обновления (***Refresh Rate Percentage***) связана с качеством/степенью сжатия изображения. Качество изображения влияет на производительность системы: чем выше качество, тем ниже степень сжатия изображения и ниже производительность системы. При высокой степени обновления (> 80) сжатие будет низким. В результате для работы приложения потребуется больше сетевых ресурсов. Это может замедлить работу программы. Рекомендуемые значения параметров приведены в таблице:*

Качество	Описание	Результат
80 и выше	Очень высокое качество	Изображения сохраняются с максимальным качеством при минимальном сжатии. Требует много места на жёстком диске и большую пропускную способность сети
50	Нормальное, настройки по умолчанию	Изображения записываются со стандартным качеством. Используется оптимальное соотношение между степенью сжатия и занимаемым местом на диске. При уменьшении качества труднее найти небольшие различия кадров.
40	Низкое качество	Изображения сохраняются с минимальным качеством и с максимальной степенью сжатия. Занимают минимальное место на диске и не сильно нагружают сеть.

6 Выделить опцию **Re-initialize video view delay, mm:ss** (Задержка на повторную инициализацию видеоокна, мм:сс), если требуется выполнять обновление изображения на экране. При выделении этой опции изображение будет автоматически обновляться с указанным интервалом. Эта функция особенно полезна при использовании маршрутов движения настраиваемой камеры или предустановок.

7 В разделе видеонаблюдения (Video) необходимо выполнить следующие настройки:
- **Show metrics** (Показывать данные) – отображать для выбранной камеры число кадров в секунду (Fps) и число битов в секунду (Bps). Эта информация отображается в верхней части видеоокна (и на рабочем столе Video).
- **Show camera controls** (Показывать кнопки управления камерой) – для купольных камер. Эта опция позволяет операторам управлять купольной камерой. Для фиксированных камер недоступна.
- **Show overlay** (Показывать субтитры) – выводить на рабочий стол видеонаблюдения данные идентификации камеры (имя камеры и сервер).
- **Auto-hide text** (Автоматически скрывать текст) - при выделении этой опции система не будет отображать информацию, имеющую отношение к камере наблюдения.
- **Enable camera zoom** (Сделать доступным зум) – отображать на экране значение зума для выбранной камеры.

ПРИМЕЧАНИЕ: *Опция Enable video pattern (Разрешить использование автотура) становится доступной после выбора компонентов, которые будут отображаться в этом видеоокне*

8 Поставить флажок в поле **Enable video pattern** (Разрешить использование автотура), чтобы поочередно выводить изображения в указанное видеоокно. Если в настройках выбран формат 2X2, то видеошаблон будет состоять из четырёх изображений, поочерёдно выводимых на экран с задержкой, указанной в поле **Camera display delay** (Длительность отображения камеры). Если опция не выделена, видеоокно будет показывать статическое изображение.

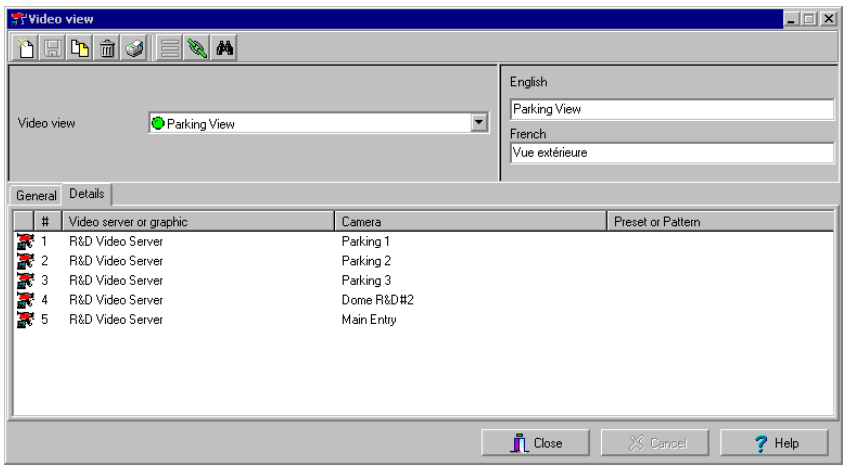
9 Отметить флажком поле **Delay before launching sequence, m:ss** (Задержка перед запуском последовательности, м:сс), чтобы указать задержку переключения перед началом последовательного вывода изображения в видеоокно.

10 Указать задержку отображения камеры **(Camera display delay)**, предустановок (**Preset display delay)**, маршрутов движения **(Pattern display delay)** и окна графики **(Graphic display delay)**.

ПРИМЕЧАНИЕ: *Эти параметры описывают временной интервал в течении которого , вам будет отображаться предыдущее изображение на экране видео или графики перед сменой изображения. Минимальные значения (значения по умолчанию) приведены в таблице ниже. Максимальное значение составляет 9:59 секунд.*

Задержка	Минимальное значение (сек)
Delay before launching sequence (Задержка перед запуском последовательности)	2 сек
Camera display delay (Задержка отображения камеры)	3 сек
Preset display delay (Задержка отображения предустановки)	5 сек
Pattern display delay (Задержка отображения автотура/pattern)	10 сек
Graphic display delay (Задержка отображения графики)	5 сек

11 Открыть закладку ***Details*** (Подробные сведения) для просмотра данных о выделенном видео окне: видеосерверах (video servers), камерах наблюдения (cameras), а также (если используются) о предустановках камеры (presets) и маршрутах (patterns).



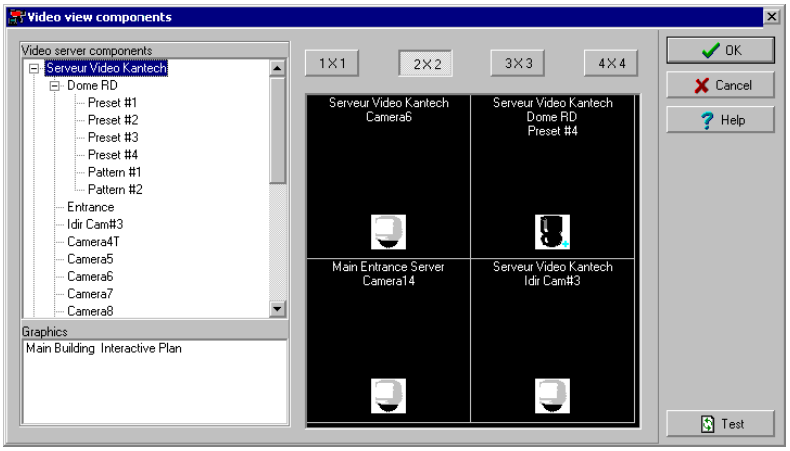
Создание и редактирование видеоокон

Использование предустановок и маршрутов движения позволяет пользователям настроить автоматическую работу купольных камер. Видео, передаваемое камерами наблюдения, отображается на АРМ. Предварительная настройка режимов видеонаблюдения обеспечивает оптимизацию времени наблюдения. Система EntraPass предоставляет широкие возможности выбора режима наблюдения, в зависимости от нужд пользователей:

- Одна камера
- Несколько камер
- Несколько графиков и камер
- Окно "одного" видеосервера – создаётся перетягиванием мышью этого сервера в видеоокно.
- Несколько видеосерверов: в зависимости от нужд пользователей, в системе EntraPass предусмотрена возможность создания изображений с нескольких видеосерверов.

Изменение видеоокна

1 В окне видеонаблюдения (Video view) нажать кнопку **Modify Video view components** (Изменить компоненты видеоокна), чтобы изменить или создать новое содержание на рабочем столе видеонаблюдения.



2 В левой колонке выбрать камеру (camera), предустановки камеры (preset) или маршруты движения (pattern) и перетащить выбранный объект в правую часть окна. Для идентификации камеры используется имя камеры и соответствующая иконка. Для идентификации предустановки используется имя камеры и имя предустановки.

ПРИМЕЧАНИЕ: *Какую-либо конкретную камеру можно вывести одновременно сразу в несколько ячеек видеоокна, однако в этом случае обязательно должна быть выделена опция* **Enable video sequence** (Разрешить последовательный вывод кадров в разные ячейки видеоокна). *Вывод графика допускается только в одну ячейку видеоокна. Допускается вывод камер с другого видеосервера, однако источник видео должен быть от одного и того же поставщика.*

3 С помощью кнопок в верхней части окна указать число ячеек, на которые должно быть разбито видеоокно:

- 1 X 1 – одна ячейка
- 2 X 2 – 4 ячейки
- 3 X 3 – 9 ячеек
- 4 X 4 – 16 ячеек

ПРИМЕЧАНИЕ: *Окно "одного" видеосервера создаётся перетягиванием этого сервера в экран наблюдения. В этом случае в видеоокне будут отображаться все камеры с этого сервера.*

ПРИМЕЧАНИЕ: *От числа изображений, выводимых на экран видеонаблюдения, зависит скорость передачи данных по сети. Например, в режиме 4X4 пропускная способность сети будет ниже, чем при работе в режиме 1X1.*

4 Для просмотра результатов выбора изображений следует нажать кнопку **Test** (Проверить). Настраиваемое видеоокно появляется на рабочем столе Video для видеонаблюдения: **Desktops** (Рабочие столы) > Desktop dedicated to video monitoring (Рабочий стол для видеонаблюдения).

ПРИМЕЧАНИЕ: *Чтобы удалить камеру из ячейки видеоокна, следует щёлкнуть по ней правой кнопкой мыши, и выбрать в контекстном меню команду* ***Delete*** *(Удалить).*

5 Нажать кнопку **Close** (Закрыть), расположенную в левом нижнем углу (или “X” в правом верхнем углу), чтобы закрыть тестовое окно.

Video Triggers - События, инициирующие включение-выключение видеозаписи

Это события, возникновение которых влечёт за собой запуск или остановку записи. Любое событие, связанное с компонентом выбранного типа, может включать-выключать запись, включая особые события, поступающие с видеосервера. Для каждого типа инициирующего события должен быть указан компонент-источник. Например, для сообщения о взломе двери (Door forced) должен быть указан компонент “Door” (Дверь). Число инициирующих событий не ограничено.

Назначение параметров инициирующих событий для запуска Video Trigger

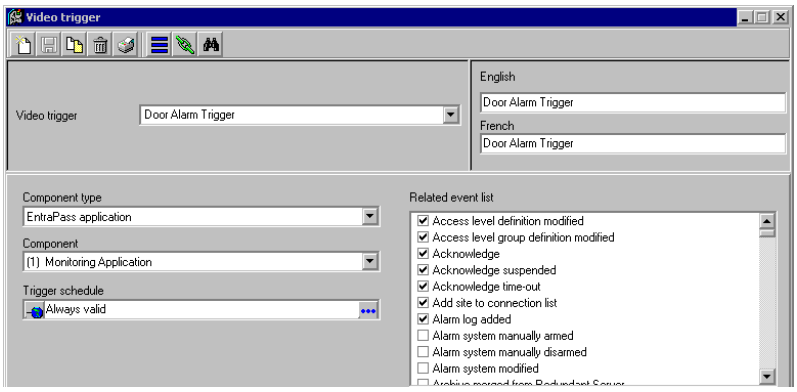
Необходимо указать следующую информацию:

- Название на двух языках
- Component type - тип компонента, используемого для включения video trigger. События связаны с компонентами системы: тревожными системами (alarm system), областями, guard tour, шлюзами, сайтами/лучами, контроллерами и т.п.

В зависимости от того, какое событие происходит с выбранным компонентом, запись запускается или останавливается.

ПРИМЕЧАНИЕ: *Список параметров зависит от типа видеосервера, подсоединённого к системе EntraPass. Этот список будет зависеть от доступности функций сервера и его последующего оснащения. Любые события EntraPass могут использоваться в качестве запуска video trigger.*

1 На панели инструментов Video нажать кнопку **Video trigger** (Инициирующие события). Откроется окно Video trigger.



2 Нажать иконку New (Создать) или выбрать уже созданный video trigger (инициирующее событие), который необходимо изменить. Назначить этому trigger описательное имя.

ПРИМЕЧАНИЕ: *При попытке сохранить настройки без указания типа компонента или без назначения компонента для настраиваемого trigger, система выдаёт на экран предупредительное сообщение.*

3 В выпадающем списке **Component** (Компонент) указать, какой компонент необходимо использовать для инициации записи. Это может быть дверной контроллер, например

4 В поле **Trigger schedule** (Расписание включения trigger) указать расписание возможности работы данного trigger. При необходимости можно указать особое расписание для включения этого trigger в поле (**Definition** (Описания) > **Schedule** (Расписания)). Если никакого расписания для события не выбрано, trigger работать не будет.

5 В списке **Related event list** (Список связанных событий) указать одно или несколько событий, связанных с video trigger.

Параметры записи (Recording Parameters)

Меню **Recording Parameters** позволяет пользователям назначать параметры видеозаписи и назначить источник записи (Intellex, камера итд) и привязывать все это к определенному триггеру. Для каждого события записи вам следует указать параметры: источник-видеосервер, камера и др.

Запись может останавливаться по указанному таймеру (максимальное время записи) или по инициирующему событию (команды от видео trigger), если какой-либо video trigger используется для остановки записи.

Для каждого инициирующего события триггера должен быть указан компонент-источник. Например, для сообщения о взломе двери (Door forced open) должен быть указан компонент “Door” (Дверь). Также следует указать действие для этого trigger (запуск или остановка записи).

Система EntraPass даёт возможность связать несколько параметров записи с одним trigger. В этом случае, все записи будут связаны с одним событием, и будет возможно сохранить все записанные видеофрагменты как запись одного события.

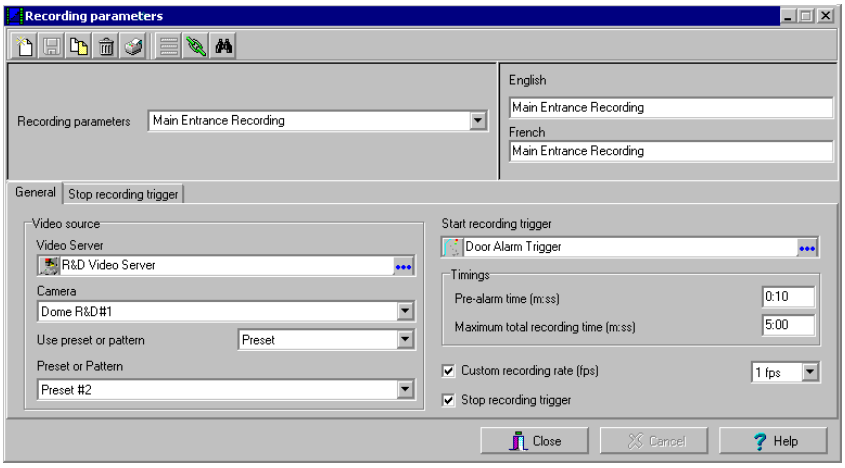
Настройка параметров записи

Окно Video record (Запись видео) позволяет настроить параметры записи видеофрагментов по командам от EntraPass. Для доступа к этому меню необходимо обладать соответствующими полномочиями.

Количество настраиваемых параметров записи не ограничено. Необходимо указать следующую информацию:

- Название на двух языках (если система настроена на два языка)
- Источник видеозаписи (сервер и камера)
- Предустановки и маршруты движения
- Trigger, инициирующий запись
- Время предтревожной записи
- Максимальное общее время записи и др.

1 На панели инструментов в окне Video нажать кнопку **Recording parameters** (Параметры записи). На экране должно открыться окно Recording parameters с открытой закладкой **General** (Общие параметры).



2 Нажать кнопку **New** (Создать) для создания новых параметров записи или выбрать один из пунктов в выпадающем списке **Recording parameters** и присвоить ему описательное имя.

3 В окне **Video server** (Видеосерверы) открыть видеосервер, который будет использоваться для назначения параметров записи.

4 В выпадающем списке **Camera** выбрать камеру для этих параметров записи.

ПРИМЕЧАНИЕ: *Если выбрана купольная камера, пользователь может указать имя и номер предустановки* (**Preset**) *или маршрута движения камеры* (**Pattern**). *Настройка этих функций позволяет направить камеру в нужном направлении для выполнения записи. Однако функция предтревожной записи не всегда хорошо работает при использовании предустановок/маршрутов. Фактически, предтревожная запись может включиться в момент, когда камера находится не в том положении, из которого должна выполняться запись при возникновении инициирующего события.*

5 Во всплывающем окне **Start recording trigger** (trigger начала записи/инициирующее событие записи) выбрать video trigger, который необходимо связать с настраиваемыми параметрами записи. Всплывающее окно Video trigger содержит список всех видео триггеров, назначенных в системе.

6 В меню **Timings** (Временные настройки) необходимо указать следующие параметры:
- **Pre-alarm time, m:ss** (Время предтревожной записи, м:сс) – позволяет получить с сервера Intellex видеофрагмент, записанный перед началом записи по тревоге. Например, если запись началась в 2:00 после полудня, а длительность предтревожной записи установлена равной 1 мин. 0 сек., то записанный видеофрагмент будет иметь начало в 1 ч 59 мин.
- **Maximum total recording time, m:ss** (Максимальная общая длительность записи, м:сс) – эта опция служит для указания максимальной длительности записи. Сюда включено время предтревожной записи, но не входит время посттревожной записи. Максимальное значение – 5 минут.

7 Отметить флажком опцию **Custom recording rate, fps** (Скорость записи по выбору пользователя, к/с), чтобы разрешить пользователям выбирать частоту смены кадров при записи и использовать её вместо настроек Intellex.

ПРИМЕЧАНИЕ: *Эта функция будет действовать только при условии, что ранее при настройке параметров сервера Intellex была выделена опция* **Use Auto Rate Mode** *(Использовать автоматический режим выбора скорости). При выделении опции* **Use Camera Selectable Rate** *(Использовать скорость по выбору камеры) функция* **Custom recording rate** *(Скорость записи по выбору пользователя) будет недоступна в системе EntraPass.*

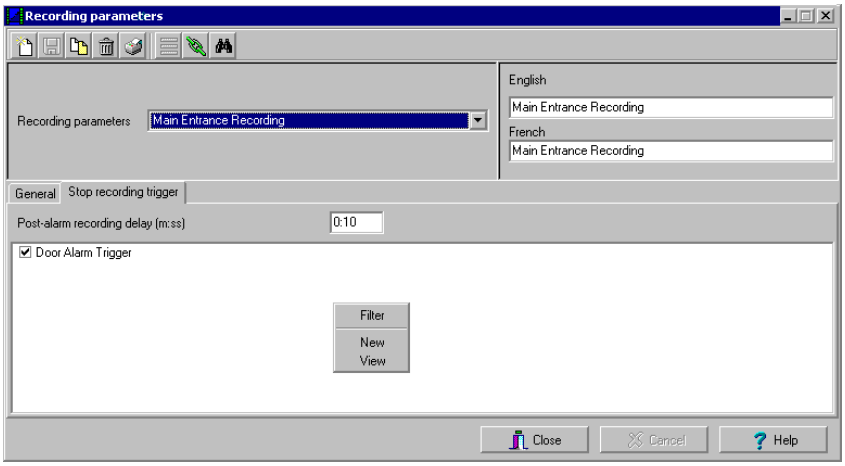
8 Стрелками вверх-вниз указать скорость записи для параметров записи. Это значение будет использоваться системой EntraPass исключительно для выбранных параметров записи. По умолчанию установлено значение 2,5 к/с. Среднее значение составляет 7,5 к/с. При установке скорости ниже этой величины на экране нет плавности движения. Если скорость больше, чем 7,5 к/с, например, 8,5 к/с, то движение на экране будет плавным. Некорректный выбор скорости записи может отрицательно повлиять на производительность компьютера.

ПРИМЕЧАНИЕ: *Скорость записи измеряется в кадрах в секунду (к/с). Выражение "кадров в секунду" в данном случае означает, сколько изображений будет записано за одну секунду. Запись в реальном времени составляет 25 к/с.*

Настройка параметров остановки записи

Для того чтобы связать назначенные параметры записи с видео триггером, который будет инициировать остановку записи, то вам следует отметить флажком поле **Stop recording trigger** (видео триггер для отстановки записи). После этого в окне Recording parameters появится закладка **Stop recording trigger** (видео триггер для отстановки записи).

1 Из окна Recording parameters (параметры записи) выбрать закладку **Stop recording trigger** (видео триггер для отстановки записи).



- **Post-alarm recording delay, m:ss** (Длительность посттревожной записи, м:сс) – позволяет завершить запись с некоторой задержкой после остановки записи при помощи “end recording delay” (задержка окончания записи). При установке курсора в этом поле на экране отображается допустимое значение задержки.
- **Trigger** (триггер) – выбрать триггер (одно или несколько), которое будет останавливать запись.

ПРИМЕЧАНИЕ: *Для того чтобы создать новый триггер, следует щёлкнуть правой кнопкой мыши по окну, в котором отображаются триггеры.*

Список событий видео(Video Event List)

В окне Video Event List отображаются все видеофрагменты, записанные системой и хранящиеся в базе данных видеосервера, а также видеофрагменты, хранящиеся в архиве в видеохранилище EntraPass Video Vault. Происхождение этих видеофрагментов может быть следующим:

- Видео триггеры
- Запросы, сделанные вручную операторами
- Автоматическая запись с видеосерверов

ПРИМЕЧАНИЕ: *Для того чтобы выполнять любые действия с событиями, отображаемыми в списке видеособытий (Video Event list), операторы должны иметь соответствующие полномочия для доступа к видеосерверу. Например, если оператор не наделён правами для использования конкретного видеосервера, он(а) не увидит события, переданные с этого сервера. Права доступа для пользователей системы назначаются при настройке уровня безопасности:* ***System*** *(Системные настройки) >* ***Security level*** *(Уровни безопасности).*

Порядок работы со списком событий видео (Video Event List)

В окне Video Event List отображаются все видеособытия вместе с описанием. Операторы системы EntraPass имеют возможность выполнять следующие действия:

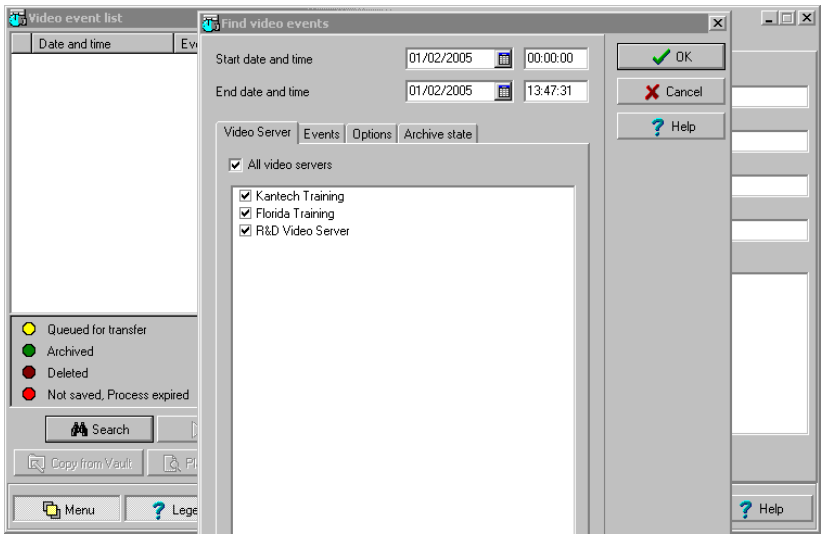
- Искать конкретное событие, связанное с видеофрагментом, по дате и времени создания этого видеофрагмента
- Просматривать записанный видеофрагмент
- Экспортировать видеофрагмент для дальнейшего анализа
- Просматривать или копировать видеофрагменты из видеохранилища EntraPass Video Vault
- Повторять все оборванные пересылки видеофрагментов, предназначенных для архивирования, но неудачно переданных в видеохранилище EntraPass Video Vault.

Поиск событий видео

В меню **Video > Video event list** нажать кнопку **Search** (Поиск), чтобы найти и просмотреть нужные видеофрагменты. Если кнопка **Search** не отображается на экране, щёлкнуть кнопку **Menu** (Меню), чтобы она появилась.

- Закладка **Video server** (Видеосерверы) служит для поиска видеофрагмента на конкретном видеосервере.
- Закладка **Events** (События) позволяет фильтровать события.
- Закладка **Options** (Опции) служит для указания размера искомого видеофрагмента. Для выполнения этой задачи пользователь должен обладать соответствующими полномочиями.
- Закладка **Archive state** (Статус архива) позволяет фильтровать архивированные события по состоянию архива.

1 В окне Video Events List нажать кнопку **Search** (Поиск). Откроется окно Find video events (Поиск видеособытий).

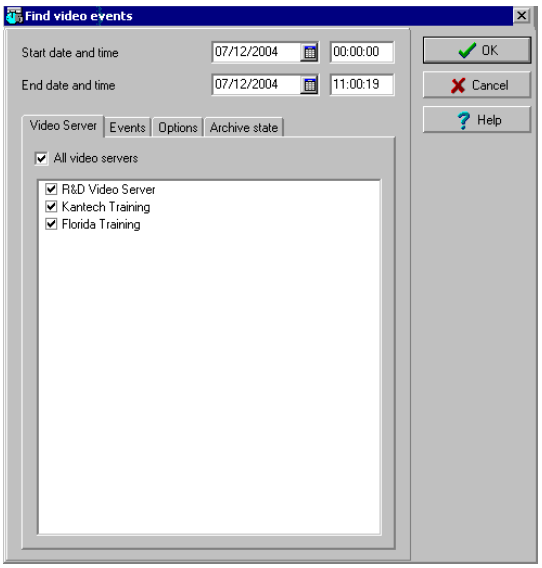


ПРИМЕЧАНИЕ: *Если кнопки* **Menu** *(Меню) и* **Legend** *(Описание) не активированы, то в этом окне не будет показываться описание и кнопки, расположенные в нижней части.*

2 В окне Find video events (Поиск видеособытий) указать дату и время начала (поле **Start date and time**), а также дату и время окончания (поле **End date and time**) для искомых видеофрагментов.

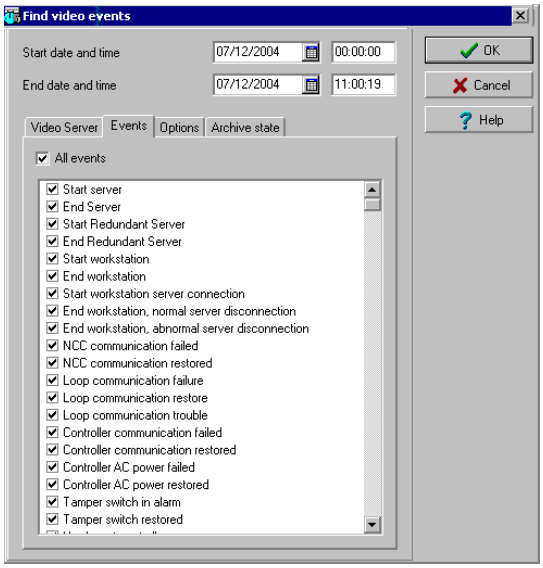
ПРИМЕЧАНИЕ: *Кнопка* **Legends** *(Описания) служит для отображения сведений о статусе видеособытий. Кнопки* ***Play*** *(Воспроизведение) и* ***Copy from Video Vault*** *(Копирование из видеохранилища) доступны в том случае, когда выбранные видеособытия уже находятся в архиве EntraPass Video Vault.*

3 Указать видеосервер, который требуется включить в поиск. Для поиска на всех видеосерверах, настроенных в системе, следует поставить флажок в поле **All video servers** (Все видеосерверы).

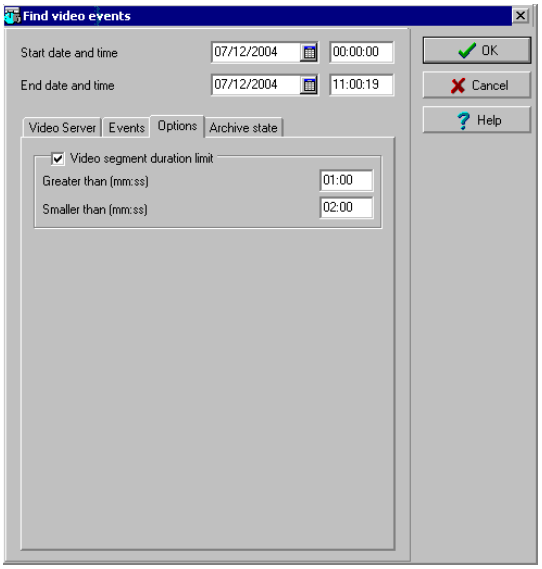


ПРИМЕЧАНИЕ: *Если событие зарегистрировано на двух и более видеосерверах, то при выделении хотя бы одного из них это событие будет включено в список.*

4 Открыть закладку **Events** (События), чтобы отфильтровать события, которые должны быть включены в отчёт. Можно выделить поле **All events** (Все события) или отметить флажками отдельные события.

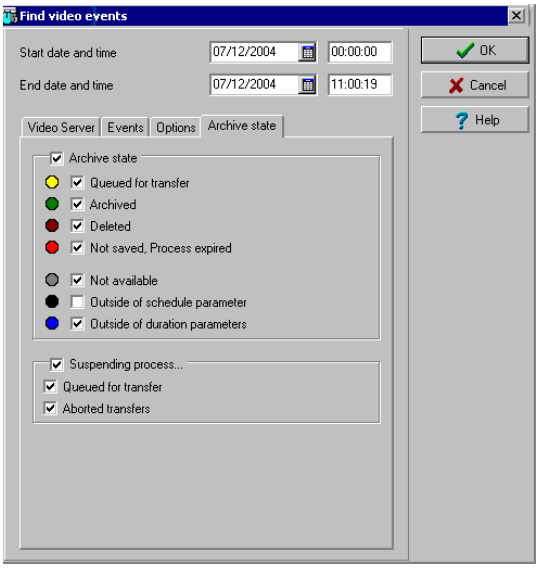


5 Открыть закладку **Options** (Опции), чтобы отфильтровать видеофрагменты по их длительности.



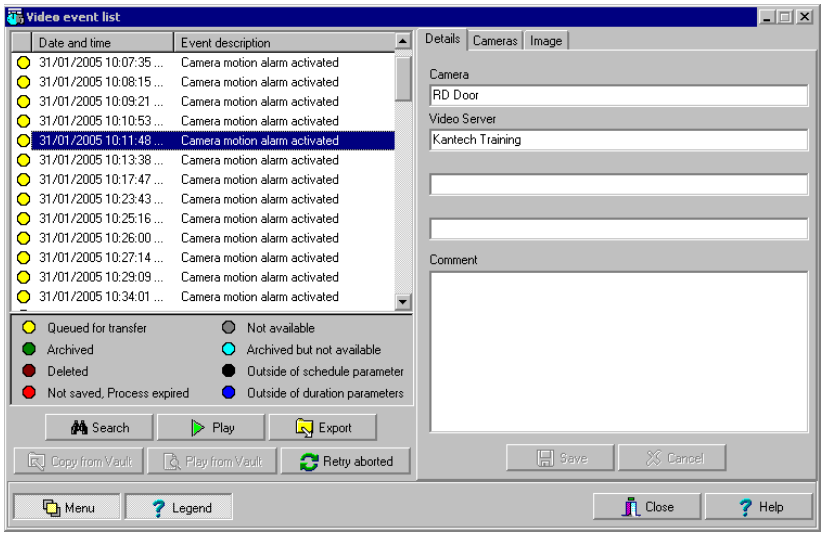
6 Поставить флажок в поле **Size filter** (Фильтровать по размеру), указать длительность в поле **Greater than, mm:ss** (Больше, чем, мм:сс) и в поле **Smaller than, mm:ss** (Меньше, чем, мм:сс). Значения этих параметров указываются в минутах и секундах. Данная функция позволяет выбрать видеофрагменты, длительность которых находится в определённом диапазоне.

7 Открыть закладку **Archive State** (Статус архива), чтобы отфильтровать события по состоянию архивирования.



8 Выделить поле **Archive state** (Статус архива), если необходимо указать, какие события включить в список. Чтобы включить все события, не следует ставить флажок напротив этих функций.

9 Нажать **OK,** чтобы вернуться в окно Video event list (список событий видео).



ПРИМЕЧАНИЕ: *Кнопки* ***Play*** *(Воспроизведение) и* ***Copy from Video Vault*** *(Копирование из видеохранилища) доступны в том случае, когда выбранные видеособытия уже находятся в архиве видеохранилища. Архивированные события помечены зелёным флажком.*

10 Назначение кнопок меню описано ниже в таблице:

Кнопка	Описание
Search	Кнопка **Search** (Поиск) служит для поиска событий, связанных с видеофрагментами. Для деталей, см. *Поиск событий видео на странице 237*.

Кнопка	Описание
Play	Кнопка **Play** (Воспроизведение) служит для просмотра видеособытия. При нажатии этой кнопки на рабочем столе видеонаблюдения (Video) отображается видеофрагмент с событием. Если для его записи использовалась только одна камера (в большинстве случаев), то отображается длительность видеособытия. Если запись выполнялась с нескольких камер на одном сервере, то видеосервер будет использовать самый оптимальный режим разбиения окна на ячейки. Если событие зарегистрировано на двух и более видеосерверах, то предусмотрена возможность выбрать один конкретный видеосервер. Например, режим 2x2 для отображения 4 камер (или меньше), 3x3 для отображения не более 9 камер и 4x4 для показа, максимум, 16 камер. При разной длительности событий их воспроизведение выполняется по наиболее длительному событию. Следует помнить, что эта функция имеет ограничения, если используется в системах, не настроенных на режим непрерывной записи, так как в этом случае не будут показаны камеры, не попавшие в указанный временной интервал.
Copy from Vault	Кнопка **Copy from Video Vault** (Копирование из видеохранилища) позволяет извлекать видеофрагменты из архива, хранящегося в видеохранилище.
Play from Vault	Кнопка **Play from Video Vault** (просматривать из видеохранилища) позволяет просматривать видеособытия, хранящиеся в архиве видеохранилища.
Retry aborted	Кнопка **Retry aborted** (Повторить незавершённое архивирование) служит для запуска любого приостановленного процесса создания архива.
Menu Legend	Кнопка **Menu** (Меню) предназначена для вывода на экран кнопок, расположенных в нижней части окна, а кнопка **Legend** (Описание) позволяет вывести на экран описание статусов видеособытий, отображаемых на экране.
Export	Кнопка **Export** (Экспортировать) служит для передачи файлов в формате KVI (Kantech Video Intellex), KVA (Kantech Video AVI), IMG и AVI. Эти форматы позволяют пользователям сохранять все данные, связанные с видеособытием (например, иконку события или ключевой кадр, описание и пр.
Save	Кнопка **Save** (Сохранить) становится доступной после ввода данных в поле **Comment** (Комментарий). Она служит для сохранения комментариев, связанных с видеособытием.
Cancel	Кнопка **Cancel** (Отмена) становится активной после внесения изменений в поле **Comment** (Комментарий). Позволяет отменить изменения комментария и вернуться к предыдущей его версии.

Воспроизведение фрагментов видео

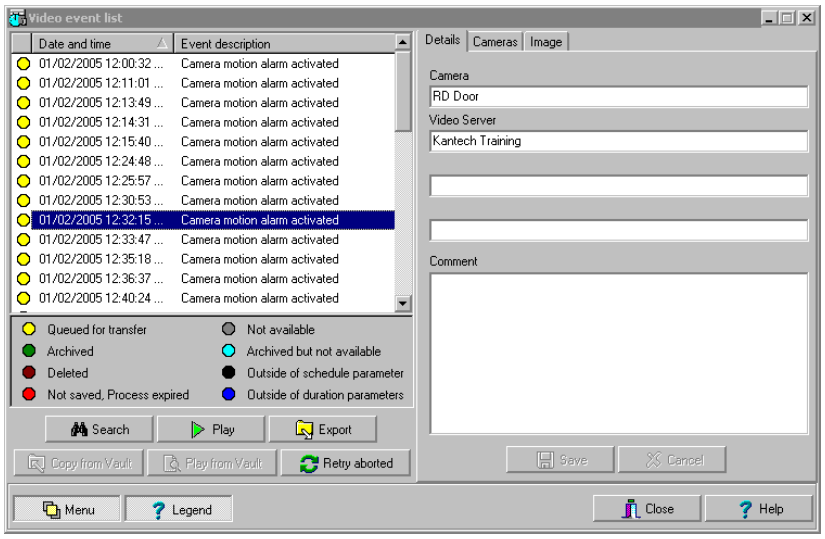
Окно Video Event List разделено на две части: слева отображаются все видеособытия, отвечающие установленным критериям поиска. В нижней части окна даны состояния для каждого события. Кроме того, там же находятся кнопки, необходимые для выполнения различных действий с видеозаписями.

Правая панель содержит три закладки: :

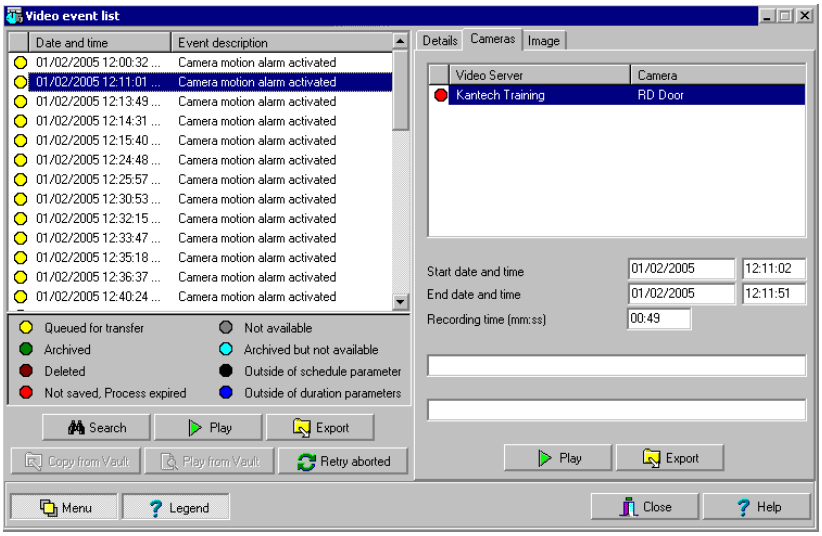
- Под закладкой **Details** (Подробные сведения) находится текстовое описание видеособытия, включая такие данные, как имя видеосервера, на котором оно было записано, имя оператора, который был зарегистрирован в системе в тот момент и др.
- В закладке **Camera** (Камеры) отображаются камеры наблюдения, связанные с выбранным событием.
- Закладка **Image** (Изображение) содержит ключевой кадр для последовательности кадров. Ключевой кадр предназначен для предварительного просмотра видео. Именно в этом разделе меню выбирают ключевой кадр и назначают его для выбранного видеофрагмента.

ПРИМЕЧАНИЕ: *Для воспроизведения видеозаписей можно использовать левую панель (кнопка **Play**) или закладку **Camera.** Кроме того, можно просматривать записи с камеры при помощи рабочего стола сообщений (Message). Для этого следует выбрать видеособытие (которое идентифицируется по иконке камеры на рабочем столе сообщений), щёлкнуть по нему правой кнопкой мыши и выбрать в контекстном меню команду* **View video segment** *(Посмотреть видеофрагмент).*

1 Выбрать событие в списке видеособытий Video event list и нажать кнопку **Play** (Воспроизведение). Изображение будет выведено в окно Video Playback (Воспроизведение видеофрагментов).



2 Открыть закладку **Camera** (Камеры) для просмотра сведений о камерах, которые выполняли запись выбранного события. Для этого следует открыть закладку **Camera** на правой панели.



- **Start/End dates and time** (Дата и время начала/окончания) – когда возникло событие видео записи.
- **Recording time, mm:ss** (Время записи, мм:сс) – длительность видеофрагмента. Это время указывают при настройке параметров записи (меню **Video** > **Recording parameters**).
- **Video trigger** (Событие, инициирующее начало/окончание записи) – если используется, то необходимо настроить в меню **Video trigger** и затем выбрать в меню **Recording parameters**.

ПРИМЕЧАНИЕ: *Индикатор статуса рядом с именем видеосервера указывает на текущий статус подключения сервера.*

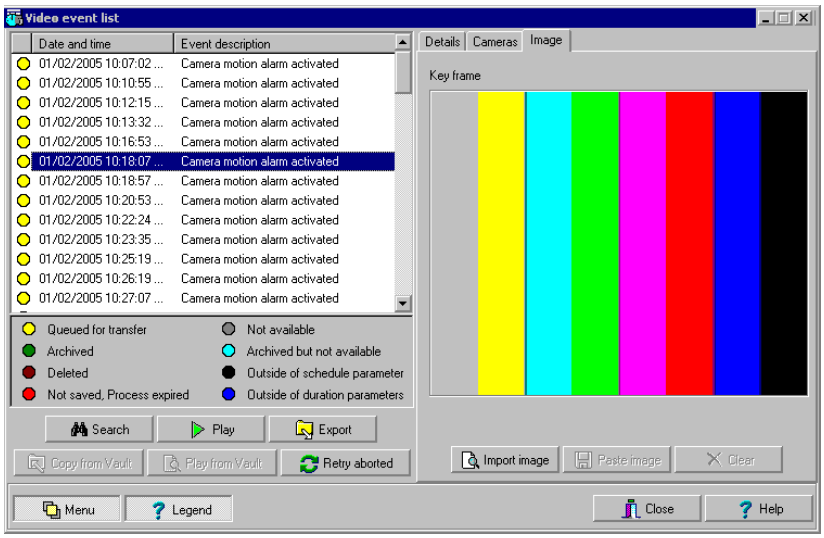
3 У пользователя есть выбор:
- Нажать кнопку **Play** (Воспроизведение), чтобы просмотреть видеофрагмент с выбранной камеры наблюдения в течение времени записи. Видеозапись отображается так же на рабочем столе видеонаблюдения.
- Нажать кнопку **Export** (Экспортировать) для дальнейшего использования видеофрагмента. Для большей информации смотрите *Экспортирование видео файлов на странице 243*.

iПривязка ключевых кадров к видеозаписям

Пользователи системы EntraPass имеют возможность сохранить любой наиболее представительный кадр видеофрагмента и использовать его в качестве ключевого кадра для всей видеозаписи. Эта опция может пригодиться, если событие зарегистрировано двумя и более камерами наблюдения и необходимо назначить для этой записи самый представительный кадр. Пользователи включают воспроизведение видеособытия и определяют, какой кадр лучше всего подходит для использования в качестве ключевого для этого видеофрагмента, захватывают его с помощью функции Snap, вставляют, сохраняют и используют как ключевой кадр, наиболее подходящий для данного видеофрагмента.

Кроме того, допускается установка ранее сохранённого изображения и привязка его к видеофрагменту в качестве ключевого кадра, а также использование кадра, ранее захваченного кнопкой Snap.

1 В списке видеособытий Video event list выбрать событие и открыть закладку **Image** (Изображение) на правой панели.



2 В окне Image доступны следующие функции:
- **Import image** (Импортировать изображение) – нажмите на кнопку **Import** (импортировать), чтобы вытянуть ранее сохранённое или экспортированное изображение из файла.
- **Paste image** (Вставить изображение) – использовать кадр, ранее захваченный кнопкой Snap. Кнопка **Paste image** (Вставить изображение) доступна только при условии, что изображение было до этого захвачено (скопировано) во время просмотра видеозаписи. Таким образом, сначала следует просмотреть видеофрагмент, выбрать самый важный кадр и захватить его кнопкой Snap, а затем вставить его при помощи функции Paste как ключевой кадр для этого фрагмента.
- **Clear** (Отмена) – служит для удаления изображённого кадра из окна просмотра

Экспортирование видео файлов

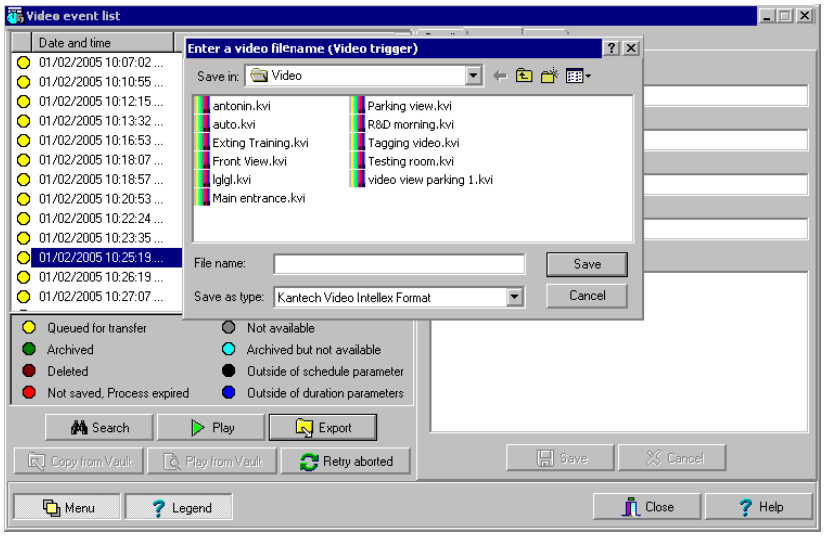
Система EntraPass экспортирует видеофрагменты в четырёх форматах, включая KVI и KVA.

- KVI (формат Kantech Video Intellex). Видеоданные хранятся в формате Intellex (.img). Для просмотра видеозаписи с помощью программы VideoPlayerIntellex.exe нужно просто щёлкнуть дважды по имени файла.
- KVA (формат Kantech Video AVI). Видеоданные хранятся в формате AVI (.avi). Для просмотра видеозаписи используется программа VideoPlayerWindow.exe.
- Формат AVI
- Формат IMG

Пользователи системы EntraPass могут экспортировать видеофайлы следующим образом:

- Из списка Video Events List (без предварительного просмотра видеофайлов).
- Из окна воспроизведения видеозаписей – в этом случае видеозапись предварительно просматривают.

1 В списке событий видео **Video event list** выбрать событие для экспортирования



2 Нажать кнопку **Export** (Экспортировать). При этом открывается окно Enter a video filename (Укажите имя видеофайла).

3 Указать имя файла в поле File name (Имя файла). По умолчанию файл сохраняется в формате Kantech KVI. Файл хранится вместе с программными файлами EntraPass, путь сохранения: \Kantech\Server-GE\Video. Чтобы затем запустить этот файл, достаточно щёлкнуть по нему мышью.

ПРИМЕЧАНИЕ: *Видеофайлы можно просматривать в окне View exported videos (Просмотреть экспортированные видеофайлы): закладка (**Video** > **View exported video**). Вместе с видеофайлом отображается его имя, дата и время. В этом окне можно также предварительно посмотреть, какие ключевые кадры связаны с видеофайлом (при их наличии).*

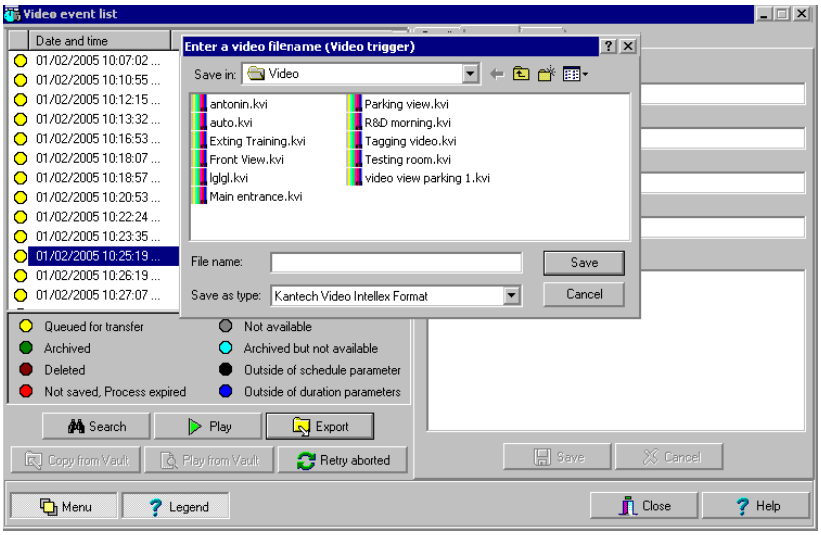
4 Нажать **Save** (Сохранить), чтобы закрыть окно Enter filename. После этого открывается окно Description and password (Описание и пароль).

Защита видеозаписей паролем

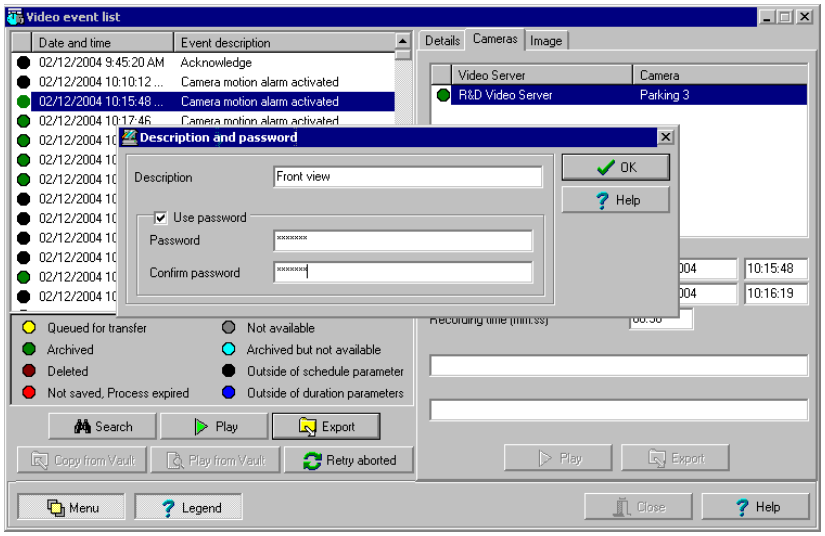
Экспортированные видеофайлы можно защитить паролем. В таком случае для просмотра видео пользователи должны будут ввести пароль.

ПРИМЕЧАНИЕ: *Защита паролем доступна только для файлов формата KVI и KVA.*

1 Выбрать видеофайл для экспортирования, нажать кнопку **Export.**



2 Ввести описание этого видеофрагмента в окне Enter Video filename и нажать **Save** (Сохранить). Открывается окно Description and password (Описание и пароль).



3 Поставить флажок в поле **Use password** (Использовать пароль), чтобы повысить уровень защищённости этого видеофрагмента. В таком случае для получения доступа к просмотру видео операторы должны ввести пароль.

4 Указать пароль в поле Password и подтвердить его в поле Confirm password

5 Нажать **OK**, чтобы закрыть окно Description and password. Нажать **OK**, чтобы закрыть окно с подтверждением удачного завершения экспортирования файла.

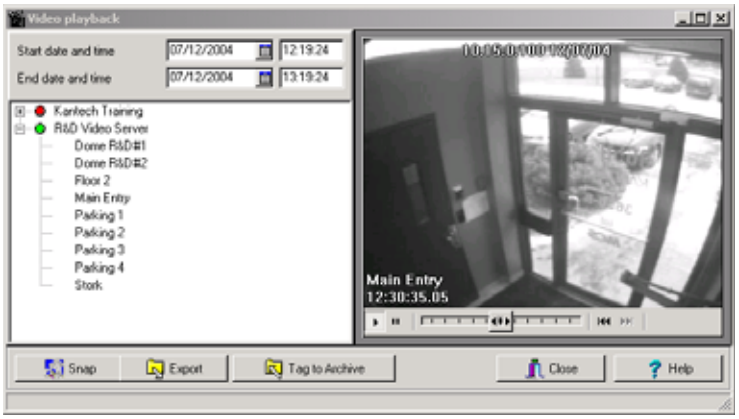
Воспроизведение файлов видео

Функция Video Playback позволяет просматривать по одной видеозаписи с любой камеры за один раз. Для этого необходимо указать временной интервал для воспроизведения. Максимально допустимое время – один час. Для этого:

- Выбрать камеру в панели слева
- Перетащить её в окно просмотра.

Просмотр записей видео в окне Video Playback

1 В окне Video playback (Воспроизведение видеофайлов) указать дату и время начала (поле **Start date and time**), а также дату и время окончания (поле **End date and time**) для искомых видеофрагментов. Максимальное время – один час. Таким образом, можно просматривать видеособытия, возникшие в один и тот же день в течение одного часа.



2 На панели слева выбрать камеру и перетащить в окно справа. Воспроизведение выполняется для указанного времени начала и окончания. На панели справа внизу расположены кнопки воспроизведения, паузы, остановки, быстрой прокрутки вперёд/назад.

ПРИМЕЧАНИЕ: *Если запрашиваемый видеофайл недоступен, в нижней части окна появляется соответствующее сообщение, а кнопки **Snap** (Захват изображения) и **Export** (Экспортировать) остаются неактивными. Если видеофайл доступен, появляется сообщение Requesting video (Запрашивается видеофайл).*

- **Snap** (Захват изображения) – копирует отображаемое изображение на экране и сохраняет его в папку \tmp\image, чтобы затем использовать в качестве ключевого кадра видеофрагмента. Затем захваченное изображение автоматически появляется в окне View exported videos (Просмотреть экспортированные видеофайлы). Рекомендуется добавить комментарий к сохранённому кадру; этот комментарий будет показан рядом с изображением.
- **Export** (Экспортировать) – экспортировать видеофрагмент для дальнейшего использования.
- **Tag to archive** (Пометить для архивирования) – пометить видеофрагмент как предназначенный для архивирования.

ПРИМЕЧАНИЕ: *Ползунок в нижней части панели (справа) позволяет увеличивать и уменьшать скорость воспроизведения видеозаписи.*

3 Для сохранения отдельного кадра видеозаписи следует нажать кнопку **Snap**

4 Оставить имя по умолчанию или указать другое имя сохраняемого кадра. Путь сохранения изображения: Program files\Kantech\Server_GE\Tmp\Image. Для просмотра сохранённых кадров можно воспользоваться программой просмотра графических файлов Windows®, например, Paint. Для этого нужно просто дважды щёлкнуть по названию файла мышью.

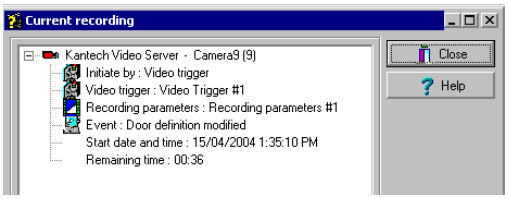
Записи, выполняемые в данный момент (Current Recording)

Функция Current recording (Текущие записи) позволяет просмотреть список всех записей, которые выполняются в текущий момент. Эта информация зависит от того, по какой причине производится запись: :

- запись начата по срабатыванию видео триггера
- запись начата по команде оператора
- запись начата по сигналу тревоги на видеосервере

Просмотр текущих записей

1 На панели инструментов в окне Video нажать кнопку **Current recording** (Текущие записи). В открывшемся окне будут выведены все выполняемые в данный момент записи.



Ниже в таблице приведены сведения, отображаемые в окне Current recording в зависимости от того, что является причиной записи:

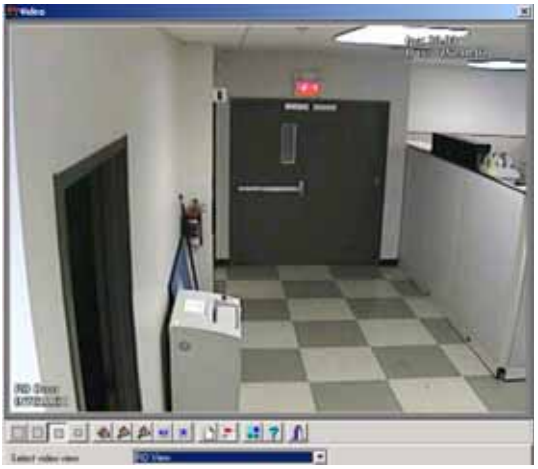
Чем вызвана запись	Сведения
Тревога на видеосервере	• Initiated by - чем вызвана запись • Event name – имя события • Start date and time – дата и время начала
Video trigger	• Initiated by - чем вызвана запись • Video trigger – инициирующее событие • Recording parameters - параметры записи • Event – событие • Start date and time – дата и время начала • Remaining time for the recording – оставшееся время записи
Оператор	• Initiated by - чем вызвана запись • Workstation – рабочая станция • Operator name – имя оператора • Start date and time – дата и время начала • Remaining time for the recording – оставшееся время записи

Рабочий стол видеонаблюдения

Рабочий стол Video позволяет операторам наблюдать в режиме реального времени изображение, передаваемое камерами наблюдения, подключёнными к сети и настроенными соответствующим образом.

Вывод на экран окна видеонаблюдения

1 Открыть закладку **Desktop** (Рабочий стол) в главном окне приложения EntraPass. Выбрать рабочий стол **Video**. Окно видеонаблюдения Video View откроется на этом рабочем столе. t



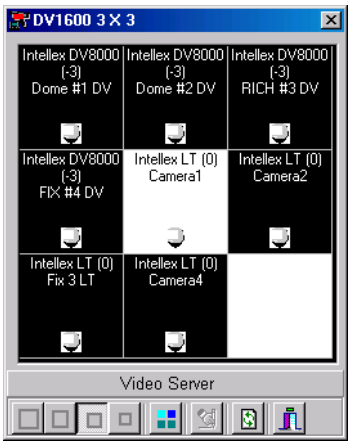
ПРИМЕЧАНИЕ: *При первом запуске рабочий стол Video откроется пустым. На экране будет сообщение "No video view selected" (Не выбрано видеоокно).*

2 Выбрать видеоокно в выпадающем списке **Select video view** (нижняя строчка окна). Чтобы изменить содержание окна, перейти в меню: **Video view** > выбрать определённый вид **View** > нажать кнопку **Modify Video view components** (Изменить компоненты видеоокна).

3 Кнопки, расположенные в нижней части окна, позволяют выполнять различные задачи:

Кнопки	Описание
	Эти кнопки служат для выбора размеров отображаемого видео. **ПРИМЕЧАНИЕ.** Чем больше размеры изображения, тем больше требуется ресурсов компьютера для его обработки. Таким образом, увеличение размеров изображения ведёт к замедлению работы.
	Эти кнопки доступны для пользователей с уровнем доступа оператора, настроенного в разделе Operator security level (уровни доступа оератора). С их помощью операторы могут выполнять запланированные задачи, например, просмотр видеозаписей с определённой постоянной или переменной задержкой, создание видеособытий с постоянными параметрами или со своими настройками. Более подробная информация по программированию этих кнопок *смотрите в Главе 12 'Назначение уровней безопасности' на странице 406.*
	Эти кнопки служат для создания (**Create**) и (**Edit**) редактирования видеоокон.
	Кнопка **Show view selector** (Вызов переключателя видов) служит для мозаичного отображения всех камер, настроенных в системе.
	Кнопки **Help** (Справка) и **Close** (Закрыть). Стандартные кнопки системы EntraPass.

4 Нажать кнопку **Show view selector** (Вызов переключателя видов) для отображения окна View selector. Это небольшое окно служит для выбора режима разбиения экрана при выводе изображений с нескольких камер или при наблюдении за движением одной камеры по определённому маршруту. Например, при выборе одной ячейки в окне переключателя видов, последовательность будет работать в выбранной ячейке.



ПРИМЕЧАНИЕ: *Если вызвать* View selector (*переключатель видов) во время записи с камеры, то иконка камеры будет мигать, пока запись не закончится.*

5 В отображаемом окне можно вызвать кнопки управления купольной камерой (pan/tilt, зум, фокус) нажатием на иконку камеры. Доступные опции зависят от используемой цифровой системы видеонаблюдения. Подробное описание приведено в руководстве к системе видеонаблюдения.

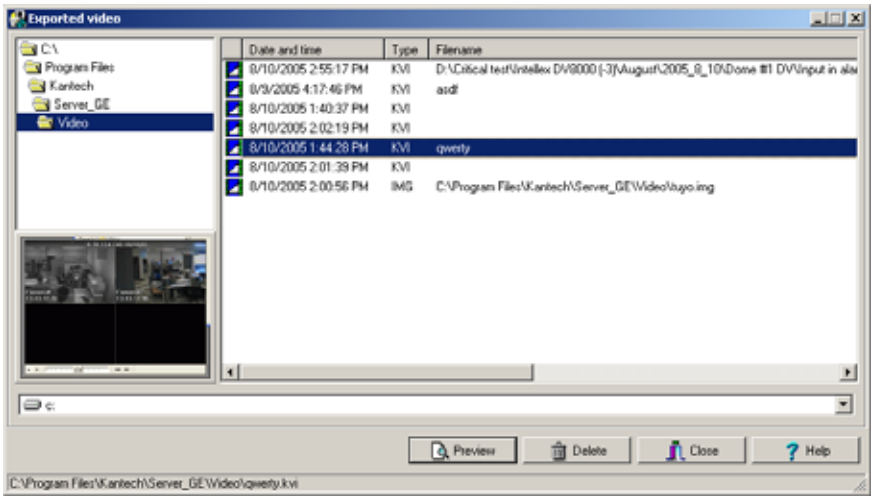
ПРИМЕЧАНИЕ: *Если купольная камера настроена на автотуры, то изображение может передаваться по шаблону, состоящему из одного или нескольких маршрутов движения. Более подробные сведения по настройке смотрите Назначение окон видео VideoView на странице 228.*

Просмотр экспортированных видеофайлов

Система EntraPass позволяет пользователям просматривать все экспортированные файлы. Таким образом, пользователи могут вывести на экран список всех экспортированных видеофайлов и просмотреть ключевые кадры ко всем файлам формата KVI и KVA.

Кроме того, пользователи могут выполнить предварительный просмотр экспортированного видеофрагмента перед его полноценным просмотром.

1 На панели инструментов в окне Video нажать кнопку **View exported video** (Посмотреть экспортированные видеофайлы). Папка Video открывается автоматически. Она содержит список всех экспортированных видеофрагментов.



2 Выбрать видеофрагмент. В левой нижней части окна должна появиться пиктограмма видеофрагмента. В списке файлов указаны дата и время создания видео (Date And Time), формат файла (**Type**) и его имя (**File Name**). Чтобы получить более подробные сведения об экспортированном видеофрагменте, следует нажать кнопку **Preview** (Предварительный просмотр). Во время предварительного просмотра видеофрагмента система отображает информацию о камере и версии программного обеспечения (закладка **Image**, кнопка **About**).

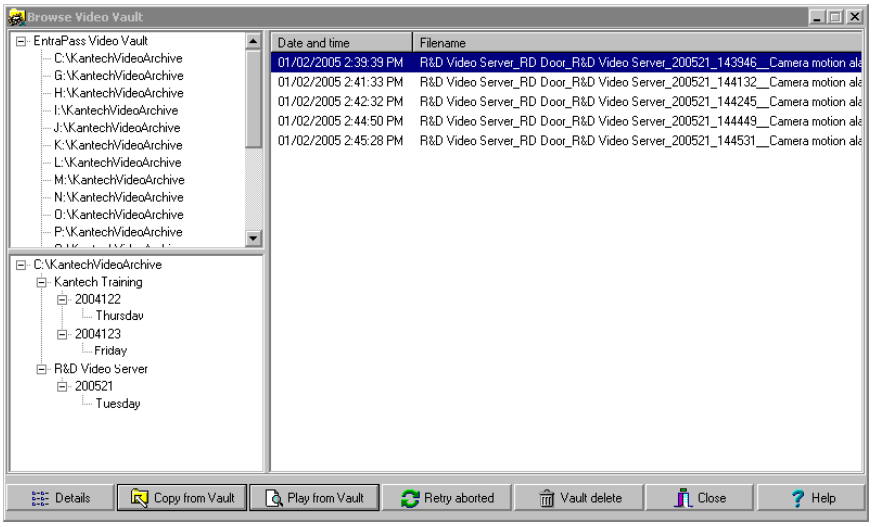
Просмотр видеохранилища EntraPass Video Vault

Видеохранилище EntraPass Video Vault предоставляет простой способ сохранения важных видеоданных для дальнейшего их использования. Как известно, видеозаписи имеют ограниченный ресурс, который зависит от настроек видеосервера и его возможностей. Поскольку видеофайлы занимают много места на диске, применение системы архивации данных типа EntraPass Video Vault позволяет лучше организовать хранение и облегчить извлечение файлов из архива.

Процессы архивирования контролируются с помощью интерфейса пользователя EntraPass Video Vault. В интерфейсе Browse EntraPass Video Vault используется такая же навигационная панель, как в системе Windows, что позволяет операторам, с соответствующими полномочиями, просматривать видеофрагменты, хранящиеся в архиве в EntraPass Video Vault.

Просмотр видеофрагментов из архива видеохранилища EntraPass Video Vault

1 В главном окне Video нажать кнопку Browse Video Vault (Просмотр видеохранилища).



2 Для воспроизведения определённого видеофрагмента следует выделить его и нажать кнопку **Play from Video Vault.**

Глава 7 • :Управление (Operations)

Панель инструментов в окне Operation

Закладка **Operation** (Операции) позволяет операторам производить ручные действия с различными компонентами системы (шлюзами, лучами/сайтами, контроллерами, оборудованием третьих компаний и т.д.). Такими действиями могут являться: сброс или включение функции мониторинга над устройством, блокировка считывателей. Ручное управление можно при необходимости использовать для перекрытия указанных расписаний или обработки специальных запросов, когда необходимо. Когда вы запускаете ручном режим управления, то пользователя есть возможность просматривать состояние выбранных компонентов в режиме реального времени. Кроме того, можно редактировать компоненты, обращаясь к ним напрямую из окна Operation.

Панель инструментов в меню Operation

Каждое окно Operation имеет панель инструментов с несколькими иконками. В разных окнах набор иконок будет разным. Однако во всех рабочих окнах обязательно есть пять кнопок, которые описаны ниже. .

Кнопка	Описание
	Кнопка **Select all** (Выделить всё) служит для выделения всех объектов или компонентов, отображаемых в списке.
	Кнопка **Unselect all** (Отменить выделение всех) предназначена для отмены выделения всех объектов или компонентов, которые были ранее выделены в списке.
	Кнопка **Enable Graphic** (Разрешить использование графических схем) показывает изображение, прикреплённое к выделенному компоненту (например, двери) и отображает также связанные с ним компоненты (например, считыватели карт). Для того чтобы компоненты отображались в реальном времени, кнопку Enable graphic следует использовать вместе с кнопкой **Enable animation** (Разрешить анимацию).
	Кнопка **Enable animation** (Разрешить анимацию) автоматически делает активной кнопку **Enable graphic** (Разрешить графику). При этом текущий компонент (например, дверь) становится активным, и его статус отображается в реальном времени.
	Кнопка **Help** (Подсказка) открывает интерактивную помощь для текущего активного окна.

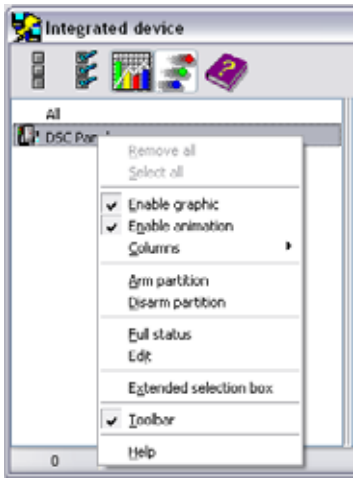
ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Контекстное меню окна Operation

Чтобы вызвать контекстное меню, следует щёлкнуть правой кнопкой мыши в любом месте окна Operation. Пункты контекстного меню соответствуют иконкам на панели инструментов в рабочем окне. Кроме того, при вызове контекстного меню в таких окнах, как Gateway, Луч/Site, состояние Guard Tour или область вам появляются дополнительные пункты. State, в нём появляются три дополнительных функции:

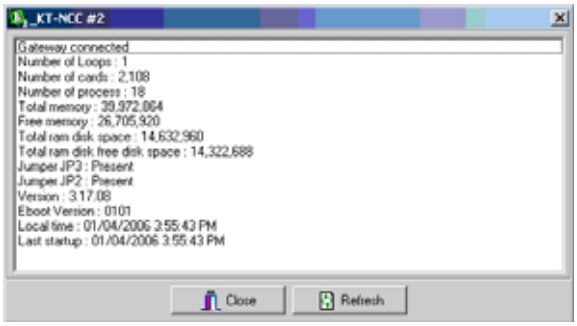
- **Full status** (полное сотояние)**.** Открывает окно состояния, что отражает текущую информацию о компоненте, который выбран из списка. Для дополнительных деталей смотрите "Меню состояния компонента" на странице 254.
- **Edit** (правка)**:** вызов окна выбранного компонента для редактирования его данных.

- **Extended selection box** (Окно расширенного режима выбора) – окно для поиска определённого компонента.



Меню состояния компонента

Окно сообщения, которое сожержит сообщения о шлюзе, лучах, областях, и состоянии guard tour может быть назначено при помощи нажатия правой кнопки мыши внутри связвающего окна под вкладкой **Operation** (Управление) и выбора пункта **Status** (состояние) в конекстном меню.



На примере, котторый приведен выше, информация отображена для Global Шлюза. Перечислим основные сведения, которые могут отображаться в этом окне:

Параметр	Описание
Статус Шлюза	Показывает, есть подключение шлюза к сети или нет.
Number of sites Количество лучей/сайтов	Показывает число сайтов/лучей для этого шлюза.
Number of cards (Число идентификационных карт)	IПоказывает число карт, обрабатываемых этим контроллером.
Number of processes (Число процессов)	Показывает число процессов.
Total RAM memory (всего оперативной памяти на диске)	Показывает общее количество оперативной памяти на диске.
Free memory (памяти свободно)	Показывает общее количество доступного дискового пространства.
Total RAM disk space (всего емкость оперативной памяти)	Показывает общее количество оперативной памяти.
Free RAM disk space (свободно дискового пространства оперативной памяти)	Показывает общее количество доуступной оперативной памяти.
Jumper J3 (джампер J3)	Показывает состояние переключателя J3. **Present** (присутствует): Jumper J3 is active **Absent** (отсутствует): Переключатель J3 - неактивный (может быть упущен на плате)
Jumper J2 (джампер J2)	Показывает состояние переключателя J2. **Present**(присутствует): Переключатель J2 - активный **Absent**(отсутствует): Переключатель J2 - неактивный (может быть упущен на плате)
Version (Версия)	Отображает версию программного и аппаратного обеспечения.
eBoot Version (версия прошивки)	Отображает версию eBoot прошивки.
Local Time (Местное время)	Показывает текущее местное время контроллера.
Last startup (Последний запуск)	Отображает дату последнего запуска системы.

ПРИМЕЧАНИЕ: *Информация, отображаемая в окне состояния, зависит от вашей конфигурации системы и будет различна, из какого окна в меню Operations был сделан запрос (шлюза, сайта/луча,guard tour, области).*

Ручное управление Шлюзом

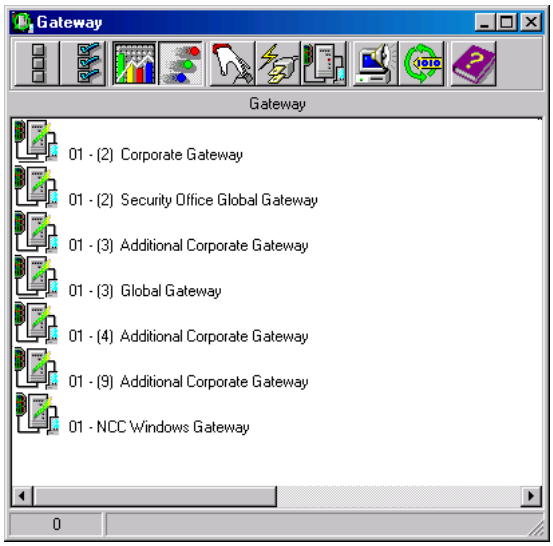
Ручной режим работы со шлюзом позволяет операторам обращаться к шлюзам для обновления данных, исполнение различных типов сбросов, и принудительная прошивка firmware через Шлюзы.

Кнопка	Назначение
	Soft reset (мягкий сброс): не оказывает влияния на базу данных. Команда посылает новую информацию в Шлюз для обновления текщих компонентов (реле, входы, двери и выходы).
	Hard reset (Жёсткая перезагрузка) – удаление имеющейся базы данных шлюза и загрузка вместо неё новых данных. Команды перезагрузки следует применять с осторожностью. Перед перезагрузкой шлюза рекомендуется проконсультироваться со службой технической поддержки.
	Reload (Повторная загрузка данных) – удаление содержимого базы данных шлюза, перезагрузка шлюза и повторная загрузка данных из базы данных системы.
	Broadcast (Широковещательный запрос) – отправка сигнала к выбранному компоненту вручную.
	Forced reload firmware (принудительная загрузка firmware): при нажатии этой кнопки будет принудительно перезагружено firmware (KT-NCC).

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выбор шлюза

1 В главном окне рабочей станции EntraPass открыть закладку **Operation** (Управление) и нажать кнопку **Gateway** (Шлюз), чтобы открыть меню шлюза, содержащее все подключённые к системе шлюзы.



ПРИМЕЧАНИЕ: *Более подробно смотрите в Главе 17 "Лучи/Сайты и Шлюзы" на странице 573.*

Обновление физических компонентов

1 Выберите Шлюз, для которого вы хотите произвести мягкий сброс.
2 Нажмите на кнопку **Soft reset**. Эта команда будет посылать новую информацию на Шлюз для обновления физических компонентов (реле, входы, выходы, двери).

Исполнение жесткого сброса Шлюза

ПРИМЕЧАНИЕ: *Команды перезагрузки следует применять с осторожностью. Перед перезагрузкой контроллера рекомендуется проконсультироваться со службой технической поддержки.*

1 Выделить шлюз, требующий жёсткой перезагрузки.
2 Нажать кнопку **Hard reset**. По этой команде будет выполнено удаление имеющейся базы данных шлюза и загрузка вместо неё новых данных.

Повторная загрузка данных шлюза

Система EntraPass позволяет операторам выполнять повторную загрузку данных, обновляя значения параметров системы с помощью системной базы данных. Когда требуется перезагрузка шлюза:

- После значительных изменений в базе данных системы (регистрация новых идентификационных карт, новых устройств, изменение описаний компонентов, создание новых расписаний);
- В случае неисправности одного или нескольких контроллеров (например, если возникает сбой при получении данных).

После повторной загрузки шлюз реорганизует/перерабатывает полученные данные и пересылает их на все лучи/сайты и контроллеры.

ПРИМЕЧАНИЕ: *Во время выполнения повторной загрузки связь с контроллерами временно прерывается.*

1 Выбрать шлюз, требующий повторной загрузки данных.
Нажать кнопку **Reload data** (Повторно загрузить данные). Данные шлюза будут обновлены.
2

Broadcasting/Посылка широковещательного запроса

1 Выбрать Шлюз на который вы хотите послать широковещательный запрос типа broadcast.
2 Нажмите на кнопку **Broadcast** (широковещательный запрос). Эта команда будет отправлять ручной запрос на Шлюз.

Принудительная загрузка frimeware

1 Выберите KT-NCC, на котором вы хотите обновить прошивку.
2 Нажмите кнопку **Forced reload firmware** (принудительное обновление прошивки). Эта команда будет принудительно обновлять прошивку на KT-NCC.

ПРИМЕЧАНИЕ: *Кнопка остается неактивной,если вы выбираете компонент отличный от KT-NCC по ошибке.*

Операции с лучами/сайтами при работе в ручном режиме

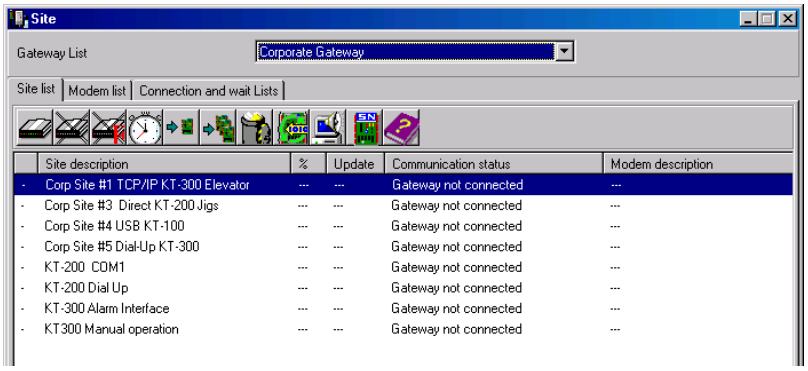
Режим ручного управления лучами/сайтами используется для опроса неприкреплённых к ним контроллеров. Например, если контроллер был добавлен в систему без указания серийного номера, то при помощи этой команды можно получить его серийный номер. Это преимущество применимо только в Шлюзах Corporate и Global.

Кнопка	Описание
	Connect to remote site (Соединение с удалённым лучом/сайтом) – служит для подключения к удалённому сайту при помощи предварительно настроенного соединения по dial-up линии.
	Disconnect remote site (Отключение от удалённого сайта/луча) – служит для **завершения** соединения между этой рабочей станцией EntraPass и удалённым сайтом/лучом.
	Force disconnect site (Принудительное разъединение с лучом) – немедленное отключение от удалённого сайта, даже во время перезагрузки системы. Эта опция доступна только для шлюзов Corporate Gateway.
	Disable remaining time (Запретить отсчёт оставшегося времени) – не прерывать соединение до повторного нажатия этой кнопки. Вызывает прекращение отсчёта времени до завершения соединения, указанного в настройках. Игнорирует любое время бездействия.
	Update remote site (Обновить удалённый сайт/луч) – служит для подключения к выбранному сайту и обновления его параметров.
	Update all remote sites (Обновить все удалённые сайты/лучи) – служит для подключения и обновления параметров на всех сайтах/лучах, начиная с первого сайта в списке. .
	Remove site from connect and wait list (Исключить сайт/луч из списка соединений) – прекратить соединение с выбранным сайтом после того, как все сайты были настроены на обновление.
	Reload IP Link firmware (Перезагрузить прошивку IP Link) – выполнить перезагрузку выбранного обеспечения Kantech IP Link. ***ПРИМЕЧАНИЕ.*** *Из соображений безопасности системный администратор может сделать эту иконку недоступной.*
	Broadcast IP Device (Устройство широковещательного запроса) – отправка сигнала к выбранному модулю Kantech IP Link, а также для безопасного соединения через IP с KT-400.

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выполнение операций с лучами/сайтами при работе в ручном режиме

1 В окне **Operation** (Управление) нажать иконку **Site** (Сайт/Луч), чтобы открыть окно Site. Выбрать шлюз, к которому подключен сайт/луч.



2 Чтобы выполнить опрос не прикреплённого к сайту контроллера, нажать кнопку **Controller** (Контроллер). На этот контроллер будет отправлено сообщение с запросом идентификации. После того как контроллер получит это сообщение с луча, он отправит на АРМ сообщений сообщение-подтверждение связи.

3 Оператор может посмотреть серийный номер контроллера на АРМ сообщений.

ПРИМЕЧАНИЕ: *В колонке % отображается эффективность связи с выбранным лучом/сайтом. Если эта величина невелика (например, ниже 75%), то это может указывать на плохое качество связи с лучом. Проблемы со связью могут быть вызваны различными причинами, например, воздействием электромагнитных помех, повреждением соединительных кабелей и т.п.*

Сообщения о состоянии соединения, доступные в списке меню

Сообщения в списке диалогового меню отображают состояние соединения с лучом/сайтомю. В примере, показанном ниже, перечислены сообщения о состоянии соединения для KT-NCC, для Шлюзов Global и Corporate.

Шлюзы KT-NCC и Global

Сообщение	Описание
Site/Loop Communication OK (Связь с сайтом/лучом в порядке)	Все контроллеры сайта поддерживают связь со шлюзом.
Site /Loop Communication Trouble (Проблемы со связью на луче/сайте)	Хотя бы у одного из контроллеров луча нет связи со шлюзом.
Site/Loop Communication Failure (Нет связи с сайтом/лучом)	Нет связи между контроллерами сайта и шлюзом.
Site/Loop Communication Cannot be Opened (Невозможно открыть связь с лучом/сайтом)	Шлюз не может открыть порт связи для луча.

Шлюзы Corporate

Сообщение	Описание
Site Communication OK (Связь с сайтом/лучом в порядке)	Все контроллеры сайта поддерживают связь со шлюзом.
Site Communication Trouble (Проблемы со связью на луче/сайте)	Хотя бы у одного из контроллеров луча нет связи со шлюзом.
Site Communication Failure (Нет связи с сайтом/лучом)	Нет связи между контроллерами сайта и шлюзом.
Site Communication Cannot be Opened (Невозможно открыть связь с лучом/сайтом)	Шлюз не может открыть порт связи для луча.

Управление контроллерами при работе в ручном режиме

Это меню служит для выполнения различных операций по сбросу и перезагрузке контроллера: мягкая и жёсткая перезагрузка, повторной загрузка и обновление прошивки контроллера.

Кнопка	Описание
	Soft reset (Мягкая перезагрузка) – не затрагивает базу данных контроллера. Эта команда отправляет новые данные на контроллер для обновления его физических компонентов (реле, входов, дверей и выходов).
	Hard reset (Жёсткая перезагрузка) – удаление имеющейся базы данных контроллера и загрузка вместо неё новых данных. Команды перезагрузки следует применять с осторожностью. Перед перезагрузкой контроллера рекомендуется проконсультироваться со службой технической поддержки.
	Reload (Повторная загрузка) – повторная загрузка базы данных контроллера, например, после некорректной загрузки из-за сбоев в работе.
	Reload controller firmware (Загрузка прошивки контроллера) – загрузка прошивки контроллера (KT-NCC, KT-100, KT-300).
	Unlock reader keypad (Разблокировать клавиши считывателя): позволяет разблокировать клавиши считывателя карт на контроллерах KT-100, KT-300. .
	Reset reader power (Сброс питания считывателя) – выполняет сброс питания на считывателе контроллера. Эта команда доступна только для контроллеров типа KT-300.
	Forgive (Сброс счётчиков) – сбрасывает на нуль счётчики карт входящих и выходящих посетителей или счётчики карт в локальной зоне контроля.
	Anti-passback cards list (Список карт с запретом повторного прохода) – отображает число карт в каждой локальной зоне, получает список карт в локальной зоне контроллеров, перемещает карты (в системе KT-400) и позволяет узнать, где находится карта. Эта функция доступна только для шлюзов Corporate Gateway.

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выбор контроллера

1 В окне Operation (Операции) выбрать иконку **Controller** (Контроллер) и открыть окно Controller, из которого можно выполнить перезагрузку контроллера.

2 На панели **Gateway/Site** (Шлюз/Сайт/Луч) выбрать шлюз или сайт/Луч. Контроллеры, присоединённые к этому шлюзу/сайту/Лучу, отображаются на панели справа.

- В списке **Controller** (Контролер) выделить контроллер, с которым необходимо поработать. Он должен быть выделен другим фоном. Для работы с группой контроллеров выбрать группу в **Controller Group** (Группы контроллеров) на нижней правой панели.

ПРИМЕЧАНИЕ: *Если в системе определены только один сайт/луч или Шлюз, список с изображением луча с контроллерами или Шлюзами не будет отображаться в окне контроллеров.*

Выполнение мягкой перезагрузки контроллера

Мягкая перезагрузка обновляет данные в контроллере.

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Soft reset** (Мягкая перезагрузка). Эта команда отправляет новые данные на контроллер для обновления его физических компонентов (реле, входов, дверей, выходов и др.).

Выполнение жёсткой перезагрузки контроллера

Жёсткая перезагрузка представляет собой удаление имеющейся базы данных контроллера и загрузка вместо неё новых данных.

ПРИМЕЧАНИЕ: *Команды перезагрузки следует применять с осторожностью. Перед перезагрузкой контроллера рекомендуется проконсультироваться со службой технической поддержки.*

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Hard reset** (Жёсткая перезагрузка). Эта команда отправляет новые данные на контроллер для обновления его физических компонентов (реле, входов, дверей, выходов и др.).

Повторная загрузка контроллера в ручном режиме

Система EntraPass позволяет операторам выполнять повторно загрузку базы данных контроллера, например, после некорректной загрузки из-за сбоев в работе.

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Reload** (Повторная загрузка). База данных контроллера будет загружена повторно.

Загрузка прошивки контроллера вручную

Система EntraPass позволяет вручную выполнять загрузку прошивки контроллера для контроллеров для KT-100, KT-NCC и KT-300. Загрузка прошивки может потребоваться после обновления прошивки или апгрейда системы.

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Reload controller firmware** (Загрузка прошивки контроллера).

Разблокировка клавиш считывателя вручную

EntraPass позволяет разблокировать клавитуру считывателя для контроллеров KT-100 и KT-300 из APM.

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Unlock reader keypad** (Разблокировать клавиши считывателя).

Сброс питания считывателя в ручном режиме

EntraPass Global Edition позволяет вам сбрасывать питание считывателя на KT-300.

1. В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2. Нажать на панели инструментов кнопку **Reset reader power** (сбросить питание считывателей) на панели инструментов.

Сброс счётчиков карт внутри и вне охраняемой территории или всех карт в локальной зоне контроля

Эта функция обнуляет счётчики карт внутри и снаружи помещения.

1 В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.
2 Нажать на панели инструментов кнопку **Forgive** (Сброс). Владельцы карт, находящиеся внутри или за пределами контролируемой зоны, не будут приниматься в расчёт, до тех пор пока в следующий раз не воспользуются своими картами и не предъявят их на входе или выходе.

Подсчёт числа карт внутри и вне охраняемой территории

Если хотя бы один контроллер работает в режиме запрета повторного прохода, то эта функция позволяет определить список карт, находящихся внутри (**Cards in**) или вне (**Cards out**) охраняемой территории. Для этого необходимо активировать на считывателе функцию запрета повторного прохода (мягкий или жёсткий запрет) и описать в настройках дверь, как "входную" или "выходную".

1 В меню Controller (Контроллер) в разделе **Gateway/Site** (Шлюз/Сайт/Луч) указать **KT-400-IP**. Теперь в разделе **Controller** появится список контроллеров, прикреплённых к выделенному компоненту.
2 Выделить нужный контроллер или группу контроллеров.
3 Нажать на панели инструментов кнопку **Get Card List** (Получить список карт). На экране появится список карт, находящихся в контролируемой зоне или вне неё, для выбранного контроллера или группы контроллеров.

ПРИМЕЧАНИЕ: *Данная операция выполняется только на одном контроллере единовременно, так как занимает много времени. Эта опция доступна только для шлюзов Corporate Gateway.*

4 Нажать правой кнопкой мыши в нужном месте и вызвать функцию **Find card position** (Определить положение карты).

В меню **Get card position** выбрать опцию **Start with** (Начиная с....), **Begin with** (Начинается с...) или **Contains** (Содержит...), чтобы сузить критерии поиска.

5 В открывшемся списке найти искомую карту и нажать кнопку **Get position** (Определить положение).

Сброс счётчиков карт вошедших и вышедших или всех карт в локальной зоне контроля

Эта функция обнуляет счётчики идентификационных карт вошедших и вышедших.

1 В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров
2 Нажать на панели инструментов кнопку **Forgive** (Сброс). Владельцы карт, находящиеся внутри или за пределами контролируемой зоны, не будут приниматься в расчёт, до тех пор пока в следующий раз не воспользуются своими картами и не предъявят их на входе или выходе.

Управление дверями при работе в ручном режиме

Это меню позволяет авторизованному оператору вручную изменять состояние дверей (одной или группы). Операторы имеют возможность вручную отпирать/запирать дверь, временно ставить/снимать блокировку одной или группы дверей, активировать/деактивировать считыватели указанных дверей.

Кнопка	Описание
	Lock door or group of doors (Блокировать дверь или группу дверей) – вручную блокировать указанные двери (одну или группу).
	Unlock door or group of doors (Разблокировать дверь или группу дверей) – указанная дверь или группа дверей будут разблокированы в ручном режиме и останутся разблокированными до следующего достоверного изменения в расписании автоматической блокировки или до решения оператора заблокировать их вручную.
	Temporarily lock/unlock door or group of doors (Временно блокировать/разблокировать дверь или группу дверей) – временно разблокировать указанные двери (одну или группу) на указанный срок задержки. После окончания времени задержки дверь (группа дверей) будет снова перевзята автоматически.
	Return to schedule (Вернуться к выполнению расписания) – снова применить расписание блокировки к указанной двери или группе дверей.
	Enable card reader (Разрешить использование считывателя карт) – разрешить использование ранее деактивированного считывателя карт, установленного на двери.
	Disable card reader (Запретить использование считывателя карт) – деактивировать считыватель карт, чтобы у посетителей не было доступа к двери даже при наличии прав доступа.
	Arm door (Поставить дверь на охрану) (Только Corporate Шлюз с KT-400)– делать запрос для поставки на охарну тревожную панель, то есть заблокировать дверь и активировать охранную панель, чтобы никто не мог войти в здание или в помещение.
	Disarm door (Снять дверь с охраны) (Только Corporate Шлюз с KT-400) – сделать запрос на снятие с охраны тревожной системы, то есть разблокировать дверь и деактивировать охранную панель, чтобы посетители, предъявившие идентификационные карты и получившие доступ, могли войти в здание или в помещение.

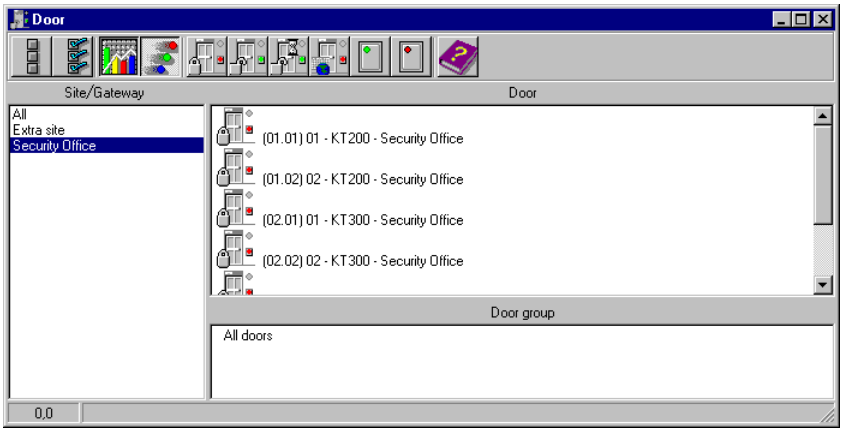
ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Существуют разные причины, по которым может потребоваться выполнить одну из перечисленных операций; например, когда необходимо на короткий срок «disable reader» отключить считыватель карт, чтобы закрыть доступ через дверь и др. Таким образом, оператор может заблокировать дверь, которая прежде была разблокирована вручную оператором или автоматически согласно расписанию. Если дверь заблокирована вручную через меню Operation (Управление), то её блокировка будет снята после возникновения одного из следующих событий:

- предъявление действительной идентификационной карты (с повторной блокировкой после доступа), или
- следующее достоверное изменение расписания автоматической разблокировки (для двери, настроенной на работу по расписанию), или
- разблокировка двери оператором в ручном режиме работы.

Выбор двери или группы дверей

1 В окне Operation (Операции) нажать иконку **Door** (Двери). Открывается окно Door.



2 Нажать на кнопку **Enable animation** (Разрешить анимацию), чтобы в режиме реального времени отображался состояние двери.
- На панели слева показан список всех сайтов/шлюзов под заголовком **Sites/Gateways**. Выбрать все или один сайт/шлюз.
- Отдельные двери, прикреплённые к сайту(лучу)/Шлюзу, выбранному на панели слева, отображаются справа в верхней части окна. Если слева выбрана опция **All** (Все), то справа отображаются все двери системы. Можно выделить одну, несколько или все двери.

ПРИМЕЧАНИЕ: *Если в системе только один сайт или шлюз, панель со списком сайтов (лучей) или шлюзов не будет отображаться в окне контроллеров.*

- Группы дверей, прикреплённые к сайту(лучу)/шлюзу, выбранному на панели слева, отображаются справа в нижней части окна. Если слева выбрана опция **All** (Все), то внизу справа отображаются все группы дверей системы. При этом можно выделить одну или несколько или все группы.

Блокировка двери вручную

1 В меню Door (Двери) выделить нужную(ые) дверь(и) или группу дверей.
2 Нажать на панели инструментов кнопку **Lock-door** (Заблокировать двери).

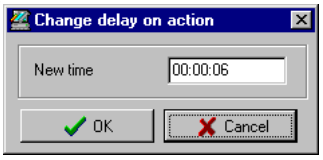
Разблокировка двери вручную

1 В меню Door (Двери) выделить нужную(ые) дверь(и) или группу дверей.
2 Нажать на панели инструментов кнопку **Unlock-door** (Разблокировать двери). Выбранные двери будут разблокированы в ручном режиме. Система предложит подтвердить выполнение операции. Дверь, настроенная на автоматическую работу по расписанию разблокировки, останется разблокированной, пока не произойдёт одно из следующих событий:
- следующее достоверное изменение расписания разблокировки, или
- блокировка двери оператором в ручном режиме.

Временная разблокировка двери

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.

ПРИМЕЧАНИЕ: *Максимальное время разблокировки составляет 4:15 (255 секунд)*



1 Нажать кнопку **Temporarily unlock** (Разблокировать временно). На экране появляется диалоговое окно Change delay on action (Изменить задержку выполнения).
2 В поле **New time** (Новое время) указать величину задержки и нажать **OK**. Выбранная дверь будет временно разблокирована по команде оператора.

ПРИМЕЧАНИЕ: *Если используется дверной контакт, то дверь будет снова заперта сразу после получения сигнала о переходе из открытого состояния в закрытое. Для этой операции не предусмотрено никакой анимационной картинки.*

Сброс двери в работу по расписанию

Система EntraPass предусматривает возвращение к выполнению расписания после работы с компонентом в ручном режиме.

1 В меню Door (Двери) выделить нужную(ые) дверь(и) или группу дверей.
2 Нажать кнопку **Return to Schedule** (Вернуться к выполнению расписания). По этой команде выполняется повторная загрузка расписания для выбранных компонентов.

Разрешить использование считывателя карт на двери

1 В меню Door (Двери) выделить нужную(ые) дверь(и) или группу дверей.
2 Нажать кнопку **Reader-enable** (Разрешить использование считывателя). Эта функция позволяет снова использовать ранее деактивированный считыватель карт, установленный на двери.

Запретить использование считывателя карт на двери

1 В меню Door (Двери) выделить нужную(ые) дверь(и) или группу дверей.
2 Нажать кнопку **Reader-disabled** (Запретить использование считывателя). Эта функция делает недоступным ранее использовавшийся считыватель карт. Ставший недоступным считыватель перекрывает доступ всем посетителям, даже тем, у кого есть права доступа.

Операции с дверями лифтов при работе в ручном режиме

В ручном режиме управления операторы, обладающие необходимыми полномочиями, могут вручную блокировать/разблокировать, временно разблокировать этажи. Это окно также отображает в режиме реального времени состояние выбранной двери лифта.

Получение доступа к лифту

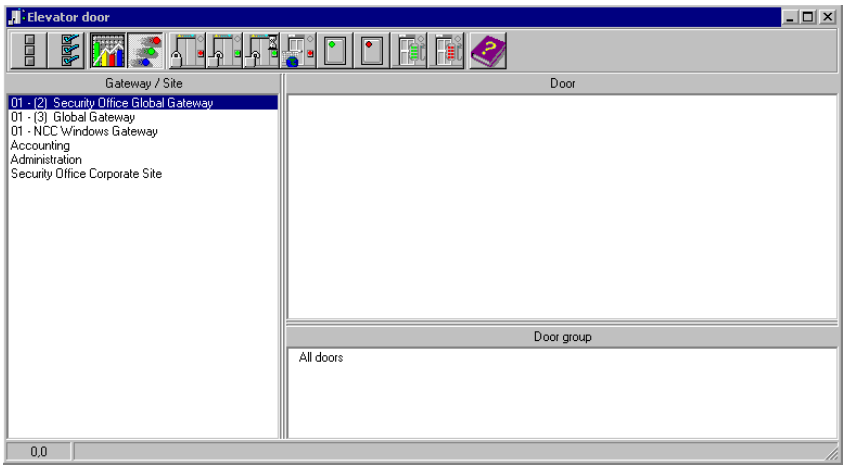
- Владелец карты нажимает кнопку "вверх-вниз". Двери лифта открываются.
- Владелец карты предъявляет свою карту считывателю (обычно уже в лифтовой кабине
- Система проверяет, достоверно ли расписание, назначенное для указанной двери. Если да, выполняется проверка, какая группа этажей имеет привязку к этой двери.
- Затем система проверяет каждый этаж из этой группы этажей (в меню группа этажей) и проверяет, достоверно ли расписание для каждого этажа этой группы.
- Для выбора посетителями будут доступны только этажи с достоверным расписанием (то есть будет доступна панель лифта и кнопки выбора этих этажей). .

Кнопка	Описание
	Lock elevator floor or group of elevator floors (Блокировать этаж или группу этажей лифта) – вручную блокировать указанный этаж (группу этажей) лифта.
	Unlock elevator floor or group of elevator floors (Разблокировать этаж или группу этажей лифта) – указанный этаж (группа этажей) лифта будут разблокированы в ручном режиме и останутся разблокированными до следующего достоверного изменения расписания автоматической блокировки или до решения оператора заблокировать их вручную.
	Temporarily lock/unlock elevator floor or group of elevator floors (Временно блокировать/ разблокировать этаж или группу этажей лифта) – позволяет блокировать/разблокировать указанный этаж (группу этажей) лифта на указанный срок. После окончания времени задержки этаж (группа этажей) будет снова автоматически заблокирована.
	Return to schedule (Вернуться к выполнению расписания) – снова применить расписание блокировки к указанной двери или группе дверей.
	Enable card reader (Разрешить использование считывателя) – разрешить использование ранее деактивированного считывателя карт.
	Disable card reader (Запретить использование считывателя карт) – деактивировать считыватель карт, чтобы у посетителей не было доступа на этаж из лифта даже при наличии прав доступа.
	Enable elevator floor (Разрешить доступ на этаж) – разрешить доступ на этаж (группу этажей), на который раньше не было доступа.
	Disable elevator floor (Запретить доступ на этаж лифта) – перекрыть доступ на этаж (группу этажей), чтобы у посетителей не было доступа к нему через лифт даже при наличии прав доступа.

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выбор двери лифта

1 В окне **Operation** (управление) нажать иконку **Elevator Door** (Двери лифта



2 Нажать на кнопку **Enable animation** (Разрешить анимацию), чтобы в режиме реального времени отображался состояние двери лифта.

- The left-hand pane displays the list of all **Sites/Gateways** (все лучи/сайты и Шлюзы). Выбрать все или один сайт(луч)/шлюз.
- Отдельные двери лифта, прикреплённые к сайту(лучу)/шлюзу, выбранному на панели слева, отображаются в верхней части окна справа. Если слева выбрана опция **All** (Все), то справа отображаются все лифтовые двери в системе. Можно выделить одну, несколько или все лифтовых дверей.
- В поле **Elevator door groups,** расположенном в нижней части окна справа отображаются группы лифтовых дверей, прикреплённые к сайту(лучу)/шлюзу. Если слева выбрана опция **All** (Все), то внизу справа отображаются все группы лифтовых дверей в системе. При этом можно выделить одну или несколько или все группы лифтовых дверей.

Закрытие лифтовых кабин/Блокировка двери лифтовой кабины

1 Выбрать одну дверь лифта или целую группу.

2 Нажать на панели инструментов кнопку **Lock** (Закрыть). Эта команда позволяет вручную закрыть группу этажей, которая прежде была разблокирована вручную оператором или автоматически согласно расписанию.

ПРИМЕЧАНИЕ: *Дверь, для которой не назначено расписание разблокировки, можно заблокировать только вручную. Чтобы заблокировать все ранее разблокированные двери, следует воспользоваться функцией* **Unlock** *(Разблокировать) в меню Manual operation on doors (Ручное управление дверями).*

Разблокировка этажей через двери лифта

1 Выбрать одну дверь лифта или целую группу.

2 Нажать на панели инструментов кнопку **Unlock elevator floors** (Разблокировать этажи лифта), чтобы разблокировать заблокированные раньше этажи. По этой команде будут доступны только те этажи лифта, которые помечены флажком «X» в колонке “State” (состояние) в меню Floor group Definition (Назначение группы этажей). Если вы сделаете это, то система предложит выделить

группу этажей, которые необходимо разблокировать (сделать доступными). После выделения такой группы этажей система предложит оператору подтвердить выполнение операции.

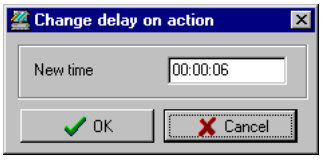
ПРИМЕЧАНИЕ: *Если для двери назначено расписание автоматической разблокировки "automatic unlocking schedule", то этажи останутся доступными до следующего достоверного изменения расписания разблокировки или до решения оператора заблокировать их вручную.*

ПРИМЕЧАНИЕ: *Дверь, для которой не назначено расписание разблокировки, можно заблокировать только вручную. Чтобы заблокировать все ранее разблокированные двери, следует воспользоваться функцией Unlock (Разблокировать) в меню Manual operation on doors (Ручное управление дверями).*

ПРИМЕЧАНИЕ: *После завершения ручной операции разблокировки для выбора будут доступны только те этажи, которые отмечены флажком в меню Floor group (Группы этажей), колонка State (состояние). Кроме того, в случае потери связи и переходе контроллеров на автономный режим работы для выбора будут доступны только этажи, отмеченные флажком, а расписание доступа будет игнорироваться.*

Временная разблокировка доступа на этажи через двери лифта

Система EntraPass позволяет разблокировать доступ на этаж через двери лифта на установленный срок. После окончания времени задержки дверь лифта будет снова автоматически заблокирована. Максимальное время разблокировки: 4:15 (255 секунд).



1. Нажать кнопку **Temporarily unlock** (Разблокировать временно). На экране появляется диалоговое окно Change delay on action (Изменить задержку выполнения).
2. В поле **New time** (Новое время) указать величину задержки и нажать **OK**. Выбранный этаж будет временно разблокирован по команде оператора.

ПРИМЕЧАНИЕ: *По этой команде будут временно доступны (доступны для выбора) только те этажи лифта, которые помечены флажком "X" в колонке "State" (Статус) в меню Floor group Definition (Назначение группы этажей).*

ПРИМЕЧАНИЕ: *Для этой операции не предусмотрено никакой анимационной картинки. Чтобы временно разблокировать все этажи, следует воспользоваться командой "Temporarily unlock door" (Временно разблокировать дверь) в меню "Manual operation on doors" (Ручное управление дверями).*

Сброс расписания лифтовой двери

Система EntraPass предусматривает возвращение к выполнению расписания для двери лифта после работы с компонентом в ручном режиме.

1. В меню Elevator door (Двери лифта) выделить нужную(ые) дверь(и) или группу дверей.
2. Нажать кнопку **Return to Schedule** (Вернуться к расписанию). По этой команде выполняется повторная загрузка расписания для выбранных компонентов.

Разрешить доступ на этаж лифта

1. В меню Elevator floor (Этаж лифта) выделить нужный(ые) этаж(и) или группу этажей.
2. Нажать кнопку **Enable elevator floor** (Разрешить доступ на этаж из лифта). Эта функция разрешает доступ на этаж или группу этажей, которые раньше были отключены (disabled).

Запретить доступ на этаж из лифта

1. В меню Elevator floor (Этаж лифта) выделить нужный(ые) этаж(и) или группу этажей
2. Нажать кнопку **Disabled elevator floor** (Отключить доступ на этаж из лифта). Эта функция делает недоступным ранее доступный этаж лифта. Ставший недоступным этаж перекрывает доступ всем посетителям, даже тем, у кого есть права доступа.

Операции с реле при работе в ручном режиме

Этот раздел меню используется для изменения вручную состояния реле (одного или группы). Здесь доступны команды активации/деактивации, а также временной активации реле (одного или группы). Это окно также отображает в режиме реального времени статус выбранного(ых) реле.

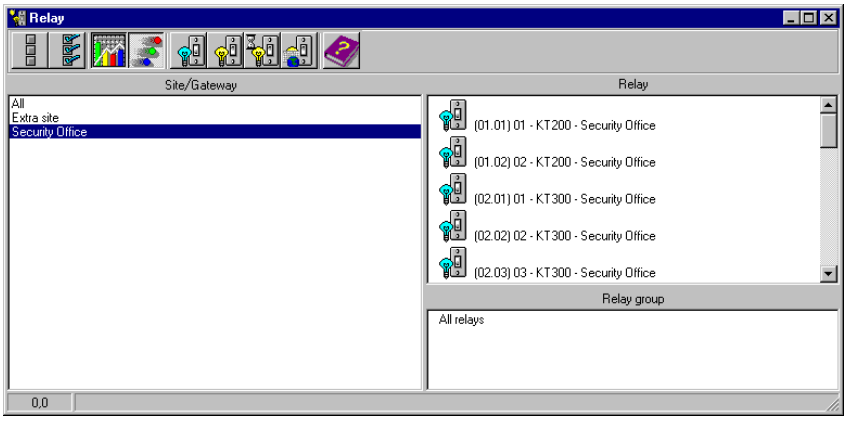
Данная функция позволяет вручную выключать реле; например, когда вход, запрограммированный на активацию реле, переходит в тревожный режим по непонятным причинам. .

Кнопка	Описание
	Deactivate relay (Деактивировать реле) – позволяет оператору деактивировать реле, которое перед этим было активировано по одной из следующих причин: по команде оператора, по расписанию, в результате возникновения события или по тревожному входу.
	Activate relay (Активировать реле) – позволяет оператору активировать реле, которое перед этим было деактивировано по одной из следующих причин: по команде оператора, по расписанию, в результате возникновения события или по тревожному входу.
	Temporarily activated relay (Временно активировать реле) – временно активировать реле (одно или группу) на указанное время.
	Return to schedule (Вернуться к выполнению расписания) – возобновить работу по расписанию после работы с компонентом в ручном режиме.

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выбор реле

1 В окне Operation (Управление) нажать иконку **Relay** (Реле).



2 Нажать на кнопку **Enable animation** (Разрешить анимацию), чтобы в режиме реального времени отображался статус реле.

- На панели слева показан список всех сайтов(лучей)/шлюзов под заголовком **Sites/Gateways**. Выбрать все или один сайт(луч)/шлюз.
- Отдельные реле, прикреплённые к сайту(лучу)/шлюзу, выбранному на панели слева, отображаются справа в верхней части окна. Если слева выбрана опция **All** (Все), то справа отображаются все реле системы. Можно выделить одно, несколько или все реле.
- **Группы реле**, прикреплённые к сайту(лучу)/шлюзу, выбранному на панели слева, отображаются справа в нижней части окна. Если слева выбрана опция **All** (Все), то внизу справа отображаются все группы реле в системе. При этом можно выделить одну или несколько или все группы.

Деактивация реле вручную

1 Выделить реле (одно или группу).
2 Нажать кнопку **Deactivate Relay** (Деактивировать реле).

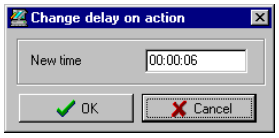
ПРИМЕЧАНИЕ: *Если вручную деактивировать реле, которое обычно активируется по расписанию, оно не будет активироваться, пока расписание его активации не станет достоверным. Это означает, что если реле должно срабатывать по расписанию, а его деактивировали вручную, то его нужно снова активировать вручную на оставшееся время действия по расписанию, так как одно реле может использоваться для разных компонентов системы, и его активация или деактивация влияет на работу этих компонентов.*

Активация реле вручную

1 Выделить реле (одно или группу).
2 Нажать кнопку **Activate Relay** (Активировать реле). Выбранные реле будут активированы. Данная функция позволяет оператору активировать реле, которое перед этим было деактивировано по одной из следующих причин: по команде оператора, по расписанию, в результате возникновения события или по тревожному входу.

Временная активация реле

1 На панели справа верхнее поле предназначено для выделения отдельных реле, в нижней части находится кнопка для выделения всех реле (**All Relays**).
2 Нажать кнопку **Activate relay temporarily** (Активировать реле временно). На экране появляется диалоговое окно Change delay on action (Изменить задержку выполнения).
3 В поле **New time** (Новое время) указать величину задержки и нажать **OK** (мин. сек.). Выбранное реле будет временно разблокировано по команде оператора.



ПРИМЕЧАНИЕ: *Выбранные реле будут активированы временно. Это позволяет оператору временно активировать реле, которое перед этим было деактивировано по одной из следующих причин: по команде оператора, по расписанию, в результате возникновения события или по тревожному входу. Для указания длительности активации реле на экран выводится диалоговое окно с запросом времени задержки. После окончания этой задержки реле будет деактивироваться автоматически.*

Перезагрузка расписания реле/ Возвращения режима работы реле по расписанию

Система EntraPass предусматривает возвращение к выполнению расписания после работы с компонентом в ручном режиме.

1 В меню Relay (Реле) выделить нужное(ые) реле или группу реле.
2 Нажать кнопку **Return to Schedule** (Вернуться к расписанию). По этой команде выполняется повторная загрузка расписания для выбранных компонентов.

Операции с входами/inputs при работе в ручном режиме

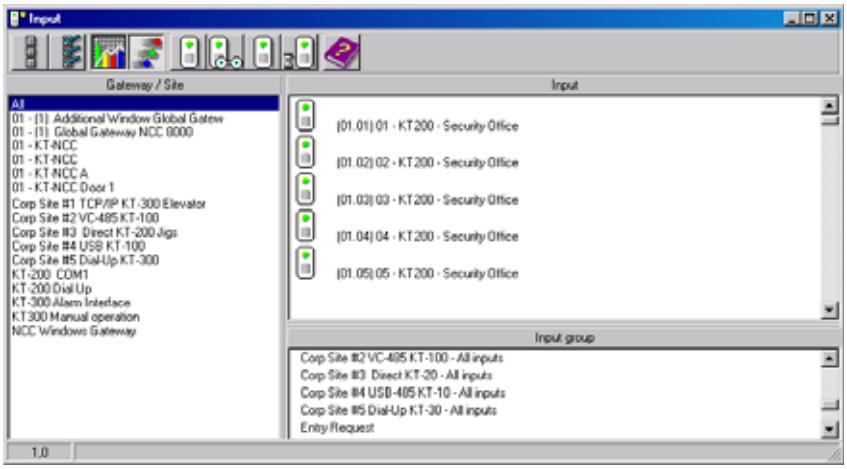
Этот раздел меню позволяет вернуть вход в нормальное состояние, прекратить мониторинг входа, выполнять мониторинг состояния определённого входа постоянно, временно шунтировать выбранный вход, если его статус, описанный в меню Device (Устройства), перед этим изменился.

Кнопка	Описание
	Input normal (Вернуть нормальный статус) – вернуть вход в нормальное состояние, в соответствии с настройками в меню Device (Устройство).
	Input continuous supervision (Непрерывный мониторинг входа) – постоянно следить за выбранным входом.
	Input with no supervision (Прекратить мониторинг входа) – отменить мониторинг входа, независимо от расписания, и возобновить его при следующей активации по расписанию.
	Input no supervision temporarily (Shunt) (Временное прекращение мониторинга входа (шунтирование)) – отключение мониторинга входа на определённое время.

ПРИМЕЧАНИЕ: *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Операции с входами при работе в ручном режиме

1 В окне Operation (Управление) нажать иконку **Input** (Входы).



2 Нажать на кнопку **Enable animation** (Разрешить анимацию), чтобы в режиме реального времени отображался статус реле.
- На панели слева показан список всех сайтов(лучей)/шлюзов под заголовком **Sites/Gateways**. Выбрать все (**All**) или один сайт(луч)/шлюз.
- Отдельные входы, прикреплённые к сайту(лучу)/шлюзу, выбранному на панели слева, отображаются справа в верхней части окна. Если слева выбрана опция All (Все), то справа отображаются все входы системы. Можно выделить один, несколько или все входы.
- **Группы входов**, прикреплённые к сайту/шлюзу, выбранному на панели слева, отображаются справа в нижней части окна. Если слева выбрана опция **All** (Все), то внизу справа отображаются все группы входов системы. При этом можно выделить одну или несколько или все группы входов.

Возврат входа в нормальное состояние вручную

Эта функция полезна в тех случаях, когда статус входа был изменён оператором, и необходимо вернуть его в нормальное состояние. Например, если по определённому расписанию, указанному в настройках, выполняется мониторинг входа, а оператор изменил статус входа на "неконтролируемый", то с помощью этой команды можно вернуть вход в нормальное (контролируемое) состояние.

1 Выделить вход или группу входов.
2 Нажать кнопку **Input normal** (Вернуть нормальный статус входа). Выбранный вход вернётся в нормальное состояние, в соответствии с настройками в меню **Device** (Устройство).

Установка продолжительного контроля входа

Вы можете использовать это преимущество для того, чтобы контролировать вход всегда. Эта опция может быть установлена вручную.

1 Выделить вход или группу входов.
2 Нажмите кнопку **Input continuous supervision** (продолжительный контроль входа).

Прекращение мониторинга входа

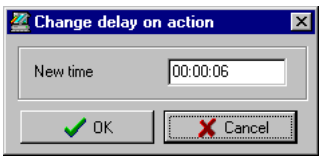
Эта команда используется для отмены мониторинга входа, независимо от его расписания (если оно настроено).

1 Выделить вход или группу входов.
2 Нажать кнопку **Input no supervision** (Прекратить мониторинг входа). Мониторинг выбранного входа будет прекращён.

Временное прекращение мониторинга входа (шунтирование)

Эту команду следует использовать для шунтирования выбранного входа на определённое время.

1 Чтобы временно шунтировать вход, его следует выделить из списка и затем нажать кнопку **Temporarily shunt.** Мониторинг выбранного входа будет временно прекращён.
2 Нажать кнопку **Input no supervision temporarily** (Временное прекращение мониторинга входа). На экране появляется диалоговое окно Change delay on action (Изменить задержку выполнения).



3 В поле **New time** (Новое время) указать величину задержки (мин:сек) и нажать **OK**. Пиктограмма рядом со входом будет указывать, что его мониторинг временно отключён/шунтирован. В случае возникновения тревоги или физического отсоединения этого входа сообщения на рабочий стол сообщений (Message) отправляться не будут.

Ручное управление над тревожной системой

Это меню позволяет вам в ручном режиме изменять состояние тревожной системы. Вы можете в ручном режиме ставить/снимать с охраны, изменять задержку отложения на перепостановку на охрану. Тревожная система может быть только использована под Шлюзами Global и NCC8000.

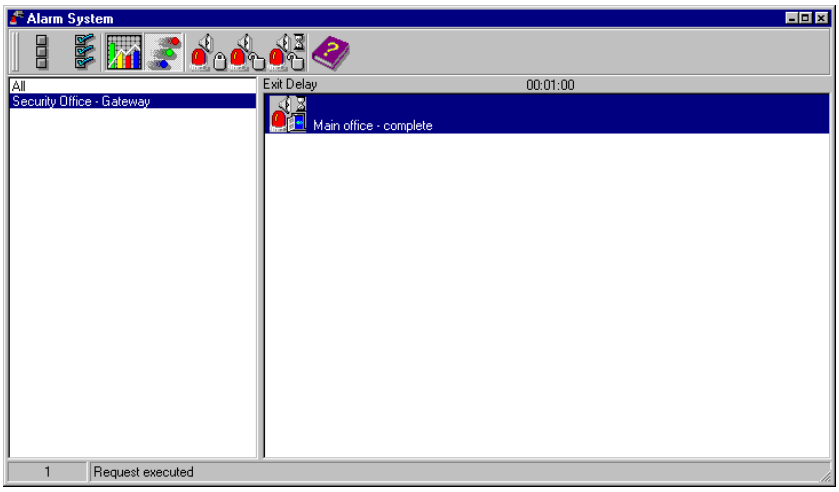
Кнопка	Описание
	Arm alarm (Поставить на охрану): Система будет поставлена на охрану по истечении задержки на постановку.
	Disarm alarm (снять с охраны): Система будет снята с охраны по истечении задержки на снятие (задержка на вход).
	Alarm postpone (отложить постановку на охрану): система будет автоматически включать режим откладывания постановки на охрану тревожной системы, пока тревожная система находится в режиме отложения тревоги “postpone mode”.

Вы можете также смотреть оставшееся время в любом случае для любого раздела для задержек на вход/выход, задержек на отложение постановки на охрану.

ПРИМЕЧАНИЕ: *Невозможно в ручном режиме включить режим отложения тревожного раздела из этого окна при условии, что он назначен производить данную операцию при помощи прикладывания карты к считывателю.*

Исполнение ручного управление над тревожной системой

1 Из окна Operation (Управление), Нажмите кнопку **Alarm system** (тревожная система).



2 Нажмите кнопку **Enable animation** (разрешить анимацию), чтобы видеть в режиме on-line состояние тревожной системы.
- Левая панель отображает список всех шлюзов. Вы можете выбрать любой или указать один из них.
- Любая тревожная система, назначенна для опреденного шлюза, которая выбрана слева, будет отображена на правой панели. Если вы выберите All слева, то все тревожные системы будут отображены справа. Вы можете указать одну, несколько или все тревожные системы.

Постановка на охрану тревожной системы в ручном режиме

Эта опция позволяет вам автоматически ставить на охрану по истечении задержки на выход. *Более подробно смотрите в Главе 5 ":Назначения" на странице 173*

1 Выберите шлюз или тревожную систему.

2 Нажмите на кнопку **Arm alarm** (Поставить на охрану). Выбранная система будет автоматчически поставлена на охрану.

Снятие с охраны тревожной системы в ручном режиме

Эта опция позволяет вам автоматически сниматьс охраны систему по истечении задержки на вход. *Более подробно смотрите в Главе 5 ":Назначения" на странице 173*

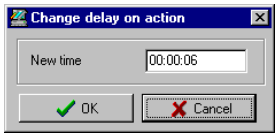
1 Выберите шлюз или тревожную систему.
2 Нажмите на кнопку **Disarm alarm** (Снять с охраны). Выбранная система будет автоматчически снята с охраны.

ПРИМЕЧАНИЕ: *Если в настоящее время действует расписание “no disarm” (не снимать с охраны) и оператор пытается снять систему с охраны. Тревожная система будет запускать задержку на выход, по истечении которой раздел опять встанет на охрану автоматически. Раздел встанет на охрану по истечении времени задежки на выход при условии, что не включен режим отложения “postpone” и если расписание “no disarm” все еще действует.*

Изменение времени отложения постановки тревожной системы в ручном режиме

Эта опция используется для изменения времени отложения постановки на охрану пока тревожная система находится в режиме отложения постановки “postpone mode”.

1 Выберите шлюз или тревожную систему.
1 Нажмите **Alarm postpone** (режим отложения)**.** Измените задержку в появившемся окне.
2 Введите новую задержку в окне **New time** delay (m:ss) и нажмите **OK**. Выбранная тревожная система будет иметь измененное время отложения постановки. Максимальное время: 16 часов.



ПРИМЕЧАНИЕ: *Это операция не будет уменьшать установленный счетчик количества возможных отложений .*

Ручное управление с Guard Tour

Это пункт позволяеи оператору инициировать, изменять задержку между пунктами обхода, изменять следующий пункт назначения обхода и заканчивать guard tour. Панель управления Guard tour может быть только использована с Глобальным Шлюзом.

Кнопка	Описание
	Start guard tour (Запустить guard tour): должна быть нажата для запуска guard tour.
	End guard tour (Окончить guard tour): должна быть нажата после посещения конечного пункта обхода guard tour.

Guard tour используется для выполнения охранных туров обхода охранниками. Оператор будет видеть события посещения каждого пункта.

Каждый Guard tour может содержать различные пункты обхода и время между ними. Если охранник не достиг нужного пункта вовремя, тогда оператор будет получать тревожное сообщение. Пунктами обхода могут являтся входа и считыватели.

ПРИМЕЧАНИЕ: *Guard Tour может быть запущен и остановлен только в ручном режиме.*

Запуск Guard Tour

1 Из выпадающего списка Gateway (Шлюз), выберите шлюз, где у вас назначен необходимый guard tour.
2 Выберите Guard tour, который вы хотите запустить из списка **Guard tours** list. После того, как вы выбрали guard tour, нажмите на кнопку “Start Guard Tour” (запустить Guard tour). Система отобразит окно выбора карты доступа:
3 Выберите картодержателя, кто будет исполнять данный Guard tour. Если какие-либо двери назначены в данный тур обхода, то данная карта должна иметь доступ к этим дверям. После того, как вы выбрали картодержателя, затем нажмите OK. Система будет отображать окно тура обхода.

ПРИМЕЧАНИЕ: *Пожалуйста, имейте в виду следующее:*

- *В течении тура, использование кнопки “modify” (изменить) будет сбрасывать время, назначенное для прохода между двумя станциями.*
- *Только один тур обхода может быть запущен в одно время на одном шлюзе.*
- *Тур должен быть всегда закончен командой “End guard tour” (окончание тура), после появления сообщения оператору “Last station in guard tour” (последняя станция тура).*
- *В течении тура, если задержка между пунктами вышла, используйте кнопку “modify”. Данная кнопка будет сбрасывать время между двумя пунктами.*

4 Нажмите кнопку **More** (более), чтобы отобразить информацию о выбранном туре. Система будет отображать пункты и задержки. Эта кнопка таже может быть использована после запуска тура.
5 Нажмите иконку **Start guard tour** для того, чтобы запустить тур. Тур может быть запущен только из этого окна. Вы можете также назначить расписание, которое будет выдавать сообщение “Guard Tour Scheduled” (необходимо выполнить тур обхода). Это будет напоминать оператору о необходимости проведения тура обхода.
6 Нажмите иконку **End guard tour** чтобы окончить тур обхода. Когда последний пункт будет посещен, то ситема будет выдавать сообщение “Last station in guard tour” (псоледняя станция тура). Затем нажмите кнопку “end guard tour” (окончить тур). После нажатия данной кнопки, система будет выдавать событие “Ending of a guard tour” (окончание тура).
7 Нажмите кнопку **End guard tour** (окончить тур), чтобы отменить тур, который был начат.

Следующие иконки отображаются справа. Они обеспечивают дополнительную информацию о туре:

- **Previous station** (предыдущий пункт)—Обеспечивает информацию (текстовую и графическую) относительно предыдущего пункта (дверь или вход) тура обхода.

- **Next station** (Следующий пункт)—Обеспечивает информацию (текстовую и графическую) относительно следующего пункта (дверь или вход) тура обхода.
- **Delay to next station** (задержка до следующего пункта)—Показывает время, необходимое для достижения следующего пункта. Если это время вышло, вам будет отображено предупреждающее сообщение.
- **State** (Состояние) - Отображает состояние тура. Возможны два состояния:
  - **Normal**—Когда тур в нормальном состояниеи.
  - **Pre-alarm** (пред тревога)—Например, если задержка запрограммирована на 2 минуты, и задержка истекла, то система будет посылать сообщение “Guard tour station late” (опоздание тура). Затем система будет инициировать пред тревожную задержку. По истечени которой, система будет сообщать тревогу “Guard tour alarm” (тревога тура) и состояние тура изменится на тревожное.
  - **Alarm** (Тревога): когда пред тревожная задержка истекает, то тогда идет тревога по guard tour.
- **Modify next station** (Изменить следующую станцию)—Эта опция позволяет оператору изменять назначение следующей станции, если тур находится в процессе выполнения.
- Когда вы изменяете следующую станцию, то система будет сообщать тревогу “Guard tour sequence modified” (Guard tour - изменение последовательности обхода).
- **Modify delay to next station** (изменить задержку для следующего пункта— Эта опция будет позволять оператору изменять время, которое необходимо для достижения следующего пункта. Это изменение имеет эффект только для тура, который находится в процессе.

ПРИМЕЧАНИЕ: *Когда вы изменяете следущий пункт, система будет генерировать сообщение “Guard tour late time delay modified” (Время опоздания по туру изменено).*

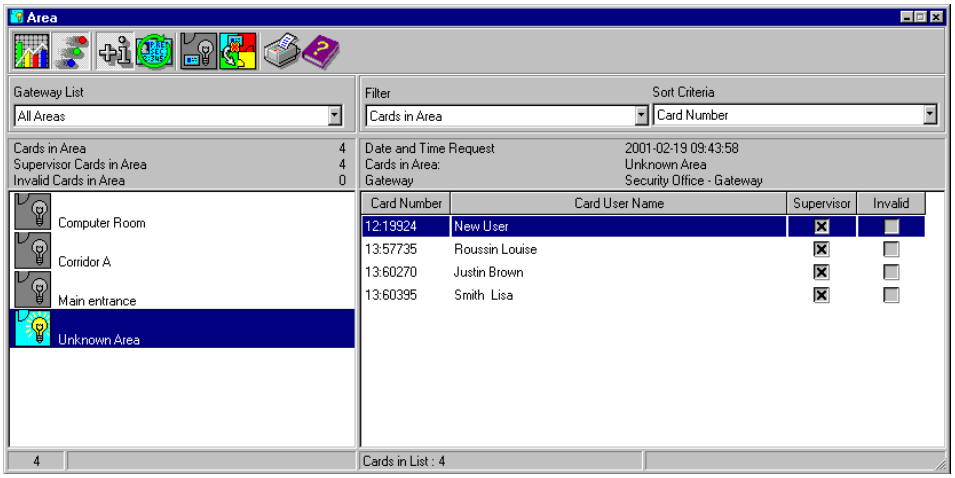
Управление областями в ручном режиме

Это преимущество используется, чтобы перемещать пустые карты, которые находятся в области, перемещать в неизвестную область. Также имеется возможность перемещать карты в опреденную область. Панель инструментов Area (Области) может быть использована только с Шлюзами Global.

Кнопка	Описание
	Get card list (Получить список карт): Вам будет отображен список карт, которые находятся в данной области. Также может быть применен фильтр и сортировка.
	Empty area (Очистить область): Все карты выбранной области будут перемещены в неизвестную область.
	Move only selected card (Переместить только выбранные карты): Выбранные карты будут перемещены в определенную область.

Вы также можете просмотреть карты ревизоров (supervisor cards), неверные карты или все карты, расположенные в данной области.

1 Из списка Gateway, выберите шлюз, для просмотра области.



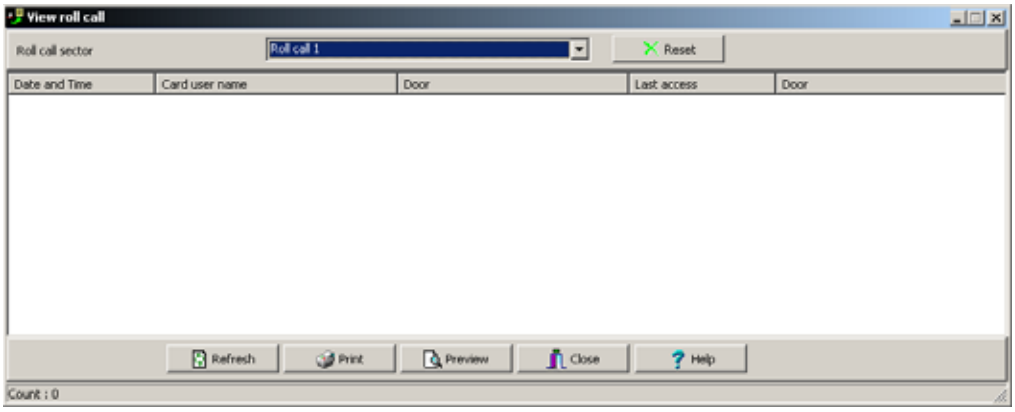
2 Выберите область на пенели слевой стороны (например, карты в области). Система будет отображать:
- количество карт, расположнные в выбранной области (все карты, ревизоры, недействительные).
- количество карт ревизоров, расположенных в данной области (назначенной с уровнем ревизоров).
- количество недействительных карт, которые расположены в данной области. Карта может быть недействительна, потому что назначенное расписание не подразумевает нахождение персонала данного уровня доступа в указанное время в данной области.

3 Из выпадающего окна **Filter** (фильтр) выберите пункт, затем нажмите кнопку **Refresh** (обновить) для того, чтобы отобразить детальную информацию по выделенному пункту.
- **Cards in Area** (Карты в области)—если выбрано, тогда система отобразит все карты, расположенные в данной области. Общее количество карт будет отображено под полем “gateway list” (список шлюзов).
- **Supervisor Cards in Areas** (карты ревизоров в области)—если выбрано, тогда система будет отображать карты ревизоров (назначеннные с supervisor level), расположенные в выбранной области. Общее количество карт будет отображено под полем “gateway list” (список шлюзов).
- **Invalid Cards in Area** (Недействительные карты в области)—если выбрано, тогда система будет отображать все карты в данной области. Общее количество карт будет отображаться в окнеслева наверху (все карты, ревизоры, недействительные). Когда карта ivalid (недействительная), то это значит, что уровень доступа карты не имеет уровень доступа в данную область. Например, пользователи остаются в области большее

количество времени чем им положено, их карты будут становится invalid (недействительные) и пользователи будут неспособны покинуть данную область.

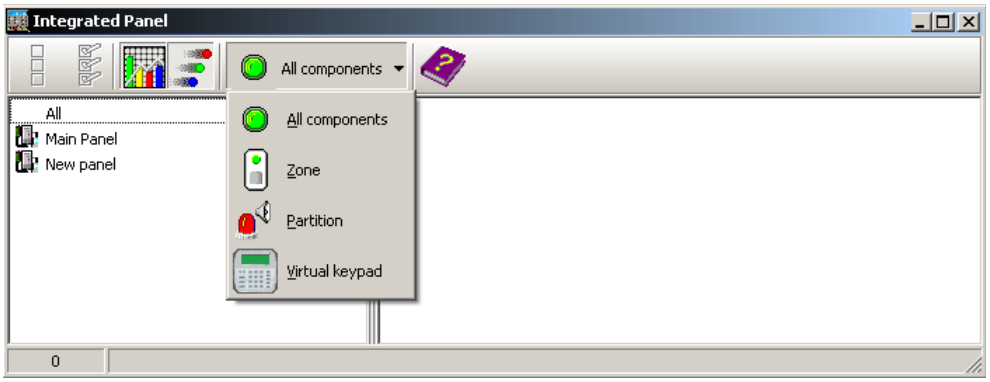
Ручное управление над View Roll Call

Это преимущество позволяет отображать вход пользователей. Когда пользователи входят в область, то эти данные отображаются на панели:



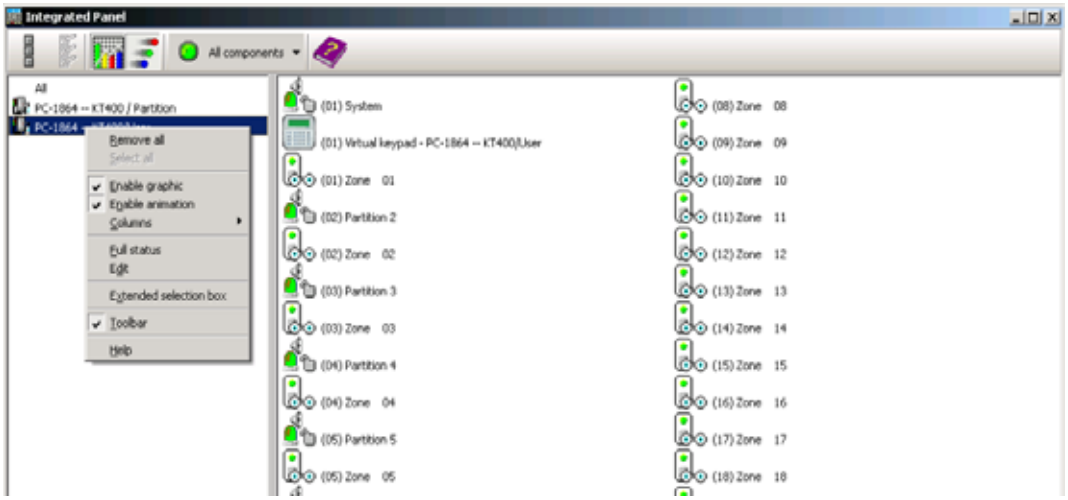
Ручные управление над интегрированными панелями

1 Из панели инстурментов **Operations** (Управление),выбериите иконку **Integrated Panel** (интегрированная панель).

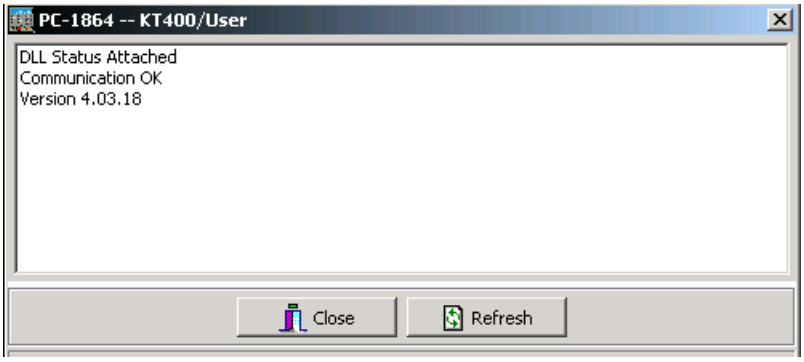


2 Если требуется, выберите определенный компонент из выпадающего списка **All components** (все компоенты).

3 Выберите из левой панели охранную панель, затем вызовите контекстное меню, нажатием правой кнопки мыши.

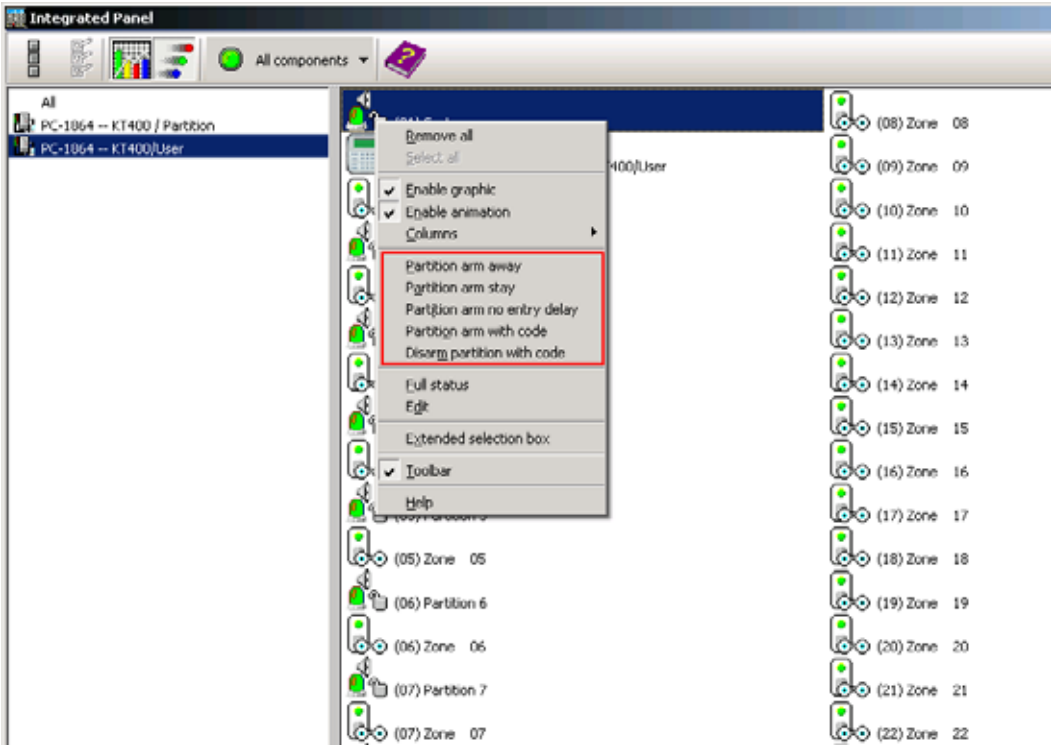


4 Выберите пункт **Full status** (полное состояние) чтобы видеть состояние интегрированной панели.



5 Выберите **Virtual Keypad** для просмотра виртуального пульта.

6 Выберите **partition** (раздел) и вызовите контекстное меню.



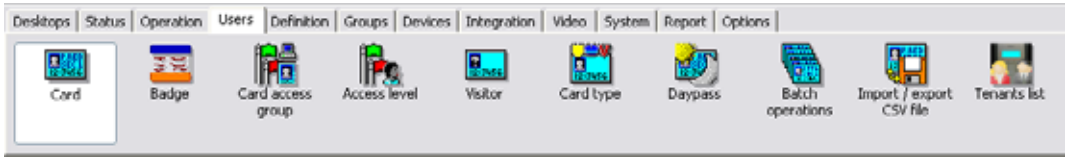
7 Выберите **Arm partition** (поставить раздел на охрану) или **Disarm partition** (снять раздел с охраны), если требуется.

ПРИМЕЧАНИЕ: *Для того, чтобы кнопка Integrated Panel была доступна, панель должна быть создана в разделе* ***Device*** *(Устройства)****> Integrated Panel*** *(Интегрированные панели)****.*** *После этого исполнить функцию* ***Logout/Login*** *(перелогиниться) для включения этой функции. Более подробно смотрите в Главе 4 "Настройка интегрированной панели охранной сигнализации" на странице 168 для большей информации относительно созддании данной панели в системе EntraPass.*

Глава 8 • Пользователи

Панель инструментов Users (Пользователи)

Меню **Users** (Пользователи) служит для работы с базами данных по владельцам идентификационных карт. Панель инструментов в окне **Users** служит для вызова следующих функций:



- Назначение и выпуск карт, а также выполнение различных задач по работе с картами (поиск, изменение или удаление выпущенных карт);
- Создание и изготовление электронных пропусков при помощи встроенных программных средств. Данная функция позволяет загружать фотографии и подписи сотрудников, а также с помощью соответствующих устройств оцифровывать изображения и помещать на карты при печати электронных пропусков;
- Создание и управление уровнем доступа для групп идентификационных карт;
- Задание уровней доступа;
- Назначение несколько уровней доступа на карту;
- Создание шаблонов для visitor card (карт посетителей);
- Назначение типов карт;
- Назначение и выпуск разовых пропусков;
- Изменение над группами идентификационных карт;
- Импорт и экспорт файлов формата CSV.

Система EntraPass оснащена программными средствами для создания и изготовления электронных пропусков. Кроме того, она позволяет импортировать или, при использовании соответствующих программ, оцифровывать и вставлять фотографии и подписи владельцев карт при подгтовке пропуска к печати.

- Назначать и изменять список жильцов для Kantech Telephone Entry System (KTES).

Назначение карт (раздел Card)

При назначении карт необходимо указать следующие параметры: номе карты (card number), имя владельца (cardholder name), тип карты (card type), уровень доступа (access level) и состояние (status), по которому карта может быть действительной (valid), недействительной (invalid), отложенной (pending), потерянной/украденной (lost/stolen) или просроченной (expired). Если в меню Card format (Формат карты) была выбрана опция **Use card multiple format** (Использовать несколько форматов карт), то вы можете изменить формат карты для каждого типа (В меню Card(Карты)). (Смотрите в Главе 14 Назначение формата представления идентификационных карт' на странице 470 для более подробной информации). Эта опция повышает гибкость системы при использовании идентификационных карт на объектах, оснащённых разными технологиями считывания карт. Другими словами, создавая новую карту пользователя, оператор имеет возможность выбрать формат карты непосредственно в меню Card, учитывая тип считывателей в тех охранных зонах, к которым будет иметь доступ данный пользователь. Если в меню System parameters (Системные параметры) отмечена флажком опция Enhanced user management (Расширенное администрирование пользователей) (Смотрите в Главе 14 Настройки регистрационных данных (Credential parameters)' на странице 494 для более подробной информации), то назначение карт будет незначительно отличаться.

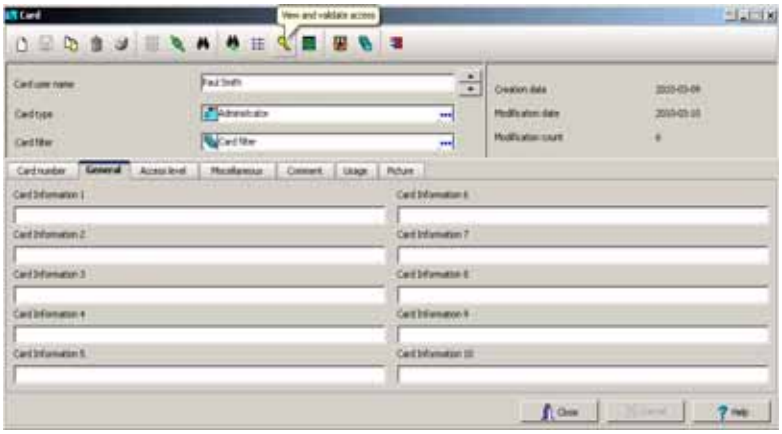
При использовании этого типа администрирования возможно создание карт пользователя без присвоения им номера. И в том и в другом случае карты идентифицируются по: имени владельца, типу карты, уровню доступа и состоянию (действительная, недействительная, отложенная, потерянная/украденная).

Карты доступны для поиска, сортировки и удаления.

Выпуск новой карты

1 В меню **Users** (Пользователи) нажать на иконку **Card** (Идентификационные карты). Открывшееся окно Card служит для ввода/проверки основной информации о владельце карты.

ПРИМЕЧАНИЕ: *Если в настройках активирована опция **Enhanced User Management** (Расширенное администрирование пользователей), то следует перейти к следующему разделу Смотрите пункт "Выпуск новой карты в режиме расширенного администрирования пользователей" на странице 285 для более подробной информации .*



2 Нажать на панели инструментов кнопку **New** (Создать). Появится поле для ввода номера карты (Card number).

3 Указать в поле **Card number** номер, напечатанный на карте, и нажать **Enter** (Ввод). Если это новая карта, то в поле **Card user name** (Имя пользователя карты) появится надпись “New user” (Новый пользователь). Если карта уже давно создана, на экране появится информация об этой карте.

4 В поле **Card user name** ввести имя владельца карты. Допускается ввод имени длиной до 50 символов.

5 Поставить флажок в поле **Copy to visitor card** (Копировать в карты посетителей). При выделении флажком этой опции содержимое всех информационных полей карты (кроме её номера) копируется в базу данных по шаблонам посетителей (Visitor template). Это позволяет архивировать данные для последующего их извлечения, если возникнет необходимость изготовить временную карту.

6 Отметить флажком опцию **Card type** (Тип карты), чтобы получить доступ к меню **Card type**. Выбрать тип для новой карты. Тип карты позволяет сортировать владельцев карт по группам; это полезная функция при изменении уже созданных групп карт, при создании отчётов и др. Более подробная информация о создании/изменении типов карт приведена в другом разделе. *Смотрите в Главе 8 Назначение типов карт' на странице 328 для более подробной информации .*

ПРИМЕЧАНИЕ: *При нажатии на правую кнопку мыши в окне Card type (Тип карты) открывается контекстное меню, позволяющее создать новый тип карты (***New***), выбрать уже созданный тип карты (***Select***) или отредактировать уже созданный тип карты (***Edit***).*

ПРИМЕЧАНИЕ: *Система автоматически отображает дату создания карты в поле* ***Creation date****, дату изменения в поле* ***Modification date*** *и счётчик изменений в поле* ***Modification count*** *в верхнем правом углу окна Card.*

7 Заполнить поля **Card Information 1 ... 10**. Это поля для ввода информации о пользователе. Они служат для хранения дополнительных сведений о владельце карты. Например, поле №1 (Card Information 1) можно использовать для указания номера трудового договора, в поле №2 (Card Information 2) записать отдел, в котором работает пользователь, поле №3 (Card Information 3) может служить для ввода домашнего адреса и т.д. Позднее информационные поля карты можно использовать при составлении отчётов, оформлении списков владельцев карт и т.п.

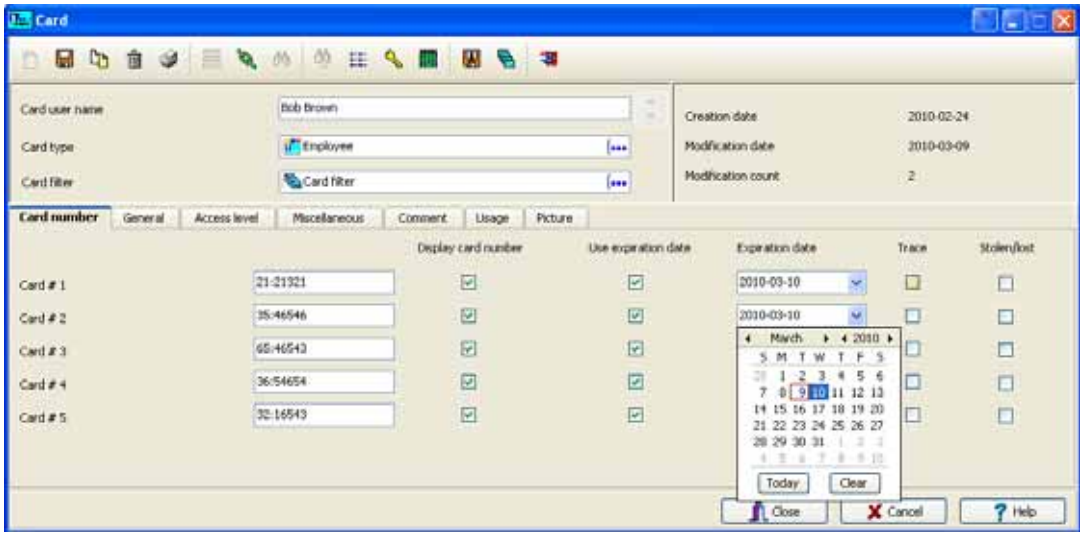
ПРИМЕЧАНИЕ: *Названия информационных полей карты тоже можно изменять. Для того чтобы переименовать название информационного поля, следует дважды щёлкнуть по нему мышкой и ввести новое имя в открывшемся поле. Допускается ввод имени длиной до 50 символов.*

8 Нажать кнопку **Save** (Сохранить).

Выпуск новой карты в режиме расширенного администрирования пользователей

ПРИМЕЧАНИЕ: *Смотрите в Главе 14 Настройки регистрационных данных (Credential parameters)' на странице 494 для более подробной информации для получения дополнительных деталей как включить режим* ***Enhanced User Management*** *(расширенное управление пользователями).*

1 В меню **Users** (Пользователи) нажать на иконку **Card** (Идентификационные карты). Открывшееся окно Card служит для ввода/проверки основной информации о владельце карты.



2 Нажать на панели инструментов кнопку **New** (Создать). В поле **Card user name** (Имя пользователя карты) ввести имя владельца карты. Допускается ввод имени длиной до 50 символов.

3 Нажать **Save** (Сохранить).

4 Дважды щёлкнуть в поле **Card type** (Тип карты), чтобы открыть окно **Card type**. Выбрать тип для новой карты. Тип карты позволяет сортировать владельцев карт по группам; это полезная функция при изменении уже созданных групп карт, при создании отчётов и др. Более подробная

информация о создании/изменении типов карт *Смотрите пункт "Назначение типов карт" на странице 328 для более подробной информации* .

ПРИМЕЧАНИЕ: *При нажатии на правую кнопку мыши в поле* ***Card type*** *(Тип карты) открывается контекстное меню, позволяющее создать новый тип карты (****New****), выбрать уже созданный тип карты (****Select****) или отредактировать уже созданный тип карты (****Edit****).*

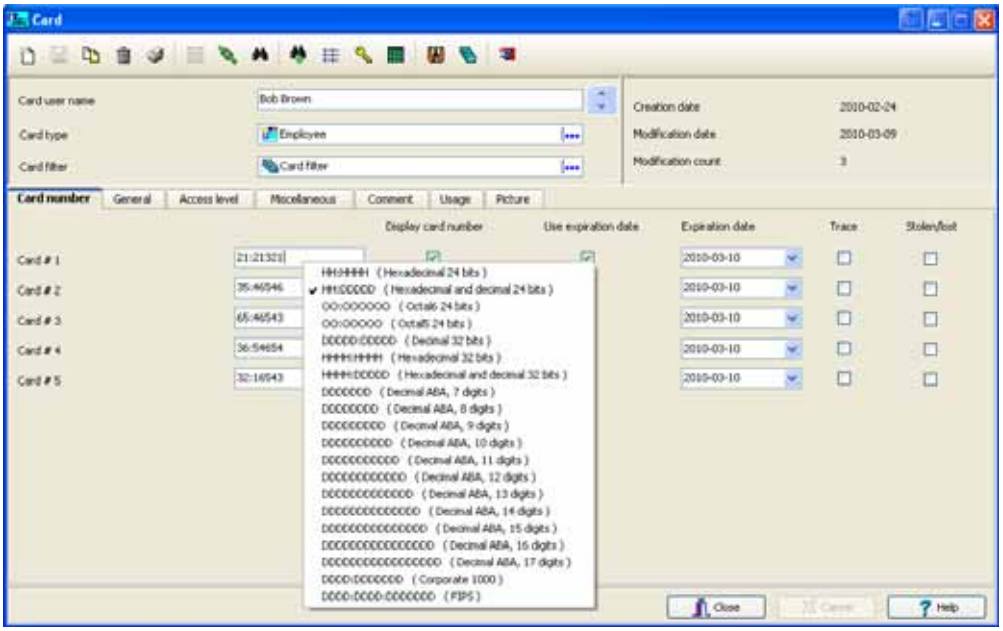
5 Открыть закладку **Card number** (Номер карты), дважды щёлкнуть по надписи **Card #1,** чтобы изменить название полей с данными карты.

6 В поле **Card number** указать номер карты.

- Если система настроена на работу с разными форматами карт Multiple Card Format, то формат выбранной карты можно изменить нажатием на правую кнопку мыши в поле **Card number**, (Смотрите в Главе 14 Назначение формата представления идентификационных карт' на странице 470 для более подробной информации) для открытия нескольких форматов карт на карту и выбрать новый формат по умолчанию для карт №1...№5. Используемый по умолчанию формат карты – HH:DDDDD (шестнадцатеричный и десятичный 24-бита).

ПРИМЕЧАНИЕ: *Уровень доступа (****Access Level****) применяется к пользователю, то есть ко всем его пяти картам.*

- **Если используется несколько форматов карт на карту(Multiple Card Format).** Список всех карт отображается при нажатии на правую кнопку мыши в поле Card number.
- **Если формат карты был установлен системным администратором.** Рядом с описанием этого формата стоит флажок.



7 При желании можно сразу же назначить номер карты в поле **Card number.** При работе с веб-станцией EntraPass WebStation можно оставить это поле незаполненным и указать номер карты позднее.

8 Если оператор обладает необходимыми правами, то он может выбрать, отображать номер карты или нет в отчётах и сообщениях на рабочих станциях EntraPass (опция **Display card number**).

ПРИМЕЧАНИЕ: *Система автоматически отображает дату создания карты в поле **Creation date**, дату изменения в поле **Modification date** и счётчик изменений в поле **Modification count** в верхнем правом углу окна Card.*

9 Отметить флажком опцию **Use expiration date** (Установить срок действия) и указать соответствующую дату в поле **Expiration date** (Конечная дата).

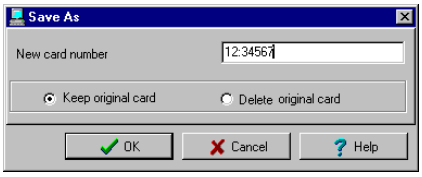
10 Чтобы осуществлять мониторинг/отслеживание карты, выделить опцию **Trace** (Отслеживать). При выделении этой опции каждое предъявление карты считывателю будет сопровождаться созданием события “Card traced” (Карта отслежена). По этим событиям можно, например, составить отчёт и отследить действия владельца карты.

11 Выделить поле **Stolen/Lost** (Потеряна/Украдена), если карта была потеряна или украдена. Такая карта больше не будет функционировать.

12 Повторить пп. 5 ... 11 для карт **Card #2 ... Card #5**, если необходимо. Перечисленные параметры могут различаться для этих пяти карт.

Создание новых карт с помощью функции "Сохранить как..."

Функция **Save as** (Сохранить как...) позволяет создавать новые карты, используя уже выпущенную карту, путём внесения необходимых изменений. Например, можно изменить только имя пользователя, и оставить неизменными все остальные данные.



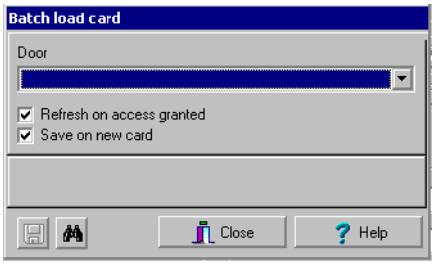
1 Внести необходимые изменения в окне Card и нажать кнопку **Save as** (Сохранить как...). Эта функция позволяет создать новую карту под новым номером.

2 В поле **New card number** ввести новый номер карты.

3 Выбрать одну из опций **Keep/Delete original card** (Сохранить/Удалить исходную карту) (как правило, исходную карту сохраняют) и нажать **OK** для сохранения новых данных. На экране должно снова появиться окно Card.

Выпуск карт с помощью функции "Групповая загрузка" (Batch Load)

Функция Batch Load позволяет операторам выпускать карты путём предъявления их считывателю двери. Номер такой карты отображается сообщением “unknown card” (неизвестная карта) или “access denied” (доступ запрещён). Во время группового считывания карт оператор может создавать новые карты или изменять уже созданные.



1 В окне Card (Карты) нажать кнопку **Batch Load** (Групповая загрузка).

2 В списке **Door** (Двери) выбрать дверь, которая будет служить для считывания карт.

3 Отметить при необходимости следующие опции:

- **Refresh an access granted** (Обновлять при разрешении доступа). Если выделить эту опцию, то при каждом разрешении доступа данные карты на экране будут обновляться.
- **Save on new card** (Сохранить как новую карту). В случае использования этой опции новые карты будут сохранены в базе данных карт вместе с сообщением “unknown card” (неизвестная карта). Если же опция не выделена, оператор должен будет вручную сохранять карту при каждом считывании.

ПРИМЕЧАНИЕ: *Если поставить флажок напротив этой опции, то первая считанная карта будет сохранена только при предъявлении следующей карты или при нажатии кнопки Save*

- Функция **Find** (Найти) позволяет осуществлять поиск в созданных картах, чтобы создать новую карту на основе уже созданной.

ПРИМЕЧАНИЕ: *При нажатии кнопки **Close** (Закрыть) без сохранения данных (если кнопка **Save** доступна) система сделает запрос о необходимости сохранения последней информации.*

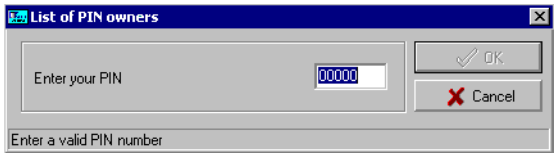
Просмотр и проверка индивидуальных PIN кодов

Система EntraPass позволяет просматривать и проверять каждый введённый код владельцев карт в окнах Card (Идентификационные карты) и Visitor (Посетители).

Просмотр карт с одинаковым кодом

1 В окне **Card** (Карты) или Visitor (Посетители) нажать кнопку **List of PIN owners** (Список владельцев кода).

2 Ввести PIN-код для проверки и нажать **OK**. На экране появится список всех операторов, код которых совпадает с указанным.



ПРИМЕЧАНИЕ: *Если в системе разрешено дублирование идентификационных кодов пользователей (**Options** > **System Parameters**), и один код используется несколькими владельцами карт, то на экране появится список пользователей с одинаковым кодом. Эту функцию полезно использовать, например, для отображения списка владельцев карт, которые используют указанный код, а также при выпуске новых карт для проверки, какие коды уже используются.*

Работа с идентификационными картами

Правка карты

- В поле **Card number** ввести номер карты и нажать **Enter** (Ввод). Указанная карта будет выведена на экран; теперь её можно изменить.
- Выберите номер карты в поле **Card number** (Номер карты) с помощью клавиш со стрелками вверх-вниз.
- В поле **Card user name** выберите имя владельца карты, используя стрелки вверх-вниз.

Поиск карты

На панели инструментов окна Card доступны два типа поиска:

Поиск данных карты

Поиск данных карты в архиве

ПРИМЕЧАНИЕ: *Смотрите в Главе 3 Поиск компонентов' на странице 53 для более подробной информации чтобы узнать как искать информацю в EntraPass.*

Удаление карты

Функция **Delete** (Удалить) позволяет оператору, обладающему необходимыми полномочиями, удалить карту из базы данных о владельцах карт. Карта, удалённая из базы данных о владельцах, может быть перевыпущена снова для повторного использования.

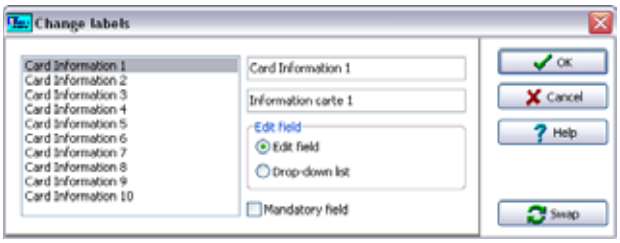
1 Найти карту, которую необходимо удалить.
2 Нажать кнопку **Delete** (Удалить) и в появившемся окошке с предупреждением (**Warning message**) выбрать **Yes** (Да).

ПРИМЕЧАНИЕ: *Несмотря на то, что при удалении карта исчезает из базы данных карт, она остаётся в архиве карт; все события, связанные с этой картой, остаются в базе данных по сообщениям о событиях. Таким образом, при необходимости может быть составлен отчёт о событиях, связанных с любой удалённой картой.*

Индивидуальная настройка названий информационных полей идентификационной карты

Информационные поля карты (**Card information**) под закладкой **General** (Общие параметры) при необходимости можно переименовать в соответствии с конкретными требованиями пользователя. В этих полях можно хранить любую информацию. Можно использовать их как окна редактирования или как выпадающие списки.

1 В меню Card следует выбрать любую карту и дважды щёлкнуть по полю **Card information** (Сведения о карте) под закладкой **General** (Общие параметры). На экране должно появиться окно **Change labels** (Изменить метки).



2 В левой части окна выбрать информационное поле, название которого необходимо изменить, и указать новое имя в правой части окна. Если для работы с системой используется два языка, следует указать два имени: одно на основном языке, а другое на дополнительном. Например, чтобы сменить название *Card Information 1 на Employee number*, следует дважды щёлкнуть по имени **Card Information 1** и ввести новое имя в свободном поле справа.
3 Выделить опцию **Edit field** (Редактируемое поле), чтобы данные появлялись одной строкой, или отметить флажком поле **Drop-down** (Выпадающий список), чтобы отображать данные в виде выпадающего списка (если необходимо). Нажать **OK** для сохранения внесённых изменений.

4 Повторить те же действия для всех полей, которые необходимо изменить.

ПРИМЕЧАНИЕ: *Отметить флажком опцию* ***Mandatory field*** *(Поле, обязательное для заполнения), если это информационное поле должно быть заполнено обязательно.*

ПРИМЕЧАНИЕ: *Для того чтобы редактировать информационные поля карты, оператор должен иметь полный доступ к базе данных. Если оператор имеет доступ только для чтения, он сможет только просматривать данные в этих полях. .*

Назначение уровней доступа владельцам карт

Для каждой карты должен быть указан уровень доступа. Уровни доступа показывают, где и когда карта будет действительной. Уровень доступа позволяет владельцу карты проходить в определённые зоны по установленному расписанию. Для большей информации по назначению уровней доступа, *Смотрите пункт "Назначение уровней доступа" на странице 326 для более подробной информации* .

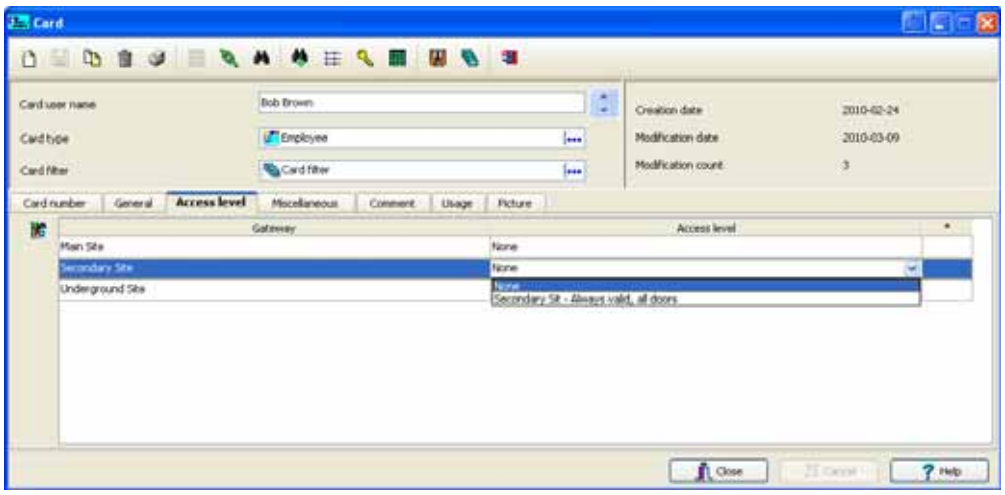
ПРИМЕЧАНИЕ: *Если изменить уровень доступа, который назначен для выбранной карты, то у пользователя карты изменится уровень доступа к дверям и изменятся расписания, связанные с этим уровнем доступа.*

Уровень доступа назначается для карты в следующем порядке:

- Создать расписания в соответствии со временем предоставления пользователю доступа к выбранным дверям;
- Назначить созданное расписание на выбранные двери (в меню задания уровня доступа Access level definition);
- Назначить для карт уровень доступа.

Назначение уровня доступа для владельца карты

1 В окне описания идентификационных карт (Card) открыть закладку **Access level** (Уровни доступа). На экране откроется окно Access level, в котором слева отображена колонка **Gateway**/**Site** (Шлюз/Сайт/Луч), а справа выпадающие списки уровней доступа **Access level.**



2 Чтобы скопировать на выбранную карту данные из её группы доступа, нажать кнопку **Card access group** (Группа доступа для карт) – эта кнопка расположена слева от колонки Gateway/Site. Колонка **Gateway**/**Site** содержит список сайтов/лучей и шлюзов, которым будет назначен уровень доступа.

3 В списке **Access level** (Уровни доступа) выбрать уровень доступа владельца карты к дверям указанного луча/объекта. Если владелец карты не должен иметь доступ к двери этого сайта, в этом поле следует указать **None** (Отсутствует).

ПРИМЕЧАНИЕ: *Чтобы в выпадающем списке **Access level** (Уровни доступа) отображались уровни доступа, их следует создать в меню **Users** (Пользователи) > **Access Level**(Уровни доступа).*

Назначение вторичного/дополнительного уровня доступа только для Global/KT-NCC/NCC 8000)

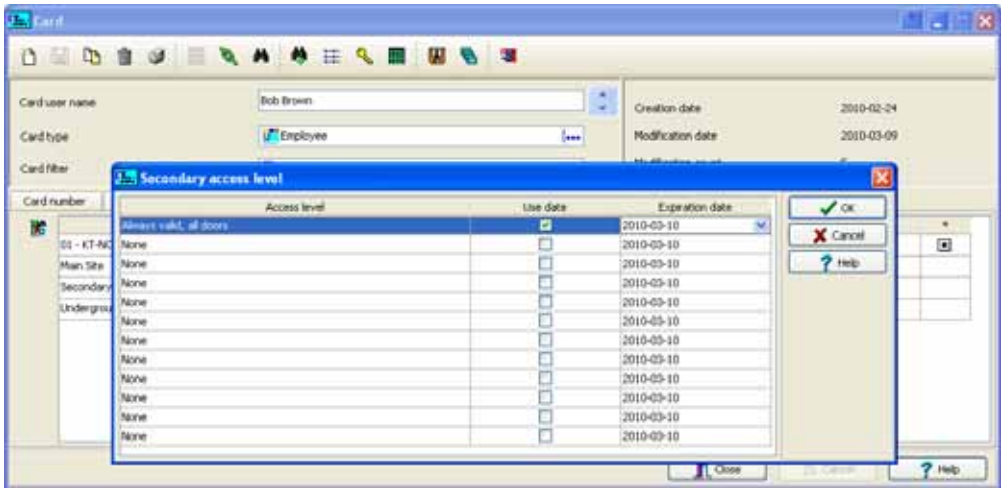
Вы можете назначить до шести вторичных/дополнительных уровней доступа на карту. Вы также можете использовать дату окончания для каждого вторичного уровня доступа. Это решает задачу

ограничения доступа к указанной двери после наступления определенной даты (кнопка отображается справа).

NOTE 1: *Когда **KT-400** работает в автономном режиме, основные и вторичные уровни доступа остаются верными.*

NOTE 2: *Когда **KT-100**, **KT-200** или **KT-300** переходят работать в автономный режим, то вторичные уровни доступа не дейтсвуют более. Действует только основной уровень доступа.*

1 Нажмите справа на кнопку, которая связывает Gateway/Site, на который вы хотите назначить вторичный/дополнительный уровень доступа.



2 Выберите уровень доступа в списке, чтобы назначить вторичный/дополнительный уровень доступа.

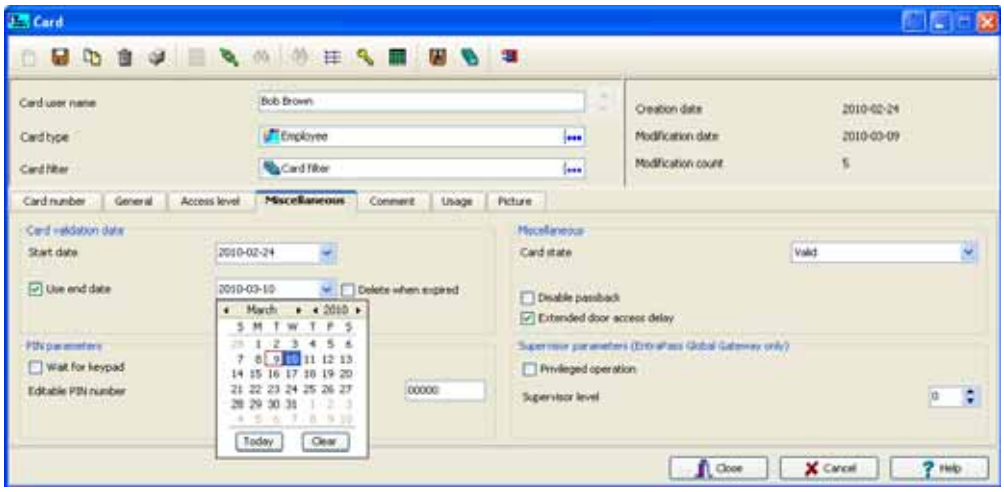
3 Если вы хотите назначить дату окончания, выберите опцию **Use date** (использовать дату). Данное действие будет открывать календарь, где вы можете выбрать дату окончания действия **Expiration date**. После того как дата будет выбрана, то она будет появляться в/под колонкой **Expiration date** (дата окончания).

ПРИМЕЧАНИЕ: *Кнопка будет отображаться зеленым индикатором при условии, что у назначен вторичный/дополнительный уровень доступа.*

Назначение дополнительных опций карт

Дополнительные функции идентификационных карт собраны в разделе **Miscellaneous** (Прочее).

1 В поле Card number выбрать номер карты при помощи стрелок вверх-вниз. В поле **Start date** (Начальная дата) указана дата создания карты. При необходимости оператор может изменить эти данные, выбрав другую дату в отображаемом на экране календаре. Начальная дата должна быть меньше или совпадать с текущей, в противном случае карте будет присвоен статус “Pending” (Отложенная), который отображается в поле **Card state** (Статус карты) справа под заголовком **Miscellaneous** (Прочее).



2 Поставить флажок в поле **Use end date** (Установить срок действия до...). Если опция будет отмечена флажком, то на экране появится календарь для выбора даты окончания действия карты. После наступления указанной даты статус карты в поле **Card state** сменится на “Expired” (Просрочена).

ПРИМЕЧАНИЕ: *При создании карты с очень коротким сроком действия (24 часа или менее), например, в качестве разового пропуска (**Day Pass**), статус карты меняется на “Expired” (Просрочена) в полночь. Такой принцип позволяет регистрировать карты всего за одну минуту.*

3 Если необходимо, отметить флажком опцию **Delete when expired** (Удалить после истечения срока действия). Эта функция используется только вместе с функцией **Use end date.** Если флажок поставлен, данные карты будут автоматически удалены после окончания указанного срока действия, а если не ставить флажок, статус карты изменится на “Expired” (Просрочена/ Истек срок действия).

ПРИМЕЧАНИЕ: *Удалённая карта – это карта, переставшая быть активной в базе данных системы. Даже после удаления карты прошлые события, связанные с этой картой, сохраняются в архивном файле.*

4 Отметить флажком опцию **Wait for keypad** (Ожидать нажатия клавиши), если для доступа ко всем дверям необходимо вводить идентификационный код, используя кнопочную панель на двери. Затем в поле **Editable PIN** (Редактируемый код) указать код, который пользователи должны будут вводить на кнопочной панели.

ПРИМЕЧАНИЕ: *В случае выбора опции **Wait for keypad** (Ожидать нажатия клавиш) доступ к двери открывается только после ввода правильного кода. Для этого в описании дверей должно быть указано, что они оснащены не только считывателем, но и кнопочной панелью (меню **Devices**(Устройства) > **Doors**(Двери)). Кроме того, расписание действия кнопочной панели для этой двери должно быть достоверным. Смотрите в Главе 4 Конфигурация дверей’ на странице 143 для более подробной информации по настройке дверей.*

5 В списке **Card state** (Статус карты) выбрать и назначить статус для данной карты. По умолчанию карта имеет статус "valid" (действительная). Предусмотрено несколько статусов карты:

- **Valid** (Действительная) – карта действует,
- **Invalid** (Недействительная) – карта НЕ действует,
- **Lost/Stolen** (Потеряна/Украдена) – карта НЕ действует,
- **Pending** (Отложенная) – карта ещё не действует.

- **Expired** (Просрочена) – карта с прошедшим сроком действия,

ПРИМЕЧАНИЕ: *Статус **Pending** (Отложенная) невозможно выбрать в списке **Card state** (Статус карты). Для этого следует изменить дату начала действия карты (Start date*

6 Выделить опцию **Disable passback** (Запрет контроль повторного прохода), если необходимо запретить для этой карты контроль повторного прохода, включенный в общих настройках.

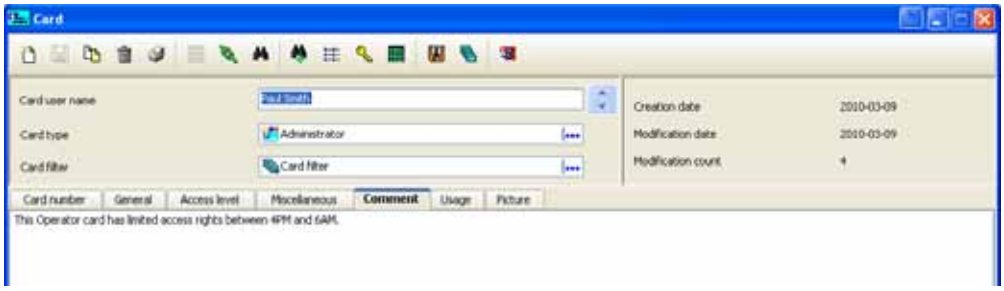
ПРИМЕЧАНИЕ: *Если данная карта предназначается для человека с ограниченными возможностями, необходимо выделить флажком опцию **Extended door access delay** (Увеличенное время доступа). Чтобы эта функция действовала, необходимо задать соответствующие задержки в меню Door (Двери). Эта функция также доступна при описании карт посетителей (Visitor card).*

7 Установите уровень ревизора (**Supervisor level)** в соответствии с привелегиями пользователей.

ПРИМЕЧАНИЕ: *Если требуется, то выберите опцию **Privileged operation** (привелигированное управление) для того, чтобы пеекрывать любые охранные настройки в отношении дверей.*

Добавление комментариев к карте

1 В окне Card (Карты) открыть закладку **Comment** (Комментарии).



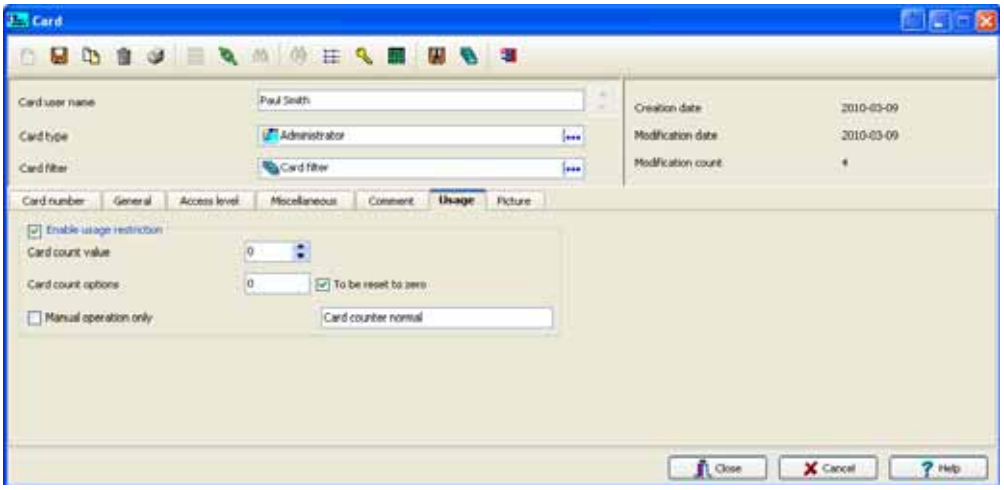
2 При необходимости ввести комментарий о владельце карты. Это поле служит для хранения в базе данных дополнительных сведений. Максимальная допустимая длина – 241 символов.

3 Нажать **Save** (Сохранить) и затем **Close** (Закрыть).

Ограничение числа использований карты

Система EntraPass позволяет установить счетчик использований карты, тем самым ограничить число использований карты.

1 В окне Card (Карты) открыть закладку **Usage** (Использование).



2 Выделить флажком опцию **Enable usage restriction** (Ограничить использование), чтобы ограничить число использований карты.

3 В списке **Card count value** (Число использований карты) выбрать максимальное допустимое число использований карты. Для ввода числа можно воспользоваться кнопками со стрелками вверх-вниз.

После указания максимального числа использований в поле Card count value, значение, отображаемое в поле Card count options, автоматически увеличивается при каждом использовании карты. После определённого числа использований оператор может отметить флажком поле Reset to zero (Обнулить), чтобы после достижения максимального значения сбросить на нуль показания счётчика.

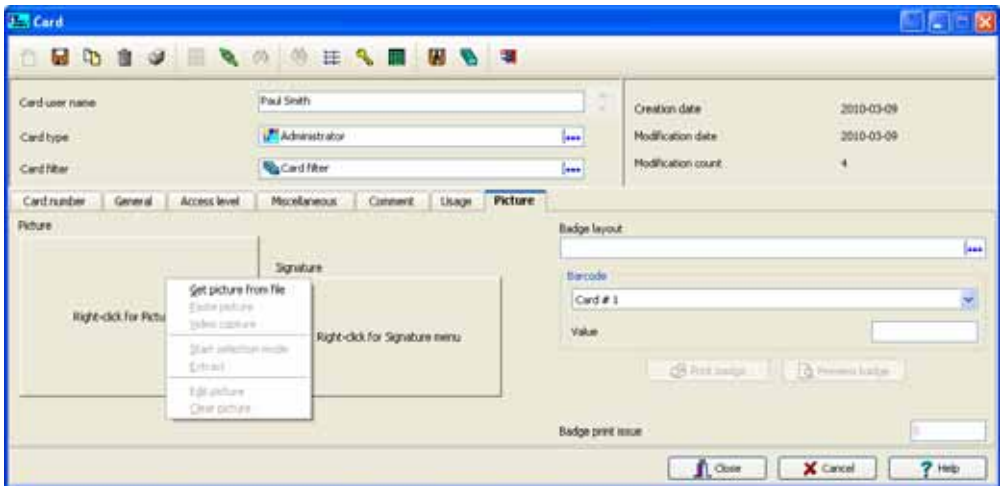
ПРИМЕЧАНИЕ:

Привязка фотографий и подписей к картам

Система даёт возможность создавать связи между фотографиями с подписями и владельцами карт, а также использовать шаблоны для создания карт и печати электронных пропусков. Фотографии и подписи можно извлекать из файлов, вставлять из буфера или оцифровывать при помощи соответствующих средств обработки изображений. Для оцифровки видеоизображений подходят любые устройства, совместимые с драйверами MCI или TWAIN. Для оцифровки подписей рекомендуется использовать такие устройства ввода подписей как Topaz, Penware TTI500 и Penware TT3100.

Назначение фотографии из файла

1 В меню Card (Карты) открыть закладку **Picture** (Изображения).



ПРИМЕЧАНИЕ: *Опция автоматического захвата изображения включена при условии, когда данное устройство установлено.*

2 Щёлкнуть по изображению правой кнопкой мыши. В открывшемся контекстном меню выбрать одно из действий:

- **Get picture from file** (Извлечь изображение из файла) – выбрать сохранённое в файл изображение.
  1 В выпадающем списке **Files of type** (Тип файлов) указать тип искомого файла или оставить в этом поле надпись **All** (Все), чтобы на экране отображались все графические файлы. Чтобы использовать предварительный просмотр, следует выделить флажком опцию **Auto displayer** (Автоматически отображать на экране).
  2 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.

ПРИМЕЧАНИЕ: *Поддерживаются следующие форматы файлов: BMP, EMF, WMF, JPG, GIF, PNG, PCD и TIF.*

- Paste picture (Вставить изображение из буфера) – для использования этой опции следует скопировать изображение в буфер и затем вставить его в это окно.

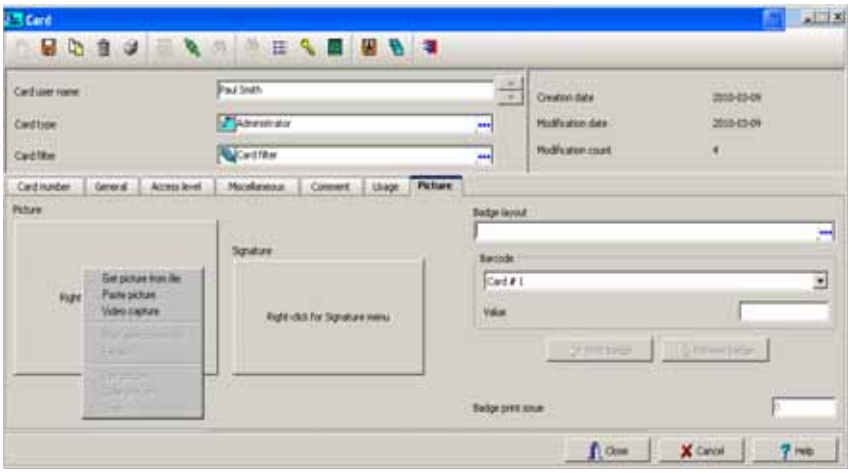
ПРИМЕЧАНИЕ: *Чтобы удалить импортированное изображение, следует щёлкнуть по нему правой кнопкой мыши, и выбрать в контекстном меню команду **Clear picture** (Удалить изображение).*

Получение фотографии с видеокамеры

Функция оцифровки изображений доступна только при условии, что в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > закладка **Video** выделена опция **Enable video capture** (Разрешить оцифровку изображений).

ПРИМЕЧАНИЕ: *Перед оцифровкой изображений, полученных с видеокамеры необходимо правильно настроить всё оборудование. Более подробные сведения приведены в руководстве. При наличии двух и более драйверов видео следует указать, какой драйвер использовать (**Options** > **Multimedia devices** > закладка **Video**).*

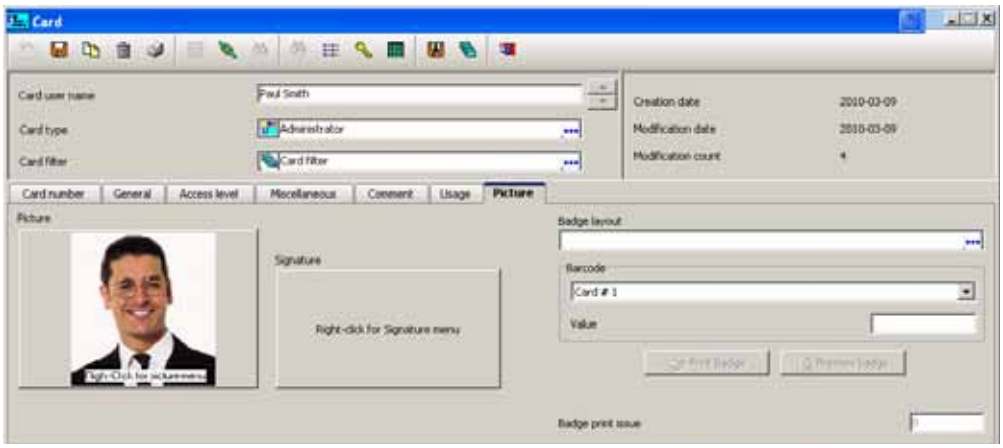
1 Щёлкнуть по изображению правой кнопкой мыши.



2 В контекстном меню выбрать функцию **Video capture** (Оцифровка изображения). Эта функция доступна только при условии, что в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > закладка **Video** выделена опция Enable video capture (Разрешить оцифровку изображений).

ПРИМЕЧАНИЕ: *В зависимости от системы оцифровки изображений могут быть доступны разные опции. При наличии двух и более драйверов видео, вам следует указать, какой драйвер нужно использовать. Смотрите в Главе 14 Конфигурация мультимедийных устройств' на странице 477 для более подробной информации по настройке драйверов захвата видео.*

3 Нажать кнопку **Freeze** (Остановить) на понравившемся изображении, затем нажать кнопку **Capture** (Захватить), чтобы вставить и сохранить изображение на экране.



4 Для указанной карты выбрать макет электронного пропуска из списка **Badge layout** (Макет электронного пропуска). *Смотрите пункт "Создание электронных пропусков" на странице 304 для более подробной информации* по описанию макета смотрите.

ПРИМЕЧАНИЕ: *Кнопки **Print badge** (Печать) и **Preview badge** (Предварительный просмотр) становятся активными только после выбора принтера и макета для изготовления электронного пропуска и выделения флажком опции Use badge printer (Использовать принтер для электронных пропусков): меню **Options > Printer > Badge printer**. Если эти кнопки активны, то доступен предварительный просмотр и печать электронного пропуска для владельца карты.*

Импортирование подписи из файла

В карту можно вставить подпись, а также импортировать другие изображения (например, логотипы или рисунки).

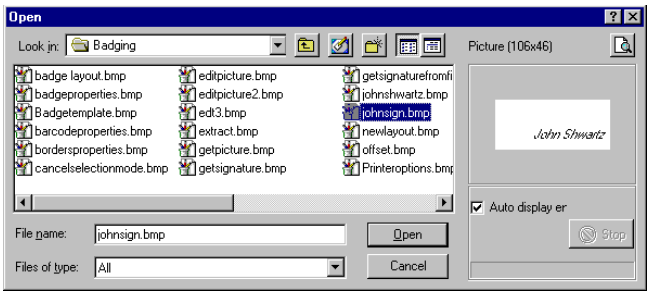
1 В меню Card (Карты) щёлкнуть по области подписи правой кнопкой мыши. Откроется контекстное меню.

2 В контекстном меню выбрать одну из следующих опций:

- **Get signature from file** (Извлечь подпись из файла) – выбрать сохранённую в файл подпись.

- **Paste signature** (Вставить подпись из буфера) – позволяет вставить подпись, которую до этого скопировали в буфер. Опция доступна при наличии содержимого в буфере.

***ПРИМЕЧАНИЕ: Устройство ввода подписей** становится доступным только после того, как в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > **Signature** (Подпись) будет указано использовать соответствующее устройство.*



3 Выбрать файл с подписью, нажать **Open** (Открыть)

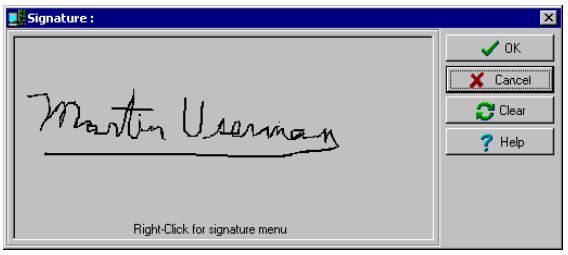
Добавление подписи с помощью устройства оцифровки подписей

Чтобы воспользоваться этой функцией, необходимо установить и правильно настроить устройство оцифровки подписей. Устройство ввода подписей становится доступным только после того, как в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > **Signature** (Подпись) будет указано использовать соответствующее устройство.

1 В меню Card (Карты) щёлкнуть по области подписи правой кнопкой мыши. Откроется контекстное меню.

2 В контекстном меню выбрать функцию **Signature pad** (Устройство ввода подписей). В открывшемся окне Signature (Подпись) можно будет предварительно просматривать подписи.

3 Нажать **OK**, чтобы вставить подпись в окно карты.



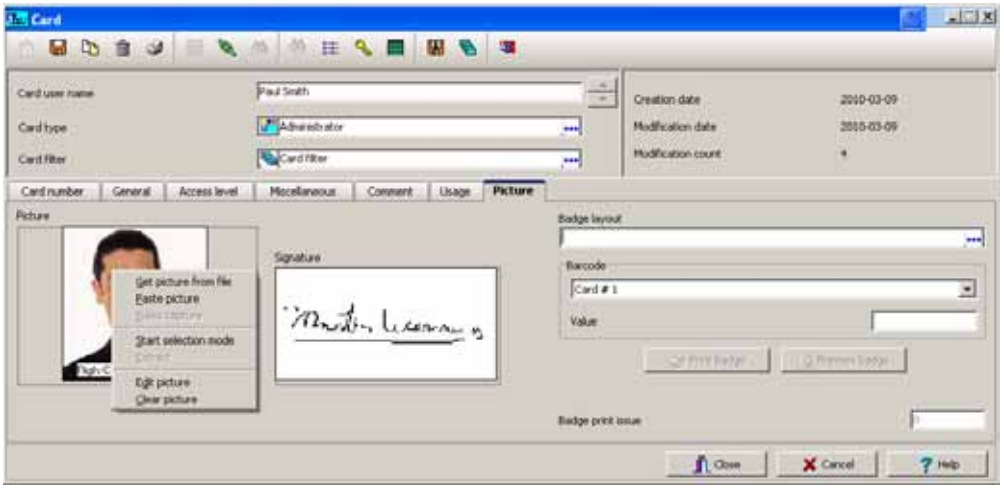
Работа с фотографиями и подписями

Встроенная функция изготовления электронных пропусков EntraPass Integrated Badging позволяет извлекать часть изображения или улучшать изображения, предназначенные для оформления идентификационных карт.

Извлечение части изображения

Если для оформления идентификационной карты пользователя требуется обрезать изображение (фотографию или подпись), содержащее избыточную информацию, и оставить только важные детали, то это можно сделать при помощи функции Extract.

1 Щёлкнуть правой кнопкой мыши по только что вставленному изображению.

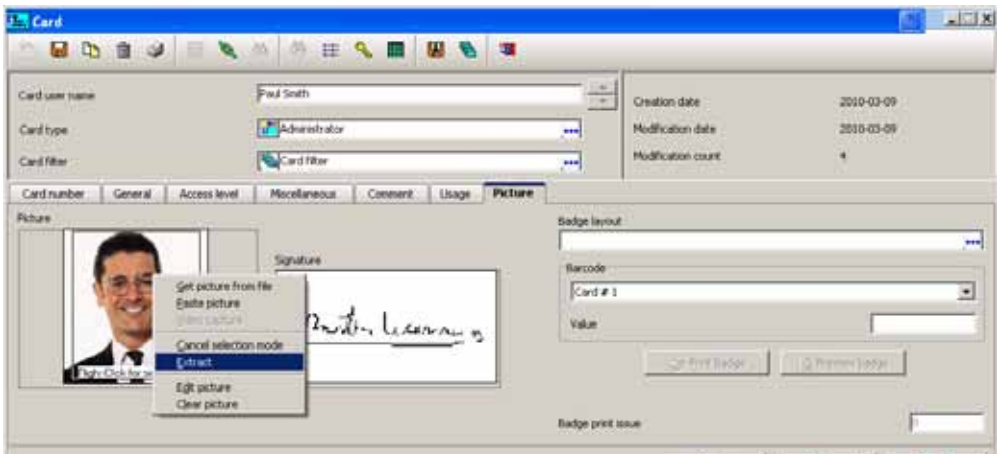


ПРИМЕЧАНИЕ: *Функция* ***Extract*** *(Извлечь) доступна сразу после перехода в режим выделения изображения (функция* **Start selection mode***). Аналогично, функция* ***Undo*** *(Вернуться назад) доступна только сразу после вставки изображения.*

2 Выбрать в контекстном меню пункт **Start selection mode** (включить режим выделения).

ПРИМЕЧАНИЕ: *Границы окна выделения можно растягивать за стороны и углы до нужных размеров. Кроме того, можно передвигать его в разные стороны.*

3 После выделения нужной части изображения снова щёлкнуть правой кнопкой мыши, чтобы вставить выделенную часть в идентификационную карту. Откроется контекстное меню.

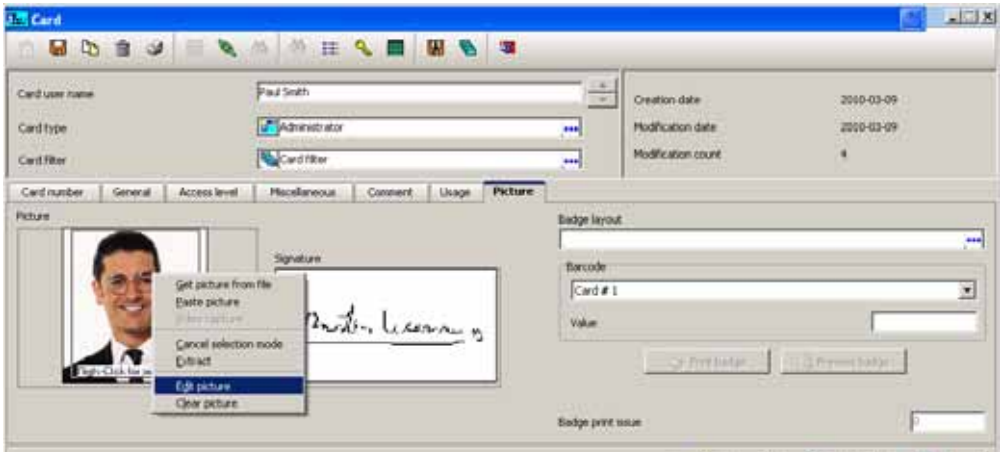


ПРИМЕЧАНИЕ: *Чтобы отменить выделение, нажать на правую кнопку мыши и выбрать в контекстном меню пункт* ***Cancel selection mode*** *(Отменить режим выделения). Выбрать пункт* ***Undo*** *(Вернуться назад) для отмены изменений. Функция* ***Undo*** *доступна только после вставки изображения.*

4 В контекстном меню выбрать функцию **Extract** (Извлечь).

Редактирование фотографии/подписи

1 Правой кнопкой мыши щёлкнуть по изображению, которое необходимо отредактировать.



ПРИМЕЧАНИЕ: *В поле* ***Barcode*** *(Штрихкод) необходимо ввести код электронного пропуска для выполнения идентификации. В выпадающем списке выделить любое значение, которое будет использоваться в качестве штрихкода. Или выделить флажком поле* ***Custom*** *(Собственные настройки) и в ставшем доступным поле* ***Value*** *(Значение) ввести собственное значение штрихкода. Если оператор не укажет собственное значение штрихкода, по умолчанию будет использован номер карты (****Card number****).*

2 В контекстном меню выбрать пункт **Edit picture or signature** (Редактировать фотографию или подпись).).

3 Настроить параметры изображения при помощи отображаемых кнопок и рычажков настройки. Функция **Reset all** (Сброс всех настроек) служит для возврата к первоначальным настройкам изображения.

- **Auto contrast** (Автоматическая настройка контраста). Эта функция позволяет улучшить контраст путём увеличения яркости светлых и тёмных точек изображения: тёмное становится темнее, а светлое ярче. Как правило, автонастройка контраста показывает хорошие результаты при необходимости немного улучшить контраст изображения простой регулировкой контраста.
- **Sharpen** (Резкость) – улучшает расплывчатое изображение, увеличивая резкость по краям.
- **Brightness** (Яркость) – эта функция позволяет осветлить изображение.
- **Reset all** (Сбросить все настройки) - используется для отмены всех изменений и возврата к первоначальному изображению.

4 Нажать **OK**, чтобы закрыть окно редактирования **Picture**.

5 Выбрать макет электронного пропуска из списка Badge layout (Макет электронного пропуска). *Смотрите пункт "Создание электронных пропусков" на странице 304 для более подробной информации по созданию макета*.

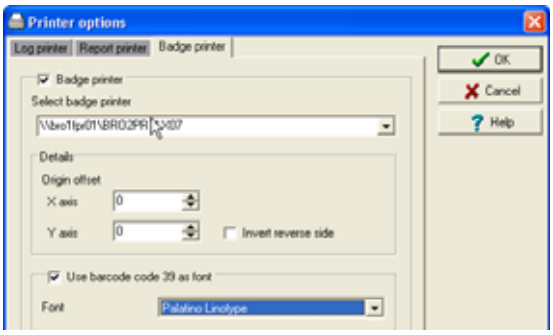
Печать электронных пропусков

Чтобы вывести на печать электронные пропуска, **карты посетителей** и **разовые пропуска,** можно воспользоваться меню **Card** (Карты), а также любыми окнами предварительного просмотра электронных пропусков (**Badge preview**). Программное обеспечение позволяет печатать как односторонние, так и двухсторонние пропуска. Перед выводом на печать следует выбрать принтер для электронных пропусков. Им может служить любой сетевой принтер или специальный принтер для изготовления электронных пропусков.

Выбор принтера для печати электронных пропусков

1 В окне EntraPass Workstation (Рабочая станция EntraPass) выбрать закладку **Options** (Опции) и на панели инструментов нажать кнопку **Printer Option** (Опции принтера).

2 В окне Printer option выбрать закладку **Badge printer** (Принтер электронных пропусков



ПРИМЕЧАНИЕ: *Для печати электронных пропусков может использоваться любой сетевой принтер. Но для печати пропусков на специальных карточках следует использовать специальный принтер электронных пропусков.*

3 Чтобы указать системе, что используется принтер электронных пропусков, следует выделить опцию **Badge printer** (Принтер электронных пропусков). Если в этом поле поставлен флажок, то в окнах Card (Карты), Visitor (Посетители) и Daypass (Разовые пропуска) появляются функции Print badge (Печать пропусков) и Preview badge (Предварительный просмотр пропусков).

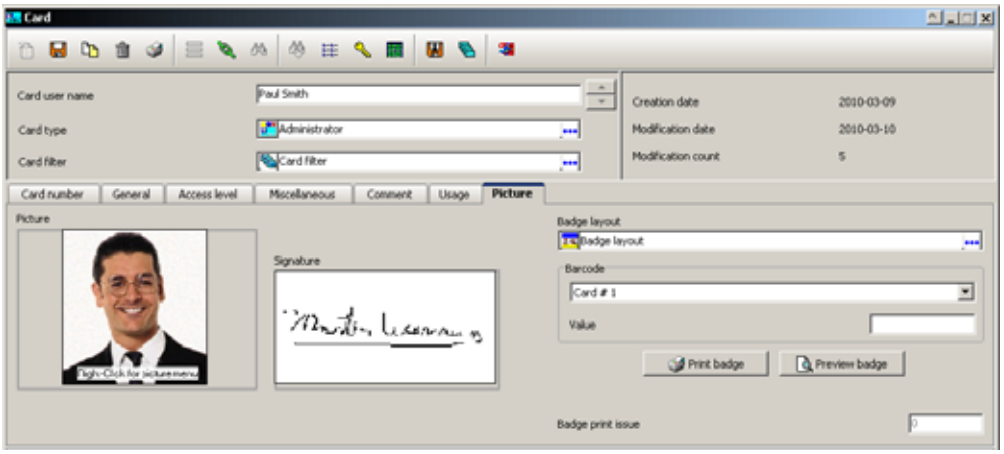
4 В выпадающем списке **Select badge printer** (Выбор принтера электронных пропусков) выбрать принтер, который будет для этого использоваться.

5 Настроить границы печати:
- Origin offset, X axis (Смещение от первоначальной точки, ось X) – указывает левую границу.
- Y axis (Ось Y) – указывает верхнюю границу.

Предварительный просмотр и печать электронных пропусков

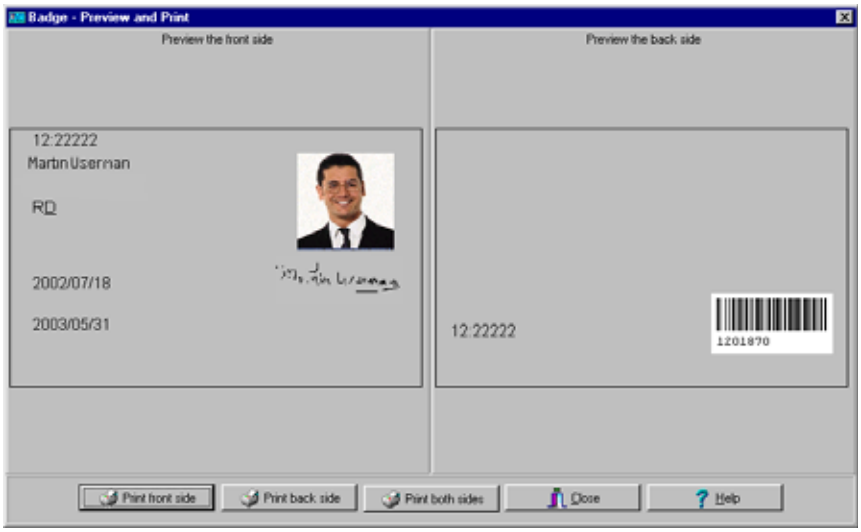
Окно **Badge - Preview and Print** (Электронные пропуска – Предварительный просмотр и печать) служит для предварительного просмотра макета электронного пропуска с заданными параметрами карты (если макет пропуска прикреплён к идентификационной карте) или с настройками по умолчанию (если макет ещё не прикреплён к конкретной карте). Программное обеспечение позволяет печатать как односторонние, так и двухсторонние пропуска.

1 В окне Card (Карты), Visitor (Посетители) или Daypass (Разовые пропуска) нажать кнопку **Preview badge** (Предварительный просмотр пропусков).



ПРИМЕЧАНИЕ: *Пока электронный пропуск не прикреплён к какой-либо идентификационной карте, в окне предварительного просмотра (**Badge design** (Создание пропуска) > **Layout** (Макет) > **Preview** (Предварительный просмотр)) отображается пропуск с настройками по умолчанию.*

2 В окне **Badge - Preview and Printing** выбрать режим печати:



- **Print front side** (Печатать лицевую сторону) – печать только лицевой стороны (изображена слева).
- **Print back side** (Печатать оборотную сторону) – печать только оборотной стороны (изображена справа). Эта кнопка активна только в том случае, если в настройках указано, что пропуск двухсторонний.
- **Print both sides** (Печатать обе стороны) – печать лицевой и оборотной стороны. Эта кнопка активна только в том случае, если в настройках указано, что пропуск двухсторонний.

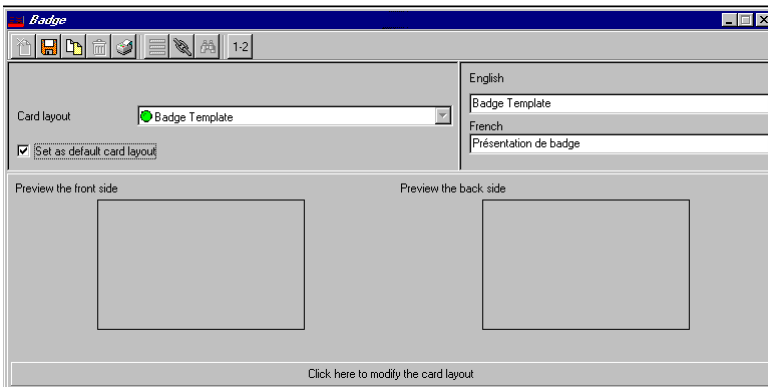
ПРИМЕЧАНИЕ: ВАЖНО! *Для того чтобы печатать электронные пропуска со штрихкодами, принтер должен быть правильно настроен. Для этого должна быть выбрана опция “black resin” (истинно чёрный цвет), иначе считыватели штрихкодов не смогут правильно определять их. При возникновении проблем с печатью или считыванием штрихкодов рекомендуется обратиться к руководству принтера.*

Создание электронных пропусков

В программное обеспечение EntraPass входит редактор макетов электронных пропусков, позволяющий создавать, сохранять, редактировать и удалять шаблоны электронных пропусков, чтобы затем привязать их к идентификационным картам и использовать для печати электронных пропусков. Таким образом, предусмотрена возможность создания и редактирования шаблонов электронных пропусков, добавление фона определённого цвета или в виде графического изображения, вставка логотипов, текста, штрихкодов, а также фотографий или подписи владельцев карт.

Создание шаблона электронного пропуска

1 В меню Users (Пользователи) нажать на иконку **Badge** (Электронные пропуска). Откроется окно Badge.

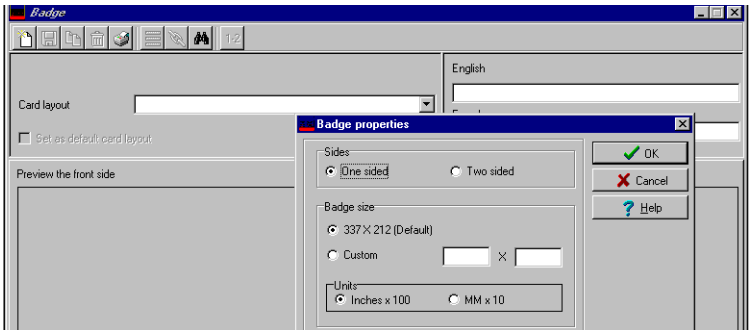


ПРИМЕЧАНИЕ: *Окно Badge содержит все инструменты, доступные в других окнах системы EntraPass: New (Создать), Save (Сохранить), Copy (Копировать), Delete (Удалить), Print (Печать), Links (Связи), Search (Поиск) (кнопка Hierarchy (иерархия) недоступна). Зато в этом окне есть дополнительная кнопка "1-2", которая позволяет изменять число сторон в макете пропуска.*

2 Нажать на панели инструментов кнопку **New** (Создать). Откроется окно Badge properties (Свойства электронных пропусков).

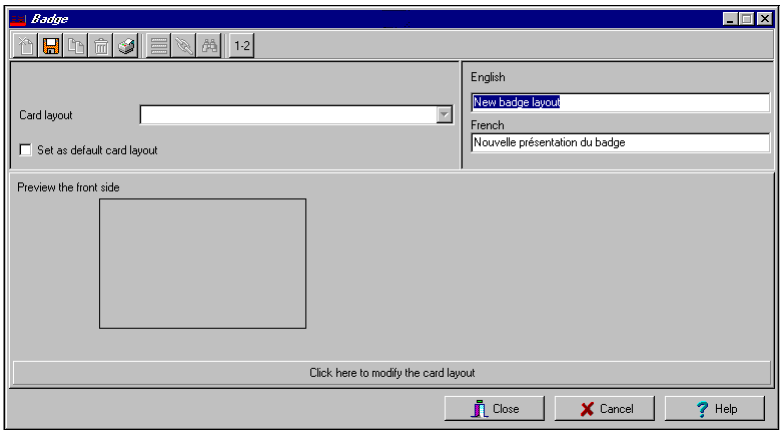
Описание свойств для макета электронных пропусков

1 В окне Badge properties (Свойства электронных пропусков) указать число сторон пропуска в поле Sides, затем выбрать размеры макета в поле Badge size (Размеры пропуска) и нажать **OK**.



2 Указать число сторон пропуска в поле Sides, затем выбрать размеры макета в поле Badge size (Размеры пропуска) и нажать **OK**.

ПРИМЕЧАНИЕ: *Размеры указываются в дюймах или в миллиметрах (сотые доли дюйма или десятые доли миллиметра). Чтобы изменить единицы измерения, следует отметить флажком соответствующую кнопку (inch – дюймы, MM – миллиметры) в поле Units (Единицы измерения).*



3 Назначить имена для шаблона пропусков в соответствующих полях для каждого применяемого языка. Допускается ввод имени длиной до 40 символов.

4 Поле **Set as default card layout** (Выбрать как макет по умолчанию) можно отметить флажком, если необходимо использовать этот новый макет для всех новых пропусков.

ПРИМЕЧАНИЕ: *Доступен только один макет по умолчанию. После выбора одного макета и выделения опции* ***Set as default card layout*** *(Выбрать как макет по умолчанию) текущий макет по умолчанию будет заменён новым.*

5 Нажать **Save** (Сохранить) для сохранения этого шаблона пропусков.

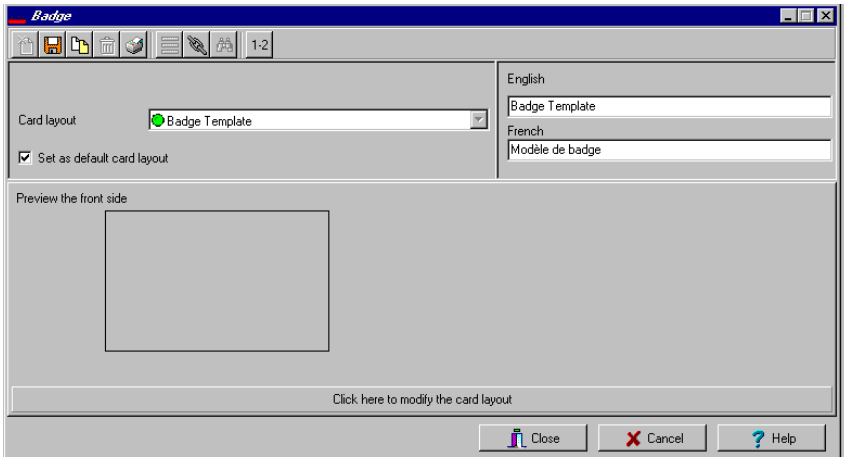
Редактирование макета пропусков

Утилита создания электронных пропусков (Badge Design) позволяет редактировать макет пропусков, делать цветной фон или использовать в качестве фона графическое изображение, изменять шрифты и пр.

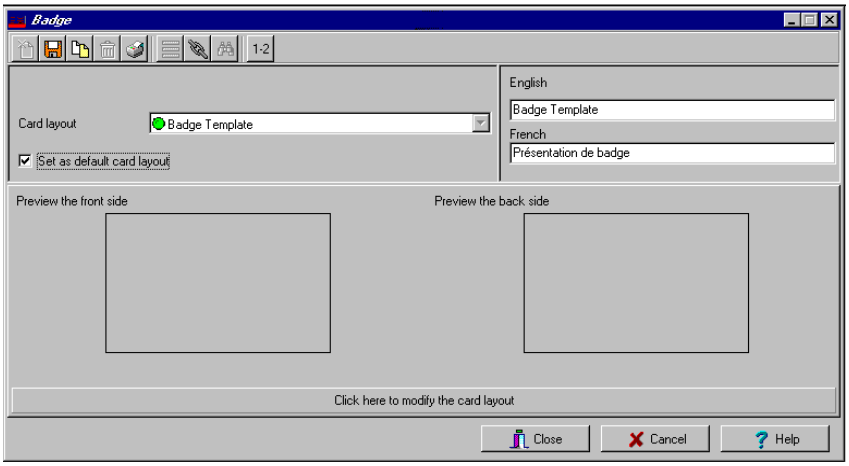
ПРИМЕЧАНИЕ: *После создания макета невозможно изменить его размеры, можно только создать новый макет. А число сторон изменять можно – следует нажать иконку* ***Sides*** *на панели инструментов окна Badge.*

Изменение числа сторон идентификационных карт

1 В окне Badge выбрать, какой электронный пропуск необходимо отредактировать.



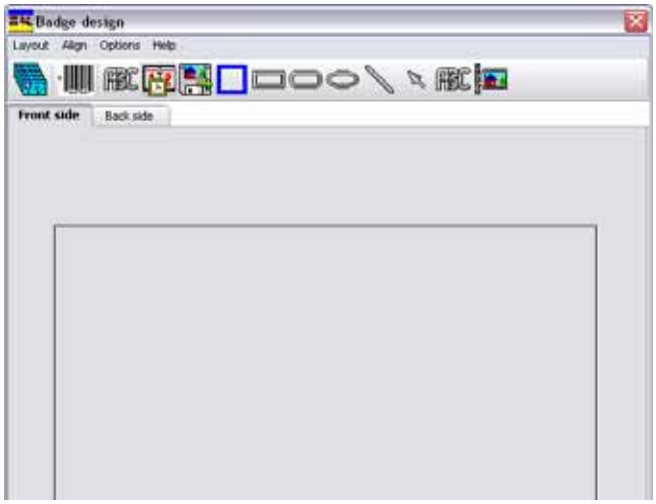
2 В инструментах окна Badge нажать кнопку "1-2".



3 Нажать **Save** (Сохранить) для сохранения новых данных.

Изменение цвета фона

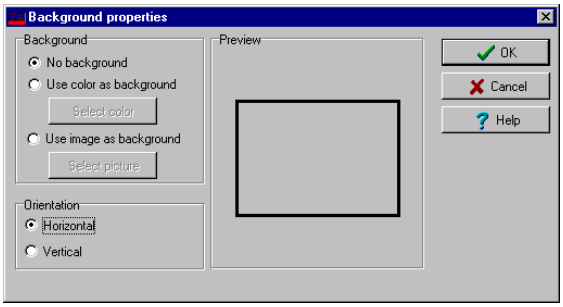
1 В окне Badge выбрать, какой электронный пропуск необходимо отредактировать.
2 Нажать кнопку **Click here to modify the card layout** (Нажать для изменения макета карты), чтобы открыть окно Badge design (Создание пропуска). Это большая кнопка внизу



ПРИМЕЧАНИЕ: *При установке курсора поверх объектов окна Badge Design (Создание пропуска) на экране появляется подсказка-пояснение к каждому объекту.*

3 Чтобы изменить цветовой фон шаблона, следует нажать на правую кнопку мыши в любом месте рабочего окна. Откроется контекстное меню **Properties** (Свойства).

4 Нажать кнопку **Properties**. Откроется окно Background properties (Свойства фона).



5 Выделить те опции шаблона, которые необходимо использовать:
- **No background** (Фон не использовать) – значение по умолчанию
- **Use color as background** (Использовать цветовой фон как задний фон) – служит для применения цветового фона ко всем разработкам.
- **Use image as background** (Использовать изображение как задний фон). Эта функция позволяет вставить картинку, которая будет отображаться на всех пропусках как фоновое изображение.
- **Orientation** (Ориентация) – служит для выбора ориентации: landscape (горизонтальная, альбомного типа) или portrait (вертикальная, портретная).

Добавление объектов в макет пропусков

Технология нажатия и перетаскивания объекта мышью позволяет объединять необходимые объекты в шаблон пропусков:

- данные в полях карты,
- штрихкоды,
- текстовые окна,
- текущая дата,
- Ранее сохранённые изображения и логотипы (формата BMP, JPG, GIF и др.),
- рамки,
- геометрические фигуры (прямоугольник, прямоугольник с закруглёнными углами, эллипс),
- линии, в том числе указатели со стрелками.

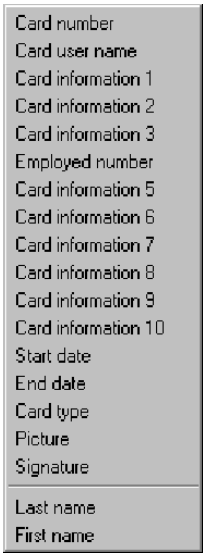
ПРИМЕЧАНИЕ: *При вставке объектов используются их настройки по умолчанию. Чтобы изменить свойства объекта, следует щёлкнуть по нему правой кнопкой мыши, и выбрать соответствующие настройки в контекстном меню.*

Вставка информационных полей карты

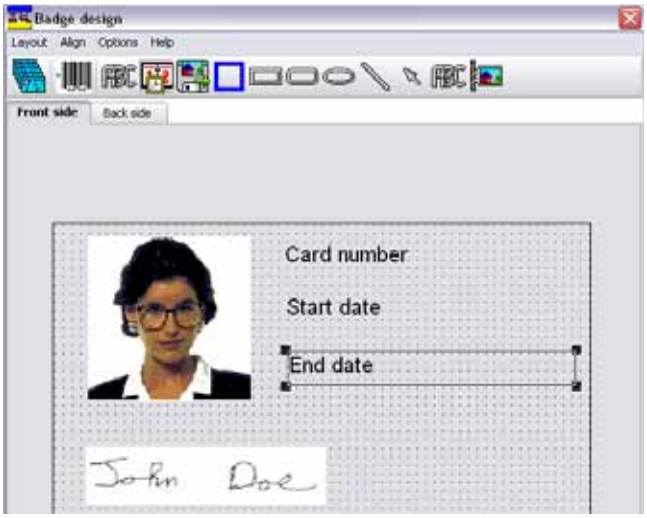
1 Чтобы добавить в шаблон электронных пропусков информационные поля карты, следует нажать на иконку **Card fields** (Поля карты). Откроется окно **Card fields.**

2 Для того чтобы изменить свойства объекта до перетаскивания его в рабочее окно, следует открыть закладку **Options** (Опции) в окне Badge Design (Создание пропуска) и выбрать пункт **Show properties on drop** (Показывать свойства при перетаскивании). В таком случае окно Properties будет открываться при каждом перетаскивании объекта в рабочую зону шаблона.

ПРИМЕЧАНИЕ: *Чтобы в окне Badge Design (Создание пропуска) была возможность выбора имени и фамилии владельца из меню Card fields (Поля карты), следует перейти в меню* ***Options*** *(Опции), открыть* ***System parameters*** *(Системные параметры), выбрать закладку* ***User name format*** *(Формат имени пользователя), поставить флажок в поле* ***Parse user name*** *(Разбор Ф.И.О. пользователя) и затем указать, по какому критерию должна выполняться сортировка имён пользователей: по имени (First name) или по фамилии (Last name). Смотрите в Главе 14 Формат имени пользователя' на странице 491 для более подробной информации относительного этого запроса.*



3 В контекстном меню выбрать информационное поле карты, которое необходимо добавить в макет шаблона, затем щёлкнуть в рабочей области шаблона, чтобы вставить это поле в шаблон.



ПРИМЕЧАНИЕ: *При добавлении фотографии в шаблон электронного пропуска вместо фотографии отображается только поле для подстановки фото. Таким образом указывается место, где будет размещена фотография. После того как пропуск будет прикреплён к карте, на экране появится фото владельца карты.*

Выравнивание объектов в макете шаблона

Выровнять объекты в макете шаблона электронных пропусков поможет сетка. Её можно использовать как визуальную помощь при размещении объектов.

Для облегчения работы по выравниванию объектов в шаблоне пропусков предусмотрено три опции:

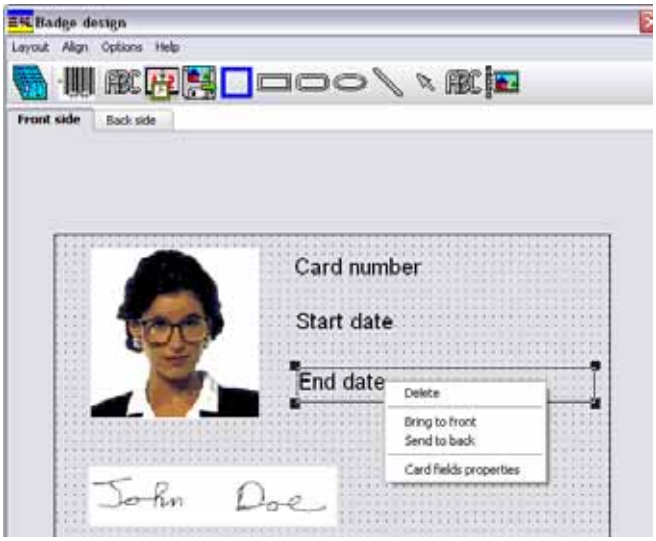
- **Show gridlines** (Показывать линии сетки) – показывать точки сетки для облегчения выравнивания объектов.
- **Align to grid** (Выравнивать по сетке) – эту опцию следует активировать до начала создания шаблона. В таком случае при перетаскивании объектов в рабочую область шаблона они будут "прилипать" к ближайшей метке сетки.
- **Grid settings** (Параметры сетки) – установка размеров ячейки сетки по горизонтали (Width) и вертикали (Height) в пикселях.

ПРИМЕЧАНИЕ: *Чтобы убрать сетку, следует в меню **Align** (Выравнивать) убрать флажок напротив* **Show gridline** (выравнивать по сетке).

Изменение свойств информационных полей карты

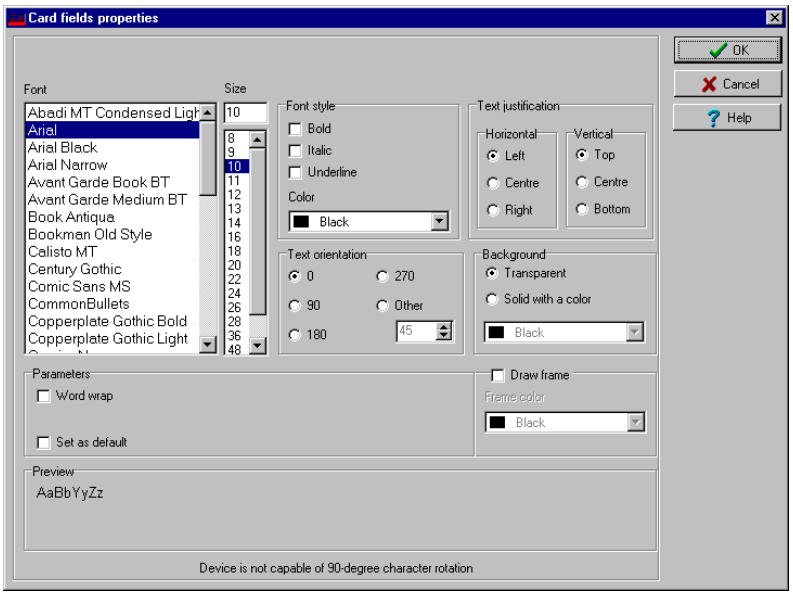
В шаблон объекты вставляются с установками по умолчанию (шрифт, цвет и т.п.). Позже эти настройки можно изменить. Например, можно изменить формат текстового блока (поля карты, статический текст, даты и т.п.).

1 В шаблоне пропусков щёлкнуть правой кнопкой мыши по вставленному объекту (например, по информационному полю карты).



2 В открывшемся контекстном меню выбрать пункт **Card fields properties** (Свойства полей карты).

ПРИМЕЧАНИЕ: *Содержание меню Properties зависит от типа выбранного объекта. Таким образом, свойства изображения будут отображаться в окне Image properties, а свойства даты в окне Current date properties.*



3 В окне Card fields properties доступны все функции форматирования текста:

- шрифт (имя, цвет, стиль (жирный, курсив, подчёркнутый)),
- фон (прозрачный или непрозрачный цветной),
- выравнивание (по горизонтали, по вертикали),
- ориентация,

- параметры (например, перенос слов на новую строку без разбивки).

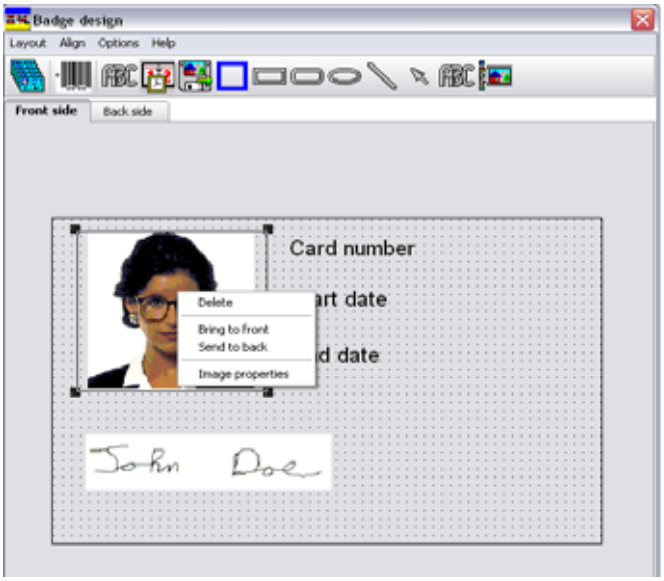
ПРИМЕЧАНИЕ: *Чтобы применить указанные настройки ко всем текстовым объектам шаблона, следует отметить флажком опцию* ***Set as default*** *(Установить в качестве настроек по умолчанию).*

ПРИМЕЧАНИЕ: *Если в поле Text Orientation (Ориентация текста) установлено “Other” (Другое), то размеры поля изменить невозможно.*

Изменение свойств изображений

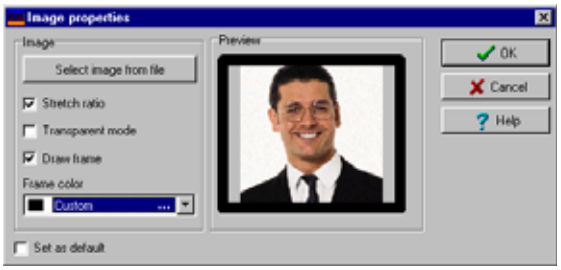
Речь пойдёт о любых изображениях, например, фотографиях, логотипах, подписях.

1 В рабочей области окна Badge design щёлкнуть правой кнопкой мыши на изображении (фотографии, логотипе, подписи), которое необходимо изменить.



2 В открывшемся контекстном меню выбрать пункт **Images properties** (Свойства изображений).

3 Здесь можно загрузить другое изображение из файла или изменить свойства того, которое отображается на экране в данный момент.



- **Stretch ratio** (Относительное растяжение) – позволяет разместить изображение в центре поля, сохраняя его оригинальные пропорции.
- **Transparent mode** (Прозрачный фон) – не использовать цветной фон,
- **Draw frame** (Нарисовать рамку) – обвести изображённый объект в рамку,
- **Frame color** (Цвет рамки) – опция доступна в случае выделения предыдущего пункта и служит для назначения цвета для рамки. В выпадающем списке можно указать любой цвет рамки по собственному выбору.

4 Чтобы назначить эти настройки для всех графических объектов шаблона пропусков, следует поставить флажок в поле **Set as default** (Установить в качестве настроек по умолчанию).

Добавление статических текстовых объектов

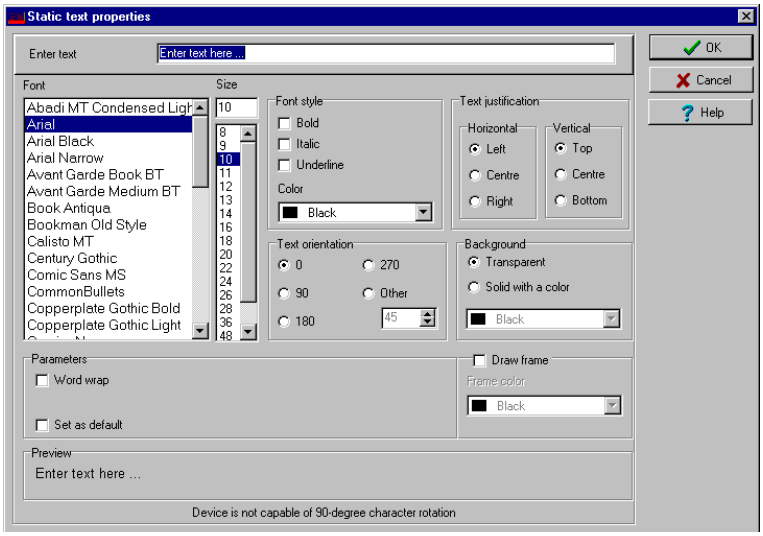
Чтобы добавить текстовый объект в шаблон пропусков, следует сначала перетащить в рабочую область текстовое окно, а потом ввести текст в окне Text properties (Свойства текста). Это же окно Text properties служит и для форматирования текста.

1 В окне Badge Design (Создание пропуска) найти на панели инструментов иконку Text (Текст). Для изменения размеров текстового окна необходимо его выделить и перетащить крестики по углам

объекта (манипуляторы размера) в нужное положение. Таким образом можно изменить высоту и ширину текстового окна.

2 *Смотрите пункт "Выравнивание объектов в макете шаблона" на странице 309 для более подробной информации* по выравниванию текстовых объектов.

3 Чтобы добавить текст в текстовое окно, следует щёлкнуть по нему правой кнопкой мыши и выбрать в открывшемся контекстном меню пункт **Static text properties** (Свойства статического текста).



4 Ввести текст в поле **Enter text** (Введите текст); затем изменить свойства текста, если требуется. В окне предварительного просмотра (Preview) можно увидеть результаты внесённых изменений.

Добавление штрихкодов

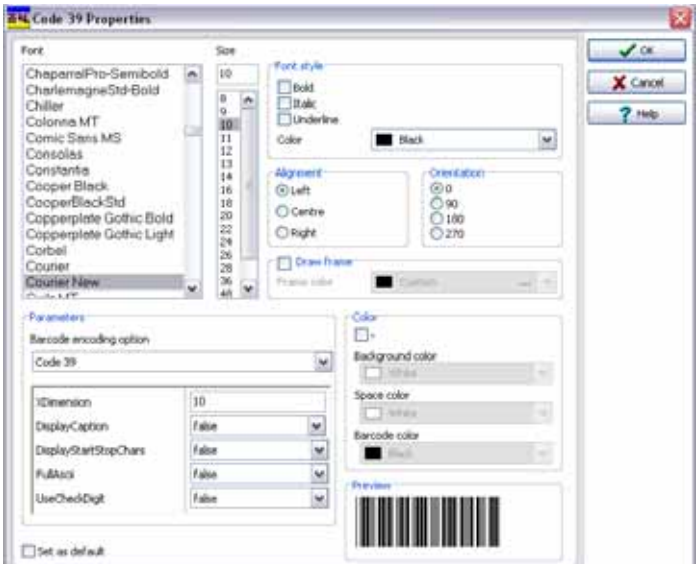
Программные средства для создания электронных пропусков позволяют размещать на пропусках штрихкоды. По умолчанию значение штрихкода совпадает с номером карты, если не указано иное.

1 В окне Badge Design (Создание пропуска) нажать на иконку **Barcode** (Штрихкоды), затем щёлкнуть по рабочей области окна Badge design.

2 *Смотрите пункт "Выравнивание объектов в макете шаблона" на странице 309 для более подробной информации* для выравнивания объекта со штрихкодом

Изменение свойств штрихкодов

1 В окне Badge design (Создание пропуска) щёлкнуть правой кнопкой мыши по штрихкоду, чтобы открыть окно Barcode Properties (Свойства штрихкода).



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

2 В открывшемся окне указать свойства штрихкодов, которые будут размещены на электронных пропусках.

ПРИМЕЧАНИЕ: *Если в поле* ***Barcode encoding option*** *(Способ кодирования штрихкода) необходимо указать код "Code 39-Modulo 43", то в поле* ***Field Checksum*** *(Контрольная сумма поля) следует поставить значение "True".*

Добавление текущей даты

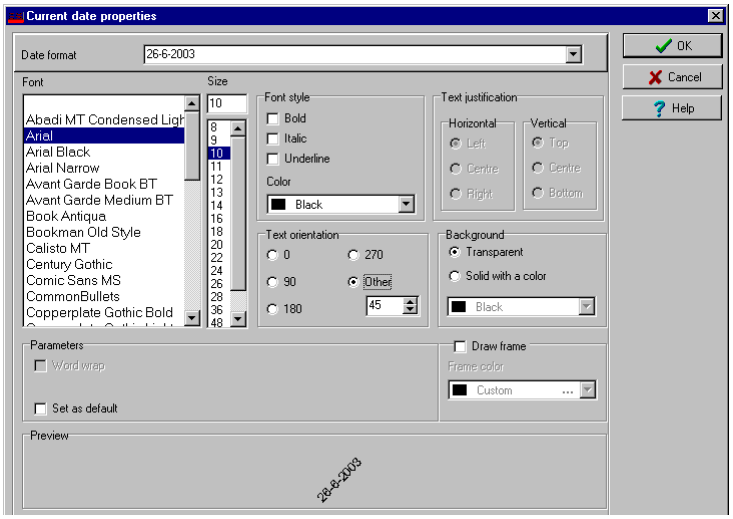
Добавление в шаблон текущей даты выполняется таким же образом, как и в случае с любым другим объектом, то есть путём выделения этого объекта на панели инструментов и вставкой его в рабочую область по щелчку мыши.

1 В окне обработки шаблона Badge Design (Создание пропуска) нажать на иконку **Current date** (Текущая дата), затем щёлкнуть мышью в рабочей области окна.

2 Щелчком правой кнопки мыши по отображаемой дате вызвать контекстное меню.

3 *Смотрите пункт "Выравнивание объектов в макете шаблона" на странице 309 для более подробной информации по выравниваю объекта.*

4 В контекстном меню выбрать пункт **Current date properties** (Свойства текущей даты).



5 В окне Current date properties (свойства текущей даты) доступны следующие функции:
- выбирать формат даты (верхнее поле).
- выбор свойств текста: шрифт, цвет, выравнивание, ориентация и др.

Добавление изображения

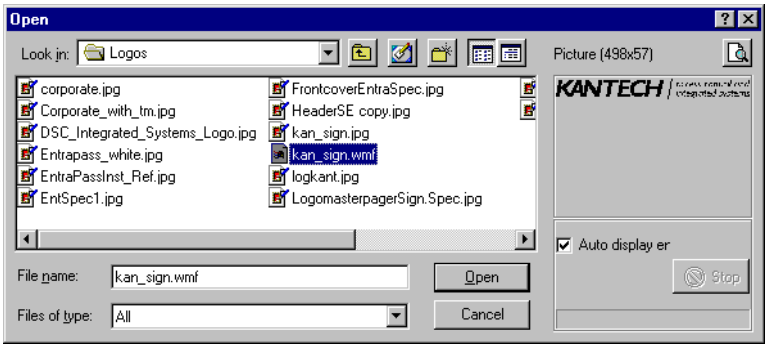
Фоновые изображения можно импортировать в шаблон из любого каталога. В макет электронных пропусков можно вставить изображения и фотографии, сканированные с цифровой камеры, а также иллюстрации, созданные в любой графической программе.

1 Для этого в окне Badge Design (Создание пропуска) следует нажать на иконку **Picture** (Изображение).

ПРИМЕЧАНИЕ: *Поддерживаются следующие форматы изображений: BMP, JPG, EMF, WMF, GIF, PNG, PCD и TIF.*

2 Вставьте изображение в рабочую область шаблона. Откроется окно Image properties (Свойства изображения).

3 Нажать на кнопку **Select image from file** (Вставить изображение из файла). В открывшемся окне Open (Открыть) выбрать файл с изображением.



Чтобы увеличить размер изображения в окне предварительного просмотра, нажать на кнопку Zoom (Масштаб).

4 Выделить нужное изображение, нажать кнопку **Open** (Открыть). Изображение появляется в рабочей области шаблона.

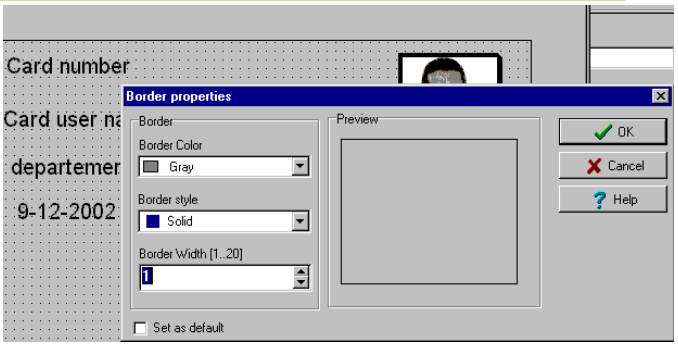
ПРИМЕЧАНИЕ: *При импортировании изображения его размеры необходимо изменить до первоначальных, как показано на иллюстрации.*

5 Используя манипуляторы размера (крестики в углах изображения) изменить размеры изображения, если необходимо, и переместить его в правую часть шаблона (при необходимости можно выровнять его по линиям сетки). *Смотрите пункт "Выравнивание объектов в макете шаблона" на странице 309 для более подробной информации .*

6 Для изменения свойств щёлкнуть по изображению правой кнопкой мыши. *Смотрите пункт "Изменение свойств изображений " на странице 311 для более подробной информации .*

Добавление других объектов

Добавление в шаблон рамки, геометрических форм (обычного и скруглённого прямоугольника, эллипса), линий (обычных и со стрелками) выполняется таким же образом, как и в случае с любым другим объектом, то есть путём выделения этого объекта на панели инструментов и вставкой его в рабочую область по щелчку мыши.

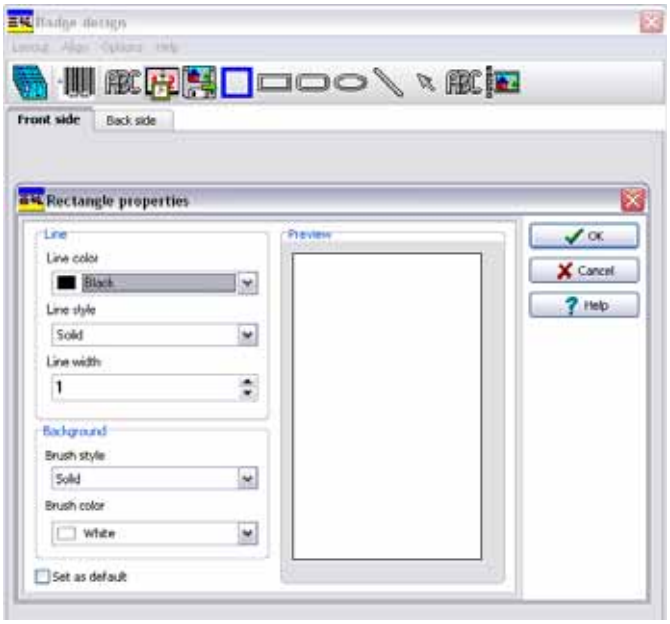


1 В окне Badge Design (Создание пропуска) выделить объект, который необходимо добавить (рядом с иконкой дискеты), затем щёлкнуть мышью в рабочей области окна. Откроется окно свойств Border properties (Свойства рамки).

2 Изменить цвет рамки в поле Border color, стиль в поле Border style и ширину в поле Border width. При желании можно установить эти настройки в качестве настроек по умолчанию, для этого следует отметить флажком опцию **Set as default**. Затем нажать **OK** для выхода из окна настройки.

Добавление геометрических форм

1 В окне Badge Design (Создание пропуска) выделить иконку прямоугольника (рядом с иконкой рамки) и щёлкнуть мышью в рабочей области окна.



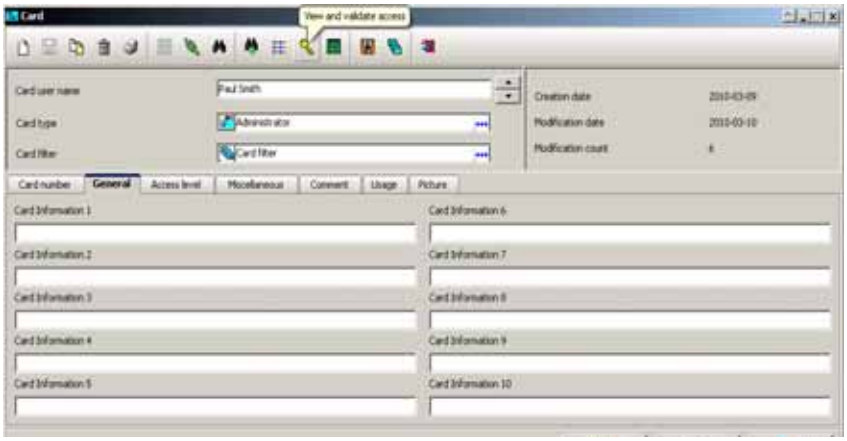
ПРИМЕЧАНИЕ: *Таким образом, можно вставлять в шаблон не только обычные, но и скруглённые прямоугольники, а также эллипсы.*

2 В окне Rectangle properties (Свойства прямоугольника) доступны следующие функции форматирования:
- Line color (Цвет линии),
- Line style (Стиль линии),
- Line width (Ширина линии),
- Background (Фон) – brush style (Стиль кисти) и brush color (Цвет кисти).

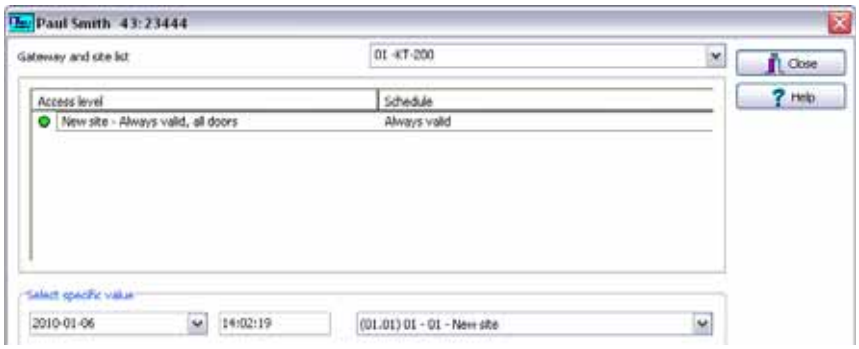
Проверка уровня доступа карты

Функция Validate card access (Проверка уровня доступа карты) служит для просмотра уровней доступа, назначенных указанному владельцу карты.

1 В окне Card (Карты) выбрать идентификационную карту.



2 На панели инструментов окна Card нажать на кнопку **View and Validate Access** (Просмотр и проверка доступа) – это иконка с ключом.



3 Выберите сайт/луч из списка **Gateway and site list** (Список лучей и шлюзов).

4 В разделе **Select specific value** (Выбор конкретных значений) указать дату (Date), время (Time) и дверь (Door), доступ к которой необходимо проверить. Система отображает уровни доступа к выбранной двери, а также расписания, связанные с этими уровнями доступа. В колонке **Access Level** (Уровни доступа) отображаются уровни доступа, назначенные для этой конкретной двери. В колонке **Schedule** (Расписания) отображается расписание, прикреплённое к указанному уровню доступа.

- **Красный** – указывает, что доступ к выбранной двери в указанное время и дату запрещён (нет допуска).
- **Зелёный** – указывает, что доступ к выбранной двери в указанное время и дату разрешён (есть допуск).

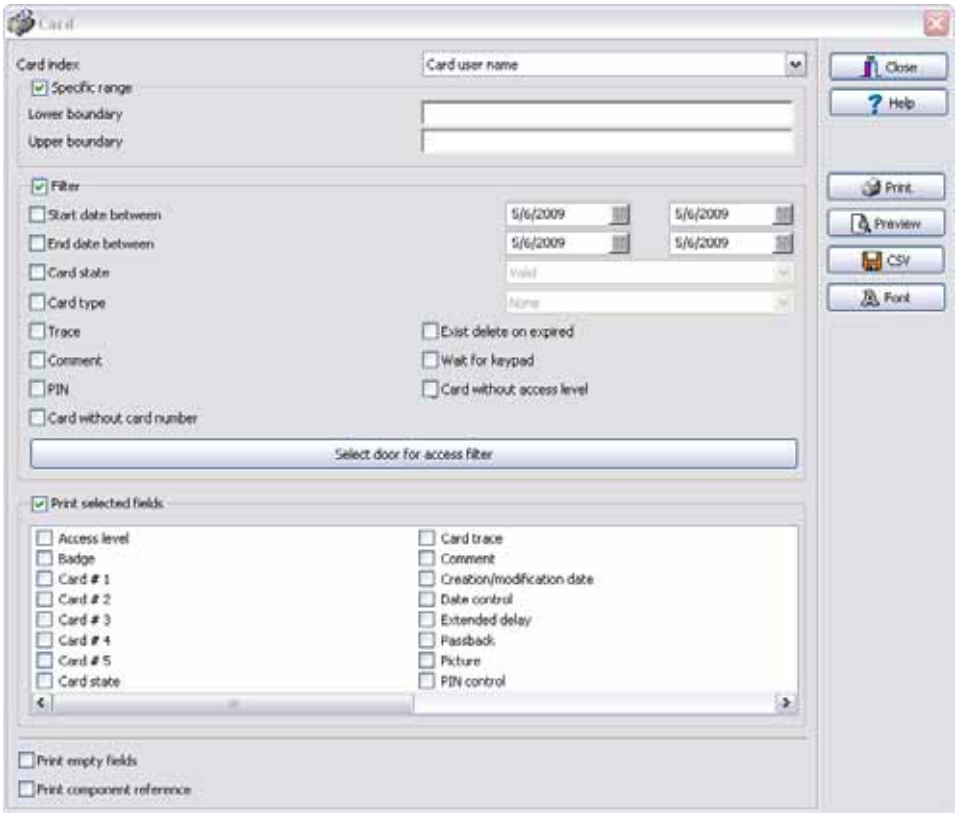
Печать идентификационных карт

Чтобы распечатать определённую группу карт, хранящихся в базе данных, следует воспользоваться функцией Print (Печать). Для уточнения списка карт предусмотрено несколько фильтров. Перед выводом на печать у оператора есть возможность просмотреть список и при необходимости изменить настройки (поля). Кроме того, с помощью кнопки **Font** (Шрифт) можно изменять тип и размер шрифта, если требуется.

ПРИМЕЧАНИЕ: *Имя владельца карты и номер карты будут отображаться всегда, независимо от настроек пользователя. По умолчанию на печать выводятся только те поля, которые содержат данные. Если ни одно поле не выделено, на печать будут выведены только те поля, в которых содержатся данные. Чтобы принтер печатал и пустые поля, следует поставить флажок в поле* ***Print empty fields*** *(Выводить на печать пустые поля).* Если вы хотите напечатать описание компонентов *(component references), выделите опцию* ***Print component references****.Чтобы просто предварительно просмотреть отчёты по картам, на компьютере должен быть установлен хотя бы один принтер.*

Печать карт

1 В окне Card (Карты) нажать кнопку **Printer** (Принтер).



ПРИМЕЧАНИЕ: *По умолчанию пустые поля не выводятся на печать. Чтобы принтер печатал и пустые поля, следует поставить флажок в поле* ***Print empty fields*** *(Выводить на печать пустые поля).*

2 В выпадающем списке **Card Index** (Индекс карты) выбрать критерий сортировки карт. Ими служат информационные поля карт.

3 Для печати карт с номерами из определённого диапазона следует отметить флажком опцию **Specific range** (Определённый диапазон). Указать информационное поле, по которому будет выполняться сортировка карт в списке. Например, если указать **Card number** (Номер карты), то карты в списке будут отсортированы по номерам в возрастающем порядке. Эта функция также может использоваться для задания определённого диапазона при помощи полей **Lower boundary** (Нижняя граница) и **Upper boundary** (Верхняя граница).

- Если требуется напечатать карты с номерами определённого диапазона, то в поле **Lower boundary** (Нижняя граница) необходимо указать начальный номер. Это поле всегда следует

заполнять вместе с полем **Upper boundary** (Верхняя граница). При этом обязательно должны быть указаны данные в поле Card index.

- Чтобы напечатать карты определённого диапазона, необходимо после ввода минимального значения в поле **Lower boundary** (Нижняя граница) указать максимальное значение в поле **Upper boundary** (Верхняя граница). Это поле всегда используется вместе с данными из поля Lower boundary и поля Card Index.

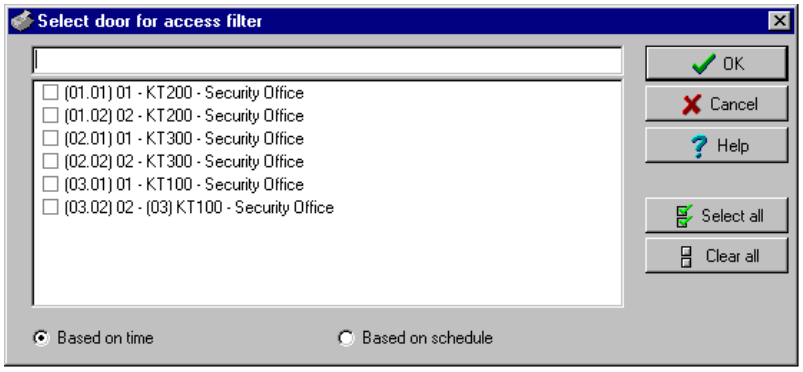
ПРИМЕЧАНИЕ: *Принтер будет печатать только те карты, которые удовлетворяют ВСЕМ критериям отбора. Например, если указано шесть критериев отбора, то карты должны удовлетворять всем шести критериям. Карты, не удовлетворяющие всем указанным критериям, не будут включены в список.*

4 Отметить опцию **Filter** (Фильтры), чтобы сузить область поиска карт. Использование фильтров помогает ограничить поиск и ускорить создание списка карт.

- **Start date between** (Начальная дата в диапазоне) – в список будут включены карты, дата создания которых находится в указанном диапазоне (закладка Miscellaneous (Прочее)).
- **End date between** (Конечная дата в диапазоне) – в список будут включены карты, срок окончания действия которых лежит в указанном диапазоне (закладка Miscellaneous).
- **Card state** (Статус карты) – поставив флажок в этом поле, следует указать необходимый статус. В список будут включены карты, статус которых совпадает с указанным (закладка Miscellaneous).
- **Card type** (Тип карты) – поставив флажок в этом поле, следует указать нужный тип карты. В список будут включены карты, тип которых совпадает с указанным (закладка Card (Карты)).
- **Exist trace** (С отслеживанием) – в список будут включены карты с активированной функцией “Card Trace” (Отслеживание использования карты) (окно Card, закладка Miscellaneous).
- **Exist comment** (С комментариями) – в список будут включены карты с комментариями (окно Card, закладка Comment).
- **Exist PIN** (С кодом) – в список будут включены карты, имеющие идентификационный код.
- **Exist delete when expired** (С удалением после окончания срока действия) – в список будут включены карты с отметкой в поле **Delete when expired** (окно Card, закладка Miscellaneous).
- **Exist wait for keypad** (С ожиданием нажатия клавиш) – в список будут включены карты с отметкой в поле **Wait for keypad** (окно Card, закладка Miscellaneous).

5 Если необходимо, отметить флажком поле **Print selected fields** (Выбрать поля для печати), чтобы печатать только указанные данные. Если отметить эту функцию, но не выделить флажком ни одного поля в прилагаемом списке информационных полей, то на печать будут выставлены карты, отобранные по выставленным выше критериям, но напечатаны будут только номер карты и имя пользователя.

6 Чтобы включить в список карты, прикреплённые к определённой двери, следует нажать на кнопку **Select door access filter** (Отобрать по доступу к двери).



7 Выбрать одну из опций: **Based on time** (Отбор по времени) или **Based on schedule** (отбор по расписанию).

ПРИМЕЧАНИЕ: *Чтобы расширить критерии отбора, следует щёлкнуть правой кнопкой мыши в окне* ***Select door access filter****.*

8 Отметить флажками поля, которые должны быть выведены на печать. При печати карт в каждое поле будут подставлены те значения, которые указаны в описании карт.

9 Получившийся список карт можно сохранить в файл стандартного формата .QRP (Quick Report) для последующего просмотра его при помощи программы Quick Viewer.

10 Кроме того, при помощи кнопки “Font” (Шрифт) можно изменить шрифт и размер шрифта для выбранного списка карт. Изменения будут автоматически показаны в окне просмотра (sample box). Для предварительного просмотра отчёта из окна Print можно воспользоваться кнопкой **Preview** (Предварительный просмотр).

Отображение последних транзакций с картой

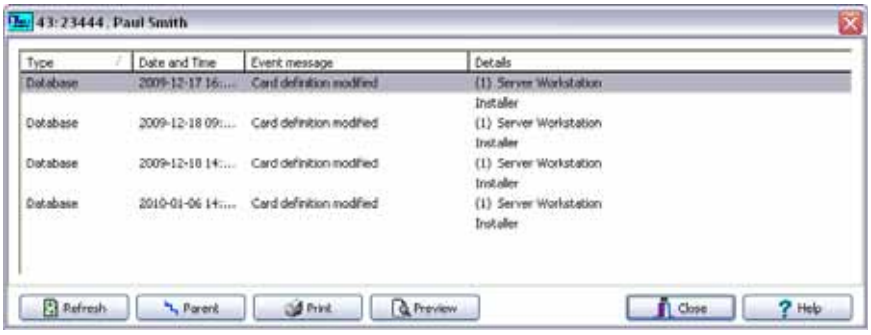
Функция **View last transactions** (Посмотреть последние транзакции) служит для просмотра последних транзакций, выполненных указанным владельцем карты. Например, в этом окне отображается “Access denied” (Доступ закрыт), как тип события, а также дата и время и сообщение о событии, которое отображается на рабочем столе сообщений Message. Система отображает 15 последних транзакций для каждой категории событий:

- События, вызывающие запрет доступа (проход не в том месте, не тот уровень доступа, не тот статус карты и т.д.),
- События, вызывающие разрешение доступа,
- События, влияющие на работу базы данных (например, изменение описания карты, реле и т.п.),
- другие/прочие (Muscellanous) – это события, сгенерированные владельцами карт,
- события по учёту рабочего времени (приход-уход).

ПРИМЕЧАНИЕ: *Более подробно об транзакциях для каждой категории событий изложено далее в разделе "Описание архивных отчётов", подраздел "Card Use Report" (Отчёты об использовании идентификационных карт).*

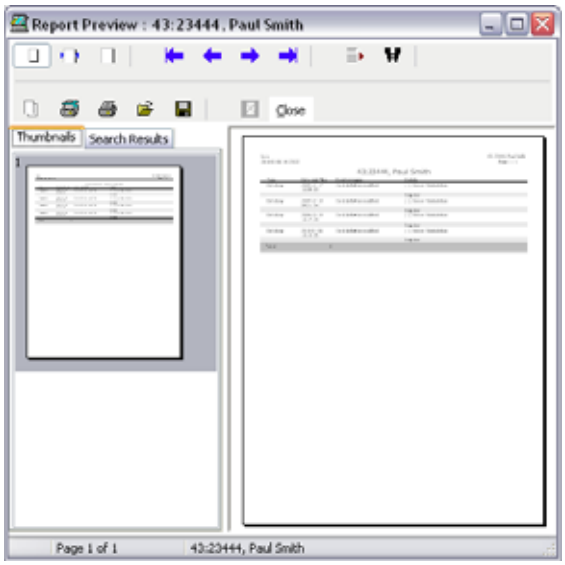
Просмотр последних транзакций с картой

1 В окне описания карты нажать на иконку **View last transaction** (Посмотреть последние транзакции)**.**



- **Type** (Тип) – показывает категорию событий.
- **Date and time** (Дата и время) – отображает дату и время, указанные в сообщении о событии.
- **Event message** (Сообщение о событии) – отображает сообщение о событии, которое было отправлено на сервер (и на APM), когда произошло это событие. Это же сообщение отображается на рабочем столе Message (меню Desktop).
- **Details** (Подробные сведения) – отображает дополнительные сведения, связанные с типом транзакций. Например, при сообщении о событии “card definition modified” (описание карты изменено) в колонке Details (Подробные сведения) перечислены приложения EntraPass, из которых были внесены изменения в карту, а также имя оператора.
- **Refresh** (Обновить) – эта кнопка служит для обновления окна и добавления в него новых транзакций по мере их появления. По мере того как владельцы карт создают события, становятся доступными новые данные.
- **Parent** (Родительский элемент) – позволяет посмотреть родительский элемент для выбранного компонента. *Смотрите пункт "Основные функции" на странице 53 для более подробной информации* .
- **Print** (Печать) – служит для вывода на печать точной копии информации, представленной в этом окне. *Смотрите пункт "Основные функции" на странице 53 для более подробной информации* .

- **Preview** (Предварительный просмотр): Кнопка **Preview** требует выбора принтера и затем отображает панель **Report Preview** (Предварительный обзор отчета).

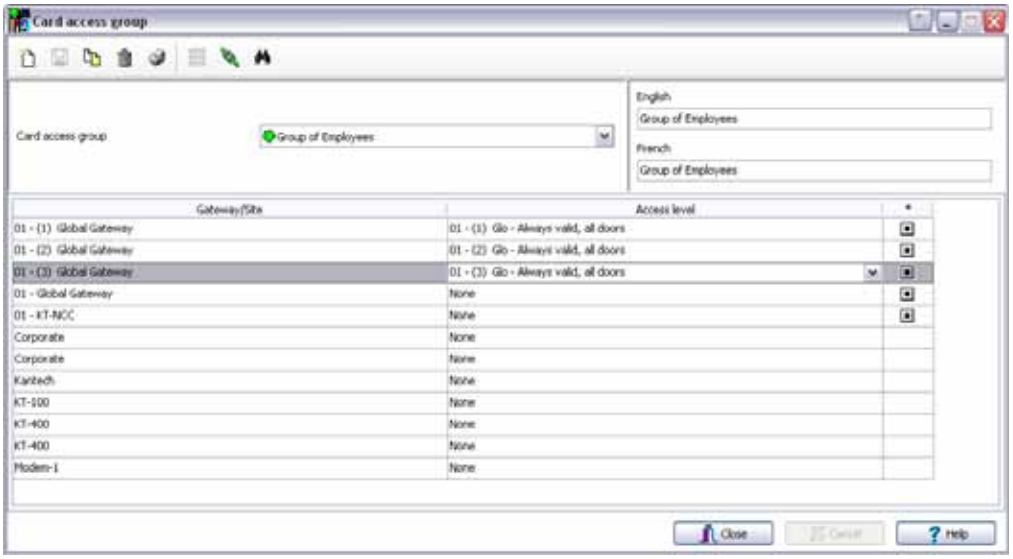


Назначение уровня доступа для группы карт

Предварительно настроенные уровни доступа для групп карт позволяют быстро назначать уровень доступа для разных сайтов/лучей системы. Групповой уровень доступа можно вызвать во время описания карты вместо повторного ввода уровней доступа для каждого сайта/луча. Причём, именно данные из группы доступа прикреплены к карте. Таким образом, можно изменять данные в групповом уровне доступа, не изменяя данные о доступе в описании каждой карты.

ПРИМЕЧАНИЕ: *При импортировании идентификационных карт функцию* ***Card access group*** *(Группа доступа для карт) может быть использована для назначения уровня доступа для этих карт.*

1 В окне Card (Карты) нажать кнопку Card access group (Группа доступа для карты).



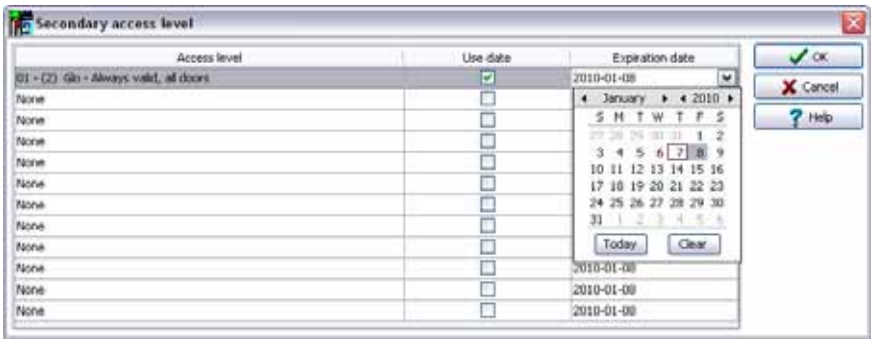
2 Чтобы изменить существующую группу доступа, выделить её в выпадающем списке **Card access group**. Чтобы создать новую группу, следует нажать кнопку **New** (Создать) и указать имя группы на используемых языках. В колонке **Site** (Сайт/Луч) отображается сайт/Луч, прикреплённый к указанной группе доступа.

3 В списке **Access level** (Уровни доступа) выбрать основной уровень доступа , который будет определять доступ к дверям по назначенным лучам.

4 Чтобы выбрать дополнительный уровень доступа для Шлюза/Луча, то нажмите квадратную иконку, следующую после **Access level** (Уровень доступа), для необходимого Шлюза/Луча.

NOTE 1: *Когда контроллер* ***KT-400*** *находится в автономном режиме, то основной и дополнительные уровни доступа действительные.*

NOTE 2: *Когда вы используете контроллеры* ***KT-100***, ***KT-200*** *или* ***KT-300*** *в автономном режиме, тогда дополнительные уровни доступа становятся недействительными. Действует только основной уровень доступа.*



3 Выберите уровень доступа из списка.

4 Если вы хотите установить дату окончания срока действия дополнительного уровня доступа, нажмите на опцию **Use date** (использовать дату и нажмите кнопку **Expiration date** (Дата окончания). Там будет появляться окно с календарем.

ПРИМЕЧАНИЕ: *Кнопка* **Access level** *будет отображаться зеленым, когда назначен дополнительный уровень доступа.*

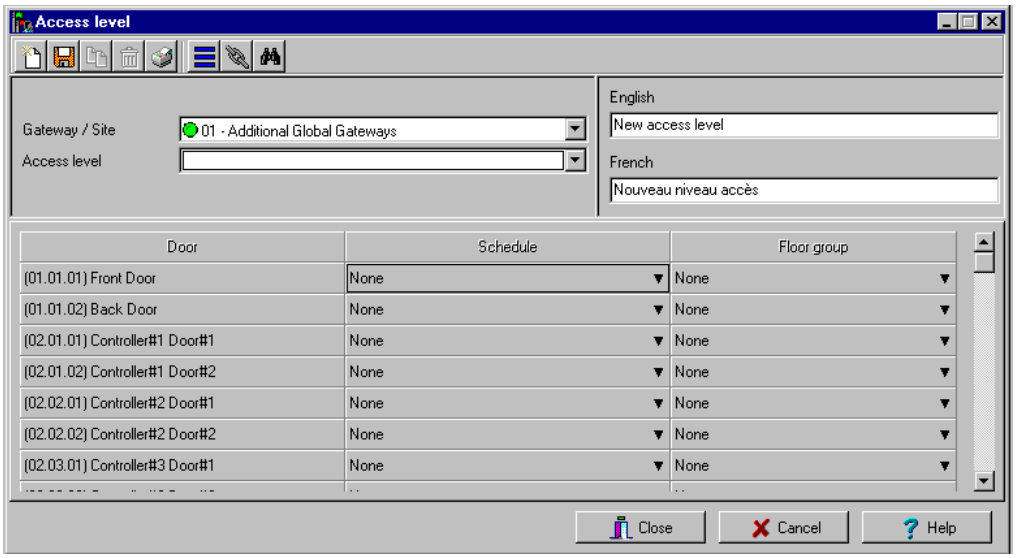
Назначение уровней доступа

Уровни доступа показывают, где и когда карта будет действительной. Предварительно настроенные группы доступа для идентификационных карт позволяют быстро назначить уровень доступа для разных шлюзов. Для каждого сайта и для шлюза (Global/KT-NCC/NCC 8000 Gateways) можно назначить до 248 уровней доступа. Уровень доступа для карты назначается следующим образом:

- Создать расписания, соответствующие времени, в которое у пользователя есть доступ к выбранным дверям;
- Назначить созданное расписание для выбранных дверей (в меню задания уровня доступа (definition -> Access level));
- Назначить для карты уровень доступа.

ПРИМЕЧАНИЕ: *По умолчанию установлен уровень доступа "**Always valid, all doors**" (Достоверный всегда, все двери) – владельцы карт, которым назначен этот уровень доступа, всегда имеют доступ ко всем дверям. Чтобы закрыть доступ к определённым дверям в определённое время, необходимо создать особый уровень доступа.*

1 В меню **Users** (Пользователи) нажать на иконку **Access level** (Уровни доступа). Открывается окно Access level.



2 В выпадающем списке Access level нажать **New** (Создать) и присвоить создаваемому уровню доступа подходящее имя.

ПРИМЕЧАНИЕ: *Компоненты, отображаемые в колонках Doors (Двери) и Schedule (Расписания) или Floor group (Группы этажей), должны быть предварительно описаны в соответствующих меню. Для назначения дверей нужно перейти в меню **Devices** (Устройства) > **Doors** (Двери). Настройка расписания выполняется в разделе: **Definition** (Описания) > **Schedules** (Расписания). Чтобы описать группы этажей, следует войти в меню **Groups** (Группы) > **Doors** (Двери).*

3 В колонке **Schedule** (Расписания) указать расписание, согласно которому владельцы карт должны будут иметь доступ к выбранной двери.

4 Если необходимо, выбрать группу этажей из колонки группы этажей.

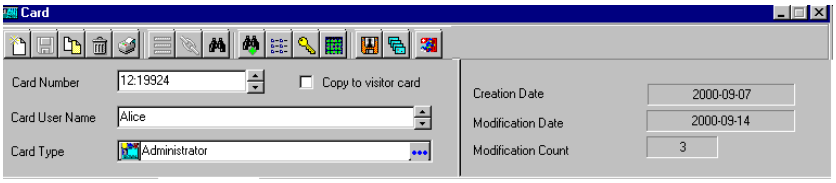
Назначение карт посетителей

Карта посетителя выпускается для временного применения. Она используется в качестве шаблона для ввода информации о пользователе. Карты посетителей можно создавать двумя способами:

- копированием информационных полей карты в базу данных карт посетителей (Visitor Card), когда в системе создаётся новая карта или разовый пропуск,
- созданием новой карты посетителя (Visitor Card).

Создание карты посетителя (Visitor card) при создании новой карты

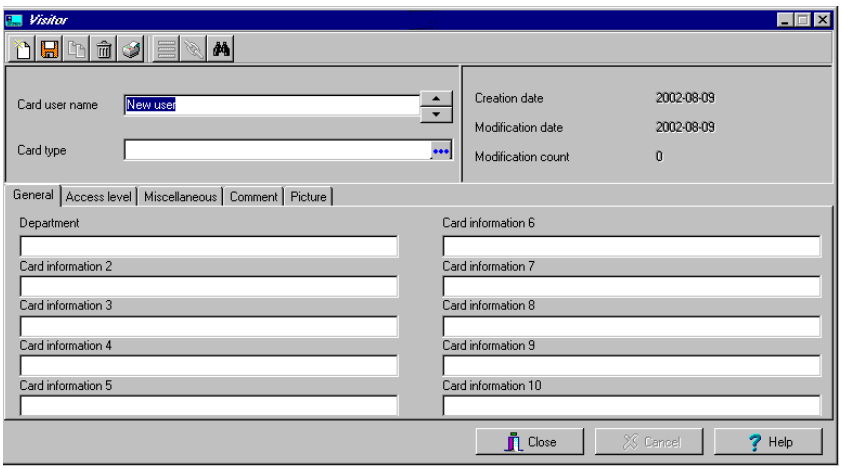
1 В окне Users (Пользователи) нажать на иконку **Card** (Идентификационные карты). Открывается окно Card.



2 Поставить флажок в поле **Copy to visitor card** (Копировать в карты посетителей). Данные этой карты будут позже использоваться при создании новых карт и изготовлении разовых пропусков (day passes).

Создание карты посетителя (Visitor Card) при помощи шаблона карт

1 В окне Card (Карты) нажать на панели инструментов на иконку **Visitor card** (Карты посетителей).



2 В полях карты посетителя (**Visitor**) ввести необходимые данные.

ПРИМЕЧАНИЕ: *Смотрите пункт "Назначение карт (раздел Card)" на странице 284 для более подробной информации относительно создании разовых пропусков и карт посетителей. Закладка Picture (Изображение) даёт возможность размещать на картах фотографии и подписи, а также изготавливать электронные пропуска (доступна также функция предварительного просмотра).*

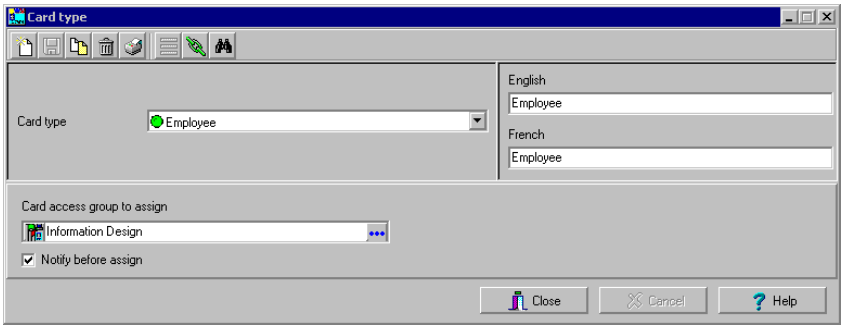
Назначение типов карт

Тип карты позволяет сортировать владельцев карт по группам, а затем изменять уже созданные группы карт или создавать отчёты. Кроме того, эта функция может использоваться, чтобы запретить доступ к данным карты конкретному оператору. Например, можно запретить оператору выпускать или просматривать определённые группы карт. В частности, если карты имеют тип "Администратор", то операторы, не имеющие соответствующих полномочий, не смогут выпускать, просматривать, изменять, удалять или изготавливать карты этого типа.

ПРИМЕЧАНИЕ: *Система имеет пять уже установленных типов карт: administrator (администратор), employee (работник), security (охранник), maintenance (обслуживающий персонал) и visitor (посетитель). Тип карты можно назначать для групп карт, отсортированных по уровню доступа. Таким образом, если тип карты связан с определённой группой доступа, то информация об уровне доступа у этой группы карт автоматически распространяется и на владельца этой карты.*

Создание нового типа карт

1 В меню **Users** (Пользователи) нажать на иконку **Card type** (Тип карты). Открывается окно Card type.



2 В окне Card type нажать кнопку **New** (Создать) и ввести необходимые данные на используемых языках в полях справа.

3 В списке **Card access group to assign** (Назначить группу доступа для карт) выбрать существующую группу доступа или создать новую. *Смотрите в Главе 8 Назначение уровня доступа для группы карт' на странице 324 для более подробной информации* о группах доступа.

4 *Смотрите пункт "Пользователи" на странице 283 для более подробной информации* по порядку прикрепления владельца к определённому типу карты смотрите.

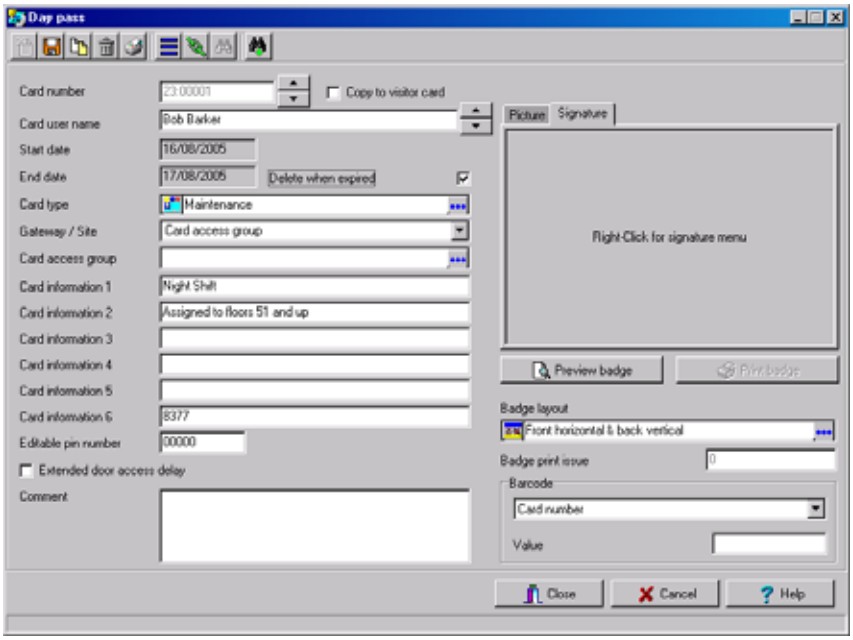
Назначение разовых пропусков

Разовые пропуска выписываются временным работникам, служащим других филиалов компании, покупателям и т. д. Эта опция позволяет быстро предоставить доступ разовым посетителям. Даже если владелец разового пропуска не вернёт его назад, его срок действия закончится в с наступлением нового дня (в полночь), и пропуск потеряет свою силу.

Для создания разовых пропусков можно воспользоваться профилями посетителей, скопированными в меню “Visitor definition” (Назначение посетителей), для поиска нужного посетителя служит кнопка “Find visitor”. Кроме того, для создания нового пропуска можно использовать действующий разовый пропуск.

Создание разового пропуска (Day Pass)

1 В меню **Users** (Пользователи) нажать на иконку **Day pass** (Разовые пропуска). Открывается окно Day Pass.



2 Данные в информационные поля для создаваемой карты можно внести вручную или используя базы данных по картам. *Смотрите пункт "Пользователи" на странице 283 для более подробной информации* .

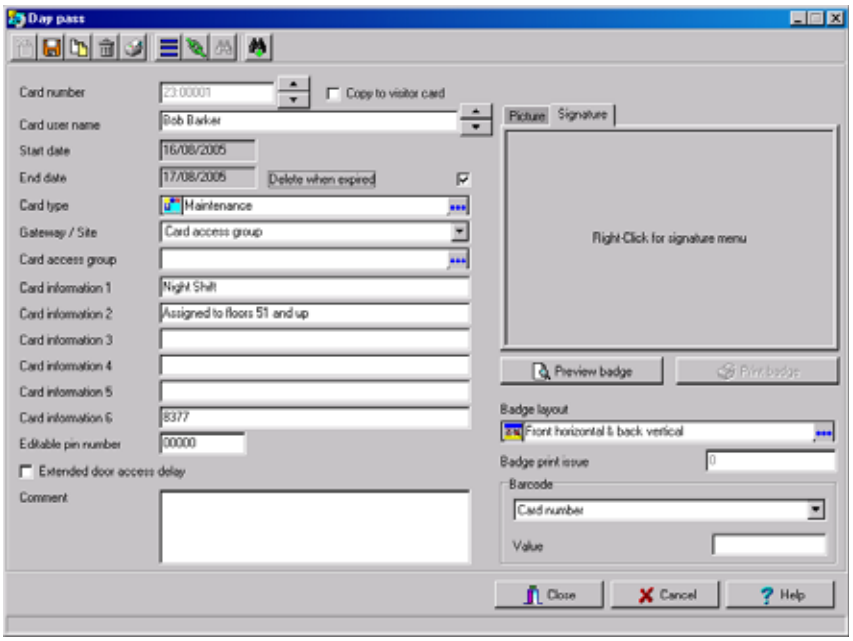
3 Отметить флажком опцию Copy to visitor card (Копировать в карты посетителей), чтобы сохранить этот разовый пропуск в базе данных посетителей.

ПРИМЕЧАНИЕ: *For more information of visitor cards, Смотрите пункт "Назначение карт (раздел Card)" на странице 284 для более подробной информации по картам посетителей. Закладка Picture (Изображение) даёт возможность размещать на картах фотографии и подписи, а также изготавливать электронные пропуска (доступна также функция предварительного просмотра).*

Создание нового разового пропуска с помощью функции "Сохранить как..."

Функция **Save as** (Сохранить как...) позволяет создавать новые разовые пропуска, используя уже выпущенный пропуск, путём внесения необходимых изменений и назначения нового номера карты. Например, можно изменить только имя пользователя, и оставить неизменными все остальные данные.

1 В меню **Users** (Пользователи) нажать на иконку **Day pass** (Разовые пропуска). Открывается окно Day Pass.



2 Чтобы найти подходящую действующую карту, следует щёлкнуть по иконке с биноклем и выбрать, какую карту лучше продублировать.

3 Внести необходимые изменения в информационные поля карты и нажать кнопку **Save as** (Сохранить как...).

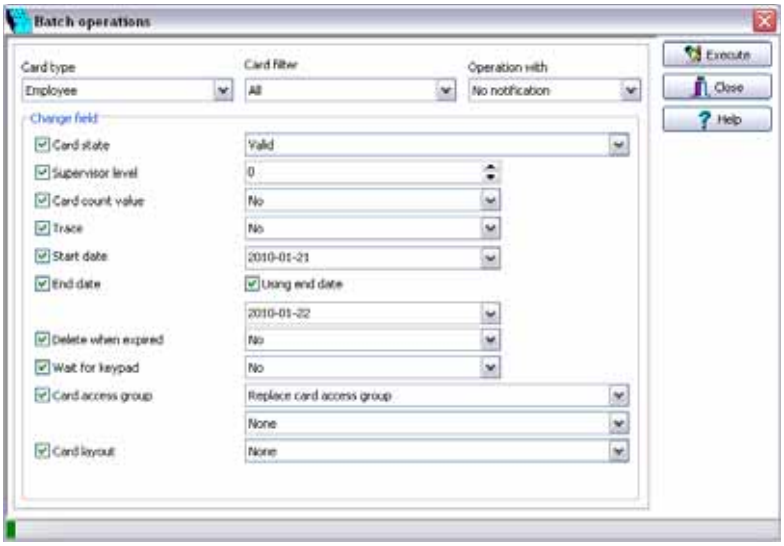
4 Система предложит назначить созданной карте новый номер.

Операции с группами (Batch Operations)

Это меню используется для изменения группы карт определённого типа. Например, можно изменить дату окончания срока действия (“end date”) для всех карт типа “administrator” (администратор). Индивидуальные поля появляются только в том случае, если поставить флажок в соответствующем месте.

Выполнение операций с группой карт

1 В меню Users (Пользователи) нажать на иконку **Batch operations** (Операции с группами).



2 Выбрать группу пользователей в выпадающем списке **Card type** (Тип карт). Все карты этого типа будут изменены.

3 Выбрать фильтр карт, чтобы сузить групповую операцию с картами среди выбранных типов карт.

4 Выбрать нужную функцию в выпадающем списке **Operation with** (Операция с...).
- **No notification** (Без уведомления) – система не будет выдавать уведомления и не будет запрашивать подтверждение оператора.
- **Notification** (С уведомлением) – система будет отображать ход выполнения операции.
- **Notification and confirmation** (С подтверждением и с уведомлением) – в отдельном окне будет отображаться ход выполнения операции и для каждого владельца карты потребуется подтверждение оператора на выполнение операции.

5 Отметить флажком опцию, которую требуется изменить для карт указанного типа.
- **Card state** (Статус карты) – применить этот новый статус карты ко всем владельцам карт указанного типа.
- **Supervisor level** (Уровень ревизора) — если выбран уровень ревизора, система будет устанавливать уровни в соответствии со значениями, назначенными в системе.
- **Card count value** (Число использований карты) – назначить это число использований карты ко всем владельцам карт указанного типа.
- **Trace** (Отслеживание) – отслеживать использование карт всеми владельцами карт указанного типа.
- **Start date** (Дата начала действия) – указанные карты начнут действовать только с этой даты. Эта новая дата будет применена ко всем владельцам карт указанного типа.
- **End date** (Дата окончания действия) – указанные карты перестанут действовать после наступления этой даты. Эта новая дата будет применена ко всем владельцам карт указанного типа.
- **Delete when expired** (С удалением после окончания срока действия) – указанные карты будут удалены после наступления даты окончания действия, указанной в меню Card Definition (Описание карт).
- **Wait for keypad** (Ожидание нажатия клавиш) – все владельцы карт указанного типа должны будут для получения доступа к двери, помимо предъявления действительной карты, ввести свой идентификационный код на кнопочной панели (если она активирована).

- **Card access group** (Группа доступа) – чтобы изменить группы доступа карт для указанного типа карт (**Card type**), используются два выпадающих списка. В первом списке описаны действия, которые можно выполнять с картами указанного типа. Второй список содержит группы доступа карт (уже описанные в системе), которые будут использоваться для выполнения выбранного действия.
  - **Replace card access group** (Заменить группу доступа карт)/**Replace**– заменить текущий уровень доступа на тот, который выбран в выпадающем списке.
  - **Update card access group** (Обновить группу доступа карт)/**Update** (Обновить) – заменить текущий уровень доступа на тот, который указан в выпадающем списке, за исключением позиций, у которых текущий уровень доступа имеет значение "None" (Отсутствует). Новые уровни доступа не добавляются.
  - **Add new access level** (Добавить новый уровень доступа)/**Add** (Добавить) – используется в тех случаях, когда добавляются новые позиции и необходимо добавить уровни доступа этих позиций к текущему списку. Все позиции/сайты/лучи с текущим уровнем доступа "None" (в списке Current access level) будут обновлены и заменены на позиции с новым уровнем доступа, указанным в списке New access level.
  - **Update add access level** (Обновить и добавить уровни доступа)/**Merge** (Объединить) – служит для слияния позиций из обоих списков. Новые позиции имеют приоритет перед текущими.

Примеры групповых операций с уровнями доступа карт

Текущий уровень доступа	Новый уровень доступа	Replace (Заменить)	Update (Обновить)	Add (Добавить)	Merge (Объединить)
Site Y1	Site X1	Site X1	Site X1	Site Y1	Site X1
Site Y2	Site X2	Site X2	Site X2	Site Y2	Site X2
Site Y3	None	None	Site Y3	Site Y3	Site Y3
None	Site X4	Site X4	None	Site X4	Site X4

- **Card layout** (Макет карт) – просмотреть список макетов шаблонов для идентификационных карт.
- **Card filter**: Применяет выбранный фильтр какрт для всех карт, в выбранном типе карт (card type).

6 Чтобы запустить процесс, нажать кнопку **Execute** (Выполнить). Система предложит подтвердить выполнение операции.

7 Нажать **Yes** (Да) для продолжения работы. После начала выполнения операции в левом нижнем углу окна загорается красный индикатор. Этот индикатор будет гореть до окончания процесса.

Импорт и экспорт файлов CSV

Функция CSV Import/Export предназначена для импорта/экспорта файлов формата CSV (Comma Separated Value). Импорт/экспорт данных из одного приложения в другое позволяет совместно использовать эти данные в обоих приложениях. Файлы формата CSV доступны для редактирования во многих приложениях (Excel, NotePad и др.). Функция CSV Import/Export используется в следующих случаях:

- выполняется обновление системы EntraPass DOS или WinPass 64 и необходимо извлечь карты, созданные в этих предыдущих версиях.
- необходимо импортировать базу данных по картам в систему начисления заработной платы. Использование функции импорта/экспорта позволит значительно сократить время настройки базы данных по владельцам карт.
- если установлена новая база данных, то вместо того чтобы перепрограммировать все данные, уже доступные в старой базе данных, системный администратор может экспортировать данные из старой базы (имена, отделы, номера карт и т.п.) в файл CSV, который может быть затем импортирован в новую базу данных.

ПРИМЕЧАНИЕ: *Функция CSV Import/Export устанавливает несколько правил: формат данных у каждого поля в старой и новой базе должен совпадать. Например, поле статуса карты может содержать только три значения: 0=действительная карта, 1=недействительная карта, 2=карта потеряна/украдена.*

Для импорта/экспорта данных можно воспользоваться уже настроенными шаблонами Kantech или создать свои собственные шаблоны.

Использование уже настроенного шаблона

Доступно два шаблона: EntraPass (1,2,3) и WinPass 64. Шаблон можно использовать на основе принципа "как есть", а можно изменить его.

1 В меню Users (Пользователи) нажать на кнопку **Import/Export** CSV.

2 В выпадающем списке **Select operation** (Выберите операцию) выбрать действие: **Import** (Импортировать) или **Export** (Экспортировать).

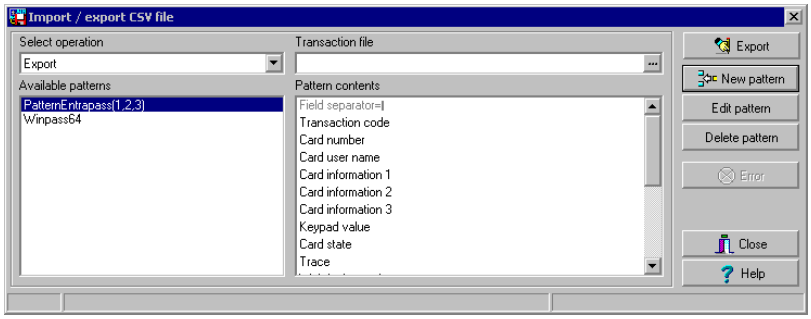
3 На панели **Available Patterns** (Доступные шаблоны) выбрать шаблон. Это зависит от настроек обновляемого программного обеспечения.

4 Чтобы изменить шаблон (при необходимости), нажать кнопку **Edit** (Редактировать).

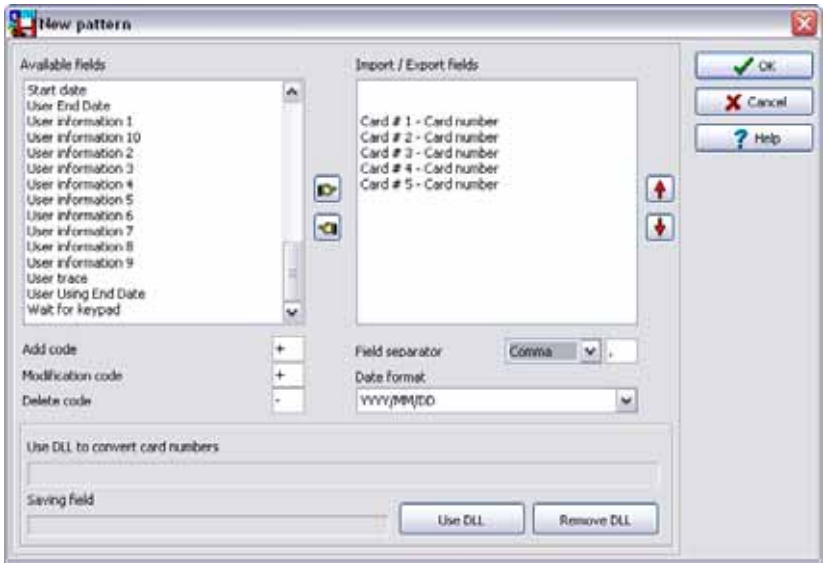
Создание нового шаблона для импорта/экспорта данных

Это меню служит для создания собственной маски импорта/экспорта, которая будет использоваться для импорта/экспорта CSV файлов.

1 В меню **Users** (Пользователи) нажать на кнопку **Import/Export CSV File**. При этом должно открыться окно Import / Export CSV file (Импорт/Экспорт CSV файлов).

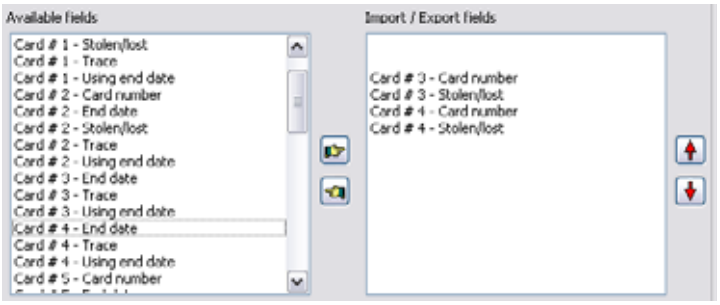


2 В меню Import/Export CSV file нажать на кнопку **New Pattern** (Новый шаблон). В окне New pattern отображается список всех полей, доступных в базах данных по идентификационным картам в системе EntraPass. Эти поля имеют особые форматы данных, которые должны совпадать в новой и старой базах данных. Например, поле статуса карты может содержать только три значения: 0=действительная карта, 1=недействительная карта, 2=карта потеряна/украдена.



3 При помощи кнопок с изображением руки-указателя выбрать поля, которые необходимо включить в новый шаблон. Поля **Transaction code** (Код транзакции) и **Card number** (Номер карты) входят в этот список по умолчанию. После выбора полей следует упорядочить данные кнопками с красными стрелками вверх-вниз (то есть разместить их в том порядке, в каком они будут записаны в файле CSV).

ПРИМЕЧАНИЕ: *Номер карты должен всегда быть выбран в каждом шаблоне, включая специфицческие карты. Например, Если вы выберите поле* ***Card #3 - Stolen/Lost****, Вы должны также выбрать поле* ***Card #3 - Card Number.***



4 Указать коды **Add code** (Код добавления) и **Modification code** (Код изменения). По этим кодам система во время импортирования файла определяет, какую карту нужно изменить, а какую добавить к базе данных. По умолчанию оба кода имеют значения “+”.

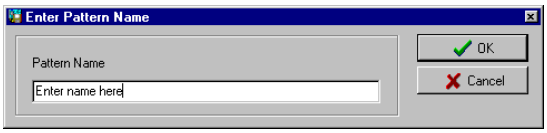
5 Выбрать **Delete code** (Код удаления). По этому коду система во время импортирования файла определяет, какую карту нужно удалить из базы данных. По умолчанию это код имеет значение “-”.

6 Указать значение в поле **Field separator** (Разделитель полей). Этот код предназначен для разделения используемых полей при импорте или экспорте данных. Как правило, для этого используется знак запятой (,). На это следует обратить особое внимание при добавлении имён и фамилий пользователей, разделённых знаком запятой. Разделитель поля может быть: tab, space(пробел), comma(запятая), semicolon (;) и др.

7 Выбрать нужный формат даты в поле **Date format**. Импорт/экспорт даты будет выполняться в указанном формате. Чаще всего используется формат YYYY/MM/DD (YYYY – год, MM – месяц, DD - день). Также возможны другие форматы:
- MM/DD/YYYY
- DD/MM/YYYY
- YY/MM/DD
- MM/DD/YY
- DD/MM/YY

ПРИМЕЧАНИЕ: *Опция **Use DLL** (Использовать DLL) предназначена для запуска программы конвертирования используемых номеров идентификационных карт. Чтобы не использовать эту программу, следует выбрать опцию **Remove DLL** (Исключить DLL).*

8 Нажать **OK** для выхода из окна Pattern. Откроется окно для ввода имени нового шаблона



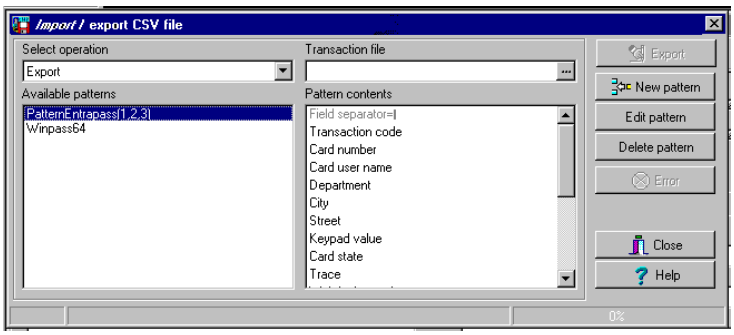
9 Указать имя нового шаблона в открывшемся окне в поле Pattern name и нажать **OK**. Система автоматически вернётся к окну Import/Export CSV file (Импорт/Экспорт CSV файлов). Только что созданный шаблон появится в списке **Available patterns** (Доступные шаблоны).

10 Чтобы добавить или удалить информационные поля из созданного шаблона, следует щёлкнуть по нему дважды и внести необходимые изменения. Теперь можно импортировать или экспортировать данные с помощью этого нового шаблона.

Экспорт идентификационных карт

Иногда требуется экспортировать данные из базы данных по идентификационным картам в другое приложение. Для этого можно использовать уже созданный шаблон или создать новый.

1 В меню **Users** (Пользователи) нажать на кнопку **Import/Export CSV File**. При этом должно открыться окно Import / Export CSV file (Импортирование/Экспортирование CSV файлов).

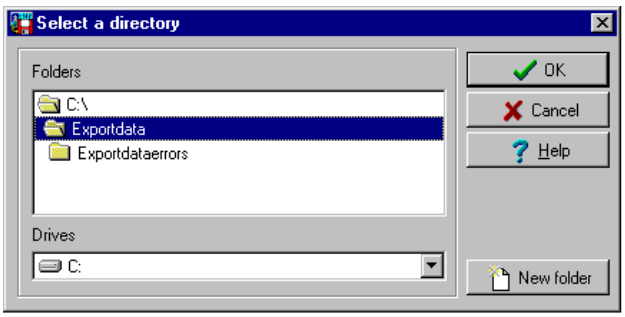


2 В выпадающем списке **Select operation** (Выберите операцию) выбрать опцию **Export** (Экспортировать).

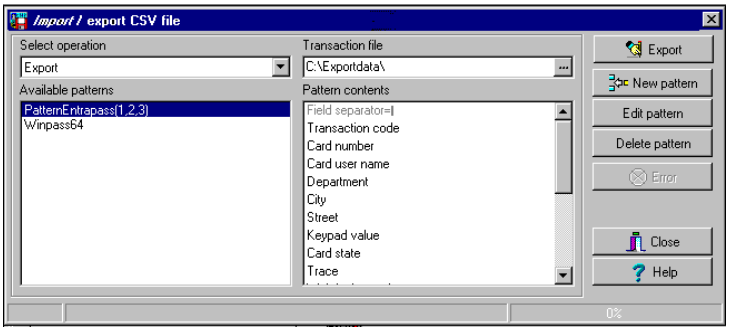
3 В расположенном слева списке **Available patterns** (Доступные шаблоны) выделить шаблон, с помощью которого необходимо экспортировать карты. При необходимости можно отредактировать шаблон таким образом, чтобы он соответствовал шаблону того приложения, в

которое будут перенесены данные; либо можно создать новый шаблон. (*Смотрите пункт "Создание нового шаблона для импорта/экспорта данных" на странице 333 для более подробной информации* по созданию шаблона).

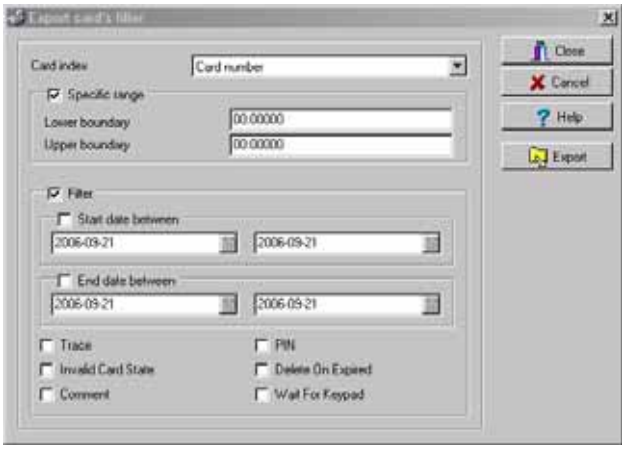
4 В поле **Transaction file** (Файл транзакции) указать путь сохранения создаваемого файла данных. Для открытия этого CSV файла можно использовать Excel, NotePad и другие программы.



5 После указания/создания папки для экспорта данных следует нажать **OK** и вернуться в окно Import/Export CSV file.

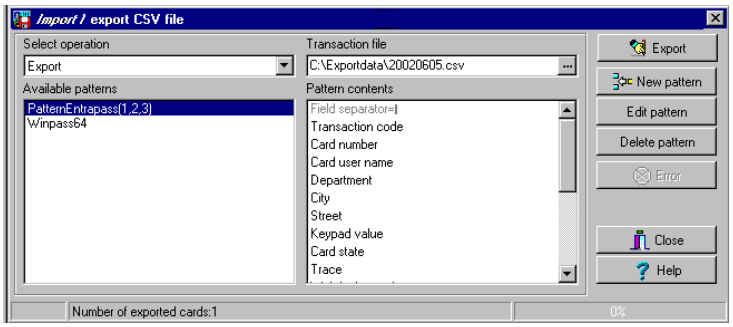


6 Нажать кнопку **Export** (Экспортировать), которая становится активной после указания пути сохранения файла. В открывшемся окне отобрать карты, предназначенные для экспорта.



ПРИМЕЧАНИЕ: *В создаваемый файл будут включены только те карты, которые удовлетворяют ВСЕМ критериям отбора. Карты, не удовлетворяющие всем указанным критериям, не будут включены в файл.*

7 В окне Export Card's filter (Фильтры экспортируемых карт) отобрать карты, предназначенные для экспорта. После выделения всех необходимых полей нажать кнопку **Export** (Экспортировать). При этом должно открыться окно Import/Export CSV file.



ПРИМЕЧАНИЕ: *В поле* ***Transaction file*** *(Файл транзакции) указывается название создаваемого файла и путь сохранения. По умолчанию файл с экспортируемыми данными записывается в определённую папку (в проиллюстрированном примере это папка Exportdata). В строке состояний (нижняя строка окна) отображается число экспортированных карт (в данном случае, это 1 карта). Имя файла по умолчанию – YYYYMMDD.csv. Для просмотра созданного файла можно использовать, например, NotePad.*

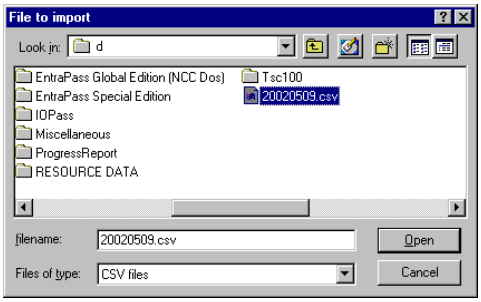
Импорт идентификационных карт

1 В меню **Users** (Пользователи) нажать на кнопку **Import/Export CSV File**. На экране появляется диалоговое окно Import/Export CSV file.

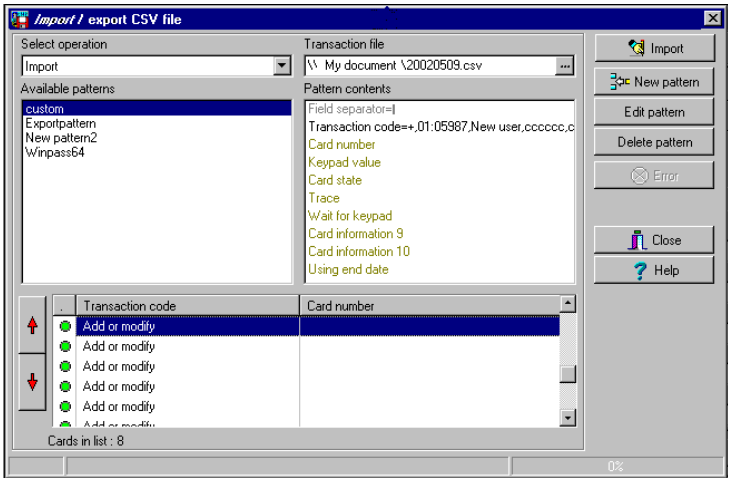
2 В выпадающем списке **Select operation** (Выберите операцию) выбрать опцию Import (Импортировать).

3 В списке **Available patterns** (Доступные шаблоны) выделить шаблон, с помощью которого необходимо импортировать данные. (*Смотрите пункт "Создание нового шаблона для импорта/экспорта данных" на странице 333 для более подробной информации* по созданию шаблона).

4 В поле **Transaction file** (Файл транзакции) указать путь, где хранится CSV файл, содержащий импортируемые данные.



5 Выбрать файл и нажать **Open** (Открыть). При этом система снова вернётся в окно Import/Export CSV file.



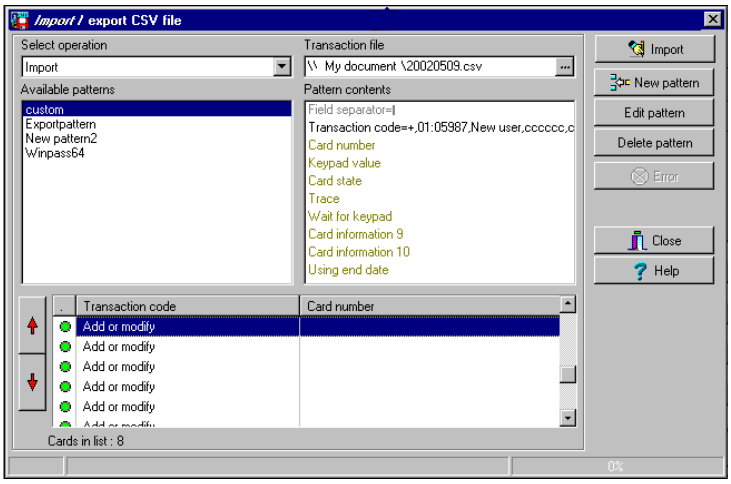
6 Проверить отсутствие ошибок (или исправить найденные ошибки) и нажать **Import** (Импортировать) для завершения операции.

ПРИМЕЧАНИЕ: *Система сканирует файл с импортируемыми данными и отображает результаты при помощи цветового кода. Каждая позиция отображается вместе с цветовым флажком. Жёлтый или красный цвет указывает на ошибку. Ошибки часто возникают из-за несоответствия шаблонов. В этом случае необходимо выбрать другой шаблон или исправить используемый шаблон таким образом, чтобы все позиции в шаблоне совпадали с позициями в файле данных. Кроме того, ошибки могут быть даже при отображении зелёного флажка напротив кода транзакции.*

Исправление ошибок импорта/экспорта

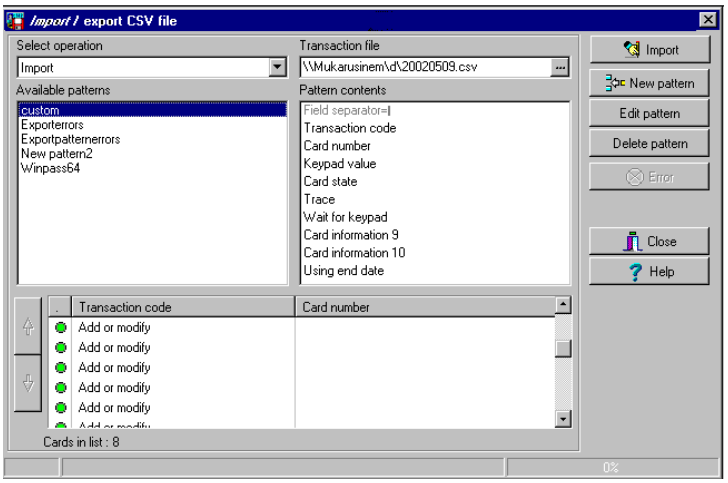
Функция CSV Import/Export устанавливает несколько правил: формат данных у каждого поля в старой и новой базе должен совпадать. Например, поле статуса карты может содержать только три значения: 0=действительная карта, 1=недействительная карта, 2=карта потеряна/украдена. Используемый шаблон должен совпадать с шаблоном исходного файла. Эта часть поможет исправить ошибки, возникающие при импорте/экспорте данных.

1 Нажать кнопку **Import** или **Export**, чтобы начать транзакцию (в приведённом ниже примере выполняется импорт CSV данных). В нижней строке окна отображается число карт в списке.



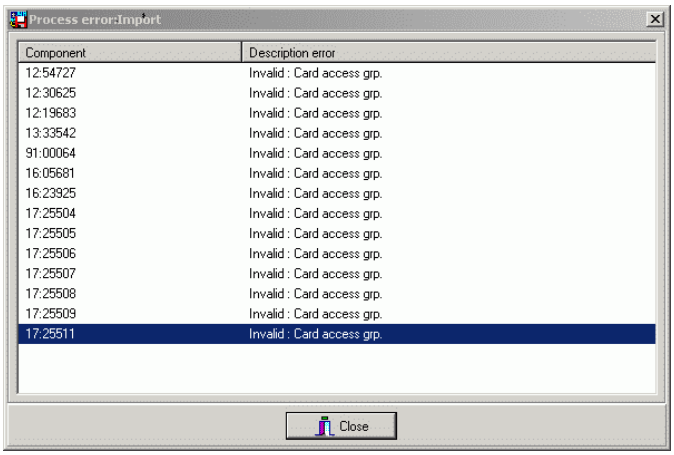
ПРИМЕЧАНИЕ: *Несмотря на то, что позиции в колонке* ***Transaction code*** *(Код транзакции) отмечены зелёным флажком, колонка* ***Card number*** *(Номер карты) осталась пустой. Это указывает на неправильное конвертирование шаблона.*

2 Нажать кнопку **Import** (Импортировать).



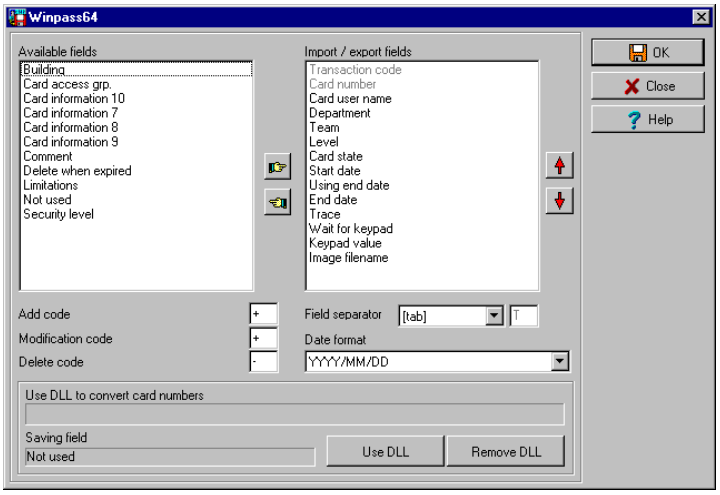
ПРИМЕЧАНИЕ: *Кнопка* ***Error*** *(Ошибки) стала активной, поскольку система обнаружила ошибки при импортировании данных.*

3 Чтобы увидеть информацию об ошибках, нажать кнопку **Error.** Окно Process error (Ошибки обработки) содержит те позиции, которые оказались неверными в используемом шаблоне. Это говорит о том, что ваш шаблон неверный.

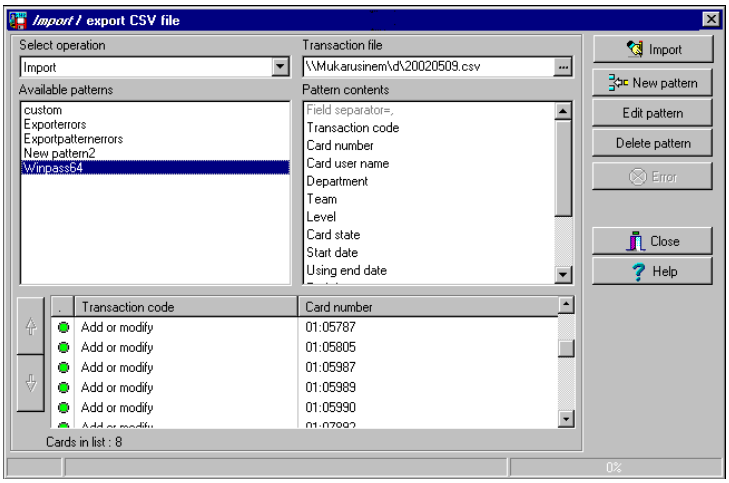


4 Нажать **Close** (Закрыть), чтобы вернуться в окно Import/Export.

5 В окне Import/Export CSV дважды щёлкнуть по шаблону, используемому для импортирования данных (в нашем примере это шаблон Custom).



6 В выпадающем списке **Field separator** (Разделитель полей) выбрать **Comma** (Запятая) и нажать **OK.** Данные в поле **Card number** указывают, что теперь транзакция импорта пройдёт успешно.



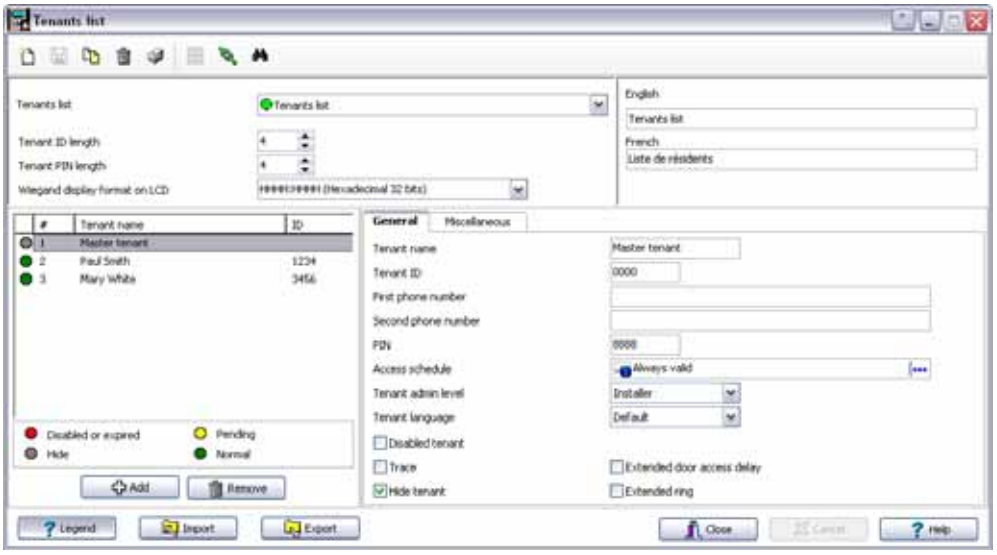
Список жильцов

Житель - это постоянно проживающий житель данного строения или работник данной компании. Житель может предоставлять доступ посетителю. Лист жителей может быть создан в EntraPass, который будет использован в KTES.

Создание нового списка жильцов

1 Из панели инструментов **Users** (Пользователи), нажмите кнопку **Tenants list** (список жильцов).
2 Исправьте имя списка жильцов в колонке **Tenants list**. По умолчанию это **New tenant list**.
3 Укажите длину ID номера жильца в колонке **Tenant ID length** (1 до 5). Значение по умолчанию 4.
4 Укажите длину PIN кода в графе **Tenant PIN length** (4 до 6). По умолчанию - 4.
5 Выберите формат данных Wigand на LCD в поле **Wiegand display format on LCD**. Возможные значения:
   - Шестьнадцатеричные 24 бит
   - Шестьнадцатеричные и десятичные 24 бита
   - Шестьнадцатеричные 32 бита
   - Шестьнадцатеричные и десятичные 32 бита
   - Десятичные ABA 8 цифр
   - Десятичные ABA 10 цифр

   Значение по умолчанию Шестьнадцатеричные 32 бита

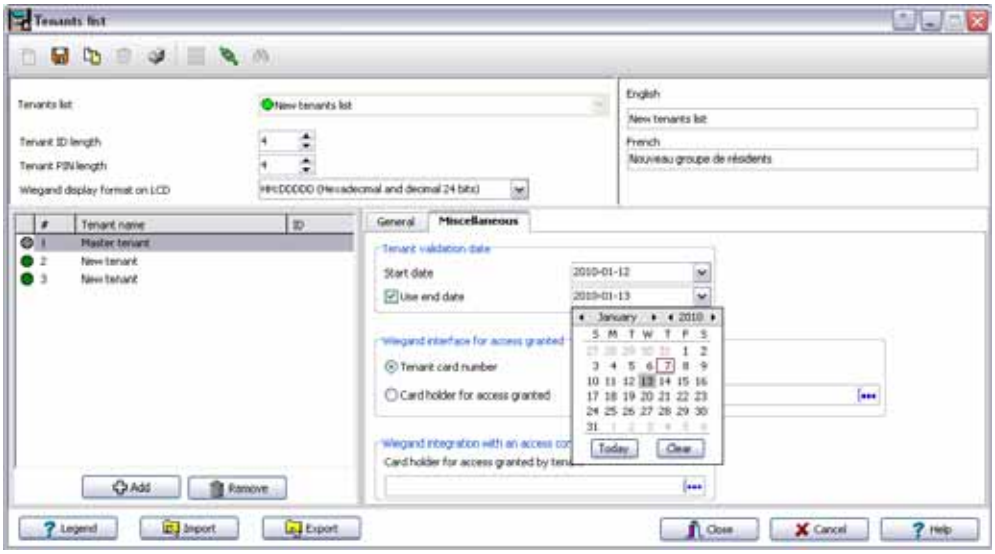


Добавление новых жильцов в список

1 Нажмите на вкладку **General** (Общие).
2 Нажмите на кнопку **Add** (**+**) (Добавить). Вы можете нажать на кнопку **Legend**, чтобы отобразить актуальное состояние для каждого жильца.
3 Настройте параметры жильцов:
   - **Tenant name** (Имя жильца): Введите имя жильца (20 символов максимум). ПО умолчанию **New tenant**.
   - **Tenant ID**: Введите ID номер жильца. ID номер жильца - это идентификационный код состоящий от 1 до 5 цифр, который использует посетитель, чтобы связаться с жильцом. Количество цифр уже было создано при создании списка жильцов. ПО умолчанию это 0000.
   - **First phone number**: Укажите первый телефонный номер. Этот номер используется когда посетитель набирает жильца напрямую из устройства KTES. Если вы не введете этот телефонный номер, KTES не сможет позвонить жильцу и этот житель не будет отображатья в списке в директории KTES также. (15 цифр максимум). Значение по умолчанию - пусто.
   - **Second phone number**: Укажите второй телефонный номер. Этот номер используется KTES, когда нет ответа по первому номеру. (15 цифр максимум). Значение по умолчанию - пусто.
   - **PIN**: Укажите индивидуальный PIN код для каждого жильца (4-6 цифр). Количество цифр уже было создано при создании списка жильцов. Значение по умолчанию 0000.

- **Access schedule**: Введите расписание доступа. По причинам безопасности, **Access Schedule** должно быть установлено исходя из времени доступа жильцом. Житель может войти в здание в течении определенному времени с учетом назначенных выходных дней и каникул. Значение оп умолчанию **Always valid** (Верно всегда). Смотрите в Главе 5 Назначение расписаний' на странице 174 для более подробной информации по назначению расписаний.
- **Tenant admin level**: Укажите уровень администратора для жильца (Installer, Owner, Maintenance or Tenant/инсталлятор, собственник, сервисный работник, житель). Значение по умолчанию**Tenant**.
- **Tenant language**: Укажите значение по умолчанию, используемое для жильцов KTES/ (язык системы, English, French, Spanish, Особенный). Значение по умолчанию **Default** Смотрите в Главе 4 Настройка Kantech Telephone Entry System (KTES)' на странице 134 для более подробной информации по языкам системы.
- **Disabled Tenant** (Запрещенный житель): Статус **Disabled Tenan**t позволяет вам активировать реле и/или производить тревогу. Значение по умолчанию невыбрано (**enabled**) (включено).
- **Trace**(Трассировка): Опция позволяет вам активировать реле и/или генерировать событие трассировки. Значение по умолчанию не выбрано (**not traced**)(трассирвока отключена).
- **Hide tenant** (Скрыть жильца): Эта опция используется если вы хотите, чтобы имя жильца отображалось на LCD или было скрыто. Значение по умолчанию невыбрано. (**displayed**)(отображать имя жильца на LCD).
- **Extended door access delay**: расширенная задержка на вход для людей с ограниченными физическими возможностями, которым необходимо большое время для входа. Значение по умолчанию не выбрано (**нет расширенной задержки**).
- **Extended ring** (Расшитренный звонок): Система будет позволять звонить жильцу более долгое время, чем обычно. Значение по умолчанию не выбрано (**нет расширенного звонка**).

4 Выберите вкладку **Miscellaneous** (Дополнительно).



5 В графе **Tenant validation date** установите период действия прав доступа для жильца:

- **Start date** (Время начала): Это дата с которой житель может получить доступ к системе. Введите дату в поле (mm/dd/yyyy) или нажмите на календарь и выберите дату.
- **Use end date** (Время окончания): Это дата, после которой житель не может больше иметь доступ в данную систему и его статус в это помещение анулируется. Введите дату в формате (mm/dd/yyyy) или нажмите на календарь и выберите дату. Значение по умолчанию пусто.

6 Установите тип интерфейса в поле **Wiegand interface for access granted**:

- **Tenant card number** (номер карты жителя): 64-х битный номер, который оссоциируется с каждом жильцом. Этот номер используется при получении прав на доступ от KTES.
- **Card holder for access granted (**Картодержатель для предоставления доступа) **(недоступно в EntraPass KTES Edition)**: Это номер картодержтеля будет первым номером карты, используемым жильцом для доступа через KTES.

7 **Wiegand integration with an access controller** (Wigand интеграция с контроллером доступа):
- **Card holder for access granted by tenant** (Картодержатель для доступа, предоставленного жильцом): Это номер карты, который генерируется выходом Wiegand когда доступ предоставляется жильцом посетителю. Это опция доступна, когда опция **Wiegand integration with an access controller** (Wigand интеграция с контроллером доступа) была выбрана в KTES (Смотрите в Главе 4 Настройка Kantech Telephone Entry System (KTES)' на странице 134 для более подробной информации).

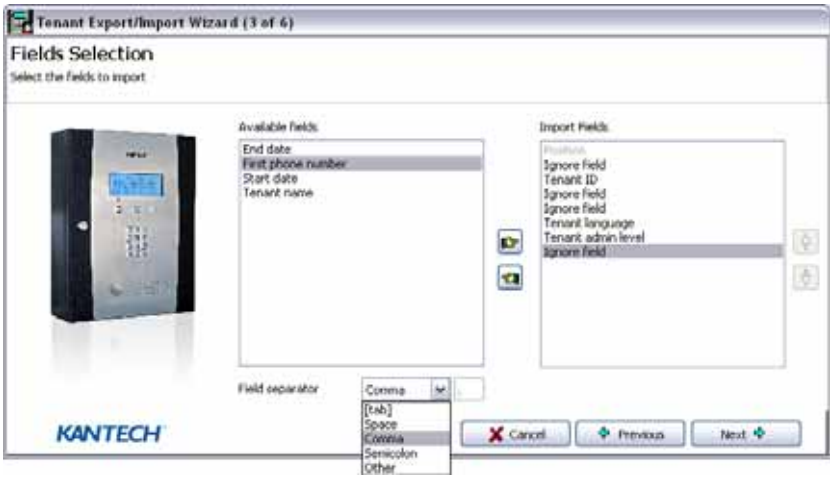
Импортирования списка жильцов

В потребности упростить импорт списка жильцов, была реализована функция, которая сопровождает вас по различным шагам.

Шаг 1: Нажмите кнопку **Import** чтобы запустить **Tenant Export/Import Wizard** (Помощник импорта/экспорта жильцов).

Step 2: Нажмите кнопку **Next** и выберите CSV файл для импорта.

Шаг 3: Нажмите на кнопку **Next** и выберите справа поле, котрое будет импортировано. Используйте клавиши влево/вправо, чтобы добавить и удалить выбранные поля. Может быть выбран разделитель поля (field separator) (по умолчанию Comma/запятая).



Шаг 4: Нажмите на кнопку **Next** и выберите жителей, которые должны быть импортированы.

Шаг 5: Нажмите на кнопку **Next** и затем нажмите кнопку **Import** для выполнения управления.

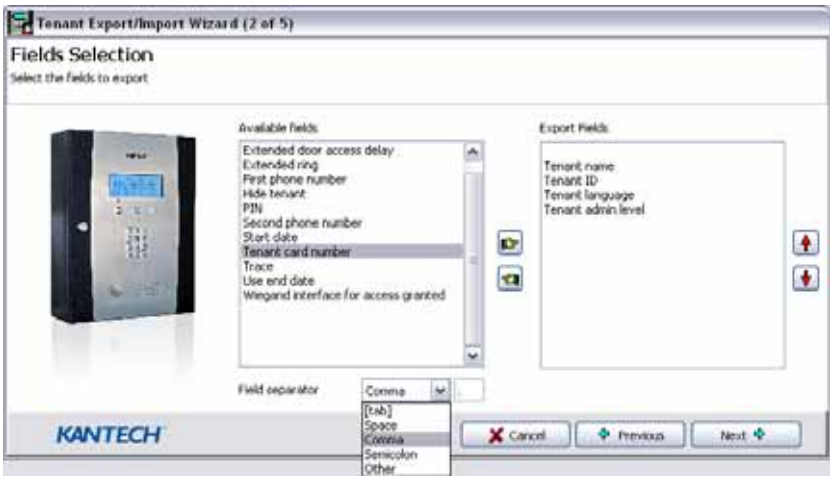
Шаг 6: Нажмите на кнопку **Next чтобы** увидеть общее количество импортированных данных.

Экспорт списка жильцов

Была также реализована процедура автоматического экспорта списка жильцов.

Шаг 1: Нажмите на кнопку **Export** чтобы запустить **Tenant Export/Import Wizard** (Помощник экспорта/импорта).

Шаг 2: Нажмите кнопку **Next** и выберите поля слева, которые должны быть экспортированы. Используйте кнопки лево/право чтобы добавлять или удалять поля данных. Различные поля могут быть использованы. По умолчанию, это Comma (точка с запятой).



Шаг 3: Нажмите кнопку **Next** и выберите жильцов, список которых необходимо экспортировать.

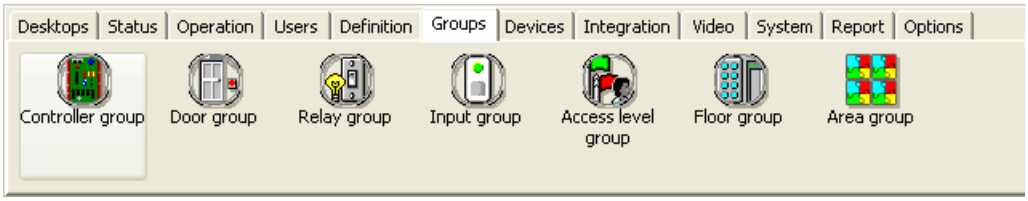
Шаг 4: Нажмите кнопку **Next** (Следующий) и выберите местоназначения CSV. Нажмите кнопку **Export** (Экспорт).

Шаг 5:Нажмите кнопку **Next**, чтобы увидеть всю экспортированную информацию.

Глава 9 • :Группы

Панель инструментов Группы

Чтобы применять функции системы сразу к целой группе компонентов, следует объединить компоненты в группы. Это полезная функция при проведении групповых изменений.



NOTE: *Каждый компонент системы, перед тем как включить в группу, следует назначить.*

Система предусматривает создание следующих групп компонентов:

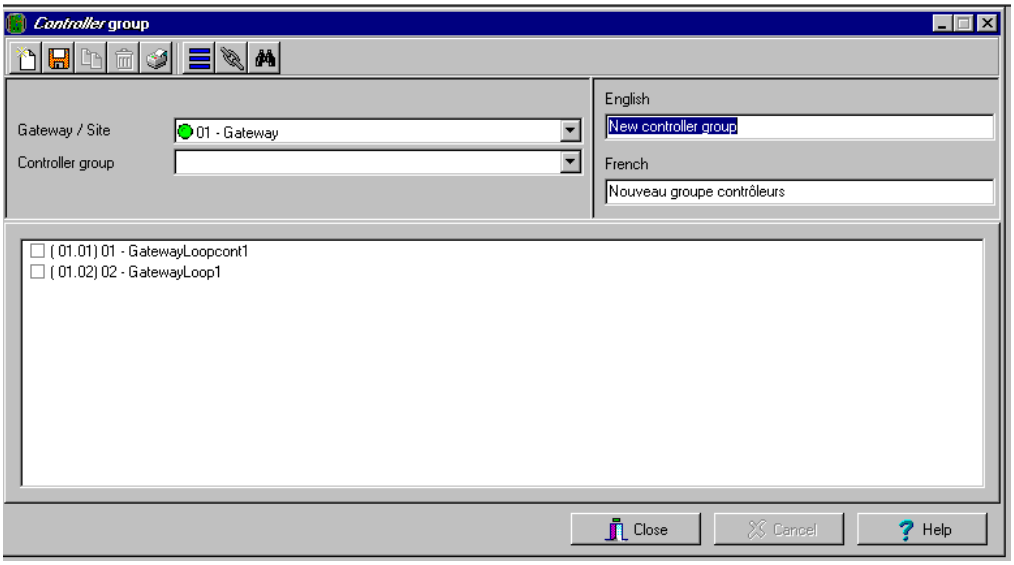
- Группы контроллеров
- Группы дверей
- Группы реле
- Группы входов
- Группы уровней доступа
- Группы этажей
- Группы областей

NOTE: *Когда выбран шлюз NCC 8000, Global или KT-NCC, то компоненты (контроллеры, входы, уровни доступа и пр.) группируются по шлюзу. Когда выбран Шлюз Corporate, тогда группировка происходит по лучу.*

Создание групп контроллеров

Для объединения нескольких контроллеров одного сайта в группу следует использовать меню Controller group (Группы контроллеров). Группой контроллеров затем можно, например, управлять в ручном режиме (например, выполнить повторную загрузку).

1 В окне Groups (Группы) нажать на иконку **Controller** (Контроллеры).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе.

3 В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт или шлюз, контроллеры которого необходимо объединить в группу.

4 Чтобы создать новую группу контроллеров, нажать кнопку **New** (Создать). Чтобы изменить существующую группу, выделить её в выпадающем списке **Controller group** (Группы контроллеров) и внести необходимые сведения об этой группе на используемых языках.

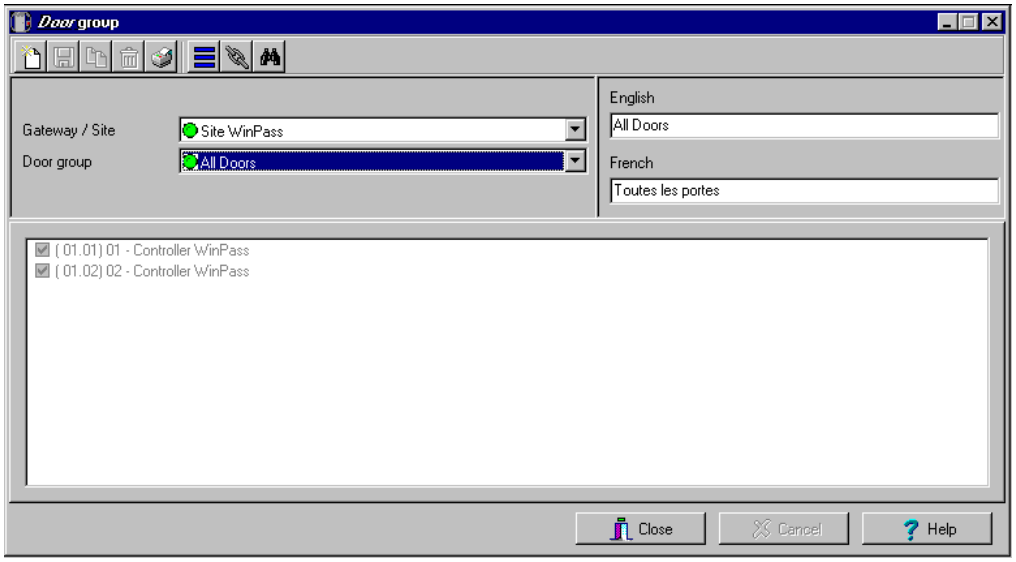
5 Из списка контроллеров, подключённых к выбранному сайту, выделить компоненты, которые должны быть объединены в группу.

NOTE: *Смотрите в Главе 4 Настройка конфигурации контроллеров' на странице 110 для более подробной информации по контроллерам.*

Создание группы дверей

Меню Door group (Группы дверей) служит для объединения дверей определённого сайта в группу. Затем этой группой дверей можно управлять в ручном режиме, например, отпереть все двери группы.

1 В окне Groups (Группы) нажать на иконку **Door** (Двери).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе.

3 В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт или шлюз, двери которого необходимо объединить в группу.

4 В выпадающем списке **Door Group** выбрать группу дверей, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой группы. Затем внести необходимые сведения об этой группе на используемых языках.

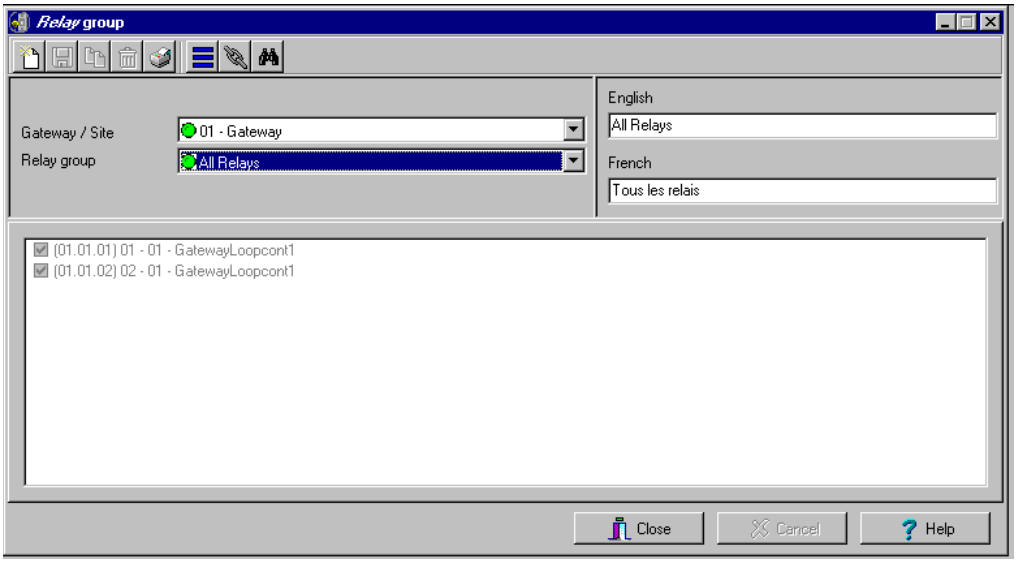
5 В списке дверей выбрать компоненты, которые должны быть включены в группу.

NOTE: *Смотрите в Главе 4 Конфигурация дверей' на странице 143 для более подробной информации о дверях.*

Создание групп реле

Меню Relay group (Группы реле) служит для объединения реле определённого сайта в группу. Затем этой группой реле можно управлять в ручном режиме, например, временно активировать все реле группы.

1 В окне Groups (Группы) нажать на иконку **Relay** (Реле).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе.

3 В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт или шлюз, реле которого необходимо объединить в группу.

4 В выпадающем списке **Relay Group** выбрать группу реле, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой группы. Затем внести необходимые сведения об этой группе на используемых языках.

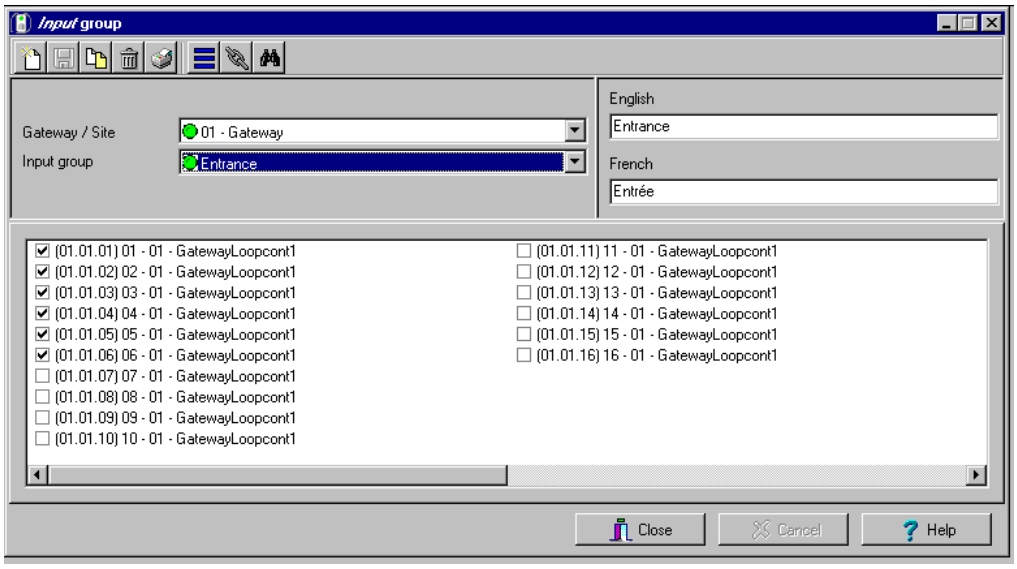
5 В списке реле выбрать компоненты, которые должны быть включены в группу.

NOTE: *Смотрите в Главе 4 Настройка реле' на странице 158 для более подробной информации о реле.*

Создание групп входов

Меню Input group (Группы входов) служит для объединения входов определённого сайта в группу. Затем этой группой входов можно управлять в ручном режиме, например, шунтировать все входы группы.

1 В окне Groups (Группы) нажать на иконку Input (Входы).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе.

3 В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт, входы которого необходимо объединить в группу.

4 В выпадающем списке **Inputs Group** выбрать группу входов, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой группы. Затем внести необходимые сведения об этой группе на используемых языках.

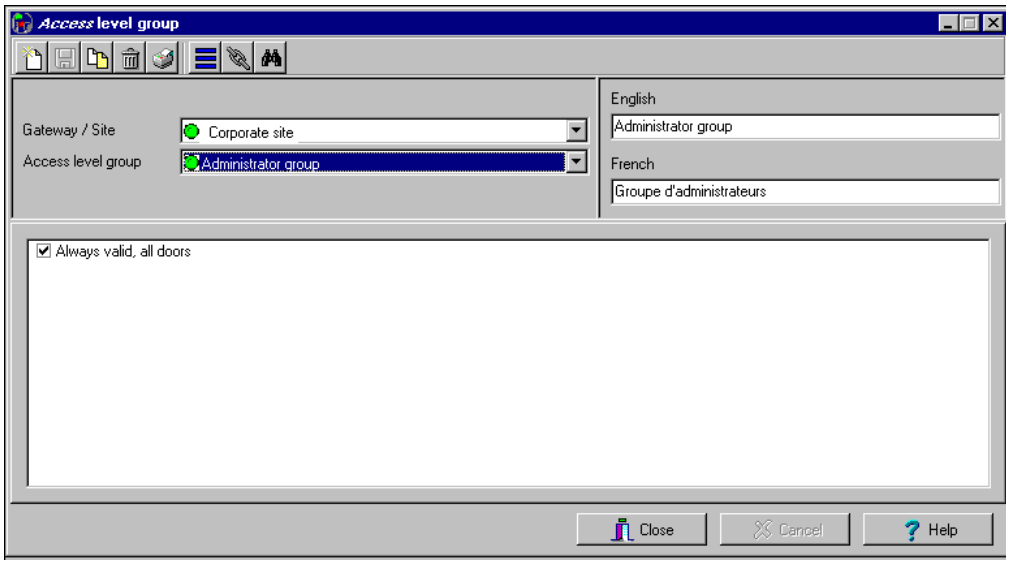
5 В списке входов выбрать компоненты, которые должны быть включены в группу.

NOTE: *Смотрите в Главе 4 Конфигурация входов (раздел Input)' на странице 160 для более подробной информации .*

Создание групп уровней доступа

Меню Access level group служит для объединения в группу разных уровней доступа на одном сайте.

1 В окне Groups (Группы) нажать на иконку **Access level group** (Группы уровней доступа).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе.

3 В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт или шлюз, уровни доступа которого необходимо объединить в группу.

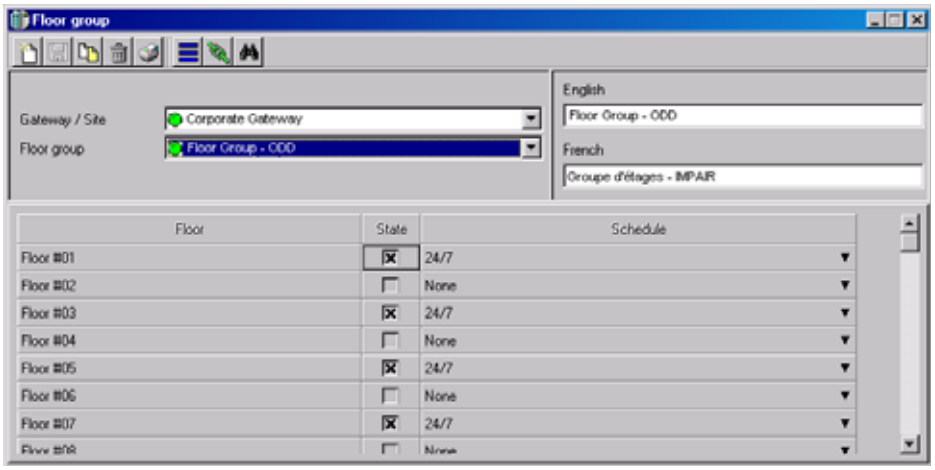
4 Нажать кнопку **New** (Создать) для создания новой группы и присвоить имя на используемых языках.

5 Отметить те уровни доступа, которые должны входить в указанную группу.

Создание групп этажей

Это меню служит для объединения в группы этажей, созданных в меню Floor Definition. Группы этажей используются при выполнении разных операций в системе, например, ручное управление (расписания разблокировки), уровни доступа и др.

1 В окне Groups (Группы) нажать на иконку **Floor/Elevator door** (Двери этажей/лифтов).



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все сайты, описанные в системе. В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить сайт или шлюз, этажи которого необходимо объединить в группу.

3 В выпадающем списке **Floor group** выбрать уже созданную группу, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой группы. Назначить группе имя в соответствующих полях для каждого применяемого языка.

4 В списке этажей, описанных в системе, отметить в колонке **State** (Статус) этажи, которые необходимо включить в группу. Только этажи, с отметкой в поле **State** будут доступны, когда:

- выполнена ручная разблокировка, или
- "вход" запрограммирован и действует, например, как нажимная кнопка для предоставления доступа на этажи посетителям (меню **Devices** > меню описания входов **Input** > закладка **Elevator**),
- Владельцы карт подносят карту к считывателю, чтобы получить доступ на этажи, когда контроллер работает в автономном режиме (из-за потери связи). Для выбора будут доступны только те этажи, которые отмечены флажком “X”.

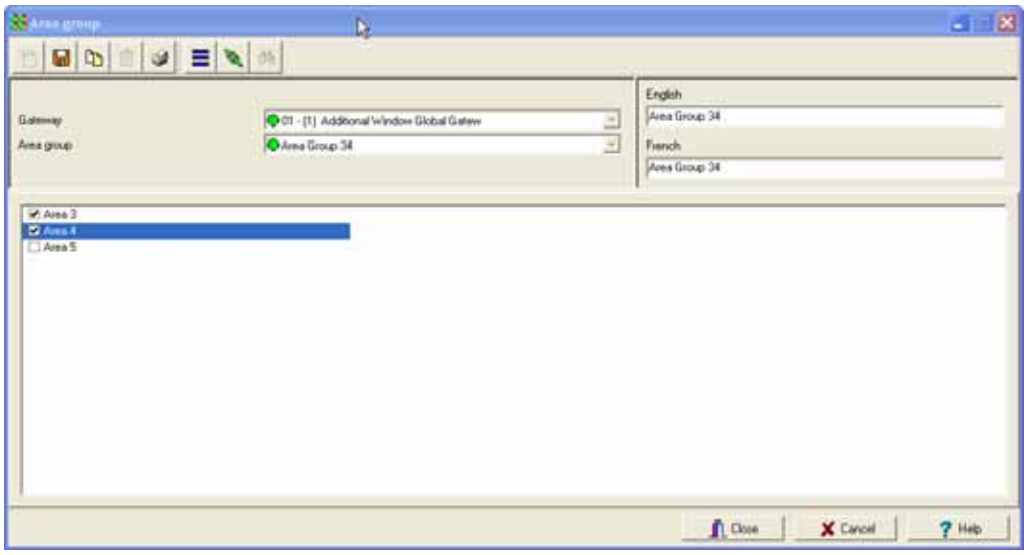
5 Only floors that have state selected will be enabled when:

- выполнена ручная разблокировка, или
- "вход" запрограммирован и действует, например, как нажимная кнопка для предоставления доступа на этажи посетителям (меню **Devices** > меню описания входов **Input** > закладка **Elevator**),
- Владельцы карт подносят карту к считывателю, чтобы получить доступ на этажи, когда контроллер работает в автономном режиме (из-за потери связи). Для выбора будут доступны только те этажи, которые отмечены флажком “X”.
- Расписание для каждого этажа назначено в колонке Schedule (расписание) (только шлюзы NCC 8000, Global).

Создание группы областей

Группа областей используется для контроля определенных областей для muster отчетов (отчет о сборе людей). Области должны быть настроенны в меню Area на вкладке **Definition** (Назначение),до того, как вы будете производить группировку.

1 Под вкладкой **Groups** (Группы), нажмите на иконку **Area group** (Группа областей) для открытия панели.



2 Нажать на кнопку **View hierarchy** (Посмотреть иерархию), чтобы вывести на экран все шлюзы, описанные в системе. В выпадающем списке **Gateway/Site** (Шлюз/Сайт) выделить шлюз, области которого необходимо объединить в группу.

3 В выпадающем списке **Area group** выбрать уже созданную группу, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой группы. Назначить группе имя в соответствующих полях для каждого применяемого языка.

4 Из списка назначенных областей, выберите области, которые вы хотите включить в группу областей.

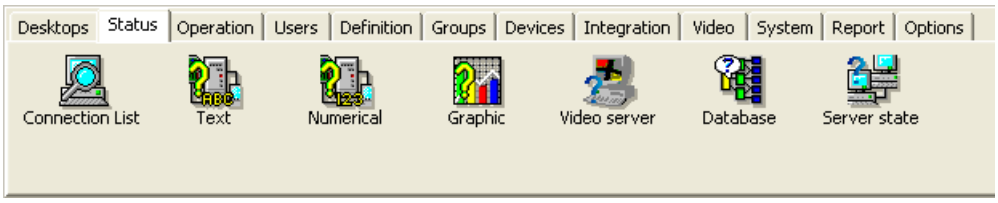
5 Нажмите иконку **Save** (Сохранить).

.

Глава 10 • :Состояние системы

Панель инструментов состояния

С помощью меню **Status** операторы могут просматривать состояния разных устройств и компонентов системы:



- Кнопка **Connection list** (Список соединений) предоставляет информацию о приложениях, зарегистрированных на сервере (имя оператора, локальная идентификация и др.).
- Кнопка **Text** (Текст) позволяет просматривать в текстовом формате статус приложений, шлюзов, сайтов, контроллеров (KT-100, KT-200 или KT-300), дверей, реле, входов. Отображаемый статус зависит от того, какой контроллер установлен.
- Кнопка **Numerical** (Цифры) позволяет просматривать статистическое состояние всех компонентов по выбранному шлюзу. Например, можно посмотреть число входов, находящихся в тревожном состоянии.
- Кнопка **Graphic** (Графика) служит для отображения графического состояния контроллера.
- Кнопка **Database** (База данных) предоставляет информацию о структуре базы данных. Кроме того, оператор может выполнить действия по настройке конфигурации или использовать команды ручного управления из окна базы данных.
- Кнопка **Video Server** (Видеосерверы) служит для отображения статусов, имеющих отношение к работе видеохранилища EntraPass Video Vault.

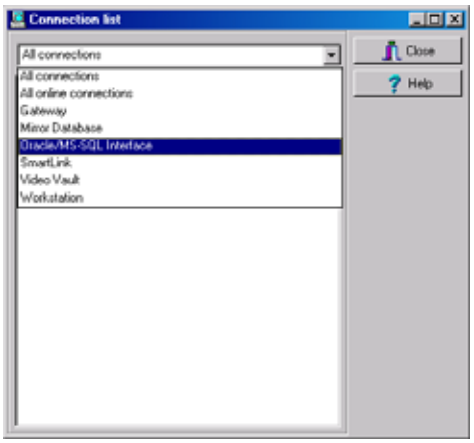
Список соединений (Connection List)

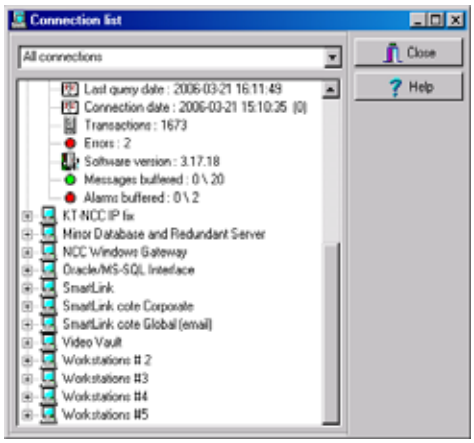
В окне Connection List (Список соединений) отображаются сведения о выделенном приложении, например, имя оператора, дата последнего запроса, локальный идентификационный номер и др. Кроме того, его можно использовать для проверки наличия связи между приложениями EntraPass и сервером.

Просмотр списка соединений системы

1 В окне Status (Статус) нажать иконку **Connection** (Соединения). Открывается окно **Connection list**.

Выпадающий список содержит все приложения и позволяет просматривать их все сразу или по отдельности. Можно выделить все приложения (All connections) или один определённый шлюз и посмотреть параметры соединения для выделенного(ых) приложения(й).





2 Чтобы увидеть подробную информацию о приложении, следует нажать

- **Красная** метка указывает на отсутствие связи между приложением и сервером.
- **Зелёная** метка означает, что приложение EntraPass подключено к серверу.
- **Protocol** (Протокол) – отображает протокол (язык), который используется для связи с сервером. Протокол оповещает систему о том, как осуществлять обмен данными между компьютерами.
- **Local identification** (Локальная идентификация) – устанавливает название приложения в сети. Это имя используется сервером для идентификации приложения.
- **Network identification** (Сетевая идентификация) – предоставление IP-адреса приложения в сети или имени компьютера по протоколу NetBEUI.
- **Operator name** (Имя оператора) – отображает имя оператора, зарегистрированного в текущий момент в этом приложении. Имя оператора используется для выполнения разных задач, например, чтобы определить, кто внёс изменения в карту, кто подтвердил тревогу и др. *Смотрите в Главе 12 Назначение операторов' на странице 402 для более подробной информации* о том, как сменить имя оператора.
- **Last query date** (Дата последнего запроса) – отображает время последнего опроса приложения с сервера. Сервер и приложение регулярно обмениваются данными.
- **Connected date** (Дата подключения) – отображает дату и время, в которые было установлено соединение приложения с сервером. Эта дата может быть использована для формирования события и для хранения в архивах.
- **Transactions** (Транзакции) – отображает число запросов, выполненных приложением (число обменов данными с сервером), в частности, запросы отчётов.
- **Errors** (Ошибки) – число ошибок, обнаруженных приложением. При отключении приложения счётчик ошибок обнуляется.
- **Messages/Alarms buffered** (Число сообщений/тревог в буфере) - 0/1

- **0:** число сообщений/тревог, хранящихся в буфере на сервере для этого приложения, когда с этим приложением нет связи. Это число становится равным нулю, когда связь между приложением и сервером восстанавливается, и сообщения передаются приложению.
- **1:** число сообщений/тревог, отправленных данному приложению с момента подключения сервера. Если сервер отключается, этот счётчик сбрасывается на ноль.

NOTE: *В буферной памяти сервера может храниться до 100 000 сообщений и 100 000 тревог на каждую рабочую станцию EntraPass (по умолчанию 5 000). Эти настройки можно изменить в меню назначения рабочей станции (Workstation Definition). Кроме того, можно указать, какие сообщения следует сохранять в буфере в случае его переполнения: новые или старые. Сообщения сохраняются в буферной памяти только при условии, что рабочая станция отключена от сети (не подключена к серверу); и что поля "Apply operator parameters for messages" (Применить параметры оператора к сообщениям) и "Apply operator parameters for alarms" (Применить параметры оператора к тревогам) не помечены флажком. Смотрите в Главе 4 Конфигурация приложений EntraPass' на странице 64 для более подробной информации).*

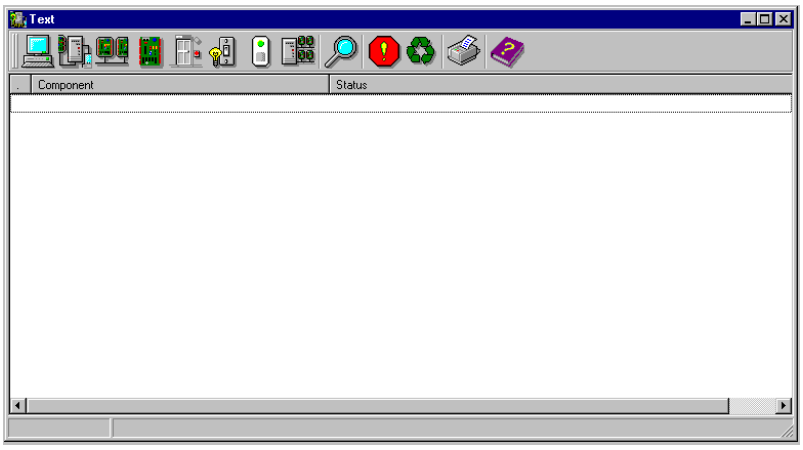
Состояние текста

Окно **Text status** (состояние текста) позволяет отобразить состояние выбранного компонента (и его составляющих), а также все характеристики, используемые для описания этого компонента, в текстовой форме. Эта функция применяется ко всем устройствам системы: приложениям, шлюзам, сайтам, контроллерам, дверям, реле и входам. Текстовое окно имеет дополнительные кнопки/иконки для выполнения следующих задач:

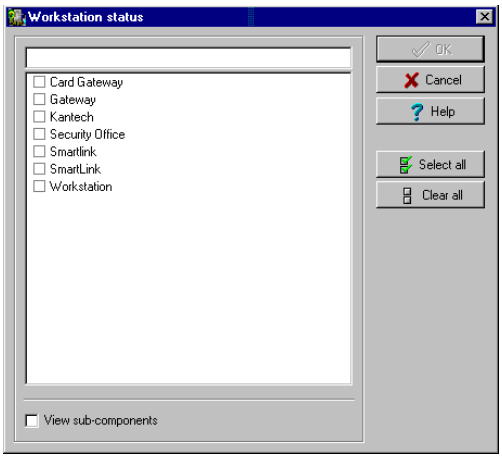
- Первые восемь кнопок представляют устройства системы: Workstation (Рабочие станции), Gateway (Шлюзы), Site (Сайты), Controller (Контроллеры), Door (Двери), Input (Входы) и Output (Выходы). Когда кнопка, представляющее системное устройство выбрана, то все компоненты, назначенные в системе отображены для выбора.
- **Summary / Detailed list** (Сводка/Подробный список) – иконка лупы служит для отображения компонентов, статус которых отличается от нормы. В этом окне отображается сводный список или подробный перечень.
  - Summary (Сводный список) – показывает компоненты, статус которых отличается от нормы.
  - Detail (Подробный список) – показывает все компоненты, независимо от их статуса.
- **Stop display** (Остановить вывод на экран) – используется, чтобы остановить вывод на экран слишком большого объёма данных. Выполняется отмена или прерывание процесса.
- **Refresh** (Обновить) – обновляет статус выбранных компонентов.
- **Print** (Печать) – служит для вывода на печать отображаемого состояния. Функция Preview позволяет посмотреть получившийся список на экране перед выводом на печать.

Вывод на экран состояние компонентов

1 В меню **Status** (состояние) нажать кнопку **Text Status** (Текстовое состояние). Открывается окно Text (Текст).



2 В окне Text выделить иконку компонента, статус которого необходимо показать. Если выделена иконка **Workstation** (Рабочая станция), система выведет на экран список приложений EntraPass, описанных в системе.



3 Оператор может выделить нужное приложение EntraPass флажком или указать в верхней строке окна несколько символов, входящих в состав его имени, чтобы выполнить поиск в базе данных. Например, вместо "Security Office" (Служба безопасности) оператор может набрать только "Sec". Система выделит первое слово, содержащее введённые символы. Если необходимо выделить все компоненты, следует воспользоваться кнопкой **Select all** (Выделить все). Чтобы выделить некоторые компоненты, следует поставить флажок напротив каждого из них. Чтобы снять выделение со всех выбранных компонентов, следует нажать **Clear all** (Очистить все). Для возврата к предыдущему экрану меню без внесения изменений и без выделений следует нажать кнопку **Cancel** (Отмена).

4 Чтобы получить подробные сведения о составляющих выделенного компонента, необходимо поставить флажок в поле **View sub-components** (Посмотреть составляющие компонента) – в нижней части окна. Например, если флажком отмечен контроллер, то при выделении этой функции все компоненты контроллера (двери, реле, входы) с соответствующим статусом будут отображаться в этом окне. Позволяет собрать в одном окне все компоненты и отсортировать двери, реле или входы по сайтам.

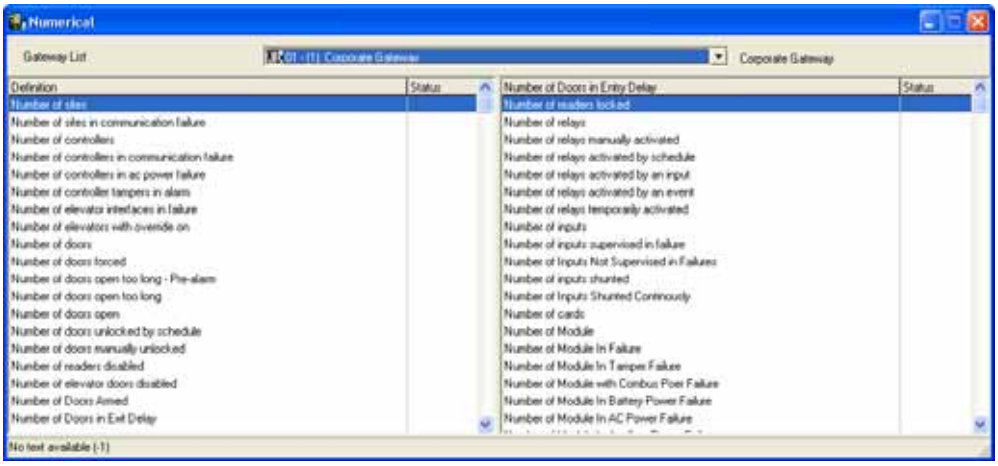
5 Для возврата к предыдущему окну с использованием выделенных опций и подтверждение вашего выбора нажать **OK.**

NOTE: *Кнопка* ***Magnifying glass*** *(Экранная лупа) служит для отображения компонентов, статус которых отличается от нормы. В положении "Summary" отображаются только те компоненты, состояние которых отличается от нормы. В положении "Detailed" система отображает полное состояние всех компонентов.*

Цифровой статус (Numerical Status)

Это меню позволяет определить число компонентов для указанного шлюза, статус которых отличается от нормального.

1 В меню **Status** (Статусы) нажать кнопку **Numerical Status** (Цифровой статус). Открывается окно Numerical.



2 В выпадающем списке **Gateway** (Шлюзы) выделить шлюз, для которого необходимо отобразить состояние. В открывшемся окне будет показано число карт для выбранного шлюза, число входов в тревоге, число активированных вручную реле, число принудительно открытых дверей и др. Эту функцию очень удобно использовать для определения числа описанных в системе карт.

Графический статус (Graphic Status)

Данная функция служит для отображения графического статуса контроллера дверей, включая состояние всех его компонентов (выходов, входов, подачи питания, наличия связи и пр.), в виде различных геометрических фигур разного цвета (кругов, прямоугольников и т.п.).

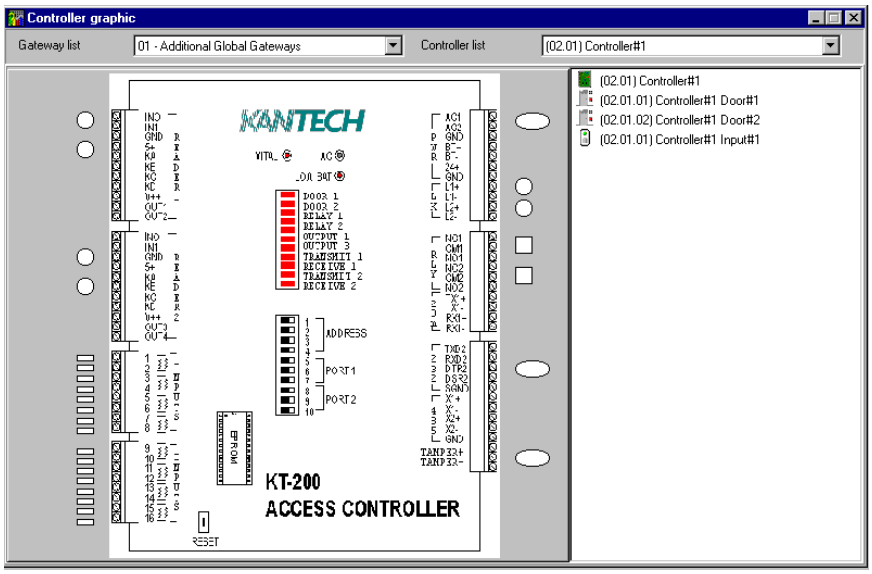
- Контроллер изображён в виде эллипса.
- Двери показаны кругами.
- Реле изображается в виде квадрата.
- Прямоугольником обозначены входы. Прямоугольники могут быть ориентированы горизонтально (KT-200 и KT-300) или вертикально (KT-100).

Просмотр состояние контроллера

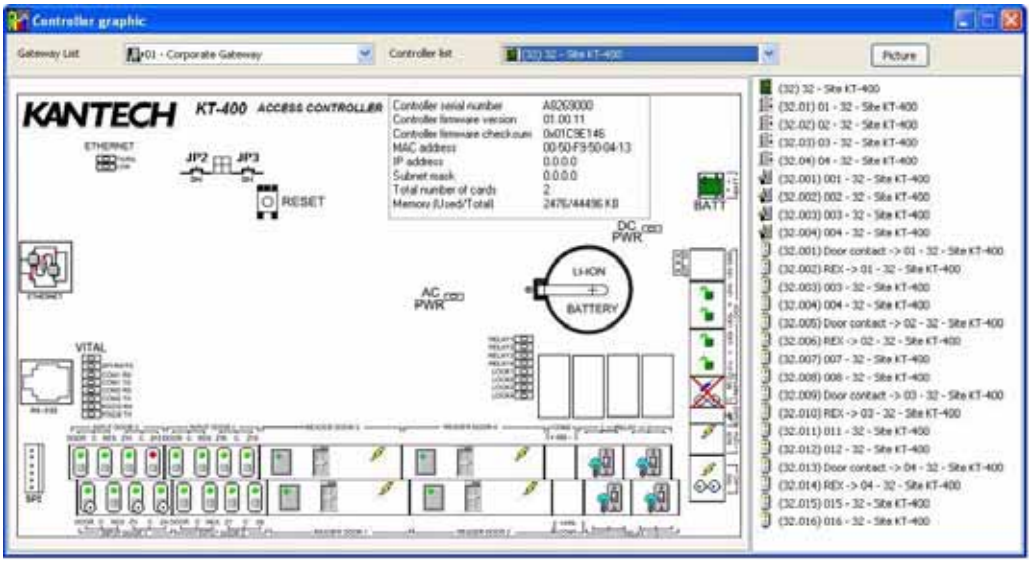
1 В выпадающем списке **Gateway** (Шлюзы) выделить шлюз, на котором расположен проверяемый контроллер. Для отображения всех контроллеров в списке следует использовать кнопку “All gateways” (Все шлюзы).

2 В выпадающем списке **Controller** (Контроллеры) выделить контроллер, для которого необходимо показать статус.

На примере контроллера KT-200



На примере контроллера KT-400



NOTE: Внешний вид схемы зависит от типа выбранного контроллера.

3 Чтобы выяснить, что обозначает тот или иной элемент схемы, следует поместить курсор на этот элемент. Выделенный таким образом компонент будет отмечен другим фоном в списке справа.

4 Выделить контроллер в списке **Controller list** (справа), щёлкнуть дважды по компоненту, статус которого необходимо определить.

- **Красный** – компонент находится под контролем, но в неисправном состоянии.
- **Зелёный** – компонент находится под контролем и в исправном состоянии.
- **Жёлтый** – неконтролируемый компонент в неисправном состоянии.
- **Серый** – неконтролируемый компонент в исправном состоянии.
- **Синий** – реле активировано (в результате события или по команде оператора).

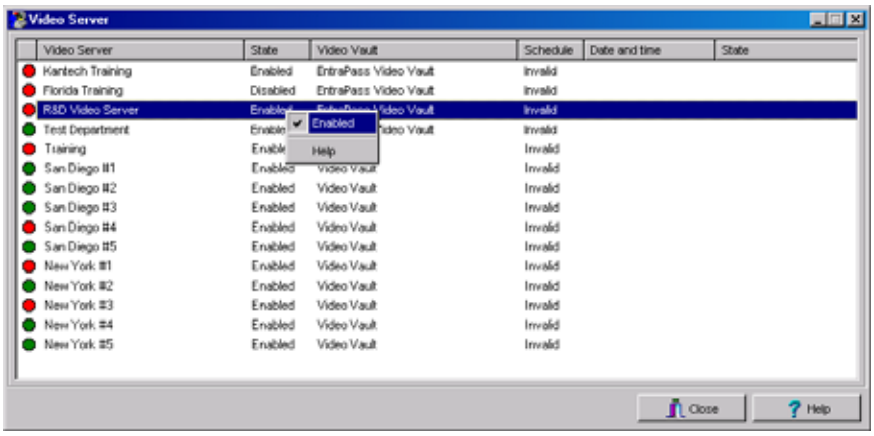
NOTE: *Если на один шлюз приходится более одного луча/сайта на Шлюз, то число в скобках (xx) указывает номер контроллера, а остальные цифры обозначают номер компонента.*

Состояние видеосерверов

Эта опция используется для контроля состояния видеосерверов, участвующих в процессе архивирования данных в видеохранилище EntraPass Video Vault. Опция **Video Server** (Видеосерверы) доступна из меню **Status** (Статусы). В окне Video Server отображаются все видеосерверы и их состояния.

Просмотр состояния видеосервера

1 Нажать иконку **Video Server** (Видеосерверы), предварительно открыв закладку **Status** (Состояние). В открывшемся окне Video Server будут отображаться все видеосерверы и их состояния.



- **State** (Состояние) – разрешение (Enabled) или запрет (Disabled) на создание видеоархивов
- **Video Vault** (Видеохранилище) – связь с видеохранилищем EntraPass Video Vault
- **Schedule** (Расписания) – достоверное (Valid) или недостоверное (Invalid) расписание для создания архивов
- **Date and Time** (Дата и время) – дата и время последней транзакции этого видеосервера с видеохранилищем EntraPass Video Vault
- **State** (Состояние) – описание последней транзакции этого видеосервера с видеохранилищем EntraPass Video Vault

Разрешение/запрет создания видеоархивов

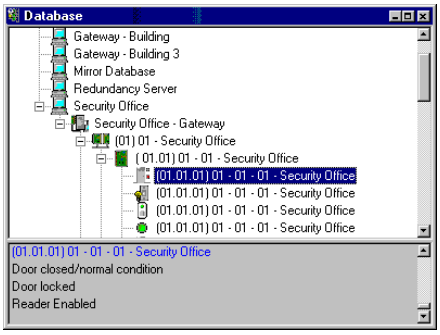
NOTE: *Эта опция доступна только в случае установки видеохранилища EntraPass Video Vault.*

1 Правой кнопкой мыши выделить сервер, для которого требуется разрешить/запретить создание видеоархивов.
   - В контекстном меню выбрать **Enable** (Разрешить), чтобы включить архивирование.
   - Или выбрать в контекстном меню **Disable** (Запретить), чтобы прекратить архивирование.

Состояние баз данных

В этом окне вместе с изображением структуры базы данных показаны статусы всех её компонентов. Отображаются все приложения (подключенные и неподключенные), шлюзы, сайты/лучи с контроллерами и др. Система позволяет управлять всеми компонентами в ручном режиме непосредственно из этого окна, а также изменять их конфигурацию.

1 В окне Status выделить иконку **Database** (База данных). Откроется окно Database.

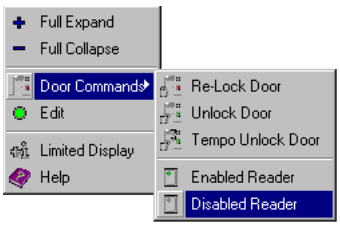


***NOTE:** Иконки соответствуют типу компонентов.*

2 В окне Database выделить нужное приложение. В нижней части окна отображается фактический статус выбранного компонента, а также его полное имя.

3 Чтобы изменить параметры компонента, выделить его прямо в окне Database. Допустим, выделена дверь (door). Щелчком правой кнопки мыши по выделенному компоненту вызвать контекстное меню.

4 В открывшемся каскадном меню вызвать нужную команду.



***NOTE:** Список команд в контекстном меню будет разным для разных компонентов.*

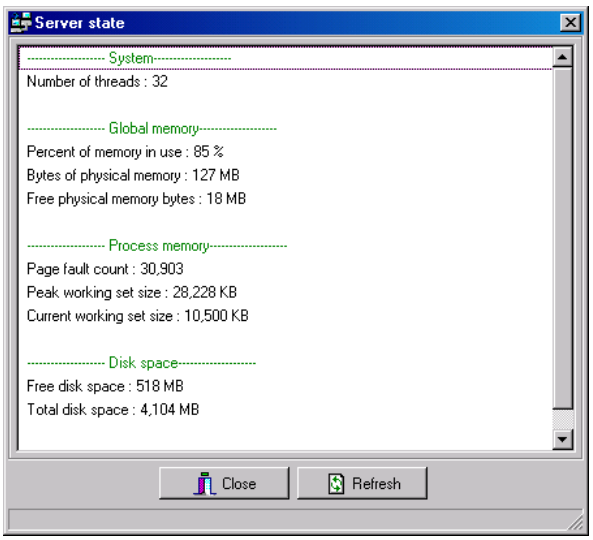
5 Внести необходимые изменения, чтобы вернуться в окно Database status (Состояние базы данных). В контекстном меню, вызываемом **правой кнопкой мыши**, доступны следующие команды:

- **Full expand** (Развернуть) – эта функция позволяет полностью развернуть все ветви схемы, чтобы увидеть все компоненты. Со знаком "+" будут отображаться только те приложения, которые подключены к серверу.
- **Full collapse** (Свернуть) – эта функция позволяет полностью свернуть схему, чтобы спрятать все составляющие корневого компонента.
- **Edit** (Редактировать) – выделив включённый в схему компонент (например, вход) и вызвав меню редактирования, оператор вносит изменения в назначение этого компонента в открывшемся окне описаний. После завершения редактирования данных возвращается в исходное меню.
- **Limited display / No limited display** (Ограничить/Не ограничивать отображаемые данные) – в нижней части окна отображается статус компонента, выделенного щелчком мыши.
- При выборе опции **Limited display** система удаляет предыдущий статус и отображает статус следующего выделенного компонента.

***NOTE:** Пиктограммы, расположенные слева от компонентов, указывают их тип.*

Состояние сервера (Server State)

Окно Server state содержит подробные сведения о сервере, а именно: системные данные (System), характеристики глобальной памяти (Global memory), сведения об оперативной памяти (Process memory) и ёмкости диска (Disk space).

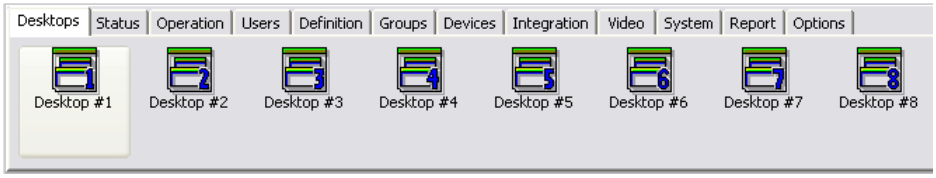


Глава 11 • Рабочие столы EntraPass

Панель инструментов DESKTOPS/РАБОЧИЕ СТОЛЫ

Рабочие столы предназначены для получения и отображения на экране сообщений о событиях (текущих или архивных), индикации тревог, просмотра фотографий владельцев карт, графических схем системы и пр. Рабочий стол также может быть использован для подтверждения о получении тревожных сообщений, отображения инструкций оператору и пр. В данной системе предусмотрено восемь (8) рабочих столов с предварительной настройкой. Их можно описать следующим образом:

Рабочие столы предназначены для получения и отображения на экране сообщений о событиях (текущих или архивных), индикации тревог, просмотра фотографий владельцев карт, графических схем системы и пр. Рабочий стол также может быть использован для подтверждения о получении тревожных сообщений, отображения инструкций оператору и пр. В данной системе предусмотрено восемь (8) рабочих столов с предварительной настройкой. Их можно описать следующим образом:



- Рабочий стол 1: Все системные события
- Рабочий стол 2: Системные события и фотографии
-
- Рабочий стол 3: Избранные/Отфильтрованные события системы
- Рабочий стол 4: Избранные/Отфильтрованные сообщения системы и фотографии и др.
- Рабочий стол 5: Окно тревог
- Рабочий стол 6: Графический дисплей
- Рабочий стол 7: Окно сетевых тревог
- Рабочий стол 8: Видеонаблюдение (если в EntraPass разрешено использовать функцию Video).

Перечислим окна, которые можно комбинировать с другими рабочими столами:

- Инструкции оператору
- Фотографии
- Архивные отчёты

Система позволяет выводить на экран несколько окон одновременно. В зависимости от назначенного уровня безопасности, операторы могут изменять настройки каждого из перечисленных окон (цветовой фон, размеры, панели инструментов и др.). Однако операторы не смогут изменять, перемещать, разворачивать или сворачивать рабочие столы, для которых у них назначен уровень "только для чтения" (read-only).

ПРИМЕЧАНИЕ: *Изменять настройки рабочих столов по своему усмотрению могут только операторы с соответствующим уровнем безопасности (доступа) (закладка* **System** *(Системные настройки) >* **Security Level** *(Уровни безопасности). У них также есть возможность разрешить операторам со статусом "Read-only" (Только для чтения) изменять настройки своих рабочих столов. Но в этом случае изменения будут действовать только в текущей сессии!*

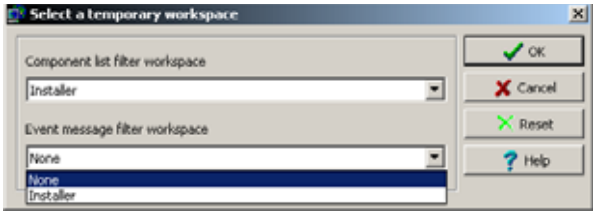
Индивидуальная настройка рабочего пространства

Система EntraPass позволяет операторам, имеющим соответствующие права, по своему желанию настраивать своё рабочее пространство, создавать временное рабочее пространство и изменять свойства рабочих столов. Уровни безопасности для операторов назначаются в разделе **System** (Системные настройки) > **Security Level** (Уровни безопасности).

Создание временного рабочего пространства

1 В окне Desktop (Рабочие столы) щёлкнуть правой кнопкой мыши ниже строкой меню.

2 Выбрать в контекстном меню пункт Select a temporary workspace (Выбрать временное рабочее пространство).

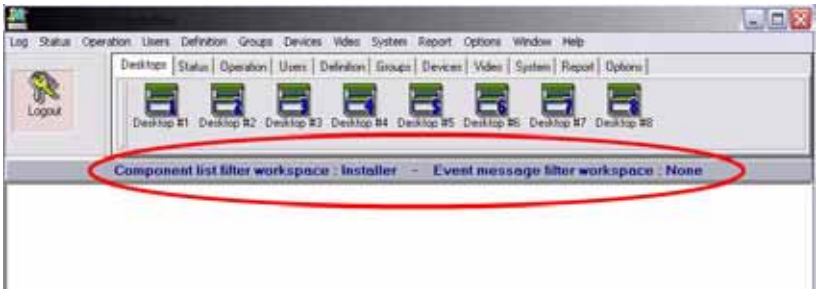


3 Выбрать необходимое в списках **Component list filter workspace** (Рабочее пространство с избранным списком компонентов)) и **Event message filter workspace** (Рабочее пространство с избранными сообщениями о событиях).

- **Component list filter workspace** (Рабочее пространство с избранным списком компонентов) – позволяет отобрать особый список компонентов в действующем рабочем пространстве.
- **Event message filter workspace** (Рабочее пространство с избранными сообщениями о событиях) **(по желанию)** – позволяет отобрать из действующего рабочего пространства только что поступившие сообщения, не лежавшие в буфере.

ПРИМЕЧАНИЕ: *Во временном рабочем пространстве обязательно должен выполняться отбор по* ***Component list filter workspace****. Если будет использован только фильтр* ***Event message list filter workspace****, заголовок временного рабочего пространства не будет отображаться на экране.*

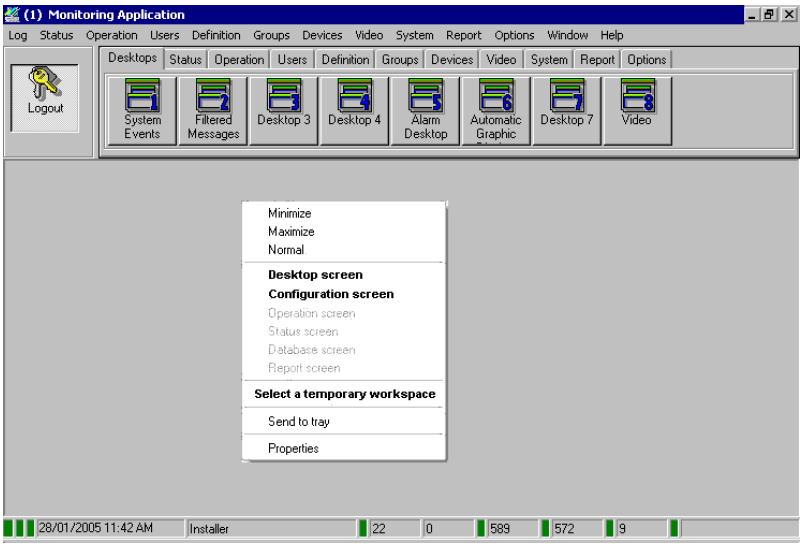
4 Нажать **OK**. На экран будет выведен заголовок временного рабочего пространства с именами используемых фильтров.



5 Для возврата к первоначальному рабочему пространству необходимо снова выполнить **пункты 1 – 4** или дважды щёлкнуть по заголовку, чтобы создать или изменить временное рабочее пространство.

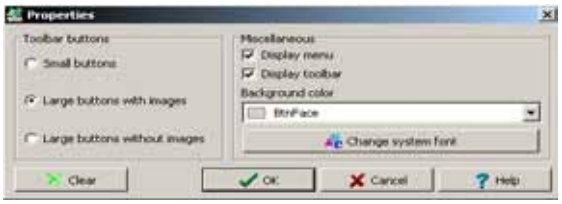
Изменение свойств экрана

1 В окне Desktop (Рабочие столы) щёлкнуть правой кнопкой мыши в любом месте окна.



2 В открывшемся контекстном меню выбрать пункт **Properties** (Свойства).

3 В появившемся на экране окне Properties указать необходимые настройки экрана: изменить при необходимости размер кнопок, выбрать другой цвет фона и др.



- **Small buttons** (Малые кнопки) – отображаются небольшие кнопки без текстовой подсказки. Рекомендуется использовать операторам, хорошо знакомым с интерфейсом EntraPass и не нуждающимся в дополнительных описаниях.
- **Large buttons with images** (Большие кнопки с изображениями) – отображение пиктограмм вместе с описанием.
- **Large buttons without images** (Большие кнопки без изображений) – большие кнопки, пиктограммы на кнопках не отображаются.
- **Display menu** (Показывать меню) – отображение на экране системного меню.
- **Display toolbar** (Показывать панель инструментов) – отображение панели инструментов для системного меню.
- **Background color** (Цветовой фон) - указать цветовой фон всего рабочего пространства.
- **Change system font** (Изменить системный шрифт) – изменить шрифт для всех интерфейсов пользователя.

Индивидуальная настройка специальных рабочих столов

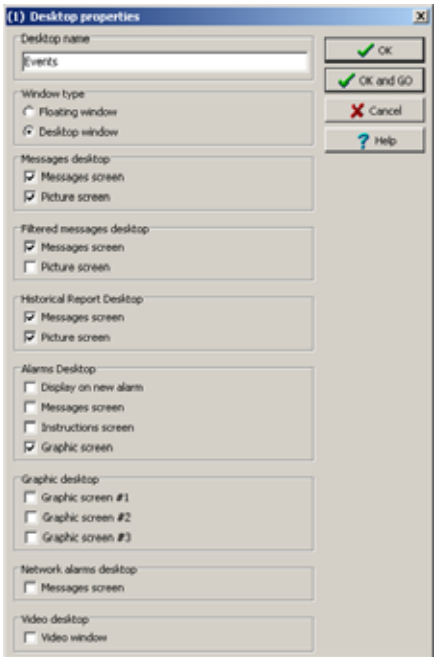
Система EntraPass позволяет операторам, имеющим соответствующие права, настраивать рабочие столы по своему желанию. Помимо этого, операторы с полным доступом могут разрешать операторам с доступом "только для чтения" индивидуально настроить свои рабочие столы. Они также могут настраивать специальные рабочие столы и передавать эти настройки другим операторам при помощи функции Assign desktop (Назначить рабочий стол). Далее даются объяснения, как индивидуально настроить рабочие столы:

- Индивидуальная настройка рабочего стола оператором с полным доступом
- Индивидуальная настройка рабочего стола для оператора с доступом "только для чтения"
- Передача индивидуально настроенного рабочего стола

Индивидуальная настройка рабочего стола оператором с полным доступом

Операторы с полным доступом имеют право настраивать рабочие столы по своему усмотрению. Для того чтобы наделить оператора полным доступом, следует войти в меню **System** (Системные настройки) > **Security Level** (Уровни безопасности).

1 Выделить рабочий стол, который необходимо индивидуально настроить, вызвать контекстное меню правой кнопкой мыши, выбрать в меню пункт **Properties** (Свойства), чтобы открыть окно Desktop properties (Свойства рабочего стола).



2 В поле **Desktop name** (Имя рабочего стола) присвоить настраиваемому рабочему столу содержательное имя.

3 Указать тип окна в разделе Window type:
   - **Floating window** (Плавающее окно) – плавающие окна можно помещать в любом месте рабочего пространства и изменять по размеру. В частности, можно указать, что эти окна должны находиться поверх всех других окон или на заднем плане. Если плавающее окно находится на заднем плане, его можно переместить на передний план, вызвав контекстное меню щелчком правой кнопки мыши (функция **Bring to front**).
   - **Desktop window** (Окно рабочего стола) – это окно нельзя вынести за пределы рабочего пространства. Отправить такое окно на задний план невозможно. Он всегда остаётся в пределах главной рабочей области.

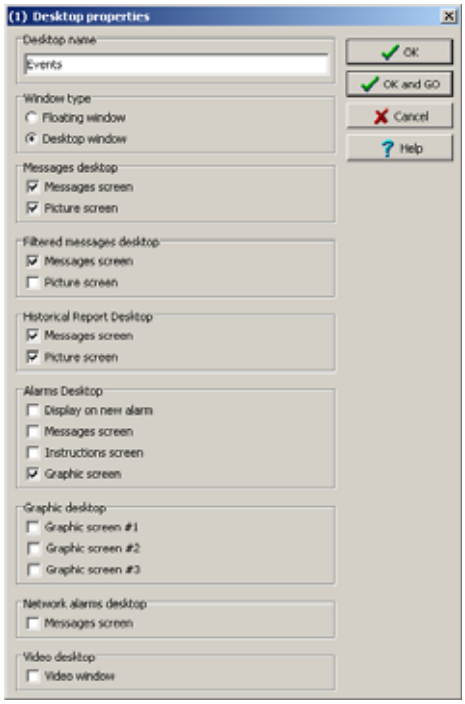
4 Сохранение изменений.
   - Кнопка **OK** – служит только для сохранения изменений, без отображения окна.
   - Кнопка **OK & GO** – служит для сохранения изменений и отображения на экране только что настроенного окна.

ПРИМЕЧАНИЕ: *При открытии окна рабочего стола в первый раз для правильного отображения информации может потребоваться изменить его размеры. Для этого следует установить курсор мыши на край рамки и после того как курсор превратится в двунаправленную стрелку, растянуть окно до нужного размера. После этого следует переместить окно в нужное положение в пределах рабочей области.*

Индивидуальная настройка рабочего стола для оператора с доступом "только для чтения"

Руководитель службы безопасности или оператор, наделённый соответствующими полномочиями, может разрешить операторам с более низким уровнем безопасности изменить их рабочий стол на время текущей сессии.

1. Войти в систему, используя имя и пароль оператора с полным доступом.
2. Выделить рабочий стол, который необходимо индивидуально настроить, вызвать контекстное меню правой кнопкой мыши, выбрать в меню пункт **Properties** (Свойства), чтобы открыть окно Desktop properties (Свойства рабочего стола).



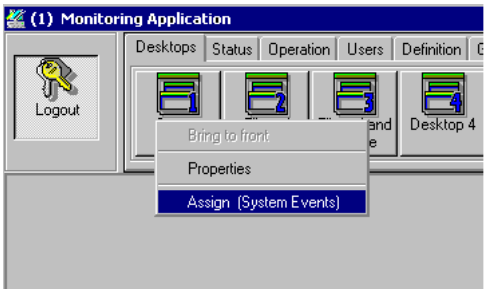
ПРИМЕЧАНИЕ: *Кнопка **Permit** (Разрешить) появляется, если зарегистрировавшийся в системе оператор имеет доступ "только для чтения". Разрешение действует только на время текущей сессии, пока оператор не выйдет из системы.*

3. Нажать кнопку **Permit** (Разрешить). Открывается окно Operator Login (Регистрация оператора). Ввести имя пользователя в поле User name и пароль в поле Password. Нажать **OK**. После этого система предоставляет временное разрешение.

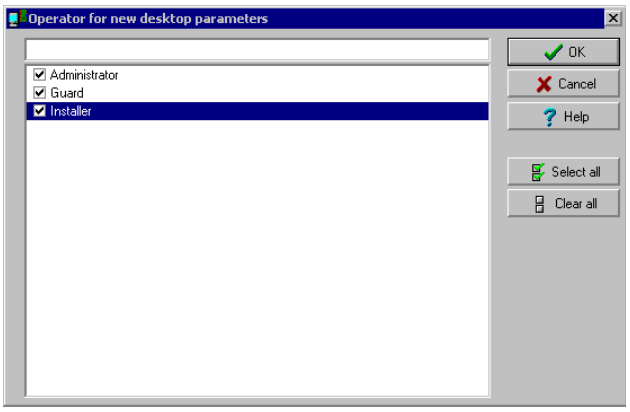
Передача индивидуально настроенного рабочего стола

Ещё одна привилегия, предоставляемая руководителю службы безопасности (или оператору, наделённому соответствующими полномочиями), заключается в возможности настроить рабочий стол по своему усмотрению и затем назначить те же настройки другим операторам, не имеющим прав изменять свои настройки рабочего стола из-за низкого уровня доступа.

1 Правой кнопкой мыши щёлкнуть по рабочему столу, настройки которого следует поменять.



2 Выбрать в появившемся контекстном меню опцию **Assign (desktop)** (Назначить (рабочий стол)).



3 В открывшемся окне указать, каким операторам назначить текущие свойства рабочего стола (выделить флажком соответствующие поля). Выделять можно по одному оператору или сразу всех кнопкой **Select all** (Выделить все).

Рабочий стол сообщений (Message Desktop)

По умолчанию первый рабочий стол служит для вывода на экран сообщений и называется **Messages List** (Список сообщений). Он содержит все системные события. Каждое событие отображается вместе с особой пиктограммой, датой и временем, описанием и компонентами, связанными с этим событием (контроллерами, фотографиями владельцев карт (при их наличии) и пр.). При выводе на экран нового события список прокручивается вверх. Новые события добавляются в конец списка (внизу окна).

Просмотр и сортировка системных событий

По умолчанию первый рабочий стол служит для отображения системных событий. Выделив в списке какое-либо событие, оператор прерывает последовательность поступления новых событий (автоматическое пролистывание событий по мере их поступления прекращается, и зелёный индикатор, расположенный в левом нижнем углу рабочего стола, становится красным). По умолчанию пролистывание автоматически возобновляется через определённый установленный период времени, если эта функция не отключена в настройках. В этом случае для возобновления пролистывания в обычном режиме следует нажать кнопку **Restart Scroll** (Возобновить пролистывание).

ПРИМЕЧАНИЕ: *Если в настройках рабочий стол описан как окно сообщений и окно изображений, то при его выборе отображаются одновременно два окна.*

1 Выбрать первый рабочий стол. По умолчанию все системные события отображаются в порядке поступления; в нижней строке окна выдаётся информация о выделенном в списке событии.

ПРИМЕЧАНИЕ: *Цвет текста в сообщении можно изменить в меню:* ***System*** *(Системные настройки) >* ***Events parameters*** *(Параметры событий). Кроме того, можно изменить порядок отображения сообщенийю. Смотрите в Главе 11 Индивидуальная настройка экрана событий для стола сообщений Message' на странице 374 для более подробной информации .*

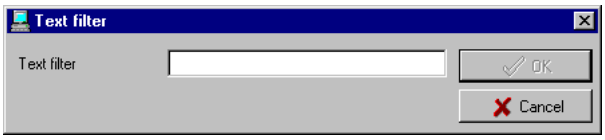
2 В окне Message list (Список событий) есть возможность изменить критерий сортировки сообщений (функция **Sorted by**). Сообщения можно сортировать по следующим критериям:

- **Sequence** (Последовательно) – сообщения выдаются в обычной последовательности (используется по умолчанию). Новые события добавляются в конец списка (в нижней части окна). (Эта функция недоступна для списков архивных сообщений Archived Messages Lists).
- **Date and time** (Дата и время) – при такой последовательности сортировки стандартное пролистывание событий не работает. Эта функция используется, чтобы узнать, когда произошло событие. Это время может отличаться от "стандартной последовательности" событий, например, при работе с сайтами, связь с которыми осуществляется по коммутируемой линии, или после сбоя в подаче питания.
- **Event** (События) – при использовании этой опции система сортирует события в колонке **Event message** (Сообщения о событиях), выстраивая их в алфавитном порядке и группируя *идентичные* события. Например, все события **Input in alarm** (Вход переведён в статус тревоги) будут сгруппированы вместе и выстроены в алфавитном порядке.
- **Message type** (Тип сообщения) – при выборе этой опции система сортирует события в колонке **Event message** (Сообщения о событиях), выстраивая их в алфавитном порядке и

группируя *схожие* события. Например, все события **Site** (Сайт/Луч) будут сгруппированы вместе и выстроены в алфавитном порядке.

ПРИМЕЧАНИЕ: *Чтобы вернуться к отображению списка событий с настройками по умолчанию, следует выбрать в выпадающем списке* **Sorted by** *(Способ сортировки) опцию* **Sequence** *(Последовательность).*

3 Кнопкой **Text filter** (Текстовый фильтр), расположенной в верхней части окна, открыть меню Text filter. В поле Text filter ввести ключевое слово, чтобы вывести на экран все сообщения из списка Message list, которые содержат это ключевое слово.

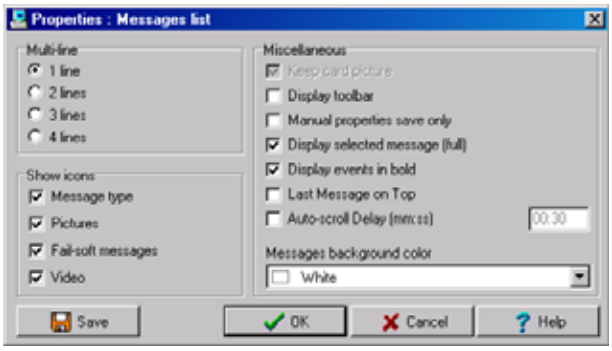


Чтобы закрыть окно Text filter, нажать **Cancel** (Отмена) или закрыть окно кнопкой (X).

4 Чтобы вернуться к нормальному режиму отображения сообщений в окне Messages list, нажать кнопку **Text filter.**

Индивидуальная настройка экрана событий для стола сообщений Message

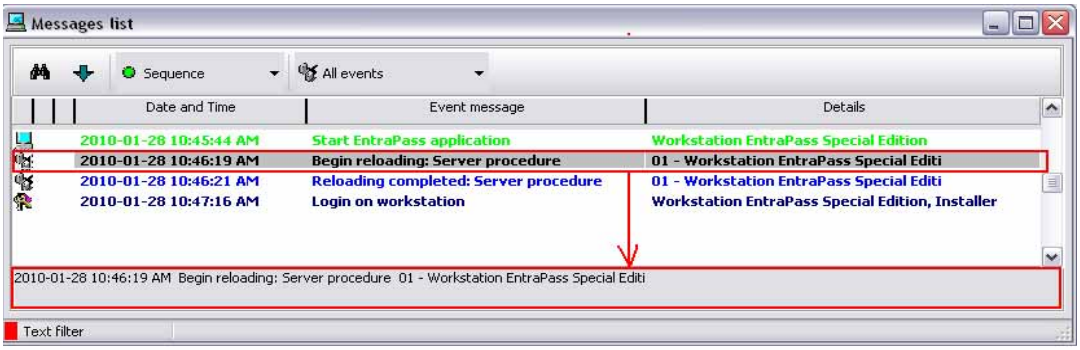
1 На рабочем столе **Message** вызвать контекстное меню щелчком правой кнопки мыши и выбрать пункт Properties (Свойства).



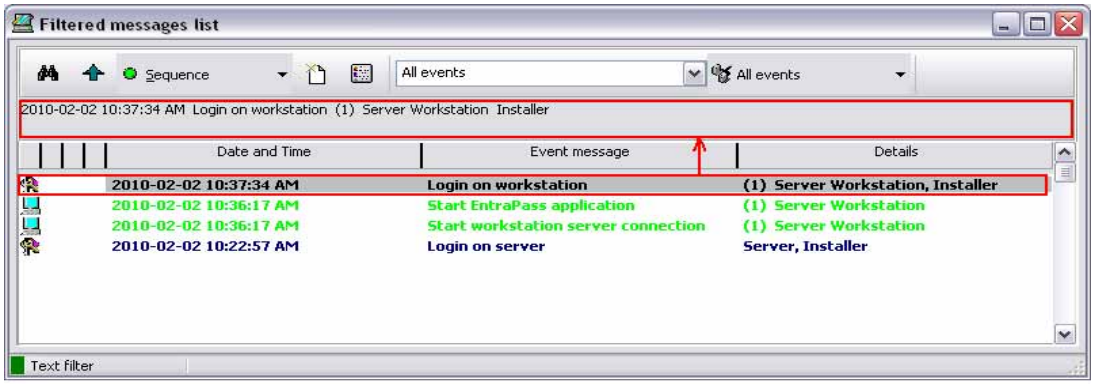
2 В окне Properties (Свойства) выбрать необходимые параметры отображения информации.

- **Multi-line** (Несколько строк) – как правило, сообщения о событиях отображаются на одной строке. Однако можно увеличить число строк между сообщениями, поставив флажок в соответствующем поле (1, 2, 3 или 4 строки).
- **Show icons** (Показывать пиктограммы) – при необходимости напротив каждого события будут отображаться пиктограммы разного типа.
  - **Message type** (Тип сообщения) – рядом с событием будет отображаться пиктограмма, указывающая на тип этого события. Например, событие типа "взлом двери" отображает пиктограмма в виде двери (рука символизирует принудительное управление; дискета означает действие, влекущее изменение в базе данных и т.п.). События, связанные с доступом, отображаются в виде пиктограмм входа/выхода.
  - **Picture** (Фотография) – рядом с событиями, содержащими фотографии владельцев карт, будет отображаться пиктограмма идентификационной карты.
  - **Fail-soft messages** (Сообщения о работе в безопасном режиме) – рядом с событиями, возникшими при работе контроллеров в автономном режиме, будет отображаться знак (+).
  - **Video** (Видеонаблюдение) – выводить на выбранный рабочий стол видеоданные с видеосервера, подключенного к Вашей системе.
- Раздел **Miscellaneous** (Прочее) позволяет выбрать дополнительные опции:
  - **Keep card picture** (Оставлять на экране фотографию карты) – система оставит на экране фотографию с последней идентификационной карты, связанной с событием, пока не произойдёт следующее событие с фотографией карты (опция Picture window (Окно фотографии) должна быть выделена).
  - **Display toolbar** (Показывать панель инструментов) – отображает/скрывает панель инструментов в верхней части рабочего стола Message.

- **Manual properties save only** (Сохранять свойства только вручную) – при выделении этой опции сохранение данных выполняется при нажатии кнопки **Save** (Сохранение); после выделения этой опции кнопка исчезает с экрана. Система сохраняет значения всех параметров, указанных в окне **Properties** (Свойства), а также положение данного окна на рабочем столе Messages (Сообщения).
- **Display selected messages - full** (Показывать выделенные сообщения – полное описание) – в нижней части окна **Message** будет добавлено небольшое окошко. В этом окошке отображается указанное событие и его полное описание. Данная функция может оказаться очень полезной, если окно Message слишком мало, чтобы вывести в него полное описание события.
- **Display events in bold** (Показывать события жирным шрифтом) – позволяет повысить удобочитаемость текстовых сообщений, отображаемых на рабочих столах EntraPass: Message list (Список сообщений), Filtered messages (Избранные сообщения) и Alarm desktop (Рабочий стол тревог). Более того, если цвет, выбранный для сообщения, совпадает с цветом заднего фона, то сообщение будет отображаться чёрным жирным шрифтом, так чтобы его всегда будет хорошо видно. (Эта функция недоступна для списков архивных сообщений Archived Messages Lists).
- **Last Message on Top** (Последнее сообщение сверху) - по умолчанию все сообщения о событиях отображаются в порядке поступления; в нижней строке окна выдаётся информация о выделенном событии. Эта опция позволяет отображать события в обратном порядке; при этом информация о выделенном событии отображается сверху.



Ascending Order



Descending Order

- **Auto-scroll delay** (Задержка автоматического пролистывания) – время задержки с момента выделения одного из пунктов в списке сообщений до момента включения режима автоматического пролистывания списка. По умолчанию эта опция включена с установленной задержкой. По желанию её можно отключить, и тогда оператор должен будет нажимать кнопку **Restart Scroll** (Возобновить пролистывание). (Эта функция недоступна для архивных сообщений **Archived Messages**).
- **Message background color** (Цветовой фон сообщений) – позволяет изменять цвет заднего фона в окне сообщений.

ПРИМЕЧАНИЕ: *Чтобы изменить цвет шрифта сообщений, следует войти в меню* **System** (Системные настройки) **> Event parameters** (Параметры событий).

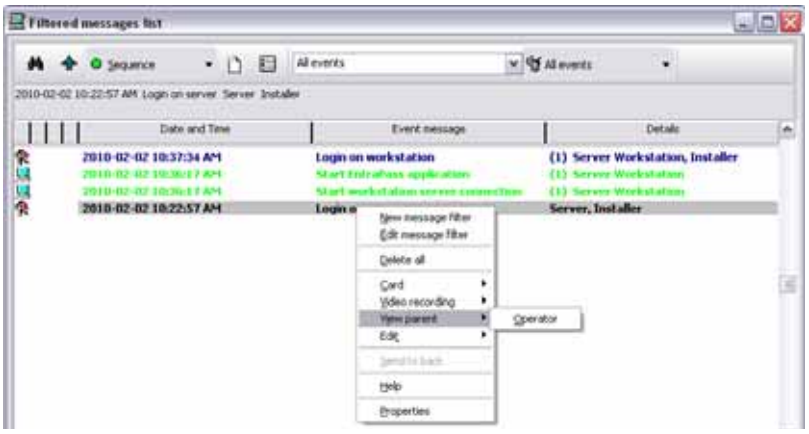
Выполнение разных задач с системными сообщениями

Система EntraPass позволяет выполнять самые разные задачи с системными сообщениями. А именно:

- Удаление сообщений
- Просмотр информации о карте
- Проверка состояния карты и операций с картой
- Изменение свойств рабочего стола (например, параметры отображения информации) и др.
- Просмотр, редактирование и экспорт видеозаписей
- Просмотр архивных видеозаписей из видеохранилища EntraPass Video Vault

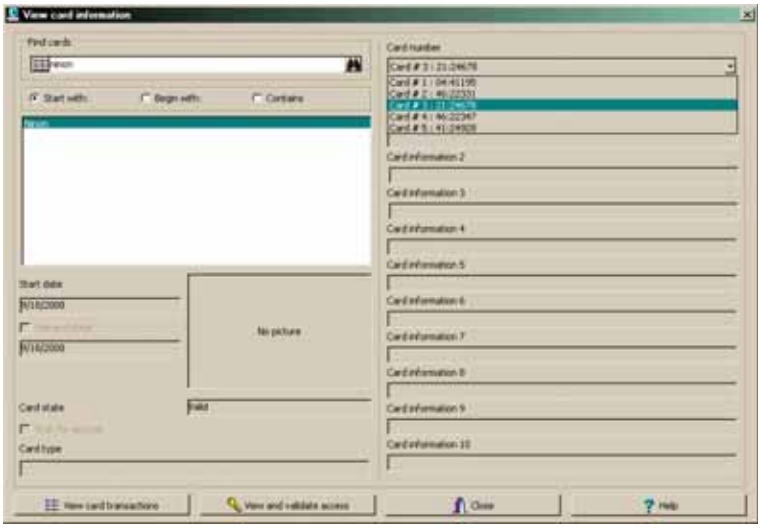
ПРИМЕЧАНИЕ: *Многие задачи доступны только для определённых рабочих столов. Например, при щелчке правой кнопкой мыши по сообщению о тревожном событии открывается контекстное меню с задачами, выполняемыми с тревожными событиями. Смотрите в Главе 11 Рабочий стол тревог' на странице 384 для более подробной информации .*

1 На столе сообщений Message вызвать контекстное меню правой кнопкой мыши.



2 Выполнить одно из следующих действий:

- **New message filter (Новый фильтр сообщений):** Эта опция отображает **Message filter** (фильтр сообщений) для на назначения нового фильтра сообщений. *Смотрите в Главе 12 Назначение фильтров сообщений' на странице 432 для более подробной информации* .
- **Edit message filter (Редактировать фильтр сообщений):** Эта опция отображает окно фильтра сообщений (**Message filter)** для его редактирования. *Смотрите в Главе 12 Назначение фильтров сообщений' на странице 432 для более подробной информации* .
- **Delete all** (Удалить все) – позволяет удалить все отображаемые события.
- **Card** (Карта) – это меню содержит две функции: **View card transactions** (Просмотр операций с картами) и **Search card** (Поиск карт). Функция **View card transactions** позволяет вывести на экран всю информацию о доступе применительно к владельцу карты, из-за которого возникло событие, связанное с нарушением доступа. Меню **Search card** позволяет искать карты в базе данных и выводить на экран сведения обо всех номерах карт, выпущенных для владельца, имя которого указано в окне **View card information** (Посмотреть сведения о карте). В этом окне операторы могут выполнять множество задач, включая просмотр и проверку сведений, содержащихся в карте (номер карты, имя владельца, статус карты (действительна или недействительна), тип карты и др. Кроме того, они могут выбрать карту и посмотреть операции с нею или посмотреть и проверить уровень доступа карты. *Смотрите в Главе 8 Назначение карт (раздел Card)' на странице 284 для более подробной информации* относительно просмотра уровня доступа и последних операций с картами.



- **Video recording** (Видеозапись) – это меню содержит три опции: **Play** (Воспроизведение), **Play/Edit/Export** (Воспроизведение/Редактирование/Экспорт) и **Play from Vault** (Воспроизведение из видеохранилища). Первая опция (**Play**) служит для просмотра видеозаписей в окне Playback (Воспроизведение), позволяющим захватить (скопировать) кадр и сохранить для дальнейшего использования. Вторая опция (**Play/Edit/Export**) предоставляет возможности, схожие с функциями, доступными в списке видеособытий (Video Event List). Операторы могут увидеть подробные сведения о событии (номер камеры, сервер, комментарии), сведения о камере и др. Видеособытия так же можно просматривать и экспортировать. Кнопка **Play from Video Vault** (Копирование из видеохранилища) позволяет просматривать видеособытия, хранящиеся в видеохранилище EntraPass Video Vault.

ПРИМЕЧАНИЕ: *Если иконки камеры не отображаются, достаточно щёлкнуть правой кнопкой мыши по сообщению о видеособытии, в контекстном меню выбрать пункт Properties (Свойства) и в разделе Show icons (Показывать пиктограммы) отметить флажком пункт Video (Видеозаписи).*

- **View parent** (Показывать родительский элемент) – отображается вышестоящий элемент для каждого компонента, связанного с выделенным событием.
- **Edit** (Редактировать) – служит для редактирования каждого компонента, связанного с выделенным событием. При выборе этой функции появляется контекстное меню, в котором отображаются компоненты, связанные с выделенным событием. Например, событие *Site definition modified* (Изменено назначения сайта/луча) имеет связи с приложением EntraPass, оператором, зарегистрированным в системе во время возникновения события, а также с сайтом/лучом, связанным с этим событием. Данная функция позволяет редактировать любой из этих трёх компонентов, отображённых в контекстном меню.
- **Send to back** (Перенести на задний план) – эта опция работает только для плавающих окон (Floating). При использовании данной опции активное окно оказывается за главным окном приложения. Чтобы вернуть его на передний план, следует щёлкнуть правой кнопкой по кнопке рабочего стола и выбрать в контекстном меню пункт **Bring to front** (Перенести на передний план).
- **Help** (Помощь): Отображает On_line помощь (**EntraPass Online Help**).
- **Properties** (Свойства) – служит для изменения настроек для выбранного рабочего стола.

Рабочий стол фотографий пользоватлей(Picture)

Если в настройках рабочего стола Message выделена опция **Picture screen** (Окно изображений), то при его выводе на экран всегда одновременно с ним отображается окно Picture. События, связанные с доступом, отображаются вместе с фотографией владельца карты, если соответствующая опция выделена в описании фильтра сообщений (System > Message filters). For details, *Смотрите в Главе 12 Назначение фильтров сообщений' на странице 432 для более подробной информации .*

Изменение свойств окна Pictures

1 В окне **Message list and picture** (список сообщений и изображение) выбрать событие доступа, затем щёлкнуть правой кнопкой мыши по фотографии владельца карты.

ПРИМЕЧАНИЕ: **Send to back** (Отправить на задний план) – эта опция работает только для плавающих окон (Floating). При использовании данной опции активное окно (окно с фотографией Picture) оказывается позади главного окна рабочего стола Message. Чтобы вернуть его на передний план, следует щёлкнуть правой кнопкой по кнопке рабочего стола Message и выбрать в контекстном меню пункт **Bring to front** (Перенести на передний план). В контекстном меню выбрать пункт **Properties** (Свойства).

2 В выпадающем списке **Aspect** (Вид) указать размеры окна с фотографией.
- **Design size** (Оригинальные размеры) – фотография владельца карты будет отображаться в натуральную величину.
- **Stretch** (Растянуть) – эта опция позволяет растянуть изображение до размеров окна без сохранения пропорций. Фотография может выглядеть искажённой.
- **Stretch ratio** (Растянуть пропорционально) – позволяет растянуть изображение до размеров окна с сохранением пропорций.

3 **Display multiple pictures** (отобразить несколько фотографий). Данная опция позволяет вам выводить в это окно до 4-х фотографий. Когда эта опция выделена, вы можете установить показывать подписи “Message” или указать определенную дверь для каждого из окна.

4 Выберите **Apply all the following items for all cells** (Применить все следующие пункты для всех ячеек) для назначения параметров для всех ячеек.

5 Выбрать данные, которые необходимо вывести на экран вместе с фотографией владельца карты:

- **Door** (Дверь) – дверь, где предъявлена карта, будет отображаться поверх фотографии владельца.
- **Event** (Событие) – отображать на экране сообщение о событии.
- **Card information** (Данные карты) – поверх фотографии владельца будут отображаться информационные поля карты.
- **Comment** (Комментарий) – отображается в поле, расположенном под фотографией владельца карты. В этом поле будет стоять комментарий, который был указан при назначении карты.

ПРИМЕЧАНИЕ: *если дверь назначена для ячейки (фото) и опция **Door** (дверь) выбрана (**Display selected fields**) (Отобразить выбранные поля), имя двери будет отображаться в синим вместо обычного синего цвета.*

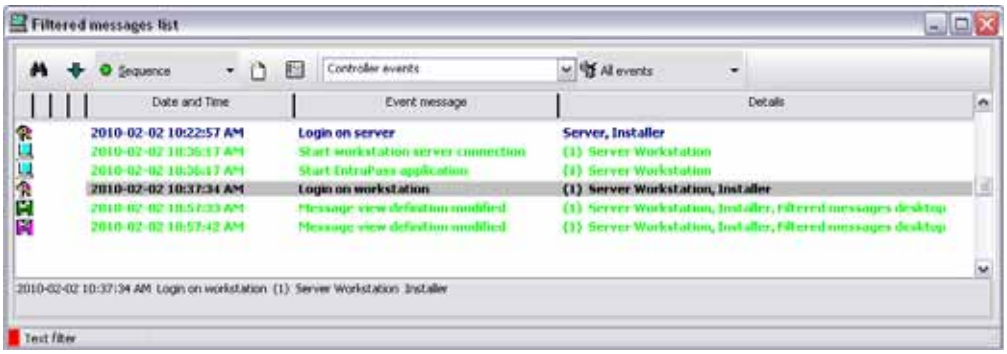
Рабочий стол отфильтрованных собщений (Filtered Messages Desktop)

Рабочий стол Filtered Messages служит для отображения избранных/отфильтрованных сообщений. Например, можно создать фильтры для отображения сообщений, связанных с работой конкретного контроллера или определённого шлюза. При использовании этих фильтров сообщения будут отображаться на рабочем столе Filtered Message. Избранные сообщения следует описать в меню Message filters (Фильтры сообщений): **System** > **Message filters**.

ПРИМЕЧАНИЕ: *При использовании фильтров система извлекает события, которые уже отображаются на рабочем столе сообщений Message, и отбирает из них события, соответствующие настройкам выбранного фильтра.*

Настройка рабочего стола избранных сообщений (Filtered Messages Desktop)

1. В главном окне Desktop (Рабочие столы) выбрать рабочий стол, который нужно настроить как рабочий стол для избранных сообщений (**Filtered messages**).
2. Назначить имя для (Filtered message desktop) и его тип (окно Message(сообщения), окно Picture(изображение) или оба окна вместе).



3. Настроить текстовый фильтр (**Text filter**) для отображения избранных сообщений. *Смотрите в Главе 11 Рабочий стол сообщений (Message Desktop)' на странице 373 для более подробной информации по настройке рабочего стола сообщений*.

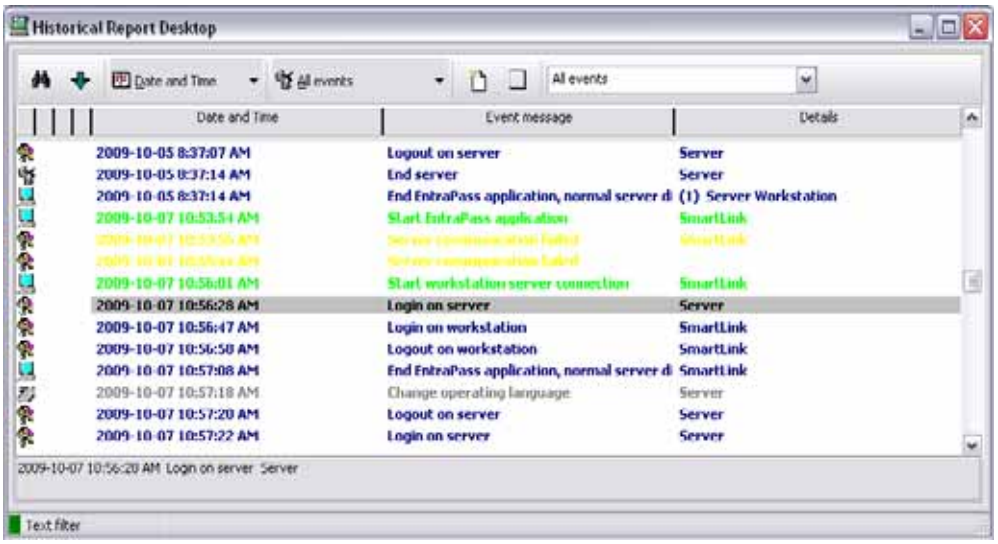
Рабочий стол архивных отчётов (Historical Report Desktop)

Рабочий стол **Historical Report** (Архивные отчёты) позволяет операторам отображать события, поступающие из предварительно настроенных исторических отчётов, определять статус создания отчёта и просматривать (если это допустимо) видеособытия, хранящиеся в видеохранилище EntraPass Video Vault**.** От уровня безопасности каждого оператора зависит, какие архивные отчёты ему доступны. Список сообщений **Historical Report** ничем не отличается от остальных списков сообщений EntraPass, за исключением дополнительной комбинированной панели, позволяющей операторам выбирать один из предварительно настроенных архивных отчётов.

Архивные отчёты настраивают в меню Report (Отчёты) > Historical Report (Архивные отчёты). Уровни безопасности операторов для пользования отчётами можно изменить в меню **System** (Системные настройки) **> Security Level** (Уровни безопасности) **>** закладка **Report** (Отчёты).

Настройка рабочего стола архивных отчётов (Historical Report Desktop)

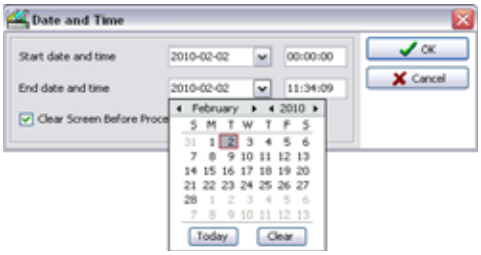
1. В главном окне Desktop (Рабочие столы) выбрать кнопкой рабочий стол, который нужно настроить для архивных отчётов (**Historical Reports**).
2. Назначить этому рабочему столу имя и указать его тип (окно Message (Сообщения), окно Picture (Фотографии) или оба окна вместе).



3. Выбрать критерии отбора, по которым будут отображаться архивные данные: **Date and Time** (Дата и время), **Event** (События) или **Message Type** (Тип сообщения).

ПРИМЕЧАНИЕ: *Функция последовательной сортировки недоступна для списков архивных сообщений.*

4. При необходимости ввести текстовую строку, которая будет использоваться для поиска определённых архивных сообщений.
5. На комбинированной панели указать, какой архивный отчёт (**Report**) необходимо создать. Список доступных отчётов соответствует уровню безопасности оператора.
6. После выбора отчёта на экране появляется окно **Date and Time** (Дата и время), в котором следует указать, за какой период должен быть сгенерирован отчёт.
7. Указать начальные (**Start**) и конечные (**End**) дату и время или открыть календарь щелчком по иконке календаря и указать даты при помощи календаря, а затем ввести время.



8. Чтобы очистить окно архивных отчётов от предыдущих результатов поиска, поставить флажок напротив опции **Empty screen box process request** (Очистить окно).
9. Нажать **OK**. Индикатор статуса, расположенный в левом нижнем углу экрана, во время генерации архивного отчёта будет гореть не зелёным, а

синим цветом. Он снова станет зелёным после окончания передачи данных, и после этого архивные данные будут выведены на экран в соответствии с назначенными критериями отбора.

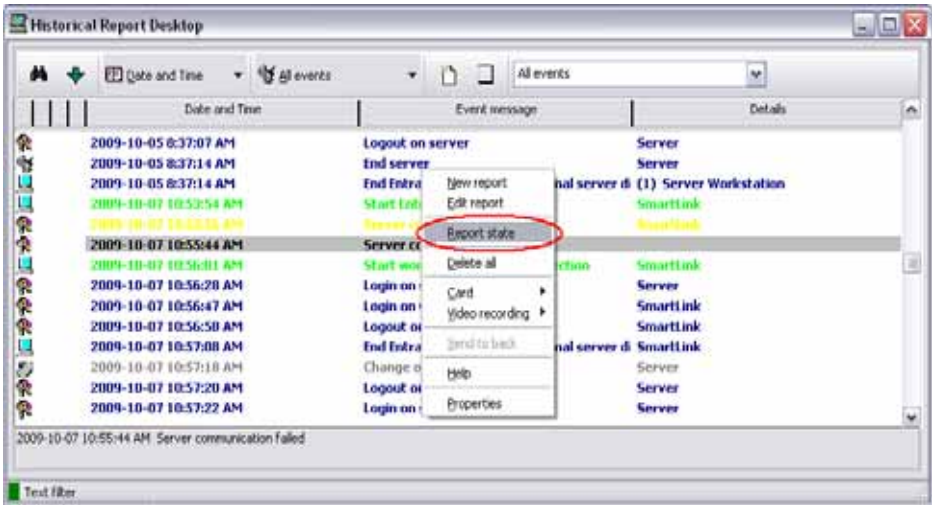
Создание и редактирование архивных отчётов из рабочего стола

- When your security level allows you to create new reports, you can access the Historical Report dialog from the **New Report** command in the Historical Report Desktop pop up menu. For more information on Historical Reports, see *see "Historical Reports Definition" on page 449.*
- When your security level allows you to edit existing reports, you can access the Historical Report dialog from the **Edit Report** command in the Historical Report Desktop popup menu. For more information on Historical Reports, *see "Historical Reports Definition" on page 449.*

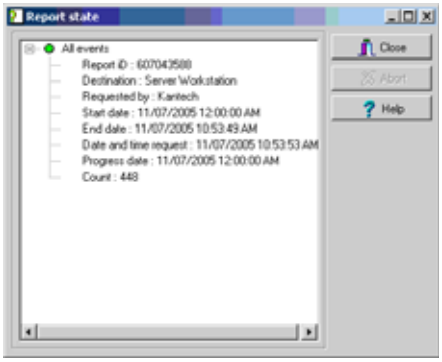
Отображение состояния архивного отчёта в реальном времени

Эта функция позволяет наблюдать за ходом создания определённого отчёта в списке архивных отчётов.

1 В окне Historical Report Desktop (Рабочий стол архивных отчётов) щёлкнуть по одной из позиций правой кнопкой мыши. На экране появится контекстное меню.



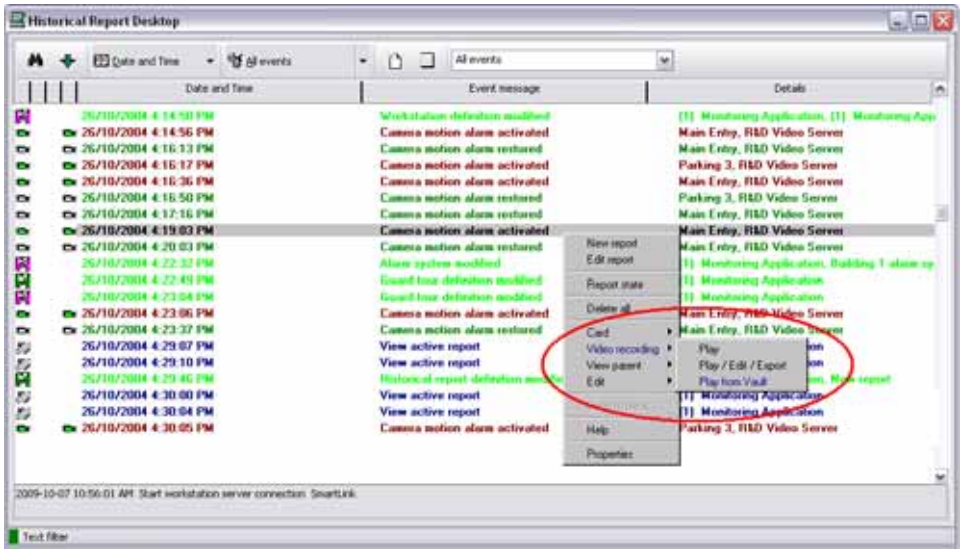
2 Выбрать пункт **Report State** (состояние отчёта). Окно Report State содержит сведения о генерации отчёта.



3 После завершения создания отчёта все данные в окне Report State исчезают. Нажать **Close** (Закрыть).

Воспроизведение архивных видеозаписей
:Анимированные иконкииз списка сообщений на рабочем столе

1 Выделить видеозапись, которую необходимо просмотреть, и вызвать контекстное меню правой кнопкой мыши.



2 Если видеофрагмент хранится в видеохранилище Entrapass Video Vault, то в контекстном меню будет доступна опция **Play from Vault** (Воспроизведение из видеохранилища). После вызова этой функции откроется окно Video Playback (Воспроизведение видеофайлов), и начнётся воспроизведение выбранного видеофрагмента.

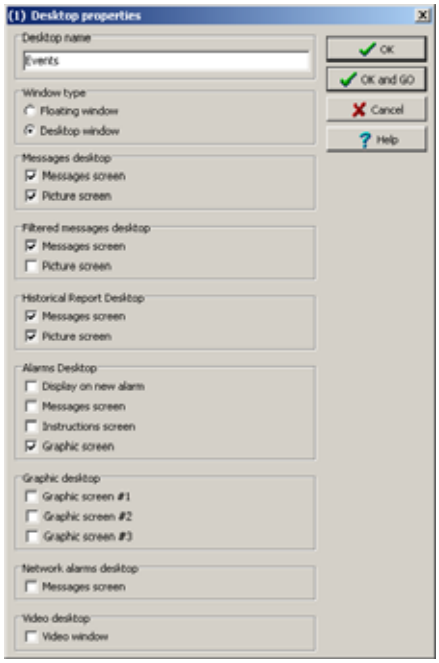
Рабочий стол тревог

Рабочий стол тревог служит для просмотра и подтверждения тревожных событий. Тревожные события описывают в меню Event Parameter: **System** (Системные настройки) **> Event Parameters** (Параметры событий). Любое событие можно описать как тревожное. Тревожные события требуют подтверждения оператора и отображаются на рабочем столе Alarms. Для всех тревог необходимо указать расписание: меню **System** (Системные настройки) > **Event parameters** (Параметры событий), **Alarm settings** (Настройки тревог). В случае возникновения тревоги в период действия расписания операторы обязаны подтвердить получение сигнала тревоги. Тревоги отображаются на экране с указанием даты и времени, описания тревоги, подробных сведений, инструкций оператору (если их назначили) и прикреплённых графических схем или видеофайлов. Новые события добавляются в конец списка тревог, если в настройках не указано иное в спускающееся форме (меню Alarm Desktop Properties (Свойства рабочего стола тревог)).

ПРИМЕЧАНИЕ: *Системный администратор может запретить вывод тревожных сообщений на рабочие столы. В таком случае рабочие столы тревог не будут доступны любому пользователю. Смотрите в Главе 14 Сетевая тревога (Network Alarm)' на странице 483 для более подробной информации по отключению опции сетевой тревоги.*

Назначение рабочего стола тревог (Alarms Desktop)

1 В главном окне Desktop (Рабочие столы) выбрать рабочий стол, который нужно настроить как рабочий стол тревог, и указать тип окна: Floating (Плавающее) или Desktop window (Окно рабочего стола).



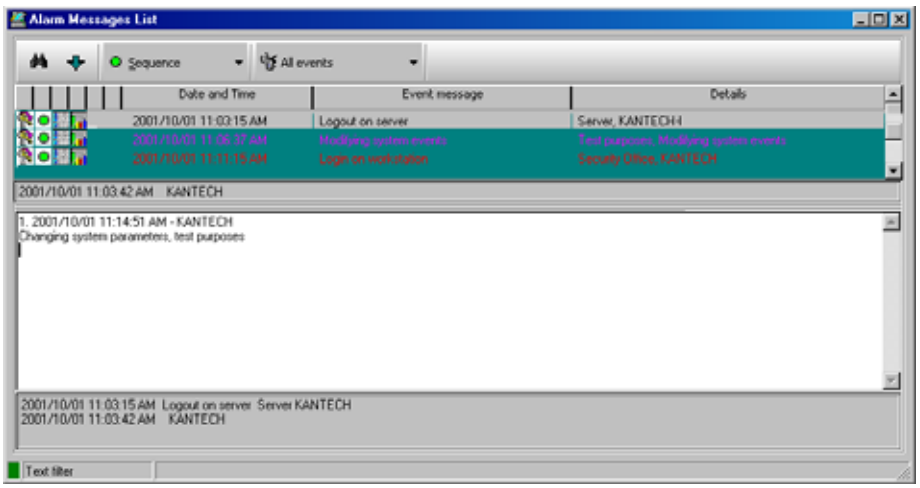
2 Указать дополнительные окна, которые будут связаны с рабочим столом тревог:
- **Display on new alarm** (Показывать при возникновении новой тревоги) – автоматически открывать рабочий стол тревог при возникновении тревоги.
- **Message screen** (Окно сообщений) – служит для просмотра и подтверждения тревог, для которых в меню описания параметров событий (**System** (Системные настройки) > **Event Parameters** (Параметры событий) > **Alarm settings** (Настройки тревог) указано расписание подтверждения (Acknowledgement schedule), или показывает кнопку автоподтверждения, если эта функция настроена в меню описания настроек операторов (**System** (Системные настройки) > **Operator** (Операторы) > **Privileges** (Особые права)).
- **Instructions screen** (Окно инструкций оператору) – отображает инструкции оператору, прикреплённые к событию, которое требует подтверждения (например, вызов полиции, отправка сообщения в клиентское приложение и др.). Для назначения инструкций оператору следует войти в меню **System** (Системные настройки) > **Instructions** (Инструкции). Затем можно создать связи между инструкциями и событиями.

- **Graphic screen** (Окно графических схем) – позволяет определить место, где возникла тревога (если в системе описаны графические планы). *Смотрите в Главе 5 Назначение графических схем' на странице 195 для более подробной информации* .

ПРИМЕЧАНИЕ: *Рабочий стол тревог можно настроить как окно сообщений (Message), окно графики (Graphic) и окно инструкций для оператора (Instruction). Все эти три функции можно применить к одному рабочему столу одновременно. Если в настройках рабочего стола выделены все три функции, то на экране будет отображаться сразу три окна. Для удобства работы с окнами рекомендуется изменить их положение и размеры.*

Просмотр тревожных системных сообщений

1 Открыть рабочий стол тревог (**Alarm**). Тревожные события отображаются в соответствии с выбранными критериями (поле **Sorted by**).



2 Для того чтобы добавить комментарий, дважды щёлкнуть по списку событий (в середине окна). В открывшемся окне Add a comment (Добавить комментарий) ввести необходимый текст. После ввода текста нажать **OK**, чтобы закрыть окно. Тревожное событие будет отмечено знаком +, который указывает на наличие комментария к событию.

3 Способ сортировки сообщений можно изменить в выпадающем списке **Sorted by** (Способ сортировки):
- **Sequence** (Последовательно) – сообщения выдаются в порядке их поступления. Этот способ сортировки используется по умолчанию. Список сообщений прокручивается до конца каждый раз при выводе на экран новой тревоги.
- **State** (Статус) – сортировка тревог выполняется по их статусу (подтверждены, должны быть подтверждены или отмечены). При использовании этой функции стандартное пролистывание событий не работает. Чтобы вернуться к отображению списка событий с настройками по умолчанию, следует выбрать в выпадающем списке Sorted by (Способ сортировки) опцию Sequence (Последовательность).
- **Date and time** (Дата и время) – сортировка тревог выполняется в зависимости от даты и времени их возникновения.
- **Event** (События) – система выполняет сортировку событий в колонке **Event message** (Сообщения о событиях), выстраивая их в алфавитном порядке и группируя *идентичные* события. Например, все события **Input in alarm** (тревога по входу) будут сгруппированы вместе.
- **Priority** (Приоритет) – сортировка событий по приоритету, как описано в меню **Event Parameters** (Параметры событий).

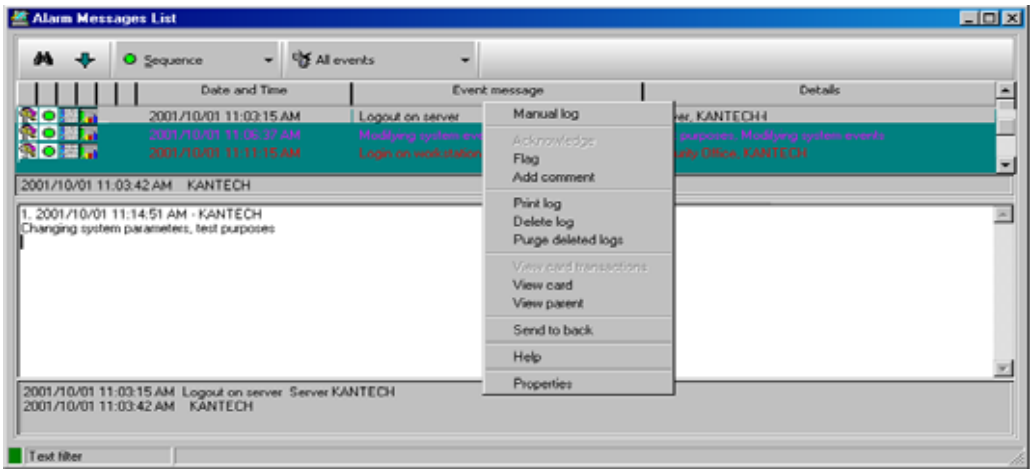
4 Правой кнопкой мыши в любом месте окна вызвать окно Properties (Свойства), в котором необходимо активировать индикаторы состояния тревог:
- **Красный** – требуют подтверждения или временно отложены. Если сообщения отложены, то отображается время задержки. По окончании времени задержки система снова требует подтверждения от оператора. Чтобы подтвердить отложенное тревожное сообщение до окончания времени задержки, следует щёлкнуть по отображаемой задержке. При этом таймер будет обнулён.
- **Зелёный** - подтверждены.

- **Жёлтый** - Отмечены.
- **Чёрный** – удалены. Чтобы просмотреть тревожные сообщения, удалённые вручную, следует отметить флажком опцию **View deleted logs** (Посмотреть удалённые записи) в меню **Properties** (Свойства).
- **Синий** – ручная запись

5 Кнопками **Manual / Automatic** (Вручную/Автоматически) выбрать способ подтверждения сообщений. Эта опция доступна только тем операторам, у которых есть соответствующее разрешение в меню Operator Definition (Назначение операторов). *Смотрите в Главе 12 Назначение операторов' на странице 402 для более подробной информации .*

ПРИМЕЧАНИЕ: *Опция ручного/автоматического подтверждения сообщений (**Manual / Automatic**) доступна только на рабочем столе тревог (Alarms Desktop). После того как оператор с такими правами выйдет из системы, вновь восстановится "ручной" режим подтверждения (по умолчанию).*

6 Щёлкнуть правой кнопкой мыши по сообщению для вызова дополнительных функций, доступных для тревожных сообщений:

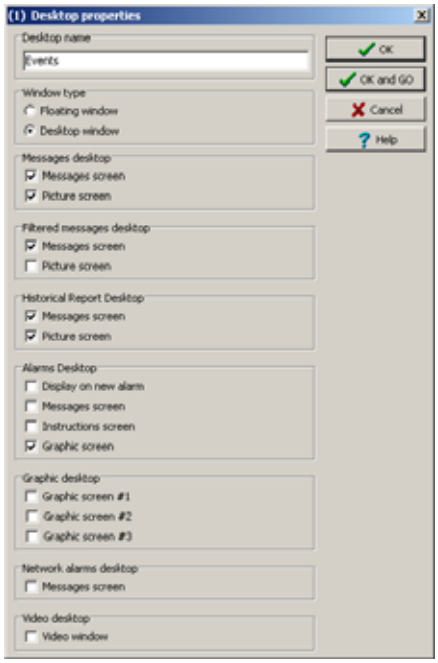


- **Manual log** (Ручная запись) – при выборе этой опции открывается окно Manual log, в котором оператор имеет возможность добавлять комментарии к событию, и следовательно, создавать события, настроенные под свои собственные требования (приоритет, подробные сведения о событии, цвет и пр.). При добавлении ручной записи рядом с тревожным сообщением отображается пиктограмма "рука" и синяя метка. Для того чтобы эти знаки были видимыми, должно быть разрешено отображение пиктограмм (щёлкнуть правой кнопкой по тревожному событию > **Properties** (Свойства) > **Show icons** (Показывать пиктограммы)).
- **Acknowledge** (Подтверждение) – если оператор подтвердил получение тревожного сообщения, то рядом с событием появляется зелёная метка.
- **Flag** (Поставить флаг) – эта опция позволяет отметить выбранное событие флажком. Рядом с отмеченными событиями появляется жёлтая метка.
- **Add comment** (Добавить комментарий) – позволяет операторам вводить комментарий к выделенному событию. Добавленные комментарии отображаются в нижней части окна тревог. Синий знак плюса (+) рядом с тревожным сообщением показывает, что к этому сообщению был добавлен комментарий. (Знак (+) виден, если разрешено показывать на экране пиктограммы: правой кнопкой щёлкнуть по тревожному событию > **Properties** (Свойства) > **Show icons** (Показывать пиктограммы).
- **Print log** (Печатать запись) – служит для вывода на печать тревожного сообщения.
- **Delete log** (Удалить запись) – пометить выбранное тревожное сообщение, как удалённое (чёрная метка указывает, что на сообщении установлена метка удаления). Чтобы посмотреть записи с метками удаления перед окончательным их уничтожением, следует вызвать контекстное меню нажатием правой кнопки мыши в любом месте экрана и перейти в меню **Properties** (Свойства), а затем **View deleted logs** (Показать удалённые записи).
- **Purge deleted log** (Уничтожить удалённые записи) – служит для окончательного удаления записей, помеченных как удалённые.

Автоматическое отображение рабочих столов тревог

Система EntraPass позволяет автоматически выводить на экран графические схемы – с любого рабочего стола – непосредственно при возникновении тревоги. Благодаря этой функции дежурные операторы автоматически видят все новые тревоги, не открывая рабочий стол тревог и дополнительные, связанные с ним окна. Если на рабочем столе тревог отмечена флажком опция **Display on new alarm** (Показывать при возникновении новой тревоги), то стол тревог (и связанные с ним окна) будут появляться на экране сразу при возникновении тревоги, независимо от того, какое окно будет активным в тот момент.

1 Настроить рабочий стол и описать его как стол тревог: для этого следует отметить флажком пункты меню Alarms desktop.



2 Отметить флажком опцию **Display on new alarm** (Показывать при возникновении новой тревоги), чтобы операторы могли автоматически видеть новые тревоги, не открывая рабочий стол тревог и дополнительные, связанные с ним окна.

ПРИМЕЧАНИЕ: *Если эта опция выделена, например, при назначении рабочего стола избранных сообщений(Filtered message desktop), и иконка рабочего стола выделена, то рабочий стол избранных сообщений (Filtered message desktop) будет отображен (цвет фона его иконки станет синим), но окна под надписью Display on new alarm отображаться не будут – они будут появляться на экране только при возникновении новой тревоги. Если эти окна открылись (при поступлении новой треоги), нажать "X" в правом верхнем углу одного из них, то все открытые окна закроются одновременно. Если опция Display on new alarm не выделена, то рабочий стол тревог и все дополнительные окна будут отображаться только по ручному принудительному вызову (то есть при нажатии иконки этого рабочего стола).*

3 Нажать **OK and Go**, чтобы сразу применить внесённые изменения.

ПРИМЕЧАНИЕ: *После настройки одного из рабочих столов в качестве стола тревог, открывающегося при возникновении новой тревоги, рекомендуется снова открыть его и расположить все окна на экране таким образом, чтобы с ними было удобно работать, а затем снова нажать **OK and GO**. После этого все окна будут открываться так, как Вы их настроили.*

Подтверждение тревог/событий

Как правило, операторы должны подтверждать получение тревожных сообщений (например, о вторжении, о переключении входа в тревожный режим и др.), нажимая в ответ, например, кнопку подтверждения. В системе EntraPass операторы подтверждают тревожные сообщения, появляющиеся в дополнителных окнах-предупреждениях или в окне рабочего стола тревог.

ПРИМЕЧАНИЕ: *Систему можно настроить таким образом, чтобы тревожные сообщения отображались в сопровождении звукового сигнала. Смотрите в Главе 14 Конфигурация мультимедийных устройств' на странице 477 для более подробной информации по настройке тревожных звуковых сигналов.*

Опции подтверждения настраивают в меню назначения приложения EntraPass: **Devices** (Устройства) > **EntraPass application** (выбранная рабочая станция) > закладка **Alarm,** Acknowledgement parameters (Параметры подтверждения)). События, требующие подтверждения оператора, необходимо описать в меню: **System** (Системные настройки) > **Event Parameters** (Параметры событий).

ПРИМЕЧАНИЕ: *Если компонент, переключившийся в режим тревоги, привязан к какому-либо окну видеонаблюдения, то при возникновении тревоги на экране автоматически появится видеоокно с изображением, передаваемым в реальном времени, или с видеозаписью когда это событие произошло.*

Автоматическое подтверждение

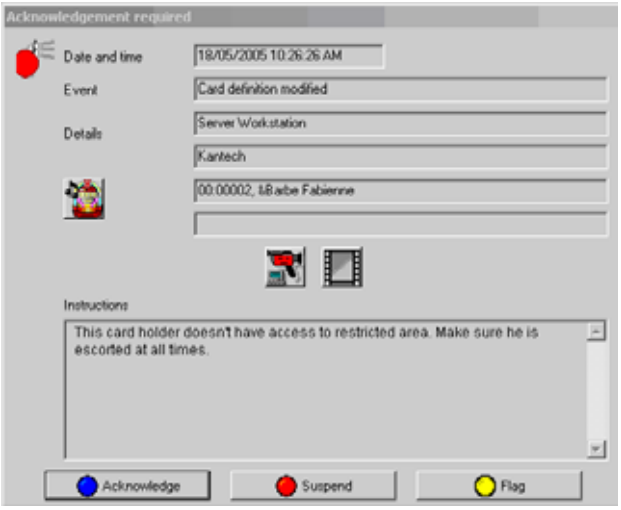
В системе предусмотрено автоматическое подтверждение тревог, без участия оператора. Эта опция активируется в меню Operator Definition (Назначение операторов): **System** (Системные настройки) > **Operators** (Операторы) > **Privileges**, **Auto acknowledge** (Особые права, Автоматическое подтверждение).

ПРИМЕЧАНИЕ: *Чтобы кнопка **Manual** (Ручной режим) отображалась в окне рабочего стола тревог (Alarm Desktop), обязательно нужно завершить рабочую сессию EntraPass и снова открыть её после выделения опции **Auto acknowledge** (Автоматическое подтверждение).*

ПРИМЕЧАНИЕ: *Использование этой опции доступно только для операторов, обладающих соответствующими правами. В случае использования функции **Automatic acknowledge** (Автоматическое подтверждение) окно-предупреждение на экране не появляется, поэтому отложить подтверждение тревоги на некоторый срок невозможно. После включения этой опции в меню описания операторов (Operator), на рабочем столе тревог (Alarms) появляется дополнительная кнопка Manual (Ручной режим). Эта кнопка служит, чтобы переключать подтверждение сообщений в ручном и в автоматическом режиме.*

Порядок подтверждения тревожных сообщений

1 После появления окна с заголовком **Acknowledgement required** (Требуется подтверждение) необходимо выполнить следующие действия:



- Нажать кнопку **Acknowledge** (Подтверждение), чтобы подтвердить получение сообщения о тревожном событии. После этого красная метка, стоящая рядом с сообщением и показывающая его статус, станет зелёной.
- Нажать кнопку **Suspend** (Отложить), чтобы отсрочить на некоторый срок подтверждение сообщения и выполнить в это время другие неотложные операции. Предупреждение о тревоге будет отложено на определённое время, указанное в описании приложения (меню **EntraPass application**). После окончания установленного времени задержки система снова предложит оператору подтвердить получение сообщения.

- Нажать кнопку **Flag** (Поставить флаг), если необходимо подтвердить получение тревожного сообщения о пометить его для дальнейших действий. Сообщение с флагом будет выделено жёлтой меткой.
- Нажать **Mute** (Выключить зуммер), чтобы отключить тревожную сигнализацию.

ПРИМЕЧАНИЕ: *Если для тревожного сообщения не указано никаких инструкций оператору, то окно с заголовком* ***Acknowledgement required*** *(Требуется подтверждение) будет отображаться без инструкций оператору*

ПРИМЕЧАНИЕ: *Если компонент, переключившийся в режим тревоги, привязан к какому-либо окну видеонаблюдения, то при возникновении тревоги на экране автоматически появится это видеоокно с изображением, передаваемым в реальном времени, или с видеозаписью.*

Подтверждение тревоги в окне рабочего стола тревог

1. Выделить тревожное сообщение, требующее подтверждения (например, которое было ранее отмечено флагом) и щелчком правой кнопки мыши вызвать контекстное меню.
2. Выбрать в контекстном меню пункт **Acknowledge** (Подтверждение). Индикатор статуса рядом с сообщением станет зелёным.

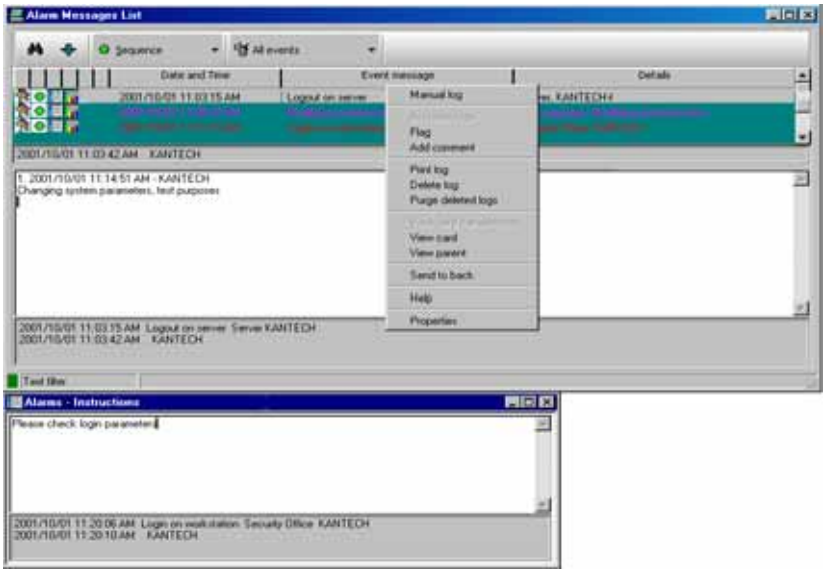
ПРИМЕЧАНИЕ: *Чтобы отметить тревожное сообщение флагом для каких-либо определённых целей, следует выделить его и щелчком правой кнопки мыши вызвать контекстное меню, в котором выбрать пункт* ***Flag*** *(Поставить флаг). Кроме того, можно просто щёлкать по этому сообщению до тех пор, пока метка не станет нужного цвета.*

Рабочий стол инструкций для оператора (Instruction Desktop)

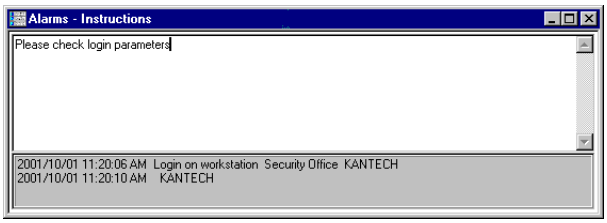
Окно инструкций (Instruction) показывает команды, которые необходимо выполнить при сообщении о тревоге. Инструкции отображаются на экране только в том случае, если эта опция разрешена в настройках параметров событий: **System** (Системные настройки) > **Event parameters** (Параметры событий), **Alarm settings** (Параметры тревог).

Просмотр инструкции к тревожному сообщению

1 Чтобы видеть исинтрукции к тревожным сообщениям, рабочий стол тревог (Alarms desktop) можно настроить как окно сообщений (Message) и окно инструкций (Instruction) или просто как окно инструкций. Если рабочий стол сконфигурирован как окно сообщений и окно инструкций, то оба окна отображаются одновременно.



2 Кроме того, чтобы вывести на экран инструкцию к выбранному сообщению, можно щёлкнуть по этому сообщению правой кнопкой мыши.



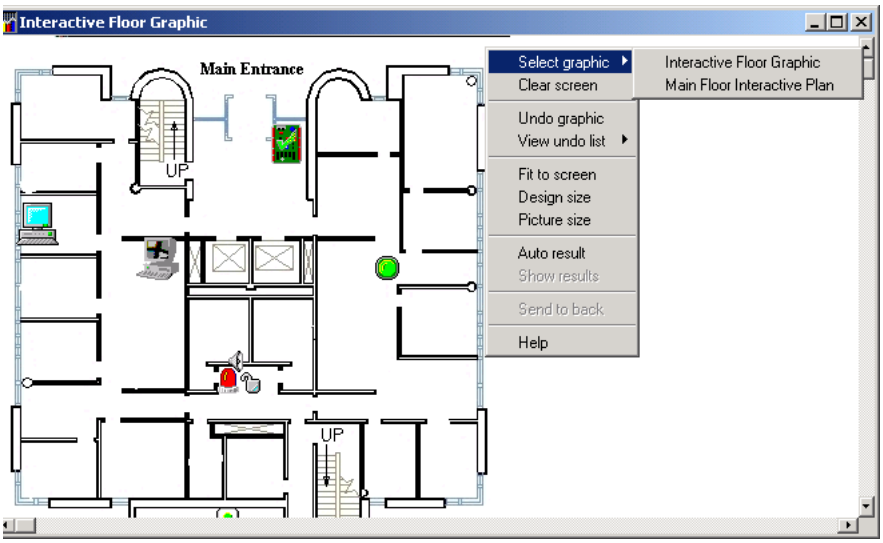
ПРИМЕЧАНИЕ: *Данная функция может оказаться очень полезной, если рабочий стол тревог слишком мал, чтобы вывести в него полное описание события.*

Рабочий стол графических схем (Graphic Desktop)

Рабочий стол Graphic desktop позволяет определить на графических планах место, где возникла тревога (если графики назначены в системе). Графическая схема соответствует охраняемой территории объекта, на которой расположены компоненты (приложения EntraPass, контроллеры, входы, реле и др.). С помощью графических схем операторы могут легко определить точное место расположения компонента на сайте или увидеть статус компонентов и устройств, в том числе контролируемых зон, групп зон, дверей, контактов, детекторов движения, контроллеров, прикреплённых к графическим планам системы. Если система настроена на учёт всех присутствующих в охраняемой зоне, то при возникновении аварийной ситуации на графическом плане по иконкам будет видно, когда весь персонал покинет контролируемую зону. Операторы могут вручную управлять компонентами непосредственно на графических схемах (например, отпирать/запирать двери). *Смотрите в Главе 5 Назначение графических схем' на странице 195 для более подробной информации* по настройке поэтажных планов.

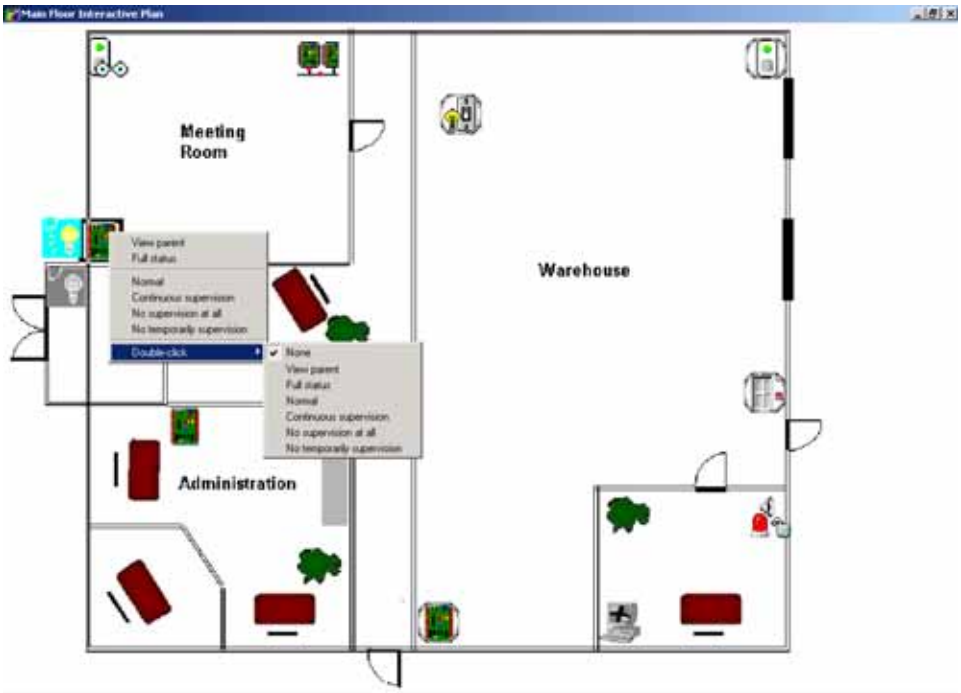
Просмотр графических схем на рабочем столе Graphic Desktop

1. Правой кнопкой мыши выделить иконку рабочего стола, который должен использоваться для графики, назвать его, например, Graphics; затем указать тип окна: плавающее (**Floating**) или "рабочий стол" (**Desktop**).
2. Нажать **OK and Go**, чтобы вывести этот рабочий стол на экран.
3. Правой кнопкой щёлкнуть в любом месте рабочего стола, чтобы вызвать контекстное меню, и указать, какой схему/график необходимо отображать на этом рабочем столе.



ПРИМЕЧАНИЕ: *Если окно рабочего стола оказалось меньше, чем размеры графического плана, то для просмотра плана его можно перемещать в пределах окна, захватывая щелчком и буксируя в нужное положение мышью.*

4. Пользователь может вызвать контекстное меню щелчком правой кнопки мыши в любом месте графической схемы, чтобы выполнить следующие действия:
   - Отрегулировать размеры экрана для выбранной схемы: **Fit to screen** (Вписать в страницу), **Design size** (Размеры чертежа) или **Picture size** (Размеры изображения
   - Выделить опцию **Auto result**, чтобы в случае нарушения связи система отображала сообщение с указанием причины потери связи. Если опция **Auto result** не используется, операторы должны будут вручную запрашивать результаты для выбранного компонента при помощи функции **Show result** (Показывать результаты).
5. Вызвать контекстное меню щелчком правой кнопки мыши по компоненту с проблемами.



ПРИМЕЧАНИЕ: *Тревожные статусы компонентов отображаются при помощи анимированных иконок. Щёлкнув по анимированной иконке, оператор может вызвать контекстное меню, чтобы просмотреть элементы вышестоящего звена (родительские компоненты) и узнать более подробно о тревожной ситуации.*

6 Выбрать в контекстном меню пункт **Full status** (Полный статус), чтобы вывести на экран список ошибок, связанных с одним или со всеми компонентами, имеющими статус тревоги.

7 Выделить пункт **Double click** (Двойной щелчок), чтобы разрешить операторам изменять статус тревожного компонента на рабочем столе Graphic. Поясним сказанное на примере компонента "Дверь": если в меню ***Double click*** была выбрана опция **Unlock** (Отпереть), то операторы смогут вручную отпирать дверь двойным щелчком мыши по изображению этой двери на графической схеме в окне Graphic.

ПРИМЕЧАНИЕ: *Если функция Double click была изменена с рабочего стола графических схем (Graphic desktop), система не сохранит внесённые изменения. Чтобы изменить значение по умолчанию для этой функции, следует зайти в меню* ***описания графических схем*** *(**Definition** (Назначения) > **Graphics** (Графические схемы), окно Design (Проект), щёлкнуть правой кнопкой мыши по компоненту > выбрать пункт **Default dblclick** (Двойной щелчок по умолчанию)). Смотрите в Главе 5 Назначение графических схем' на странице 195 для более подробной информации по созданию графических схем и использованию компонентов на схемах.*

Мониторинг груп областей для Muster отчета

Muster отчеты создаются для контроля и мониторинга специфических областей, когда происходит тревожная ситуация. Информация, которая автоматически направляется на принтеры, содержит информацию о количестве людей в определенной области, когда происходит тревога. Информация может быть обновлена через определенный предварительно назначенный промежуток времени.

Информация о Muster отчете может быть также отображена на графическом дисплее. Там иконки более узнаваемы.

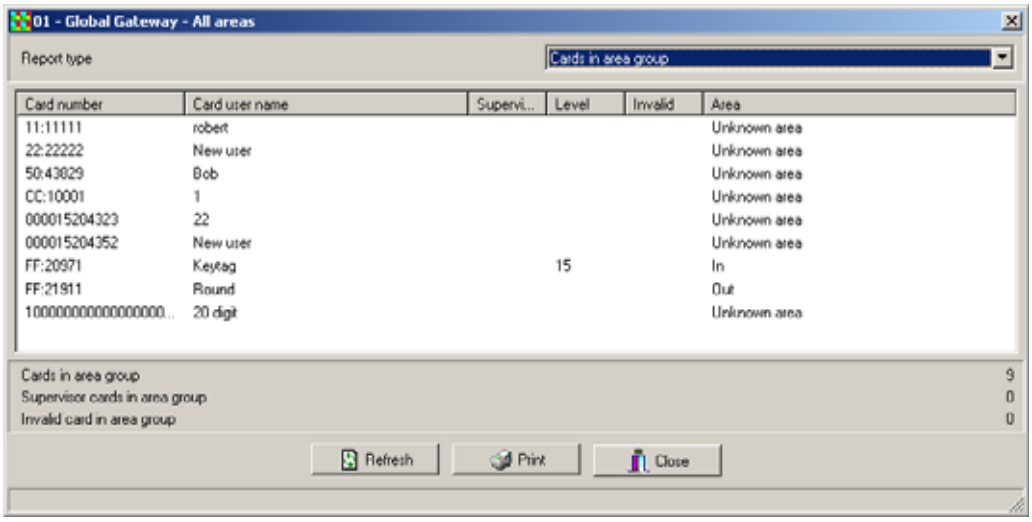
Иконка	Описание
	Area group is active (Группа областей активна): картодержатели все еще находятся внутри одной или нескольких областей в данной группе областей.

Иконка	Описание
	Area group is empty (Группа областей пустая): Все области внутри данной группы пустые.
	Area is active (Область активна): картодержатели все еще в области.
	Area is empty (Область пустая): Все картодержатели покинули данную область.

Информация о Muster отчете может быть также отображена в окне Area Group report (отчет о группе областей).

1 В окне График, нажмите правой кнопки мыши на компоненте, который представляет группу областей, которую вы хотите контроллировать. Контекстное меню будет выскакивать на экран.

2 Выберите **Get cards in area group** (Получить карты в группу областей). Карты в данной группе областей будут вам отображены.



- Данное окно содержит имя карты, номер и область, где в настоящее время находитс данная карта.
- Muster отчет также показывает статус карты: ревизор (supervisor), его уровень, если карта недействительная.

- Эта информация может быть обнавлена автоматически путем нажатия кнопки **Refresh** (Обновить).
- Эта информация может быть выведена на печать путем нажатия на кнопку **Print**.

Рабочий стол сетевых тревог (Network Alarms Desktop)

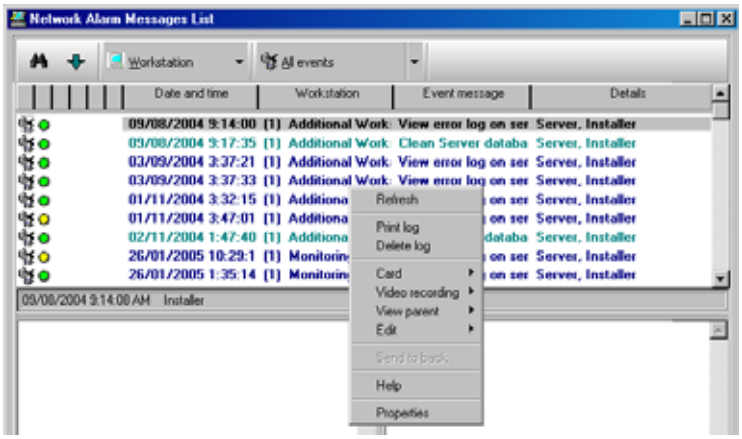
Рабочий стол сетевых тревог служит для просмотра и подтверждения *всех* тревожных событий в системе. На этом столе отображаются только события, требующие подтверждения оператора, и запрограммированные в меню **Event Parameters** (Параметры событий).

ПРИМЕЧАНИЕ: *Сетевые тревоги (Network Alarms) доступны на всех рабочих станциях системы. По умолчанию сервер отправляет сетевые тревоги на все рабочие станции во время запуска. Чтобы сетевые тревоги не отправлялись автоматически на другие компьютеры, следует воспользоваться опцией* ***No reload on startup*** *(Не выполнять повторную загрузку при запуске):* ***Devices*** *(Устройства) >* ***EntraPass application*** *(Приложение EntraPass)* ***>*** *закладка* ***Network Alarm*** *(Сетевые тревоги). Эту опцию можно использовать в случае медленного соединения между рабочей станцией и сервером.*

Операторы смогут увидеть только те сетевые тревоги, которые были отправлены в приложения, перечисленные в меню назначения их уровня безопасности «Security level» «Definition menu».

Просмотр сетевых тревог

1 Открыть рабочий стол сетевых тревог (Network Alarms desktop).



2 Щёлкнуть правой кнопкой мыши в любом месте окна, чтобы вызвать контекстное меню:

- **Refresh** (Обновить) – эта опция позволяет операторам загружать новые тревожные сообщения на рабочий стол сетевых тревог (Network alarms desktop). Функция Refresh особенно полезна, если сервер не загружает автоматически сетевые тревоги при запуске; то есть при использовании опции **No reload network alarms on startup** (Не загружать сетевые тревоги при запуске), которая находится в меню описания рабочей станции: **Devices** (Устройства) > **Workstation** (Рабочие станции) > закладка Messages 1 из 2.
- **Print log** (Печатать лог) – служит для вывода на печать тревожного сообщения.
- **Delete log** (Удалить запись) – уничтожает тревожные записи в системе. При выделении этой опции на экране появляется окно Delete network alarms (Удалить сетевые тревоги). В этом окне следует указать параметры удаления (**Deletion option**): Selected (Выделенные), All (Все) или Custom (Специальные) сообщения).

ПРИМЕЧАНИЕ: *Чтобы ограничить число записей, хранящихся в базе данных по тревогам, следует указать* ***Maximum records in system logs*** *(Максимальное число записей в системных журналах) в меню:* ***Options*** *(Опции)* ***> Server parameters*** *(Параметры сервера)* ***>*** закладка ***Server*** *(Сервер)****.*** *Эта опция служит для ограничения тревожных сообщений в базах данных сервера и рабочих станций.*

Рабочий стол видеонаблюдения (Video Desktop)

Если в системе EntraPass разрешена функция Video (Видеонаблюдение), то один из рабочих столов можно настроить как рабочий стол видеонаблюдения.

Назначение рабочего стола видеонаблюдения

1. В окне **Desktop** (Рабочие столы) щёлкнуть правой кнопкой мыши в любом месте окна, чтобы вызвать меню Desktop properties (Свойства рабочего стола).
2. В поле **Desktop name** (Имя рабочего стола) назначить имя новому рабочему столу.
3. Указать тип окна для этого рабочего стола.
4. Отметить флажком опцию **Video window** (Видеоокно).

Порядок работы с рабочим столом видеонаблюдения

1. В окне Desktop (Рабочие столы) выбрать рабочий стол, который будет использоваться для видеонаблюдения. Откроется окно видеонаблюдения (Video).

2. В нижней части окна выбрать иконку, чтобы указать, например, размер окон или вызвать панель Panel (небольшое окно, привязанное к видеоэкрану). Описание доступных иконок приведём в таблице:

Иконка вида	Описание
	Большое окно, 1024x768 пикселей
	Среднее окно, 800x600 пикселей
	Небольшое окно, 640x480 пикселей
	Миниатюрное окно, 400x300 пикселей
	Создать новое видеоокно

Иконка вида	Описание
	Показать панель windows
Воспроизведение видеофайлов	Эти кнопки появляются на нижней панели рабочего стола видеонаблюдения, если зарегистрировавшийся оператор имеет особые полномочия для просмотра и создания видеособытий. Эти специальные кнопки обеспечивают быстрый способ просмотра или создания видеособытий.
	Редактирует текущее видеоокно
	Выдает подсказку по работе с рабочим столом видеонаблюдения
	Закрывает окно видеонаблюдения (Video)

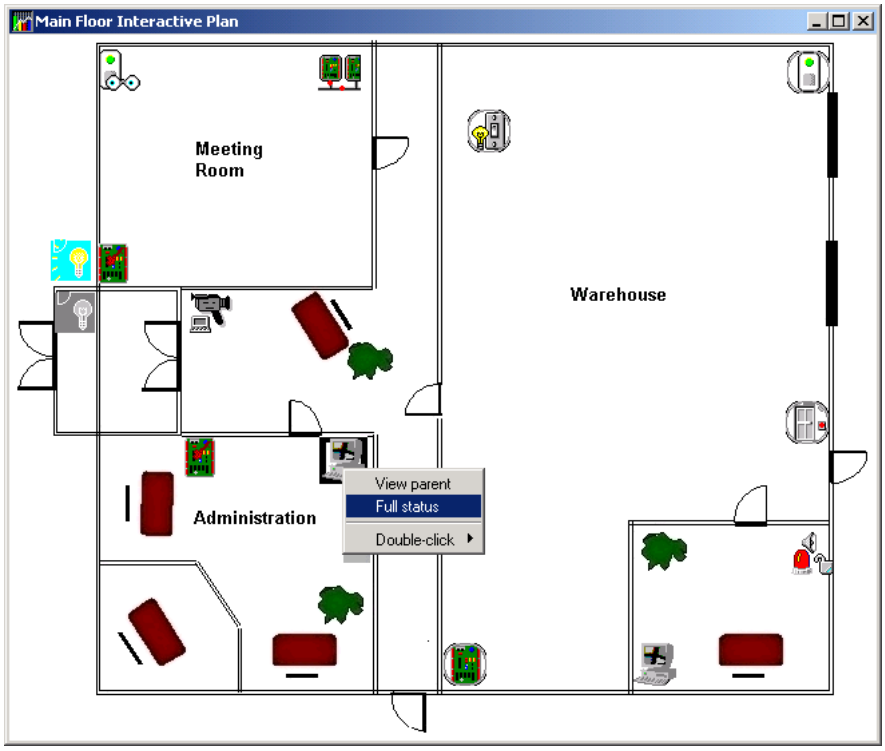
Состояние видеосервера

Система EntraPass обеспечивает отображение параметров видеоустройств, подключённых к видеосерверу. Операторы имеют возможность, например, просматривать информацию о передаче данных по сети (изображения и оцифрованный звук).

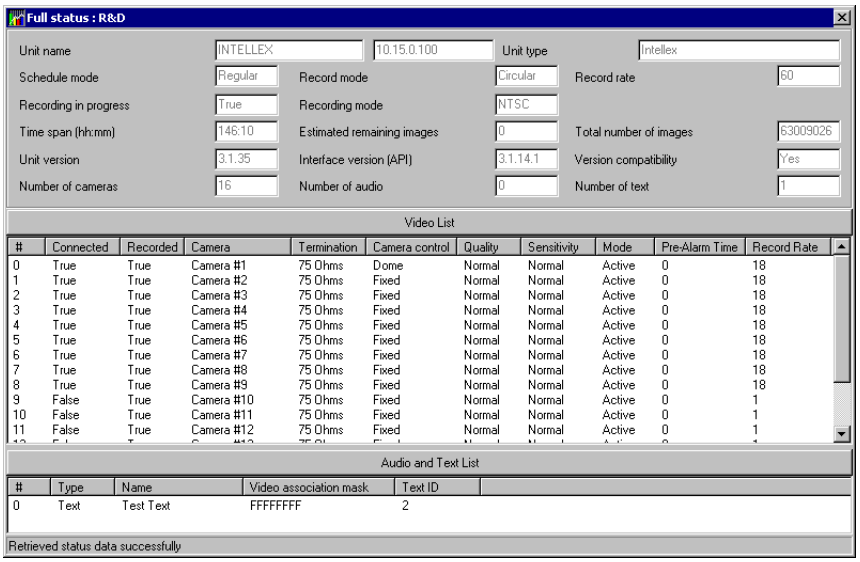
ПРИМЕЧАНИЕ: *Установка и использование функций видеонаблюдения требуют значительных сетевых ресурсов (LAN или WAN). Для оптимизации работы сети рекомендуется обратиться к администратору сети.*

Просмотр полного состояние видеосервера

1 В окне рабочего стола Graphic Desktop (Рабочий стол графических схем) щёлкнуть правой кнопкой мыши по иконке Video Server (Видеосервер), чтобы вызвать контекстное меню.



2 В контекстном меню выбрать пункт **Full status** (Полный статус), чтобы отобразить на экране информацию о статусе видеосервера.



ПРИМЕЧАНИЕ: *Содержание окна Full Status (Полный статус) зависит от типа видеосервера, подсоединённого к системе EntraPass.*

Краткое описание всех отображаемых на экране полей приведено ниже в таблице:

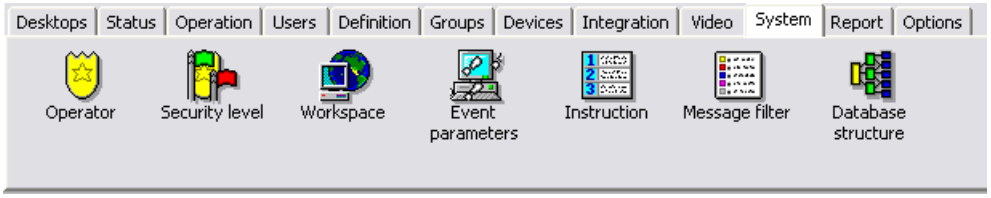
Параметр	Описание
Unit name (Имя устройства)	Сетевое имя удалённой системы видеонаблюдения (например, в проиллюстрированном примере "Intellex"). В соседнем поле отображается IP-адрес видеорегистратора.
Unit type (Тип устройства)	Тип устройства: Intellex, Iris (сетевой клиент) и др.
Schedule mode (Режим расписания)	Текущий режим расписания работы удалённого устройства DVR. Показывает, как видеорегистратор выполняет запись видеоизображений. В этом поле доступны следующие опции: • **Regular** (Обычный график) • **Single** (Только с одной камеры) • **Custom** (Специальное расписание, индивидуально устанавливаемое оператором).
Recording in progress (Выполняется запись)	Статус текущей записи удалённого устройства системы видеонаблюдения. Доступные опции: • **True** (Запись выполняется). • **False** (Запись остановлена).
Time span (Временной интервал)	Временно интервал (в секундах) между самым давним и самым свежим кадрами в базе данных.
Unit version (Версия устройства)	Официальная версия устройства видеонаблюдения.
Number of cameras (Кол-во камер наблюдения)	Кол-во камер наблюдения, подключённых к видеосерверу. Источником видеоданных, как правило, является камера наблюдения, однако вместо камеры может использоваться телевизионная станция или другой источник видеопотока. Допустимые значения – от 0 до 16.
Record mode (Режим записи)	Режим записи может быть нецикличным и цикличным. • **Linear** (Нецикличный) – запись продолжается до тех пор, пока не закончится доступное место для записи; • **Circular** (Цикличный) – видеорегистратор будет заранее предупреждать о нехватке места для записи. В таком случае оператор должен решить, продолжать запись или остановить её. По умолчанию установлен цикличный режим записи (Circular).
Recording mode (Стандарт записи)	Стандарт записи удалённого записывающего устройства. В разных странах используются разные стандарты записи. Доступные опции: • **NTSC** – используется, в основном, в Америке и во многих азиатских странах, включая Японию и Южную Корею, или • **PAL** – применяется, как правило, в Германии, Великобритании, Китае, Австралии и Бразилии.
Estimated remaining images (Примерное число оставшихся кадров)	Расчётное число кадров, которые ещё можно записать в базу данных, пока не закончится свободное место для записи. Эта опция полезна только в том случае, если используется нецикличный режим записи (Linear).
Interface version/API (Версия интерфейса API)	Отображает версию интерфейса, используемого для связи между системой EntraPass и выбранным видеосервером.

Параметр	Описание
Number of audio (Число звуковых каналов)	Число звуковых каналов, доступных на видеосервере. Источником звуковых данных, как правило, является микрофон, однако вместо него может использоваться и другой источник звука.
Record rate (Скорость записи)	Частота смены кадров при записи. Эта величина указывает суммарную скорость записи видеорегистратора, обозначающую число кадров за одну секунду. Допустимые значения: 1, 2,5, 7,5, 15, 30, 60, 120 и др.
Total number of images (Общее число кадров)	Суммарное число кадров, записанных в базе данных удалённого устройства.
Version compatibility (Совместимость версий)	Совместимость между версией видеорегистратора и версией используемого приложения.
Number of text (Число текстовых каналов)	Число каналов с текстовыми данными, доступных из системы видеонаблюдения. В качестве источника текстовых данных может использоваться кассовый аппарат или другое устройство.

Глава 12 • Системные настройки

Панель инструментов System (Системные настройки)

Меню **System** (Системные настройки) служит для указания настроек системных операторов, назначения уровней безопасности, параметров событий, инструкций оператору и фильтров сообщений. Помимо этого, данное меню можно использовать для просмотра структуры базы данных EntraPass.



Системные настройки объединены в следующие группы:

- **Operator** (Операторы) – имена пользователей, обязательный тип карты, регистрационные имена и пароли операторов системы EntraPass

***ПРИМЕЧАНИЕ: Mandatory card type** (Обязательный тип карты) - это опциональное поле. Если эта опция не выделена, то оператор будет создан в любом случае*

- **Security level** (Уровни безопасности) – служит для разрешения или запрещения доступа к логическим компонентам системы (рабочим столам, информационным полям карт и т.п.) при повседневной работе операторов.
- **Workspace** (Рабочее пространство) – это меню используется, чтобы разрешить или запретить доступ операторов к просмотру и настройке физических компонентов системы (шлюзов, сайтов, реле и т.п.).
- **Event parameter** (Параметры событий) – описание приоритетов, цветов, расписаний (вывода на экран, на принтер или с требованием подтверждения) для системных событий
- **Instruction** (Инструкции оператору) – позволяет создавать инструкции оператору по тревожному сообщению.
- **Message filter** (Фильтр сообщений) – служит для пересылки сообщений из одного приложения EntraPass в другое и для задания критериев сортировки сообщений, отправляемых на рабочий стол избранных сообщений (Filtered Message).
- **Database structure** (Структура базы данных) – позволяет выводить на экран физические и логические компоненты системы EntraPass, сортировать их или изменять их параметры.

Назначение операторов

Меню **Operator** (Операторы) служит для назначения системных операторов в систему, задания их уровней доступа и описания прав. Оператор отвечает за создание учетных записей, за выпуск карт, выполняет определённые действия с компонентами системы в ручном режиме управления, запрашивает отчёты, ставит систему на охрану и т.п. В целях обеспечения безопасности каждый оператор, имеющий доступ к базе данных, должен иметь свой профиль, чтобы отслеживать все его действия в системе. Для того чтобы оператор мог использовать и работать в системе EntraPass и получал сообщения о событиях, необходимо создать его учётную запись или изменить учётные записи, созданные по умолчанию.

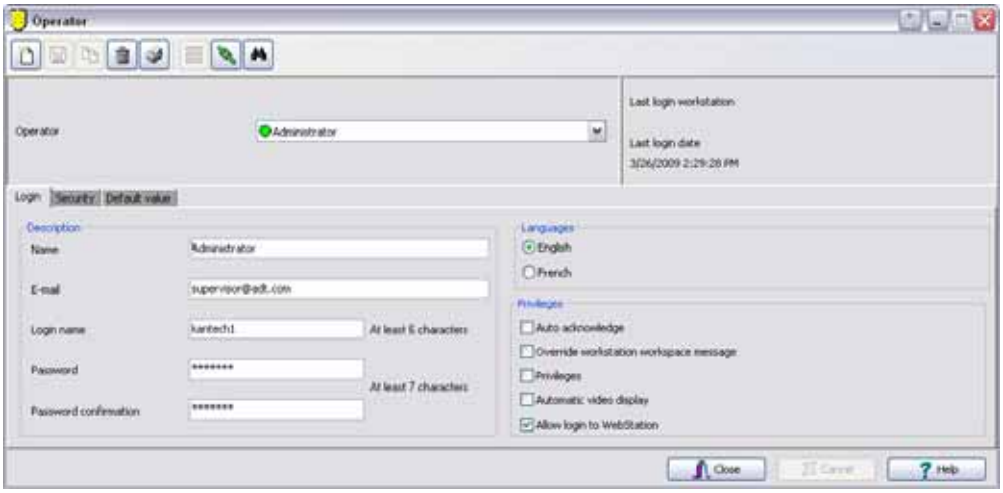
Система уже настроена на работу с тремя операторами. Все они имеют разные уровни доступа:

- Installer (Установщик) – регистрационное имя и пароль "kantech". Полный доступ для просмотра, изменения, удаления и вывода на печать компонентов.
- Administrator (Администратор) – регистрационное имя "Kantech1", пароль "kantech". Умеренный доступ, ограничения на доступ к системным меню.
- Guard (Охранник) – регистрационное имя "Kantech2", пароль "kantech". Ограниченный доступ к системным меню.

ПРИМЕЧАНИЕ: *Вы можете назначать операторов, используя уже настроенных операторов в системе или создавая новые записи. Смотрите в Главе 12 Назначение уровней безопасности' на странице 406 для более подробной информации .*

Создание или изменение данных оператора

1 Открыть закладку **System** (Системные настройки) и нажать кнопку **Operator** (Операторы), чтобы открыть одноимённое окно.



ПРИМЕЧАНИЕ: *В правом верхнем углу окна отображается, когда и на какой рабочей станции EntraPass оператор был зарегистрирован в последний раз.*

2 Указать имя оператора в поле **Name**. Имя оператора может содержать до 40 буквенно-цифровых символов (включая пробелы). Это имя будет отображаться в списках сообщений на рабочих столах и в отчётах.

3 Указать электронный адрес оператора в поле **e-mail** (по желанию).

4 Указать регистрационное имя в поле **Login name**. Это описательное имя оператора, которое может содержать от 6 до 20 буквенно-цифровых символов (включая пробелы).

ПРИМЕЧАНИЕ: *В процессе регистрации операторы должны ввести своё регистрационное имя и пароль, чтобы получить доступ. Регистрационное имя отображается в сведениях о событии, если оно возникло в результате действий оператора (например, при ручном управлении, регистрации в системе, выходе из системы и т.п.).*

5 В поле **Password** (Пароль) указать пароль, который будет использовать оператор при регистрации вместе с регистрационным именем. Пароль может состоять из буквенных и

цифровых символов общей длительностью от 7 до 20 символов. Пароль не отображается на экране (вместо символов отображаются звёздочки), его нельзя вывести на печать.

ПРИМЕЧАНИЕ: *Пароль* ***чувствителен к регистру*** *– все операторы должны быть предупреждены об этом!*

6 В поле **Password Confirmation** (Подтверждение пароля) снова ввести пароль оператора для подтверждения, используя верный регистр. Если пароль в этом поле не идентичен предыдущему, появляется сообщение об ошибке.

7 В разделе **Language** (Языки) следует отметить язык меню на экране для выбранного оператора. Для того чтобы изменения вступили в силу, оператор должен выйти из системы и зарегистрироваться снова. Если после завершения сеанса оператор выйдет из приложения, то следующий зарегистрировавшийся в этом приложении оператор увидит окно запуска приложения на том языке, на котором работал предыдущий оператор.

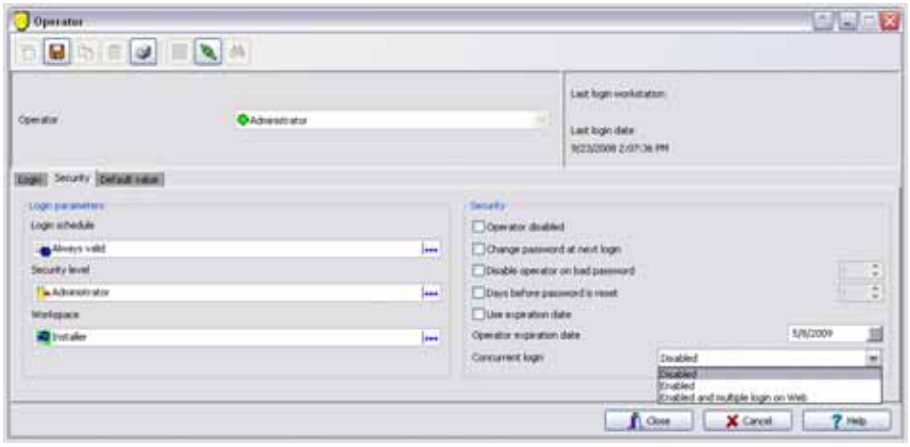
8 В разделе Privileges (Особые права):

- Если необходимо, выделить опцию **Auto acknowledge** (Автоматическое подтверждение). При выделении этой опции на рабочем столе тревог (Alarms) появляется дополнительная кнопка **Manual** (*Смотрите в Главе 12 Системные настройки' на странице 401 для более подробной информации*). Оператор должен решить, как подтверждать события – вручную или автоматически. Это право оператора.
- Если необходимо, отметить флажком опцию **Override workstation workspace message** (Игнорировать сообщения рабочего пространства АРМ). В случае выделения этого поля, базовая конфигурация рабочего пространства рабочей станции игнорируется. Оператор получает сообщения о событиях со всех рабочих станций и шлюзов.
- Если необходимо, то отметить флажком поле **Privileges** (Особые права), чтобы оператор мог просматривать скрытые камеры. Назначение камер следует выполнить в меню: **Video** (Видеонаблюдение) > **Camera** (Камеры) > опция **Show camera** (Показывать камеру).
- **Automatic video display** (Автоматический вывод видео на экран) – автоматически выводить на экран видеофрагменты, снятые по тревоге, для оператора, зарегистрировавшегося в системе. Если рабочий стол тревог правильно настроен и открыт, то видео автоматически будет выведено в его окно. Если АРМ тревог не открыт, тогда система проверит видеонастройки для указанной рабочей станции (**Devices** (Устройства) > **Messages 2 of 2** (Сообщения 2 из 2), **Disable autodisplay of video views** (Запретить автоматическое отображение окон видеонаблюдения)). Если эта опция не активирована (Отключена), тогда будет выполнена проверка настроек видеонаблюдения для данного оператора: **Operator** (Оператор) > **Automatic video display** (Автоматическое отображение видео).

ПРИМЕЧАНИЕ: *Опция* ***Override workstation workspace message*** *(Игнорировать рабочее пространство рабочей станции) относится к особым правам, предоставляемым операторам. Таким образом, операторы могут получать сообщения обо всех событиях, независимо от того, на какой рабочей станции они зарегистрировались в данный момент. При выборе этой опции вместе с опциями рабочей станции* ***Apply operator parameters for messages*** *(Применить параметры оператора к сообщениям) и* ***Apply operator parameters for alarms*** *(Применить параметры оператора к тревогам) базовая конфигурация игнорируется, и события будут отобраны в соответствии с уровнем доступа оператора, который в данный момент зарегистрирован на этой рабочей станции.*

- Если требуется, выделить опцию **Allow login to WebStation** (Разрешить регистрацию на веб-станции) для оператора. Возможность установки флажка напротив опции появляется только после регистрации веб-станции (WebStation) на сервере EntraPass Server

9 Открыть закладку **Security** (Уровни безопасности) для настройки параметров доступа оператора.



10 В выпадающем меню **Login Schedule** (Расписание для входа в систему) указать расписание доступа оператора в систему. При необходимости можно создать определённое расписание для любого оператора (**Definition** (Назначения) > **Schedule** (Расписания)) и затем прикрепить его к этому оператору.

ПРИМЕЧАНИЕ: *Чтобы оператор мог регистрироваться в разных приложениях EntraPass или на сервере EntraPass, следует пройти в меню* ***System*** *(Системные настройки) >* ***Security Level*** *(Уровни безопасности) > закладка* ***Miscellaneous*** *(Прочее) и установить флажок напротив опции* ***Allow login on application*** *(Разрешить регистрацию в приложении) и/или* ***Allow login on server****" (Разрешить регистрацию на сервере).*

11 В списке **Security Level** (Уровни безопасности) выбрать уровень доступа оператора к различным компонентам программного обеспечения. Уровень безопасности определяет, какие меню доступны для оператора при выполнении им различных операций: изменении базы данных, создании новых компонентов, просмотре сведений о компонентах и событиях и т.д.

ПРИМЕЧАНИЕ: *В системе EntraPass предусмотрена возможность создания до 250 индивидуально настроенных уровней безопасности; в заводских настройках предусмотрены три уровня безопасности: Installer (Установщик), Administrator (Администратор) и Guard (Охранник). Работники с правами установщика по умолчанию имеют доступ ко всем компонентам системы. Установщики должны настроить другие уровни безопасности таким образом, чтобы ограничить доступ операторов к командам и/или функциям меню.*

12 В выпадающем списке **Workspace** (Рабочее пространство) выбрать рабочее пространство оператора, то есть указать, к каким компонентам системы (рабочим столам, информационным полям карт и т.п.) будет иметь доступ оператор при выполнении своих ежедневных обязанностей.

ПРИМЕЧАНИЕ: *Система EntraPass выпускается с одним настроенным рабочим пространством для установщика, которое доступно при установке EntraPass.*

13 Перейти к закладке **Security** (Безопасность) для изменения параметров безопасности для текущего профиля оператора:

- **Operator disabled** (Оператор заблокирован) – служит для временного отстранения от работы или ограничения в правах оператора до завершения установленного срока действия его полномочий. Если указать имя оператора и выделить эту опцию, то выбранный оператор не сможет запустить данное приложение.
- **Change password at next login** (Изменить пароль при следующем входе в систему) – эту опцию следует отметить, если необходимо, чтобы оператор сменил пароль при следующей регистрации в системе.
- **Disable operator on bad password** (Запретить доступ при неверном вводе пароля) – служит для ограничения числа попыток ввода пароля. Например, если указано три (3) попытки, то после трёх неудачных вводов своего пароля оператор будет заблокирован.
- **Days before password is reset** (Частота изменения пароля, дней) – эта опция помогает организовать работу с паролями операторов. После окончания срока, указанного в этом поле, оператору будет предложено сменить свой пароль.

- **Use expiration date** (Срок окончания действия полномочий) – эта опция помогает организовать работу с паролями операторов. При её выделении следует указать в соседнем поле дату окончания действия полномочий оператора.
- **Operator expiration date** (Дата окончания действия полномочий) – предназначена для блокировки прав оператора в указанный день. Используется вместе с опцией **Use expiration date**.
- **Одновременная авторизация** (concurrent logins):
  - Для одновременной авторизации в приложении EntraPas несколькими операторами под одним и тем же паролем, включите эту опцию, выберите **Enabled**.
  - Для одновременной авторизации на приложении Entra Pass и на EntraPass WebStations, выберите функцию **Enabled with concurrent logins from WebStations** (Включить одновременную авторизацию на WebStation).

ПРИМЕЧАНИЕ: *Компонент WebStation должен быть зарегистрирован на сервере EntraPass Server, для показа этой опции.*

Одновременная авторизация

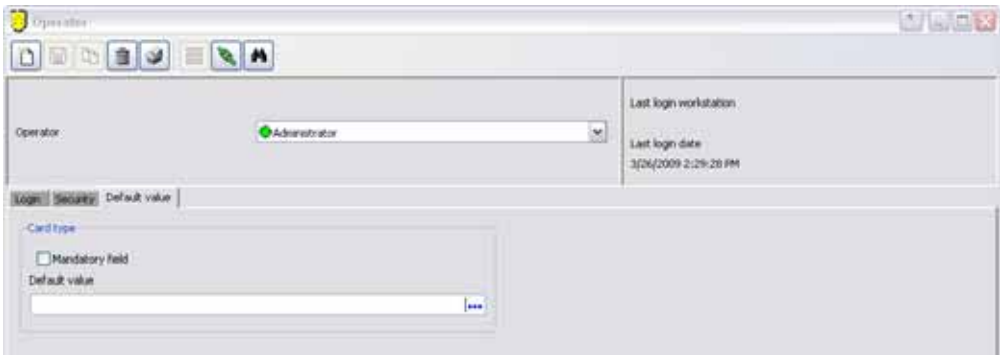
Приложение EntraPass позволяет одновременную или параллельную авторизацию на EntraPass WebStation. При условии, что это не превышает количество открытых лицензий для Entra Pass Webstation. Смотрите Табл. 12-1 для большей информации.

Table 12-1: Одновременная авторизация

Номер для заказа	Описание	Максимальное количество одновременных подключений
EntraPass Corporate Edition		
E-COR-WEB-1	1 WebStation Соединение	3
E-COR-WEB-3	3 WebStation Соединение	
EntraPass Global Edition		
E-GLO-WEB-1	1 WebStation Соединение	20
E-GLO-WEB-3	3 WebStation Соединение	

ПРИМЕЧАНИЕ: *Все внесённые в профиль оператора изменения начинают действовать при следующей попытке войти в систему.*

13 Нажмите на вкладку **Default value** (значения по умолчанию) чтобы выбрать обязательный тип карты (mandatory card type) (опция).



14 Чтобы включить опцию **Mandatory field** (обязательное поле), поставьте галочку.

15 Нажмите на многоточие, чтобы выбрать тип карты.

Назначение уровней безопасности

Уровни безопасности служат для описания прав доступа операторов к логическим компонентам системы EntraPass (рабочим столам, информационным полям карт и т.п.), а также для выполнения определённых действий с этими компонентами.

ПРИМЕЧАНИЕ: *Чтобы ограничить доступ операторов к командам и/или функциям меню, следует создать и/или настроить соответствующие уровни безопасности.*

Система выпускается с уже созданными настройками трёх операторов и трёх уровней безопасности: установщик, администратор и охранник. Уровни доступа операторов можно настраивать индивидуально. В системе предусмотрена возможность создания до 250 уровней безопасности. Каждому оператору назначается уникальное регистрационное имя, пароль и соответствующий уровень безопасности. Пароль чувствителен к регистру.

- **Installer** (Установщик):
  - **Login name and password** (Регистрационное имя и пароль) - kantech
  - **Security level** (Уровни безопасности) – по умолчанию, пользователь с правами установщика имеет полный доступ ко всем меню системы. Установщик может просматривать и изменять компоненты и имеет неограниченные права доступа к системе.
- **Administrator** (Администратор):
  - **Login name** (Регистрационное имя) – kantech1, **Password** (Пароль) – kantech
  - **Security level** (Уровни безопасности) - администратор. По умолчанию, пользователь с правами администратора имеет ограниченный доступ к некоторым системным меню.
- **Guard** (Охранник):
  - **Login name** (Регистрационное имя) – kantech2, **Password** (Пароль) – kantech
  - **Security level** (Уровни безопасности) - охранник. По умолчанию, пользователь с правами охранника имеет ограниченный доступ к системным меню.

Создание/Изменение уровней доступа операторов

Процедура назначений уровней безопасности для операторов является очень важной для всей системы. Действительно, если уровень безопасности предоставляет полный доступ к меню системы, то операторы с этим уровнем доступа смогут изменять системные параметры. Поэтому необходимо следить, чтобы уровень доступа операторов соответствовал их служебным обязанностям. Все пункты в меню Security Level (Уровни безопасности) расположены в виде корневого дерева, так что для выбора доступны все компоненты. Структура дерева позволяет выделять отдельные компоненты при описании уровней доступа в режиме ручного управления.

Каждый уровень доступа отмечен своим цветом: полный доступ – зелёного, доступный только для чтения – жёлтого, а полный запрет – красного цвета. Руководитель службы безопасности или оператор, наделённый соответствующими полномочиями, может быстро изменить или назначить новые доступные компоненты для более низких уровней безопасности просто двойным щелчком мыши по выбранному компоненту, меняя цветовой код, пока он не будет соответствовать нужному уровню безопасности.

ПРИМЕЧАНИЕ: *Операторы не увидят те позиции меню, к которым у них нет доступа.*

1 В закладке **System** (Системные параметры) нажать на иконку **Security level** (Уровни безопасности). На экране должно открыться окно Security level с открытой закладкой **Menu** (Меню).

2 В выпадающем списке выбрать уровень безопасности, настройки которого необходимо изменить.

- Чтобы создать новый уровень безопасности, следует нажать кнопку **New** (Создать) и ввести необходимые данные на используемых языках в полях справа.

3 В списке под закладкой **Menu** установить многократным двойным щелчком мыши нужный статус для всех компонентов: **No access** = красный (Доступ запрещён)**, Read-only** = жёлтый (Доступно только для чтения) или **Full access** = зелёный (Полный доступ)**.**

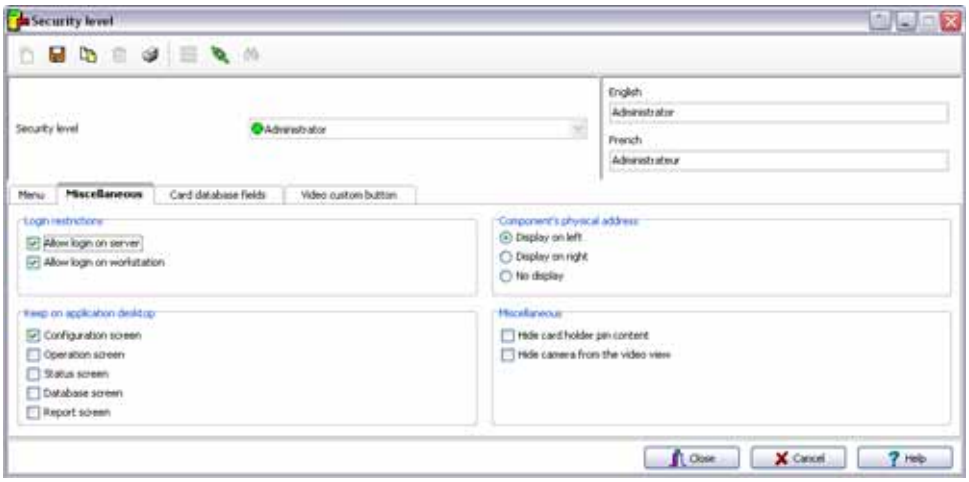
ПРИМЕЧАНИЕ: *Пользователи с правами "только для чтения" не имеют прав для вывода данных на печать в системе EntraPass.*

Назначение регистрационных прав для оператора

Закладка **Miscellaneous** (Прочее) позволяет вам назначать регистрационные параметры операторов (логин/пароль) и параметров отображения на экране различной информации:

- Опции авторизации оператора: вы можете разрешить или отключить необходимость авторизации на АРМ или на сервере.
- Активные окна, которые могут держаться на рабочем столе: EntraPass позволяет операторам на рабочем столе пять активных окна.
- Опции отображения компонентов: компоненты могут быть отображены с или без физического адреса. Физический адрес может появляться слева или справа имени компонента.

1 Открыть закладку **Miscellaneous,** чтобы настроить параметры выбранного уровня безопасности.



2 В разделе **Login restrictions** (Ограничения авторизации) выделить нужные опции:

- В поле **Allow login on server** (Разрешить регистрацию на сервере) поставить отметку, если необходимо разрешить оператору регистрироваться на сервере EntraPass (основном или резервном).
- В поле **Allow login on workstation** (Разрешить регистрацию на рабочей станции) поставить отметку, если необходимо разрешить оператору регистрироваться в любом приложении в системе.

3 Раздел **Keep on application desktop** (держать приложения на рабочем столе) позволяет увеличить число активных окон на рабочем столе пользователей. С помощью этой опции операторы могут открывать до пяти окон одновременно: одно окно конфигурации и четыре окна другой категории. Все окна системы EntraPass можно разделить на пять категорий

- **Configuration screen** (Окно настройки конфигурации) – к этой категории относятся все меню, используемые при программировании системы. Сюда входят меню **User** (Пользователи), в том числе такие разделы как Card (Идентификационные карты), Badging (Электронные пропуска), Card access group (Группы доступа для карт), Access level (Уровни доступа), Visitor (Карты посетителей), Card type (Тип карт); меню **Definition** (Описания); меню **Group** (Группы); меню **Devices** (Устройства); меню **System** (Системные настройки); меню **Video** (Видеонаблюдение); **Historical reports** (Архивные отчёты) и **Time and attendance report** (Отчёты по учёту рабочего времени).
- **Operation screen** (Окно управления) – к этой категории относятся все пункты меню Operations и функция просмотра видеозаписей.
- **Status screen** (Окно состояния) – в эту группу входят окна меню Status (Состояние), меню Current recording (Текущие записи) и Report state (Статус отчётов).
- **Database screen** (Окно базы данных) – в эту категорию входят следующие меню: Option (Опции), включая подменю Card format (Формат карты), Authentication password (Аутентификационный пароль), Select languages (Выбор языков), Printers options (Опции принтера), Changes date and time (Изменение даты и времени) и др.; пункты меню User (Пользователи): Daypass (Разовые пропуска), Batch operations (операции с группами) и Import/ Export CSV (Импорт/экспорт файлов CSV); View Report (Отчёты по видеонаблюдению), Operation on T&A (Операции по учёту рабочего времени) и View exported videos (Просмотр экспортированных видеофайлов).
- **Report screen** (Окно отчётов) – в эту группу входят запросы для создания быстрых отчётов (Quick Report), архивных отчётов (Historical report) и отчётов по учёту рабочего времени (Time and attendance report), а также Video list (Списки видеозаписей).

ПРИМЕЧАНИЕ: *Благодаря перечисленным выше опциям операторы имеют возможность вывести на рабочий стол несколько активных окон одновременно. Выдвинуть окно на передний план или отправить на задний план можно простым нажатием **[ALT-F6]**.*

4 В разделе **Components physical address** (Физический адрес компонента) указать, каким образом система должна отображать на экране физический адрес компонента. От этого зависит также способ сортировки компонентов.

- **Display on left** (Показывать слева) – при выделении этой опции компоненты будут отсортированы по своему адресу (например, 01.01.01 Controller xyz).
- **Display on right** (Показывать справа) – при выделении этой опции сортировка компонентов выполняется по имени компонента (например, 01.01.01 Controller xyz).
- **No display** (Не отображать) – при выделении этой опции адрес не отображается (например, Controller xyz), а сортировка компонентов выполняется по имени компонента.

5 На вкладке **Miscellaneous** (Дополнительно):

- **Hide card holder pin content** (Спрятать PIN код карты)**:** если выбрано, то эта функция имеет возможность спрятать PIN код картодержателя от просмотра.
- В случае использования функции видеонаблюдения программное обеспечение EntraPass позволяет запретить видеонаблюдение на отдельных объектах для определённых уровней доступа операторов, используя опцию **Hide camera from video views** (Скрыть камеры от видеонаблюдения).

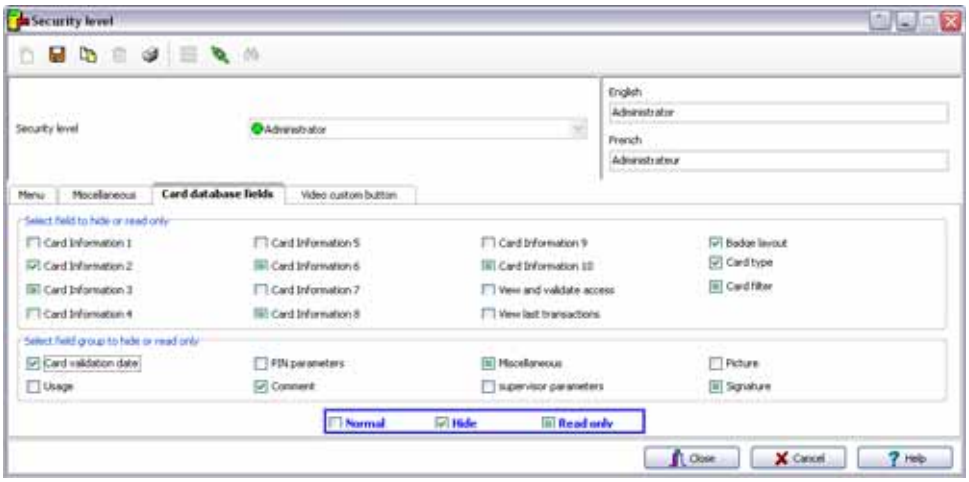
ПРИМЕЧАНИЕ: *Опция **Hide camera form video view** означает, что система должна сначала проверить, разрешён ли доступ, а затем загрузить изображение с камер в окно видеонаблюдения. Например, если уровень безопасности оператора настроен таким образом, что доступ к видеосерверу разрешён, но не ко всем камерам, описанным в видеосервере, и есть доступ к выбранному видеоокну, то камеры, которые не были выделены при назначении доступа к видеосерверу, будут скрыты от наблюдения. Смотрите в Главе 12 Ограничение доступа к отдельным камерам наблюдения' на странице 422 для более подробной информации .*

Как скрыть информационные поля карты

Система EntraPass позволяет сделать информационные поля карт недоступными для просмотра. Допустим, необходимо разрешить пользователям с определённым уровнем безопасности (например, охранникам) просматривать или изменять информационные поля идентификационных карт. Для этого нужно указать уровень безопасности в поле Security Level, открыть закладку **Card database Fields** (Поля карт) и поставить флажки напротив тех полей, которые должны быть скрыты.

1 Открыть закладку **Card fields**, чтобы ограничить число информационных полей в картах, которые будут видны оператору с указанным уровнем доступа.

ПРИМЕЧАНИЕ: *Параметры ревизора в поле card database field (поле карт) доступно только с EntraPass Global Edition.*

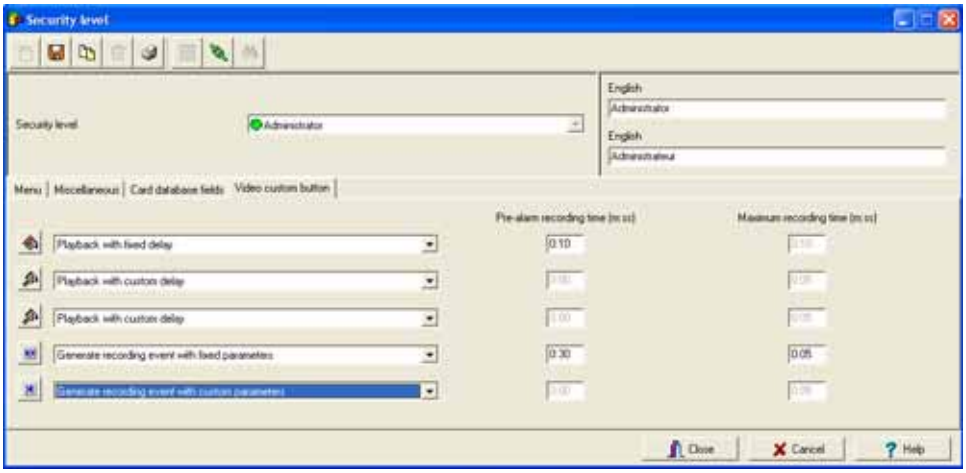


2 Указать поля (по отдельности или группами), которые должны быть скрыты для пользователей с выбранным уровнем безопасности. Выберите на нижней вкладке одно из состояний (нормальный, только чтение, скрыть).

Выбор специальных кнопок для управления в режиме видеонаблюдения

В системе EntraPass предусмотрена возможность индивидуального назначения пяти кнопок для работы в режиме видеонаблюдения (Video). Установщики и администраторы системы имеют возможность настроить по желанию кнопки, используемые операторами на рабочем столе видеонаблюдения (Video). Например, они могут выбрать кнопку для включения режима воспроизведения с фиксированной длительностью, которая определяется как сумма времени предтревожной записи и длительности основной записи, и назначить эту специальную кнопку для пользователей с определённым уровнем безопасности. В случае назначения специальной кнопки для выполнения особой задачи (просмотра или создания видеособытий), на рабочем столе появляются дополнительные кнопки (**Desktops** (Рабочие столы) > Desktop dedicated to video viewing (Рабочий стол для видеонаблюдения).

1 В выпадающем списке **Security level** (Уровни безопасности) выбрать уровень безопасности, настройки которого необходимо изменить.



2 Открыть закладку **Video custom button** (Специальные кнопки видеонаблюдения), чтобы назначить для этого оператора доступные функции. Все доступные функции перечислены ниже:
- Воспроизведение фрагмента фиксированной длительности
- Воспроизведение фрагмента любой выбранной длительности
- Генерирование события, инициирующего запись, с фиксированными параметрами
- Генерирование события, инициирующего запись, с индивидуальными параметрами

3 Выделить опции, которые нужно назначить для данного оператора.

ПРИМЕЧАНИЕ: *При нажатии кнопки с функцией* ***Playback with fixed delay*** *воспроизведение будет включено на определённый период времени. В это время включено время предтревожной записи и максимальное время записи.*

Назначение рабочего пространства

Меню Workspace позволяет системных администраторам разрешить или запретить доступ операторов к просмотру и настройке физических компонентов системы (шлюзов, сайтов, реле и т.п.). Рабочие пространства операторов зависят от типа выполняемых ими задач в системе EntraPass (создание и редактирование компонентов, просмотр компонентов, печать списков или отчётов и др.). Те операторы, для которых специально назначено определённое рабочее пространство, не могут просматривать и изменять компоненты EntraPass, не входящие в это рабочее пространство. Кроме того, рабочие пространства операторы могут использовать для того, чтобы выделить те данные, которые они хотят видеть на экране. Например, системному администратору, имеющему доступ ко всем компонентам системы, может потребоваться отображать на экране только отдельные компоненты. В этом случае он может создать особое рабочее пространство для данной среды и работать только с желаемыми параметрами.

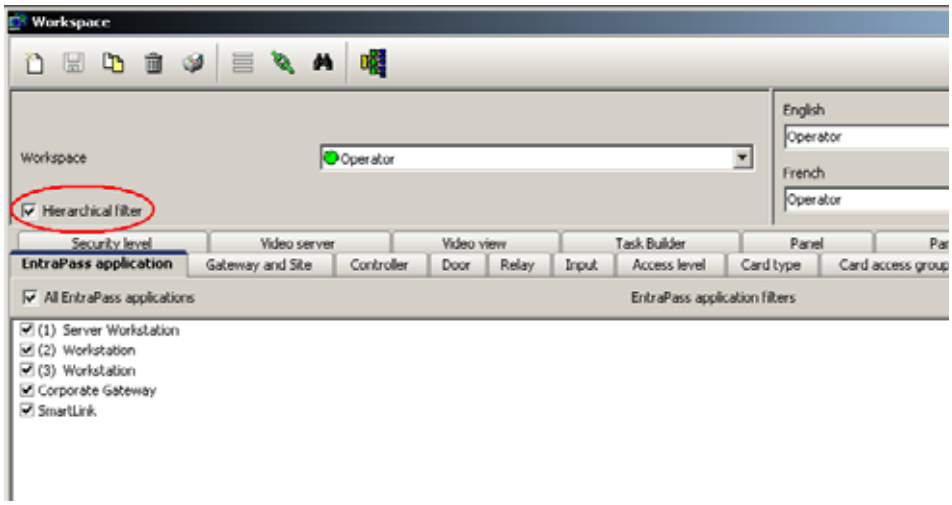
ПРИМЕЧАНИЕ: *Система EntraPass выпускается с одним настроенным рабочим пространством для установщика, которое создаётся при установке EntraPass.*

Использование фильтров для рабочего пространства

- **Hierarchical filter** (Иерархический фильтр) – компоненты в списке отображаются в зависимости от того, какой родительский компонент был выбран. Например, при выборе луча (родительский элемент) система автоматически перестраивается и отображает только соответствующие контроллеры (дочерние элементы). А при выборе определённого контроллера (родительский элемент) система автоматически выводит на экран только соответствующие двери (дочерние элементы) и т.п.

ПРИМЕЧАНИЕ: *Если в закладке ничего не отображается, следует убедиться, что указанные компоненты действительно относятся к выбранному родительскому объекту.*

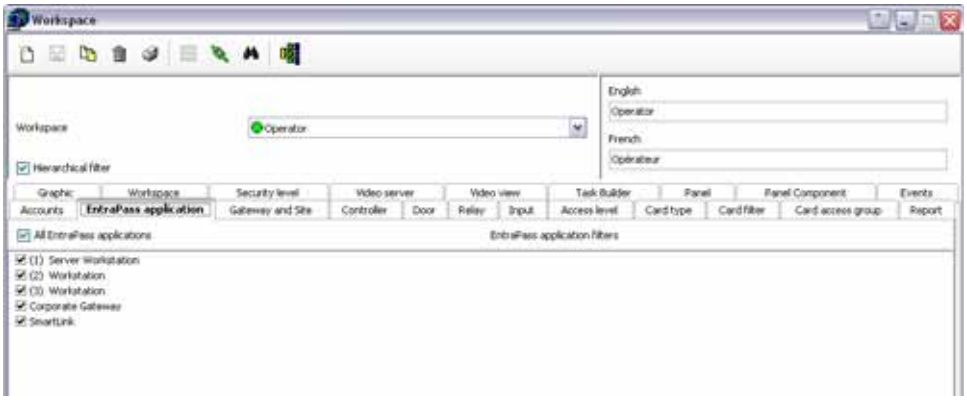
- После того как вы выбрали Иерхаический режим фильтрации, он будет оставаться под всеми вкладками.



Выбор приложений Entra Pass

Это преимущество позволяет вам выбрать приложения, которые будут доступны оператору, который назначен в этом рабочем пространстве (workspace). В следующем примере, рабочее пространство (Administrator) не будет видеть сообщения, отправляемые приложением EntraPass SmartLink, потому что это не назначено для этого рабочего пространства.

1 На вкладке **Workspace** (Рабочее пространство), выберите то рабочее пространство, которое вы хотите назначить или править.



ПРИМЕЧАНИЕ: *Если для выбранного оператора разрешена опция Network alarms message desktop (Рабочий стол сообщений о сетевых тревогах), настраиваемая в меню Desktops (Рабочие столы), то на экране будут отображаться только те тревожные события, которые возникли в указанных в этом окне приложениях и компонентах EntraPass. В этом случае рабочее пространство выступает в качестве фильтра для рабочего стола "Network alarms message desktop".*

- Если необходимо, выделить поле **All EntraPass applications** (Все приложения EntraPass), чтобы все отображаемые на экране приложения сделать доступными для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые приложения EntraPass из общего списка.

2 Сохранить внесённые изменения.

Назначение шлюзов и сайтов

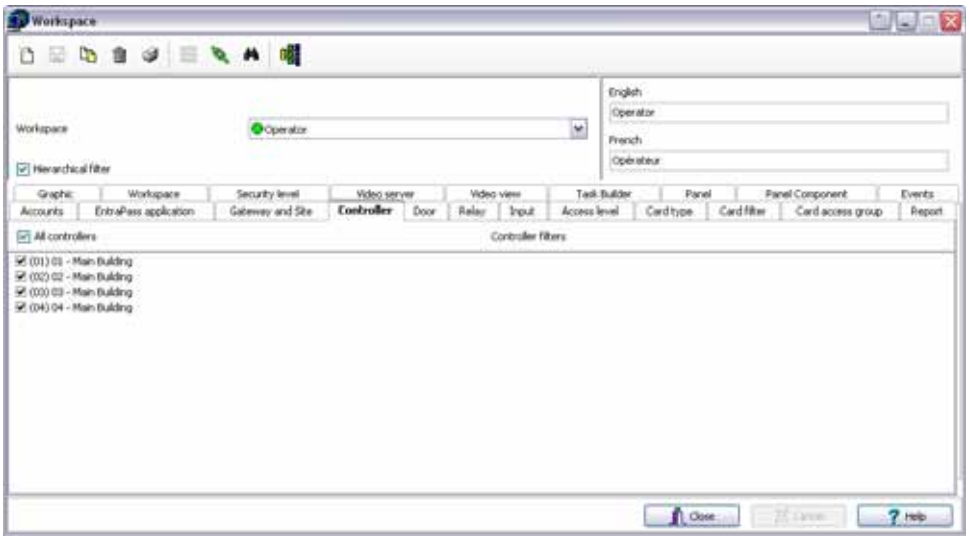
1 Открыть закладку **Gateway and Site** (Шлюзы и сайты/лучи), чтобы выделить список шлюзов и лучей, доступных оператору, за которым закреплено данное рабочее пространство.

- Если необходимо, выделить опцию **All gateways and sites** (Все шлюзы и сайты/лучи), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все шлюзы и сайты, отображаемые на экране.
- Либо выделить определённые шлюзы и сайты/лучи из общего списка

2 Сохранить внесённые изменения.

Назначение контроллеров

1 Открыть закладку **Controller** (Контроллеры), чтобы выделить список контроллеров, доступных оператору, за которым закреплено данное рабочее пространство.



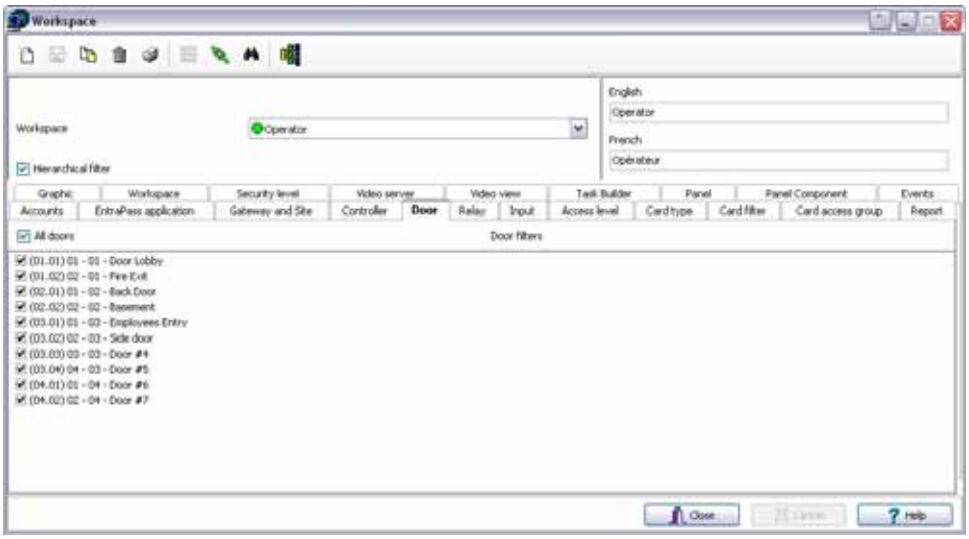
- Если необходимо, выделить опцию **All controllers** (Все контроллеры), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все контроллеры, отображаемые на экране.
- Либо выделить определённые контроллеры из общего списка.

2 Сохранить внесённые изменения.

ПРИМЕЧАНИЕ: *При выделении контроллера выполняется выделение всех компонентов, закреплённых за этим контроллером или связанных с ним (например, дверей, реле, входов, выходов). Кроме того, необходимо выделить шлюз, к которому относится данный контроллер (закладка **Gateway and Site**). Если не выделить шлюз, то контроллер будет недоступным, даже если его выделить в списке.*

Назначение дверей

1 Открыть закладку **Door** (Двери), чтобы выделить список дверей, доступных оператору, за которым закреплено данное рабочее пространство.

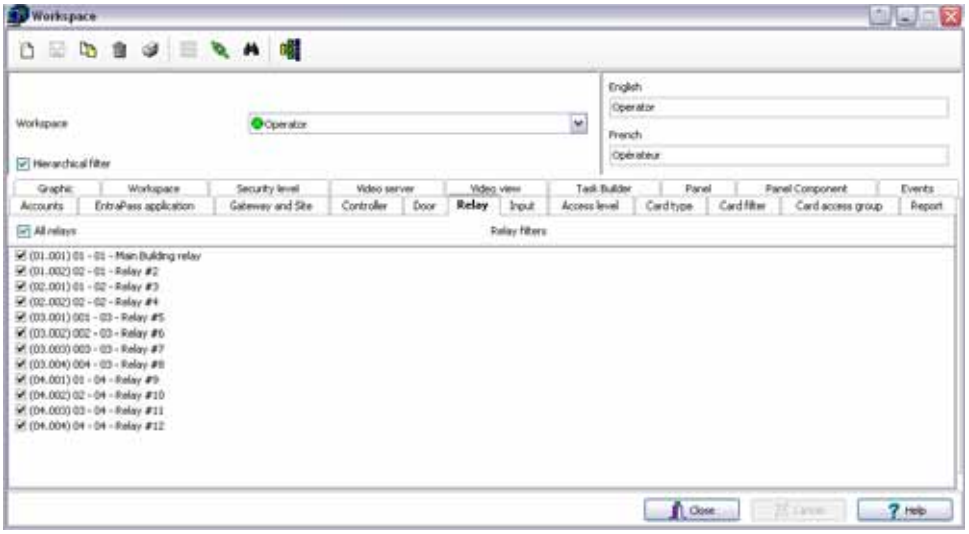


- Если необходимо, выделить опцию **All doors** (Все двери), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все двери, отображаемые на экране.
- Либо выделить определённые двери из общего списка.

2 Сохранить внесённые изменения.

Назначение реле

1 Открыть закладку **Relay** (Реле), чтобы выделить список реле, доступных оператору, за которым закреплено данное рабочее пространство.

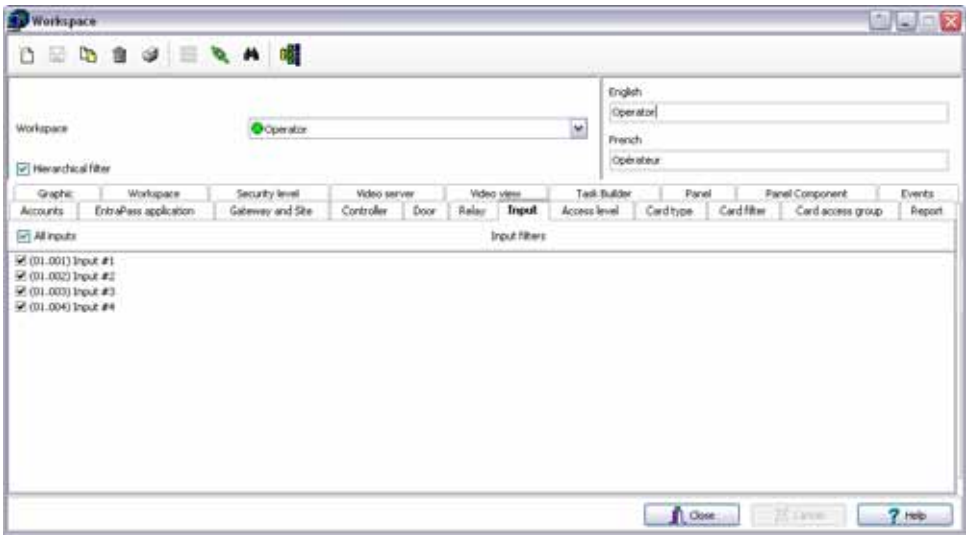


- Если необходимо, выделить опцию **All relays** (Все реле), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все реле, отображаемые на экране.
- Либо выделить определённые реле из общего списка.

2 Сохранить внесённые изменения.

Назначение входов

1 Открыть закладку **Input** (Входы), чтобы выделить список входов, доступных оператору, за которым закреплено данное рабочее пространство.



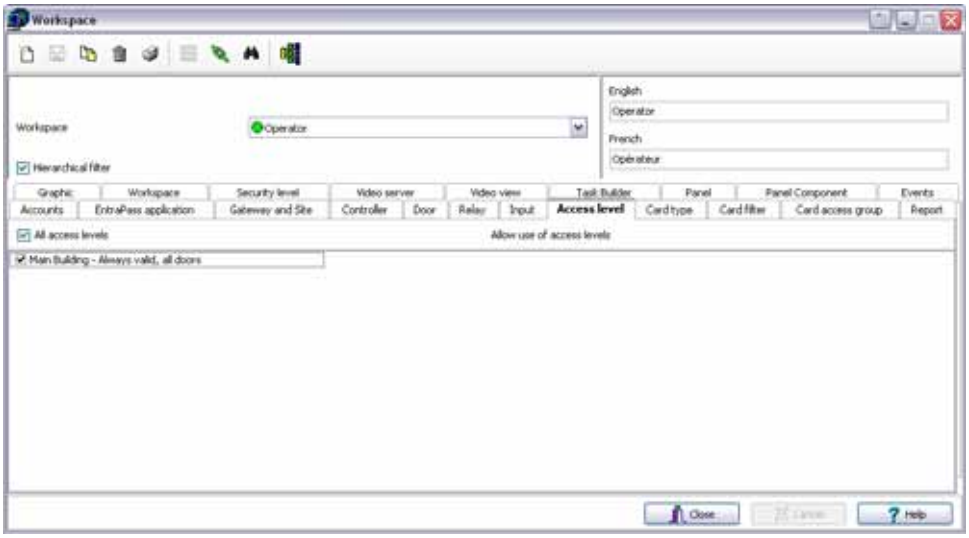
- Если необходимо, выделить опцию **All inputs** (Все входы), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все входы, отображаемые на экране.
- Либо выделить определённые входы из общего списка.

2 Сохранить внесённые изменения.

Назначение уровней доступа

Привязка определённых уровней доступа к рабочему пространству позволяет указать, какие уровни доступа оператор может настраивать или изменять. Например, охранник службы безопасности может иметь право выпускать карты, действительные только для определённой двери или определённого уровня доступа.

1 Открыть закладку **Access level** (Уровни доступа), чтобы выделить список уровней доступа, действительных для оператора, за которым закреплено данное рабочее пространство.



- Если необходимо, выделить опцию **All access levels** (Все уровни доступа), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все отображаемые на экране уровни доступа.
- Либо выделить определённые уровни доступа из общего списка.

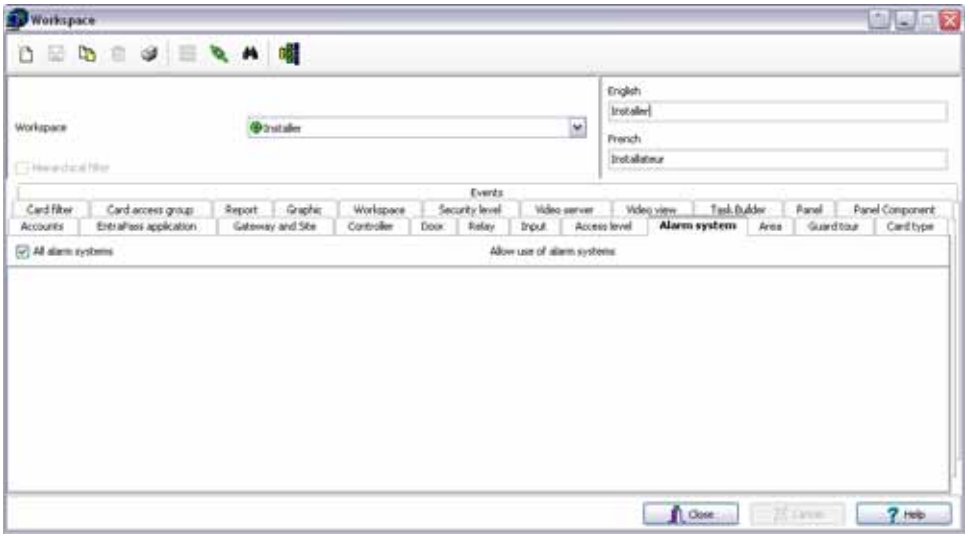
2 Сохранить внесённые изменения.

ПРИМЕЧАНИЕ: *Кроме того, необходимо выделить шлюз, к которому относится описанный уровень доступа. Если шлюз не будет выделен, то уровень доступа будет недоступным, даже если его выделить в списке.*

Назначение тревожной системы

Соотношение тревожной системы с рабочей областью позволяет вам контроллировать тревожные системы, которые оператор может назначать и изменять.

1 Нажмите на вкладку **Alarm system** (Тревожная система), чтобы выбрать список тревожных систем, которые будут доступны оператору, которому назначено данное пространство.



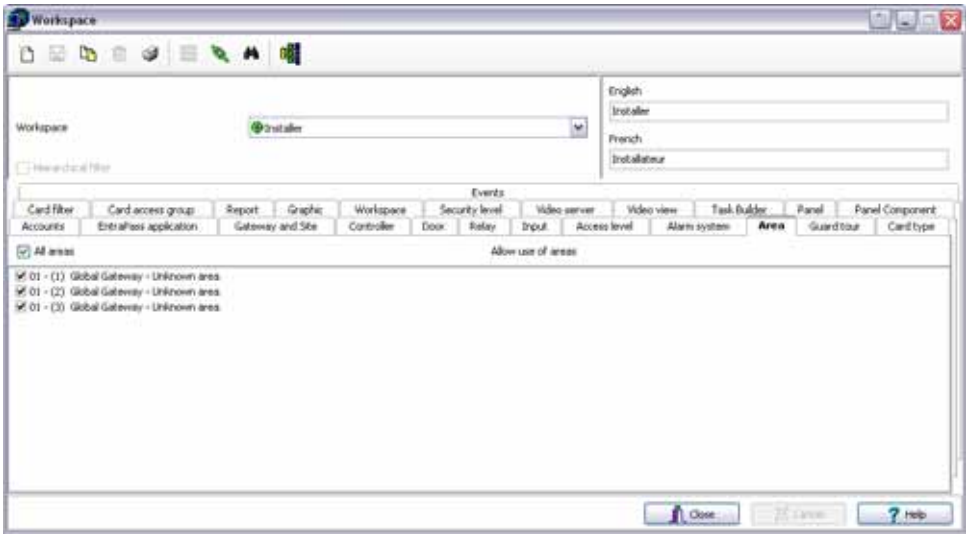
- Выберите **All alarm systems** (все тревожные системы), если вы хотите, чтобы все тревожные системы были доступны оператору этой рабочей области.
- Вы можете также выбрать определенные тревожные системы из отображаемого списка.

2 Сохраните ваши изменения.

Назначение областей

Соотношение областей с рабочей областью позволяет вам контроллировать области, которые оператор может назначать и изменять.

1 Нажмите на вкладку **Area,** чтобы увидеть лист доступных областей, которые будут доступны оператору, который назначен на этой области.



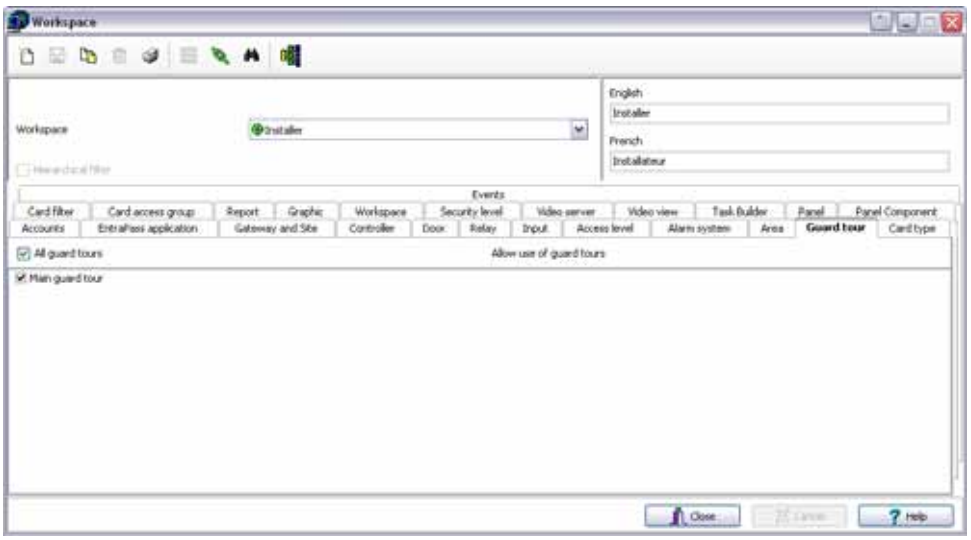
- Выберите вкладку **All areas** (Все области), если вы хотите чтобы все области были доступны оператору, назначенному в этой области.
- Вы можете также выбрать области из отображаемого списка.

2 Сохраните ваши изменения.

Назначения Guard Tours

Соотношение guard tour с рабочим пространством позволяет вам контроллировать перечень guard tour, которые могут быть назначены или изменены оператором этой рабочей области.

1 Нажмите на вкладку **Guard tour,** чтобы выбрать из списка доступных guard tour, которые будут доступны охраннику, которому будет назначено данное рабочее пространство.



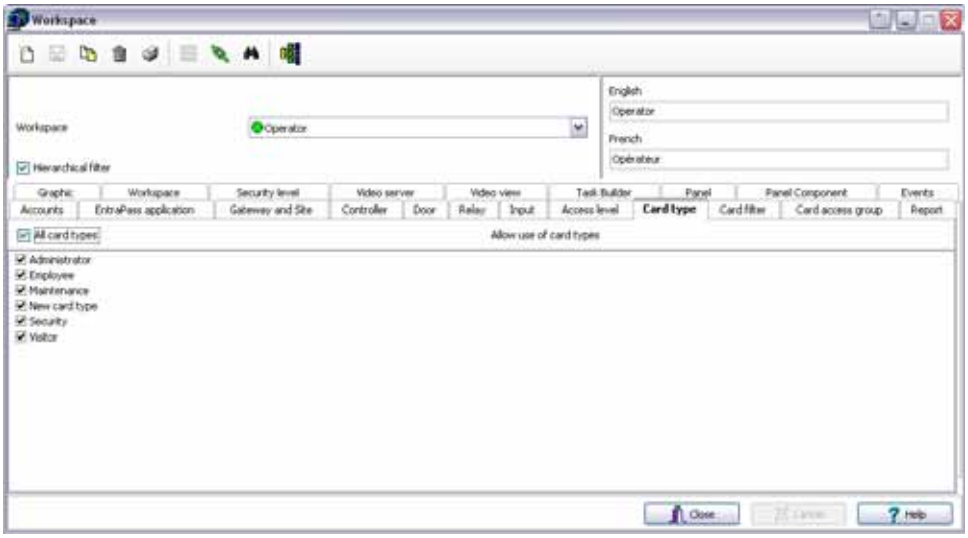
- Выберите **All guard tours** (все guard tour), если вы хотите чтобы оператору были доступны все туры, который назначен для работы в данной рабочей области.
- Вы можете также выбрать список индивидуальных guard tour из отображенного списка.

2 Сохраните ваши изменения.

Назначение типов идентификационных карт

Эта функция ограничивает возможности операторов. А именно, типы карт, не отмеченные в этом меню, не будут доступны оператору при создании и редактировании карт. Допустим, требуется запретить операторам, работающим в рабочем пространстве Guard, выпускать карты определённого типа, например, Security. Для этого следует выделить рабочее пространство Guard и в закладке Card type снять флажок напротив строки Security.

1 Открыть закладку **Card type** (Типы карт), чтобы выделить типы карт, доступных оператору, за которым закреплено данное рабочее пространство.



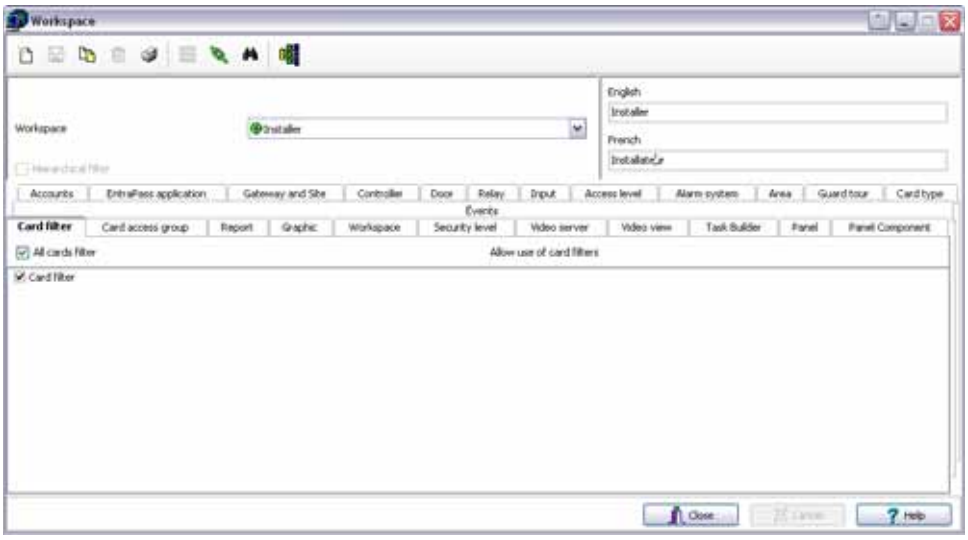
- Если необходимо, выделить опцию **All card types** (Все типы карт), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все типы карт.
- Либо выделить определённые типы карт из общего списка.

2 Сохранить внесённые изменения.

Назначение фильтров карт

Соотношение фильтров карт с рабочим пространством, позволяет вам контроллировать фильтры карт, которые оператор может назначать и изменять.

1 Нажмите на вкладку **Card Filter** (Фильтр карт), чтобы выбрать список фильтров карт, которые будут доступны оператору, который назначен для работы с этим рабочим пространством.



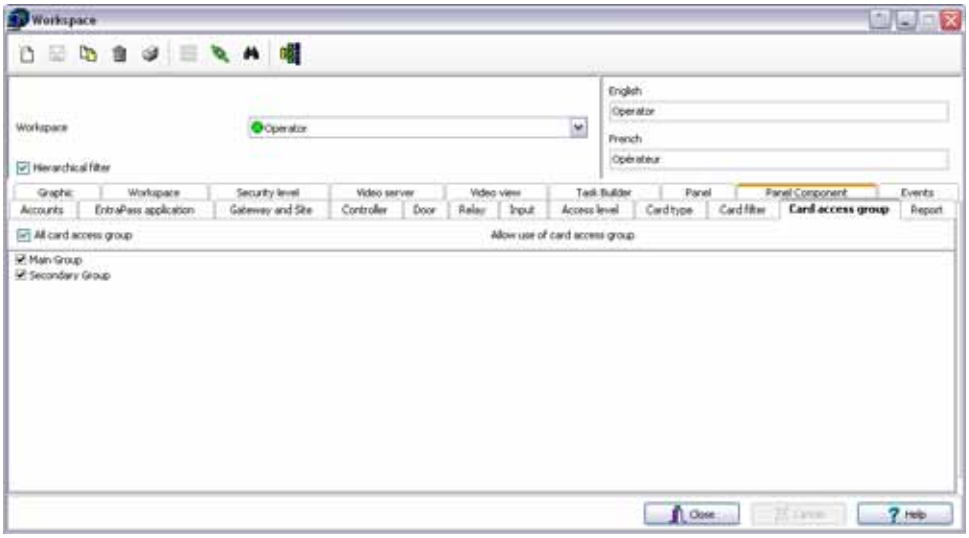
- Нажмите на на **All cards filter** (Все фильтры карт), если вы хотите назначить все фильтрв карт для данного рабочего пространства.
- Также вы можете указать индивидуальный фильтр.

2 Сохраните изменения

Назначение групп доступа для идентификационных карт

Эта функция предоставляет операторам доступ к определённым группам доступа для групповых операций с картами в пределах их рабочего пространства.

1 Открыть закладку **Card access group** (Группы доступа для идентификационных карт), чтобы выделить список групп, доступных для оператора, за которым закреплено данное рабочее пространство.



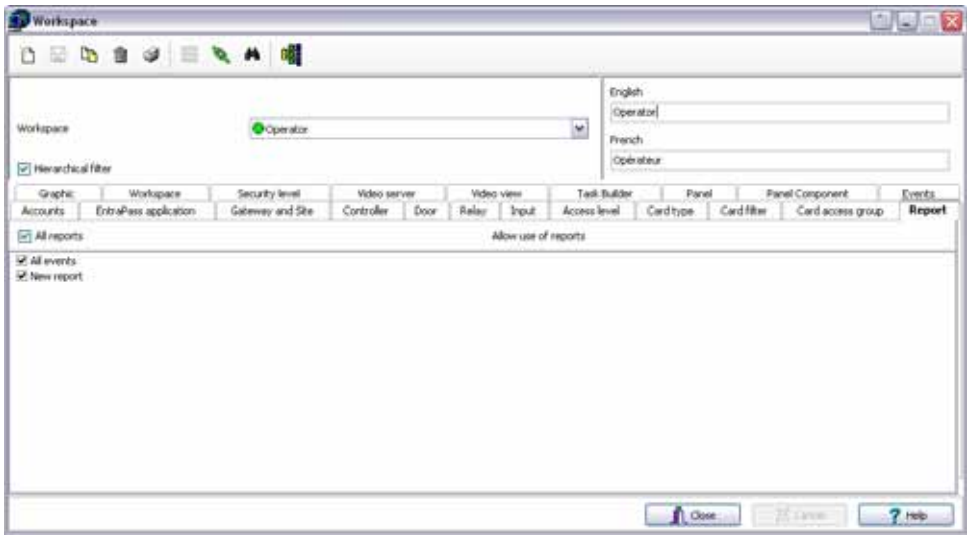
- Если необходимо, выделить опцию **All Card access group** (Все группы доступа карт), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все отображаемые на экране группы доступа карт
- Либо выделить определённые группы доступа из общего списка.

2 Сохранить внесённые изменения.

Назначение отчётов

Эта функция предоставляет операторам доступ к отчётам в пределах их рабочего пространства. Например, системный администратор (System Administrator) может иметь доступ ко всем создаваемым отчётам, а руководителю службы охраны (Guards' Supervisor) будут доступны только все отчёты, имеющие отношение к маршруту обхода охраны (Guard Tour). Генерация отчётов выполняется из списка **Archived Message list** (Список архивируемых сообщений) на рабочем столе рабочей станции. Если отчёты привязаны к определённым рабочим пространствам, то они будут доступны только тем операторам, которые работают в этих рабочих пространствах.

1 Открыть закладку **Report** (Отчёты), чтобы выделить список отчётов, доступных оператору, за которым закреплено данное рабочее пространство.

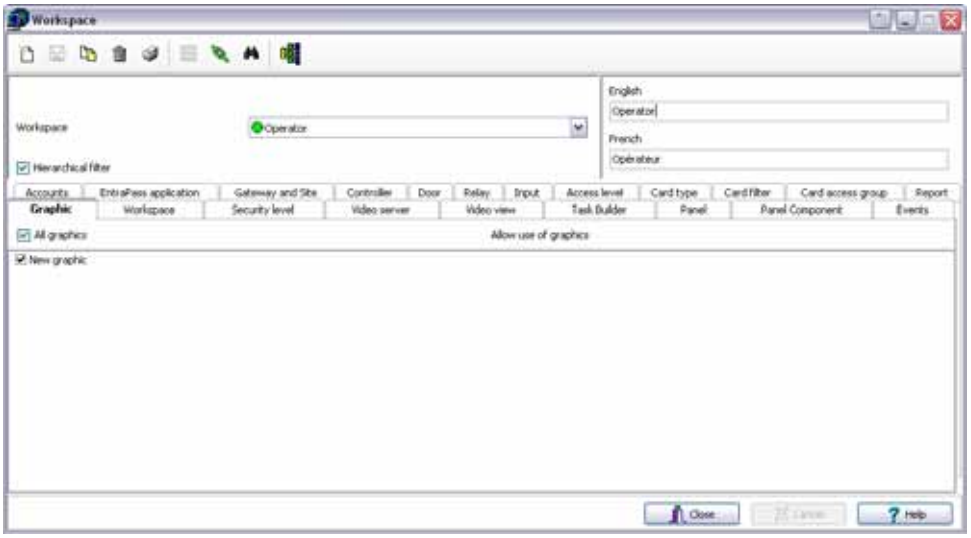


- Если необходимо, выделить опцию **All reports** (Все отчёты), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все отчёты.
- Либо выделить определённые отчёты из общего списка, отображаемого на экране.

2 Сохранить внесённые изменения.

Назначение графических схем

1 Открыть закладку **Graphics** (Схемы), чтобы выделить список схем, доступных оператору, за которым закреплено данное рабочее пространство.



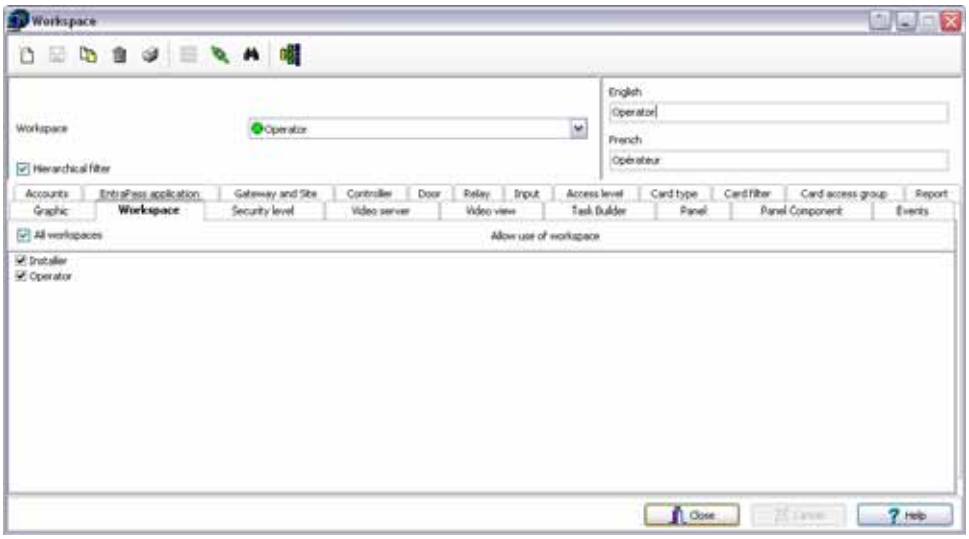
- Если необходимо, выделить опцию **All graphics** (Все схемы), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все схемы.
- Либо выделить определённые схемы из общего списка.

2 Сохранить внесённые изменения.

Назначение рабочего пространства

Эта функция предоставляет операторам доступ к информации, которая относится к другим рабочим пространствам, закреплённым за другими операторами. Например, охранники (Guard) работают в некотором рабочем пространстве, назначенном для охраняемой ими зоны и обеспечивающем доступ к определённому типу данных, которые они могут просматривать и редактировать в системе EntraPass. А начальник службы охраны (Guard's Supervisor) должен иметь доступ ко всем данным, которыми владеют все охранники его отдела. В таком случае, список рабочих пространств начальника (Supervisor) будет содержать все рабочие пространства охранников (Guard), описанные в системе.

1 Открыть закладку **Workspace** (Рабочие пространства), чтобы выделить список рабочих пространств, доступных оператору, за которым закреплено данное рабочее пространство.



- Если необходимо, выделить поле **All workspaces** (Все рабочие пространства), чтобы сделать доступными все рабочие пространства из списка для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые позиции из общего списка.

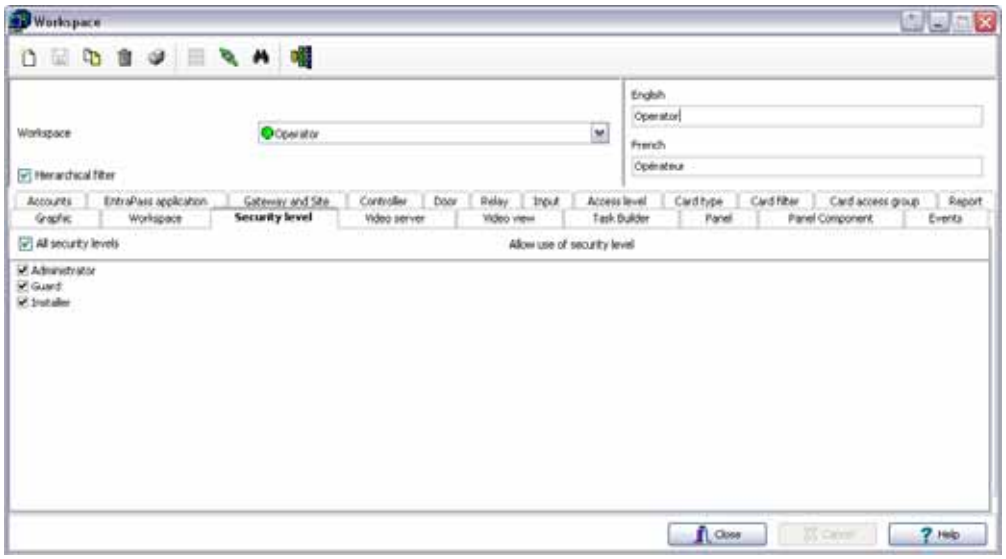
2 Сохранить внесённые изменения.

Задание уровней безопасности

Вкладка Security level (Уровни безопасности) в рабочем пространстве только ограничивает операторов на раздачу уровней безопасности при создании операторов.

1 Открыть закладку **Security level** (Уровни безопасности), чтобы выбрать уровни безопасности для данного рабочего пространства. Смотрите в Главе 12 Назначение уровней безопасности' на

странице 406 для более подробной информации , если необходимо создать новый уровень безопасности.



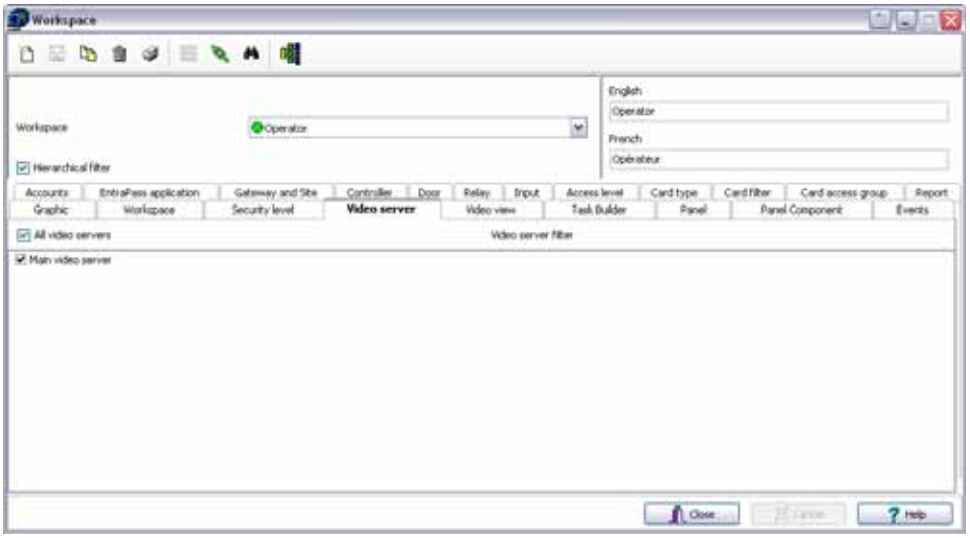
- Выбрать опцию **All security levels** (Все уровни безопасности), чтобы назначить все уровни для данного рабочего пространства.
- Либо выделить определённые уровни безопасности из общего списка.

2 Сохранить внесённые изменения.

Назначение видеосерверов

Список видеосерверов позволяет разрешить или запретить доступ операторов к определённым видеосерверам и камерам наблюдения. Например, если уровень безопасности для данного рабочего пространства разрешает доступ к видеосерверу, то всё равно есть возможность запретить доступ к определённой камере. Таким образом, эта функция упрощает процедуру назначения доступа к видеосерверу, видеоокну или к другим разделам меню видеонаблюдения.

1 Открыть закладку **Video server** (Видеосервера), чтобы выделить список видеосерверов, доступных оператору, за которым закреплено данное рабочее пространство.



- Если необходимо, выделить поле **All video servers** (Все видеосервера), чтобы сделать доступными все видеосервера из списка для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые видеосервера из общего списка.

2 Сохранить внесённые изменения.

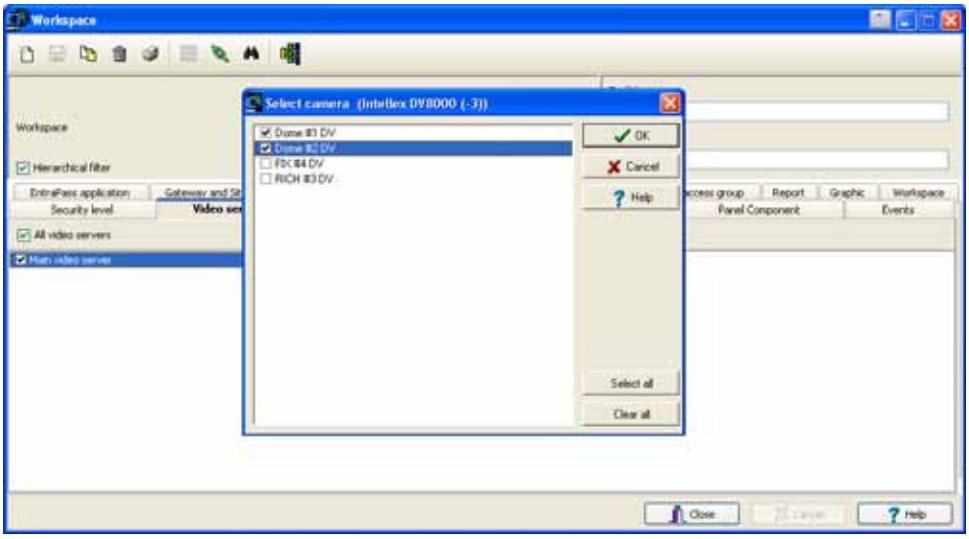
ПРИМЕЧАНИЕ: *Чтобы назначить, какие видеоокна доступны для выбранного оператора, в рабочем пространстве этого оператора должно быть разрешён доступ к видеосерверу, связанному с этими видеоокнами. Если же операторам разрешён доступ к видеоокну, но не разрешён доступ к соответствующему видеосерверу в том рабочем пространстве, в котором работают эти операторы, то это видеоокно будет для них недоступно*

Ограничение доступа к отдельным камерам наблюдения

В системе EntraPass есть возможность разрешить доступ к видеосерверу и одновременно запретить доступ к определённым камерам, зарегистрированным на этом сервере

ПРИМЕЧАНИЕ: *Чтобы оператор не видел изображение с камеры, к которой у него нет доступа, следует, прежде всего, отметить флажком опцию* ***Hide camera from view*** *(Скрыть камеру от наблюдения) в меню Security level (Уровни безопасности). В таком случае камера не будет отображаться в видеоокнах, даже если оператор имеет полный доступ к видеосерверу, к которому эта камера подключена.*

1 В окне Workspace (Рабочее пространство) открыть закладку **Video server** (Видеосервер
2 Отметить флажком видеосервер, к которому подключена нежелательная для просмотра камера, и дважды щёлкнуть по его имени. Пи этом должно открыться окно Select camera (Выбрать камеры наблюдения).



3 В окне Select camera снять выделение с тех камер, которые должны быть скрыты от наблюдения при работе в данном рабочем пространстве. .
4 Нажать **OK**, чтобы закрыть окно Select camera. При этом выделение с видеосервера под закладкой Video view снято не будет. Исключение камеры из списка лишь закрывает доступ к этой камере, но не к соответствующему видеосерверу.
5 Сохранить внесённые изменения.

Назначение окон видеонаблюдения

1 Открыть закладку **Video views** (Видеоокна), чтобы выделить список видеоокон, доступных оператору, за которым закреплено данное рабочее пространство.

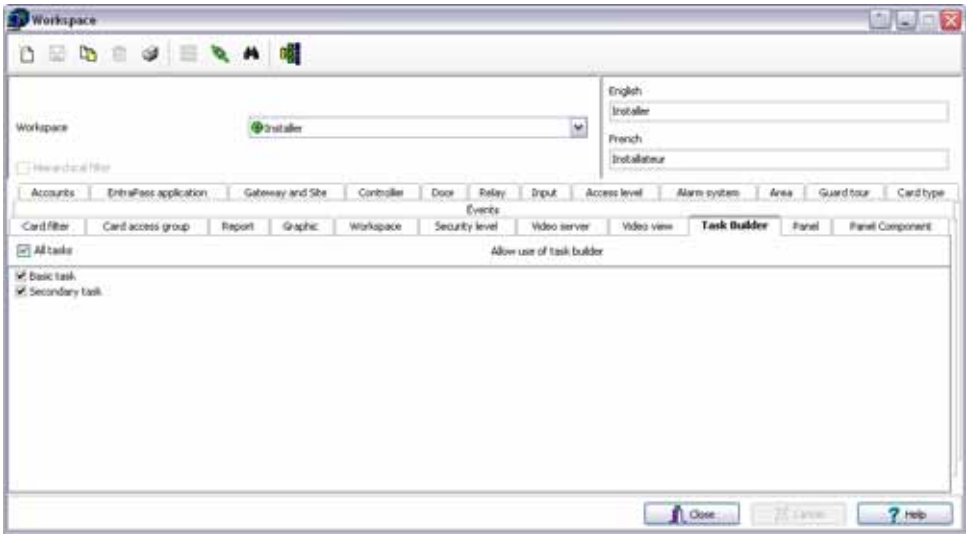
- Если необходимо, выделить поле **All video views** (Все видеоокна), чтобы сделать доступными все видеоокна из списка для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые видеоокна из общего списка.

2 Сохранить внесённые изменения.

Назначение задач

Соотношение задач с рабочей областью позволяет вам контроллировать задачи, которые оператор может назначать или изменять.

1 Нажмите на вкладку **Task Builder** чтобы выделить список задач, которые будут доступны для этого оператора, который назначен для этого рабочего пространства.



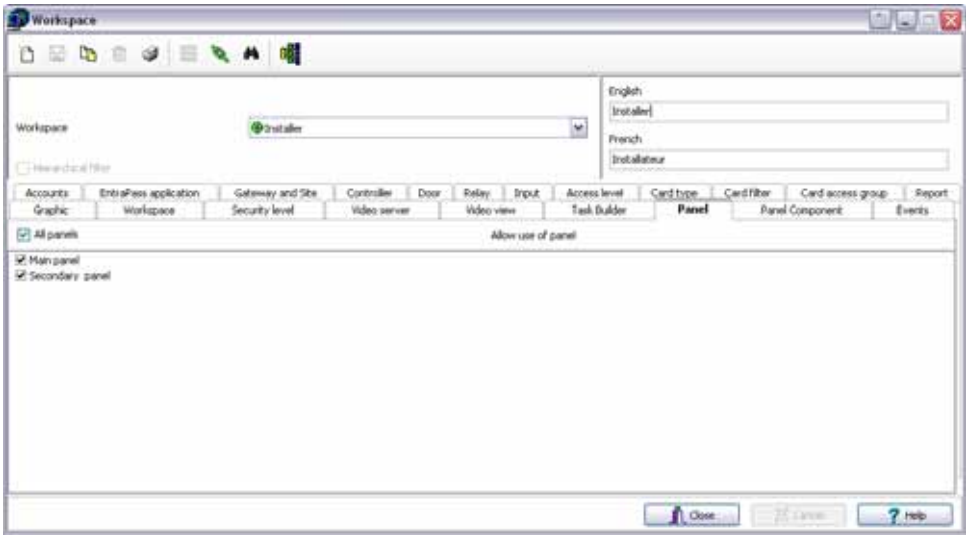
- Выберите вкладку **All tasks** (Все задачи), если вы хотите чтобы все задачи были доступны для операторы, назначенного для этого рабочего пространства.
- Вы также можете выбрать индивидуальные задачи из этого списка.

2 Сохраните ваши изменения.

Назначение охранных панелей

Соотношение панелей с рабочим пространством позволяет вам контроллировать панели, которые оператор может назначать или изменять.

1 Нажмите на вкладку **Panel** (Панель) и выберите список панелей, которые будут доступны оператору, кто назначен для этого рабочего пространства.



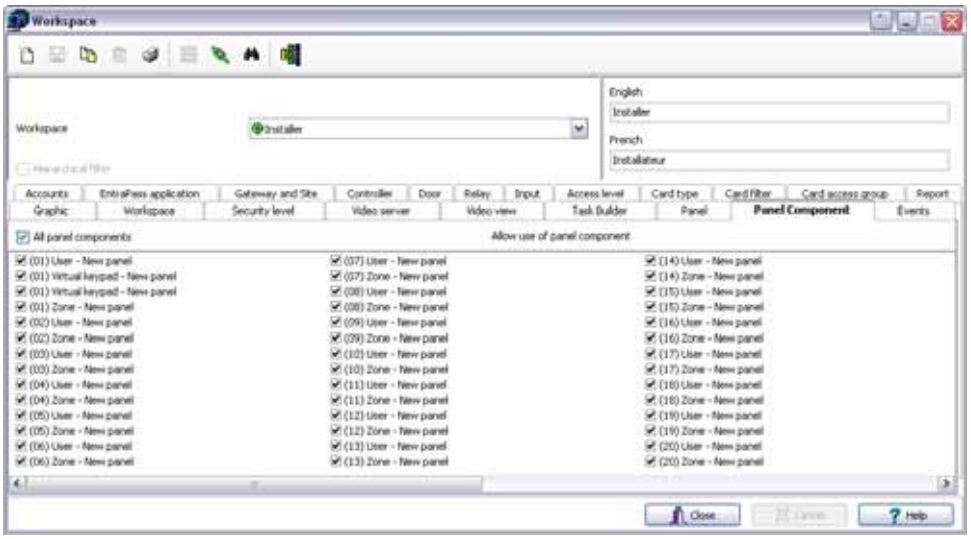
- Выберите **All panels,** если вы хотите, чтобы все панели были доступны для оператора, назначенного для этого рабочего пространства.
- Вы можете выбрать индивидуальные панели из отображаемого списка.

2 Сохраните изменения.

Назначение компонентов охранной панели

Соотношение компонентов охранной панели с рабочим пространством позволяют вам контроллировать компоненты охранной панели, которые оператор может изменять и назначать.

1 Нажмите на вкладку **Panel Component** (компоненты панели) и выберите те компоненты панели, которые будут доступны для оператора, прикрепленного к этой рабочей области.



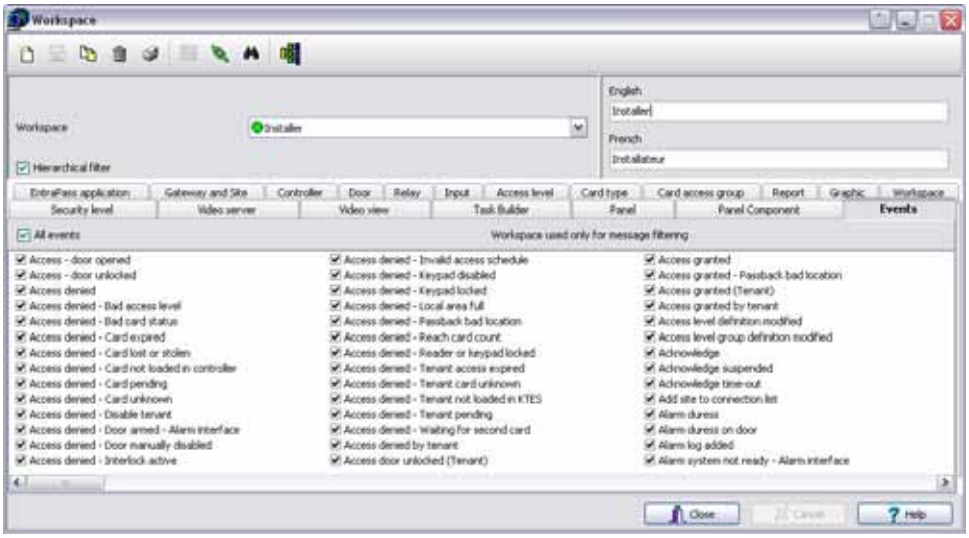
- Выберите **All panel components** (Все компоненты панели) если вы хотите, чтобы все компоненты были доступны для оператора, назначенного для этой рабочей области.
- Вы можете также выбрать отдельные компоненты из этого списка.

2 Сохраните ваши изменения.

Назначение событий

Этот раздел меню служит для назначение сообщений о событиях, отображаемых на экране для операторов, за которыми закреплено данное рабочее пространство.

1 Открыть закладку **Events** (События), чтобы выделить список событий, которые будут отображаться на экране рабочей станции оператора.



- Выделить события, видимые для оператора, за которым закреплено данное рабочее пространство.

2 Сохранить внесённые изменения.

Назначение пункта параметров событий (событие/реакция)

Назначение параметров событий является одной из наиболее важных функций системы. Для каждого события можно указать, как на него будет отвечать система. Например:

- Посылать сообщения о событиях на устройства вывода (например, на рабочий стол сообщений или на принтер журналов),
- Отправлять команды в приложение SmartLink
- Задавать расписания, которые позволяют, например, посылать тревожные сигналы в приложение EntraPass только ночью,
- Отправлять определённые сообщения о событиях в определённое приложение EntraPass и др.

Всего предусмотрено более 400 системных событий. Наиболее часто среди них используются следующие:

- Access granted (Доступ разрешён)
- Input in alarm (Вход переведён в статус тревоги)
- Card modified by operator (Карта изменена оператором) и др.

События связаны с компонентами системы, в том числе дверями, контроллерами, шлюзами, приложениями Entrapass, тревожными системами и др. Каждое сообщение о событии привязано к какому-либо компоненту системы и устройствам вывода или группе таких устройств. Например, событие *Access granted* (Доступ разрешён) можно настроить независимо для каждой двери или по умолчанию для всех дверей сразу. Эта гибкость позволяет выполнять различные команды и ответные действия по принципу "от двери до двери".

Назначение параметров событий

Меню **Event parameters** (Параметры событий) позволяет индивидуально настроить системные события по желанию пользователя. Таким образом, пользователь может указать, какие события следует автоматически выводить на печать или подтверждать по определённому расписанию. Кроме того, предусмотрена отправка инструкций операторов о тревоге через другие средства связи (например, по электронной почте, на пейджер и др.) при формировании тревог. По умолчанию все события должны отображаться на всех рабочих столах сообщений во всех приложениях EntraPass, настроенных в системе. Однако можно вручную настроить системные события в соответствии с собственными требованиями, установив специальные связи между событиями и компонентами. Существует два типа связей: специальные и по умолчанию.

- **Связи по умолчанию** (Default) – те связи, которые установлены в системе изначально. По умолчанию все сообщения о событиях, возникающих на всех компонентах, связаны с этими компонентами и отображаются на рабочих столах сообщений. Пользователь может использовать установки по умолчанию.

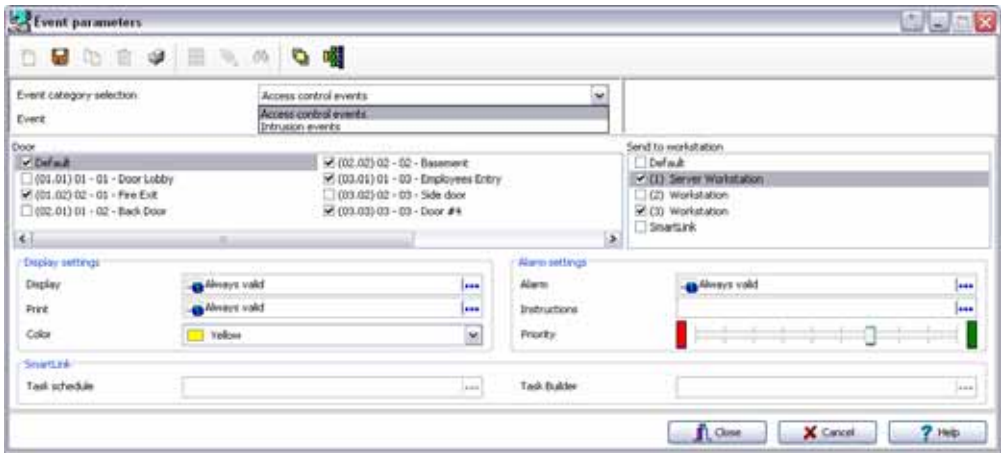
Связи по умолчанию		Замечания
Компонент	**Рабочая станция**	
Настройки по умолчанию	Настройки по умолчанию	Сообщения обо всех событиях, поступающие со всех компонентов, посылаются на все рабочие станции.
Настройки по умолчанию	Специальные настройки (Рабочая станция 2)	Сообщения обо всех событиях, поступающие со всех компонентов, посылаются только на рабочую станцию 2.
Специальные настройки (Дверь 1)	Настройки по умолчанию	Только сообщения от компонента "Дверь 1" посылаются на все рабочие станции.

- **Специальные связи (Manual association)**– настраиваются администратором и служат для отправки сообщений на рабочие столы, предназначенные для определённых событий. В приведённой ниже таблице показаны три типа специальных связей:

Специальные связи		Пример
Компонент	**Рабочая станция**	
Специальные настройки	Специальные настройки	События, генерируемые компонентом "Дверь 1", посылаются только на рабочую станцию 1.
Специальные настройки	Настройки не указаны или по умолчанию	События, генерируемые компонентом "Дверь 1", посылаются на все рабочие станции (по умолчанию).
Настройки не указаны или по умолчанию	Специальные настройки	События, генерируемые любым компонентом (по умолчанию), посылаются только на рабочую станцию 1.

ПРИМЕЧАНИЕ: **Связи в ручном режиме** *имеют приоритет перед настройками по умолчанию. Если между сообщением о событии и компонентом установлены специальные связи, то настройки по умолчанию игнорируются. Для восстановления настроек по умолчанию необходимо удалить специальные связи. Специальные связи следует назначать с осторожностью. Наиболее частое применение этой опции – приложение SmartLink.*

1 Открыть закладку **System** (Системные настройки) и нажать иконку **Event parameters** (Параметры событий).



2 Из выпадающего списка **Event category selection** (выбор категории событий), выберите категорию между **Access control events** (события контроля доступа) и **Intrusion events** (события охранной сигнализации).

3 В выпадающем списке **Event** (События) выделить событие, для которого необходимо указать настройки.

ПРИМЕЧАНИЕ: *По умолчанию все события должны посылаться на рабочие столы сообщений (Message) всех рабочих станций EntraPass, настроенных в системе, в режиме расписания Always valid (Достоверно всегда). Рекомендуется сохранять настройки по умолчанию, особенно при назначении этих настроек для всех событий/компонентов. Однако может возникнуть необходимость создать специальные (в ручном режиме) связи для определённого события, когда необходимо сформировать определённое сообщение или сигнал тревоги в ответ на это событие. Выбранное событие появится на всех дверях и будет отображаться на всех рабочих станциях EntraPass.*

4 В разделе **Display settings** (Параметры отображения) указать опции для отображения на экране: по умолчанию все события должны посылаться на рабочий стол сообщений (Message) на всех

рабочих станциях EntraPass, настроенных в системе, в режиме расписания **Always valid** (Достоверно всегда).

ПРИМЕЧАНИЕ: *При работе с приложением EntraPass SmartLink это расписание должно остаться "Always valid" (Достоверно всегда), иначе сообщения/команды* ***не будут*** *посылаться в это приложение.*

5 В меню **Print** (Печать) выбрать расписание для вывода сообщения о событии на печать. В период действия расписания сообщение о выбранном событии будет распечатано на принтере, который подключён к рабочей станции, принявшей это сообщение.

6 В выпадающем списке **Color** (Цвет) выбрать цвет, который будет использоваться для отображения сообщения на экране сообщений (Message). По умолчанию используется следующая цветовая кодировка сообщений:
- **Красный** – для тревожных событий;
- **Зелёный** – при возвращении элементов в нормальное состояние
- **Жёлтый** – для предупреждений и ошибок;
- **Синий** – для остальных событий.

7 В меню **Alarm Settings** (Параметры тревог) необходимо выполнить следующие настройки:
- **Alarm (Schedule)(**Тревога/расписание) – в период действия расписания, сообщение о выбранном событии будет отправлено на рабочий стол тревог (Alarms) на выбранных рабочих станциях и будет требовать подтверждения оператора.
- **Instructions** (Инструкции оператору) – выбрать команду, которая будет отправлена на рабочий стол инструкций (Instruction) с событием, требующего подтверждения. Инструкции оператору будут посылаться только во время действия расписания **Alarm (Schedule)**.

ПРИМЕЧАНИЕ: *В приложении SmartLink для подачи команд не требуется, чтобы расписание тревог было достоверным. Поле* ***Alarm schedule*** *(Расписание тревог) может оставаться пустым, а команда всё равно будет отправлена.*

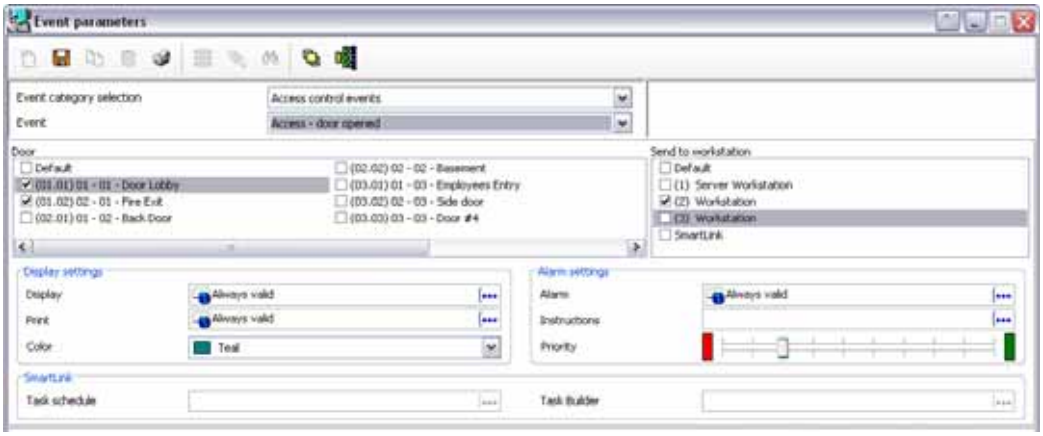
8 Назначить уровень приоритета для события в поле **Priority** (Приоритет). От этого зависит, в какой последовательности тревожные сообщения будут отображаться на экране для оператора. Приоритеты назначаются самым обычным образом (0 = наивысший, 9 = низший).

9 На вкладке **SmartLink**, нажмите многоточие, чтобы выбрать **Task schedule** (расписание задачи).

10 Нажмите на многоточие чтобы выбрать **Task Builder** (Строитель команд).

Создание связей

1 В окне **Event parameters** (Параметры событий) выбрать категорию событий (Event Category) и событие (**Event**) из выпадающего списка. На панели компонентов (слева) выбрать компонент и затем выбрать рабочую станцию EntraPass, на которую будет отправляться сообщение.

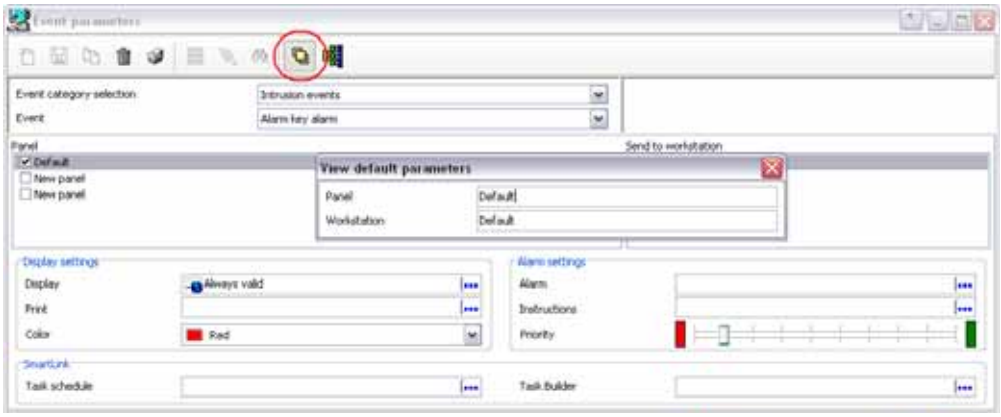


2 Нажать **Save** (Сохранить) для создания новой связи. В приведённом на иллюстрации примере сообщение о событии "A*ccess - Door opened" (Полный доступ – дверь открыта),* возникающем на выбранных дверях, отправляется на указанные рабочие станции (выделена на панели справа).

ПРИМЕЧАНИЕ: *Кнопка* ***Save*** *(Сохранить) становится доступной только после создания связи между выделенным событием и компонентом.*

Просмотр параметров по умолчанию /(Посмотреть связи).

1 На панели компонентов (слева) выбрать компонент и затем выбрать приложение EntraPass, в которое будет отправляться сообщение о событии.



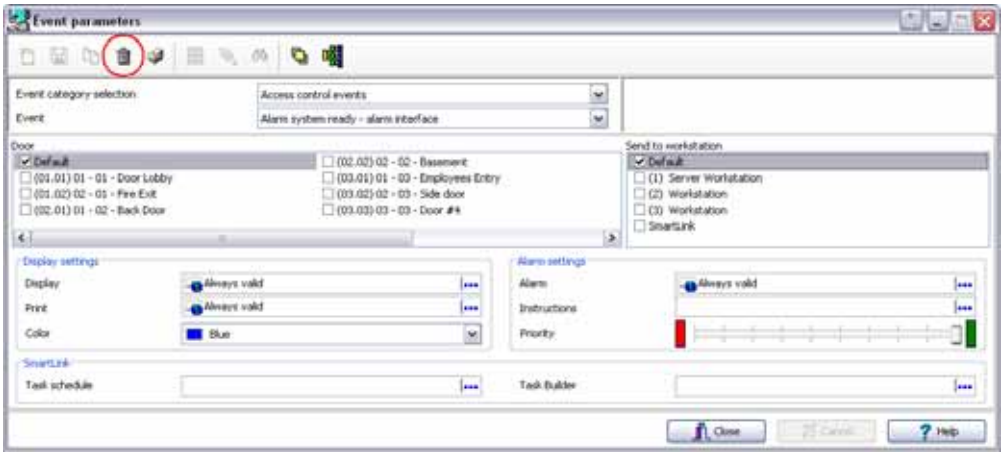
2 Нажмите на кнопку **View default parameters** (Вид параметров по умолчанию) на панели инструметов для того, чтобы увидеть список параметров. Вы сможете увидеть где события были установлены по умолчанию и где вручную.

3 Click again on the **View default parameters** icon to close the message box.

Удаление и восстановление связей

В какой-то момент может потребоваться, чтобы сообщения о событии, связанном с определённым компонентом, перестали отправляться на рабочий стол Message всех рабочих станций, или на некоторых из них. Для этого необходимо удалить существующие связи. Данную операцию следует выполнять с особой осторожностью.

1 В окне Event parameters (Параметры событий) выбрать категорию и затем событие из списка **Event** (События), которое необходимо изменить.



2 Нажать на панели инструментов кнопку **Delete** (Удалить).

3 В окне Delete event parameters (Удалить параметры событий) выбрать одну из следующих опций:

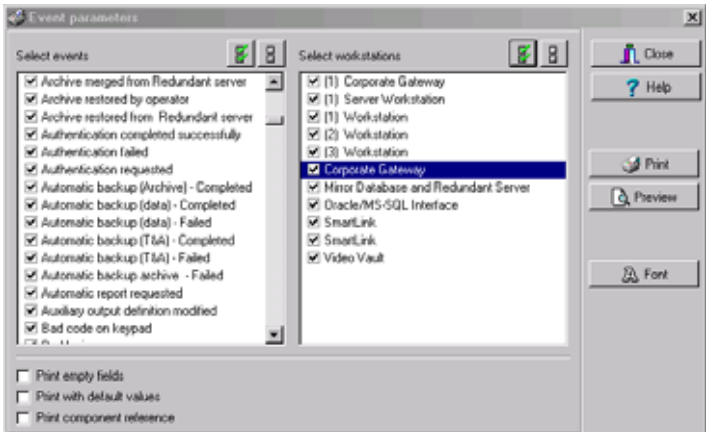
- **Restore default** (Восстановить настройки по умолчанию) – применить заводские настройки к параметрам тревог и параметрам отображения.
- **Suppress messages**: очистить поля в разделах Alarm settings (Параметры тревог) и Display settings (Параметры отображения), чтобы подготовить их к вводу новых данных. Сразу после удаления настроек необходимо заново ввести их.

- **Cancel** (Отмена) – отменить команду удаления.

Вывод на печать параметров событий

Система EntraPass позволяет вывести на печать параметры событий **events parameters** (параметры тревог и параметры отображения) для выбранных событий.

1 В окне Event parameters (Параметры событий) нажать иконку **Printer** (Принтер).



2 На панели **Select events** (Выделить события) выбрать события, которые должны быть включены в распечатку, или нажать кнопку **Select all** (Выделить все), чтобы выделить все события из отображаемого на экране списка.

3 На панели **Select workstations** (Выделить рабочие станции) указать, какие рабочие станции EntraPass должны быть включены в распечатку, или нажать на кнопку **Select all** (Выделить все), чтобы выделить все рабочие станции EntraPass в отображаемом списке.

- Чтобы принтер печатал и пустые поля, следует поставить флажок в поле **Print empty fields** (Выводить на печать пустые поля). Будет напечатано только имя пустого поля.
- **Print with default values** (Печать с настройками по умолчанию) – при выделении этой опции система выведет на печать связи по умолчанию вместе со специальными связями.

ПРИМЕЧАНИЕ: *Если **не выделить** флажком это поле, то в отчёт попадут только специальные/ручные связи (без связей по умолчанию). Если специальные/ручные связи не назначены (компонент X и рабочая станция Y), то отчёт окажется пустым.*

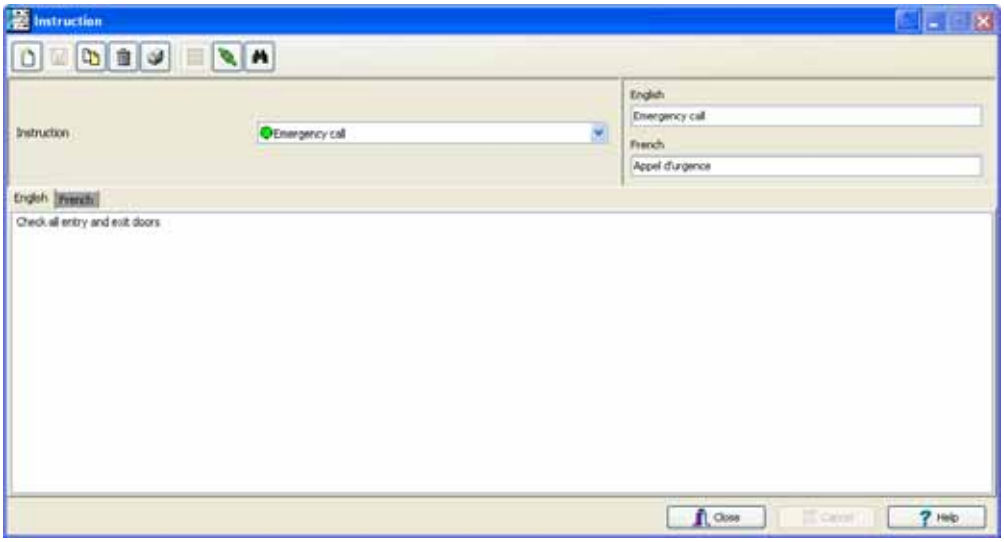
- **Print components reference** (Печатать ссылки компонентов) – печатать физический адрес следующим за идентификационными данными компонента.
- С помощью кнопки **Font** (Шрифт) можно изменять тип и размер шрифта для отчёта, если требуется.
- Если требуется, нажать кнопку **Preview** (Предварительный просмотр) для проверки текста перед выводом на печать.

Назначение инструкций оператору

Этот раздел меню служит для назначения инструкций оператору, которые должны быть привязаны к определённым событиям. При формировании сигнала тревоги эти инструкции будут отображаться в окне Instruction (инструкции) (меню рабочих столов Desktop) для подтверждения. Как правило, каждая строка содержит одну команду; инструкции могут состоять из нескольких команд (строк). Таким образом, удаётся обеспечить более высокую гибкость на случай, если необходимо внести изменения.

Назначение инструкции

1 В главном окне **System** (Системные настройки) нажать на иконку **Instruction** (Инструкции).



2 Чтобы создать новую инструкцию, нажать на кнопку **New** (Создать). Чтобы изменить уже созданную команду, выбрать её из выпадающего списка **Instruction.**

3 Назначить имя инструкции в соответствующих полях для каждого применяемого языка.

4 Выбрать закладку с названием одного из языков, чтобы ввести инструкцию. Инструкции вводят только на *одном* выбранном языке.

ПРИМЕЧАНИЕ: *В каждой команде можно ввести до 511 символов (включая пробелы).*

5 *Смотрите в Главе 12 Назначение пункта параметров событий (событие/реакция)' на странице 426 для более подробной информации* по соотношению инструкции оператора с событиями.

Назначение команд SmartLink при использовании конструктора команд Task Builder

Смотрите в Главе 5 Панель управления конструктора команд (Task Builder)' на странице 204 для более подробной информации .

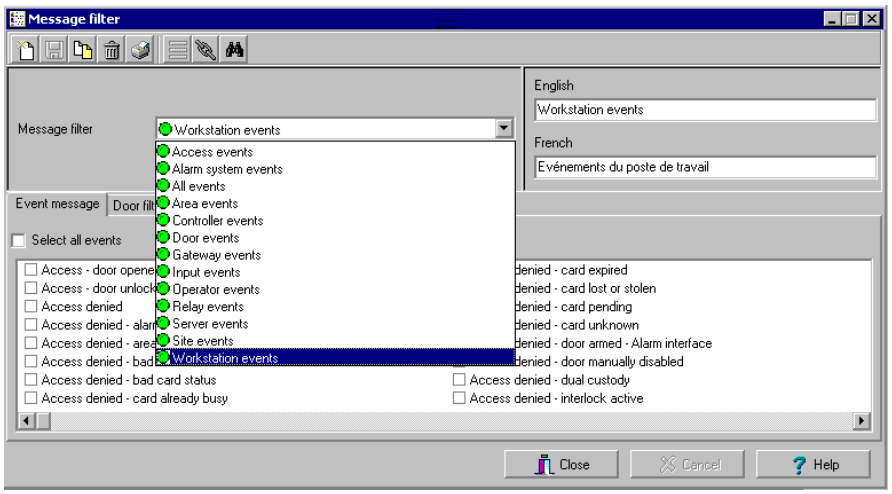
Назначение фильтров сообщений

Функция Message filter (Фильтр сообщений) предназначена для назначения фильтров, используемых на рабочем столе Filtered Messages (Избранные сообщения). Эти фильтры служат для определённого отбора событий. Например, вы можете назначить специальные фильтры для оператора: охранник может видеть только события тура обхода. Затем вы можете создать специальные фильтры, чтобы события тура обхода (guard tour) отправлялись на рабочую станцию охранникам. Существует много предварительно настроенных фильтров, например: события доступа, события контроллера и др. Эти фильтры доступны всем операторам. Для выбора или создания фильтров можно воспользоваться непосредственно рабочим столом “Filtered Messages” (Избранные сообщения) или меню Message Filters (Фильтры сообщений).

ПРИМЕЧАНИЕ: *Смотрите в Главе 11 Рабочий стол отфильтрованных собщений (Filtered Messages Desktop)’ на странице 380 для более подробной информации .*

Назначение события для фильтра сообщений

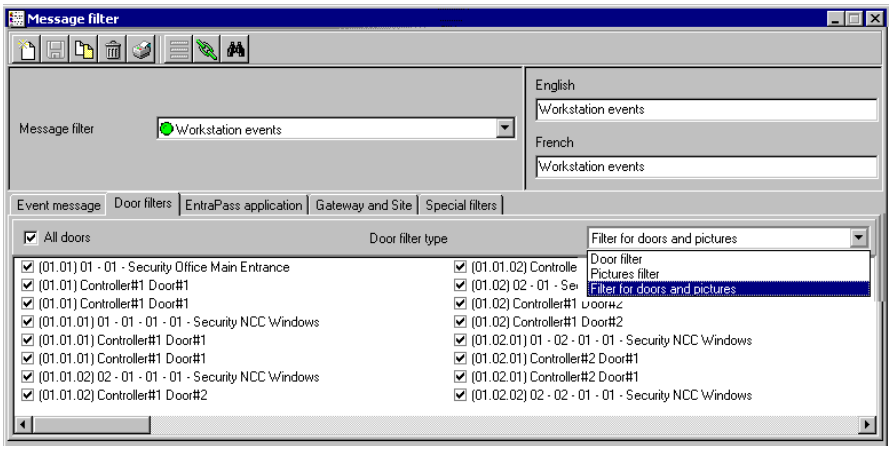
1 В главном окне System (Системные настройки) нажать на иконку **Message Filter** (Фильтр сообщений). Открывается окно Message filter.



2 В выпадающем списке **Message filter** выделить тип сообщения о событии (например, Door events или Relay events), для которого требуется настроить фильтр. Чтобы создать новый фильтр, нажать кнопку **New** (Создать).

3 Выбрать события в списке **Event list,** которые должны появиться в выбранном фильтре. Выделить поле **Select all events** (Выделить все события), если не требуется отобрать только часть из них. Допустим, в фильтре событий, связанных с работой дверей (**Door filter**), требуется выделить все события или выбрать только события по запрещению доступа (**Access-denied**).

4 Открыть закладку **Door filters** для отбора дверей, которые будут отправлять сообщения на рабочий стол избранных сообщений (Filtered Messages Desctop). Кроме того, при отборе событий, связанных с доступом (Access events), вместе событием может отображаться фотография владельца карты (если фотографии владельцев есть в базе данных). Можно указать, какие двери будут отображать фотографию владельца карты после формирования события для этой двери.

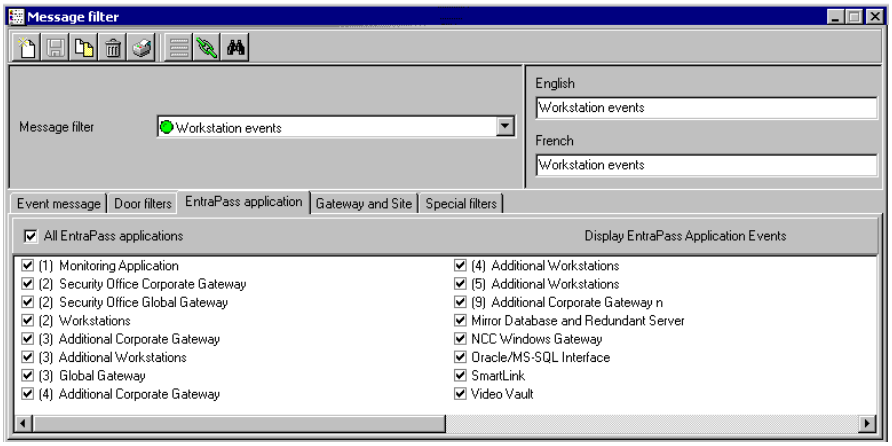


5 Выделить все двери при помощи опции **All doors** (Все двери) или выбрать определённые двери, для которых при возникновении события будет отображаться фото владельца карты.

6 В списке **Door filter type** (Типы фильтров дверей) выбрать фильтр, который будет использоваться при отборе событий, связанных с дверями:

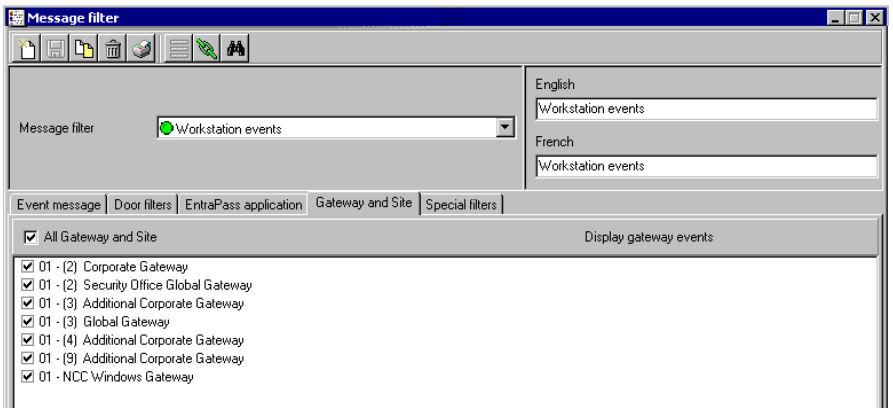
- **Door filter** (Фильтр дверей) – на рабочий стол Filtered Message (Избранные сообщения) будут отправляться только события, связанные с указанными дверями.
- **Pictures filter** (Фильтр фотографий) – на рабочий стол Filtered Message (Избранные сообщения) будут отправляться только фотографии владельцев карт, связанные с картами, которые были предъявлены на указанных дверях.
- **Filters for doors and pictures** (Фильтры для дверей и фотографий) – на рабочий стол Filtered Message (Избранные сообщения) будут отправляться сообщения, связанные с указанными дверями, а также фотографии владельцев карт, которые привели к возникновению событий на указанных дверях.

7 Открыть закладку **EntraPass applications** (Приложения EntraPass), чтобы выбрать приложения, с которых будут отправляться сообщения на рабочий стол Filtered Messages (Избранные сообщения).



8 Поставить флажок в поле **All EntraPass applications** (Все приложения EntraPass) для рабочего стола Filtered Messages, чтобы получать все сообщения о событиях, происходящих во всех приложениях EntraPass, настроенных в системе. Кроме того, можно сделать так, чтобы отображались только события, поступающие с указанных приложений. Для этого следует указать приложение EntraPass, с которого необходимо получать сообщения о событиях.

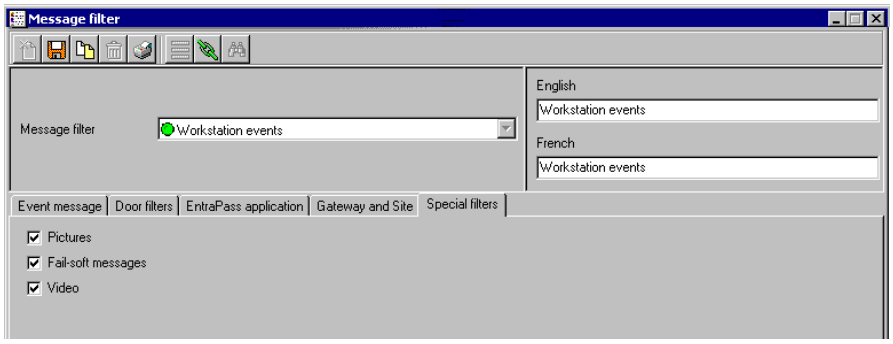
9 Открыть закладку **Gateway and site** (Шлюзы и сайты/лучи), чтобы отобрать шлюзы и сайты/лучи, с которых будут отправляться сообщения на рабочий стол Filtered Messages (Избранные сообщения).



10 Отметить флажком опцию **All events** (Все сообщения), чтобы получать сообщения о событиях, происходящих на компонентах шлюзов или сайтов/лучей. Можно выбрать шлюз или сайт, который будет отправлять сообщения о событиях для отображения их на экране.

ПРИМЕЧАНИЕ: *При использовании фильтров система извлекает события, которые уже отображаются на рабочем столе сообщений Message, и отбирает из них события, соответствующие настройкам выбранного фильтра. Если события, возникшие на определённом шлюзе, отображаются на столе сообщений, а этот шлюз не выделен в настройках фильтра, то эти события не будут отображаться при использовании этого фильтра.*

11 Открыть закладку **Special filter** (Особые фильтры), чтобы отфильтровать события по их типу.



- **Picture** (Фотографии) – на рабочем столе Filtered Message (Избранные сообщения) будут отображаться все события, которые связаны с фотографией владельца карты.
- **Fail-soft** (Автономный режим) – на рабочем столе Filtered Message (Избранные сообщения) будут отображаться все события, созданные контроллером при работе в автономном режиме во время потери связи. Такие сообщения отмечены знаком "+" на столе Filtered Message (и на столе Message), если эта опция выделена флажком при описании свойств списка сообщений (меню **Desktop** > рабочий стол **Message** > щёлкнуть правой кнопкой по событию > **Properties**).
- **Video** (Видеозаписи) – все события, сопровождаемые видеозаписью, отправляются на рабочий стол Filtered Messages (Избранные сообщения).

ПРИМЕЧАНИЕ: *При использовании фильтров система извлекает события, которые уже отображаются на рабочем столе сообщений Message, и отбирает из них события, соответствующие настройкам выбранного фильтра. Если события, возникшие на определённом шлюзе, должны отображаться на столе сообщений, а шлюз не указан в настройках фильтра, то при наложении этого фильтра такие события отображаться на экране не будут.*

ПРИМЕЧАНИЕ:

Описание структуры базы данных

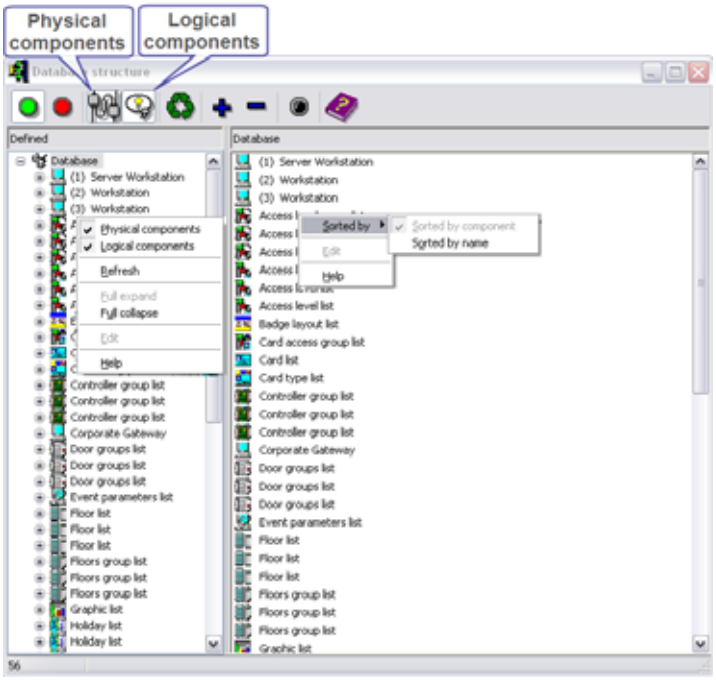
Меню Database structure (Структура базы данных) служит для просмотра базы данных системы. В нём отображается вся структура базы данных и в том числе:

- *Физические компоненты* системы (приложения EntraPass, шлюзы, сайты/лучи, контроллеры, двери, реле, входы и дополнительные выходы), а также.
- *Логические компоненты* (карты, расписания, отчёты, инструкции оператору, группы, области, тревожные системы и др.).

В окне Database structure операторы могут редактировать или сортировать компоненты системы.

Просмотр компонентов базы данных

1 В главном окне **System** (Системные настройки) нажать на иконку **Database structure** (Структура базы данных).



ПРИМЕЧАНИЕ: *Если в системе EntraPass разрешена функция Video (Видеонаблюдение), то её компоненты отображаются в проводнике базы данных Database.*

2 Чтобы на экране отображались только физические компоненты (**Physical component**), следует нажать на иконку физических компонентов. В таком случае будут отображаться только физические компоненты базы данных.

ПРИМЕЧАНИЕ: *По умолчанию физические компоненты отображаются* ***ВСЕГДА.***

3 Чтобы на экране отображались логические компоненты (**Logical components**), нажать иконку логических компонентов. После нажатия на иконку логические компоненты базы данных будут отображаться на экране вместе с физическими компонентами.

4 Вызвать функцию **Refresh** (Обновить), если необходимо обновить экран и получить самые последние данные с сервера базы данных.

5 Вызвать функцию **Full expand** (Развернуть), если необходимо полностью развернуть все ветви схемы, чтобы увидеть все вложенные компоненты. Например, если применить эту функцию к контроллеру, то в правой части окна будут показаны компоненты контроллера (двери, реле, входы).

6 Нажать **Collapse** (Свернуть), если необходимо полностью свернуть все ветви схемы и скрыть все вложенные компоненты.

7 Чтобы изменить настройки компонента, следует вызвать контекстное меню щёлчком правой кнопки мыши по этому компоненту и выбрать в меню пункт **Edit** (Редактировать). На экране появится окно описания этого компонента, в котором можно будет изменить его параметры.

8 Если необходимо выполнить сортировку компонентов, рекомендуется вызвать контекстное меню щёлчком правой кнопки мыши по компоненту и выбрать в этом меню пункт **Sort** (Сортировать). Сортировка компонентов, список которых отображается на правой панели окна, облегчает поиск. Доступны сортировка по имени и сортировка по компоненту.

ПРИМЕЧАНИЕ: *Кроме того, можно указать, каким образом система должна отображать на экране физический адрес компонента. От этого зависит также способ сортировки компонентов. Смотрите в Главе 12 Назначение уровней безопасности' на странице 406 для более подробной информации .*

Глава 13 • Отчеты

Панель инструментов Report (Отчеты)

Данное программное обеспечение позволяет пользователям выполнять настройку и генерирование отчётов. Отчёты могут генерироваться автоматически или по ручному запросу оператора. Возможна передача отчётов по электронной почте или при помощи интерфейса SmartLink.

Существуют пять типов отчётов:

- **Quick reports** (Быстрые отчёты) – выполняются для определённой группы событий (например, группы дверей, контроллеров и др.) и для определённого типа событий (нормальные, некорректные и др.).
- **Historical reports** (Архивные отчёты) – это отчёты по архивным событиям и по использованию карт. В архивные отчёты входят архивные и избранные/отфильтрованные события, а отчёты по использованию карт содержат события, связанные с использованием карт.
- **T & A reports** (Отчёты по учёту рабочего времени) – эти отчёты выполняются для указанных дверей и карт, по которым ведётся учёт рабочего времени.
- **Muster Reports** (Отчеты о сборе людей): Эти отчеты уже назначены в соотвествии с преднастроенным входом (input) внутри группы областей.
- **Roll Call Reports** — это отчет в виде снимка/фотографии о том, что кто поднес карту к считывателю или группе считывателей, внутри определенного периода времени.

Панель инструментов окна **Report** позволяет также выполнять следующие действия:

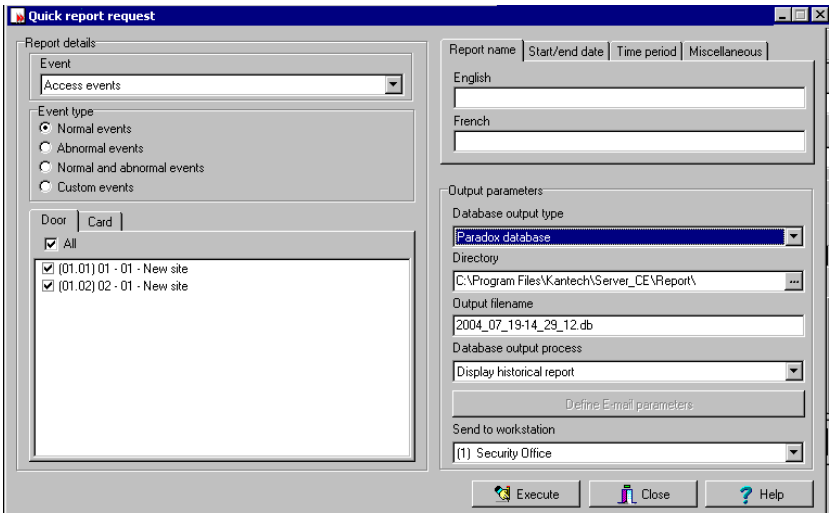
- **View reports** (Посмотреть отчёты) – эта функция позволяет оператору выбирать уже настроенные отчёты и выводить их на экран или на принтер.
- **View Report states** (Посмотреть статусы отчётов) – служит для просмотра статусов всех отчётов, которые были созданы ранее.
- **Perform Manual operations** (Выполнять ручные операции) – используется в отчётах по учёту рабочего времени, позволяет добавлять, вставлять и удалять записи.

Назначение быстрых отчётов (Quick Report)

Функция Quick report обеспечивает быстрый способ создания отчётов для событий определённого типа. Например, можно всего за несколько секунд создать отчёт по корректным или некорректным событиям доступа. Файлы быстрых отчётов можно просматривать с использованием программы EntraPass Quick Viewer, при помощи которой можно выводить на экран файлы быстрых отчётов и все файлы формата QRP. Сюда входят файлы отчёта, сохранённые при предварительном просмотре отчёта. Программа Quick Viewer запускается из меню Windows® **Start (Пуск)**. Таким образом, специальное программное обеспечение для просмотра файлов не требуется.

Назначение быстрого отчёта

1 На панели инструментов **Report** (Отчёты) нажать кнопку **Quick report request** (Запрос быстрого отчёта).

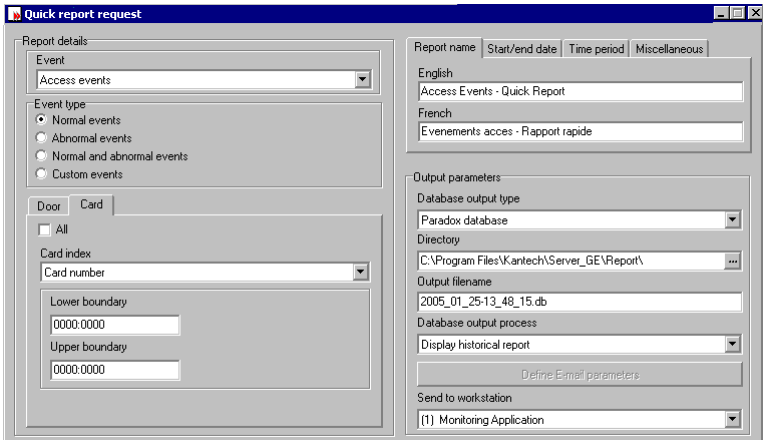


2 В выпадающем списке **Event** (События) выделить тип сообщения о событии для активного отчёта (уровни доступа, контроллеры, двери, реле, входы, операторы, события ручного управления и др.). Если выбраны события доступа (access events), то в этом окне появляется закладка **Card** (Карты).

3 В опциях **Event type** (Тип событий) указать тип событий, которые должны быть включены в отчёт.
- **Normal** (Корректные) – система может создавать отчёты по корректным событиям. Например, в отчёте о доступе корректными событиями будут события типа "Доступ разрешён".
- **Abnormal** (Некорректные) – это события типа "Доступ запрещён" (не тот уровень доступа, требуется уровень руководителя/ревизора), "Некорректный разрыв связи между рабочей станцией и сервером", "Потеря связи со шлюзом", а также все события, связанные с незавершённым процессом (неудачная повторная загрузка контроллера, например). Данные события рассматриваются системой как некорректные (abnormal).
- **Normal & abnormal** (Корректные и некорректные) – эту опцию выбирают, если необходимо включить в отчёт как корректные, так и некорректные события.
- **Custom events** (Специальные события) – служит для включения в отчёт событий, выбранных пользователем. Если опция **Custom events** отмечена флажком, появляется закладка **Custom**. Эта функция позволяет оператору указать компоненты, которые сгенерировали выбранные события в соответствии с настройками в поле “event”.

ПРИМЕЧАНИЕ: *В случае использования поля **Event** (События) оператор должен указать, какие компоненты использовать, а какие нет. Если выбрать любое событие (например, access - доступ), то система будет отображать на экране все двери данного шлюза. Если выбрать Controllers (Контроллеры), то будут отображаться все контроллеры данного шлюза. После выбора события (например, controller events – события контроллеров) следует указать, какие контроллеры (списки контроллеров) должны быть включены в отчёт.*

4 Открыть закладку **Card** (Карты), чтобы установить фильтры по картам для создания отчёта. Закладка **Card** отображается только в том случае, когда события отчёта связаны с картами.



5 В выпадающем списке **Card index** (Индекс карты) выбрать критерий, который будет использоваться в качестве фильтра. Например, если указать “Card number” (Номер карты), то в отчёт будут включены события доступа с картами, номера которых удовлетворяют указанным параметрам.

ПРИМЕЧАНИЕ: *Если выбран критерий Card number (Номера карт), то в полях* ***Lower boundary*** *(Нижняя граница) и* ***Upper boundary*** *(Верхняя граница) следует указать крайние значения номеров карт. Если выбран критерий* ***Card user name*** *(Имена пользователей карт), то эти же поля служат для ввода текстовых данных. Например, в поле* ***Lower boundary*** *(Нижняя граница) можно ввести букву* ***A****, а в поле* ***Upper boundary*** *(Верхняя граница) букву* ***F****, и тогда в отчёт будут включены события для выбранной двери, в которых будут участвовать только карты с указанными номерами, но не все, а лишь те, чьё имя начинается с букв от* ***A*** *до* ***F****. Если выбрать* ***All*** *(Все), то поля для ввода данных исчезнут с экрана.*

6 Открыть закладку **Report name** (Имя отчёта), указать имя, которое будет отображаться в этом отчёте.

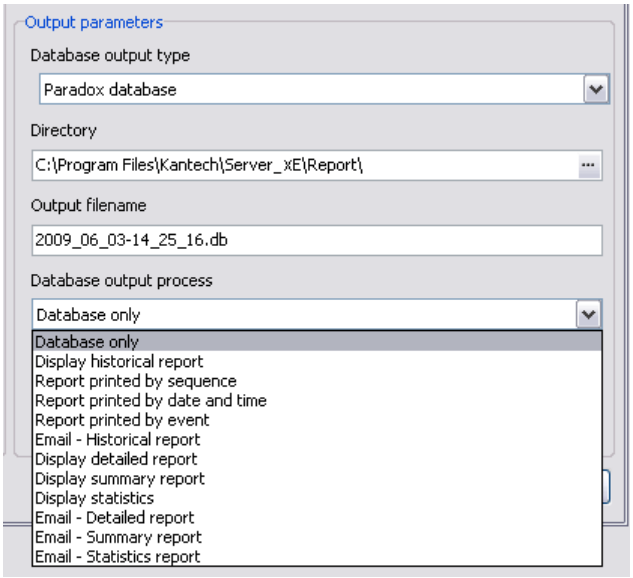
7 Под закладкой **Start/end date** (Начальная/Конечная дата) указать дату и время, с которого система должна начать отбор событий. Например, если в этом поле указать время 7:00, то событие, случившееся в 6:00, в отчёт включено не будет. Для отбора событий, которые случились в определённом временном интервале, рекомендуется использовать закладку **Time period** (Временной интервал).

8 Открыть закладку Time period и отметить флажком опцию Specific time frame (Определённые временные рамки), чтобы включить в отчёт события, удовлетворяющие этому временному интервалу. Указать заданное время для отчёта.

9 Если необходимо записать новый файл поверх предыдущего, то следует открыть закладку **Miscellaneous** (Прочее) и отметить в ней опцию **Overwrite existing output file** (Записать поверх старого файла). В таком случае старый файл с выходными данными отчёта будет заменён новым.

10 Указать выходные параметры отчёта: :

- **Database output type** (Тип выходных данных) – указать выходной формат данных для базы данных (Paradox, Dbase IV или .CSV).
- **Directory** (Путь) – указать путь для записи и хранения отчёта. По умолчанию используется папка: C:\ProgramFiles\Kantech\Sever_G\Report\your file.xx.
- **Output filename** (Имя выходного файла) – указать имя файла с выходными данными. По умолчанию отчёты сохраняются на диск в папку: C:\ProgramFiles\Kantech\Sever_G\Report\your file.xx. Имя файла с отчётом содержит дату и время, в которое отчёт был создан. Если требуется, можно изменить имя файла, но нельзя изменять расширение файла (после точки).



- **Database output process** (Способ вывода базы данных) – указать, каким образом должны быть выведены данные. Для каждого способа вывода данных используется определённый шаблон отчёта.
  - **Database only** (Только база данных) – отчёт будет сохранён в базу данных системы.
  - **Display (historical, detailed, summary or statistics) report** (Показать архивный, детализированный, суммарный или статистический отчёт на экране) – отчёт будет выведен на экран.
  - **Report printed** (Печать отчёта) – указать способ сортировки: Sequence (Последовательно), Date (Дата) или Events (События). Отчёт будет выведен на печать в соответствии с выбранным способом сортировки.
  - **E-mail (historical, detailed, summary or statistics) report** (Отправить архивный, детализированный, суммарный или статистический отчёт по электронной почте) – отчёт будет отправлен на указанный достоверный электронный адрес.
- **Send to workstation** (Отправить на рабочую станцию) – указать, на какую рабочую станцию должен быть отправлен быстрый отчёт. Список содержит все рабочие станции, на которые были установлены приложения SmartLink. Если интерфейс SmartLink установлен на две и более рабочих станций, включённых в сеть, то оператор имеет возможность создавать отчёты на одной рабочей станции и отправлять результаты на другую рабочую станцию, указав SmartLink, соответствующий той рабочей станции, на которую нужно вывести отчёт.

11 Чтобы запустить процесс, нажать кнопку **Execute** (Выполнить).

12 Чтобы увидеть отчёт, нажмите кнопку **Preview** (Предварительный просмотр).

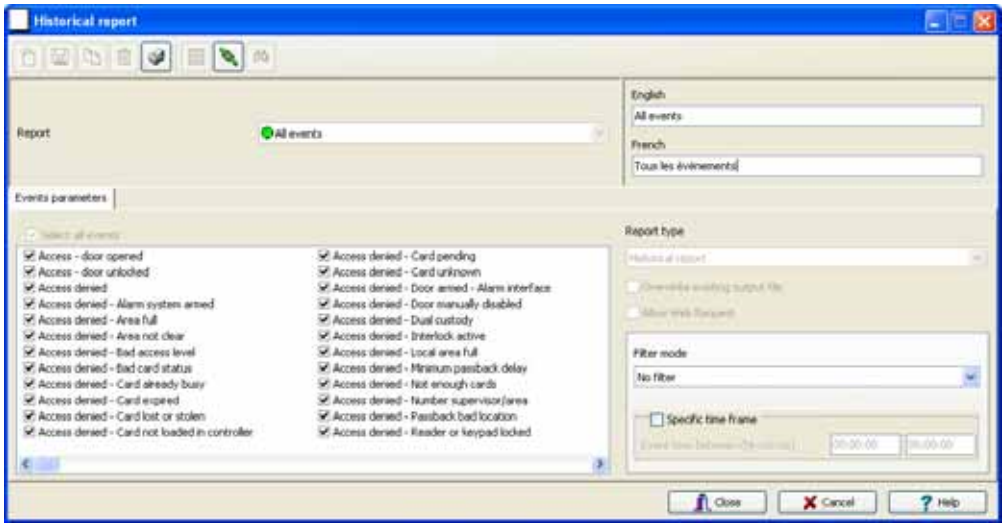
Назначение архивных отчётов

Функция назначения архивных отчётов позволяет пользователям назначать архивные отчеты и отчеты по использованию карт с индивидуальными параметрами автоматического выполнения. Отчёты с автоматическими настройками генерируются автоматически в указанное время. Однако при необходимости создание таких отчётов можно инициировать вручную. Меню “Historical Report Request” (Запрос архивных отчётов) позволяет операторам запускать отчёты в обход автоматических настроек. Если запрос отчёта выполнен вручную, то автоматические настройки игнорируются.

Назначение отчёта по умолчанию "All Events" (Все события)

Оператор может сгенерировать отчёт по умолчанию, в который будут входить все события. Этот отчёт относится к группе архивных отчётов (Historical report). В системе EntraPass обеспечена возможность отправки автоматических отчётов по электронной почте.

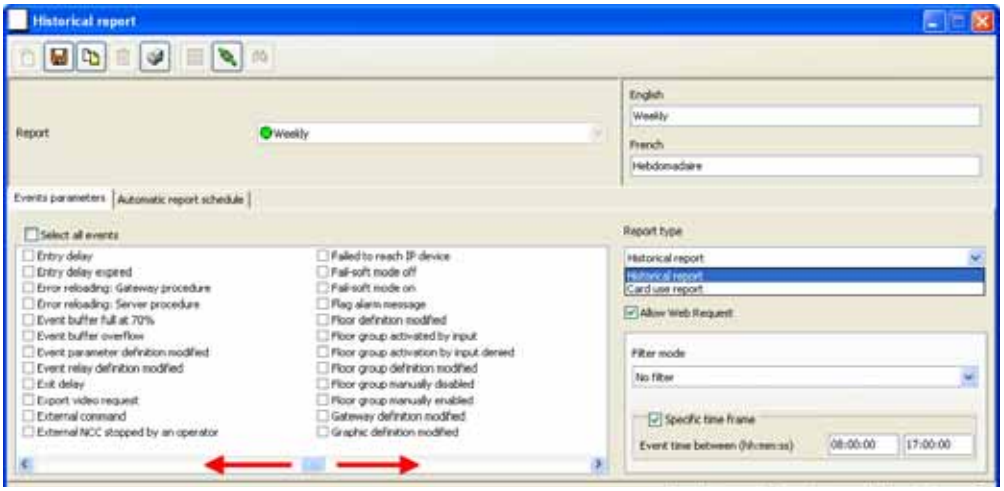
1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **Historical report** (Архивный отчёт). На экране появится окно Historical report.



2 В отчёте **All Events** доступными для редактирования будут только поля для изменения языков.

Назначение архивного отчёта с индивидуальными настройками

1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **Historical report** (Архивный отчёт). На экране появится окно Historical report.



2 Чтобы создать новый отчёт, следует нажать на панели инструментов кнопку **New** (Создать) и ввести необходимые данные на используемых языках в полях справа. Чтобы изменить уже созданный отчёт, его необходимо выбрать из выпадающего списка **Report** (Отчёты).

3 Можно поставить флажок в поле **Select all events** (Выделить все события). В этом случае все 548 возможных событий будут отмечены флажками и включены в отчёт. Или можно указать отдельные события, которые требуется включить в список. При просмотре событий следует перемещать список вправо-влево.

4 Отметить флажком опцию **Overwrite existing output file** (Записать поверх старого файла), чтобы система каждый раз заменяла старый файл отчёта на новый при автоматической генерации отчёта в соответствии с автоматическими настройками, указанными в разделе **Automatic report schedule** (Расписание автоматических отчётов).

5 Отметить флажком опцию **Allow WebStation Request** (Разрешить запрос веб-станции), чтобы запрос архивного отчёта выполнять через веб-станцию EntraPass WebStation. Возможность установки флажка напротив опции появляется только после регистрации вебстанции (WebStation) на сервере EntraPass Server.

ПРИМЕЧАНИЕ: *Если **архивный отчёт** создаётся **с использованием** фильтров (в выпадающем списке указан **Filter mode**), то на экране появляются дополнительные закладки для выбора событий: **Components** (Компоненты) и **Cards** (Карты).*

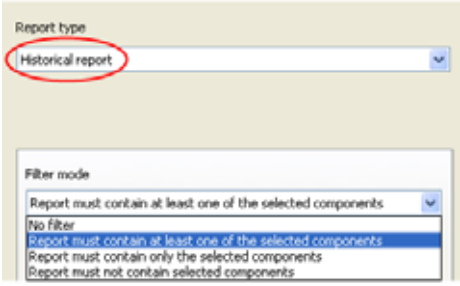
6 *Только для архивных отчётов (Historical Reports).* В случае выбора отчёта типа **Historical report** (Архивный отчёт) следует отметить флажком опцию **Specific time frame** (Определённые временные рамки). В этом случае система будет использовать при создании отчёта указанные временные рамки. В отчёт войдут только те события, которые возникли в указанном временном интервале. Например, если указан интервал с 8:00 до 8:30, то в отчёт будут включены только те события, которые произошли в это время.

7 Выберите закладку **Automatic report schedule** (Расписание автоматических отчётов), чтобы указать необходимые данные для создания автоматического отчёта. *Смотрите в Главе 13 Настройка расписания автоматических отчётов' на странице 446 для более подробной информации .*

Назначение компонентов для архивного отчёта с индивидуальными настройками

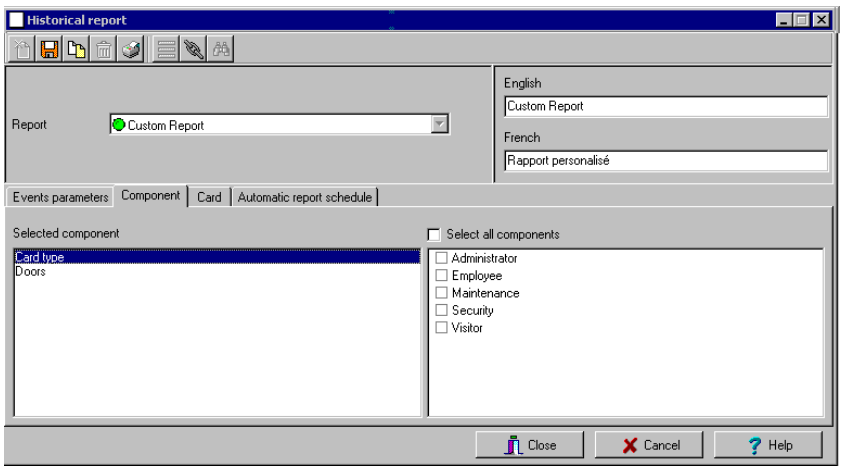
Если архивный отчёт (**Historical report**) создаётся с использованием фильтров (в выпадающем списке **Filter mode** указан фильтр), то **при выборе соответствующих событий** на экране появляются дополнительные закладки: **Components** (Компоненты) и **Cards** (Карты), только когда выбраны связываемые события. Необходимо указать компоненты и карты для создаваемого отчёта.

1 *Только для архивных отчётов (Historical Reports).* Выбрать один из трёх способов отбора (**Filter modes**). Эти фильтры служат для отбора определённых событий, возникших на указанных компонентах. Существуют разные способы отбора. В случае использования этого поля оператор должен указать, какие компоненты и карты использовать, а какие нет.



2 Указать отдельные события или поставить флажок в поле **Select all events** (Выделить все события).

3 Перейти к закладке **Components** (Компоненты). В окне Components перечислены все типы компонентов, которые имеют прямую ссылку на выбранные события.

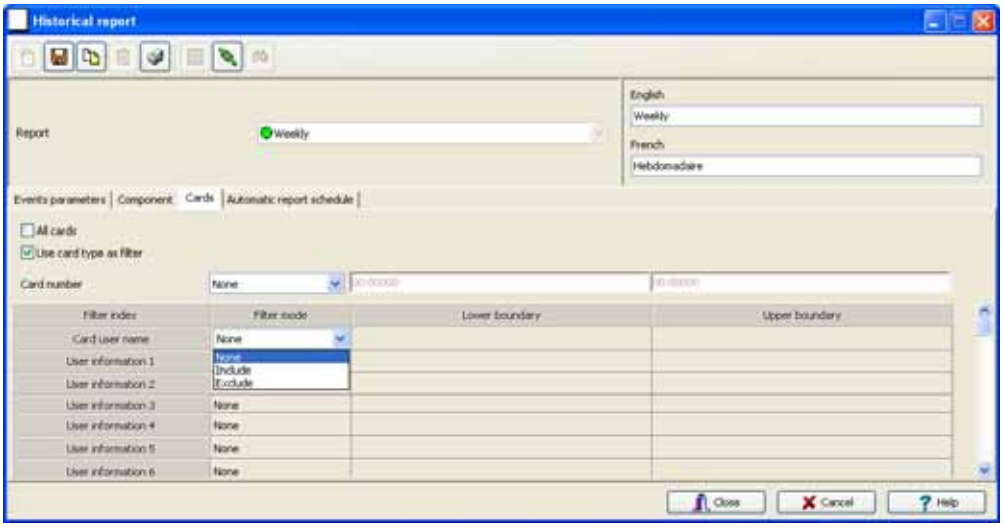


4 Указать тип события. На панели справа появятся все его составляющие. Если выделить **Card type** (Тип карты), то на панели справа будут отображаться все типы карт, описанных в системе. Если выделить Doors (Двери), то справа будут показаны все двери, используемые в системе доступа.

ПРИМЕЧАНИЕ: *При выделении позиции в колонке слева (Selected components) она меняет цвет (становится красной). При снятии выделения цвет снова становится таким же, каким был прежде (по умолчанию).*

Назначение дополнительных функций карт для архивного отчёта с индивидуальными настройками

1 В окне Historical report (Архивные отчёты) перейти к закладке **Cards** (Карты). Она отображается только в том случае, если при выборе типа событий были указаны события, связанные с предоставлением доступа (Access events). Эта закладка содержит дополнительные фильтры для создаваемого отчёта, позволяя отобрать определённые события.



2 Выделить флажком опцию **All Cards** (Все карты), если необходимо включить в отчёт все карты. Если сделать именно так, то все другие поля исчезнут. Если поставить флажок напротив опции **Use card type as filter** (Использовать тип карт в качестве фильтра), то появляется возможность использовать дополнительные фильтры при создании отчёта. Перед оператором появляются поля, которые можно использовать как фильтры, устанавливая/снимая выделение, и для каждого выделенного параметра следует указать нижнюю и верхнюю границы.

3 Указать, какие информационные поля будут использоваться в качестве фильтра (колонка **Filter index**). Например, если указать “Card number” (Номер карты), то в отчёт будут включены события доступа с картами, номера которых удовлетворяют указанным параметрам.

4 В колонке **Filter mode** (Способ отбора) указать нужное в выпадающем списке: **None** (Не использовать), **Include** (Включить), **Exclude** (Исключить), то есть выбрать, какое действие (исключить или включить) необходимо выполнить с позициями, удовлетворяющими критериям отбора в указанном диапазоне (между верхней и нижней границами). После выбора действия (Exclude или Include) становятся активными поля для задания границ (Lower boundary и Upper boundary).

5 Указать значения в полях Lower boundary (Нижняя граница) и Upper boundary (Верхняя граница) в соответствии с выбранным действием в поле **Filter mode.** Например, можно отбирать идентификационные карты по именам владельцев (буквенный фильтр) или по номерам карт (в этом случае в полях для задания верхней и нижней границы необходимо вводить цифры). При отборе по имени владельца карты можно, например, задать в полях **Lower/Upper boundary** значения от A до F. Таким образом, в отчёт будут включены события для выбранной двери, в которых будут участвовать только карты с указанными номерами, но не все, а лишь те, чьё имя начинается с букв от A до F.

ПРИМЕЧАНИЕ: *Для одного и того же отчёта в колонке Filter index разрешается устанавливать не один, а несколько фильтров одновременно. Отбор событий будет производиться несколько раз, в зависимости от того, сколько фильтров указано использовать для данного отчёта.*

Назначение отчёта об использовании идентификационных карт

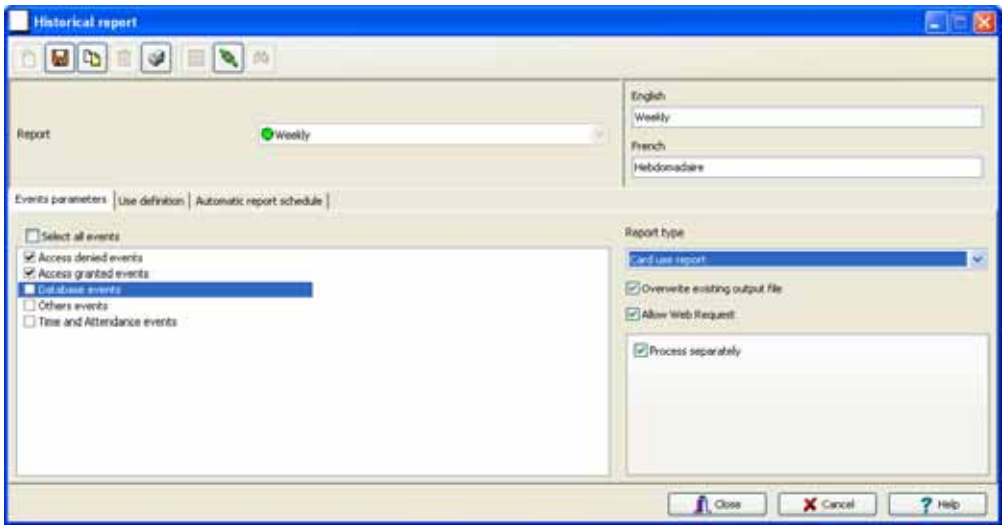
Функция Card use report служит для создания отчётов, в которых перечислены владельцы карт, создававшие/не создававшие события за последние несколько дней или начиная с некоторой указанной даты. Например, может возникнуть необходимость запросить отчёт, в который войдут события типа “Access granted” (Доступ разрешён), зарегистрированные начиная с указанной даты.

ПРИМЕЧАНИЕ: *Если выделить опцию Card use report (Отчёт об использовании карт), то в окне Historical report (Архивные отчёты) появляется закладка Use definition (Назначение использования карт). Под этой закладкой находятся параметры, связанные с частотой использования карт, например, можно отобрать карты, предъявлявшиеся начиная с указанной даты, или неиспользовавшиеся в течение последних 30 дней и др.*

В системе предусмотрено пять типов событий:

- Access denied (доступ отклонен) (проход не в том месте, не тот уровень доступа, не тот статус карты и т.д.),
- Доступ предоставлен
- События, влияющие на работу базы данных (например, изменение описания карты и т.п.)
- Другие события
- События по учёту рабочего времени (приход-уход).

1 В окне Historical report (Архивные отчёты) выбрать нужный отчёт из выпадающего списка **Report** (Отчёты). Чтобы создать новый отчёт, следует нажать на панели инструментов кнопку **New** (Создать) и ввести необходимые данные на используемых языках в полях справа.



2 Выбрать **Card use report** (Отчёт об использовании карт) в выпадающем списке **Report type** (Тип отчёта). Если выбрана опция **Card use report**, то на панели слева отображаются только события, связанные с использованием карт.

3 Поставить флажок в поле **Select all events** (Выделить все события) (в этом случае окошко для выделения отдельных событий отображаться не будет) или указать отдельные события, которые необходимо включить в отчёт.

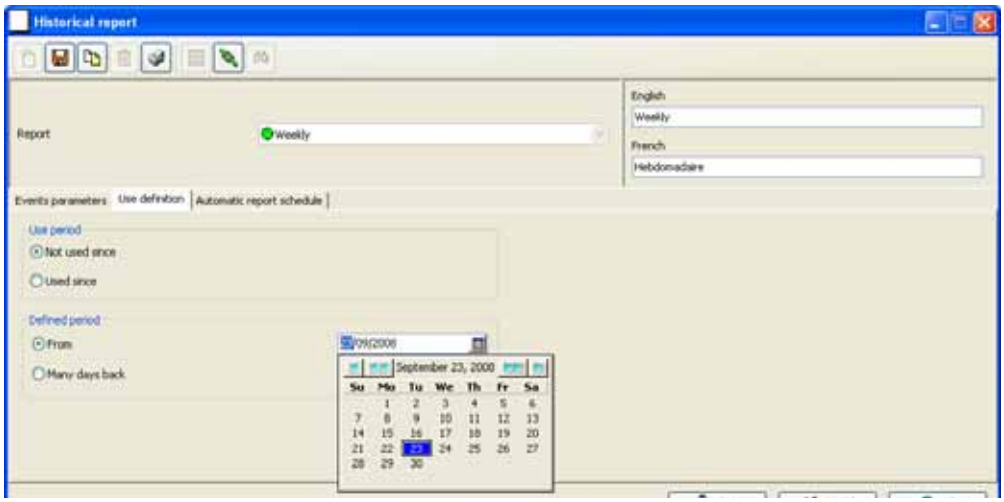
4 Отметить флажком опцию **Overwrite existing output file** (Записать поверх старого файла), чтобы система каждый раз заменяла старый файл отчёта на новый при автоматической генерации отчёта в соответствии с автоматическими настройками, указанными в разделе **Automatic report schedule** (Расписание автоматических отчётов).

5 Отметить флажком опцию **Allow WebStation Request** (Разрешить запрос веб-станции), чтобы запрос архивного отчёта выполнять через веб-станцию EntraPass WebStation. Возможность установки флажка напротив опции появляется только после регистрации вебстанции (WebStation) на сервере EntraPass Server.

6 Кроме того, при необходимости можно отметить флажком опцию **Process separately** (Обрабатывать раздельно), чтобы указанные события были обработаны независимо для каждой карты. Допустим, необходимо создать отчёт для событий с запретом доступа (Access denied events) и для событий с разрешением доступа (Access granted events). Если опция **Process separately** не активирована, отчёт будет содержать все эти события. Если пометить флажком **Process separately**, отчёт будет содержать отдельно события с разрешением доступа и отдельно события с запретом доступа.

ПРИМЕЧАНИЕ: *Опция **Process separately** (Обрабатывать раздельно) доступна только при условии, что у выбранного отчёта указан тип **Card use report** (Отчёт об использовании карт).*

7 Перейти к закладке **Use definition** (Назначение использования карт), чтобы указать временные интервалы и параметры использования карт: **Not used since** (Не использовавшиеся начиная с...) или **Used since** (Использовавшиеся начиная с...).



ПРИМЕЧАНИЕ: *Закладка **Use definition** (Описание использования) доступна только при условии, что у выбранного отчёта указан тип **Card use report** (Отчёт об использовании карт).*

8 Чтобы указать расчётный период, следует отметить флажком поле **From** (Начиная с...) и ввести дату в поле **From.** Или выбрать дату в календаре, вызвав его при помощи соответствующей кнопки **Calender** (Календарь). Кроме того, можно ввести дату при помощи стрелок вверх-вниз, либо задать временной интервал по числу дней, прошедших с нужной даты: опция **Number of days back** (... дней назад).

9 После завершения ввода параметров для создания отчёта необходимо сохранить настройки. Чтобы запросить отчёт, следует нажать кнопку **Report request** (Запросить отчёт) на панели инструментов в окне Report (Отчёты).

10 Открыть закладку **Automatic report schedule** (Расписание автоматических отчётов), чтобы указать необходимые данные для создания автоматического отчёта. *Смотрите в Главе 13 Настройка расписания автоматических отчётов' на странице 446 для более подробной информации* о назначении автоматических отчётов .

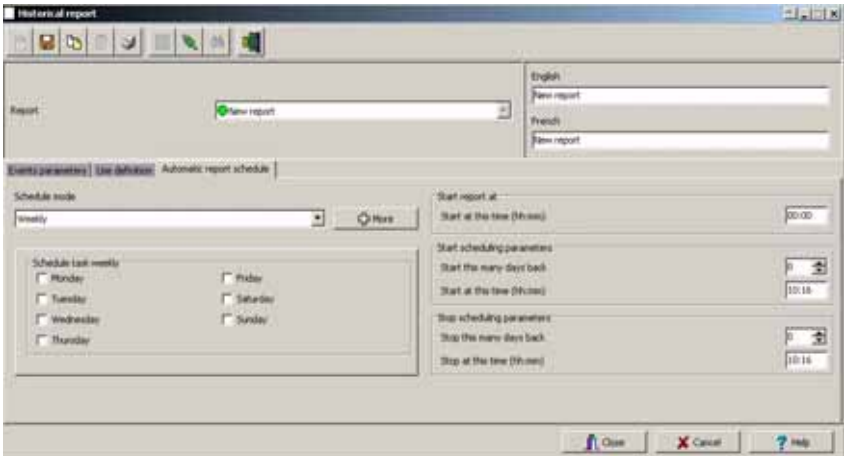
Настройка расписания автоматических отчётов

(Для архивных отчётов и отчётов по использованию карт)

Закладка **Automatic report schedule** служит для настройки параметров, необходимых для создания отчётов в автоматическом режиме. В эти настройки входят следующие параметры:

- Частота генерации отчёта (frequency): не создавать, создавать еженедельно, ежемесячно или однократно
- Охваченный временной период
- Способ вывода отчёта: на дисплей, на принтер или др.
- Выходной формат данных (dBase, Paradox, CSV)
- Пункт назначения (рабочая станция)
- Выбор языка и имени файла)

1 В окне Historical report (Архивные отчёты) перейти к закладке **Automatic report schedule** (Расписание автоматических отчётов).



2 В выпадающем списке **Schedule mode** (Режим расписания) выбрать необходимую частоту создания отчёта:
   - **None** (Не использовать) – запрашивать отчёт вручную (смотрите *раздел "Запрос архивных отчётов*").
   - **Weekly** (Еженедельно) – генерировать отчёт еженедельно. В этом случае необходимо также указать день недели, в который должен создаваться автоматический отчёт.
   - **Monthly** (Ежемесячно) – создавать отчёт один раз в месяц. Здесь необходимо также указать день (например, вторая пятница каждого месяца или 15-й день месяца), в который должен создаваться автоматический отчёт.
   - **Once** (Однократно) – создавать отчёт автоматически при наступлении указанной даты.

3 В поле **Start at this time** (Начальное время) указать время, в которое система должна приступить к генерированию отчёта.

4 Указать **Scheduling parameters** *(Календарные параметры событий).*

ПРИМЕЧАНИЕ: *Эти настройки будут* ***игнорироваться****, если отчёт будет запрашиваться вручную оператором.*

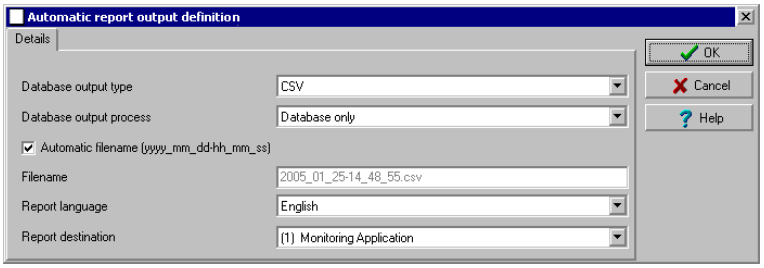
- **Start this many days back** (Начальная дата - ... дней назад) – в отчёт будут собраны события, зарегистрированные некоторое указанное число дней тому назад. Отсчёт дней выполняется начиная с текущей даты.
- **Start at this time** (Начальное время) – после указания начальной даты следует указать начальное время сбора событий (например, 7:00). Например, если в этом поле указано время 7:00, то событие, случившееся в 6:00, в отчёт включено не будет.
- **Stop this many days back** (Конечная дата - ... дней назад) – в отчёт будут собраны события, зарегистрированные некоторое указанное число дней тому назад. Отсчёт дней выполняется начиная с текущей даты.
- **Stop at this time** (Конечное врем) – после указания конечной даты следует указать конечное время (например, 5:00 вечера). Таким образом, система будет отбирать события, произошедшие до указанного дня и до указанного момента времени. Например, если в этом поле указать время 7:00, то событие, случившееся в 8:00, в отчёт включено не будет. Для

отбора событий, которые случились в определённом временном интервале, рекомендуется использовать закладку **Specific time frame** (Временной интервал).

ПРИМЕЧАНИЕ: *Начальное и конечное время используются только при указании начальной и конечной даты. Например, если указаны начальная дата и время "понедельник, 8:00" и конечная дата и время "пятница, 17:00", то система будет выполнять отбор событий, произошедших в интервале с понедельника, 8:00 по пятницу, 17:00. Начальное и конечное время устанавливаются* ***не для каждого дня*** *в заданном интервале, а только для указания границ интервала.*

Дополнительные настройки автоматического отчёта

1 Чтобы сделать дополнительные настройки автоматического отчёта, генерируемого по расписанию, следует нажать кнопку **More** (Дополнительно). При нажатии кнопки **More** на экране появляется окно Automatic report output definition (Описание выходных данных автоматического отчёта).



2 В выпадающем списке **Output type** (Тип выходных данных) указать выходной формат отчёта. Доступны форматы Paradox, Dbase IV и CSV.

ПРИМЕЧАНИЕ: *В поле* ***Database output process*** *(Способ вывода базы данных) можно указать, например,* ***E-mail historical report*** *(Отправить архивный отчёт по электронной почте), чтобы отправить отчёт на указанный электронный адрес. В случае выбора этой опции следует открыть закладку* ***E-mail*** *(Электронная почта) и указать электронный адрес получателя в поле* ***Send E-mail to.*** *В системе EntraPass предусмотрена возможность защиты отчётов паролем перед отправкой их по электронной почте.*

3 При желании можно поставить флажок в поле **Automatic filename** (Автоматическое назначение имени файла). По умолчанию имя файла с отчётом имеет формат YYY_MM_DD-HH_MM_SS.X, то есть год_ месяц_ день-часы, минуты_секунды.расширение файла.

ПРИМЕЧАНИЕ: *Более подробные сведения по формату и типу выходных данных приводятся чуть ниже в таблице. Она содержит сравнительные характеристики для разных форматов отчётов.*

Результаты сравнения различных форматов баз данных и их выходных файлов даны в следующей таблице:

База данных	Описание	.db	.rdf	.csv
Paradox	Помимо традиционных выходных форматов .db, .rdf база данных Paradox может создавать файлы с расширениями .px, .xg0, .xg1, .yg0, .yg1. Они содержат индексы и используются при работе с этой базой данных. Кроме того, их может использовать администратор этой базы данных.	X	X	X
Dbase IV	Популярный формат для систем управления базами данных, предназначенный для хранения данных. Поддерживается практически всеми системами администрирования баз данных и электронными таблицами. Даже системы, которые сами не поддерживают DBase формат, могут экспортировать и импортировать данные в этом формате.	X	X	-

База данных	Описание	.db	.rdf	.csv
CSV	Сохраняет отчёт в файл значений с разделителями-запятыми (имя файла.csv). Это формат данных, в котором все блоки данных разделены друг от друга запятыми. Это популярный формат для передачи данных из одного приложения в другое, так как большинство систем администрирования баз данных поддерживают импорт и экспорт данных с разделителями-запятыми.	-		X

4 Средства редактирования выходных файлов различных форматов перечислены ниже в таблице. Редактированию подлежат только файлы формата ".db".

Выходной файл	Paradox	Dbase IV	CSV
.db, средство редактирования	dBase IV, dBFast, MultiEdit, DbVista, Paradox, SmartWare and XtreeGold.	dBase III, IV, FoxPro, dBFast, DataBoss and Excel.	-
.csv, средство редактирования	-	-	Excel, Блокнот, WordPad, etc.
.rdf, средство просмотра	Средства EntraPass (Borland Database Engine)	Средства EntraPass (Borland Database Engine)	Блокнот

5 В выпадающем списке **Output process** (Способ вывода базы данных) указать шаблон отчёта. Он будет использоваться вместе с запрашиваемым отчётом. *см. 'Назначение выходного формата отчёта'*.

Назначение выходного формата отчёта

(Для архивных отчётов и отчётов по использованию карт)

1 Если указано сохранять отчёт только в базу данных, то есть выбрана опция **Database only** (*CSV, Paradox и Dbase*), то в отчёт будет включена следующая информация: последовательность событий, даты и время, сообщения о событиях, тип описания (отображает особый номер, по которому можно идентифицировать компоненты системы), описательные имена (отображает имя компонента, как он описан в системе – имя типового номера описания), а также номера карт (для событий, связанных с идентификационными картами).

ПРИМЕЧАНИЕ: *Если выбран способ генерации отчёта только для базы данных, то отчёт будет сохранён в папке отчётов в указанном формате. Он не будет выведен ни на принтер, ни на экран.*

2 *Только для баз данных Paradox:* если выбрана опция **Display Historical report - Display card last transaction report** (Показывать на экран архивный отчёт – Показывать на экране отчёт по последним транзакциям карт), то отчёт будет автоматически отображаться на экране после окончания процесса генерации. Перед тем как отправить отчёт на печать, оператор может индивидуально скорректировать отчет. *Смотрите в Главе 13 Предварительный просмотр архивных отчетов' на странице 466 для более подробной информации* по индивидуальной настройке отчётов. В отчёт будет включена следующая информация: последовательность событий, даты и время, сообщения о событиях, номера карт (для событий, связанных с идентификационными картами) и описания 1 – 4, в которых содержатся подробные сведения о событиях.

3 Только для баз данных Paradox: если выделена опция **Report printed by sequence** (Распечатка отчёта в порядке последовательности), то события отчёта будут отсортированы по номерам (в том порядке, как они были созданы в системе) и автоматически выведены на печать на принтере на указанной рабочей станции.

4 Только для баз данных Paradox: если выделена опция **Report printed by date and time** (Распечатка отчёта по дате и времени), то события отчёта будут отсортированы по дате и времени и автоматически выведены на печать на принтере на указанной рабочей станции.

ПРИМЕЧАНИЕ: *Отчёты, которые должны быть распечатаны на принтере (п. 3 и 4), будут сохранены в папке отчётов в указанном формате. Они будут выводиться на принтер, но не будут отображаться на экране.*

5 Только для баз данных Paradox: если выделена опция **Report printed by event** (Распечатка отчёта по событиям), то события отчёта будут отсортированы по сообщениям о событии (в алфавитном порядке) и будут автоматически выведены на печать на принтере на указанной рабочей станции. Отчёт будет сохранён в папке отчётов в указанном формате, но на экране отображаться не будет.

Отчёты по учёту рабочего времени

Отчёты по учёту рабочего времени будут сохранены в папке для хранения отчётов и не будут выведены ни на экран, ни на принтер. Для просмотра отчётов пользователь должен будет вручную запросить его или использовать меню View Report (Просмоторщик отчетов).

1 *Т*олько для баз данных CSV: опция **Single file with all data** (Один файл со всеми данными). Отчёт генерируется в один файл, содержащий данные и описания (даты и время, идентификационные номера транзакций, номера карт, имена владельцев карт и описания дверей).

2 Только для баз данных типа CSV, Paradox и DBase IV: опция **Database with transactions** (База данных с транзакциями). Отчёт будет сгенерирован в виде одного файла, в который будут включены все данные и транзакции. Он будет содержать информацию: дату и время, ID транзакции/операции, номер карты и имя их владельцев.

3 Только для баз данных Paradox: если выбрана опция **Display time and attendance report** (Показывать на экран отчёт по учёту рабочего времени), то отчёт будет автоматически отображаться на экране после окончания процесса генерации. Перед тем как отправить отчёт на печать, оператор может индивидуально изменить его настройки. В отчёт будет входить следующая информация: номера карт, имена владельцев карт, время входа и время выхода, содержимое информационных полей карт, указанных в описании отчёта, а также общее количество часов для каждого владельца карты. *Смотрите в Главе 13 Предварительный просмотр отчётов по учёту рабочего времени' на странице 467 для более подробной информации по тому, как редактировать отчет перед печатью*.

4 Для баз данных Paradox и DbaseIV: опция **Two (2) databases with all data** (Две базы данных со всеми данными) позволяет генерировать отчёт в виде двух раздельных файлов:

- **В одном файле содержится следующая информация:** даты, время, сообщения о событиях (тип транзакций), pkcard (номера карт), pkdoor (номера дверей), pkdoorgroup (номера групп дверей).
- **Во второй файл включены данные:** описание pk (объяснение к параметрам pkcard, pkdoor и pkdoorgroup), номера карт, объекты и содержимое информационных полей карт, указанных в меню описания отчёта.

ПРИМЕЧАНИЕ: *Под обозначением PK понимают уникальный номер компонента в системе.*

5 *Для баз данных типа Paradox и DbaseIV:* опция **Single database with all data** (Одна база данных со всеми данными) служит для создания отчёта в виде одного файла, содержащего данные и описания (даты и время, идентификаторы транзакций, номера карт, имена владельцев карт, описания дверей и последовательность событий).

6 **CSV compilation time and attendance** (Составление отчёта по учёту рабочего времени в формате CSV) (только для *CSV*). При генерировании отчёта будут создаваться два файла. В один файл войдут общие данные, например, количество часов работы по отделам компании, а в другом будет находиться подробная информация. В зависимости от того, за какой срок составляется отчёт, колонка "day" будет содержать данные для каждого дня.

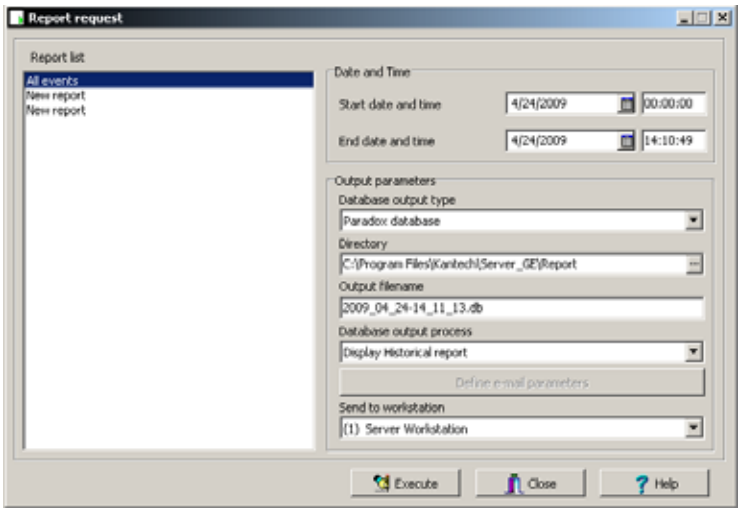
- **Automatic filename** (Автоматическое назначение имени файла) – эту функцию следует использовать для автоматического назначения даты и времени, в качестве имени файла. Эта функция не может быть использована вместе с опцией "Overwrite existing output file" (Записать поверх старого файла).
- **Filename** (Имя файла) – если один и тот же отчёт необходимо перезаписывать регулярно (например, еженедельно), то здесь можно указать имя файла, и тогда новый отчёт, сгенерированный по всем указанным параметрам, будет записываться поверх старого.
- **Destination** (Путь для файла с результатами) – путь для автоматического сохранения/распечатки отчёта. Кроме того, можно активировать опцию "**Overwrite existing output file**" (Записать поверх старого файла), чтобы указать другой выходной файл.
- **Report language** (Язык отчёта) – это поле позволяет включить в отчёт дополнительную информацию. Доступные варианты перечислены в выведенном на экран списке.

Выполнение запроса архивных отчётов

С помощью этой функции операторы могут запрашивать предварительно настроенные архивные отчёты (**Historical reports**) или отчёты об использовании идентификационных карт (**Card use reports)**, которые были созданы при помощи меню Historical Report. Кроме того, операторы могут отправлять отчёты по электронной почте одному или нескольким адресатам.

ПРИМЕЧАНИЕ: *Если в отчёте указаны автоматические настройки, то они будут игнорированы. Необходимо указать новые данные.*

1 На панели инструментов **Report** (Отчёты) нажать кнопку **Report request** (Вызов отчёта). На экране появится окно Report request.

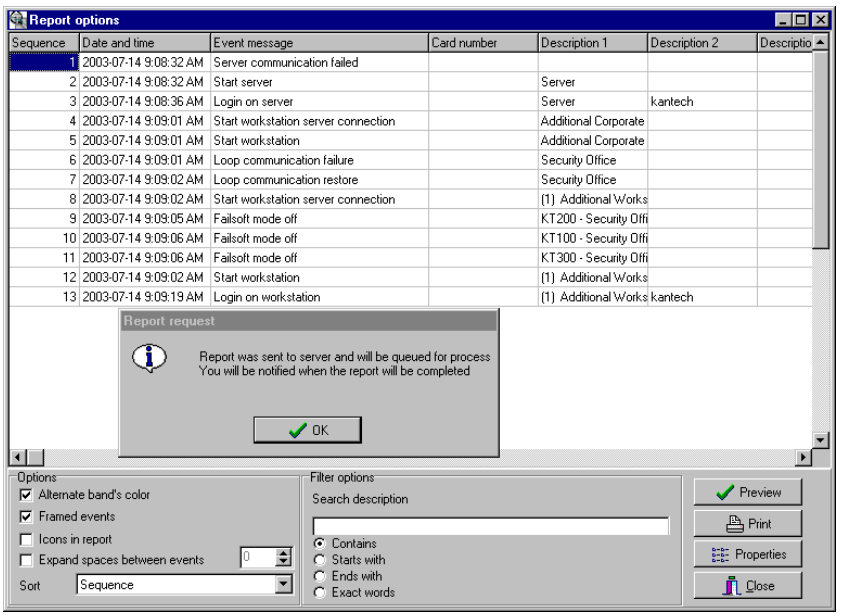


2 На панели слева (**Report list**) указать, какой отчёт должен быть выполнен.

3 При необходимости указать выходные параметры в разделе **Output parameters**, в том числе в поле **Database output type** (Тип базы данных) выбрать одну из опций: Paradox, DBase IV, CSV, PDF, Excel, RTF или Text, указать папку назначения, имя выходного файла и др. *Смотрите в Главе 13 Назначение выходного формата отчёта' на странице 448 для более подробной информации* .

ПРИМЕЧАНИЕ: *Если выбран отчёт типа Card use report (Отчёт об использовании карт), то раздел "Date and time" (Дата и время) будет недоступен.*

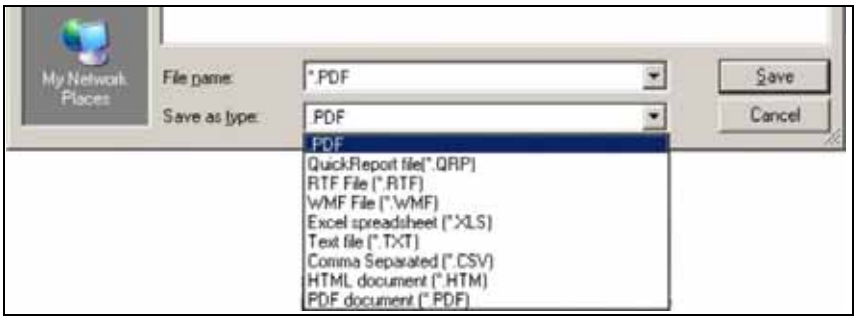
4 Нажать кнопку **Execute** (Выполнить). На экране появится сообщение системы о выполнении отчёта. Система выведет на экран окно Report options (Параметры отчёта) и затем свернёт его на панель задач.



5 Нажать кнопку **Preview button** (Кнопка предварительного просмотра), чтобы настроить отчёт и установить необходимые фильтры. Повысить удобочитаемость отчёта можно, например, путём добавления полос другого цвете, обрамления событий в рамку, прикрепления к событиям иконок и др. или путём сортировки событий в отчёте (по идентификационному номеру событии, в алфавитном порядке или по дате и времени).

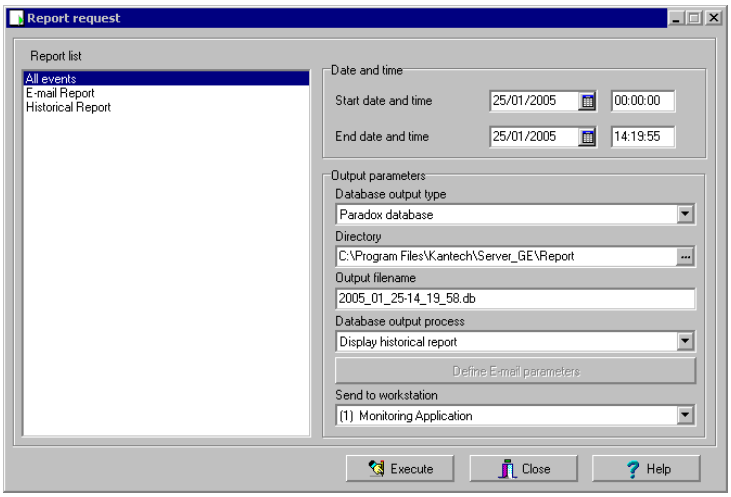
6 Ввести **описание** в поле **Search description** (Поиск описания). При вводе параметров фильтрации отчёты обновляются в режиме реального времени.

7 Кнопка **Preview** (Предварительный просмотр) позволяет предварительно просмотреть отчёт, кнопка **Properties** (Свойства) служит для просмотра данных отчёта. Если нажать кнопку **Preview,** система выведет результаты отчёта на экран. В этом окне можно сохранить отчёт в различном формате или распечатать его на принтере.



Запрос отчёта о событиях

1 На панели инструментов **Report** (Отчёты) нажать кнопку **Report request** (Вызов отчёта). На экране появится окно Historical report request.



2 Указать начальное время (**Start time**) и конечное время (**End time**). По умолчанию конечная дата и время установлены на текущее время системы.

3 Оператор может установить свои выходные параметры или оставить значения по умолчанию.

ПРИМЕЧАНИЕ: *Необходимо хорошо понимать различия разных типов выходных данных и форматов. Смотрите в Главе 13 Назначение выходного формата отчёта' на странице 448 для более подробной информации .*

4 Чтобы увидеть статус отчёта, нажать иконку **Report state** (состояние отчёта) на панели инструментов. .

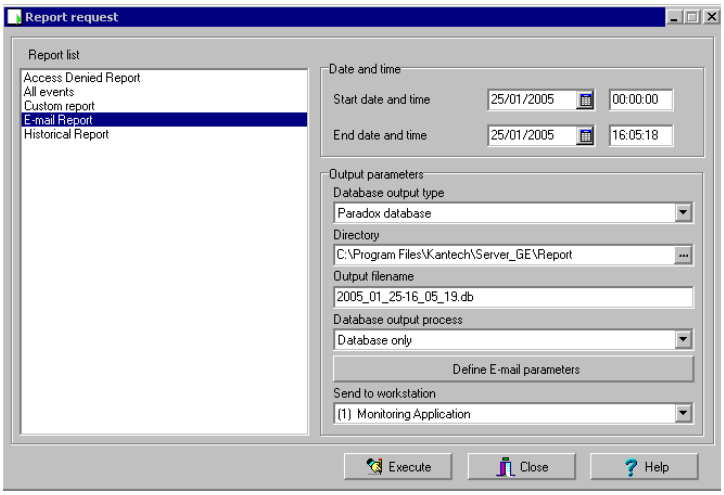
5 Нажать иконку **View report** (Посмотреть отчёт) на панели инструментов, чтобы посмотреть отчёт на экране. По умолчанию имя отчёта установлено YYYY_MM_DD_-HH_MM_SS.db (YYYY – год, MM – месяц, DD – день, HH – часы, MM – минуты, SS – секунды, .db – расширение файла).

Отчёты, отправляемые по электронной почте

EntraPass позволяет вам отправлять отчеты по электронной почте одному или нескольким адресатам. Эта функция доступна во время назначения рабочей станции EntraPass и при указании формата выходных данных отчёта. Архивные отчёты (Historical reports), отчёты по учёту рабочего времени (Time and attendance reports), а также быстрые отчёты (Quick reports) можно отправлять на любой достоверный электронный адрес.

Настройка отчёта для отправки по электронной почте

1 На панели инструментов Report (Отчёты) нажать кнопку Quick report request (Вызов быстрого отчёта), Report request (Запрос отчёта) или T and A request (Запрос отчёта по учёту рабочего времени).

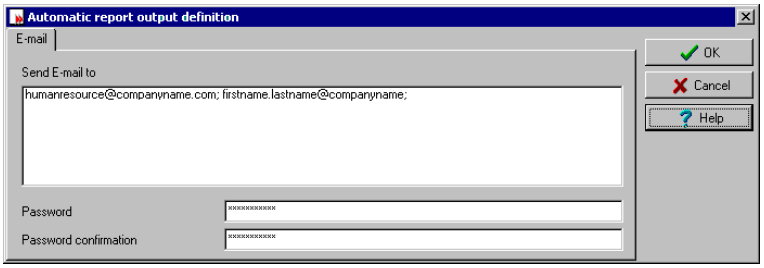


2 На панели **Report List** (Список отчётов) указать, какой отчёт необходимо отправить по электронной почте.

3 Настроить параметры отчёта.

4 В выпадающем списке **Database Output Process** (Способ вывода базы данных) указать **e-Mail report** (**detailed** – подробный, **summary** – сводный или **statistics** - статистический) вы хотите послать**.**

5 Нажать кнопку **Define E-mail parameters** (Назначить параметры электронной почты), чтобы открыть окно Automatic report output definition (Назначение выходных данных автоматического отчёта).



6 В поле **Send E-mail to** (Получатель) указать электронный адрес назначения. При перечислении нескольких адресов их следует разделять знаком "точка с запятой" (;).

7 Нажать **OK**, чтобы закрыть окно.

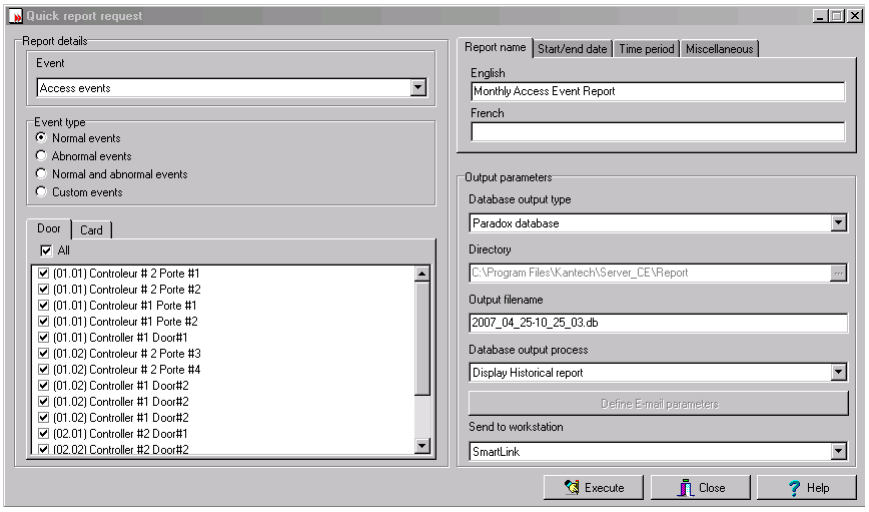
ПРИМЕЧАНИЕ: *Отправка отчётов не ставит под угрозу безопасность и защищённость данных. Файлы формата rpf при желании могут быть защищены паролем. Получить доступ к таким файлам смогут только те пользователи, которые будут знать правильный пароль. Файлы CSV защитить паролем невозможно.*

8 Нажать кнопку **Execute** (Выполнить), чтобы отправить отчёт на указанный адрес. Отчёт будет отправлен на рабочую станцию, указанную в выпадающем списке Send to workstation (Отправить на рабочую станцию), а также указанным адресатам.

Отправка отчётов на рабочие станции при помощи интерфейса SmartLink

В системе EntraPass предусмотрена возможность отправки отчётов на рабочие станции с установленным интерфейсом SmartLink (даже если на этих машинах не установлена система EntraPass). Если SmartLink установлен на двух и более АРМ, объединённых в сеть, то при помощи SmartLink оператор может генерировать отчёт на одной рабочей станции и отправлять результаты на другую рабочую станцию.

1 Открыть закладку **Report** (Отчёты), выбрать тип отчёта и нажать соответствующую иконку. Данная опция доступна в меню Quick Report Request (Запрос быстрого отчёта), Report Request (Запрос отчёта) и Time and Attendance Request (Запрос отчёта по учёту рабочего времени).



2 Чтобы отправить отчёт на другую рабочую станцию с установленным интерфейсом SmartLink, сначала необходимо выделить уже настроенный отчёт или внести в программу описание нового.

3 В выпадающем списке **Send to workstation** (Отправить на рабочую станцию) выделить пункт SmartLink, соответствующий той рабочей станции, на которую необходимо отправить отчёт.

- После окончания генерации отчёта он появится на экране рабочей станции-получателя.
- При использовании интерфейса SmartLink в режиме службы отчёт не будет выводиться на экран компьютера. Вместо этого он будет сохранён в папку, предназначенную для сохранения отчётов.

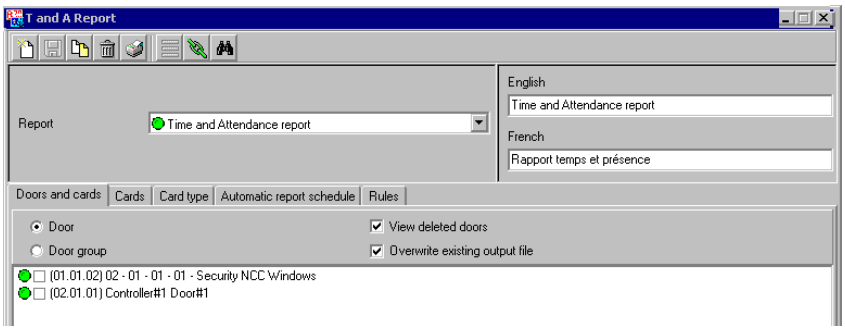
Назначение отчётов по учёту рабочего времени

Эта функция служит для индивидуальной настройки отчётов по учёту рабочего времени с параметрами автоматического выполнения.

ПРИМЕЧАНИЕ: *Эти отчёты могут иметь* ***автоматические настройки****, и тогда система будет генерировать их в указанное время, или могут запрашиваться оператором* ***вручную*** *при помощи нажатия иконки "Time and attendance report request" (Запрос отчёта по учету рабочего времени). Если запрос отчёта выполнен вручную, то автоматические настройки* ***игнорируются****.*

Назначение отчётов по учёту рабочего времени

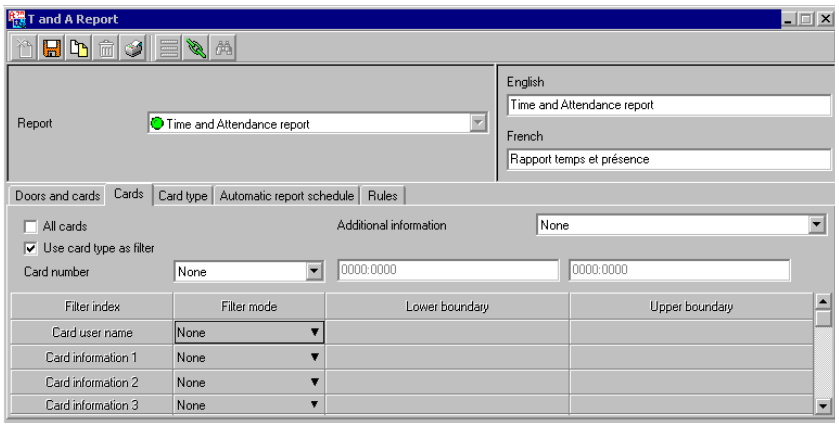
1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **T & A Report** (Отчёт по учёту рабочего времени).



2 Если выбрана опция **Doors** (Двери), то на экране будут отображаться только двери, предназначенные для учёта рабочего времени (это должно быть указано в меню назначения дверей Door). Нажать кнопку **View deleted doors** (Посмотреть удалённые двери), чтобы добавить в список двери, помеченные для удаления. В случае выделения опции **Door group** (Группы дверей) опция **View deleted doors** будет недоступна. В этом случае на экране будут показаны группы дверей; оператор может выбрать некоторые из них.

3 Выделить флажком опцию **Overwrite existing output file** (Записать поверх старого файла), если необходимо записывать новый файл поверх старого. Если не использовать эту опцию, система будет создавать другие файлы с выходными данными.

4 Открыть закладку **Card** (Карты), чтобы установить фильтры по картам для создания отчёта.



ПРИМЕЧАНИЕ: *Закладка* **Card type** *(Тип карт) появляется, если поставить флажок напротив опции* ***Use card type as filter*** *(Использовать тип карт в качестве фильтра.*

5 Выбрать критерий отбора в колонке Filter index (Индекс фильтра), затем в колонке Filter mode (Способ отбора) указать нужное действие в выпадающем списке: **None** (Не использовать), **Include** (Включить), **Exclude** (Исключить). После выбора критериев и способа отбора следует указать верхнюю и нижнюю границы значений (**Upper boundary** и **Lower boundary**). Если в выпадающем списке в колонке Filter mode (Способ отбора) выделить **None** (Не использовать), то в список будут включены все позиции. Например, если при отборе по номерам карт установить в

поле Filter index значение **None**, то в отчёт будут включены все события, вызванные действиями с картами.

6 Чтобы добавить данные в критерии сортировки, следует выбрать параметр в выпадающем списке **Additional information** (Дополнительные сведения).

ПРИМЕЧАНИЕ: *Описанные действия следует повторить для всех информационных полей карт, которые перечислены в колонке Filter index (Индекс фильтра). Например, оператор может использовать имена пользователей в качестве критерия отбора и указать в поле Lower boundary (Нижняя граница) букву A, а в поле Upper boundary (Верхняя граница) букву F, и тогда в отчёт будут включены события, в которых участвуют только карты владельцев с именами, начинающимися с букв от A до F (а остальные не войдут в отчёт, даже если номера карт соответствуют указанному диапазону).*

7 Открыть закладку **Card type** (Типы карт), если она доступна, и указать типы карт, которые должны быть включены в отчёт. Закладка **Card type** (Тип карт) появляется, если поставить флажок напротив опции **Use card type filter** (Использовать тип карт в качестве фильтра).

8 Открыть закладку **Automatic report schedule** (Расписание автоматических отчётов), чтобы указать необходимые данные для создания автоматического отчёта. *Смотрите в Главе 13 Настройка расписания автоматических отчётов' на странице 446 для более подробной информации* .

9 Открыть закладку **Rules** (Правила) и указать правила, по которым следует вести учёт рабочего времени и создавать отчёты. Чтобы для некоторых периодов времени назначить определённые значения, следует создать правила. Например, всем работникам, пришедшим в офис утром в интервале с 7:50 до 8:15, в отчётах может быть записано время прихода 8:00.

- Выберите пункт **Keep only the first entry (first IN) and the last exit (last OUT)** (рассматривать только первый приход и последний уход). Будет показываться время с момента первого входа и последенего выхода.

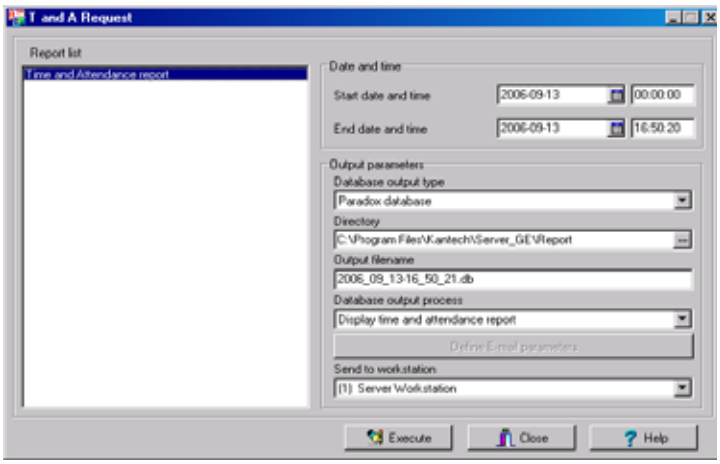
Запрос отчёта по учёту рабочего времени

С помощью этой функции операторы могут запрашивать предварительно настроенные отчёты (Time and attendance reports), созданные при помощи меню Time and Attendance Report Definition (Назначение отчёта по учёту рабочего времени). Эта функция позволяет запрашивать отчёт вручную, игнорируя автоматические настройки.

ПРИМЕЧАНИЕ: *Если в отчёте указаны автоматические настройки, то они будут игнорированы.*

Как вручную запросить отчёт по учёту рабочего времени

1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **T & A Report Request** (Запрос отчёта по учёту рабочего времени). На экране появится окно **T and A Request.**



2 На панели слева (**Report list**) (список отчетов) указать, отчет по учету рабочего времени, который вы хотите выполнить.

3 В поле **Date and time** указать временной интервал для сбора событий, а также настроить другие параметры в разделе **Output parameters** (Выходные параметры).

4 Чтобы запустить процесс, нажать кнопку **Execute** (Выполнить).

ПРИМЕЧАНИЕ: *Отчёт по учёту рабочего времени будет автоматически сохранён в папку для результатов в приложении, указанном в поле Send to workstation (Отправить на рабочую станцию).*

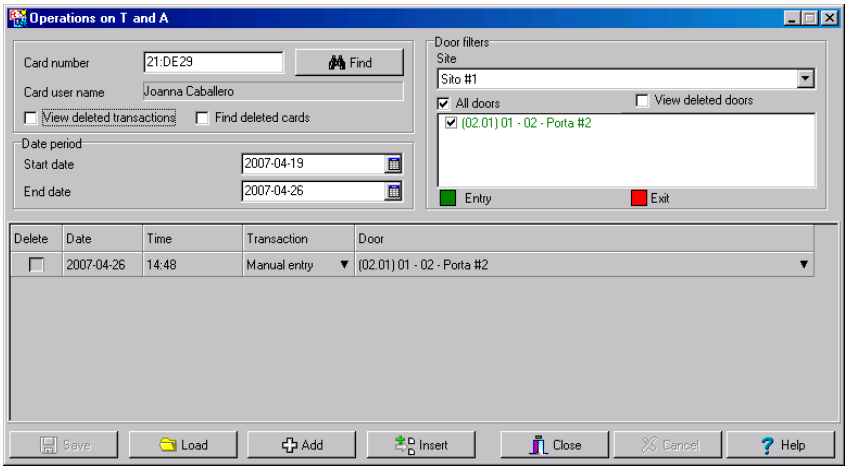
ПРИМЕЧАНИЕ: *При работе с файлами типа Paradox система выводит на экран окно предварительного просмотра отчёта. В других выходных форматах необходимо вручную запрашивать отчёт, иначе он не будет выведен ни на экран, ни на принтер. Чтобы просмотреть все сгенерированные отчёты, следует воспользоваться кнопкой View Report (Посмотреть отчёт) на панели инструментов Report (Отчёты). Смотрите в Главе 13 Назначение выходного формата отчёта' на странице 448 для более подробной информации .*

Операции с базой данных по учёту рабочего времени

Меню Operation on T and A позволяет вручную добавлять, вставлять и удалять транзакции в базе данных по учёту рабочего времени. Эта функция пригодится, например, в организациях, где учёт рабочего времени используется при начислении заработной платы.

Добавление транзакции в базу данных по учёту рабочего времени

1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **Operation on T & A** (Операции с базой данных по учёту рабочего времени).



2 Указать в поле **Card number** номер карты, для которой необходимо внести изменения в базу данных по учёту рабочего времени, и нажать кнопку **Load** (Загрузить). Если номер карты неизвестен, можно воспользоваться кнопкой **Find** (Поиск).

ПРИМЕЧАНИЕ: *Загрузка данных выполняется только после заполнения поля Card number (Номер карты) – это поле должно быть заполнено обязательно.*

3 Выбрать опцию **View deleted transactions** (Показать удалённые транзакции), чтобы увидеть транзакции, которые были удалены ранее. Удалённые транзакции будут выделены меткой “X” в колонке **Delete** (Удаление).

4 Чтобы выполнить поиск среди удалённых карт, следует отметить опцию **Find deleted cards** (Найти удалённые карты). Эта опция не применяется к записям, которые были добавлены вручную.

5 В поле **Start date** (Начальная дата) указать дату, с которой система должна начать отбор событий. Можно воспользоваться кнопкой **Calender**, чтобы открыть календарь и указать в нём дату. Учитываться будут только те события, которые случились в этот день или позже.

ПРИМЕЧАНИЕ: *Для загрузки данных поле Start date должно быть заполнено обязательно.*

6 В поле **End date** (Конечная дата) указать дату и время для окончания сбора событий. Учитываться будут только те события, которые случились в этот день или раньше. Если конечная дата не будет указана, система будет учитывать все данные вплоть до текущей даты.

7 В выпадающем списке **Site (Луч)** выделить сайт/луч, двери которого используются при учёте рабочего времени.

ПРИМЕЧАНИЕ: *Шлюз должен быть указан обязательно.*

8 При необходимости может быть выделена опция **All Doors** (Все двери), и тогда будут учитываться все двери, отображённые на экране в этом поле. Или необходимо указать определённые двери. На экране будут отображаться все события, связанные с учётом рабочего времени, зарегистрированные на определённых дверях.

9 Отметить флажком опцию View deleted doors (Показывать удалённые двери), чтобы показать на экране те двери, которые больше не учитываются в системе учёта рабочего времени (но учитывались раньше).

ПРИМЕЧАНИЕ: *Для загрузки данных поле Doors должно быть заполнено обязательно.*

10 Ввести необходимые данные в таблицу транзакций. В таблице транзакций отображаются транзакции, выполненные для указанного владельца карты:

- В колонке **Delete** (Удаление) отображаются удалённые транзакции, если флажком отмечена опция View deleted transactions (Показать удалённые транзакции). Они отмечены знаком "X".
- В колонке **Date** (Дата) показаны даты транзакций. В случае ручного ввода в базу данных новой транзакции в этом поле следует указать её дату.
- В колонке **Time** (Время) отображается время, в которое владелец карты вошёл или вышел из контролируемой зоны. В случае ручного ввода в базу данных новой транзакции в этом поле следует указать время (входа или выхода).
- В колонке **Transaction** (Транзакция) показан тип транзакции. Каждой транзакции входа должна обязательно соответствовать одна транзакция выхода.
  - **Entry** (Вход) – указывает, что это транзакция входа, созданная владельцем карты посредством предъявления своей карты считывателю на входе в контролируемую зону.
  - **Exit** (Выход) – указывает, что это транзакция выхода, созданная владельцем карты посредством предъявления своей карты считывателю на выходе из контролируемой зоны
  - **Manual entry** (Вход, созданный вручную) – указывает, что это транзакция входа, которая была вручную добавлена в базу данных системы. При добавлении транзакции оператор должен указать какая это транзакция – входа или выхода. Каждой транзакции входа должна обязательно соответствовать одна транзакция выхода.
  - **Manual exit** (Выход, созданный вручную) – указывает, что это транзакция выхода, которая была вручную добавлена в базу данных системы. При добавлении транзакции оператор должен указать какая это транзакция – входа или выхода. Каждой транзакции входа должна обязательно соответствовать одна транзакция выхода.
- В колонке **Door** (Двери) отображаются двери, через которые прошёл данный пользователь. При добавлении транзакции вручную оператор должен указать дверь в соответствии с типом транзакции (входа или выхода).

ПРИМЕЧАНИЕ: *При добавлении транзакции входа в списке дверей отображаются только двери, описанные в системе как “Entry doors” (Входные двери). При добавлении транзакции выхода в списке дверей отображаются только двери, описанные в системе как “Exit doors” (Выходные двери).*

11 Нажать кнопку **Load** (Загрузить), чтобы для данного владельца карты загрузить транзакции с сервера. Для этого необходимо указать в поле Card number номер карты, указать сайт/Шлюз в поле Site/Gateway, выбрать двери и нажать кнопку **Load** (Загрузить). После загрузки транзакций эта кнопка становится недоступной.

12 Для того чтобы добавить транзакцию к существующему списку транзакций, следует нажать кнопку **Add** (Добавить). Новая транзакция будет добавлена в конец списка.

13 Чтобы вставить транзакцию в список между другими транзакциями или вместо любой транзакции, следует воспользоваться кнопкой **Insert** (Вставить).

14 Нажать **Cancel** (Отмена), чтобы отменить любое добавление или изменение, выполненное ПЕРЕД сохранением.

ПРИМЕЧАНИЕ: *Если оператор удаляет транзакцию, которая была добавлена вручную, то она удаляется из списка окончательно, в отличие от транзакций, которые были сгенерированы контроллерами. Последние при удалении помечаются знаком "X" в колонке Delete (Удаление).*

Muster Отчеты - Отчеты о сборе людей

Muster отчеты в EntraPass позволяют вам получать отчеты, которые используются в аварийных ситуациях. В тревожных ситуациях необходимо знать где в данный момент находится персонал. Когда происходит тревога по входу (аварийная ситуация, например), muster отчет может автоматически отображаться, где указано присутствие людей в преднастроенной области. Muster отчет может быть направлен на e-mail и на принтеры (до 32 принтеров). EntraPass будет в первую очередь направлять отчеты на принтер, затем будет происходить отправка на e-mail. Muster отчеты поступают в формате PARADOX при печати и будут направляться на e-mail в формате CSV.

ПРИМЕЧАНИЕ: *если отчет не может быть напечатан или не может быть отправлен на e-mail, тогда сообщение об ошибке будет появляться.*

Графики на рабочих столах будут отображать состояние групп областей. Иконки будут отображать сосотояние области (активная или пустая).

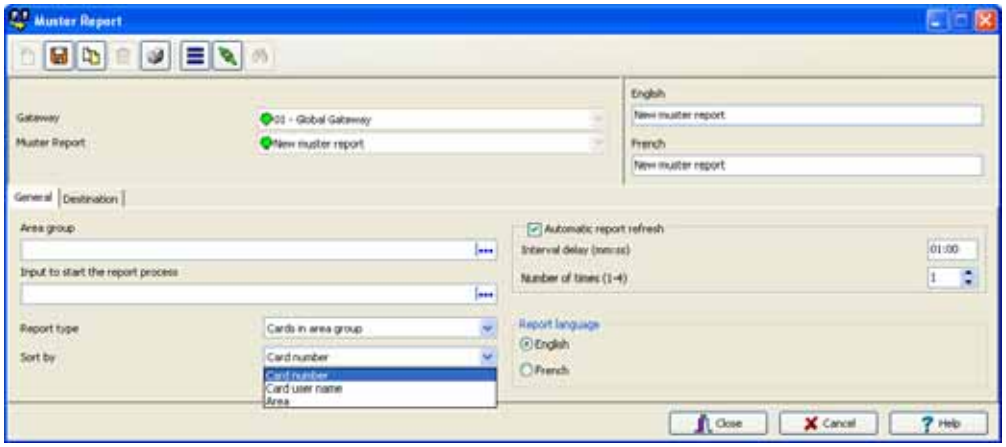
Определеннные условия должны быть назначены для запуска muster отчета:

- Должна быть предназначена muster область (область сбора персонала). Весь персонал должен собраться в определенных точках сбора когда происходит аварийные ситуации.
- Группы областей должны быть настроены для содержания областей, которые должны быть контроллированы в течении тревожной ситуации. Если вам только необход èмо контроллировать одну область, тогда вам необходимо создать группу областей, которая будет содержать одну область. *Смотрите в Главе 9 Создание группы областей' на странице 354 для более подробной информации .*
- Двери, с назначенным anti-passback, которые являются частью muster группы областей, должны иметь установку "**Области после**" (Area before) как "Неизвестная область. Когда происходит тревожная ситуация, работники прикладываются к определенному считывателю, который назначается как вход в "Unknown area". Это обозначает точку сбора при тревожной ситуации. Люди прикладываются к считывателю определенному, и тем самым оказываются в неизвестной области. Это говорит о том, что люди собрались в данной области. *Смотрите в Главе 4 Назначение дверей под Шлюзом Global/KT-NCC' на странице 150 для более подробной информации по настройки двери на anti-passback.*
- Определенный вход/input должен быть настроен в качестве запуска muster отчета. (Отчет о сборе людей). *Смотрите в Главе 4 Конфигурация входов (раздел Input)' на странице 160 для более подробной информации по настройке входа (input).*
- Графические иконки (Grafics) могут быть расположены на рабочем столе. Даные иконки могут отображать группу областей, которая контролируется при аварийной ситуации.

Muster отчеты для экстренных ситуаций

До настройки данного отчета, вы должны быть уверены что группа областей уже настроена. Вы должны выбрать вход/Input (новый или уже назначенный), который будет запускать Muster отчет автоматически. Каждый Muster отчет настроен для работы с одной группой областей от одного input/входа.

1 Под вкладкой **Report** (Отчеты), нажать иконку **Muster report** (Muster отчет).



2 Нажмите кнопку **View hierarchy** (Видеть иерархию) чтобы отобразить все шлюзы, назначенный в системе; затем из выпадающего списка **Gateway** (Шлюз), выберите шлюз в котором вы хотите назачить muster отчет.

3 Из выпадающего списка **Muster Report** (Muster отчет), выберите существующий отчет для изменения или нажмите кнопку **New** для создания нового отчета. Затем введите имя отчета в разделе language section.

4 Выберите **Area group** (Группа областей), которую вы хотите назначить для отчета.

5 Выберите **Input to start the report process** (тревожный вход для запуска muster отчета). При тревоге по данному входу будет автоматически запускаться muster отчет.

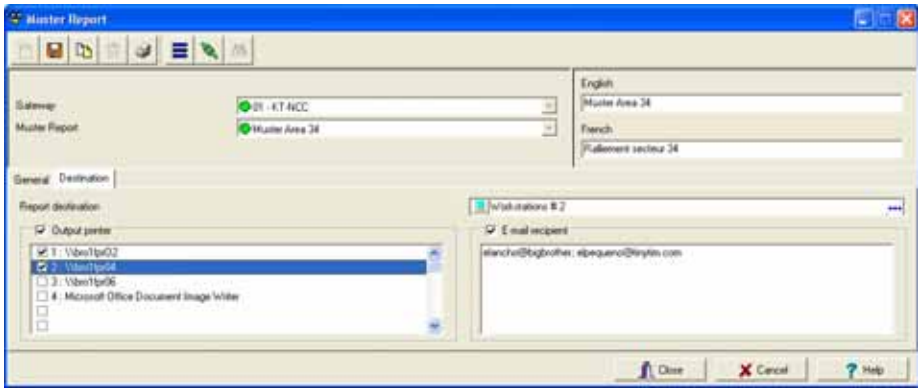
6 Укажите для воспроизведения **Report type** (Тип отчета):
- **Cards in area group** (Карты в группе): Вам будет предоставлен список карт, которые в настоящий момент находяться в данной группе областей.
- **Supervisor cards in area group** (Карты ревизоров/руководителей в группе областей): вам будет предоставлен только список карт ревизоров в настроенной группе областей.
- **Invalid cards in area group** (Недействительные карты в области): вам будет предоставлен список недействительных карт в этой группе областей (исключение: карты, которые в ручную перенесены в данную область без необходимости иметь уровень доступа для входа в данную область).

7 Выберите приоритет по сортировке **Sort by**.

8 Выделите пункт **Automatic report refresh** (Автоматическое обновление отчета) если вы хотите, чтобы EntraPass генерировала более чем один отчет автоматически. Отчеты будут содержать информацию о дате. Имеется в виду, что при тревожной ситуации может быть подготовлено несколько отчетов с заданным интервалом времени. Это поможет вам наглядно видеть процесс эвакуации людей из данной области.
- Укажите интервал задержки (м,сек)**(Interval delay (mm:ss))** между изготовлением каждого отчета. Время задержки можно установить 01:00 до 59:59 минут.
- Укажите **Number of times (1-4)** (Количество отчетов 1-4) если вы хотите делать несколько отчетов (максимум 5), включая изготовление первого отчета, который будет подготовлен когда произошла тревога по входу.

9 Если система EntraPass работает в двух языках, укажите **Report languages** (языки отчета) для запуска muster отчета.

10 Двигайтесь на вклдаку **Destination** (Назначение/пункт назначения).



11 Выберите приложение **Report destination** (пункт назначения отчета). Это приложение будет управлять генерацией отчета на определенные приложения (сервер, APM, итд.).

ПРИМЕЧАНИЕ: *если данное приложение запущено как служба, вы должны указать параметры авторизации* ***(Login parameters)*** *для этого приложения или принтер не будет воспроизводить muster отчет. Смотрите в Главе 4 Конфигурация приложений EntraPass' на странице 64 для более подробной информации по настройке параметров авторизации на приложениях EntraPass. Смотрите в Главе 14 Информация по авторизации приложения в качестве службы (Service Login Information)' на странице 484 для более подробной информации по настройке параметров авторизации на сервере EntraPass.*

- Если вы воспроизводите muster отчет на принтеры, выделите пункт **Output printer** (выходной принтер) и выберите необходимый принтер. Вы можете указать до 32 принтеров. Muster отчет генерируется в формате PARADOX.
- Если вы планируете направлять отчет по e-mail, то отметьте пункт **Email recipient** (e-mail получатели) и укажите e-mail адреса получателей, используя точку с запятой (;). Muster отчет генерируется в формате PARADOX.

12 Нажмите на кнопку Save (Сохранить)

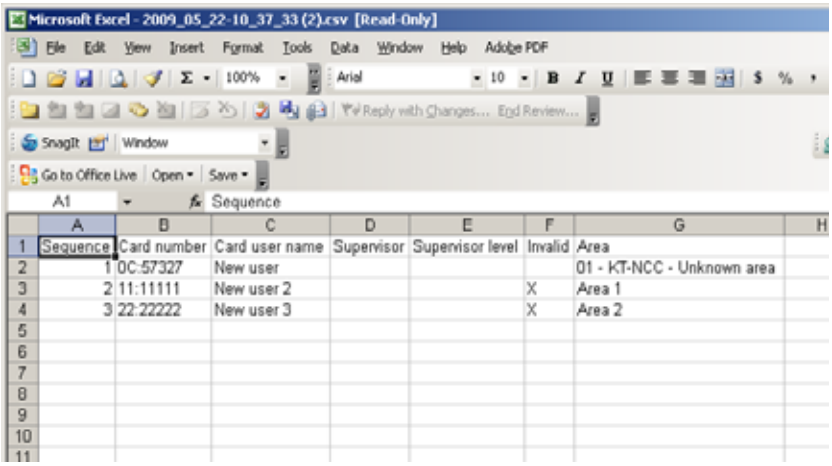
Использование Muster отчета для управлением парковкой

Создание отчетов по управлению парковкой это подобно созданию отчета в аварийных ситуациях. Вы должны выбрать группу областей и тревожный вход, который будет запускать автоматическое действие (посылать сообщение на табло, что область для парковки заполнена, запирать ворота до тех пор, пока кто-либо не покинет область, отправлять сообщение на АРМ охраны о том, что область заполнена). Тем не менее, вам требуется произвести некоторые дополнительные настройки, когда вы настраивайте систему для управления парковками. На вкладкене Area (область), вы должны быть уверены, что у вас выбрано активация реле, когда область заполнена **Disable access when area is full** (Закрыть область когда область заполнена). Это необходимо для ограничения доступа в данную область. Это может включать в себя блокировку дверей или шлагбаумов чтобы ограничить доступ в эту область. Может быть направлено сообщение на табло для извещения о том, что область заполнена. Это зависит от тревожного входа, который вы будете настраивать. *Смотрите в Главе 5 Назначение областей (Только Global/KT-NCC/NCC 8000 Шлюзы)' на странице 187 для более подробной информации по настройке областей.*

Генерация Muster отчета

Первый отчет будет воспроизведен сразу после того, как произойдет тревога по входу (например, тревожная система).

- Сообщение будет отображено на дисплее, чтобы оповестить о том, что отчет в форме PARADOX напечатан.
- если назначены e-mail получатели, будет произведена автоматическая рассылка отчетов после вывода их на принтер. В e-mail будет вложен отчет в формате CSV.



Sequence	Card number	Card user name	Supervisor	Supervisor level	Invalid	Area
1	0C:57327	New user				01 - KT-NCC - Unknown area
2	11:11111	New user 2			X	Area 1
3	22:22222	New user 3			X	Area 2

- Muster отчет содержит имя карты и область, где карты в настоящее время расположены внутри контроллируемой области.
- Muster отчет также отображает ревизоров, их уровень и недействительные карты.

ПРИМЕЧАНИЕ: *если система не сможет вывести на печать отчет или отправить на e-mail, то будет произведено оповещение об этом. Система будет продолжать снова отправить отчет на e-mail и на печать.*

- Когда параметр **Automatic refresh report** (автоматическое обновление отчета) включен, то система будет ждать в течении указанного времени. После заданной задержки, система произведет печать этого же отчета.

Отчеты Roll Call/ Отчеты о движении людей в течении определенного времени

Отчет Roll call используются в качестве фотографии о том, кто приложил карту к считывателю или группе счиывтелей в течении определенного периода. Внутри отчета roll call, одна или множество дверей в EntraPass могут быть настроены как входные группы для определенной зоны или для других критериев, которые будут позже рассмотрены в этом документе. Базируясь на последенем местоположении картодержателя, операторы будут получать отчеты о том, кто вошел в данную зону.

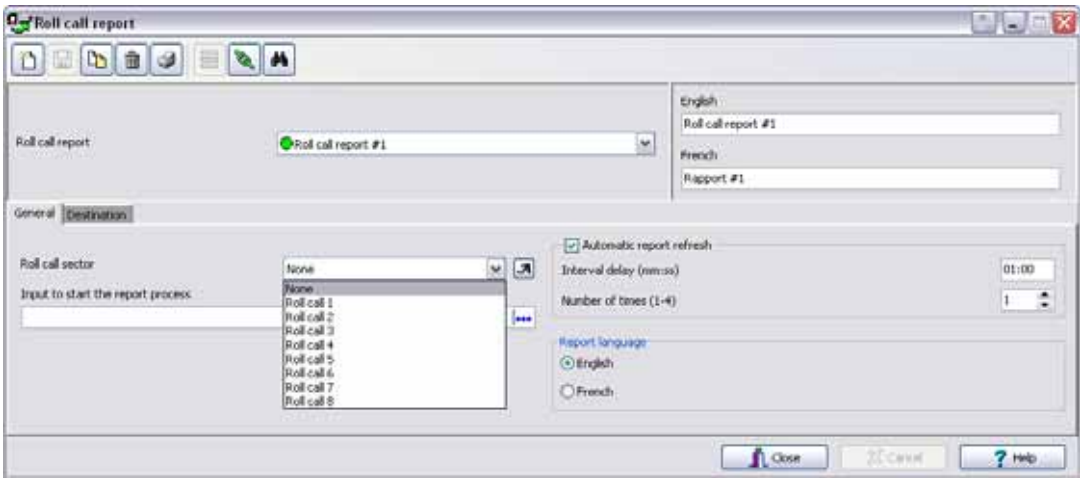
Отчеты roll call поддерживаются Сервером EntraPass. Чтобы данная операция происходила верно, сервер и шлюз должны быть запущены. Это позволяет производить верное считывание местоположение картодержателя и производить верную реакцию на тревогу по входу. Сервер EntraPass Global, Corporate и APM могут быть запущены в качестве службы windows. Отчеты Roll call могут быть запущены в обоих вариантах работы шлюза и сервера: в качестве сервиса или приложения.

Функциональность

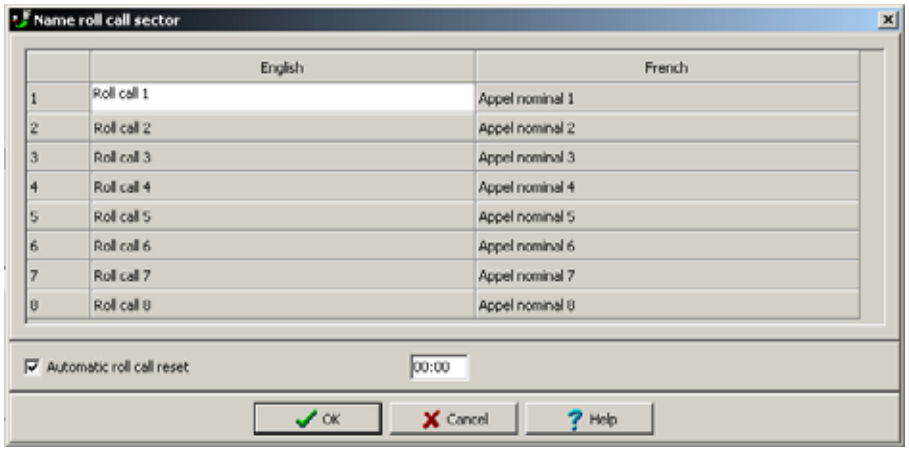
- Максимум 8 отчетов roll call могут быть назначены в EntraPass.
- Двери должны быть назначены в качестве точек отчета (1-8), чтобы получить отчет roll call. (*Смотрите в Главе 4 Конфигурация дверей' на странице 143 для более подробной информации*).
- В запущенном состоянии, отчет Roll call будет отображать список всех сотрудников, которые приложили свои карты к определенному считывателю. В отчете будут показаны только те сотрудники, кто вошел в данную зону с момента сброса данной зоны или с момента сброса времени отсчета.
- Чтобы создать функциональность “in-out” пришел/ушел, оператор должен быть уверен, что выходные двери имеют другой номер для roll call отчета. Любая другая дверь, которая не назначена в качестве номера roll call для выхода, не будет оказывать влияние на указание местоположение данного сотрудника в отчете rall call.
- Настраиваемый сброс для отчета rall call доступен. Значение по умолачанию 12:00PM (полночь) каждого дня. Эта функция очищает отчет. Сброс может быть выполнен в окне rall call отчета.
- Для ручного запроса на отчет Report (Отчет) –> Roll Call Отчет или указать тревожный вход. Отчет может быть направлен на три направления: на определенный принтер, APM, или e-mail.

Генерация отчета Roll Call

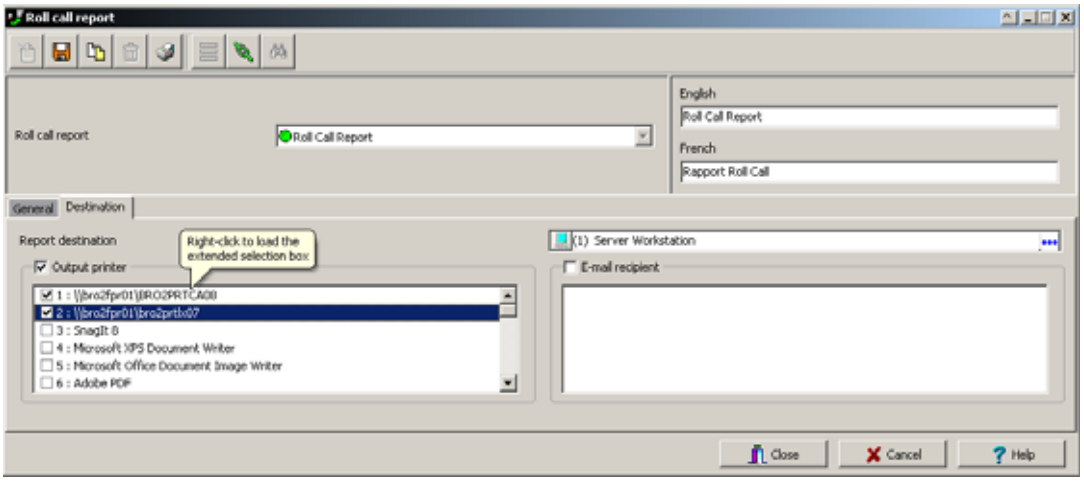
1 Под вкладкой на панели инструментов **Report** (отчет), нажмите на иконку **Roll call report** (отчет rall call):



2 Укажите номер отчета roll call. Если номер/сектор rall call отчета не отображается, нажмите кнопку, которая отображается рядом для вызова выпадающего меню:



3 Укажите пункты назначения для данного отчета



- Report Destination (Пункты назначения для данного отчета): Выберите кнопку назначения, используя кнопку многоточия.
- **Output printer** (выходной принтер): Выберите принтрер/ы из списка.
- **E-mail recipient** (получатели e-mail): Введите имена получателей данного отчета.

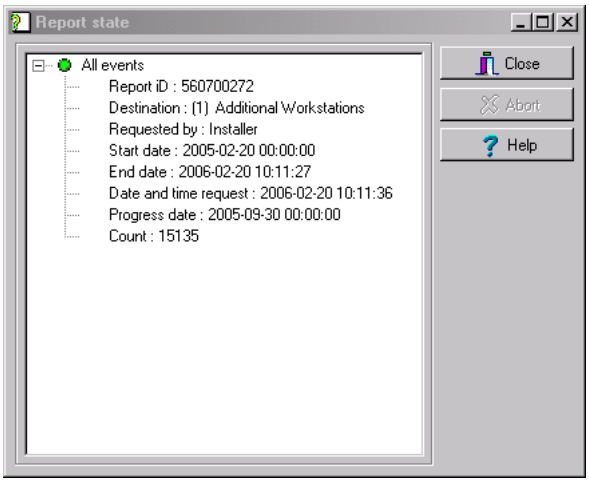
Пример отчета Roll Call

TRACKING AND MUSTER VIEW REPORT

Area Name	Card ID	Status	Card Holder	Reader
Time & Date				
On Site 15:22:07 16/03/2005	29	Valid Card, door used	Bloggs Fred	Front Door - IN
15:22:05 16/03/2005	26	Valid Card, door used	Davies David	Front Door - IN
15:22:03 16/03/2005	27	Valid Card, door used	Johnson Sam	Front Door - IN
15:22:09 16/03/2005	30	Valid Card, door used	Smith John	Front Door - IN
15:21:59 16/03/2005	28	Valid Card, door used	Wilson Jane	Front Door - IN

Состояние отчета

Используете кнопку **Report state** (состояние отчета), чтобы отобразить список состояния отчета и состояние всех запрошенных отчетов, которые все еще находятся в ожидании.



1 Для остановки ожидании/удалении отчета, выберите отчет, затем нажмите кнопку **Abort** (прервать).

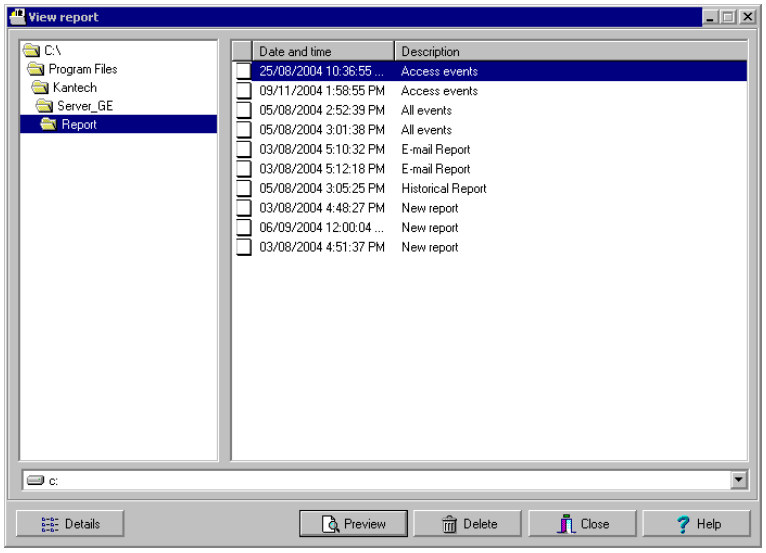
Просмотр отчётов

Функция View Report позволяет пользователям просматривать отчёты, созданные и сохранённые в системе. Операторы могут использовать эту функцию для просмотра отчётов в любом формате или чтобы настроить их перед выводом на печать.

ПРИМЕЧАНИЕ: *При создании отчёта (в формате csv, db или dbf) система автоматически создаёт файл формата rdf. Именно этот rdf-файл отображается в списке в окне View report. В случае нажатия кнопки "Preview" (Предварительный просмотр) система автоматически загружает соответствующую программу, чтобы просмотреть отчёт*

Отображение отчёта на экране

1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **View report** (Посмотреть отчёт). Система выведет на экран содержимое папки, указанной в настройках по умолчанию. Если отчёт был сохранён в другой папке, следует найти её на диске, используя кнопку со стрелкой вниз (в нижней части окна) и указать путь файла с отчётом.



2 Указать, какой отчёт необходимо отобразить на экране. Если в системе установлен принтер, то в меню будет доступной кнопка **Preview** (Предварительный просмотр). Функция Preview позволяет посмотреть отчёт на экране перед выводом его на печать.

ПРИМЕЧАНИЕ: *Чтобы предварительно просматривать отчёты и выводить их на печать на принтере, на компьютере* ***обязательно*** *должен быть установлен принтер. Чтобы настроить принтер, следует перейти в меню* ***Start*** *(Пуск) >* ***Printers*** *(Принтеры) >* ***Add Printer*** *(Добавить принтер). Более подробную информацию можно получить у системного администратора.*

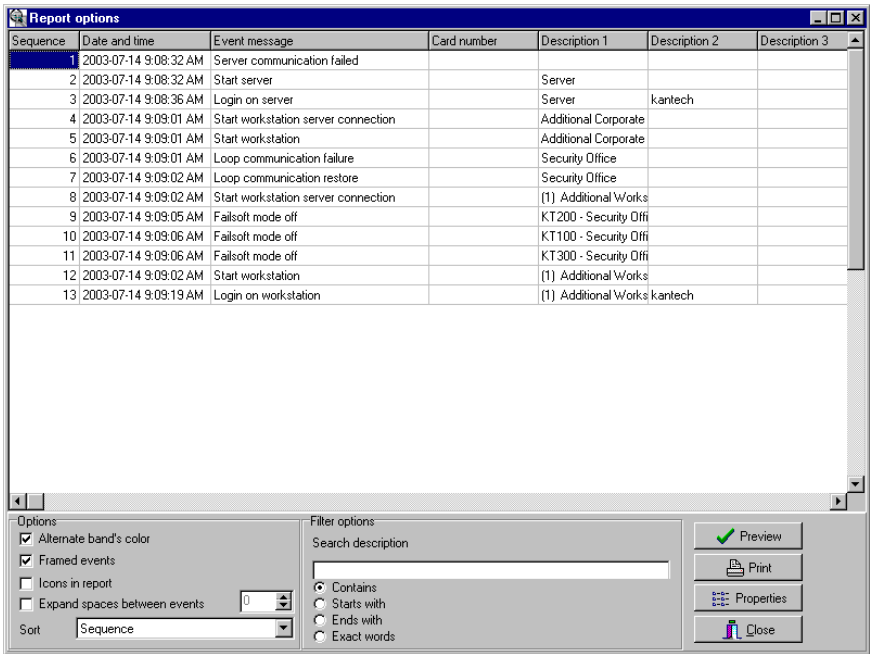
3 Чтобы увидеть информацию об отчёте, нажать кнопку **Details** (Подробные сведения). В случае нажатия кнопки **Details** на экране появляется окно Report details (Подробные сведения об отчёте), в котором отображаются данные, связанные с выделенным файлом отчёта (имя файла, заголовок, тип, дата и др.). Чтобы закрыть окно Report details, нужно снова нажать кнопку **Details** снова.

4 Нажать кнопку **Preview** (Предварительный просмотр), чтобы вывести отчёт в окно предварительного просмотра (Report preview).

Предварительный просмотр архивных отчетов

1 В окне **View** report (Просмотр отчётов) выделить на правой панели отчёт, который необходимо просмотреть. В случае выделения архивного отчёта, созданного при помощи Paradox, оператору будет предоставлена возможность индивидуально настроить его перед выводом на печать в открывшемся окне Report Options (Параметры отчёта).

ПРИМЕЧАНИЕ: *Если для отчёта указан тип CSV, то отчёт будет генерироваться в окне WordPad в текстовом формате.*



2 Указать настройки фильтров: ввести текстовую строку в поле **Search description** (Поиск описания). В отчёт будут включены только те записи, которые содержат указанную текстовую строку. Для более точного отбора можно выбрать следующие опции:
- **Contains** (Содержит). В отчёт будут включены все события, которые содержат указанный текст.
- **Starts with** (Начинается с...). В отчёт будут включены все события, которые начинаются с указанных текстовых символов.
- **Ends with** (Оканчивается на...). В отчёт будут включены все события, которые заканчиваются указанным текстом.
- **Exact words** (Точное совпадение). В отчёт будут включены все события, содержащие строго указанный текст.

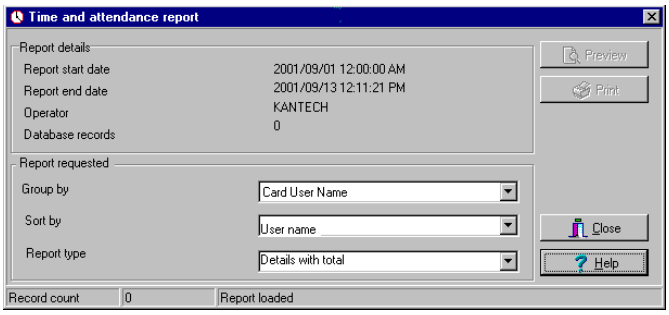
3 Нажать **Preview** (Предварительный просмотр), выберите принтер и нажмите **OK**. Система выведет на экран результаты отчёта. Из этого окна вы можете:
- Поиск по тексту внутри отчета
- Печатать отчет
- Сохранить отчет в различных форматах PDF, RTF, HTML и TXT
- Загрузить отчет (в формате .QRP)

4 Нажать **Properties** (Свойства), чтобы открыть окно Reports details (Подробные сведения об отчёте).
- **Report filename** (Имя файла отчёта) – содержит полный путь сохранения отчёта и имя файла.
- **Report title** (Заголовок отчёта) – отображает название отчёта.
- **Start date** (Начальная дата) – отчёты охватывают события в указанных временных рамках. Здесь указывается начальная дата выбранного временного интервала.
- **End date** (Конечная дата) – отчёты охватывают события в указанных временных рамках. Здесь указывается конечная дата и время выбранного интервала.
- **Requested** (Запрос сделан...) – отображает дату и время запроса отчета.
- **Delivered** (Выполнен...) – отображает дату и время выполнения отчета и печати
- **Requested by** (Кем запрошен) – содержит имя оператора, выполнившего запрос отчёта.
- **Count** (Счётчик) – отображает число транзакций (строк), включённых в отчёт.
- **Output process** (Способ вывода) – отображает список шаблонов, используемых для этого отчёта.

Предварительный просмотр отчётов по учёту рабочего времени

1 В окне **View report** (Посмотреть отчёт) указать, какой отчёт необходимо отобразить на экране. Если отчёта был назначен как «Display Time and Attendance Report» (Показывать на экран отчёт

по учёту рабочего времени) и для базы данных указан тип Paradox, то открывается следующее окно:



2 Указать параметры отображения на экране:

- **Group by** (Группировать по...) – служит для облегчения работы с отчётом. Данные отчёта могут быть сгруппированы по именам владельцев (Card user name) или по номерам карт (Card number).
- **Sort by** (Сортировать по...) – оператор может указать способ сортировки по именам владельцев (Card user name) или по номерам карт (Card number).
- **Report type** (Тип отчёта) – служит для облегчения работы с отчётом. В отчёт могут быть включены подробные сведения с общей суммой или без.

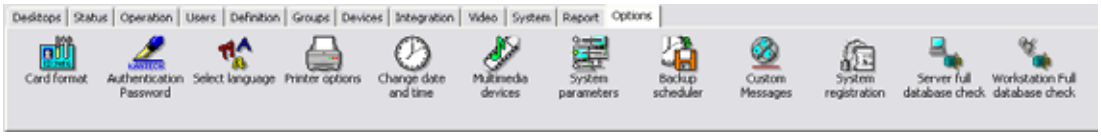
3 Нажать **Preview** (Предварительный просмотр), чтобы вывести на экран результаты отчёта. В этом окне можно сохранить отчёт (в формате .QRP) или распечатать его на принтере.

Глава 14 • Опции системы EntraPass

Панель инструментов Опции (Options)

Панель инструментов **Options** (Опции) даёт возможность пользователям изменять некоторые системные параметры. К таким параметрам можно отнести формат карт, аутентификационный пароль, дату и время или параметры сервера. Перечисленные ниже опции доступны в обоих окнах: в окне рабочей станции (Workstation) и в окне сервера (Server):

Панель Options (Опции) на АРМ



Панель Options (Опции) на сервере

- Выбор формата карты по умолчанию
- Изменение аутентификационного пароля
- Выбор языка
- Изменить тип кодонаборника

ПРИМЕЧАНИЕ: *Тип кодонаборника только появляется когда вы используете NCC DOS. Не поддерживается EntraPass v4.0x.*

- Изменение даты и времени системы
- Изменение системных параметров
- Настройка специальных сообщений
- Расписание автоматического резервного копирования tomatic

Ниже перечислим утилиты, которые доступны в меню **Option** (Опции) только в приложении Рабочая станция (EntraPass Workstation):

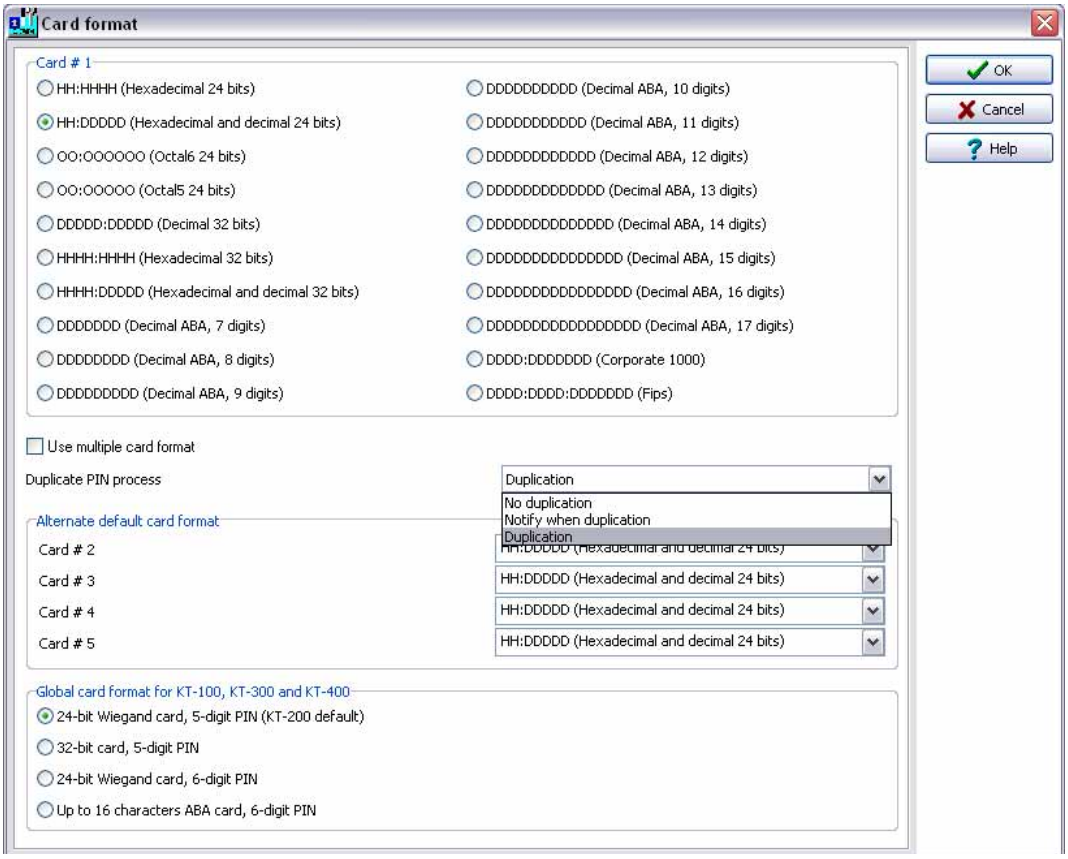
- Настройка опций принтера (принтеры для лог/журналов и электронных пропусков)
- Настройка конфигурации мультимедийных устройств (параметры тревожной сигнализации, оцифровка фотографий и подписей)
- Настройка специальных сообщений
- Регистрация системы
- Полная проверка базы данных сервера
- Полная проверка базы данных рабочей станции

Выбор формата карт по умолчанию

Программное обеспечение EntraPass поддерживает различные типы считывателей электронных карт. В зависимости от типа считывателя могут использоваться различные форматы представления карт. Меню Card format (Формат карты) даёт возможность выбрать формат карты по умолчанию и автоматически использовать эти настройки при создании новой карты.

Назначение формата представления идентификационных карт

1 В окне **Options** (Опции) нажать иконку **Card format** (Формат карт).



ПРИМЕЧАНИЕ: *Поля Card #2, Card #3, Card #4 и Card # 5 становятся активными в случае использования опции Advanced User (Продвинутый пользователь).*

2 Указать формат карты для карты №1 (**Card #1**).

- **Decimal** (Десятичный) – использует десятичную запись числа.
- **Octal** (Восьмеричный) – каждая цифра восьмеричного числа может быть представлена тремя разрядами двоичном представлении. Число "8" является основанием восьмеричной системы счисления, а любое число записывается с помощью восьми цифр (0, 1, 2, 3, 4, 5, 6 и 7). Программы часто представляют данные в восьмеричном формате, поскольку он относительно прост для понимания и легко переводится в двоичную систему счисления, используемую при программировании.
- **Hexadecimal** (Шестнадцатеричный) – каждая цифра шестнадцатеричного числа занимает четыре места в двоичном представлении. В шестнадцатеричной системе счисления основанием является число 16, а для записи чисел используются 16 цифр: традиционные цифры от 0 до 9 и буквы от A до F. Например, десятичное число "15" в шестнадцатеричной системе счисления записывается цифрой "F". Каждый шестнадцатеричный символ может быть представлен единственным сочетанием четырех бит, то есть каждый байт (8 бит) можно выразить в виде двух шестнадцатеричных цифр. Такое представление чисел удобнее для человеческого восприятия, чем двоичное счисление.
- **FIPS (**Federal Information Processing Standard): Этот формат карт использует более чем 32 бита данных.

3 Отметить флажком опцию **Use multiple card format** (Использовать несколько форматов карт), если в системе установлены считыватели карт разного типа, и при создании новых карт необходимо обеспечить возможность выбора разных считывателей, помимо считывателя, установленного по умолчанию.

4 В выпадающем списке **Duplicate PIN process** (Дублировать идентификационный PIN код) выбрать нужную опцию. Данная функция может использоваться, например, при загрузке карт партиями. Оператор может принять решение разрешить дублирование идентификационного кода. Позднее, если потребуется, дублированные коды можно изменить, чтобы избежать путаницы.

- **No duplication** (Без дублирования) – при попытке повторно ввести уже существующий код на рабочей станции выдаётся предупреждение, неправильно введённое значение сбрасывается, и система ожидает правильный код. Дублироваться, независимо от настроек, может только код 00000.
- **Notify when duplication** (Уведомление о дубликате) – сервер уведомляет оператора о существовании дублера введённого кода. Если введённый идентификационный код уже существует, на экране появляется окошко с предупреждением. Кнопка **Details** (Подробные сведения) позволяет посмотреть список владельцев карт, которым уже был назначен данный код.
- **Duplication** (Дублирование) – проверка существования дублей не выполняется, все коды будут приняты, независимо от наличия дублей.

5 Когда была выбрана опция Enhanced User Management (Расширенное управление пользователя), выберите формат карты по молчанию для **Card #2**. то п.5 следует повторить для карты №3 (**Card #3**), карты №4 (**Card #4**) и карты №5 (**Card #5**).

6 Под заголовком **Global card format for KT-100**, **KT-300 and KT-400** (Единый формат карт для контроллеров KT-100, KT-300 и KT-400) находятся опции для выбора формата в соответствии с настройками, указанными в верхней части окна.

- **24-bit Wiegand card, 5-digit PIN (KT-200 default)** (24-битная карта Wiegand, 5-значный код - заводские настройки KT-200) – до 24-битов для контроллеров типа KT-100, KT-200, KT-300 и KT-400.
- **32-bit card, 5-digit PIN** (32-битная карта, 5-значный код) – до 32 битов для контроллеров типа KT-100, KT-300 и KT-400.
- **24-bit card, 6-digit PIN** (24-битная карта, 6-значный код) – до 24 битов для контроллеров типа KT-100, KT-300 и KT-400.
- **Up to 16 characters ABA card, 6-digit PIN** (карта ABA, до 16 символов, 6-значный код) – для контроллеров типа KT-100, KT-300 и KT-400

ПРИМЕЧАНИЕ: *Контроллеры KT-100, KT-300 и KT-400 выполняют жёсткую перезагрузку при изменении формата карты. Использование карт разного формата не рекомендуется, так как это может привести к потере данных карты.*

Смена аутентификационного пароля

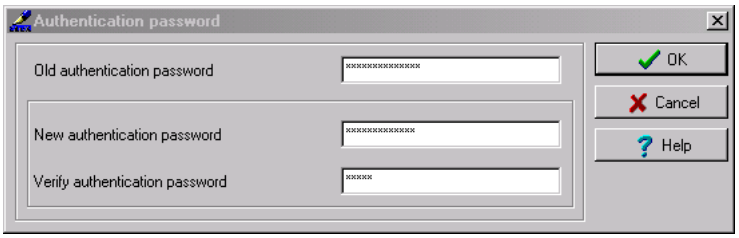
Аутентификационный пароль используется для аутентификации рабочих станций (EntraPass Workstations) на сервере EntraPass Server. Окно для ввода пароля (Authentication password) автоматически отображается на экране, пока система ещё не зарегистрирована.

Внимание:
Помните, что нет никакого пути для сброса аунтификационного пароля, если вы его забыли.

ПРИМЕЧАНИЕ: *Если никакой особый аутентификационный пароль не установлен, то для аутентификации рабочей станции пользователи должны вводить главный пароль по умолчанию. Пароль по умолчанию – kantech (нижний регистр). (Пароли чувствительны к регистру.)*

Порядок изменения аутентификационного пароля

1. В главном окне **Options** (Опции) нажать на иконку **Authentication password** (Аутентификационный пароль).



2. В поле **Old authentication password** (Старый аутентификационный пароль) указать текущий пароль (пароль чувствителен к регистру!). Пароль по умолчанию – kantech (нижний регистр).
3. В поле **New authentication password** (Новый аутентификационный пароль) указать новое значение пароля (пароль чувствителен к регистру!).
4. Повторить ввод нового пароля в поле **Verify authentication password** (Подтверждение ввода пароля). Это поле необходимо заполнить для проверки правильности ввода нового пароля (пароль чувствителен к регистру!).
5. Нажать **OK** для выхода. Если на экране появилось сообщение об ошибке, следует убедиться, что данные в поле **New authentication password** и в поле **Verify authentication password** полностью идентичны (с учётом регистра).

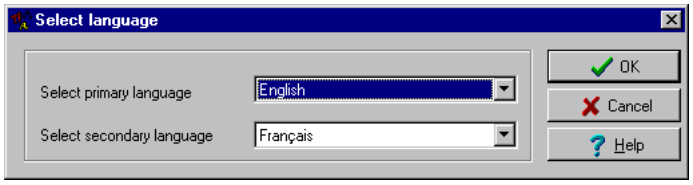
ПРИМЕЧАНИЕ: *Аутентификационный пароль отличается от пароля на доступ оператора. Аутентификационный пароль используется для аутентификации рабочих станций на сервере, а пароль оператора служит для открытия рабочей сессии.*

Выбор языка интерфейса системы

В системе EntraPass предусмотрен выбор языка интерфейса по желанию пользователя. Основные используемые языки: English (английский), French (французский), Spanish (испанский), German (немецкий) и Italian (итальянский). Утилита Vocabulary Editor (Редактор языков) позволяет добавлять другие языки с индивидуальными настройками пользователей.

Выбор языков для работы с системой

1 В главном окне системы EntraPass выбрать панель инструментов **Options** (Опции) и нажать иконку **Select language** (Выбор языков).



ПРИМЕЧАНИЕ: *В случае изменения основного языка (Primary language) работа базы данных будет временно приостановлена, и изменения вступят в силу только после выхода из системы и выполнения перезапуска. Язык базы данных изменяется в соответствии со значениями ascii символов основного языка. Надбуквенные знаки и особые символы, используемые в других языках, могут оказать влияние на базу данных.*

2 В выпадающем списке **Select primary language** (Выбор основного языка) указать язык, который должен использоваться в качестве основного языка системы. В выпадающем списке **Select Secondary language** (Выбор дополнительного языка) выбрать язык, который будет использоваться как дополнительный.

3 Выйти из системы и снова зарегистрироваться.

Выбор и настройка принтеров

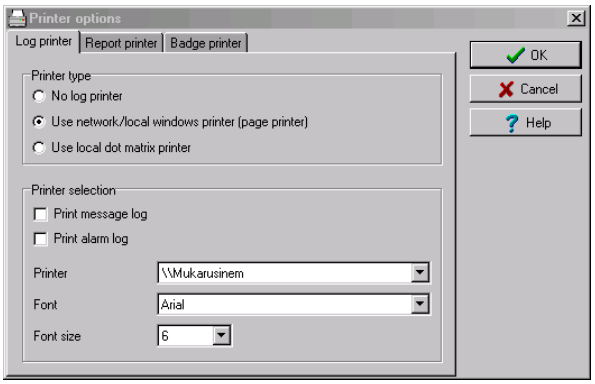
Меню **Printer options** (Опции принтера), вызываемое из меню **Options** (Опции), позволяет пользователям выбирать принтер для печати журналов событий (лог) и принтер для печати отчётов или электронных пропусков.

Выбор и настройка принтера журналов (Log Printer)

После назначения событий в меню **Events parameters** (Параметры событий) можно указать, каким образом и когда события будут напечатаны. Например, сообщения о наступлении событий можно отправлять в приложение EntraPass, на принтер или на реле, которое будет срабатывать в ответ на полученный сигнал. Оператор может установить, например, расписание для отправки сигналов тревоги на удалённый терминал в определённый момент времени.

ПРИМЕЧАНИЕ: *Для того чтобы выводить определённые события на печать в указанное время, необходимо назначить расписание работы принтера. .*

1 В окне **Printer options** выбрать закладку **Log printer** (Принтер журналов).



2 Указать параметры принтера в разделе **Printer type** (Тип принтера):
- **No log printer** (Не использовать принтер журналов) – в случае выбора этой опции события не будут выводиться на печать, даже если для них задано расписание печати.
- **Use Network/Local Windows® printer - page printer** (Использовать сетевой/локальный принтер Windows® - постраничный принтер) – все события, предназначенные для печати на принтере, будут отправляться в буфер и храниться там до тех пор, пока их количество не окажется достаточным для печати целой страницы. События будут распечатываться на сетевом/локальном принтере, а не на специальном принтере журналов.
- **Use local dot matrix printer** (Использовать локальный матричный принтер) – все события, предназначенные для печати на принтере, будут выводиться на печать по одному, одно за другим, или по одному событию на каждой странице, в зависимости от типа принтера. В поле “Printer” следует указать порт, который будет использоваться для этого принтера. Кроме того, следует указать, нужно ли печатать на этом принтере сообщения и тревоги.

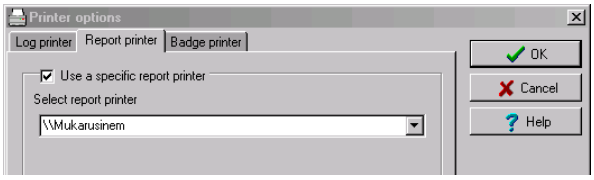
3 В разделе **Printer selection** (Выбор принтера) указать, следует ли печатать на этом принтере сообщения или тревоги.
- **Print messages log** (Печатать журнал сообщений) – в случае выбора этой опции будут распечатаны все события, для которых в параметрах событий (Events parameters) указано расписание вывода.
- **Print alarms log** (Печатать журнал тревог) – при выделении этой опции будут распечатаны все события, для которых в параметрах событий (Events parameters) указано тревожное расписание (и которые требуют подтверждение о получении).

4 В списке **Printer** (Принтеры) выбрать принтер, который будет служить в качестве принтера журналов (Log printer).
- Если была выделена опция **Dot matrix printer** (Матричный принтер), то в поле **Port** следует указать порт, через который принтер подсоединяется к компьютеру. Поле **Port** (Порт) появляется в случае выделения опции Dot matrix printer.
- Если используется сетевой/локальный принтер (**network/local printer**), следует указать шрифт в поле **Font** и размер шрифта в поле **Font size**. От типа и размера шрифта зависит, какое количество сообщений поместится на одной странице. Чем меньше размер шрифта, тем больше данных можно напечатать на каждой странице.

Выбор и настройка принтера отчётов (Report Printer)

Принтер отчётов предназначен для печати отчётов.

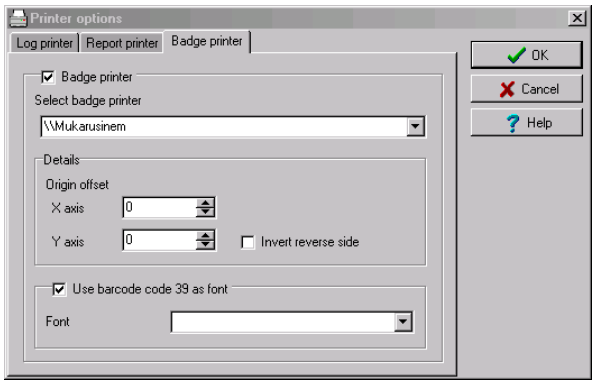
1 В окне Printer option выбрать закладку **Report printer** (Принтер отчётов).



Выбор и настройка принтера электронных пропусков (Badge Printer)

Принтер электронных пропусков предназначен для печати электронных пропусков, созданных при помощи программных средств EntraPass.

1 В окне Printer option выбрать закладку **Badge printer** (Принтер электронных пропусков).



2 Если выделить опцию **Badge printer**, то в окнах Card (Карты), Visitor (Посетители) и Daypass (Разовые пропуска) появляются функции Print badge (Печать пропусков) и Preview badge (Предварительный просмотр пропусков).

3 В выпадающем списке **Select badge printer** (Выбор принтера электронных пропусков) выбрать принтер, который будет для этого использоваться.

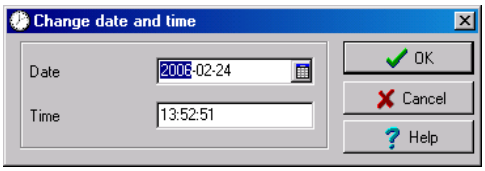
4 Если на обратной стороне пропуска требуется разместить перевёрнутую фотографию, следует выделить флажком опцию **Invert Reverse Side** (Инвертировать обратную сторону).

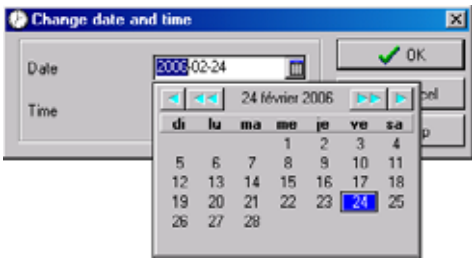
5 Если необходимо, чтобы на карте печатался номер карты в виде штрих кода, то поставить флажок в поле **Use barcode 39** (Использовать штрихкод 39) и указать шрифт в поле **Font**.

Изменение даты и времени системы

Опцию **Change System date and time** следует использовать с особой осторожностью и только при необходимости, так как эта операция может сказаться на работе логических компонентов системы контроля доступа (расписания и пр.). Если по какой-то причине всё-таки необходимо отрегулировать дату и время системы, то это лучше сделать через настройки сервера: **Options** (Опции) > **Server Parameters** (Параметры сервера) > **Time adjustment** (Настройка времени). *Смотрите в Главе 14 Опции системы EntraPass' на странице 469 для более подробной информации по настройке сетевого времени*.

1 В главном окне Option (Опции) нажать иконку **Change System date and time** (Изменить дату и время системы).





2 В поле **Date** (Дата) указать дату или выбрать её в календаре. Компоненты, соединённые с этим приложением, также получат уведомление об изменении даты.

3 Указать время в поле **Time** (Время). Компоненты, соединённые с этим приложением, также получат уведомление об изменении времени.

4 Нажать **OK** для выхода.

ПРИМЕЧАНИЕ: *Если требуется, чтобы система автоматически изменяла время при необходимости, рекомендуется воспользоваться закладкой Time adjustment (Настройка времени) в меню Server Parameters definition (Назначение параметров сервера). For details, Смотрите в Главе 14 Опции системы EntraPass' на странице 469 для более подробной информации .*

ВАЖНЫЕ ПРИМЕЧАНИЕ: Не рекомендуется изменять время в настройках Windows®. Настоятельно рекомендуется изменять время в системе через настройки параметров сервера.

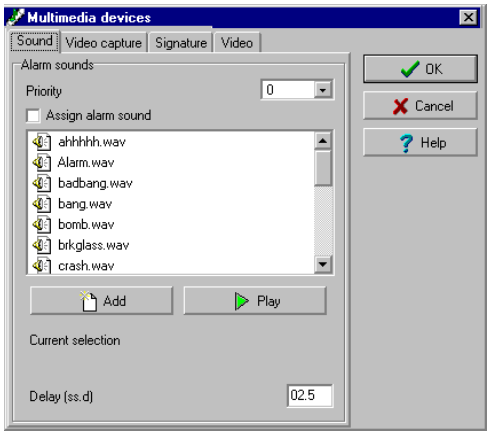
Конфигурация мультимедийных устройств

Утилита Multimedia devices (Мультимедийные устройства) позволяет установить следующие средства мультимедиа для вашей системы EntraPass:

- Звуковая тревожная сигнализация
- Устройства оцифровки/захвата изображений для бейджей
- Устройства оцифровки подписей
- Устройства видеонаблюдения

Выбор звукового сигнала тревоги

1 В главном окне Options (Опции) нажать иконку **Multimedia devices** (Мультимедийные устройства).



2 Отметить флажком опцию **Assign alarm sound** (Назначить звуковую сигнализацию), если требуется сообщать о тревоге звуковым сигналом.

3 Выбрать аудиофайл из прилагаемого списка.

4 Назначить уровень приоритета в поле **Priority** (Приоритет) для указанного звукового сигнала, который будет оповещать о тревоге.

ПРИМЕЧАНИЕ: *От уровня приоритета зависит какие тревожные сообщения будут отображаться на рабочем столе тревог (Alarm desktop). В системе EntraPass, "0" соответствует самому высокому приоритету, "9" – самому низкому. Смотрите в Главе 12 Назначение пункта параметров событий (событие/реакция)' на странице 426 для более подробной информации .*

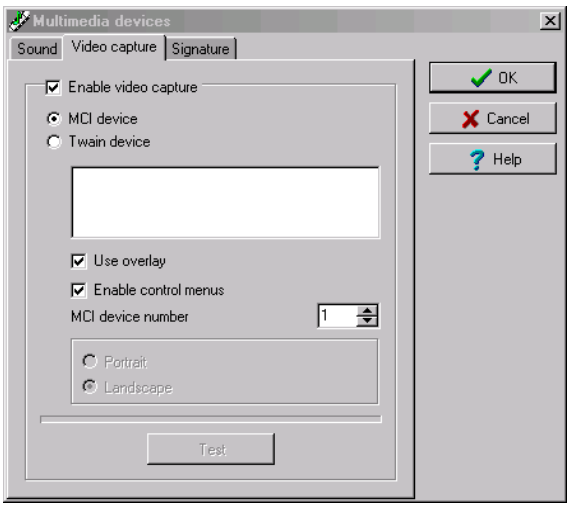
5 Нажать **Play** (Воспроизвести), чтобы прослушать звуковой сигнал. Система воспроизведёт выбранный звуковой сигнал.

6 Для того чтобы добавить новый аудиофайл из собственной библиотеки файлов, нажать кнопку **Add** (Добавить). При нажатии этой кнопки открывается новое окно, в котором можно указать новые звуковые сигналы тревоги.

ПРИМЕЧАНИЕ: *В разделе **Current selection** (Текущий выбор) отображается, какой звуковой сигнал используется в системе в текущий момент. Длительность звукового сигнала тревоги регулируется в поле **Delay** (Задержка).*

Описание параметров оцифровки/захвата изображений

1 В окне Multimedia devices (Мультимедийные устройства) открыть закладку **Video capture** (Захват изображений).

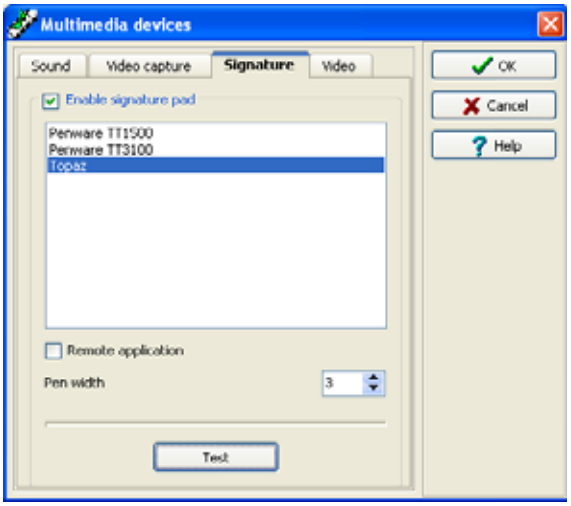


2 Поставить флажок в поле **Enable video capture** (Разрешить захват изображений), чтобы разрешить использование этой функции в системе.
- **MCI device** (Устройство MCI) – стандартные драйвера оцифровки в среде Windows®
- **Twain device** (Устройство Twain). Драйвер захвата изображений Twain (Рекомендуется.)
- **Use overlay** (Использовать наложение) – эта опция используется для устройств захвата изображений.
- **Enable controls menu** (Активировать меню управления) – позволяет применять опции (зум, наклон и поворот) к устройствам оцифровки изображений.
- **MCI device number** (Номер устройства MCI) – служит для выбора идентификационного номера устройства MCI.
- **Portrait** (Портрет) – ориентирует изображения длинной стороной по вертикали.
- **Landscape** (Пейзаж) – ориентирует изображения длинной стороной по горизонтали. (Это значение используется по умолчанию.)

3 Нажать кнопку **Test** (Проверить), чтобы убедиться, что видеокамера функционирует нормально.

Настройка устройства оцифровки подписей

1 В окне Multimedia devices (Мультимедийные устройства) открыть закладку **Signature** (Подписи).



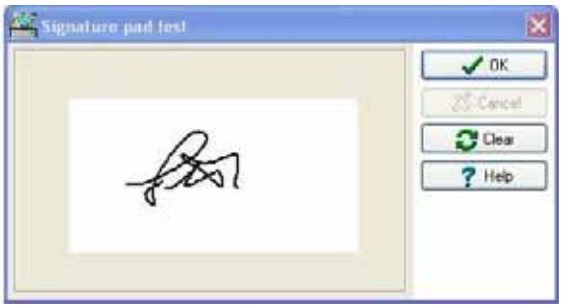
2 Выделить флажком опцию **Enable Signature pad** (Активировать устройство ввода подписей), чтобы разрешить использование такого устройства.

3 В отображаемом на экране списке поддерживаемых устройств выбрать драйвер для настраиваемого устройства.

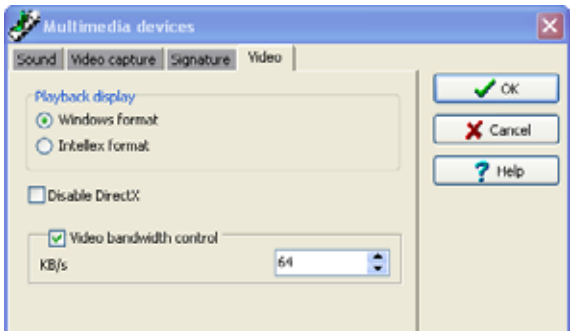
4 Отметить флажком опцию **Remote application** (Удалённое приложение), если сканер подписей установлен удалённо.

5 Выбрать ширину пера в пункте **Pen width**.

6 *Кнопка **Test** (Проверка) позволяет выяснить, как работает выбранный драйвер. При нажатии кнопки **Test** на экране появляется окно Signature Pad Test (Проверка сканера подписи). Это окно появляется на экране, если опция **Signature pad** выделена в каком-либо из окон назначения: Card (Карты), Visitor (Посетители) и Daypass (Разовые пропуска).*



7 Открыть закладку **Video** (Видео), чтобы настроить видеопараметры для функции интеграции с системами видеонаблюдения (Video Integration). Эта опция служит для выбора формата воспроизведения видеофайлов: Windows или Intellex.



- **Disable DirectX** (Запретить DirectX) – пакеты драйверов DirectX представляют собой набор библиотек, реализующих технологию Windows®, которая позволяет оптимизировать работу с графическими и мульмедийными приложениями, в том числе с видео и звуком. По умолчанию использование DirectX разрешено при использовании функции просмотра видео. Однако в определённых случаях может потребоваться запретить использование DirectX, если, например, видеофайлы отображаются неправильно или не отображаются вообще. Однако в случае отказа от использования DirectX система затрачивает больше системных ресурсов.
- Опция **Video bandwidth control** (Регулировка полосы пропускания видеоканала) позволяет уменьшать или увеличивать полосу пропускания, необходимую для передачи видеопотока в реальном времени без ухудшения качества видеоизображения и без снижения производительности компьютера. Диапазон допустимых значений – от 1 кб/с до 4096 кб/с.

ПРИМЕЧАНИЕ: *Установленное значение полосы пропускания видеоканала не может **превышать** значение этого параметра для сервера EntraPass Server*

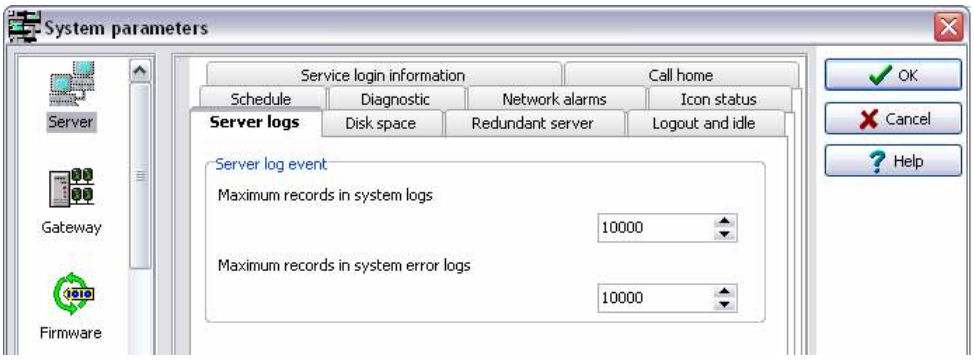
Настройка параметров системы

При помощи меню System parameters (Системные параметры) пользователь с правами системного администратора (System Administrator) получает возможность изменять параметры, используемые для назначения системы EntraPass. В этот раздел меню можно зайти с рабочей станции или с сервера. Параметры сгруппированы вместе под разными закладками, например, Server (Сервер), Gateway (Шлюз), Firmware (Прошивка), Image (Изображение) и др. Если в системе разрешено использовать функцию Video Integration (Интеграция с системами видеонаблюдения), то соответствующие параметры появляются под закладкой Video.

Параметры сервера

Под закладкой **Server** (Сервер) собраны параметры настройки максимальных размеров журналов, функции диагностики, параметры безопасности, ограничения используемого пространства на диске, сетевые тревоги и индикация состояния на иконках.

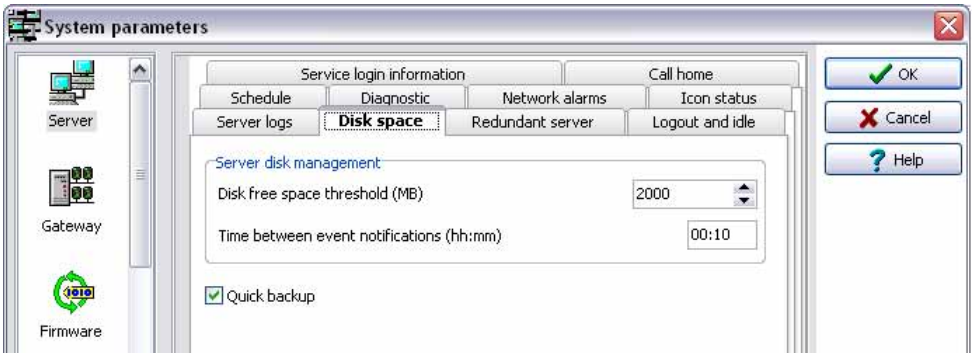
Журналы сервера (Server Logs)



При желании можно ограничить максимальное число записей, хранящихся в системных журналах и в журналах системных ошибок (до 100 000). Записи включают в себя транзакции, например, регистрация пользователя на сервере, окончание сеанса работы на сервере, разъединение или установление связи по сети, остановка или запуск сервера, запрос на регистрацию и др. Эти записи сохраняются вместе с информацией о дате/времени, рабочей станции (откуда поступило сообщение или ошибка), имени оператора и описании транзакций.

Пространство на диске (Disk Space)

Функция Disk Space предназначена для защиты от неполадок в работе системы из-за нехватки рабочего пространства на диске. Эта функция позволяет наблюдать за свободным местом на диске в целях обеспечения оптимальной работы системы или для создания отчётов. В системе EntraPass предусмотрено прекращение генерирования отчётов в случае заполнения места на диске до установленного порогового значения.



- **Disk free space threshold** (Граница свободного пространства, Мб) – из выпадающего списка следует выбрать пороговое значение, по достижении которого система будет отправлять предупреждение об уменьшении свободного пространства на диске ниже установленной

пороговой величины. Измеряется в мегабайтах. Допустимый диапазон значений: от 2000 до 99999 Мб.

- **Time between notifications** (Интервал между уведомлениями, ч) – длительность интервала ожидания между двумя уведомлениями о достижении порогового значения, указанного в поле **Disk space threshold**. Например, если в этом поле указать 00:30, система будет выдавать предупреждение каждые полчаса. Диапазон допустимых значений: от 00:10 до 24:00.
- **Quick backup** (Быстрый backup): Когда выделена эта опция, основной сервер не закрывает таблицы в течении синхронизации с резервным сервером. Сообщения могут быть получены и база данных просмотрена. Желтая иконка отображается слева тогда, когда система находится только в режиме чтения.

Резервный сервер (Redundant Server)

ПРИМЕЧАНИЕ: *Компонент резевного сервера доступен только в том случае, если он был перед этим зарегестрирован*

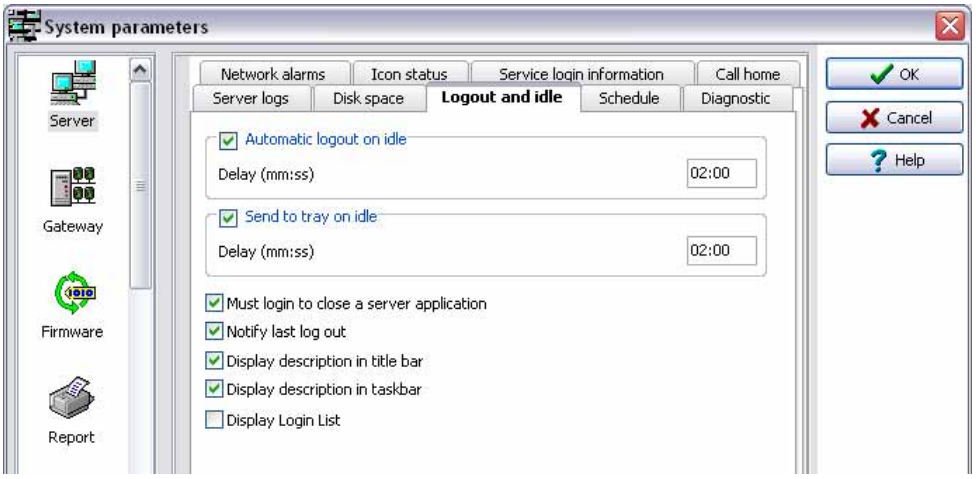
В поле **Automatic restart delay** (Задержка автоматической перезагрузки) можно установить задержку для зеркальной базы данных и резервного сервера. Диапазон допустимых значений: от 1:00 до 9:59.

Quick synchronize: When this option is checked, the main server do not close the tables during the synchronization with the mirror database. Messages can still be received and the database viewed. A yellow icon is then displayed on the left to indicate that the system is in read only mode.

ПРИМЕЧАНИЕ: *Программа интерфейса MS/SQL не поддерживается зеркальной базой данных и резервным сервером. Интерфейс MS/SQL не может подсоединяться к зеркальной базе данных и резервному серверу. Интерфейс MS/SQL будет сохранять все события в буфере.*

Завершение сеанса и бездействие (Logout and Idle)

Под закладкой Logout and Idle собраны параметры, описывающие работу системы в случае бездействия оператора и неиспользования клавиатуры в течение определённого времени.



- **Automatic logout on idle** (Если не используется, автоматически закончить сеанс) – для возобновления работы с приложением Сервер оператор должен будет снова указать своё имя и пароль. Максимальное время задержки составляет 9 минут 59 секунд.

- **Send to tray on idle** (Если не используется, отправлять в трей) – в случае бездействия оператора, зарегистрированного в системе, окно приложения будет свёрнуто и отправлено на панель задач. Максимальное время задержки составляет 59 минут 59 секунд.
- **Must login to close a Server application** (Требовать аторизацию для закрытия приложения) – эта опция обязывает операторов ввести своё имя и пароль, чтобы закрыть приложение Сервер.
- **Notify last log out** (Уведомлять о последнем выходящем из системы) – последний оператор, завершающий сеанс в системе, получит уведомление об этом.
- **Display description in title bar** (Отображать описание в строке заголовка) – имя рабочей станции/сервера будет отображаться в верхней строке окна.
- **Display description in taskbar** (Показывать описание на панели задач) – имя рабочей станции будет отображаться в нижней части экрана.
- **Display Login List** (Показывать список зарегистрировавшихся) – пять операторов, последними вошедших в любое приложение EntraPass, будут показаны в списке в окне регистрации операторов. Эта функция облегчает доступ в систему для операторов, которым достаточно будет найти своё имя в списке и ввести пароль. Она может быть полезной и для административных целей, поскольку системный администратор может быстро выяснить, кто из операторов недавно вошёл в систему на определённом приложении.

ПРИМЕЧАНИЕ: *Несмотря на очевидные преимущества, мы рекомендуем отключить функцию Display Login List, если на первом месте стоит обеспечение безопасности.*

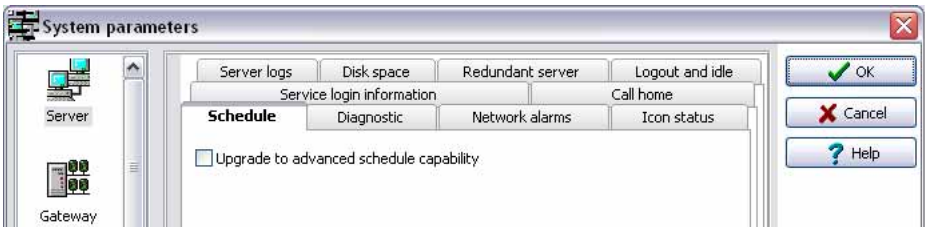
Расписание (Schedule)

Закладка **Schedule** служит для обновления структуры расписания до более совершенной модели. В усовершенствованной модели все расписания сгруппированы по шлюзам, сайтам/лучам или логическим компонентам, что облегчает работу операторов и повышает гибкость системы. Начиная с версии 3.18 и выше, эта опция не активируется автоматически при установке системы.

ПРИМЕЧАНИЕ: *Прежде чем подключать данную опцию, убедитесь, что она Вам действительно необходима.*

Расписания сгруппированы следующим образом:

- **System schedules** (Системные расписания) – применяются к логическим компонентам системы, например, параметрам событий, расписаниям регистрации операторов, событиям, инициирующим включение-выключение видеозаписи, и др. Системные расписания загружаются не для конкретного контроллера, а применительно ко всей системе. Никаких ограничений на количество системных расписаний не установлено.
- **Global schedules** (Глобальные расписания): Глобальные расписания сгрупированы по шлюзу. Они назначаются на Global шлюз. Вы можете назначить до 100 расписаний на Global шлюз для таких устройств как события реле, вторичный уровень доступа, тревожная система, области, туры обхода охранником, контроль лифтов.
- **Corporate site schedules** (Расписания для корпоративных сайтов/лучей) – отдельные расписания для каждого сайта/луча. Для каждого сайта версии Corporate можно создать 100 расписаний следующего назначения: расписание контроля подачи питания (на контроллеры), расписание разблокировки (дверей), расписание работы кнопок запроса на выход REX (двери), режим активации (реле), расписание мониторинга (за входами) и др.



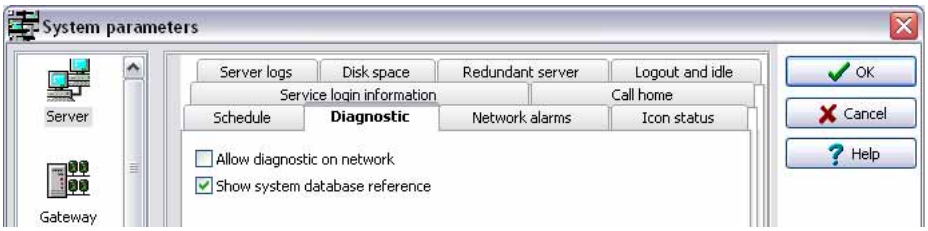
- При выделении данной опции и нажатии кнопки **OK** система выдаёт на экран предупреждение о том, что данная операция имеет необратимые последствия.

- Перед выполнением этого действия настоятельно рекомендуется создать резервную копию данных.

- После завершения процесса закладка **Schedule** исчезнет из меню System Parameter (Системные параметры).

Диагностика (Diagnostic)

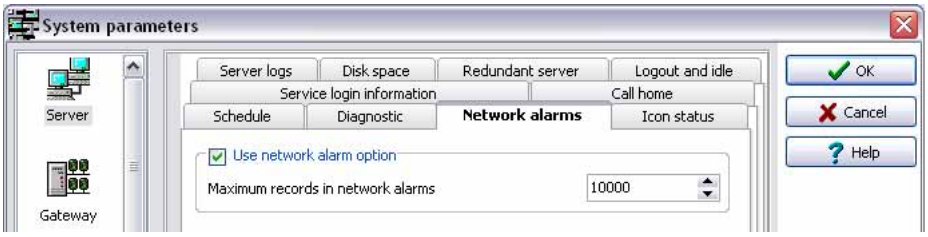
Эта функция позволяет выполнять сетевую диагностику.



- **Allow diagnostic on network** (Разрешить диагностику сети) – разрешает использование команды PING (Packet INternet Groper). Эта автономная программа служит для диагностики неисправностей в сети и/или проверяет состояние маршрута следования пакета до определенного IP-адреса. *Смотрите в Главе 16 Системные утилиты' на странице 515 для более подробной информации* о программе PING.
- **Show system database reference** (Показывать системные индексы базы данных) – показывать уникальные номера компонентов системы. Например, если в меню Door (Двери) поместить курсор мыши на одну из позиций в списке дверей, то на экран будет выведен номер этой двери. Этот уникальный номер компонента (двери) будет отображаться в виде всплывающей подсказки.

Сетевая тревога (Network Alarm)

Сетевые тревоги и связанные с ними комментарии выводятся на рабочие столы операторов. Эта опция разрешена по умолчанию, но её можно отключить, если информацию о тревогах нежелательно отображать на рабочих столах. Чтобы использовать эту опцию, необходимо указать максимальное число записей, которые будут храниться в таблице сетевых тревог.



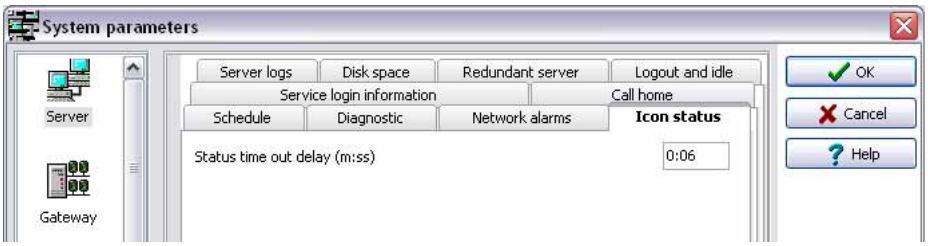
- Поставить флажок в поле **Use network alarm** (Использовать сетевые тревоги), чтобы использовать эту функцию, или не ставить флажок, чтобы запретить её использование.
- Стрелками вверх-вниз указать значение в поле **Maximum records in network alarm** (Максимальное число записей в списке сетевых тревог). Максимально допустимое значение – 100 000.

- После установки значения этого параметра сервер автоматически применит те же настройки на всех рабочих станциях в сети. Эта позволяет ограничить размер файла, чтобы он не занимал слишком много места на диске на рабочей станции и на сервере.

ПРИМЕЧАНИЕ: *После того как число записей в таблице достигнет максимума, они будут удаляться в порядке поступления. Файл, в котором находятся около 100 000 записей, занимает на диске около 100 Мб. Смотрите в Главе 11 Рабочие столы EntraPass' на странице 367 для более подробной информации по сетевым тревогам.*

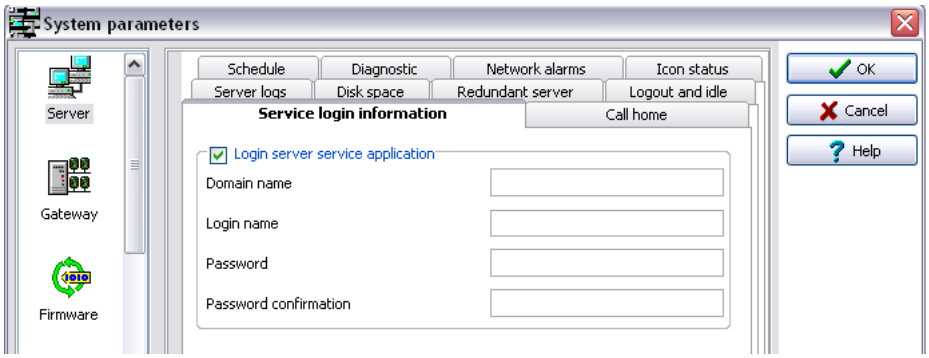
Индикация состояния на иконках (Icon Status)

Параметр **Status time out delay** (Таймаут статуса) позволяет указать задержку, после окончания которой рабочая станция пошлёт на сервер запрос о последних состояниях иконок, расположенных на АРМ. Чем больше указанное время задержки, тем меньше частота обновления иконок, и соответственно, меньше загрузка сети. Максимальное значение параметра составляет 1 мин. 30 сек.



Информация по авторизации приложения в качестве службы (Service Login Information)

Информация, введенная здесь, требуется когда сервер запущен в качестве службы и сетевые ресурсы требуют авторизации от сервера. **Service Login Information** (информация по авторизации в качестве службы) требуется для расписания backup, когда используется сетевой привод.



- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login Server service application** (Регистрационные данные для работы сервера в режиме службы).
- **Обязательно** указать имя домена или рабочей группы в поле **Domain name** и имя пользователя в поле **Login name** и дважды ввести пароль в полях **Password** (второй раз – для подтверждения).

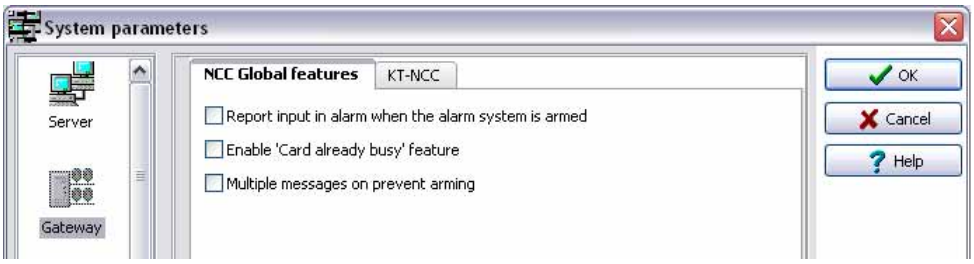
ПРИМЕЧАНИЕ: *Когда у вас нет настроенного имени домена или рабочей группы, вы должны ввести вместо этого **Имя компьютера** в поле **Domain Name**.*

Параметры Шлюза

Секция Шлюз доступна только в EntraPass Global Edition для настрйоки параметров для ваших шлюзов NCC Global и KT-NCC.

Глобальные преимущества NCC

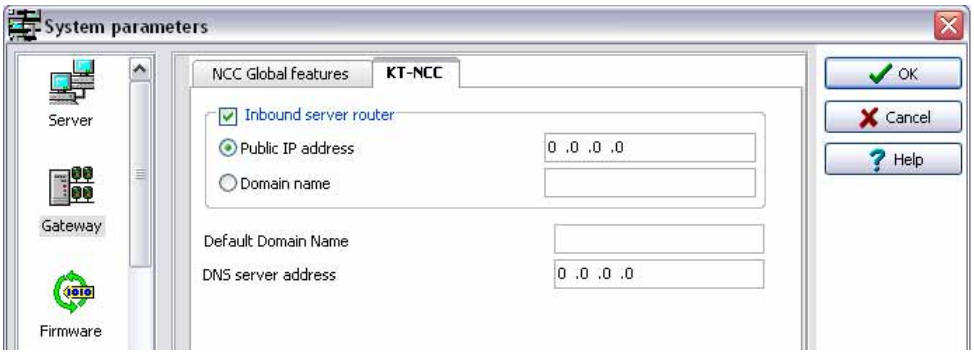
Эти парметры будут назначены для Global Шлюза.



- **Report input in alarm when the alarm system is armed** (Отчет, тревога по входу когда система поставлена на охрану): выделите этот пункт, если вы хотите чтобы система генерировала сообщения “тревога по входу “input in alarm”. Если установлено расписание мониторинга входа/input, и если данный пункт не выделен, то система будет генерировать событие “тревога по входу” даже если система не поставлена под охрану.
- **Enable card already busy feature** (Включить преимущество, карта уже занята): Если выделен это пункт, картодержатель не будет способен открыть другую дверь до тех пор пока не истечет **door open delay** (задержка открытой двери) на первой двери. Выделите данный пункт, чтобы предотвратить, чтобы картодержатели были способны открывать дверь для кого-либо еще и затем пытаться открыть другую дверь в течении действия задержки открытия для двери №1.
- **Multiple messages on prevent arming** (Несколько сообщений для предотвращения постановки на охрану)**:** тревожный вход или группа входов может быть использована для предотвращения постановки на охрану(**Definition** (Назначения)**> Alarm System** (тревожная система)**> Input**(Тревожный вход)**)**. Если система пытается встать на охрану в то время как, группа или один тревожный в тревоге, тогда система будет генерировать сообщение “aborted arming event”(Событие прерывания постановки на охрану). Если эта опция не выделена, только одно сообщение будет сгенерировано, если постановка на охрану была прервана более чем одним компонентом.

KT-NCC

В ситуации для которой, Сервер EntraPass удален от KT-NCC, вы можете настроить чтобы оба устройства KT-NCC и сервер могли общаться через Internet



- Выделите пункт **Inbound server router** и введите **Public IP address** или **Domain name** (адрес, назначеннный провайдером public сети, к которой вы подключены).

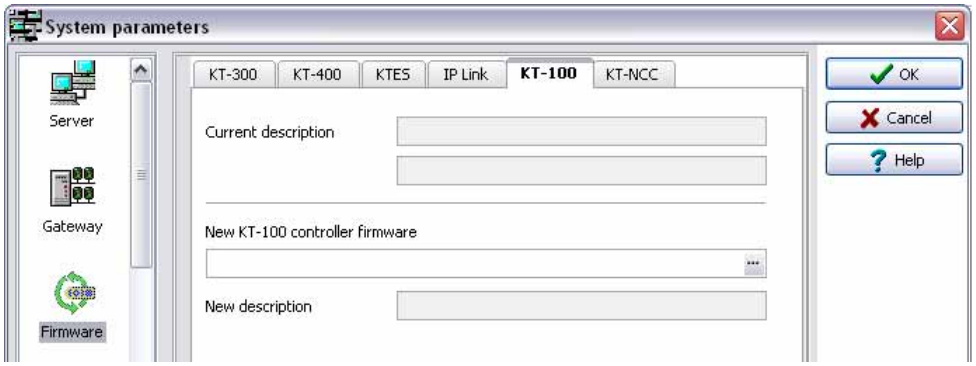
Параметры прошивки (Firmware)

Этот раздел меню содержит всю необходимую информацию о контроллерах, шлюзах и IP-модулях, а также раздел для обновления прошивки.

ПРИМЕЧАНИЕ: *Вкладка KTES будет доступна, если KTES была до этого назначена в системе. Смотрите в Главе 4 Настройка Kantech Telephone Entry System (KTES)’ на странице 134 для более подробной информации .*

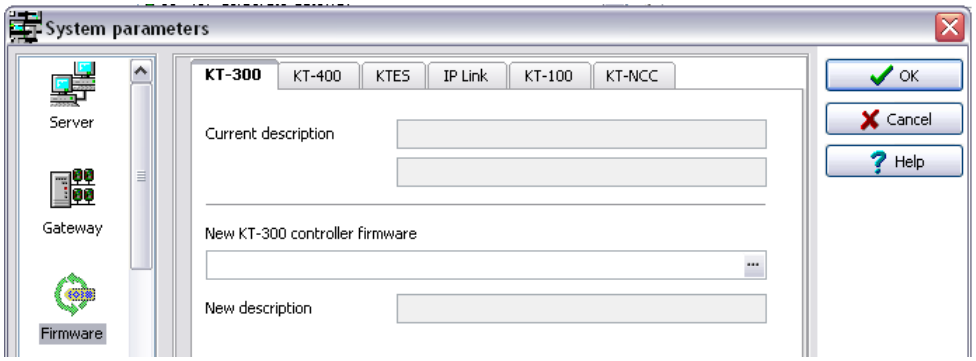
KT-100

Закладка **KT-100** указывает место размещения папки, в которой хранится прошивка для контроллеров KT-100. Эти данные будут использоваться для обновления установленных контроллеров. .



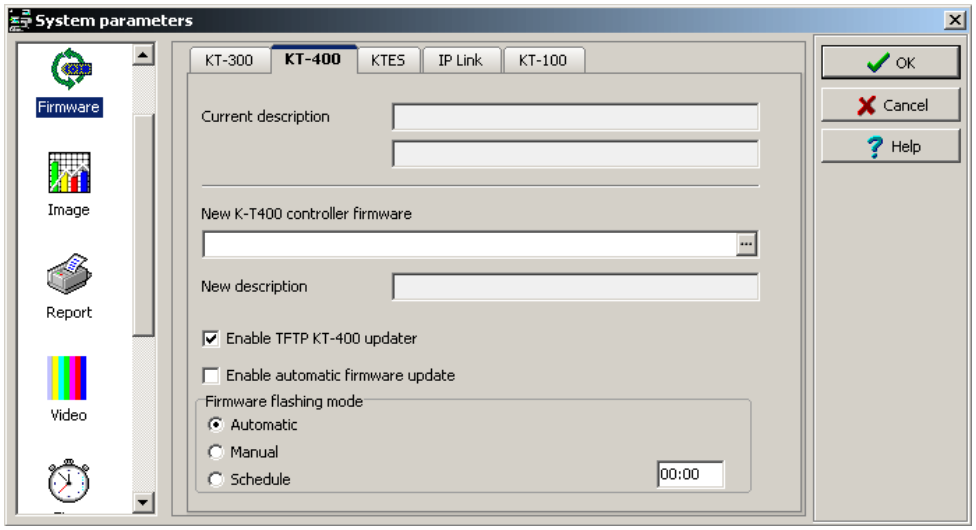
KT-300

Закладка **KT-300** указывает место размещения папки, в которой хранится прошивка для контроллеров KT-300. Эти данные будут использоваться для обновления установленных контроллеров. .



KT-400

Закладка **KT-400** указывает место размещения папки, в которой хранится прошивка для контроллеров KT-400. Эти данные будут использоваться для обновления установленных контроллеров. .



- Если в поле **Enable TFTP KT-400 updater** (Разрешить обновлять KT-400 через TFTP) поставить флажок, то операторы смогут обновлять прошивку контроллера KT-400 при помощи кнопки **Update firmware** (Обновить прошивку) в меню **Operation** (Операции) > **Site** (Сайт/Луч).

- Включить функцию автоматического обновления: Выбрать, чтобы произвести обновления для каждого KT-400 с различной версией прошивки.

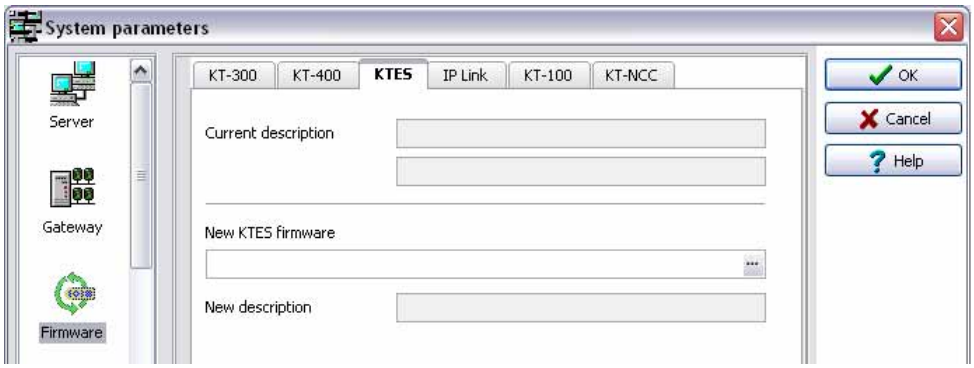
ПРИМЕЧАНИЕ: *Функция автоматического обновления системы применима только для KT-400.*

ПРИМЕЧАНИЕ: *Corporate Gateway должен быть перезапущен чтобы включить/запустить функцию обновления для KT-400 через TFTP.*

- Из соображений безопасности системный администратор может запретить использование этой опции, чтобы операторы не могли самостоятельно обновлять прошивки.

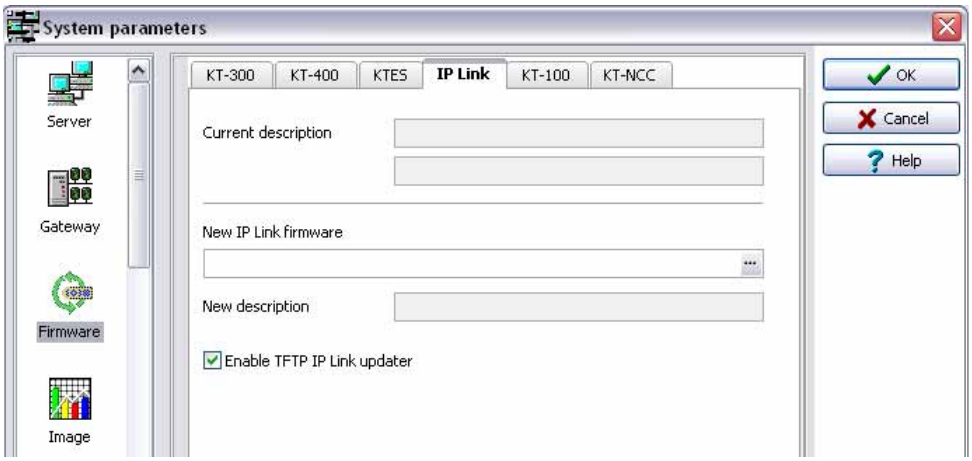
KTES

Закладка **KTES** указывает место размещения папки, в которой хранится прошивка для **KTES**. Эти данные будут использоваться для обновления установленных контроллеров **KTES.**



Kantech IP Link

Закладка **IP Link** указывает место размещения папки, в которой хранится прошивка для модуля Kantech IP Link. Эти данные будут использоваться для обновления установленной прошивки.



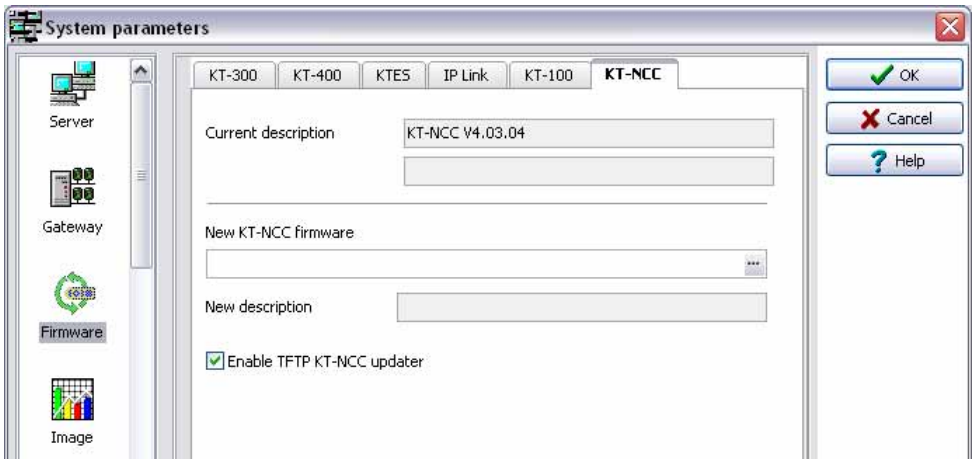
- Если в поле **Enable TFTP IP Link updater** (Разрешить обновлять IP Link через TFTP) поставить флажок, то операторы смогут обновлять прошивку модуля IP Link при помощи кнопки **Update firmware** (Обновить прошивку) в меню **Operation** (Операции) > **Site** (Сайт).

ПРИМЕЧАНИЕ: *Для Corporate Gateway, чтобы программа обновления прошивки (TFTP IP Link updater) стала доступной, необходимо перезагрузить компьютер, на котором установлен сервер (EntraPass Server).*

- Из соображений безопасности системный администратор может запретить использование этой опции, чтобы операторы не могли самостоятельно обновлять прошивки.

KT-NCC

Вкладка **KT-NCC** указывает расположение файла прошивки для KT-NCC. В отличие от других версий прошивки, KT-NCC обновляется автоматически при обновлении EntraPass Global Edition.



- Если в поле **Enable TFTP KT-NCC updater** (Разрешить обновлять **KT-NCC** через TFTP) поставить флажок, то операторы смогут обновлять прошивку модуля **KT-NCC** при помощи кнопки **Update firmware** (Обновить прошивку) в меню **Operation** (Операции) > **Site** (Сайт).

ПРИМЕЧАНИЕ: *Чтобы программа обновления прошивки (TFTP* **KT-NCC** *updater) стала доступной, необходимо перезагрузить компьютер, на котором установлен сервер EntraPass.*

- Из соображений безопасности системный администратор может запретить использование этой опции, чтобы операторы не могли самостоятельно обновлять прошивки.

Параметры изображений (Image)

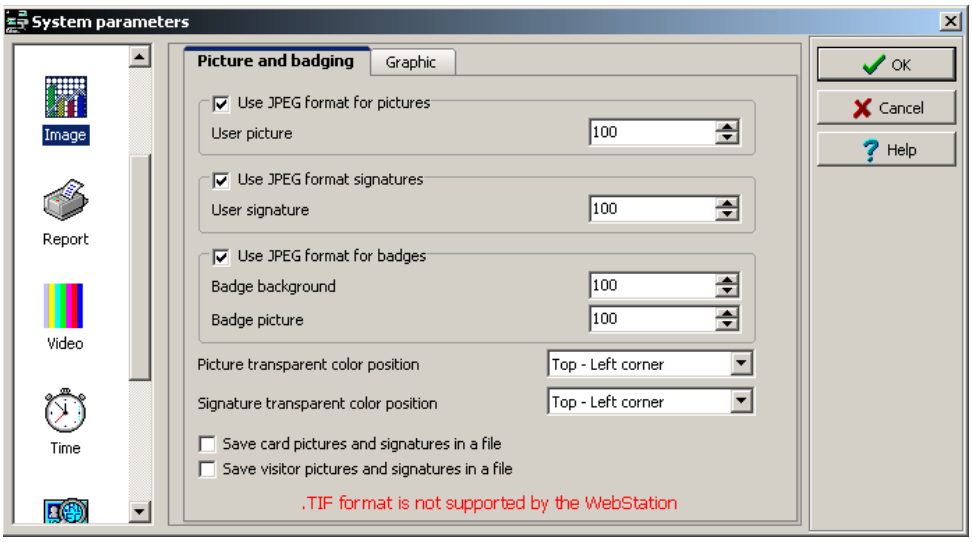
Раздел меню Image служит для назначения параметров, необходимых для создания электронных пропусков. Необходимо указать уровень качества изображений для фотографий, подписей и фоновых изображений.

- В случае использования функции создания электронных пропусков рекомендуется оставить формат изображений jpeg по умолчанию. Снижение качества изображения может привести к ухудшению качества картинок, импортированных с пропусков.
- Если функция электронных пропусков не используется, то качество изображений формата jpeg можно снизить, чтобы они не занимали много места в базе данных. Однако следует принять во внимание, что снижение качества сохранённых изображений ведёт к ухудшению качества фотографий, импортированных в электронные пропуска.

Этот параметр позволяет сохранять фотографии для идентификационных карт и карт посетителей, а также фоновую графику в файл вместо импортирования их напрямую в базу данных. Эту опцию рекомендуется использовать для сайтов с большими хранилищами фотографий и графических схем. Базы данных по фотографиям, подписям и схемам могут содержать, к настоящему моменту, до 2 Гб каждая. Этот параметр будет использоваться в тех случаях, когда сайт требует больше места для сохранения фотографий, подписей и схем.

Фотографии и электронные пропуска

Закладка Picture and badging позволяет настроить параметры качества изображений и подписей для создания электронных пропусков.



- Если в поле **Use JPEG format for pictures, signatures and badges** (Использовать формат JPEG для фотографий, подписей и бейджей) не поставлен флажок, то вместо JPEG изображения (подписи) будут сохраняться в формате TIFF.

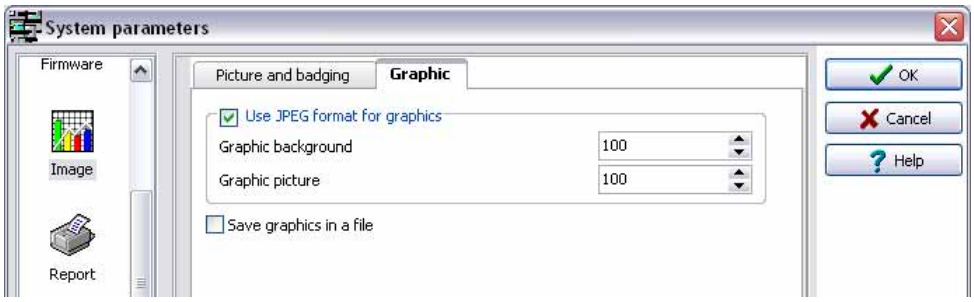
ПРИМЕЧАНИЕ: *Помните, что это может ухудшить качество изображения. Если вы непродвинутый пользователь, то лучше оставить эти настройки по умолчанию.*

- В полях **User picture** (Фотография пользователя), **Signature** (Подпись), **Badge background** (Фон электронного пропуска) и **Badge picture** (Фотография на пропуск) указывается качество сохраняемого изображения. Значение "10" соответствует плохому качеству; при установке величины "100" качество изображения будет отличным.
- Указать место размещения прозрачного цвета для фотографии и подписи **Picture (Signature) transparent color position** (Расположение прозрачного поля под фотографию/подпись). Предусмотрено четыре варианта размещения фотографии/подписи: top-right (правый верхний угол), top-left (левый верхний угол), bottom-right (правый нижний угол) и bottom-left (левый нижний угол). По умолчанию, для прозрачной области под фотографию/подпись система выбирает левый нижний угол. Операторы системы EntraPass могут выбрать более подходящий цвет.
- Если поставить флажок в поле **Save card pictures and signatures in a file** (Сохранять фотографии идентификационных карт и подписи в файл), то система создаст папки **Picture** (Фотографии) и **Signature** (Подписи) на диске **C:\Program Files\Kantech\Server_GE\Data** , где будут храниться все фотографии и подписи вместо импортирования их напрямую в базу данных.
- Если поставить флажок в поле **Save visitor pictures and signatures in a file** (Сохранять фотографии посетителей и подписи в файл), то система создаст папки **Picture** (Фотографии) и **Signature** (Подписи) на диске **C:\Program Files\Kantech\Server_GE\Data** , где будут храниться все фотографии и подписи посетителей вместо импортирования их напрямую в базу данных.

ПРИМЕЧАНИЕ: *В случае изменения существующей фотографии или подписи система EntraPass сохранит их в соответствующий файл и удалит соответствующую запись/ссылку из базы данных.*

Графические схемы (Graphic)

Закладка Graphic позволяет настроить параметры качества графических схем и планов для использования их в составе программного обеспечения EntraPass.



- Если в поле **Use JPEG format for graphics** (Использовать формат JPEG для схем) не поставлен флажок, то графические схемы и планы будут сохраняться в формате TIFF.

ПРИМЕЧАНИЕ: *Помните, что это может ухудшить качество изображения. Непродвинутым пользователям лучше оставить настройки по умолчанию без изменений.*

- В полях **Graphic background** (Фон графической схемы) и **Graphic picture** (Изображение схемы) указывается качество сохраняемого изображения. Значение "10" соответствует плохому качеству; при установке величины "100" качество изображения будет отличным.
- Если поставить флажок в поле **Save graphics in a file** (Сохранять графические схемы в файл), то система создаст папку **Graphic** (Графические схемы) на диске **C:\Program Files\Kantech\Server_GE\Data** , где будут храниться все графические схемы вместо хранения их прямо в базе данных.

ПРИМЕЧАНИЕ: *В случае изменения существующей графической схемы система EntraPass сохранит её в соответствующий файл и удалит соответствующую запись в базе данных.*

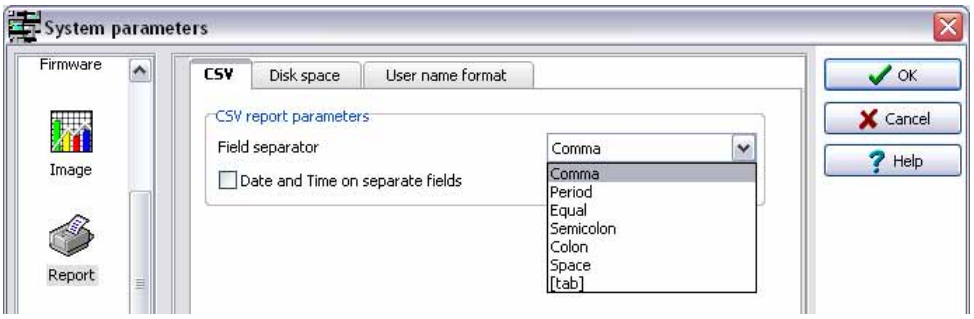
Параметры отчёта (Report)

Закладка **Report** предназначена для настройки разделителей полей в отчётах, указания порогового значения доступного пространства на диске, а также формата имен пользователей.

CSV

В этом разделе следует выбрать, какие разделители должны быть использованы в отчётах.

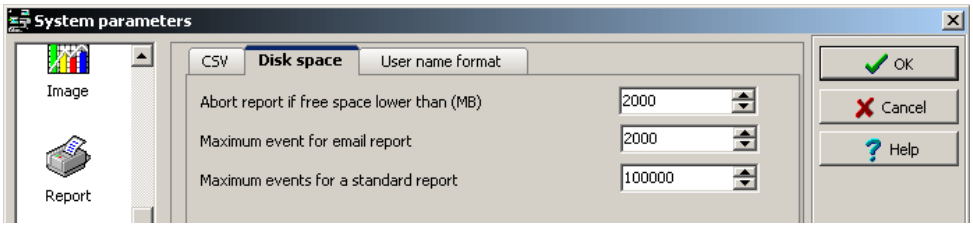
- По умолчанию система использует в качестве разделителя полей знак запятой (,). В выпадающем списке **Field separator** (Разделитель полей) это соответствует значению Comma (Запятая). При необходимости может быть установлен другой разделитель. Другие доступные варианты: Period (Точка), Equal (Знак равенства), Semicolon (Точка с запятой), Colon (Двоеточие), Space (Пробел) и Tab (Клавиша табуляции).
- Рекомендуется отметить флажком опцию **Date and time on separate fields** (Дата и время в разных полях). Если CSV (Значения, разделённые запятыми) указано использовать как способ вывода отчётов, то по умолчанию система будет включать дату и время в одно поле. При установке флажка напротив этой опции система будет разделять поля даты и времени.



Пространство на диске (Disk Space)

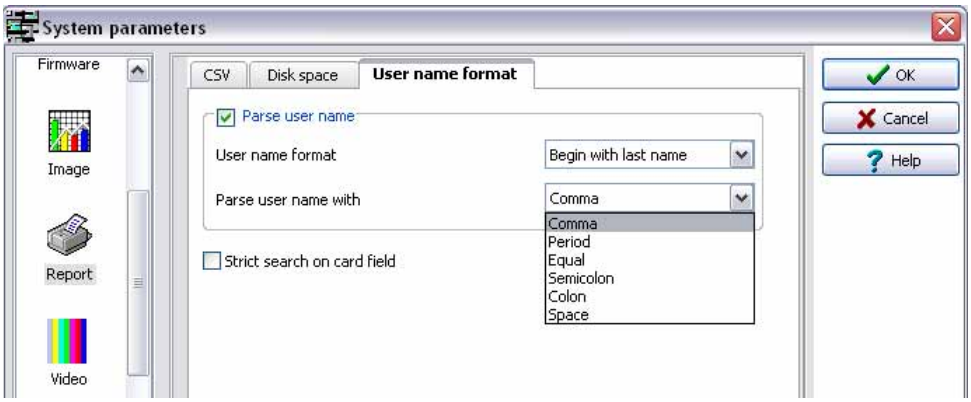
Эта функция служит мерой защиты, например, в случае запроса очень большого по объёму отчёта. В такой ситуации система прервёт выполнение отчёта и выдаст предупредительное сообщение, указывая причину отмены действия.

- **Abort report if free space lower than** (Прервать выполнение отчёта, если свободного места осталось менее...) – в этом поле следует указать минимальное доступное место на диске, необходимое для выполнения отчётов. Допустимый диапазон значений: от 2000 до 999 999 Мб.
- **Maximum event for e-mail report** (Максимальное число сообщений для электронного отчёта) – в этом поле устанавливают ограничение по объёму для электронных отчётов. Диапазон допустимых значений: от 100 до 10 000 событий.
- **Maximum event for standard report** (максимальное количество событий для стандартного отчета). Выпадающий список позволяетвам указать максимальное количество событий, которые могут быть посланы в отчете. Количество может быть от 1000 до 500,000 событий.



Формат имени пользователя

Выбор формата имён пользователей позволяет установить, как имена владельцев карт будут отображаться в системе EntraPass. .



- **Parse user name** (Разбор Ф.И.О. пользователя) – в этом поле следует поставить флажок, если необходимо выбрать способ разделения имени и фамилии.
- **User name format** (Формат имени пользователя) – указать порядок перечисления имени и фамилии. Доступные варианты: Begin with last name (Сначала фамилия), Begin with first name (Сначала имя).
- В выпадающем списке **Parse user name with** (Разделитель имени и фамилии пользователя) указать, какой разделитель должен стоять между полями имени и фамилии. Доступные варианты: Comma (Запятая), Period (Точка), Equal (Знак равенства), Semicolon (Точка с запятой), Colon (Двоеточие), Space (Пробел).
- **Strict search on card field** (Жёсткий поиск по полям карты) – это поле не следует выделять флажком, если нет необходимости использовать более старый метод жёсткого поиска (EntraPass версии 3.17 и ниже) в полях карт для составления отчётов.

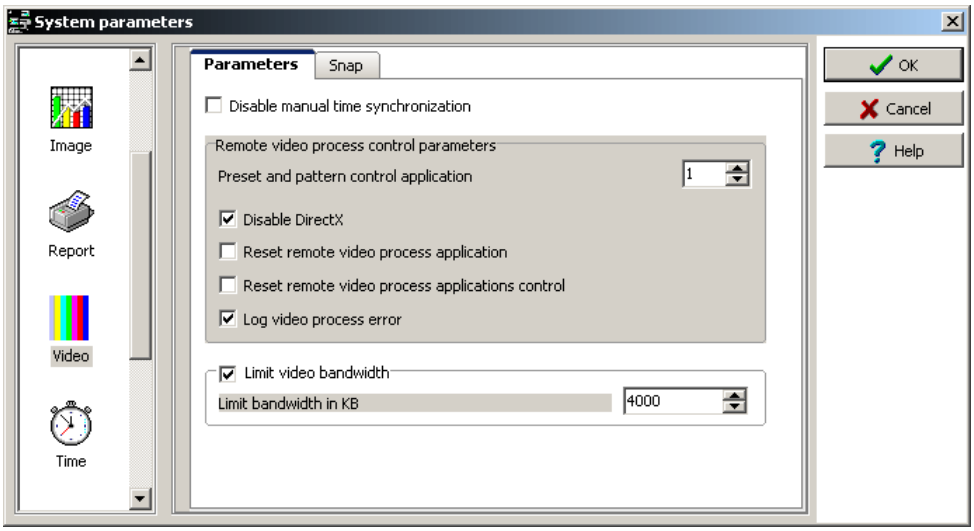
ПРИМЕЧАНИЕ: *В системе EntraPass версии 3.18 и ниже система использовала более строгий метод поиска, требовавший обязательного указания верхней и нижней границ поиска для получения результатов. Например, при составлении отчёта, в который должны быть включены все пользователи с фамилиями, начинающимися на букву А, необходимо было указать нижнюю границу "А", а верхнюю границу "AZZZZZ". Теперь для этого в обоих полях (верхней и нижней границы) достаточно указать "А".*

Параметры видеонаблюдения (Video)

Раздел **Video** будет отображаться только в том случае, если в системе EntraPass разрешено использовать функцию интеграции с системами видеонаблюдения (Video integration). Здесь можно настроить параметры синхронизации по времени, настройки видеонаблюдения в удалённом режиме и использование формата JPEG для видеоизображений.

Параметры (Parameters)

Под закладкой **Parameters** (Параметры) собраны параметры видеонаблюдения.



- **Disable manual time synchronization** (Запретить синхронизацию по времени вручную) – после изменения вручную даты и времени на сервере EntraPass не позволяет ему обновить дату и время на видеосервере. Эта функция пригодится, например, когда необходимо, чтобы независимо от фактического времени на сервере EntraPass, все записи видео на сервере остались без изменений.
- В разделе **Remote video process control parameters** (Параметры дистанционного видеонаблюдения) собраны параметры, описывающие дистанционное управление видеопроцессами между сервером EntraPass и видеосерверами, подключёнными к системе EntraPass. Сюда входят все задачи, связанные с записями, опросами, событиями, предустановками и маршрутами.
  - Поле **Preset and pattern control application** (Прилжение по управлению предустановками и маршрутами) служит для указания числа приложений, которые можно запускать одновременно для обработки предустановок и маршрутов. В системе можно разрешить запускать одновременно от 1 до 8 приложений.

ПРИМЕЧАНИЕ: *Приложение Preset and Pattern Control application запускается каждый раз, когда начинается видеозапись по предустановкам. Если для этого параметра установлено значение "1", а видеосерверов с предустановками и маршрутами, например, больше одного, то управляющее приложение будет обрабатывать предустановки на всех видеосерверах. Если необходимо увеличить число приложений Preset and Pattern Control Application, следует помнить, что одновременное выполнение нескольких приложений занимает больше системных ресурсов.*

  - **Disable DirectX** (Запретить DirectX) – пакеты драйверов DirectX представляют собой набор библиотек, реализующих технологию Windows®, которая позволяет оптимизировать работу с графическими и другими мульмедийными приложениями, включая видео и аудио. По умолчанию использование DirectX разрешено при использовании функции просмотра видео. В определённых случаях может возникнуть необходимость запретить использование DirectX, если, например, видеофайлы отображаются неправильно или не отображаются вообще.

ПРИМЕЧАНИЕ: *В случае отказа от использования DirectX система затрачивает больше системных ресурсов.*

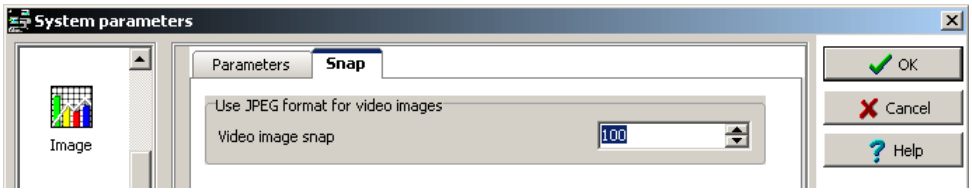
  - **Reset remote video process application** (Перезапустить приложение видеонаблюдения) – служит для прекращения и возобновления видеонаблюдения через несколько секунд с автоматической перезагрузкой приложения Remote Video Process. Эту опцию рекомендуется использовать, например, в случае отсутствия передачи видеоизображения.

- **Reset remote video process application control** (Перезапустить систему управления приложениями по видеонаблюдению) – служит для прекращения работы средств управления (записей, опросов, событий, а также предустановок и маршрутов) и автоматической перезагрузки приложения Remote Video Process.
- **Log Video process error** (Журнал ошибок обработки видеоданных) – при выделении этой опции система будет вести журнал всех ошибок обработки видеофайлов на сервере EntraPass. Журнал ошибок сохраняется в файл C:\Program files\Kantech\Server_CGE\Bin\Log. Каждое приложение Remote Video Process Control генерирует файл журнала:
  - RVP_LOG_00.txt (ошибки, генерируемые RVP0.exe)
  - RVPPoll_LOG_01.txt (ошибки, генерируемые RVPPOLL1.exe)
  - RVPEvent_LOG_02.txt (ошибки, генерируемые RVEVENT3.exe)
  - RVPRecord_LOG_03.txt (ошибки, генерируемые RVPRECORD3.exe).
  - RVPControl_LOG_04.txt (ошибки, генерируемые RVPCONTROL4.exe). Система создаст столько файлов журналов, сколько приложений будет работать одновременно (RVPControl_LOG_05 ... 08). Количество файлов с журналами ошибок будет соответствовать числу, указанному в поле **Preset and pattern control application** (Приложение по управлению предустановками и маршрутами).
- Опция **Limit video bandwidth** (Ограничить полосу пропускания видеоканала) позволяет уменьшать или увеличивать полосу пропускания, необходимую для передачи видеопотока в реальном времени без ухудшения качества видеоизображения и без снижения производительности компьютера. Диапазон допустимых значений – от 1 кб/с до 4096 кб/с. Установленное значение будет применено ко всем рабочим станциям, включая сервер EntraPass Server. Однако для некоторых рабочих станций это значение можно локально уменьшить в меню **Options** (Опции) > **Multimedia Devices** (Мультимедийные устройства) > **Video** (Видеонаблюдение), на странице 479.

ПРИМЕЧАНИЕ: *Установленное значение полосы пропускания на рабочей станции не может* ***превышать*** *значение этого параметра на сервере EntraPass.*

Захват изображения (Snap)

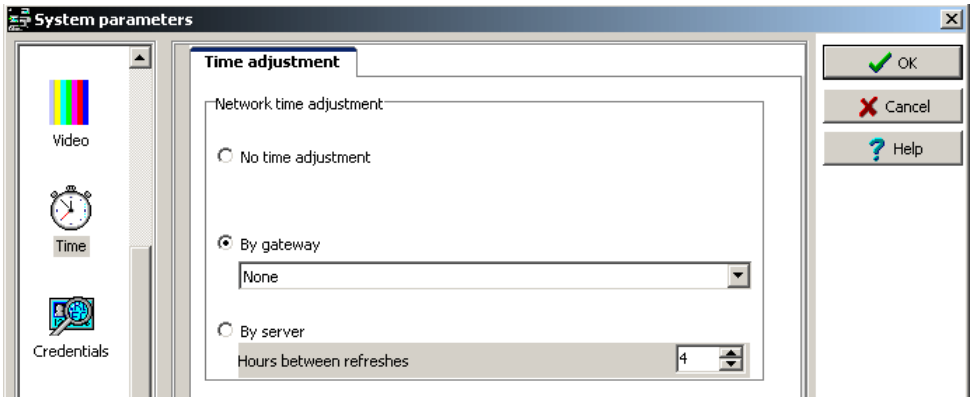
Этот раздел меню служит для описания качества изображения, захваченного и сохранённого для использования в качестве пиктограммы видеофрагмента.



- В поле **Video image capture** (Захват видеоизображения) следует указать качество сохраняемых изображений, которые будут использоваться в качестве пиктограмм к каждому видеофрагменту. Значение "10" соответствует плохому качеству; при установке величины "100" качество изображения будет отличным.

Параметры времени (Time)

В разделе **Time** (Время) следует указать, какой шлюз будет использоваться, чтобы автоматически настраивать время на всех компьютерах, подключённых к серверу EntraPass. Эта функция очень полезна при наличии удалённых сайтов/лучей.



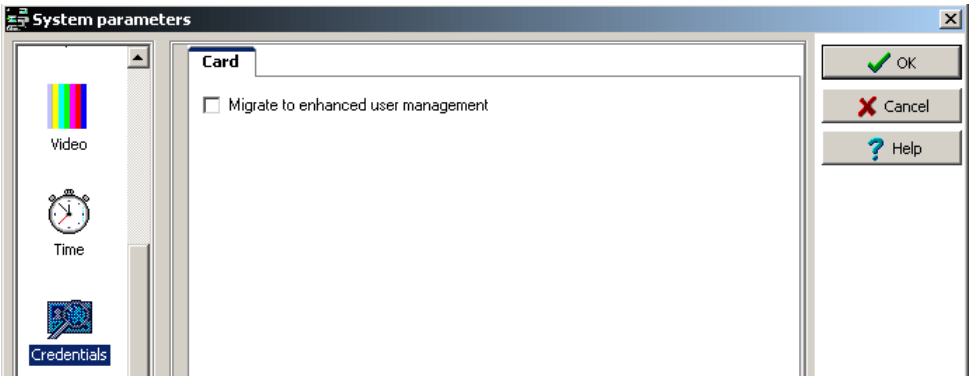
ПРИМЕЧАНИЕ: *Шлюз опрашивает первый контроллер на первом сайте в 05:47, в 13:47 и в 19:47, чтобы получить информацию о времени на контроллере.*

- **No time adjustment** (Не использовать настройку времени) – запретить использование этой опции.
- **By Gateway** (По данным шлюза) – автоматически синхронизирует время всех компьютеров по времени на шлюзе, выбранном из списка.
- **By Server** (По данным сервера) – автоматически синхронизирует время на всех компьютерах через равные интервалы времени. В поле **Hours between refreshes** (Интервал между обновлениями, часов) – необходимо также указать частоту обновления данных. Диапазон допустимых значений: от 1 до 9999 часов.

Настройки регистрационных данных (Credential parameters)

Карты (Card)

Под закладкой **Card** системные администраторы имеют возможность перестроить систему EntraPass и включить режим усиленного администрирования пользователей, чтобы работать с пользователями, выбирая по именам, как это происходит по номерам карт. Каждый владелец карты будет наделён именем пользователя и сможет иметь до 5 разных номеров карт. *Смотрите в Главе 8 Выпуск новой карты в режиме расширенного администрирования пользователей' на странице 285 для более подробной информации* . This option will be used with the EntraPass WebStation for card management. For more information on the EntraPass WebStation, please refer to the *EntraPass WebStation User Manual*, DN1709.



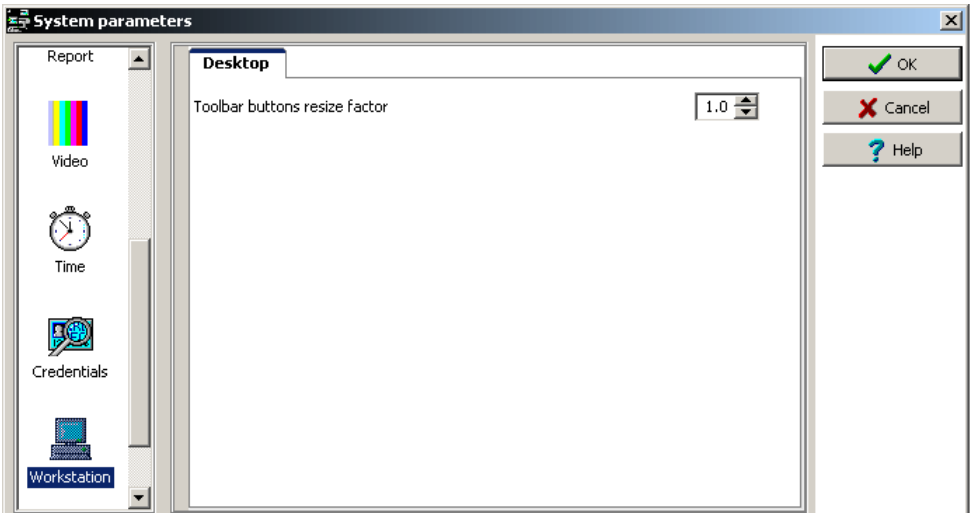
ПРИМЕЧАНИЕ: Переход в режим усиленного администрирования пользователей является **НЕОБРАТИМЫМ** процессом. Однако, в процессе миграции система создает резервную копию, с которой можно восстановить предыдущий режим работы системы.

- **Migrate to enhanced user management** (Переход в режим усиленного администрирования пользователей) – установить метку, чтобы система перешла в этот режим. *(Смотрите в Главе 8 Issuing a New Card in Enhanced User Management Environment' на странице 276 для более подробной информации).*
- При выделении данной опции и нажатии кнопки **OK** система выдаёт на экран предупреждение о том, что данная операция необратима, пока система не выполнит резервное копирование данных.

- После завершения процесса эта опция перестанет быть активной в меню **Card**.

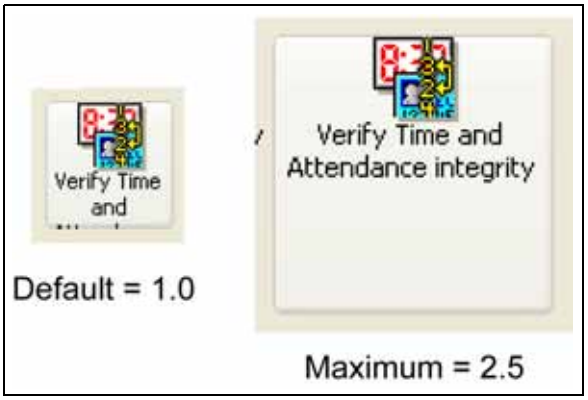
Рабочая станция и Сервер

Кнопки на панели инструментов



Размер кнопок на панели инструментов может быть увеличен до 2,5 раз относительно первоначального размера, что позволяет улучшить наглядность и читаемость текста, расположенного под каждой кнопкой. Данная опция доступна для сервера (Server) и рабочих станций (Workstations) системы EntraPass. Для того чтобы изменения на панели инструментов вступили в силу, необходимо завершить сеанс работы в системе и снова войти в неё.

иже для сравнения приведён пример минимального размера кнопки (1.0) и её максимального размера (2.5).



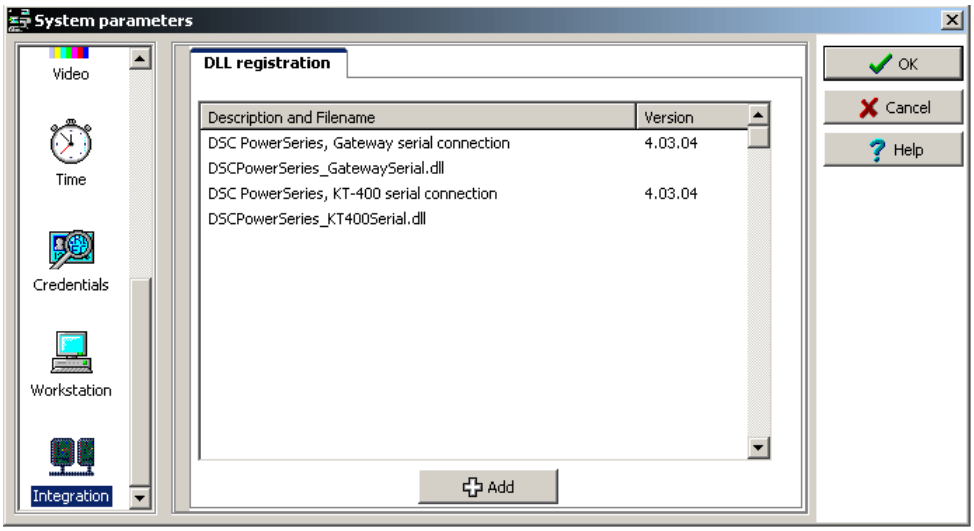
Интеграция

Панель **Integration** позволяет пользователям выбрать оборудование производителей третьих компаний, которое было интегрировано в EntraPass.

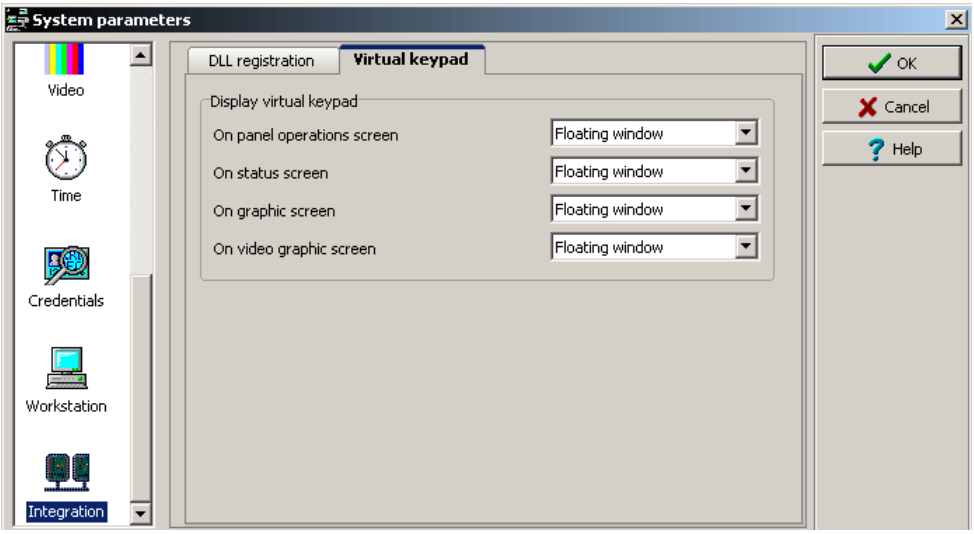
DLL registration (регистрация DLL): Доступные DLL будет использовано для указания типа подключенного оборудования к EntraPass.

- Нажмите кнопку **Add** (Добавить) для подключения другой DLL. Смотрите в Главе 4 Настройка интегрированной панели охранной сигнализации' на странице 168 для более подробной информации .

ПРИМЕЧАНИЕ: *Интеграционнная DLL должна быть установлена на сервере EntraPass, чтобы подсоединяться к Шлюзу Corporate, к которому физически подключено оборудование.*



Virtual keypad (Виртуальная панель): Панель **Virtual keypad** позволяет пользователям отображать keyppad (пульт охранной панели) на экране. Доступны три режима отображения: **Floating** (плавающий), **Modal** (Модальный) или **Stay on top** (установленный на верху).



Backup по расписанию

Резервная копия – это такая копия базы данных системы, которая используется для замены оригинальной базы данных в случае отказа компьютера. В случае неисправности одного компьютера появляется возможность восстановить резервную копию на другом компьютере (на котором установлено приложение Сервер EntraPass).

- Создавать резервные копии следует регулярно, не реже одного раза в неделю или чаще, если в базу данных часто вносятся изменения.
- Рекомендуется создавать по две резервных копии всех файлов базы данных. По соображениям безопасности их следует хранить в разных местах.
- Чтобы создать резервную копию файлов, можно воспользоваться одним из следующих способов:
  - меню под закладкой Server/Backup или
  - программа Backup Scheduler для создания автоматических расписаний или
  - любое другое программное и аппаратное обеспечение (использование программного обеспечения других компаний не рекомендуется).

ПРИМЕЧАНИЕ: *По умолчанию во время создания резервных копий или восстановления файлов базы данных сервера временно недоступны (отключены). АРМы не смогут изменять данные базы данных.*

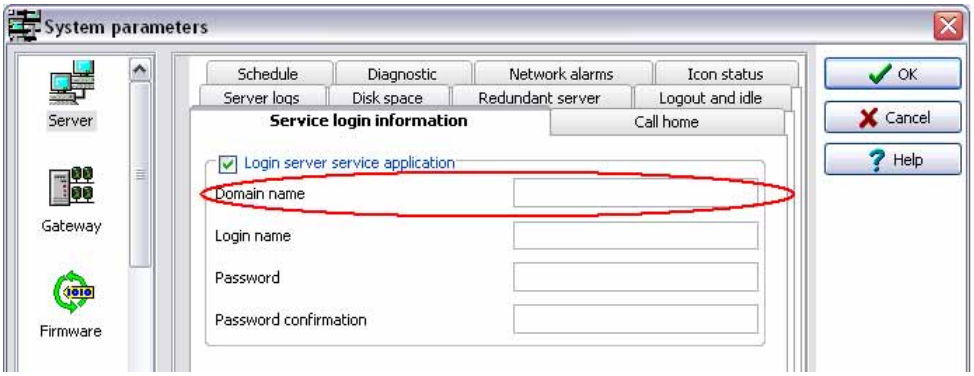
Программа-планировщик Backup Scheduler предназначена для создания расписаний резервного копирования системных данных, архивов и данных по учёту рабочего времени. Достаточно указать настройки по умолчанию, и система сделает все остальное сама!

Настройка резервного копирования, когда сервер EntraPass работает в режиме службы

Эти действия необходимы, если сервер EntraPass работает в режиме службы, и необходимо выполнить резервное копирование данных на другой компьютер **в той же рабочей группе или домене**

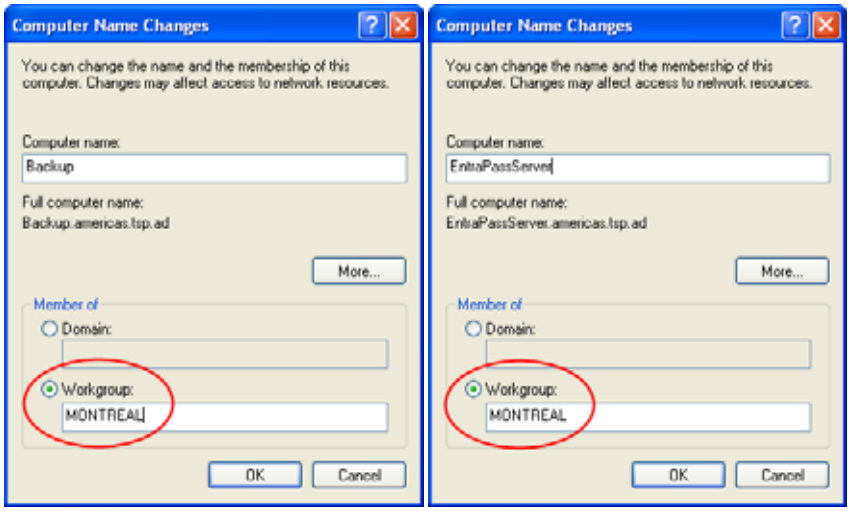
ПРИМЕЧАНИЕ: *Для выполнения описанных ниже действий на сервере EntraPass пользователь должен иметь все права администратора. При отсутствии необходимых прав или недостаточном знании средств администрирования Windows (Windows Administrative Tools) следует обращаться к администратору сети.*

1. С сервера EntraPass зайти в меню Options (Опции) > System Parameters (Системные параметры) > Server (Сервер) > Service Login Information (Данные регистрации для работы в режиме службы).



2 Указать данные в обязательных для заполнения полях: Domain name (Имя домена), Login name (Регистрационное имя), Password (Пароль) и Password Confirmation (Подтверждение пароля).

***ПРИМЕЧАНИЕ: Имя домена** или **Имя рабочей группы**, в которые входят сервер EntraPass и компьютер для резервных копий, должны быть одинковы, как в примерах ниже.*



3 Нажать **OK**.

Настройка расписаний для автоматического создания резервных копий системной базы данных

1 В меню Options (Опции) нажать иконку **Backup Scheduler** (Планировщик заданий по созданию резервных копий) .

2 Открыть закладку в соответствии с тем, какие данные предназначены для резервного копирования: **Data** (Данные), **Archive** (Архивы), **Time & Attendance** (Учёт рабочего времени) или **Video event** (Видеособытия).

ПРИМЕЧАНИЕ: *По умолчанию система автоматически создаёт резервные копии каждую субботу в 4:00 утра для всех новых установок. Настройка времени на 4:00AM имеет дополнительные преимущества, так как в это время резервное копирование не пересекается с другими задачами, выполняемыми системой, и с другими расписаниями, действующими в период около полуночи.*

3 Отметить флажком поле **Automatic backup** (Автоматическое резервное копирование), чтобы стали доступными поля для ввода параметров. В зависимости от того, какая закладка открыта, отображаются разные параметры настройки.

4 В разделе **Backup folder** указать папку для хранения резервных копий:
- **Default folder** (Папка по умолчанию) – файлы с резервными копиями будут сохраняться в папку, выбранную по умолчанию. По умолчанию, имя вложенной папки для резервных копий генерируется автоматически по следующему правилу: X_YYYY_MM_DD_HH_MM_SS, где 'X' = тип данных (системные данные – D, архивы – A, учёт рабочего времени – T), YYYY – год, MM – месяц, DD – день, HH – часы, MM – минуты, SS – секунды.

ПРИМЕЧАНИЕ: *По умолчанию система создаёт резервные копии всех файлов, находящихся в папках:* ***C:/Program files/Kantech/Server/Data*** *(данные) или* ***Archive*** *(архивы) или* ***Time*** *(учёт рабочего времени) и по видеонаблюдению video или V. Путь назначения:* ***C:/Program files/Kantech/Server/Backup/X_YYYY_MM_DD_HH_MM_SS****.*

- **Specific folder** (Особая папка) – резервные копии будут сохраняться во вложенных папках, имя которых будет соответствовать именам исходных папок.

5 Выбрать тип копирования в разделе **Backup type**: в зависимости от типа данных в этом разделе меню отображаются разные опции.
- Только для закладки **Data** (Данные):
  - **Separate files** (Отдельные файлы) – базы данных будут копироваться последовательно друг за другом.
  - **Self-extracting compressed file** (Самораспаковывающийся архив) – создание исполняемого файла (*.exe) со сжатием данных для уменьшения места на диске, занимаемого резервными копиями.
- Только для закладок **Archive** (Архивы), **Time and Attendance** (Учёт рабочего времени) и **Video Event** (Видеособытия):
  - **Separate files, full backup** (Отдельные файлы, полная копия) – создание полной копии всех баз данных.
  - **Self-extracting compressed file, (full backup)** (Самораспаковывающийся архив, полная копия) – создание исполняемого файла (*.exe) со сжатием данных для уменьшения места на диске, занимаемого резервными копиями.
  - **Separate files, incremental** (Отдельные файлы, инкрементная копия) – создание резервной копии всех баз данных. Записываются только те данные, которые были изменены с момента последнего создания резервной копии.
  - **Self-extracting compressed file, incremental** (Самораспаковывающийся архив, инкрементная копия) – создание исполняемого файла (*.exe) со сжатием данных для уменьшения места на диске, занимаемого резервными копиями. Записываются только те данные, которые были изменены с момента последнего создания резервной копии.

ПРИМЕЧАНИЕ: *Восстановление самораспаковывающегося архива после обновления системы EntraPass возможно только с сервера EntraPass, где были сделаны оригинальные самораспаковывающиеся резервные копии.*

ПРИМЕЧАНИЕ: *В случае выбора опции "full backup" каждый раз при создании резервной копии будет создаваться новая вложенная папка, содержащая данные или самораспаковывающийся файл. В случае выбора копирования инкрементного типа записываться будут только те данные, которые были изменены с момента последнего создания резервной копии. Чтобы восстановить данные, потребуется восстановить все вложенные папки последовательно друг за другом (начиная с самой первой).*

6 Указать частоту создания резервных копий.
- **Weekly** (Еженедельно) – создавать резервные копии один раз в неделю. Указать день недели (например, выполнять копирование каждый четверг).
- **Monthly** (Ежемесячно) – резервные копии будут создаваться один раз в месяц (например, резервное копирование будет выполняться в первый день каждого месяца).

- **Daily** (Ежедневно) – создавать резервные копии каждый день.
- **Now** (Сейчас) – эта опция позволяет создавать резервную копию немедленно.

7 Указать время начала резервного копирования (в формате 24:00).

8 Повторить действия в пп. 1 ... 8 для всех остальных закладок меню.

9 Нажать **OK** для сохранения.

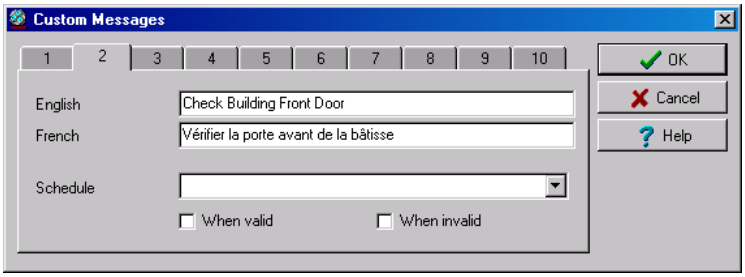
Специальные сообщения (Custom Messages)

Меню Custom Messages позволяет операторам, наделённым соответствующими правами доступа, создавать специальные сообщения, чтобы генерировать события по расписанию. Система позволяет запрограммировать до 10 специальных сообщений, предназначенных для инициирования события в установленное время. Каждое специальное сообщение будет инициироваться, когда расписание становится достоверным, недостоверным или при выполнении обоих этих условий. Другими словами, можно инициировать до 20 специальных событий, если принять во внимание начало и/или конец периода действия расписания. Каждое специальное событие будет отображаться в списке сообщений (Messages List) на рабочих столах.

Each custom events will be displayed in the Messages List on the Desktops.

Настройка специальных сообщений

1 На панели инструментов **Options** (Опции) нажать иконку **Custom Messages** (Специальные сообщения).



2 В первой закладке указать первой специальное сообщение, которое необходимо вывести в списке сообщений (Messages List). Доступно два поля для ввода сообщения на двух используемых языках.

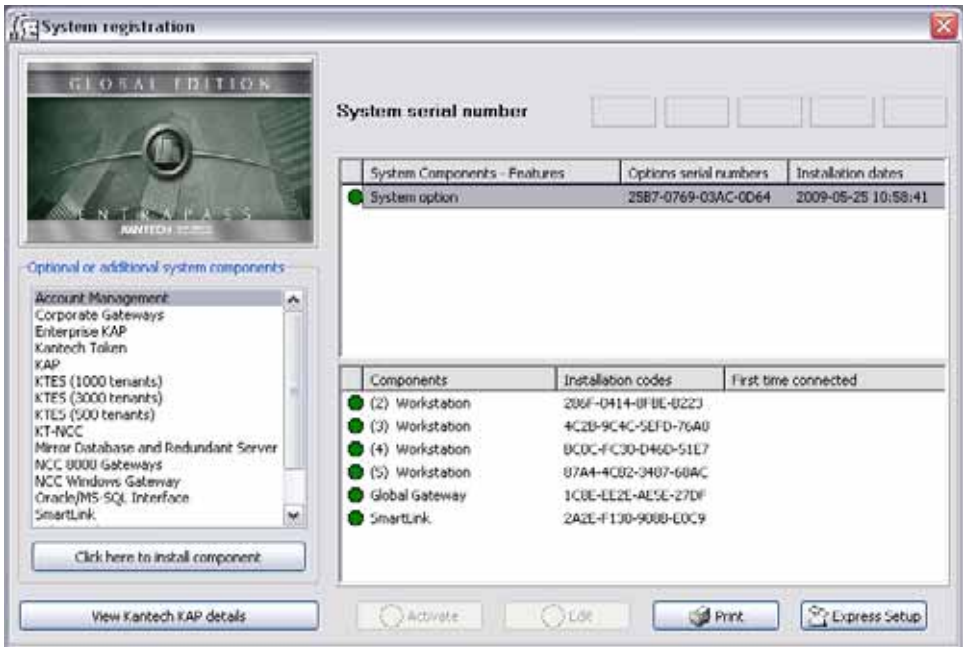
3 Указать предварительно настроенное расписание, по которому будет инициироваться специальное событие.

4 Указать, когда должно инициироваться событие: когда расписание становится достоверным (**Valid**) или недостоверным (**Invalid**) или в обоих случаях.

5 Перейти к следующей закладке и настроить второе сообщение и т.д.

Регистрация системы (System Registration)

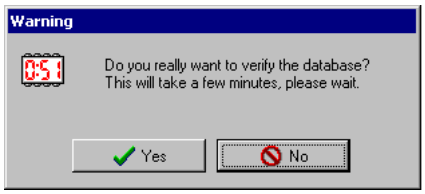
Это меню служит для регистрации новых системных приложений, например, KTES, рабочих станций APM, шлюзов, интерфейсов SmartLink и др., чтобы использовать их при работе с базами данных системы и чтобы установить связь между ними и сервером.



ПРИМЕЧАНИЕ: *Смотрите в Главе 2 :Установка программного обеспечения' на странице 9 для более подробной информации по установке и регистрации новых приложений.Перед началом установки новых приложений следует убедиться в наличии правильных серийных номеров, необходимых для установки.*

Проверка баз данных сервера и рабочих станций

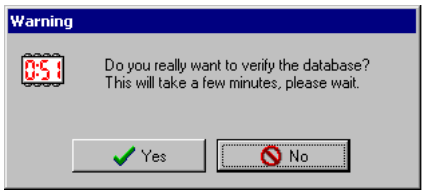
База данных сервера



1. На панели инструментов **Options** (Опции) нажать иконку **Server full database check** (Полная проверка базы данных на сервере). При этом должно открыться окно-предупреждение.
2. Нажать **Yes** (Да) для продолжения работы.

ПРИМЕЧАНИЕ: *Это поверхностная мера защиты. В случае возникновения серьёзных проблем следует запустить программу Database Utility через меню* **Start** (Пуск) *Windows®. Смотрите в Главе 16 Проверка целостности базы данных' на странице 517 для более подробной информации .*

База данных рабочей станции



1. На панели инструментов **Options** (Опции) нажать иконку **Workstation full database check** (Полная проверка базы данных рабочей станции). При этом должно открыться окно-предупреждение.
2. Нажать **Yes** (Да) для продолжения работы.

ПРИМЕЧАНИЕ: *Это поверхностная мера защиты. В случае возникновения серьёзных проблем следует запустить программу Database Utility через меню* **Start** *(Пуск) Windows®. Смотрите в Главе 16 Проверка целостности базы данных' на странице 517 для более подробной информации .*

Глава 15 • Сервер EntraPass

Сервер представляет собой специализированный компьютер, включённый в сеть, который организует доступ к базе данных системы управления. Он предназначен для получения и раздачи данных, полученных с различных шлюзов и рабочих станций, на которые приходит информация с подключённых контроллеров через лучи.

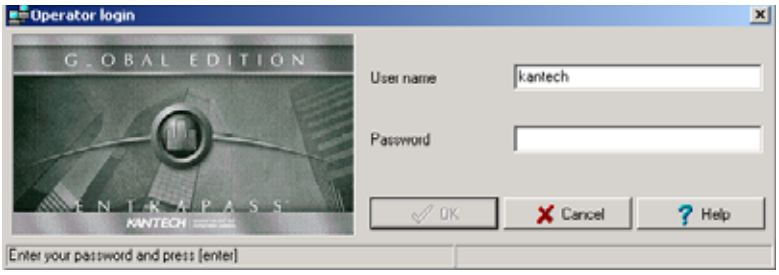
В определённых случаях для защиты данных в случае отказа основного сервера может использоваться резервный сервер с зеркальной базой данных (Redundant Server and a Mirror Database). Сервер EntraPass используется для следующих целей:

- отображение всех рабочих станций, подключенных к серверу, журналов системных событий и журнала ошибок
- регистрация новых подключений и дополнительных опций (рабочих станций, шлюзов, клиентских приложений и др.)
- создание и восстановление из резервных копий баз данных типа Data (Данные), Archive (Архивы), Time and Attendance (Учёт рабочего времени) и Video Event (Видеособытия).
- восстановление данных в базах данных: Data (Данные), Archives (Архивы), Time and Attendance (Учёт рабочего времени), Video Event (Видеособытия)
- проверка целостности баз данных
- выбор другого языка базы данных
- Очистка базы данных путём удаления записей, прикреплённых к окончательно удалённым данным

Запуск сервера

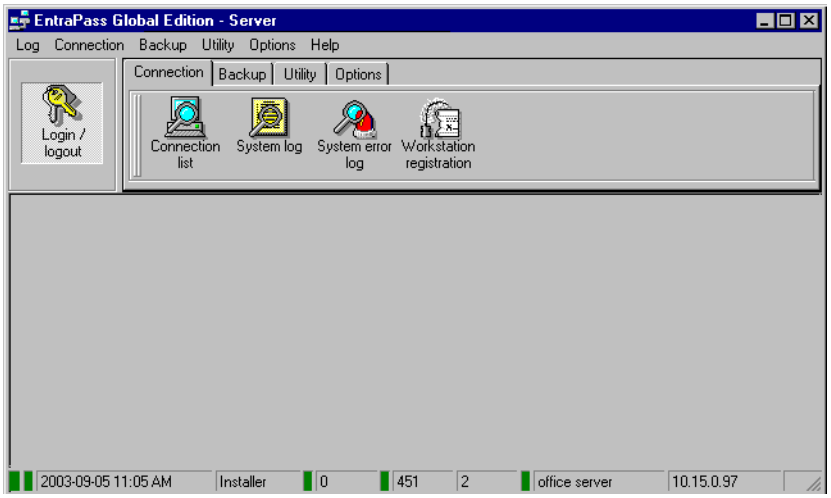
Для того чтобы получить доступ к командам управления сервером EntraPass, необходимо запустить сервер и зарегистрироваться в системе. При входе в систему операторы должны зарегистрироваться. Таким образом они получают доступ к тем разделам меню, которые соответствуют их уровню доступа, а также могут устанавливать связь и взаимодействовать с рабочими станциями. Однако для запуска сервера необязательно вводить свои регистрационные данные.

1 Достаточно в меню Пуск (Start) в операционной среде Windows® войти в меню All Programs (Все программы) > EntraPass **Global**> Server (Сервер) > Server (Сервер. Или запустить сервер щелчком мыши по ярлыку **Server** на рабочем столе (при его наличии). После окончания загрузки на экране появляется окно регистрации пользователя.



2 В окне **User name** следует указать имя пользователя, в окне **Password** нужно ввести пароль и нажать кнопку **OK** для продолжения. *Смотрите в Главе 12 Назначение операторов' на странице 402 для более подробной информации по изменению пароля .*

ПРИМЕЧАНИЕ: *Чтобы оператор мог регистрироваться на сервере, системный администратор должен установить флажок напротив опции "Allow login on server" (Разрешить регистрацию на сервере) при описании уровня доступа оператора (Operator security level). Смотрите в Главе 12 Назначение уровней безопасности' на странице 406 для более подробной информации .*



- В строке состояний в нижней части окна отображается статус соединения, цветные прямоугольные метки показывают статус логических или физических компонентов системы: **зелёный** означает, что связь в порядке, **красный** указывает на проблемы со связью, **фиолетовый** означает, что база данных заблокирована для аутентификации.
  - Статус доступности базы данных
  - Статус блокировки базы данных: становится красным, если база заблокирована
  - Системные дата и время
  - Регистрационное имя оператора, зарегистрированного в текущий момент на сервере
  - Число клиентских подключений, то есть число рабочих станций, подключённых к серверу
  - Количество записей в системных журналах (сообщений и событий)
  - Количество записей в журналах ошибок
  - Имя компьютера (NetbEUI), на котором установлен сервер
  - IP-адрес сервера

- Дополнительный IP-адрес, если резервный сервер с зеркальной базой данных осуществляет связь с сервером по протоколу TCP/IP и если их конфигурация настроена в системе
- Другие IP-адреса, если используются.

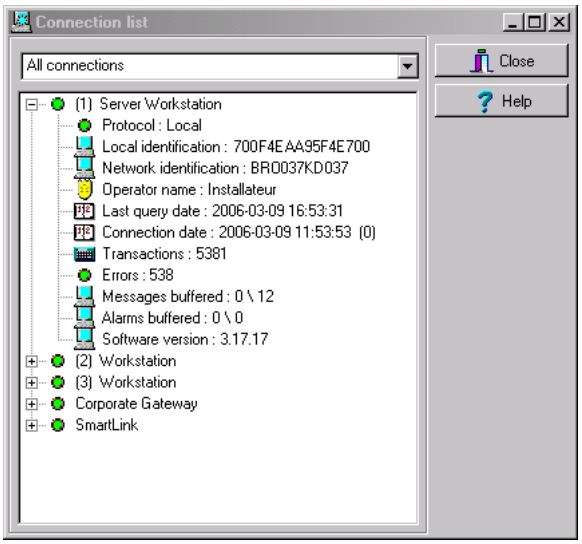
Список соединений сервера (Connection list)

Это меню позволяет операторам просматривать различные списки, отображающие текущее рабочее состояние соединения между сервером EntraPass и подключёнными к нему рабочими станциями.

Просмотр приложений, подключенных к серверу

У операторов есть возможность просматривать статус всех приложений Entrapass с помощью пользовательского интерфейса на рабочей станции или сервере.

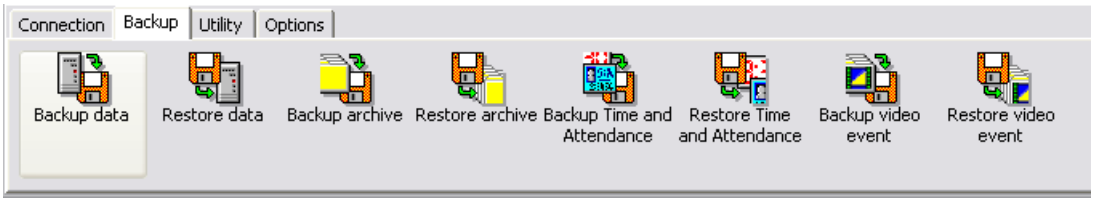
1 Из приложения Сервер (EntraPass Server) открыть закладку Connection (Соединения) и нажать иконку Connection List (Список соединений).



2 Чтобы просмотреть подробные сведения по каждой рабочей станции (коды регистрации, TCP/IP адреса, соединения, сообщения, хранящиеся в буфере, и др.), следует нажать знак плюса (+) рядом с названием рабочей станции.

Резервные копии

Панель инструметов Backup



Резервная копия – это такая копия базы данных системы, которая используется для замены оригинальной базы данных в случае отказа компьютера. Создание резервных копий позволяет защититься от случайной потери данных, например, в случае возникновения неисправности на жёстком диске или в результате случайной перезаписи или удаления данных. В случае отказа системы на одном компьютере появляется возможность восстановить резервную копию на другом компьютере (на котором установлено приложение Сервера EntraPass).

Раздел меню **Backup** предназначен для создания операторами в режиме ручного управления резервных копий системных данных (D), архивов (A) и данных по учёту рабочего времени (T). Кроме того, он служит для восстановления данных из резервных копий.

Полезные советы:

- Создавать резервные копии следует регулярно, не реже одного раза в неделю или чаще, если в базу данных часто вносятся изменения.
- Рекомендуется создавать по две резервных копии всех файлов базы данных. По соображениям безопасности их следует хранить в разных местах.
- Чтобы создать резервную копию файлов, можно воспользоваться одним из следующих способов:
  - меню программы резервного копирования EntraPass Backup или
  - программа EntraPass Backup Scheduler для создания автоматических расписаний или
  - другое программное и аппаратное обеспечение третьих производителей.

ПРИМЕЧАНИЕ: *По умолчанию, во время создания резервных копий или восстановления файлов база данных EntraPass временно недоступна. В строке состояний в главном окне приложения EntraPass второй прямоугольный индикатор статуса (в левом нижнем углу окна), отображающий статус базы данных, станет красным, что указывает на недоступность базы данных. Пока база данных не станет вновь доступной, изменения, сделанные на рабочих станциях, невозможно будет применить к базе.*

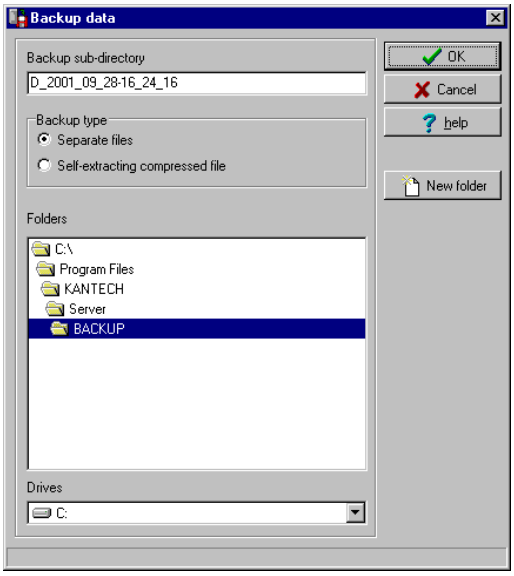
Все системны данные хранятся в файле по ссылке: C:\Program Files\Kantech\ Server_GE\XXXX. Если для создания резервных копий используется программа другого производителя, то рекомендуется выполнить резервное копирование всего директория Kantech и вложенных директориев.
Каждый раз при создании резервной копии (даже при её создании в автоматическом режиме) будет создаваться новая вложенная папка, содержащая данные или самораспаковывающийся файл. В случае создания резервных копий по инкрементному типу, чтобы восстановить данные, потребуется восстановить все вложенные папки последовательно друг за другом (начиная с самой древней).

Создание резервных копий типа D, A и T

По умолчанию имя вложенной папки для резервных копий генерируется автоматически по следующему правилу: X_YYYY_MM_DD_h_mm_ss, где 'X' = тип данных (данные – D, архивы – A, учёт рабочего времени – T), YYYY – год, MM – месяц, DD – день, h – часы, mm – минуты, ss – секунды. Рассмотрим порядок создания резервной копии на примере системных данных. Те же действия следует выполнять и при резервном копировании архивов или данных по учёту рабочего времени.

1. Выбрать тип данных для создания резервной копии: системные данные, архивы, учёт рабочего времени. В поле Backup sub-directory отображается имя вложенной папки, в которой будут

сохранены данные. Оператор может использовать имя папки по умолчанию или указать другой путь сохранения файла.



ПРИМЕЧАНИЕ: *По умолчанию система/рабочая станция создаёт резервные копии всех данных, находящихся в папках: C:\Program Files\Kantech\Server_GE\Data (данные) или Archive (архивы) или Time (учёт рабочего времени). Путь сохранения копии: C:\ProgramFiles\Kantech\Server_GE\Backup\X_YYYY_MM_DD-h_mm_ss, где X – тип данных. Кроме типа данных, название файла содержит год, месяц, день, а также время создания резервной копии.*

2 Указать тип резервного копирования:
- **Separate file** (Отдельные файлы) – базы данных будут копироваться последовательно друг за другом (стандартный режим). При копировании создаётся файл *Regdata.ini*, который содержит следующие идентификационные данные: программное обеспчение, используемое для создания резервной копии, тип резервной копии (данные/архивы/учёт рабочего времени), имя оператора, создающего копию, дата и время создания копии, а также версия ПО.
- **Self-extracting compressed file** (Самораспаковывающийся архив) – создание исполняемого файла (.exe) со сжатием данных для уменьшения места на диске, занимаемого резервными копиями. Резервная копия содержит следующие идентификационные данные: программное обеспчение, используемое для создания резервной копии, тип резервной копии (данные/архивы/учёт рабочего времени), имя оператора, создающего копию, дата и время создания копии, а также версия ПО.

ПРИМЕЧАНИЕ: *Для того чтобы использовать файл .exe по своему усмотрению для восстановления самораспаковывающегося файла резервной копии, следует убедиться, что системный код EntraPass совпадает с кодом, использованным в файле .exe, иначе ничего не получится. Если произошла поломка системы, в результате которой базы данных и приложения EntraPass перестали быть доступными, то настоятельно рекомендуется переустановить систему и восстановить данные, используя средства резервного копирования по назначению, вместо использования файла .exe по своему пониманию.*

3 В выпадающем списке **Drives** (Диски) указать диск, на который следует сохранить резервную копию. Список доступных дисков будет зависеть от настроек компьютера. Чтобы использовать при сохранении настройки по умолчанию, следует оставить всё без изменения.

4 Если необходимо создать новую папку, нажать кнопку **New folder** (Создать папку).

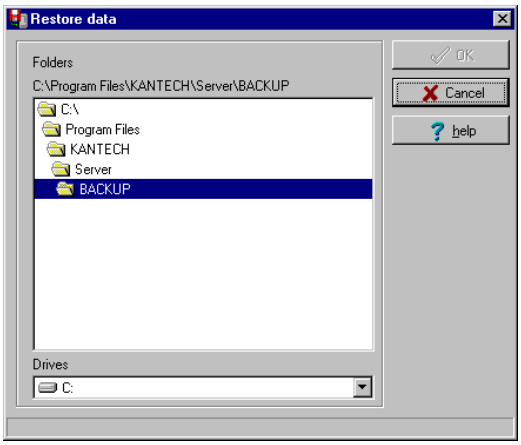
5 Нажать **OK,** чтобы запустить резервное копирование. Ход выполнения процесса копирования отображается в нижней части окна.

ПРИМЕЧАНИЕ: *Чтобы выполнять резервное копирование по расписанию или настроить автоматическое создание резервных копий, можно воспользоваться программой-планировщиком "Backup Scheduler". Смотрите в Главе 14 Опции системы EntraPass' на странице 469 для более подробной информации по настройке расписания автоматического резервного копирования. Во время создания резервных копий или восстановления файлов базы данных сервера временно недоступны. Нельзя изменять базы данных во время создания резервных копий.*

Восстановление данных (D, A и T)

Если возникает необходимость восстановить данные, необходимо перед началом этой операции создать резервную копию. Если для восстановления данных используется программа другого изготовителя, то рекомендуется выполнить восстановление всей папки Kantech и вложенных папок.

1 В меню **Backup** (Резервное копирование) нажать иконку **Restore** (Восстановить): **Data** (Данные)**, Archive** (Архивы)**, Time and attendance** (Данные по учёту рабочего времени). При этом должно открыться окно Restore data (Восстановить данные). В нём отображается путь для папки, где хранятся резервные копии.



2 Чтобы изменить путь, следует воспользоваться выпадающим списком **Drives**. Нажать **OK**, чтобы запустить процедуру восстановления данных.

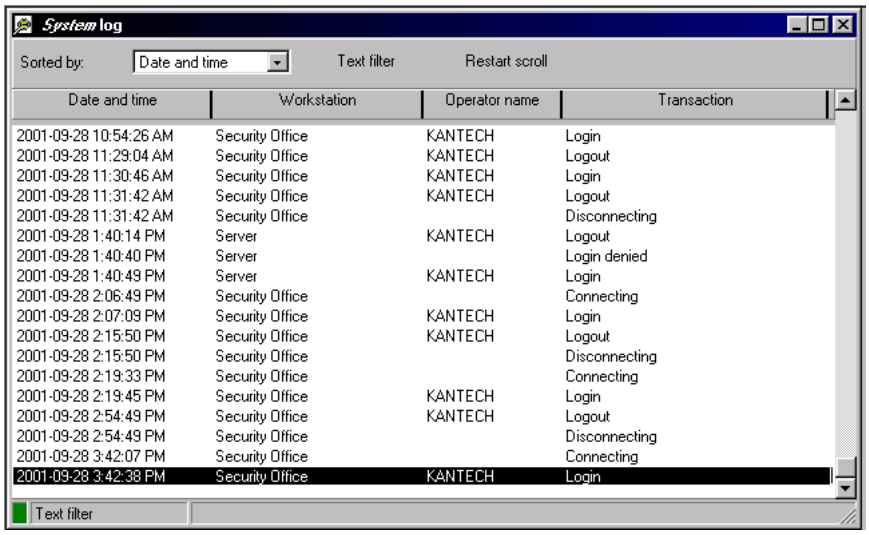
ПРИМЕЧАНИЕ: *По умолчанию система/рабочая станция восстанавливает все данные из файла C:\ProgramFiles\Kantech\Server_GE\Backup\ X_YYYY_MM_DD-h_mm_ss, где X – тип данных в папки: C:\Program Files\Kantech\Server_GE\Data (данные) или Archive (архивы) или Time (учёт рабочего времени).*

ПРИМЕЧАНИЕ: *Рекомендуется повторно загрузить шлюз после восстановления данных:* ***Operation*** *(Управление/Операции) >* ***Reload data*** *(Повторная загрузка данных).*

Просмотр журнала системных событий

Системный лог событий содержит все события о авторизациях и выходах из системы на всех АРМ, назначенных в системе. Журнал показывает дату, время, имя АРМ, имя оператора, тип оператора.

1 Для просмотра view system log (журнала системных событий), выберите иконку **View System Log** (просмотр журнала системных событий).



Date and time	Workstation	Operator name	Transaction
2001-09-28 10:54:26 AM	Security Office	KANTECH	Login
2001-09-28 11:29:04 AM	Security Office	KANTECH	Logout
2001-09-28 11:30:46 AM	Security Office	KANTECH	Login
2001-09-28 11:31:42 AM	Security Office	KANTECH	Logout
2001-09-28 11:31:42 AM	Security Office		Disconnecting
2001-09-28 1:40:14 PM	Server	KANTECH	Logout
2001-09-28 1:40:40 PM	Server		Login denied
2001-09-28 1:40:49 PM	Server	KANTECH	Login
2001-09-28 2:06:49 PM	Security Office		Connecting
2001-09-28 2:07:09 PM	Security Office	KANTECH	Login
2001-09-28 2:15:50 PM	Security Office	KANTECH	Logout
2001-09-28 2:15:50 PM	Security Office		Disconnecting
2001-09-28 2:19:33 PM	Security Office		Connecting
2001-09-28 2:19:45 PM	Security Office	KANTECH	Login
2001-09-28 2:54:49 PM	Security Office	KANTECH	Logout
2001-09-28 2:54:49 PM	Security Office		Disconnecting
2001-09-28 3:42:07 PM	Security Office		Connecting
2001-09-28 3:42:38 PM	Security Office	KANTECH	Login

2 Из выпадающего окна в пункте **Sorted by,** укажите критерий сортировки: системные сообытия будут отображаться в соответствии с вашими указаниями.
- **Date and time** (Дата и время)— Это нормальный критерий сортировки. Если вы выберите другой критерий, то вы нарушите настройки сортировки по умолчанию. После выбора критерия сортировки, нажмите на кнопку “restart scroll” “Перезагрузка отчета”.
- **Operator** (Оператор)—Когда выбрано, то все колонки будут отсортированы в соответствии с оператором, расположенные в алфавитном порядке.
- **Workstation** (АРМ)—Когда выбрано, все колонки будут сортированы по колонке **Workstation** (АРМ) в алфавитном порядке.
- **Text filter** (Текстовый фильтр)—Когда выделено, будет отображено новое окно. В этом окне введите текст. Система будет отображать вам события, содержащие указанный текст. Для возврата к нормальному режиму отображения нажмите на **text filter**.

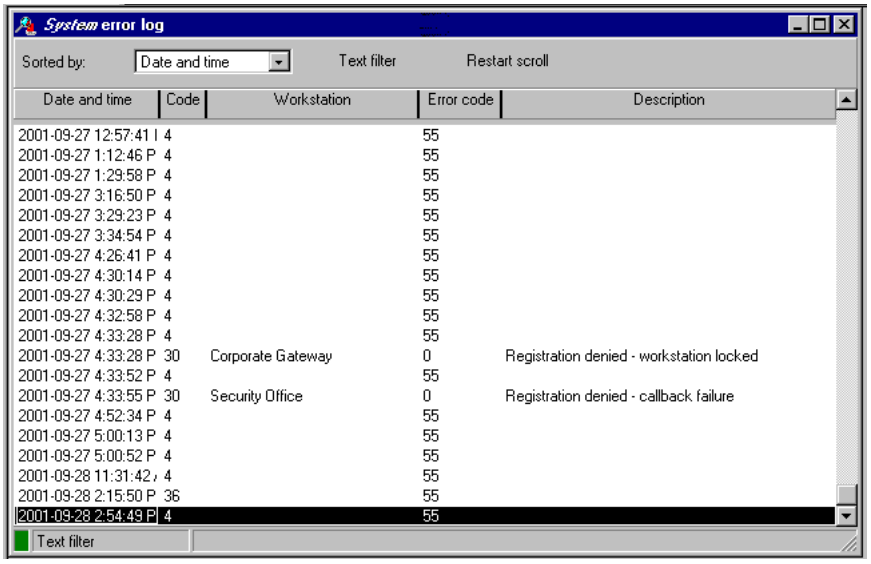
3 Вы можете изменить цвет подложки **background color**. Для того, чтобы это сделать, нажмите правой кнопкой мыши в окне и выберите цвет из списка.

4 Вы можете также очистить окно. Для того, чтобы сделать это, нажмите правой кнопкой мыши в окне, затем выберите пункт **Clear** (Стереть) из контекстного меню.

Просмотр журнала системных ошибок

Системные ошибки отображаются с датой и временей, именем АРМ, где произошла ошибка,с кодом ошибки и описанием.

1 Выберите пункт **View system errors** (просмотр системных ошибок) для просмотра всех ошибок, которые произошли в системе.



2 Вы можете нажать правой кнопкой мыши чтобы изменить задний цвет фона или очистить окно от всех данных, путем нажатия на иконку Clear (Очистить).

ПРИМЕЧАНИЕ: *Смотрите в Главе 2 Установка системы' на странице 14 для более подробной информации по регистрации системы.*

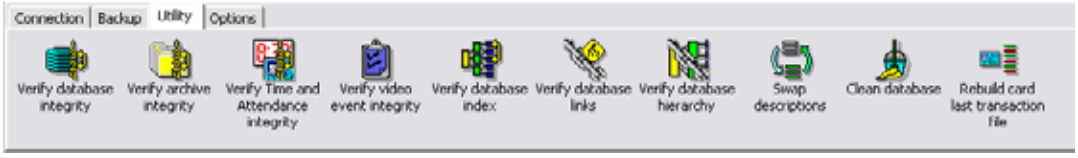
Регистрация системы

Это меню используется для регистрации новых компонентов системы, таких как KTES, APM, Шлюз, SmartLink, итд. Смотрите в Главе 14 Регистрация системы (System Registration)' на странице 503 для более подробной информации чтобы зарегистрировать системную базу данных и установить соединение с сервером.

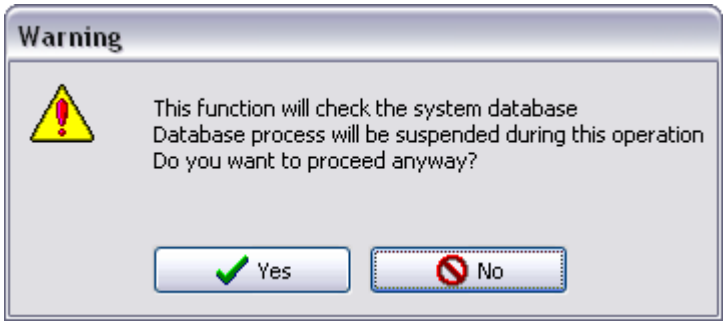
Утилиты сервера

Это меню предназначено для проверки целостности базы данных системы и для восстановления системных баз данных. Этот раздел меню доступен также и с рабочих станций. *Смотрите в Главе 16 Системные утилиты' на странице 515 для более подробной информации по системным утилитам.*

1 Открыть закладку **Utility** (Утилиты), чтобы использовать утилиты сервера.



2 Выбрать иконку на панели инструментов в соответствии с выполняемой задачей, например, **Verify database integrity** (Проверить целостности базы данных). На экране откроется соответствующее диалоговое окно.



3 Нажать кнопку **YES**. Система автоматически начинает процесс и отображает ход выполнения операции на экране.

ПРИМЕЧАНИЕ: *В некоторых окна могут быть доступны только кнопки **Yes** (Да) или **No** (Нет) вместо кнопки Rebuild.*

ПРИМЕЧАНИЕ: *При запуске утилиты Clean database (Чистка базы данных), предназначенной для очистки базы данных от ранее удалённых данных, так же появляются кнопки Yes и No.*

Глава 16 • Системные утилиты

В этом разделе собраны обслуживающие программы системы EntraPass. Эти программы доступны из меню **Start** (Пуск) Windows®. Перечисленные ниже программы запускаются с сервера или рабочей станции.

- **Database Utility** (Утилита базы данных). Служит для реиндексации архивных файлов, обновления полей базы данных, проверки архивных файлов, проверки целостности базы данных, проверки индекса базы данных, проверки ссылок и структуры базы данных при выключении сервера.
- **EntraPass Video Vault Application** (Приложение Видеохранилище) – программа предназначена для работы с архивами видеозаписей. Эта утилита обрабатывает запросы, поступающие от пользователей системы EntraPass, для просмотра архивных видеофрагментов и для управления архивированием видеоданных.
- **Express Setup** (Автоматическая установка). Программа служит для выбора конфигурации всех компонентов, имеющих отношение к шлюзу, включая тип используемых считывателей карт, способ соединения, число лучей/сайтов, число контроллеров на каждом луче и др.
- **KT-Finder** (Программа обнаружения устройств). Позволяет локально или удалённо настраивать конфигурацию IP-устройств Kantech, в том числе интерфейса Kantech IP Link, контроллера KT-400 на 4-х двери, а также сетевого контроллера связи KT-NCC (ПРИМЕЧАНИЕ).

ПРИМЕЧАНИЕ: *Сетевой контроллер KT-NCC доступен только с EntraPass Global Edition.*

- **PING Diagnostic** (Тестирование по методу "запрос-ответ"). Служит для диагностики неисправностей сети, связанных с прохождением сигнала.
- **Quick Report Viewer** (Программа просмотра быстрых отчётов). Позволяет оператору просматривать отчёты, не запуская EntraPass.
- **System Report Viewer** (Программа просмотра отчётов системы). Позволяет оператору просматривать отчёты, не запуская EntraPass. Эта утилита устанавливается из окна Setup.
- **Vocabulary Editor** (Редактор языков). Служит для перевода отображаемого на экране текста на язык, выбранный пользователем.
- **Workstation** (АРМ). Программа для конфигурации рабочей станции. Эта программа, схожая со стандартным приложением рабочей станции, позволяет администратору системы устанавливать конфигурацию логических и физических компонентов системы.
- **Migration Utility** (Утилита переноса данных). Служит для переноса информации из базы данных при обновлении системы с Special Edition на Corporate Edition или с Corporate Edition на Global Edition.
- **Интерфейс Oracle/MS-SQL** создаёт в реальном времени копию баз данных EntraPass по идентификационным картам на сервере MS-SQL или Oracle. Эта программа позволяет операторам изменять, добавлять или получать сведения по идентификационным картам в реальном времени, используя клиентскую версию MS-SQL или Oracle. База данных по идентификационным картам, содержащая информацию о владельцах карт и использующая интерфейс **MS-SQL Interface,** будет автоматически обновляться при появлении новых доступных данных в базе данных по картам в системе EntraPass.

ПРИМЕЧАНИЕ: *Программа* **MS-SQL Interface** *не поддерживается зеркальной базой данных и резервным сервером.*

- **SmartLink Interface** (Интерфейс SmartLink). Позволяет пользователям настраивать сообщения и формат данных, отправляемых на второй COM-порт или в файл на диске. Приложение SmarkLink позволяет обеспечивать взаимосвязь системы управления доступом EntraPass почти с любым интеллектуальным устройством, включая коммутаторы с видеоматрицами, системы персонального вызова (пейджеры) и т.п.
- **EntraPass Online Help** (Online помощь EntraPass)— Это та же самая информация как в инструкции. Только нажмите на клавишу (**? Help**), это сразу вызовет вам необходимую подсказку по этому разделу.

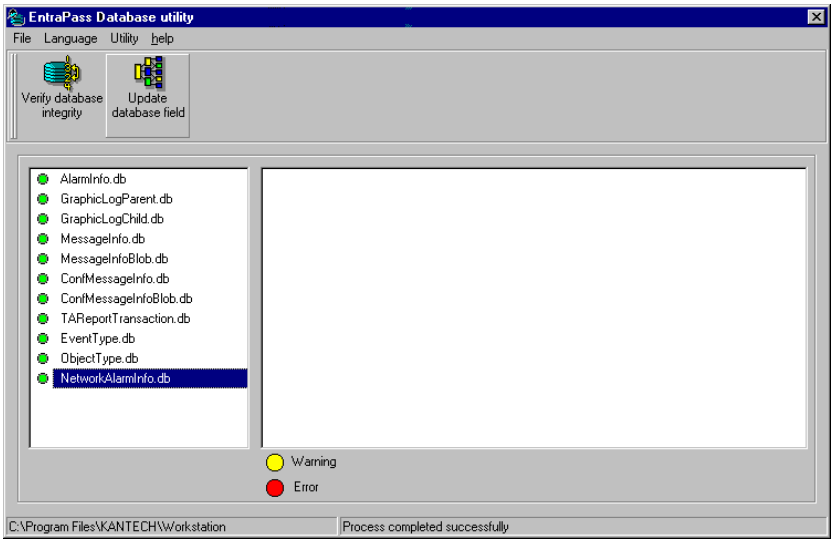
Утилиты базы данных

Программа Database utility проверяет целостность таблиц базы данных, которые используются для хранения событий, тревог, сетевых тревог и графических схем. Как правило, система сканирует все таблицы системной базы данных и исправляет ошибки (если их обнаруживает). Обычно система автоматически проверяет целостность базы данных во время процедуры запуска (на экране отображается сообщение системы). Если оператор не желает выполнять проверку базы данных при запуске, эту операцию можно запустить позже при помощи программы Database Utility. Кроме того, запуск этой программы может понадобиться, например, в случае часто повторяющихся проблем с системой. Процедуру необходимо выполнить и в случае не слишком частого использования системы, поскольку базы данных системы недоступны во время работы с базами данных. Во время некоторых проверок, например, реиндексации архивных файлов, обновления полей базы данных, проверки архивных файлов или смене языков базы данных необходимо, чтобы приложения EntraPass были закрыты. После этого можно запускать утилиту Database utility. При попытке запуска процесса, который требует закрытия приложений, оператор получает предупреждение о том, что доступ к базе данных во время этого процесса будет закрыт.

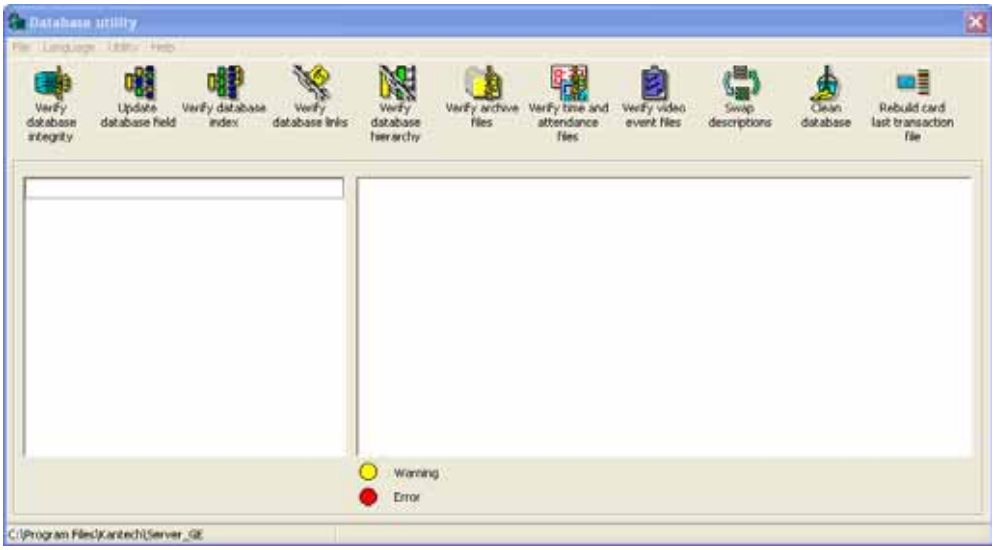
ПРИМЕЧАНИЕ: *Сервер EntraPassСервер EntraPass должен быть выключен до запуска утилиты.*

Запуск приложения Database utility

1 Для запуска утилиты можно использовать иконки под закладкой **Utility** (Утилиты) в приложении сервера EntraPass или запустить утилиты через меню **Start** (Пуск) Windows® > **All Programs** (Все программы) > **EntraPass Global Edition** > **Workstation** (Рабочая станция) > **Database Utility** (Утилиты базы данных).



ПРИМЕЧАНИЕ: *При использовании меню **File** (Файл) > **Workstation** (Рабочая станция) система отображает только две иконки: **Verify database integrity** (Проверить целостность базы данных) и **Update database fields** (Обновить поля базы данных). Меню **File > Server** предоставляет больше возможностей.*



Проверка целостности базы данных

1 Нажать на панели инструментов кнопку **Verify database integrity** (Проверить целостность базы данных). Сделать выбор, какую проверку делать: быструю **quick** или полную **complete**.
   - **Quick check** (Быстрая проверка). Выполняется сканирование таблиц базы данных, но не отображается подробный отчёт после окончания проверки.
   - **Complete check** (Полная проверка). Выполняется сканирование таблиц базы данных и отображается подробный отчёт после окончания проверки.

Обновление полей базы данных (Update Database Fields)

Эта функция выполняется автоматически, когда оператор выполняет обновление программного обеспечения. Если оператор восстанавливает базу данных (**Server** (Сервер) > панель инструментов **Options** (Опции) > **Restore** (Восстановить)), то поля базы данных автоматически обновляются при восстановлении информации. Даже при восстановлении базы данных не с сервера (копированием базы данных при помощи чужой программы резервного копирования) эта функция автоматически выполняется во время следующего запуска сервера.

1 В окне Database utility (Утилита для работы с базами данных) нажать на иконку **Update database field** (Обновить поля базы данных).

ПРИМЕЧАНИЕ: *Использование этой функции может понадобиться, например, в случае возникновения проблем при запуске сервера или рабочей станции. Если система не запускается, причиной могут быть проблемы с базой данных, когда источник и структура базы не совпадают.*

Проверка индекса базы данных (Verify Database Index)

Программа **Verify database Index** позволяет полностью восстановить индексы баз данных, используя информацию, которая была скопирована в основные базы данных, и группируя её для восстановления базы данных Registry.DB. Последнее позволяет увеличить производительность системы.

ПРИМЕЧАНИЕ: *Эту программу можно использовать в тех случаях, когда база данных повреждена, и не была создана резервная копия.*

Проверка ссылок базы данных (Verify Database Links)

Утилита Verify Database Links (Проверка ссылок базы данных) предназначена для восстановления всех ссылок в базе данных. Помимо этого, данная программа очищает базы данных, удаляя ссылки, которые уже не действуют. Например, если для одного из компонентов было назначено расписание, которое затем было удалено, то система установит в исходное состояние то поле, которое было для этого использовано в основной базе данных. Кроме того, будут удалены те записи, которые указывают на удалённые компоненты. Например, если для шлюза был назначен определённый уровень доступа, который был затем удалён, то эта запись будет удалена из базы данных. Утилита

Verify Database Links позволяет полноценно работать со ссылками между компонентами и обеспечивает корректное отображение данных при выполнении следующих действий:

- Просмотр структуры ссылок компонентов на все другие компьютеры системы,
- Удаление всех следов компонента в базе данных, если этот компонент был окончательно удалён. Например, после удаления расписания система будет использовать список ссылок, чтобы восстановить исходное состояние всех полей базы данных, в которых было записано это расписание.

ПРИМЕЧАНИЕ: *Данная программа может оказаться полезной, если обнаружено, что ссылки базы данных работают некорректно. Она может помочь и в случае, например, некорректного выхода из системы.*

Проверка ирархической структуры базы данных (Verify Database Hierarchy)

В системе EntraPass база данных имеет иерархическую структуру, то есть все компоненты имеют родительские и дочерние элементы. Функция Verify database hierarchy (Проверка иерархической структуры базы данных) предназначена для восстановления связей между родительскими и дочерними элементами внутри базы данных. Если база данных имеет серьёзные повреждения, то результаты работы этой программы будут скромными.

ПРИМЕЧАНИЕ: *Если пользователь пытается получить доступ к контроллеру, указывая шлюз и сайт, а результаты не соответствуют реальности, то это указывает на повреждение иерархической структуры базы данных. Устранить эти проблемы можно при помощи утилиты Verify database hierarchy. Если это не помогает, значит, база данных слишком сильно повреждена, чтобы её можно было восстановить с помощью этой утилиты. В таком случае необходимо восстановить базу данных полностью при помощи backup.*

Проверка архивных файлов базы данных (Verify Database Archive Files)

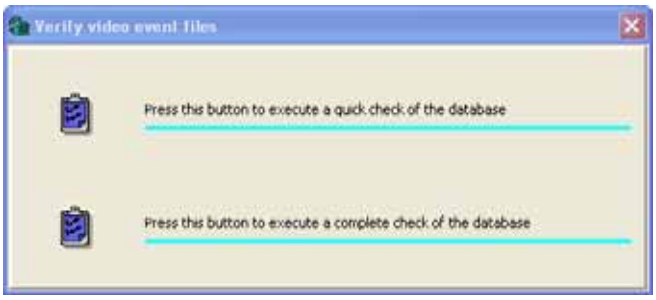
This function is used to verify archive files. It assigns a new unique sequential value to all primary indexes of archive files.

Проверка файлов по учёту рабочего времени (Verify Time & Attendance Files)

Эта функция предназначена для проверки файлов базы данных по учёту рабочего времени. Она назначает новое уникальное порядковое значение для всех исходных индексов файлов в базе данных по учёту рабочего времени.

Проверка файлов видеособытий (Verify Video Event Files)

Эта функция используется для проверки файлов видеособытий. Она назначает новое уникальное порядковое значение для всех исходных индексов файлов видеособытий. В зависимости от того, сколько видеофайлов в базе данных, оператор может выбрать быструю (**quick**) или полную (**complete**) проверку базы данных. При большом количестве файлов рекомендуется сначала выполнить быструю проверку (**quick check of the database**), и в случае обнаружения ошибок перейти к полной проверке базы данных (**complete check of the database**).



Замена описаний (Swap Descriptions)

Эта функция предназначена для того, чтобы поменять местами или заменить описания баз данных.

Очистка базы данных (Clean the Database)

Данная функция используется, чтобы окончательно удалить записи в базе данных, которые были отмечены для удаления. Большинство таких записей относятся к картам и хранятся в разделе Deleted Components (Удалённые компоненты) в базе данных. Данная опция позволяет значительно уменьшить место на диске, занимаемое базой данных. Кроме того, она улучшает работу системы, особенно при поиске информации по идентификационным картам. Эта функция никак не действует на таблицу реестра (Registry) и никак не влияет на содержание архивных отчётов.

ПРИМЕЧАНИЕ: *Перед выполнением данной операции настоятельно рекомендуется создать резервную копию базы данных! Функция* ***Clean database*** *приостанавливает работу базы данных во время выполнения её очистки.*

Восстановление файлов по последней транзакции с картой (Rebuild Card Last Transaction Files)

Эта функция предназначен для восстановления файлов по последней транзакции с картой.

Видеохранилище (EntraPass Video Vault)

Приложение Видеохранилище (EntraPass Video Vault) предназначено для удовлетворения потребностей пользователей в удобном хранении видеоинформации и организации архивов. Это приложение предоставляет простой способ сбора важных видеоданных для дальнейшего их использования. Как известно, видеозаписи имеют ограниченный ресурс, который зависит от настроек видеосервера и его возможностей. Поскольку видеофайлы занимают много места на диске, применение системы архивации данных типа EntraPass Video Vault позволяет лучше организовать хранение и облегчить извлечение файлов из архива. Видеохранилище EntraPass Video Vault предоставляет пользователям следующие возможности:

- Просмотр состояния запросов по архивированию видеоданных
- Мониторинг состояния видеосерверов, связанных с активным приложением EntraPass Video Vault
- Мониторинг журналов загрузки видеоданных
- Архивирование видеофрагментов

Видеохранилище EntraPass Video Vault обрабатывает видеофрагменты следующих типов:

- инициированные автоматически
- инициированные вручную
- инициированные видеосервером
- экспортированные с меткой для архивирования

ПРИМЕЧАНИЕ: *Для использования видеохранилища EntraPass Video Vault требуется дополнительная лицензия. Система EntraPass позволяет установить несколько приложений EntraPass Video Vault. Каждое видеохранилище должно быть настроено для работы с системой EntraPass:* **Devices** (Устройства) > **EntraPass Applications** (Приложения EntraPass).

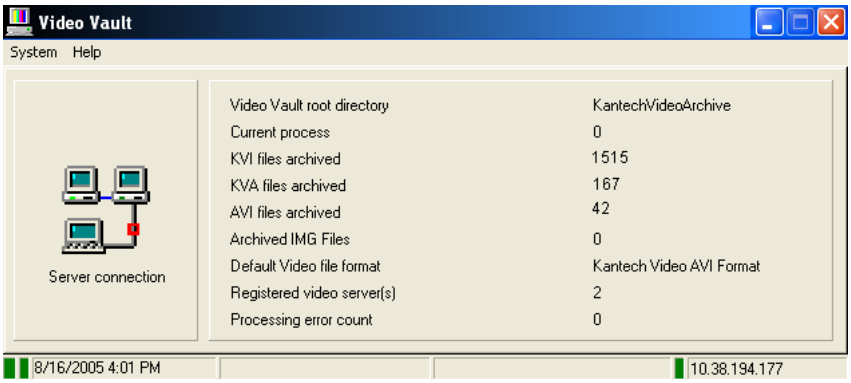
Установка видеохранилища EntraPass Video Vault

Для установки приложения EntraPass Video Vault требуется дополнительная лицензия. *Смотрите в Главе 2 Дополнительные компоненты системы EntraPass' на странице 23 для более подробной информации* по установке видеохранилища.

Запуск видеохранилища EntraPass Video Vault

Во время запуска приложение EntraPass Video Vault пытается обратиться к серверу EntraPass. Если запуск выполняется впервые, то может потребоваться ввод IP-адреса сервера (EntraPass Server). Кроме того, необходимо помнить, что запускать видеохранилище следует только после того, как будет запущен сервер.

1 Запустить приложение EntraPass Video Vault, используя контекстное меню на рабочем столе или меню **Start** (Пуск) операционной среды Windows®.

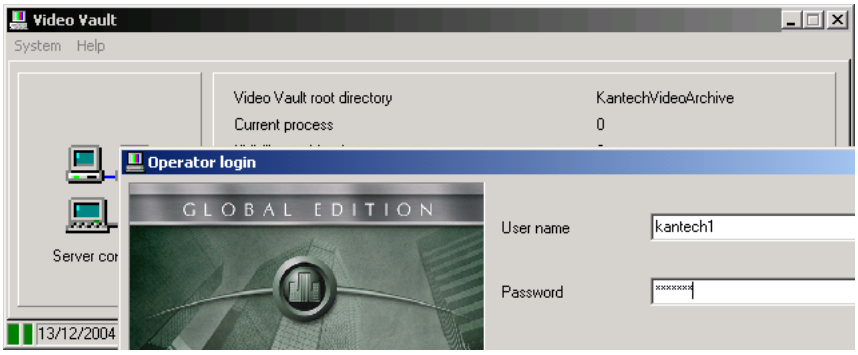


- **Video Vault root directory** (Корневой каталог видеохранилища) – папка, используемая по умолчанию для хранения видеофрагментов. Корневую папку видеохранилища указывают при настройке приложения в среде EntraPass: **EntraPass workstation application** (Приложение типа Рабочая станция) > **Devices** (Устройства) > **EntraPass Applications** (Приложения EntraPass) > **EntraPass Video Vault** (Видеохранилище). По умолчанию используется корневая папка: C:\Kantech Video Vault.

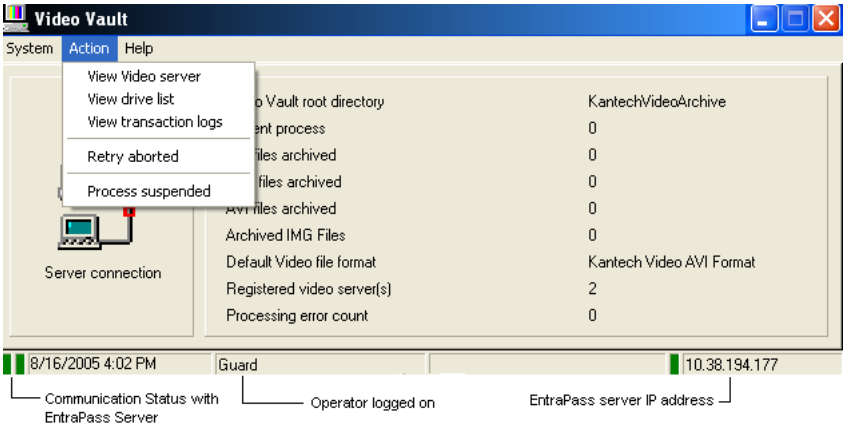
- **Current process** (Текущие процессы) – отображает число видеофрагментов, которые в текущий момент извлекаются для целей архивации.
- **(KVI, KVA, AVI, IMG) files archived** (Архивированные файлы) – показывает число видеофайлов, извлечённых приложением EntraPass Video Vault.
- **Default Video file format** (Формат архивируемых видеофайлов по умолчанию). Это формат, выбранный при настройке параметров архивирования видеоданных для видеохранилища: **EntraPass workstation application** (Приложение типа Рабочая станция) > **Video** (Видео) > **Video server** (Видеосерверы) > закладка **Video Vault Parameters** (Параметры Video Vault).
- **Registered Video Server(s)** (Зарегистрированные видеосерверы) – указывает число видеосерверов, связанных с активным приложением EntraPass Video Vault. Связь между видеохранилищем и видеосервером устанавливается при настройке видеосервера: **EntraPass workstation application** (Приложение типа Рабочая станция) > **Video** (Видео) > **Video server** (Видеосерверы) > закладка **Video Vault Parameters** (Параметры Video Vault).
- **Processing error count** (Число ошибок обработки данных) – показывает количество неудачных операций архивирования видеоданных. Чтобы определить причину незавершения процесса следует войти в меню **Video Vault** (Видеохранилище) > выбрать в меню пункт **Action** (Действие) > **Video Server List** (Список видеосерверов). Меню **Action** доступно только при условии правильного ввода имени пользователя (User name) и пароля (Password). Неудачно выполненные операции по архивированию файлов можно повторно запустить из меню Video Events List: **EntraPass workstation application** (Приложение типа Рабочая станция) > **Video** (Видео) > **Video Events List** (Список видеособытий).

Работа с архивированными видеофрагментами

1 В главном окне Video Vault войти в меню **System** (Системные настройки) > **Login** (Регистрация), чтобы выполнить запуск видеохранилища и ввести свои регистрационные данные.

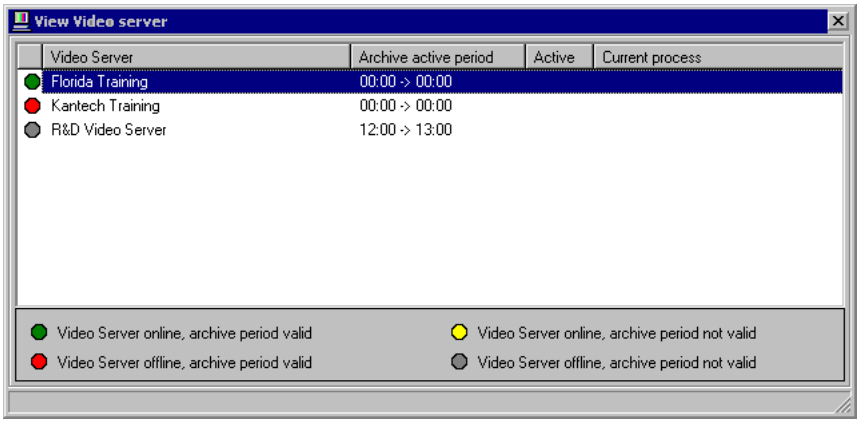


2 Указать имя пользователя в поле **User name** и пароль в поле **Password** для работы с видеохранилищем. Нажать **OK**, чтобы закрыть окно регистрации операторов Operator login. Использование одного и того же имени пользователя и пароля для одновременной регистрации в двух приложениях EntraPass недопустимо! Если пользователю необходимо одновременно работать с видеохранилищем EntraPass Video Vault и сервером EntraPass, он должен зайти туда под разными именами.



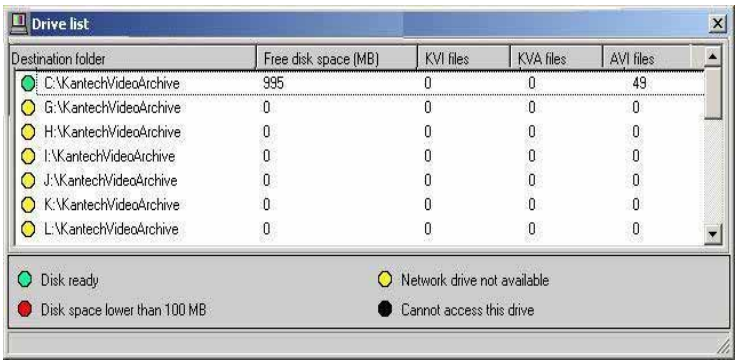
ПРИМЕЧАНИЕ: *Чтобы увидеть более подробную информацию по статистическим данным, отображаемым в главном окне, следует зарегистрироваться в приложении Видеохранилище.*

3 Для просмотра списка видеосерверов, связанных с видеохранилищем EntraPass Video Vault, и проверки статусов операций архивирования следует зайти в меню **View Video server** (Посмотреть видеосерверы).



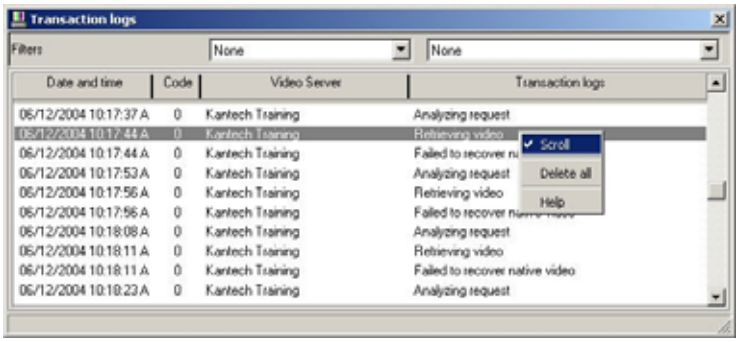
- **Video server on line, archive period valid** (Видеосервер подключён, период архивирования достоверен). В этот период сервер EntraPass извлекает видеофрагменты с видеосервера и выстраивает их для архивирования с помощью видеохранилища EntraPass Vault. Архивированию подлежат все видеофрагменты, запись которых была сделана в результате инициирующего события (автоматически или вручную), и которые были отмечены в списке Video Event List (Список видеособытий) меткой архивирования.
- **Video server offline, archive period valid** (Видеосервер отключён, период архивирования достоверен) – этот статус отмечен красным флажком. Это означает, что сервер EntraPass не может извлечь видеофрагменты с видеосервера по какой-либо причине. Видеофрагменты, записанные в этот период, не будут доступны для видеохранилища.
- **Video server online, archive period not valid** (Видеосервер подключён, период архивирования не достоверен).
- **Video server offline, archive period not valid** (Видеосервер отключён, период архивирования не достоверен).

4 Чтобы посмотреть список дисков, на которых хранятся архивные данные, выбрать в меню пункт **View drive list** (Посмотреть список дисков). Окно Drive list отображает статус всех файлов, извлечённых видеохранилищем EntraPass Video Vault с Intellex.



- Disk ready (Диск готов)
- Disk space lower than 100 MB (Места на диске менее 100 Мб)
- Network drive not available (Сетевой диск недоступен)
- Cannot access this drive (Нет доступа к диску)

5 Чтобы увидеть список ошибок, возникших при выполнении операций, выбрать меню Transaction log (Журнал транзакций).



ПРИМЕЧАНИЕ: *В журнале транзакций отображаются все транзакции, произошедшие с момента последнего запуска программного обеспечения. Поля Filters (Фильтры) позволяют вывести на экран не все транзакции, а только определённого типа, указанного пользователем.*

Редактор языков (Vocabulary Editor)

Vocabulary Editor (Редактор языков). Служит для перевода отображаемого на экране текста на язык, выбранный пользователем. Система EntraPass предоставляет возможность добавлять до 99 языков с целью замены языка, на котором выдаётся текст в графическом интерфейсе пользователя. Однако это программное обеспечение работает только с двумя языками одновременно, один из них называется "основным" (primary), а другой "дополнительным" (secondary). Для того чтобы программы работали на любых других языках, помимо английского (English), французского (French), немецкого (German), итальянского (Italian) или испанского (Spanish), необходимо сделать перевод всех слов на выбранный язык. Затем следует интегрировать переведённый словарь в программное обеспечение.

Создание нового языка выполняется в три этапа:

- Перевод исходного текста,
- Интеграция нового созданного словаря в словарь на сервере EntraPass,
- Распространение нового пользовательского словаря на все приложения

ПРИМЕЧАНИЕ: *Чтобы работать в системе с новым языком, необходимо, чтобы операционная среда (Windows®) поддерживала этот язык. В частности, клавиатура компьютера и экран (дисплей) должны поддерживать специальные символы, используемые в языке созданного словаря. Также должны поддерживать язык нового словаря и те компьютеры, на которых работают приложения EntraPass. Более подробную информацию о поддерживаемых языках можно получить у системного администратора.*

Установка редактора языков (Vocabulary Editor)

EntraPass Vocabulary Editor является автономной программой. Её можно установить и использовать независимо от других программ EntraPass. Чтобы перевести интерфейс системы на другой язык, необходимо установить программу Vocabulary Editor и перевести при помощи этой программы все слова из базы данных словаря.

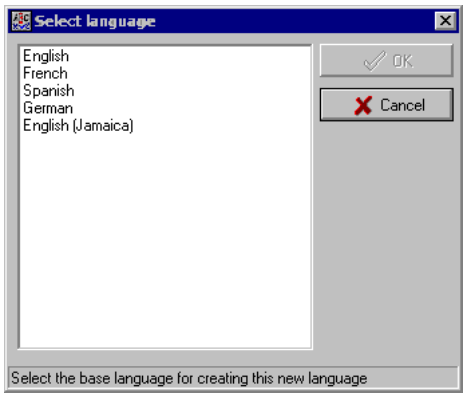
ПРИМЕЧАНИЕ: *Для установки редактора языков Vocabulary Editor не требуется приобретение дополнительной лицензии. Её можно запустить из окна настройки Setup. Смотрите в Главе 2 Установка системы' на странице 14 для более подробной информации .*

Перевод словаря системы на другой язык

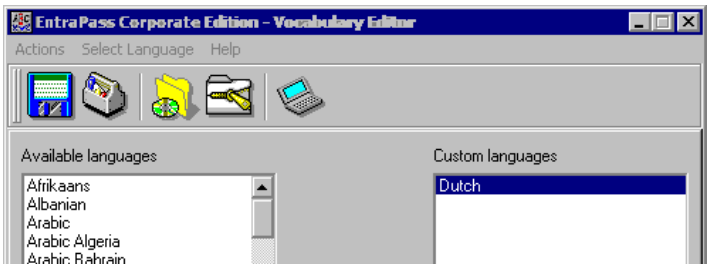
EntraPass Vocabulary Editor является автономной программой. Для её запуска не требуется запускать программное обеспечение EntraPass. Программа Vocabulary Editor поможет перевести программное обеспечение на любой язык, помимо имеющихся английского (English), французского (French), немецкого (German), итальянского (Italian) и испанского (Spanish).

1 Для запуска программы Vocabulary editor перейти в меню **Start** (Пуск) в операционной среде Windows® : нажать **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Global Edition** (Система EntraPass) > **Vocabulary Editor** (Редактор языков) > **Vocabulary Editor** (Редактор языков).

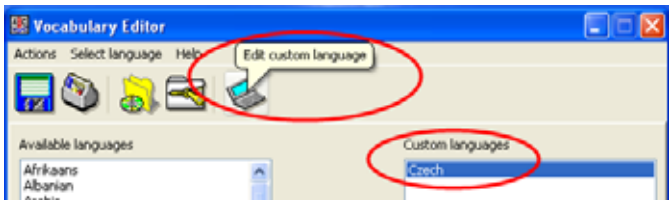
2 В списке доступных языков **Language list** найти название создаваемого языка и нажать кнопку **New** (Создать). Система снова откроет окно **Select language** (Выбор языка).

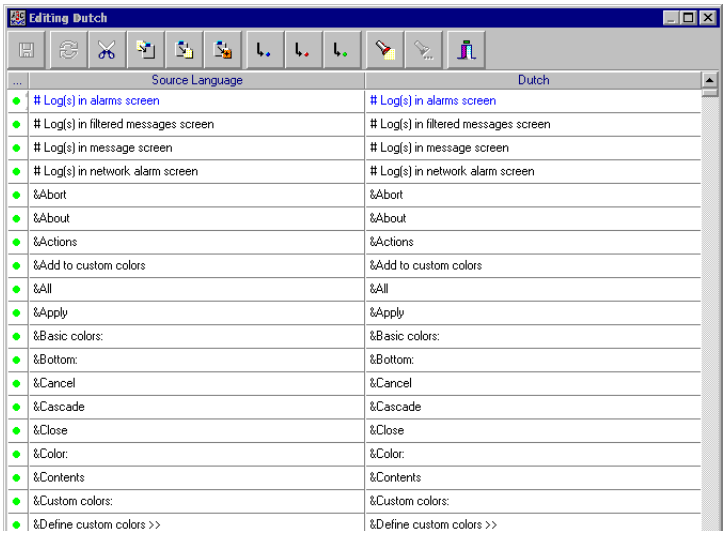


3 В списке языков найти язык для перевода, и нажать **OK**. Новый выбранный язык будет отображаться справа в колонке **Custom Languages** (Пользовательские языки).



4 Выберите Пользовательский язык из вкладки “**Custom Language”** (Пользовательский язык)**.** Затем нажмите кнопку **Edit custom language** (Правка пользовательского языка) для начала перевода. Система отобразит базу данных словаря.





ПРИМЕЧАНИЕ: *Настоятельно рекомендуется регулярно создавать резервные копии папок, в которых хранятся файлы пользовательского словаря (C:\ProgramFiles\Kantech\Vocabulary Editor\CustomDictionary\files.xxx.ath) или C:\ProgramFiles\Kantech\"Application type"\CustomDictionary\files.xxx.0.*

Ниже в таблице приведены пояснения к цветовой кодировке, используемой в программе Vocabulary Editor.

Цветовые коды программы VOCABULARY EDITOR	Описание
Зелёный	Достоверная текстовая строка
Синий/Зелёный	Новая текстовая строка
Красный	Устаревшая текстовая строка

- Колонка "Source language" (Язык исходного текста) содержит текст на основном языке, который был указан при создании словаря. Эта колонка служит "исходником", с которого выполняется перевод. Колонки, содержащие элементы программного обеспечения, не подлежат изменению пользователем.
- Правой кнопкой мыши вызвать контекстное меню или использовать панель инструментов **Language editor.** Если поместить курсор мыши на кнопку, появляется подсказка.

Интегрирование пользовательского языка в систему EntraPass

После завершения перевода необходимо интегрировать новый пользовательский словарь в словарь системы, чтобы системные операторы могли пользоваться им. Нижеуказанная таблица описывает действия с блоком словаря **vocabulary editor**. Данные опции могут быть также выбраны из меню **Actions** (Действие).

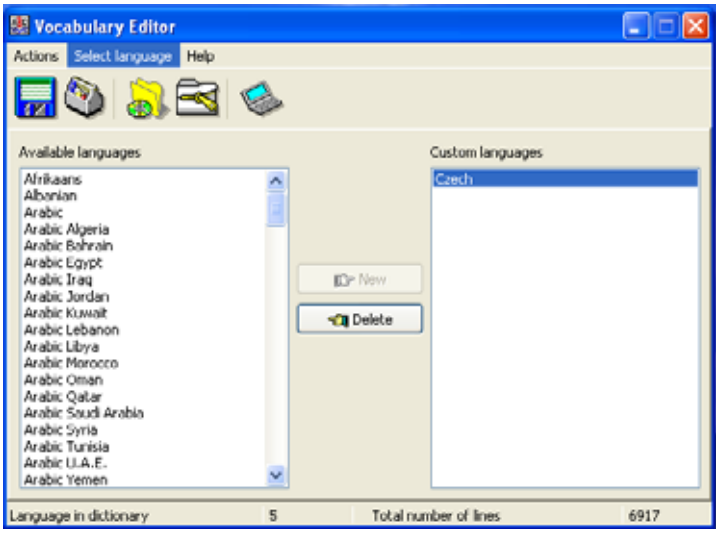
Иконка	Описание
	Apply changes to operational dictionary (Применить изменения к рабочему словарю): эта опция полезна, когда вы хотите протестировать ваши изменения до включения обновления на другие APM .
	Restore operational vocabulary (восстановить словарь): это опция позволяет пользователю просто установить язык по умолчанию. Система создает самораспаковывающийся файл, который восстанавливает оригинальный язык системы

Иконка	Описание
	Scan dictionary for new entries (сканировать словарь на новые изменения): эта опция полезна, когда вы обновляете версию программного обеспечения.
	Create self-extracting file for update (Создать самораспаковывающийся файл для обновления)**:** если вы решите создать новый файл словаря для обновления. Система создает файл **Updatedictionary.exe**. Система просит вас выбрать папку назначения для этого файла.

1 Запустить редактор языков (Vocabulary Editor). Панель инструментов в окне Vocabulary Editor содержит пять кнопок.

ПРИМЕЧАНИЕ: *Графический интерфейс пользователя (Graphic User Interface) будет отображаться только в одном из следующих пяти языков: английском (English), французском(French), немецком (German), итальянском (Italian) или испанском (Spanish).*

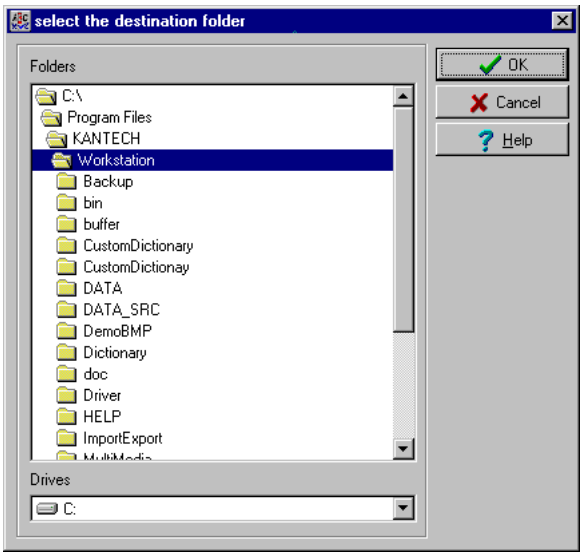
2 Выбрать созданный/переведенный словарь.



- Вы можете выбрать опцию: **Apply changes to operational dictionary** (Применить изменения к рабочему словарю): эта опция полезна, когда вы хотите протестировать ваши изменения до включения обновления на другие APM .
- Вы можете выбрать опцию: **Restore operational vocabulary** (восстановить словарь): это опция позволяет пользователю просто установить язык по умолчанию. Система создает самораспаковывающийся файл, который восстанавливает оригинальный язык системы
- Вы можете выбрать опцию: **Create self-extracting file for update** (Создать самораспаковывающийся файл для обновления)**:** если вы решите создать новый файл словаря для обновления. Система создает файл **Updatedictionary.exe**. Система просит вас выбрать папку назначения для этого файла.

3 Чтобы применить новый словарь, выбрать меню **Actions** (Действия) и выбрать опцию **Create self-extracting file for update** (Создать самораспаковывающийся файл для обновления). Система создаёт файл **Updatedictionary.exe** и предлагает указать папку для сохранения файла:

4 Указать папку для сохранения файла **Updatedictionary.exe**. По умолчанию самораспаковывающийся файл будет сохранён в папку C:\Program Files\Kantech (приложение).



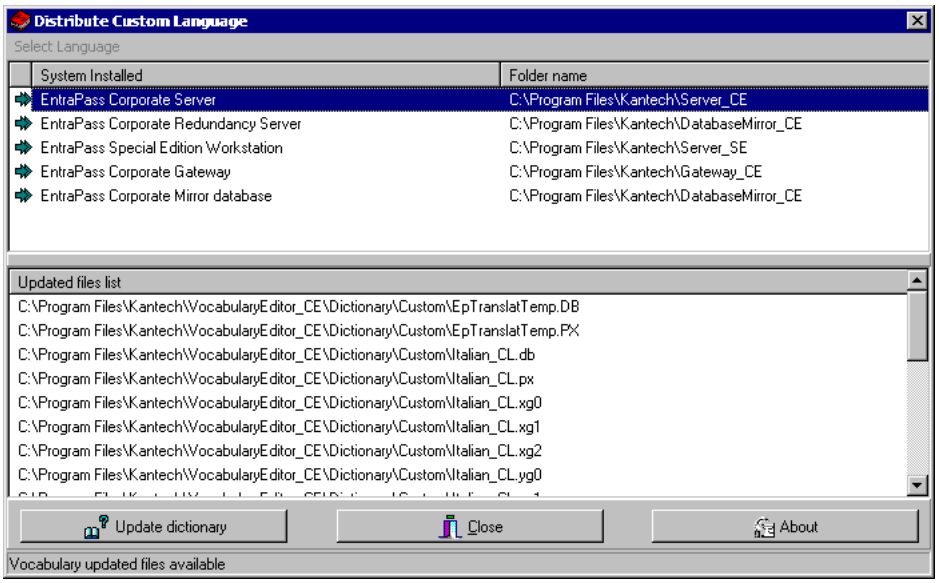
ПРИМЕЧАНИЕ: *Рекомендуется скопировать файл Updatedictionary.exe в сетевую папку, если необходимо, чтобы операторы имели доступ к этому файлу для обновления своего ПО.*

Распространение нового словаря между пользователями

Запускать файл можно только после выхода из всех программ EntraPass; иначе это действие выполнено не будет. Чтобы обновить словарь системы, сначала необходимо обновить сервер EntraPass. В случае наличия зеркальной базы данных (Mirror database) её необходимо закрыть перед выключением сервера (чтобы она не запустила резервный сервер после выключения основного). После выключения приложения Mirror database следует выключить основной сервер (Primary server), обновить его и снова запустить. Обновить зеркальную базу данных и резервный сервер, затем снова запустить её.

Обновление словаря системы

1 Выйти из всех программ Entrapass.
2 Запустить **Windows Explorer®** > **Kantech** > (**приложение EntraPass**), затем скопировать **Updatedictionary.exe** на сервер.
3 Запустить файл **Updatedictionary.exe** двойным щелчком мыши. Система выведет на экран приложения Entrapass, установленные на компьютере.



4 Выделить каждое приложение и нажать кнопку **Update dictionary** (Обновить словарь).

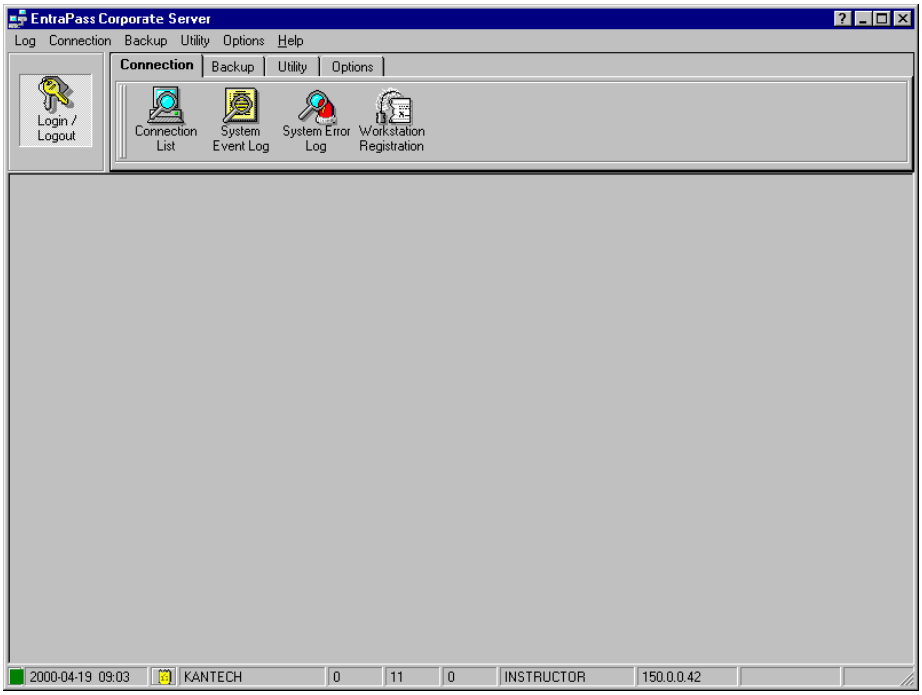
5 Файл **Updatedictionary.exe** необходимо скопировать на каждый компьютер, на котором установлено программное обеспечение EntraPass, и затем запустить его двойным щелчком мыши, чтобы выполнить обновление языков. Перед запуском самораспаковывающегося файла следует обязательно выйти из всех приложений EntraPass.

6 Выбрать приложение, которое необходимо обновить (последовательно по одному), и нажать кнопку **Update dictionary** (Обновить словарь). Система автоматически скопирует словарь в папку **Custom Dictionary** (Пользовательские словари) и объединит пользовательский словарь со словарём приложения.

ПРИМЕЧАНИЕ: *Обязательно* ***ДОЛЖНЫ*** *быть обновлены все приложения системы.*

ПРИМЕЧАНИЕ: *Если необходимо вернуться к настройкам словаря по умолчанию, следует выполнить те же действия, что и для обновления словаря.*

7 После завершения обновления базы данных словарей для основного сервера (Primary Server) и зеркальной базы данных (Mirror Database) с резервным сервером (Redundant Server) следует запустить основной сервер. server.



8 Выбрать панель инструментов **Options** (Опции) и нажать иконку **Select language** (Выбор языков).

9 В окне **Select language** указать два языка в полях Select primary language (Основной язык) и Select secondary languages (Дополнительный язык). Созданный язык тоже будет отображаться в этих списках. Обязательно выберите новый язык в этом окне, иначе операторы системы не смогут воспользоваться им.

ПРИМЕЧАНИЕ: *Например, если основным языком является английский, а второй язык французский, то при указании нового языка (например, русского) вместо английского все операторы, которым английский язык был назначен основным в меню* ***Operator,*** *теперь будут работать с русским языком. Если же выбрать русский язык как дополнительный, а операторы*

*используют английский язык, то придётся вручную указывать Russian (Русский) в меню описания настроек операторов (**Operator).** Чтобы назначить созданный язык определённому оператору, следует войти в меню **System** (Системные настройки) и выбрать пункт **Operator** (Описания операторов).*

10 Перед тем как приступить к обновлению всех приложений, рекомендуется зарегистрироваться на сервере и проверить, как отображается новый язык. Если всё в порядке, то можно выполнить обновление системы. Следует помнить, что компьютеры должны поддерживать установленный язык (экран и клавиатура).

ПРИМЕЧАНИЕ: *Для каждого устанавливаемого языка следует правильно выбирать раскладку клавиатуры: **Start** (Пуск) > **Control panel** (Панель управления) > **Keyboard** (Клавиатура). Выбранная клавитура отображается в строке состояний.*

Обновление словаря системы

Во время обновления системы новые или изменённые строки автоматически вставляются в базу словаря, а также и в пользовательский словарь. Если в словарь был добавлен новый язык, то после обновления системы следует перевести те строки, которые были добавлены/изменены в словаре. Таким образом, необходимо отредактировать словарь и создать новый самораспаковывающийся файл. Затем следует снова открыть таблицу словаря. Новые строки будут отмечены зелёными метками. Устаревшие строки (не используемые больше) будут отображаться с красными метками.

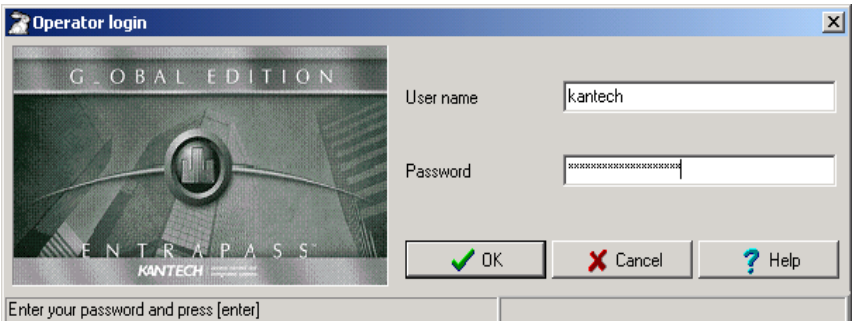
ПРИМЕЧАНИЕ: *Для упрощения работы рекомендуется всегда редактировать словарь с одного и того же компьютера и интегрировать его в систему при помощи самораспаковывающегося файла.*

Программа быстрой настройки"Express Setup"

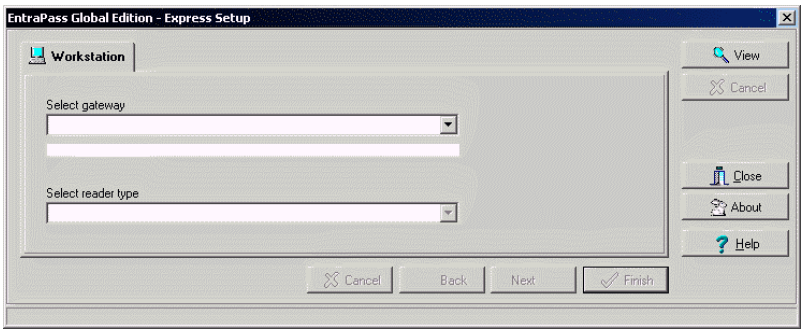
Программа Express Setup (Автоматическая установка) служит для быстрой и удобной настройки конфигурации всех компонентов шлюза: тип используемых считывателей, число сайтов/лучей, имена сайтов/лучей, число контроллеров на каждом сайте/луче и др. Например, с помощью этой программы пользователи могут изменить имя двери путём автоматического назначения настроек по умолчанию ко всем реле и входам контроллеров, подсоединённых к указанной двери.

Настройка луча/сайта NCC 8000/Global при использовании Express Setup

1 Из меню “Пуск” Windows: **Start** (Пуск)**> All Programs** (Все программы)**> EntraPass Global Edition > Server > Express Setup NCC**. Система будет отображать окно Express setup. Появится поле авторизации.

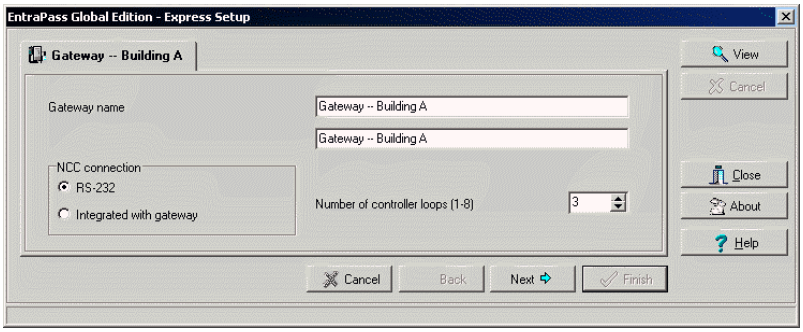


2 Введите имя оператора и пароль, нажмите ок. Окно Express Setup появится на экране.



3 Выберите **Gateway** (Шлюз) и **Reader type** (Тип считывателя), которые будут использоваться на данном шлюзе.

4 Нажмите кнопку **Next** (Следующий) для продолжения.

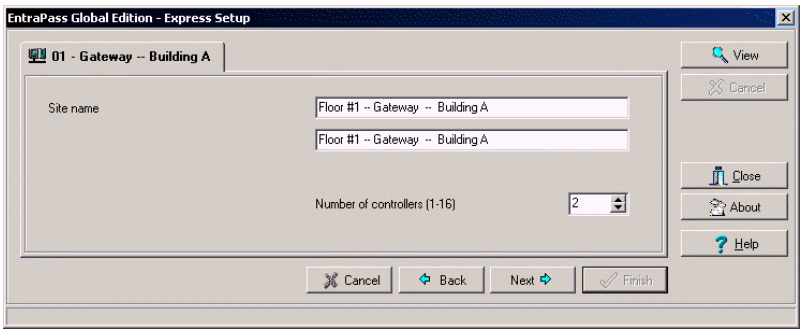


5 Вы можете изменить имя шлюза в пункте “**Gateway name”**.

- Укажите тип связи между Шлюзом и NCC в пункте “**NCC connection”**:
  - **RS-232**: Выберите этот пункт, если NCC установлен на отдельный компьютер от шлюза..
  - **Integrated with gateway** (Встроен в шлюз): Выберите этот пункт, если NCC установлен на компьютере шлюзп = один и тот же компьютер.

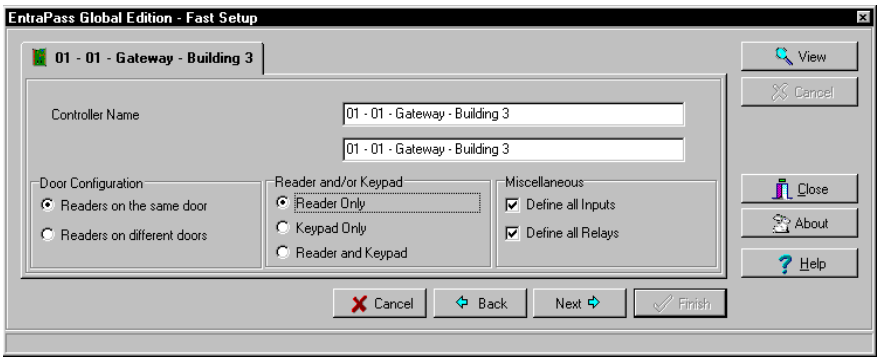
- Укажите количество лучей на данном шлюзе в пункте “**Number of controller loops”.** Максимально 8.

6 Нажмите кнопку **Next** для продолжения. Система будет отображать следующее окно. В зависимости от количества лучей, которые вы ввели в предыдущем окне, то система будет отображать следующее окно.



7 Укажите имя луча в пункте “**Site name”** и количество контроллеров на луче в пункте “**Number of controllers”**.

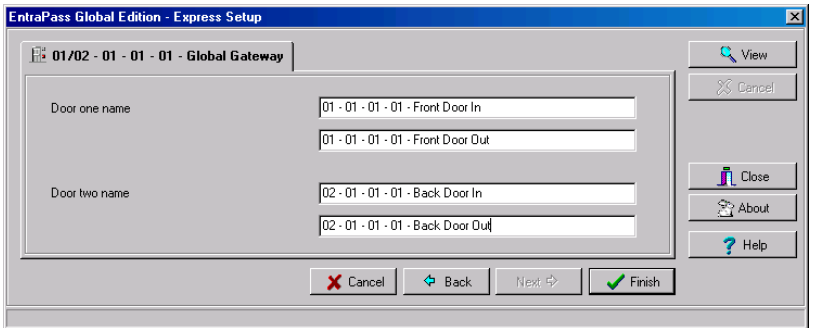
8 Нажмите клавишу **Next** для продолжения. Система будет отображать следующее окно. В зависимости от количества контроллеров на луче, которые вы указали в предыдущем пункте, система будет отображать следущее окно.



9 Укажите имя контроллера в пункте “**Controller Name”.**

- Укажите конфигурацию двери в пункте “**Door configuration**”. Там вы можете указать, что считыватели установлены на одной двери или на разных.
- Выберите опцию при необходимости **Reader and Keypad** (считыватель и кодонаборник).
- Если вы хотите, чтобы система автоматически назначила входы и реле, тогда выделите пункт “define all relays and inputs” (Назначить все реле и входы).

10 Нажмите NEXT для продолжения.

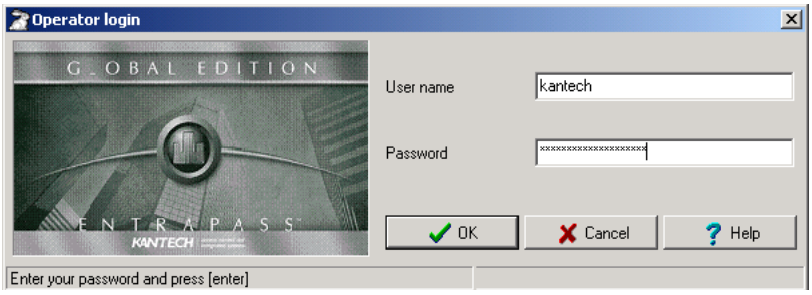


11 Укажите имена дверей (на основном и дополнительном языках) и затем нажмите кнопку “**Finish**” (Закончить).

ПРИМЕЧАНИЕ: *Если вы имеете более чем один луч на шлюзе, тогда система будет отображать последние три окна до тех пор, пока все лучи не будут назначены.*

Настройка конфигурации сайта/луча на шлюзе Corporate при помощи программы Express Setup

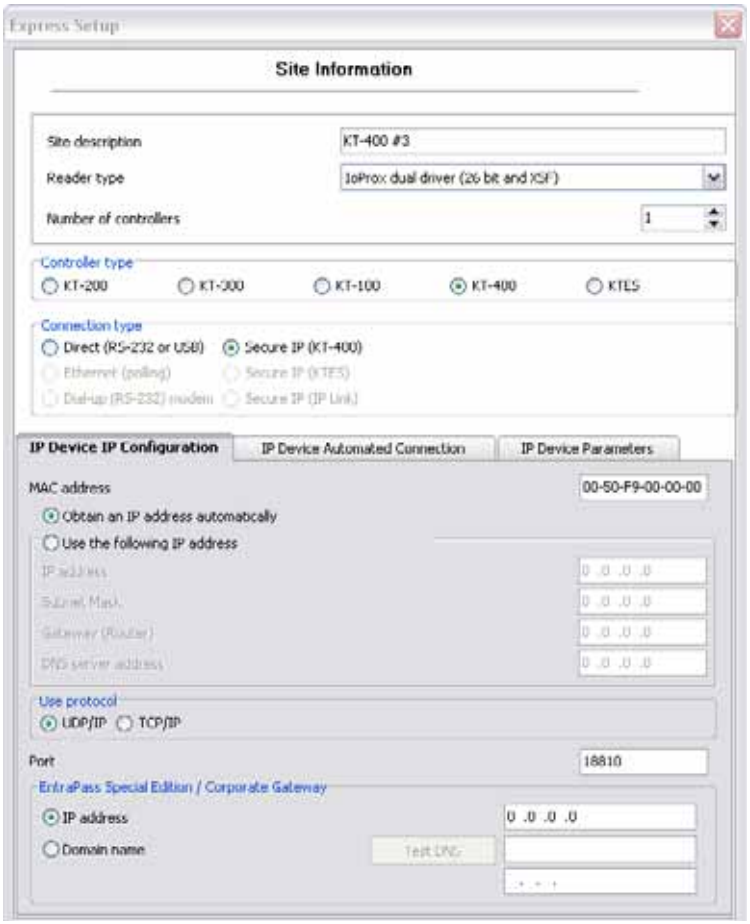
1 В меню Start (Пуск) в операционной среде Windows® войти в меню **All Programs** (Все программы) > **EntraPass Global Edition** > **Workstation/Server** (Рабочая станция/Сервер) > **Express Setup** (Автоматическая установка). Для запуска Express Setup из меню можно воспользоваться иконкой Express Setup в окне регистрации или в окне назначения шлюза.



ПРИМЕЧАНИЕ: *Окно регистрации оператора (Operator login) появляется только в случае запуска программы Express setup в автономном режиме работы.*

2 Указать имя пользователя в окне User name и пароль в окне Password и нажать кнопку **OK**. Кнопка **OK** доступна только после ввода данных в поле **Password.**

3 Указать шлюз для настраиваемого сайта и нажать иконку **New site** (Создать луч).



4 Указать имя луча в поле **Site description** (Описание луча), затем указать тип считывателя

5 Ввести данные в поле **Reader type** (Тип считывателя).

ПРИМЕЧАНИЕ: *Опция KTES только доступна для Шлюза Corporate.*

ПРИМЕЧАНИЕ: *Там нет пунктов **reader type** (Тип считывателя) или **number of controllers** (количество контроллеров) когда вы выбрали тип контроллер KTES.*

6 Указать **Reader type** (Тип считывателя).

7 Указать число контроллеров в поле **Number of controllers**.

8 Указать тип соединения в поле **Connection type**. Этот параметр указывает, как осуществляется связь между лучом и компьютером шлюза. Доступные типы соединений соответствуют выбранному типу контроллера.

- Отметить флажком поле **Direct (RS-232 or USB),** если сайт объединён с компьютером шлюза и подсоединяется к нему через последовательный порт RS-232. Если используется прямое соединение через последовательный порт, то следует указать его номер (com:), а также скорость обмена данными (как правило, 9600 или 19200). По умолчанию установлено значение 19200.
- Выделить тип соединения **Ethernet (polling/опрос)**, если луч осуществляет связь со шлюзом через терминальный сервер (Lantronix) с указанием номера порта. В полях IP address и Port следует указать IP-адрес и порт терминального сервера. Если же используется соединение типа TCP/IP, секция настроек порта будет недоступной. Для настройки терминального сервера следует выполнить указания изготовителя или инструкции, изложенные в руководстве по эксплуатации терминального сервера.
- Выделить опцию **Dial-Up (RS-232) Modem** (Связь через модем по коммутируемой линии), если используется этот тип соединения.
- Выделить опцию **Secure IP (KT-400)**, если используется этот тип безопасного соединения. Заполнить поля в соответствующих закладках.
- Выделить опцию **Secure IP (KTES)**, если используется этот тип безопасного соединения. Заполнить поля в соответствующих закладках.

- Выделить опцию **Secure IP (IP Link)**, если используется этот тип безопасного соединения. Заполнить поля в соответствующих закладках.

9 Нажать **OK**.

10 Укажите минимальную конфигурацию для контроллеров или KTES, назначенных на луче. Это включает назначение имени на контроллере/KTES, указании опции passback и ввода серийного номера.

Пример для контроллера KT-400

ПРИМЕЧАНИЕ: *Колонка **serial number** (серийный номер) появляется только для контроллеров KT-100, KT-300, KT-400 и KTES. Колонка **passback type** (тип антипасбека) появляется только для контроллеров KT-300 и KT-400. Функция запрета повторного прохода запрещает повторный вход с использованием карты, которую не предъявляли на выходе. Этот режим работает только при условии, что считыватели используются и для входа, и для выхода.*

11 Для нового луча с **KTES**, следуете пункту 15.

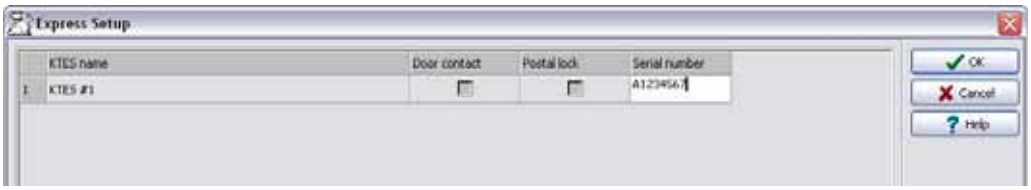
12 Отметить флажками опции **Same door 1 and 2** (Те же двери 1 и 2) и **Same door 3 and 4** (Те же двери 3 и 4), если считыватель устанавливают с каждой стороны двери. Опция **Same door 3 and 4** доступна только для контроллеров типа KT-400.

13 Указать необходимую опцию в колонке **Passback type** (Режим запрета повторного прохода): None (Не использовать), Soft (Мягкий запрет), Hard (Жёсткий запрет). Если в настройках двери указан тип Access door (Дверь для доступа), то для двери такого типа функцию запрета повторного прохода назначить нельзя. Режим запрета повторного прохода можно использовать только на входных или выходных дверях (типа Entry door или Exit door).

14 Следуйте к пункту 17.

15 Выделите опцию **Door contact** (дверной контакт).

Пример для KTES



16 Поставьте галочку для пунтка **Postal lock** (Замок для почтальона), если необходимо. Только для KTES.

17 Введите сериный номер в поле **Serial number**, если вам отображается колонка. Сериный номер (**S/N**) расположен на стикере на контроллере и представлен в виде **Axxxxxxx**.

18 Нажмите **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.

ПРИМЕЧАНИЕ: *Во время обновления базы данных системы второй индикатор состояния (в нижней строке окна) окрашен в красный цвет, что указывает, что база данных недоступна. При попытке войти в другое меню системы, пока база данных заблокирована, система будет выдавать на экран сообщение об ошибке. Следует просто подождать, пока база данных станет доступной.*

Настройки по умолчанию для контроллеров разного типа, используемые программой автоматической установки Express Setup, представлены ниже в таблице. .

Контроллер	Дверь	Реле	Входные зоны	Доп. выходы
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4

Контроллер	Дверь	Реле	Входные зоны	Доп. выходы
KT-400	4	4	16	16
KTES	1	3	4	2

Различные варианты использования тревожных входов в системе проиллюстрированы в таблице: .

Тревожный вход	Использование	Контроллеры
1	Дверной контакт двери №1	KT-100, KT-200, KT-300 and KT400
2	Дверь 1, запрос на выход (REX)	
3	Дверь 2, дверной контакт	KT-300
4	Дверь 2, запрос на выход (REX)	
5	Дверь 2, дверной контакт	KT-400
6	Дверь 2, запрос на выход (REX)	
9	Дверь 2, дверной контакт	KT-200
10	Дверь 2, запрос на выход (REX)	
9	Дверь 3, дверной контакт	KT-400
10	Дверь 3, запрос на выход (REX)	
13	Дверь 4, дверной контакт	
14	Дверь 4, запрос на выход (REX)	

Различные варианты использования тревожных входов в системе проиллюстрированы в таблице для KTES:

Тревожный вход	Использование	Kantech Telephone Entry System
1	Дверной контакт	KTES
2	Postal Lock/Замок для почтальона	
3	Кнопка запроса выхода	
4	Не используется	

Как система назначает выходы/output приведены в следующей таблице: .

Доп. выходы	Использование	Контроллеры
1	Светодиод (Дверь 1)	KT-100, KT-200, KT-300 and KTES
2	Зуммер (Дверь 1)	
3	Светодиод (Дверь 2)	KT-200 and KT-300
4	Зуммер (Дверь 2)	
1	Выход OUT1 (Дверь 1)	KT-400
2	Выход OUT2 (Дверь 1)	
3	Светодиод (Дверь 1)	
4	Зуммер (Дверь 1)	
5	Выход OUT1 (Дверь 2)	
6	Выход OUT2 (Дверь 2)	
7	Светодиод (Дверь 2)	
8	Зуммер (Дверь 2)	
9	Выход OUT1 (Дверь 3)	
10	Выход OUT2 (Дверь 3)	
11	Светодиод (Дверь 3)	
12	Зуммер (Дверь 3)	
13	Выход OUT1 (Дверь 4)	
14	Выход OUT2 (Дверь 4)	
15	Светодиод (Дверь 4)	
16	Зуммер (Дверь 4)	

ПРИМЕЧАНИЕ: *Остальные компоненты (реле и входные зоны) остаются ненастроенными, то есть они созданы, но еще не настроены. Компоненты, которые уже настроены, выделены серым цветом. Их нельзя выделить или изменить их описание. Их настройки можно изменить только в соответствующий меню описания: Devices (Устройства) > Relays/Input zones (Реле/Входные зоны).*

По умолчанию система использует следующие данные:

- Тип считывателя - IoProx Kantech XSF Format,
- Расписание контроля подачи питания (Power supervision schedule) достоверно всегда,
- Задержка включения безопасного режима (Failsoft delay) составляет 45 секунд,
- Тип резистора **НЕТ** (None) - (KT-100, KT-300, KTES),
- Ожидание второй карты (Waiting for second card) составляет 30 секунд.

Настройка конфигурации контроллера при помощи программы Express Setup

Если после добавления контроллера в новый луч, необходимо сразу выполнить сохранение данных. После этого система предложит воспользоваться программой автоматической установки Express Setup для настройки его параметров. Для запуска Express Setup из меню можно воспользоваться иконкой **Express Setup** на панели инструментов ( ) в окне Controller (Контроллер).

1 Из окна **Controller** (Контроллер), выбрать неназначенный контроллер.
2 Открыть закладку **General** (Общие параметры) и указать тип контроллера в поле **Controller type**.
3 Нажать **Save** (Сохранить). На экране появится окно с вопросом: "Do you want to use the Express Setup program to configure the associated devices?" (Хотите ли Вы использовать программу **Express Setup** для настройки соответствующих устройств?). Нажать **Yes** (Да) для продолжения работы с программой **Express Setup.**
   - Или нажать **No** (Нет), чтобы вернуться к программе **Express Setup** позже. Программу всегда можно вызвать нажатием иконки.

Пример для настройки нового контроллера KT-400

ПРИМЕЧАНИЕ: *Необходимо помнить, что контроллер KT-300 рассчитан на две двери, а KT-400 на четыре двери.*

4 Если необходимо, указать, что **Both readers are installed on the same door** (Оба считывателя установлены на одной двери). Если выделить опцию "Both readers are installed on the same door", то опция **REX contact** (Контакт устройства запроса на выход) будет недоступной.
5 Нажать кнопку **Advanced** (Дополнительно), чтобы описать другие устройства, например, двери, входы, реле и выходы.

ПРИМЕЧАНИЕ: *Компоненты перечислены в списке на панели слева. Соответствующие закладки отображаются в середине окна. Если выделить компонент, то в справа отображается его имя по умолчанию (на используемых языках), номер и настройки по умолчанию. Чтобы получить доступ к закладке с настройками компонента, необходимо выделить этот компонент. Компоненты, настройки которых уже заданы, выделены серым цветом, и не могут быть изменены в данном меню. Однако при необходимости можно изменить настройки любого компонента в другом разделе меню:* ***Devices*** *(Устройства) > Controller(Контроллеры) / Door (Двери) / Relay (Реле) / Input (Входы) / Output (Выходы).*

Настройка KTES при использовании системы быстрой настройки Express Setup

Когда вы выбираете тип соединения устройства в новый луч и нажмете сразу кнопку “**save”-** сохранить. Система предложит вам восьпользоваться сервисом **Express Setup** для установки настроеек. Вы можете запустить данный сервис, путем выбора KTES и нажатием на иконку **Express Setup** (иконка кролика) на вкладке **KTES**.

1 Из окна **Site** (луч), нажмите на кнопку **New** (Новый) для назначения нового луча. Назначьте имя на обоих языках.

2 Под вкладкой **General** (Общие), укажите тип контроллера в пункте “**Controller type**”: **Secure IP (KTES)**.

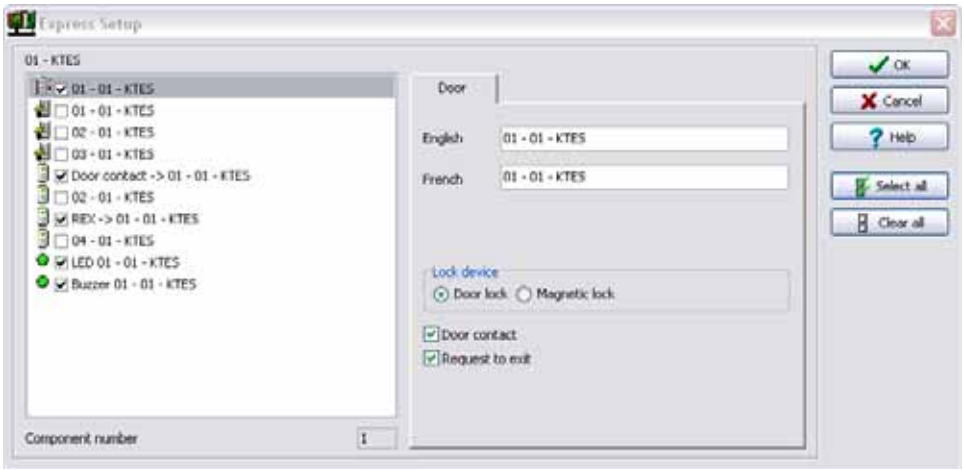
3 Нажать **Save** (Сохранить). На экране появится окно с вопросом: "Do you want to use the Express Setup program to configure the associated devices?" (Хотите ли Вы использовать программу **Express Setup** для настройки соответствующих устройств?). Нажать **Yes** (Да) для продолжения работы с программой **Express Setup.**

- Или нажать **No** (Нет), чтобы вернуться к программе **Express Setup** позже. Программу всегда можно вызвать нажатием иконки.

4 Укажите опции **Door contact** (Дверной контакт) и **REX contact** (кнопка запроса выхода).

5 Включите опцию **Postal lock** (почтовый замок), при необходимости.

6 Нажмите на кнопку **Advanced** (Дополнительно) для назначения других устройств в системе: дверей, тревожных входов, реле и выходов.

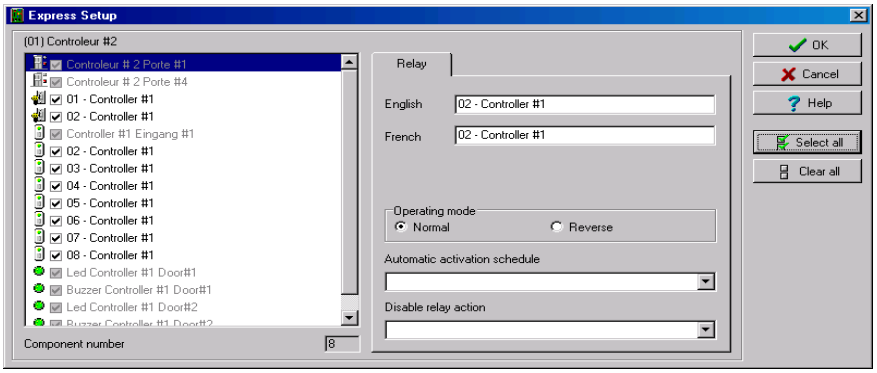


ПРИМЕЧАНИЕ: *Компоненты перечислены в списке на панели слева. Соответствующие закладки отображаются в середине окна. Если выделить компонент, то в справа отображается его имя по умолчанию (на используемых языках), номер и настройки по умолчанию. Чтобы получить доступ к закладке с настройками компонента, необходимо выделить этот компонент. Компоненты, настройки которых уже заданы, выделены серым цветом, и не могут быть изменены в данном меню. Однако при необходимости можно изменить настройки любого компонента в разделе меню:* ***Devices*** *(Устройства) >* ***Kantech Telephone Entry System****.*

Порядок назначения реле

В настройках реле можно настроить их режим работы, а также расписание активации и деактивации реле. Чтобы назначить имя какому-либо реле, его следует выделить в списке реле. В случае использования кнопки Select All (Выделить все) будут сохранены имена по умолчанию.

1 Выделить первое реле, настройки которого необходимо изменить. Справа появляется закладка Relay. Секция с полями для ввода имени на используемых языках станет доступной только после установки флажка рядом с настраиваемым реле в списке слева.



2 Установить нужные опции для режима работы в разделе **Operating mode** и режим активации (**Activation mode**).

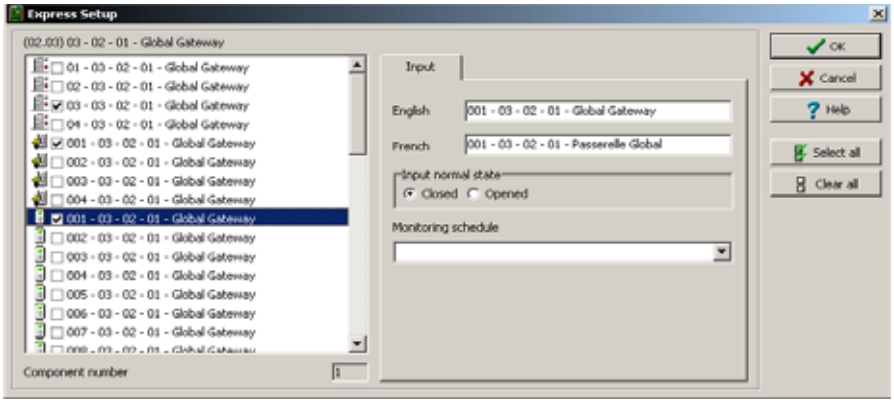
3 В выпадающем списке **Automatic activation schedule** (Расписание автоматической активации) выбрать соответствующее расписание.

4 В выпадающем списке **Disable relay action** (отключить действие реле), выберите подходящее действие.

Порядок назначения входов

По умолчанию время отклика для устройства запроса на выход (REX) составляет 250 мс, а для остальных входных зон это время равно 500 мс. Время восстановления (Alarm restore) составляет 150 мс по умолчанию. Программа Express Setup позволяет установить режим нормального состояния для входа (**Input Normal State**) и выбрать расписание мониторинга/контроллирования входа (**Monitoring Schedule**).

1 Выбрать первый ненастроенный вход (метка рядом с ним не отмечена серым фоном). Выделить этот компонент флажком и назначить для него описательное имя на используемых языках.



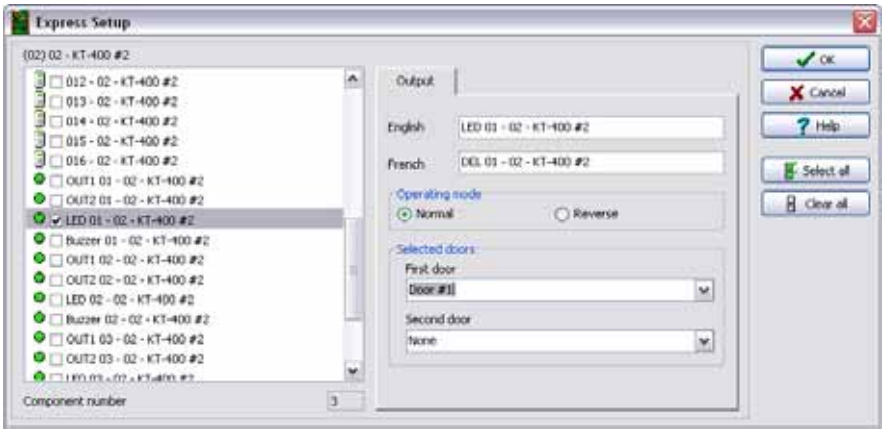
2 Выберите режим нормального состояние входа в пункте “**Input normal state**”.

3 В выпадающем списке **Monitoring schedule** (Расписание мониторинга/контроля) выбрать нужную опцию. Чтобы назначить специальное расписание для выделенного входа, следует описать его в меню: Definition (Описания) > Schedule (Расписания).

Порядок назначения дополнительных выходов (зуммер и световой индикатор LED и Buzzer)

Если вы хотите изменить настройки по умолчанию, которые были казаны ранее, тогда вы можете это сделать в режиме назначения контроллера или KTES в разделе **Devices** (Устройства)**> Output** (Выходы).

1 Выберите первый ненастроенный выход (невыделенный серый). Выделите этот пункт , и назначьте имя для него.



2 Выберите пункт **Operating mode** (Режим управления).

3 Укажите дверь, которая относится к этому выходу из выпадающего списка **Selected doors** (Выбранные двери).

Как система назначает выходы/output приведены в следующей таблице:

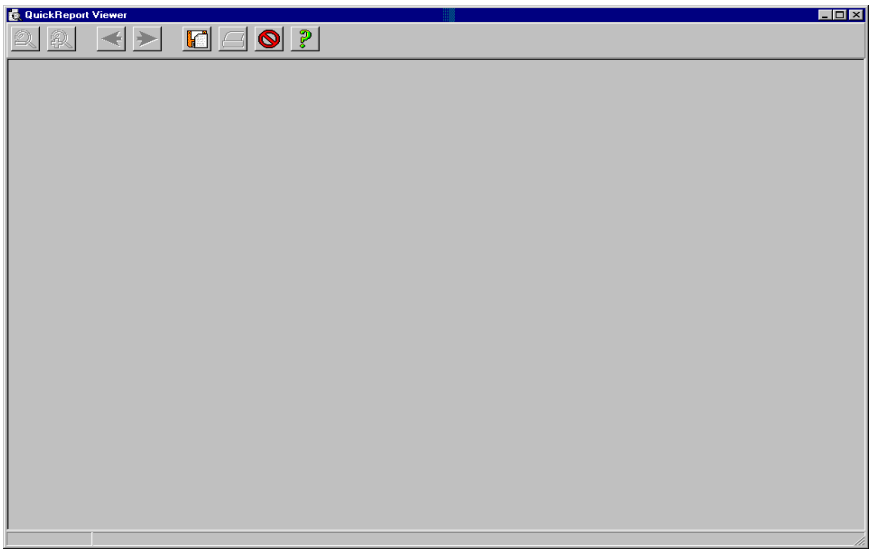
Доп. выходы	Использование	Контроллеры
1	Выход OUT1 (Дверь 1)	KT-100, KT-200, KT-300 and KTES
2	Выход OUT2 (Дверь 1)	
3	Светодиод (Дверь 1)	KT-200 & KT-300
4	Зуммер (Дверь 1)	

Доп. выходы	Использование	Контроллеры
3	Выход OUT1 (Дверь 2)	KT-400
4	Выход OUT2 (Дверь 2)	
7	Светодиод (Дверь 2)	
8	Зуммер (Дверь 2)	
11	Выход OUT1 (Дверь 3)	
12	Выход OUT2 (Дверь 3)	
15	Светодиод (Дверь 3)	
16	Зуммер (Дверь 3)	

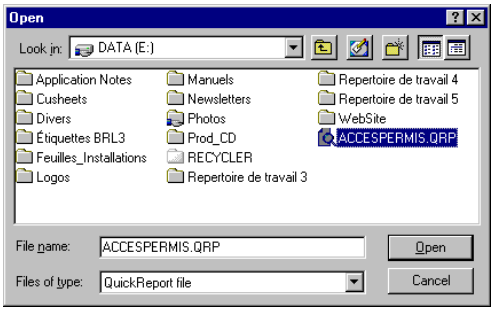
Quick Viewer - *Программы быстрого просмотра отчётов*

Quick Report Viewer позволяет оператору просматривать предварительно сохранённые отчёты, не запуская EntraPass. Эта программа предназначена для просмотра/отображения/загрузки отчётов, сохранённых во время предварительного просмотра перед выводом на принтер в формате .QRP (так называемых быстрых отчётов). *Смотрите в Главе 13 Отчеты' на странице 437 для более подробной информации по* порядку запроса и созданию отчётов. Эта программа поможет, например, просмотреть отчёт, когда система EntraPass работает в автономном режиме.

1 В меню Пуск (Start) в операционной среде Windows® войти в меню All Programs (Все программы) > EntraPass > Server (Сервер) > Quick Report Viewer.



2 Нажать кнопку **Open** (Открыть), чтобы открыть отчёт. При этом должно открыться окно **Open**.



3 По умолчанию все отчёты, сохраняемые в формате QRP, записываются в папку "My Documents" (Мои документы). Если отчёт был сохранён в другом месте, необходимо указать путь, для того чтобы система могла открыть его.

4 Нажать кнопку **Open** (Открыть), чтобы вывести отчёт в окно предварительного просмотра. После того как нужный отчёт будет выделен, система выведет его на экран компьютера.

5 На панели инструментов в окне предварительного просмотра доступны следующие кнопки:

Кнопка	Описание
	Кнопка **Zoom out** (Уменьшение) служит для уменьшения изображения.
	Кнопка **Zoom In** (Увеличение) служит для увеличения изображения (приближения).
	Кнопки **Previous Page** (Предыдущая страница) и **Next Page** (Следующая страница) используются, чтобы перейти к предыдущей/следующей странице.

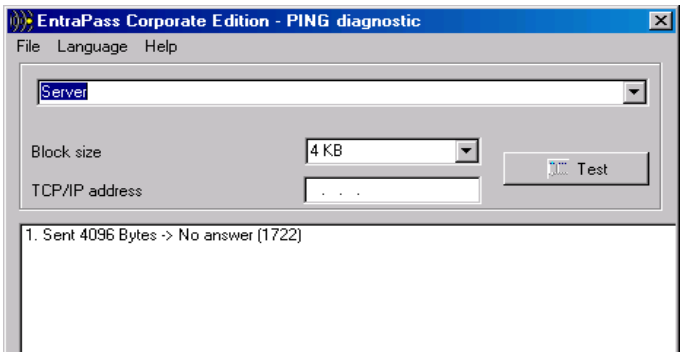
Кнопка	Описание
	Кнопка **Open** (Открыть) предназначена для открытия отчёта, находящегося в любой папке на вашем компьютере.
	Print (Печать) – служит для вывода на печать отображаемого отчёта. По этой кнопке отчёт будет автоматически отправлен на принтер, минуя меню настройки печати. Для отмены печати нажать **Cancel** (Отмена).
	Кнопка **Quit** (Выход) служит для выхода из приложения.

Диагностика по методу "запрос-ответ" (PING Diagnostic)

Эта автономная программа служит для диагностики неисправностей в сети и/или проверяет состояние маршрута следования пакета до определенного IP-адреса. Она отправляет пакет (блок) данных на указанный адрес и ждёт ответ. PING Diagnostic используется преимущественно для устранения проблем подключения Интернета.

ПРИМЕЧАНИЕ: *Эта функция будет доступна только при условии, что ранее при настройке параметров сервера была выделена опция “Allow diagnostic on network” (Разрешить диагностику сети). Смотрите в Главе 15 Сервер EntraPass’ на странице 505 для более подробной информации .*

1 В меню **Start (**Пуск) в операционной среде Windows® войти в меню **All Programs** (Все программы) > **EntraPass Global Edition** > **Workstation/Server** (Рабочая станция/Сервер) > **PING Diagnostic**.



2 В выпадающем списке выделить приложение, которое необходимо проверить: Server (Сервер), Workstation (Рабочая станция), Gateway (Шлюз) и др.).

3 Указать нужное значение в выпадающем списке **Block size** (Размер блока). Это поле используется для задания размеров блока данных, отправляемых на опрашиваемый адрес. Допустимый диапазон значений - от 1 кб до 1024 кб (1 Мб).

4 В поле **TCP/IP address** указать IP-адрес компьютера, связь с которым необходимо проверить.

ПРИМЕЧАНИЕ: *Для получения адресов TCP-IP рекомендуется обращаться к сетевому администратору.*

5 После указания адреса TCP/IP нажать кнопку **Test**, чтобы запустить процедуру тестирования. Данные будут отправлены на указанный адрес 16 раз. На экране будет отображаться число байт отправленных данных и число байт полученных данных, а также время задержки (в миллисекундах).

ПРИМЕЧАНИЕ: *Задержка между попытками отправки данных должна быть примерно одинаковой, за исключением первой попытки, когда допускается большая задержка. Если указанный адрес не отвечает, на экран будет выведено сообщение типа: Sent (block) Bytes, No Answer (1717).*

Рабочая станция – АРМ

Эта служебная программа используется в случае необходимости выполнить настройку рабочей станции или шлюза. Она содержит все меню и функции, необходимые для настройки конфигурации системы, включая настройку отображаемых событий, рабочих столов, ручного режима управления или отчётов. Установщик системы может при помощи этой программы настроить все рабочие станции сразу, не перебирая их последовательно друг за другом.

Утилиту настройки рабочих станций запускают из меню **Start** (Пуск) в операционной среде Windows®: **All Programs** (Все программы) > **EntraPass Global Corporate Edition** > **Server** (Сервер) > **Workstation** (АРМ). Эту программу можно также запустить при помощи контекстного меню на рабочем столе. Чтобы воспользоваться данной опцией, необходимо сначала создать операторов и уровни безопасности для операторов в меню **System** (Системные настройки), а затем назначить шлюзы, сайты/лучи, контроллеры в меню **Devices** (Устройства).

ПРИМЕЧАНИЕ: *Смотрите в Главе 2 :Установка программного обеспечения' на странице 9 для более подробной информации .*

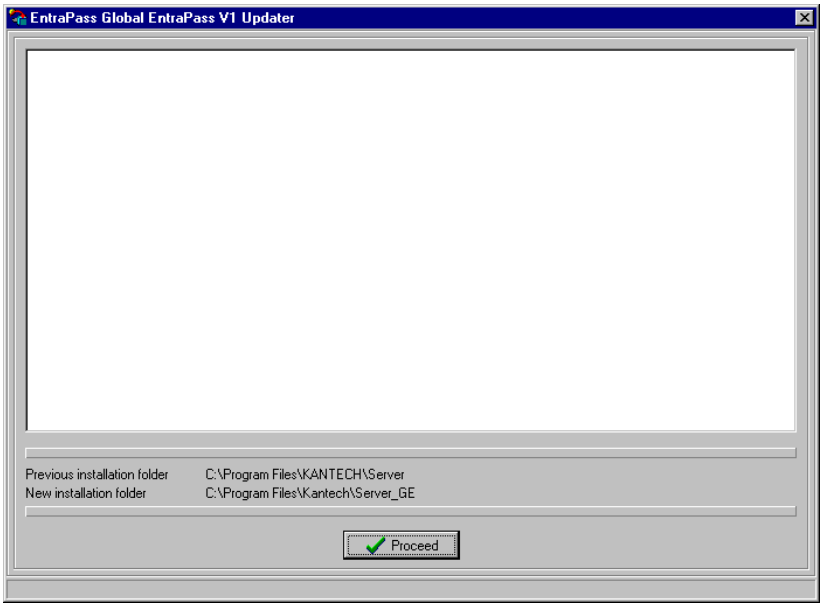
Программа обновления Global

Сервис Global Updater ипользуется для конвертации базы данных Global от версии 1 до 3. Самые последнии преимущества будут установлены в базу данных после конвертации. Также устройства могут быть переназначены на АРМ и Шлюзе. Подготовка:

- Будьте уверены, что база данных версии 3 установлена на тот же компьютер, как и версия 1.
- Запустите, авторизуйтесь и закройте базу данных версии 3.

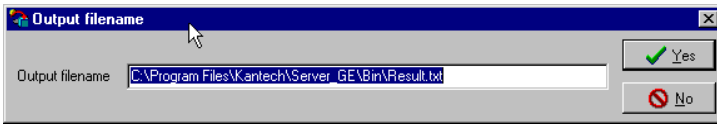
1 Запустите программу “Global Updater” из

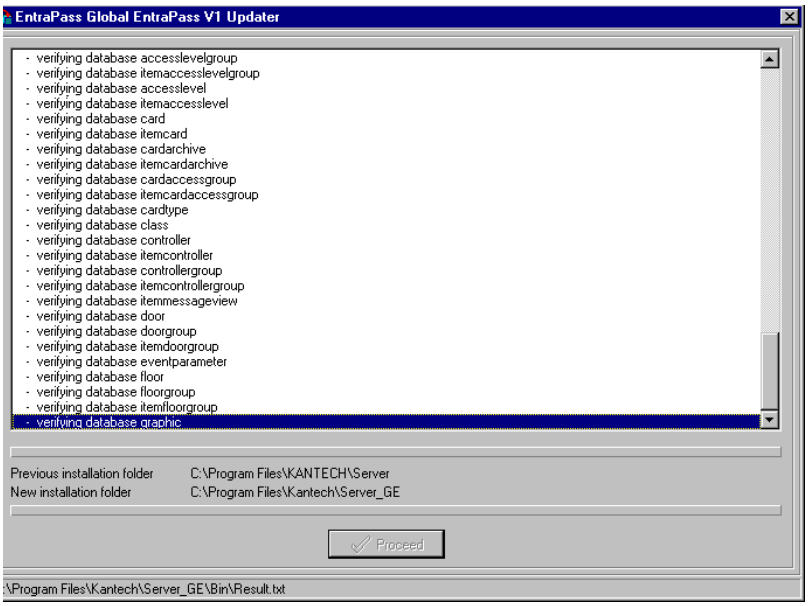
C:\Program Files\Kantech\Server_GE\Bin\GlobalUpdater.exe



2 Укажите путь до предыдущей инсталяции (версия 1) и новой установленной (версия 3), подтвердите в окне Global Updater и нажмите кнопку **Proceed** (Продолжать).

3 Создайте выходной файл, который будет содержать все системные процедуры в течении конвертации, путем нажатия кнопки **Yes.** (рекомендуется).





4 Выберите новое устройства, шлюз или АРМ, которые будут брать информацию от прежних устройств.

ПРИМЕЧАНИЕ: *Процедура будет повторяться для каждого серийно-прономированного назначения АРМ/Шлюз, который найдет в системе.*

ПРИМЕЧАНИЕ: *Информация, связанная с шлюзом может быть потеряна в течении конвертации на новый АРМ из прежнего назначения АРМ/Шлюза. Будьте уверены, что вы записали информацию о шлюзе, когда вы соберетесь проводить данное обновление.*

5 Установите тип считывателя.

6 Нажмите **OK** чтобы закрыть окно выбора типа считывателя ”Reader type”.

Утилита переноса данных (Migration Utility)

Миграция EntraPass Global Edition с версии 1 до версии 3

EntraPass предлагает вам возможность произвести обновление вашей системы EntraPass Global Edition с версии 1 до 3. Вам будет необходимо иметь инсталяционный ключ (вы можете найти его на CD) и код регистрации, обеспеченыый Kantech. До исполнения миграции, вы должны произвести backup вашей система EntraPass. *Смотрите в Главе 15 Резервные копии' на странице 509 для более подробной информации* по проведению backup вашей базы данных. Затем установите EntraPass Global Edition версии 3 и зарегестрируйте ее. *Смотрите в Главе 2 Установка системы' на странице 14 для более подробной информации* по установке EntraPass. Затем необходимо произвести миграцию базы данных от версии 1 до версии 3, используя утилиту **Migration from EntraPass Global Edition V1**. Последний шаг - это будет установить на адоптированную версию ваши системные компоненты (Vocabulary Editor, интерфейс Oracle/MS-SQL, итд). *Смотрите в Главе 2 Дополнительные компоненты системы EntraPass' на странице 23 для более подробной информации* по обновлению системных компонентов.

ПРИМЕЧАНИЕ: *Пожалуйста, произведите регистрацию ПО, до запуска приложения миграции. Для большей информации относительно миграции, обратитесь к руководству DN1541.*

Миграции версии 1 базы данных сервера

1 Из меню "Пуск" **All Programs** (Все программы) > **EntraPass Global Edition** > **Server** > **Migration from EntraPass Global Edition V1**.
   - Если EntraPass Global Edition версия 1 и EntraPass Global Edition версии 3 уже установлены на одном и том же ПК: программное обеспечение будет автоматически располагаться в ранее установленнную базу данных сервера. Идите к пункту 4.
   - Если EntraPass Global Edition версия 1 и EntraPass Global Edition версии 3 уже установлены на разных ПК:, тогда появится окно для указания пути. Вы должны в ручном режиме выбрать базу данных сервера. Выполните пункт 2 и 3.

2 Из окна выбора директории/пути, нажмите на кнопку **Network** (Сеть), чтобы указать файл версии №1 EpServer.exe. Данный *exe* файл расположен в папке Bin EntraPass Global Edition версия 1.

3 После указания файла EpServer.exe, выберите его, затем нажмите кнопку **Open**. Данная кнопка будет активной при условии, что вы указали папку установки. После того как вы выбрали файл EpServer.exe, кнопка **Proceed** (Продолжить) станет активной.

4 Нажмите на кнопку **Proceed** (Продолжить), чтобы запустить процесс миграции. Система отобразит имя выходного файла, который будет использоваться в качестве журнала по миграции. Туда будут записываться события по миграции. Рекомендуется оставить имя и путь расположения файла по умолчанию.

5 После того, как вы подтвердили имя по умолчанию для выходного файла, нажмите кнопку **Yes** для запуска процесса миграции.

ПРИМЕЧАНИЕ: *Процесс миграции может занять несколько минут в зависимости от размера исходной базы данных и вашей конфигурации ПК. В течении процесса миграции, система отображает информацию, которая связана с выполнением процесса миграции. В конце работы система отобразит список определенных компонентов, которые успешно перешли из версии 1 в версию 3.*

6 Нажмите ОК для закрытия приложения.

7 Перезагрузите ПК

8 Запустите Сервер EntraPass Global Edition версии 3, чтобы переустановить предыдущие системные компоненты.

После установки, все системные компоненты версии 1 (и новые кустановочные коды) отображаются в окне регистрации APM. Используя новый установочный код, вы можете произвести переустановку ваших системных компонентов на подходящие ПК.

ПРИМЕЧАНИЕ: *Все приложения EntraPass Global Edition, которые не были обновлены до версии 3, не смогут подсоедениться к серверу. Для обновления других приложений версии 1, таких как Vocabulary Editor или SmartLink, изучите руководство DN1541.*

9 В окне Migration указать папку, в которой находится база данных старой версии (EntraPass SE). Запустить систему EntraPass Corporate Edition. Зарегистрировать EntraPass Corporate Edition. Для получения регистрации следует обратиться в службу технической поддержки Kantech.

Смотрите в Главе 2 :Установка программного обеспечения' на странице 9 для более подробной информации

Интерфейс шлюза

Шлюз представляет собой программный интерфейс, используемый для преобразования данных, полученных с лучей/шлюзов (которые получают данные с ветвей контроллеров) и передачи их на сервер. Сервер и шлюз используют один протокол для связи, контроллеры и луч/шлюз также используют один и тот же протокол. Как правило, программное обеспечение шлюза (Gateway) установлено на одном и том же компьютере. Иногда шлюз может быть установлен на внешнем компьютере, который подключён к другому компьютеру, оснащённому программным интерфейсом Gateway (который передает данные на сервер). Система управления доступом, фактически, состоит из двух разных систем:

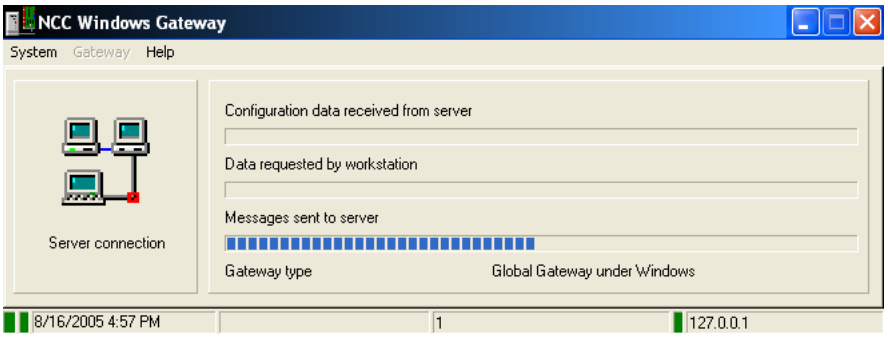
- компьютеров, которые служат для ввода данных и доступа к базе данных,
- контроллеров дверей (сгруппированных в лучи), которыми управляют через шлюз.

Меню System (Система) позволяет операторам входить/выходить из системы, а также перезагружать шлюз.

Запуск шлюза

Система предусматривает запуск интерфейса рабочей станции вместе Workstation and Gateway (АРМ и Шлюз) или по отдельности.

1 Достаточно в меню **Пуск** (Start) в операционной среде Windows® войти в меню **All Programs** (Все программы) > **EntraPass** (Программное обеспечение EntraPass) > **Gateway** (Шлюз) > **Gateway** (Шлюз). (При условии, что установлено только программное обеспечение шлюза (Gateway Only).) Или войти в меню **Start** (Пуск) **> All Programs** (Все программы) > **EntraPass** (Программное обеспечение EntraPass) > **Workstation & Gateway** (Рабочая станция и шлюз) > **Gateway** (Шлюз), при условии установки программного обеспечения и рабочей станции, и шлюза.



Перезагрузка Шлюза

Эта опция служит для повторной загрузки данных на определённый шлюз. Она позволяет обновить все или некоторые параметры, связанные с работой по сети. Данные, находящиеся на сервере, будут загружены на каждый шлюз, а потом шлюзы повторно загрузят данные на все контроллеры. При выполнении этой операции контроллеры будут работать автономно (в безопасном режиме, который используется при отсутствии соединения со шлюзом, Fail-Soft) и Шлюз не будет способен передавать информацию. Например Глобальные функции.

Процес перезагрузки данных гарантирует, что шлюз получит самую последную информацию. Тем не менее, система обновляет данные Шлюзов после каждого изменения системы. Меню HELP обеспечивает попомщь при неообходимости. В строке состояний будет отображаться дата и время системы, имя оператора, работающего в системе в текущий момент, статус (это может быть любое сообщение, например, "выполняется" и др.), а также IP-адрес сервера EntraPass (зелёный прямоугольный индикатор указывает нормальный статус основного сервера, жёлтый горит, когда работает резервный сервер).

- **Configuration data received from the server** (Параметры конфигурации, полученные с сервера) – в строке состояний отображаются данные конфигурации, передаваемые с сервера EntraPass Server. Данные конфигурации – это, например, изменения в идентификационных картах (Card modifications) и др.

- **Data requested by workstation** (Данные, запрашиваемые с рабочей станции). В строке состояний отображается состояние, что данные были запрошены с рабочих станций EntraPass Workstations (может быть любая). Это разные запрашиваемые данные, в частности, запросы состояний (Status Requests).
- **Messages generated by the gateway** (Сообщения, генерируемые шлюзом). В строке состояний отображаются сообщения, созданные на шлюзе. Это сообщения типа: Access granted (Доступ разрешён), Input in alarm (Вход переведён в статус тревоги), Access denied - bad access level (Доступ запрещён – неверный уровень доступа) и др.
- **Configuration data sent to the controllers** (Параметры конфигурации, отправленные на контроллеры). В строке состояний отображаются данные конфигурации, полученные сервером EntraPass, отправлены на контроллеры.
- Шлюз будет направлять информацию на контроллеры.

ПРИМЕЧАНИЕ: *Индикаторы выполнения показывают ход выполнения обмена данными, а также направление передачи данных (отправку и получение).*

Интерфейс MS/SQL

Программа MS/SQL Interface создаёт в реальном времени копию базы данных EntraPass по идентификационным картам на сервере MS-SQL или Oracle. Этот интерфейс позволяет операторам изменять, добавлять или получать сведения по идентификационным картам в реальном времени, используя клиентскую версию MS-SQL или ORACLE. База данных по идентификационным картам, содержащая информацию о владельцах карт, использующая интерфейс MS/SQL Interface, будет автоматически обновляться при появлении новых доступных данных в базе данных по картам в системе EntraPass.

ПРИМЕЧАНИЕ: *Интерфейс программы MS-SQL/ORACLE не поддерживается резервным сервером и зеркальной базой данных “**Mirror Database and Redundant Server**”.*

В зависимости от того, какой клиентский интерфейс (EntraPass или ORACLE/MS-SQL Client) используется для добавления или изменения идентификационных карт, программа MS/SQL Interface обеспечивает, чтобы изменения были переданы на сервер EntraPass Server и обратно, и чтобы данные, независимо от их источника, были обновлены в обе базы данных. (Более подробные сведения приведены на схеме "Процедура обмена данными").

Установка программы MS/SQL Interface

Рекомендуется установить программу MS/SQL Interface на компьютер с минимальной загрузкой, так как процедура обмена данными будет выполняться на том компьютере, на котором запущена данная программа. Рекомендуется установить программу MS/SQL Interface на компьютер с минимальной загрузкой, так как процедура обмена данными будет выполняться на том компьютере, на котором запущена данная программа.

В зависимости от размера базы данных и количества транзакций выполнение обновления может значительно загружать память компьютера. Поэтому компьютер, на котором будет установлено это программное обеспечение, должен удовлетворять тем же необходимым требованиям, которые предъявляются к компьютерам, на которых установлены рабочие станции EntraPass Workstation (*Смотрите в Главе 2 Рекомендуемые системные требования’ на странице 10 для более подробной информации*).

1. Установить компонент Oracle/MS-SQL Interface (CardGateway), следуя указаниям по установке. *Смотрите в Главе 2 Установка системы’ на странице 14 для более подробной информации* (требуется знать код установки).
2. Клиентское обеспечение ORACLE/MS-SQL обязательно ДОЛЖНО быть установлено на том же компьютере, что и программа MS/SQL Interface. Или можно установить программу MS/SQL Interface на компьютер, на котором уже установлено клиентское приложение ORACLE/MS-SQL.
3. Для того чтобы завершить установку, следует создать базу данных на сервере ORACLE/MS-SQL Server. Для этого следует **вручную** создать базу данных или использовать автоматическую встроенную функцию для **автоматического** создания базы данных на сервере (смотрите далее раздел "Настройка конфигурации программы MS/SQL Interface").

Настройка конфигурации программы CardGateway

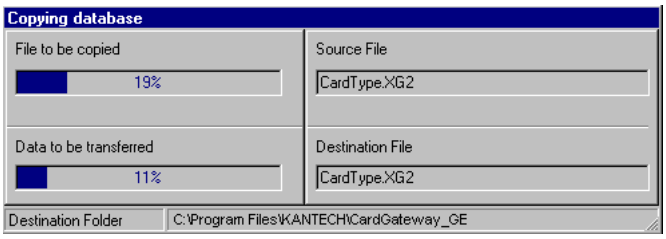
Смотрите в Главе 4 Создание баз данных сервера вручную’ на странице 74 для более подробной информации о том, как настроить конфигурацию программы MS/SQL Interface, чтобы автоматически или вручную создавать базы данных, а также указывать имена пользователей и пароли на сервере MS/SQL / ORACLE Serve.

Запуск программы CardGateway

1. Для запуска программы CardGateway следует перейти в меню **Start** (Пуск) в операционной среде Windows® : нажать **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Global Edition** (Система EntraPass) > **MS-SQL and Oracle Interface** (Интерфейс MS-SQL и Oracle) > **MS-SQL and Oracle Interface**. Язык меню на экране зависит от настроек оператора, который перед этим зарегистрировался на этой рабочей станции.

После выполнения указанных действий программа будет пытаться установить связь с сервером. Во время выполнения этого действия на экране будет отображаться следующее окно:

2 Если приложение обращается к серверу ORACLE/MS-SQL впервые, то в базе данных KANCARD создаются пять таблиц: tbCard, tbCardType, tbCardAccessGroup, tbTransactionIn и tbTransactionOut.

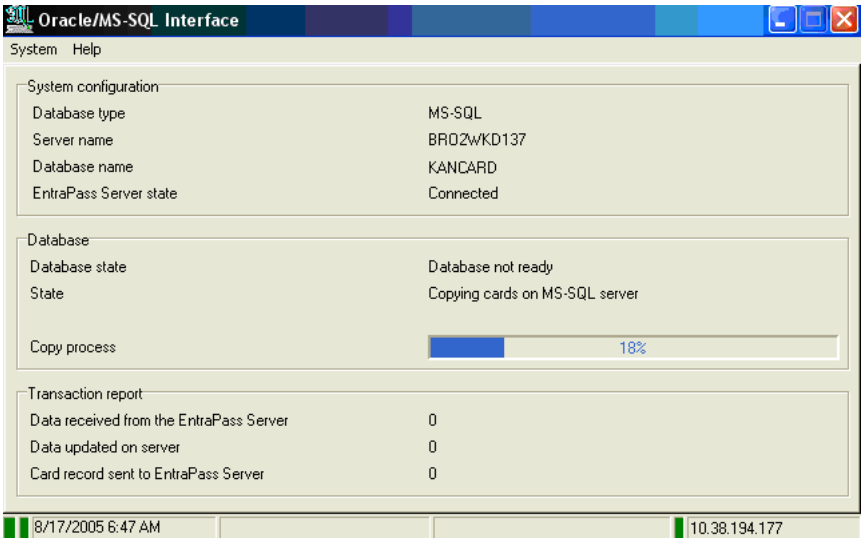


ПРИМЕЧАНИЕ: *Информация и данные, передаваемые с основного сервера EntraPass в базу данных MS/SQL Interface, будут сжаты для более быстрой передачи.*

Первые три таблицы (tbCard, tbCardType, tbCardAccessGroup) заполняются при первом подключении, в них указываются данные карт (Cards), группы уровней доступа карт (Card Access Groups) и типы карт (Card Types). Вносить данные в эти таблицы не требуется, поскольку программа MS/SQL Interface регулярно их обновляет. Они предназначены только для чтения. Таблица tbTransactionIn используется для создания, изменения или удаления карт с сервера ORACLE/MS-SQL. Программа MS/SQL Interface регулярно сканирует эту таблицу. При обнаружении карты она создаёт, изменяет или удаляет эту карту на сервере EntraPass в зависимости от того, какое значение указано для этой карты в колонке State в таблице tbTransactionIn (статус 0 означает создание или изменение карты, а статус 1 – удаление). После этого программа MS/SQL Interface удаляет карту из таблицы tbTransactionIn.

Таблица tbTransactionOut содержит историю всех созданий, изменений и удалений карт (с момента запуска программы CardGateway). Все успешные действия по созданию, изменению и удалению карты, выполненные MS/SQL Interface после чтения этой карты в таблице tbTransactionIn, содержатся также в таблице tbTransactionOut.

3 После этого открывается главное окно приложения:



System configuration (Конфигурация системы)

- **Server name** (Имя сервера) – в этом поле указывается имя сервера SQL или Oracle, которое было назначено в меню описания рабочей станции.
- **EntraPass State** (Статус системы EntraPass) – в этом поле отображается статус сервера EntraPass в режиме реального времени. В случае поломки здесь появляются сообщения о неисправности.

Database (База данных)

- **Database State** (Статус базы данных) – в этом поле отображается статус базы данных по идентификационным картам в режиме реального времени.

Transaction Report (Отчёт о транзакциях)

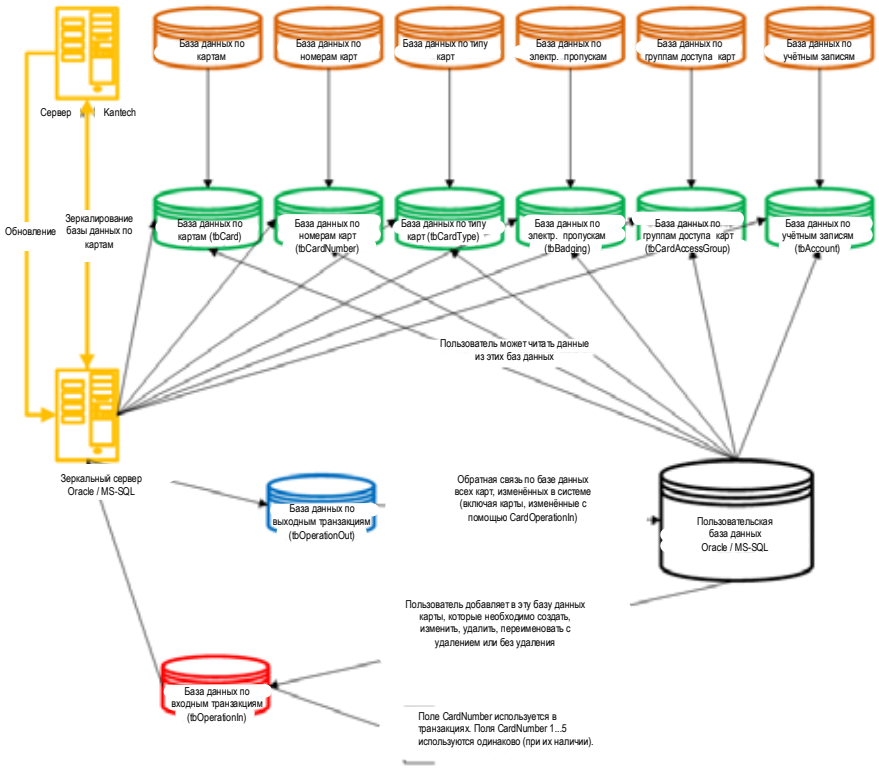
- **Data received from the EntraPass Server** (Данные, полученные с сервера EntraPass). Если данные по картам изменяются на сервере EntraPass (в базе данных), то эта информация также передается в базу данных MS/SQL Interface, где её будет собирать сервер SQL или Oracle. В этом поле отображается число транзакций, которые были выполнены и отправлены в базу данных по картам.
- **Data updated on SQL Server** (Данные, обновлённые на сервере SQL).
- **Nb of cards sent to EntraPass Server** (Число карт, отправленных на сервер EntraPass). В этом поле отображается число карт, которые были добавлены или изменены в клиентском приложении SQL или Oracle и были отправлены в базу данных сервера EntraPass (EntraPass Server).

Транзакции

Реестр содержит подробную информацию о транзакциях, которые обрабатываются программой CardGateway. Чтобы получить доступ к этому окну, необходимо ввести свои регистрационные данные.

Diagram - Схема

На приведённой ниже схеме показан процесс обмена данными между программой CardGateway и базой данных MS-SQL / ORACLE.



Интерфейс SmartLink

Интерфейс SmartLink позволяет пользователям настраивать сообщения и формат данных, отправляемых на второй COM-порт или в файл на диске. В этом разделе руководства даётся объяснение, как построить символьную строку для отправки через SmartLink. Приложение SmarkLink позволяет обеспечивать взаимосвязь системы управления доступом EntraPass почти с любым интеллектуальным устройством, включая коммутаторы с видеоматрицами, системы персонального вызова (пейджеры) и т.п. Для этого между одной из рабочих станций EntraPass и внешним устройством устанавливают связь по протоколу RS-232. Необходимые командные строки и протоколы могут быть легко отредактированы на месте в соответствии с любым типом выполняемых работ.

Система SmartLink упрощает взаимодействие с интеллектуальными устройствами других изготовителей, поскольку она обеспечивает установщика системы всеми инструментами, необходимыми для построения и поддержки фактически действующего интерфейса, не вынуждая к приобретению специальных драйверов компании Kantech. В сфере коммуникаций связь представляет собой линию или канал, по которому передаются данные. Передача данных выполняется с одного компьютера на другой, с одного устройства на другое. Таким образом, устройством связи является любое средство, используемое для передачи данных. Например, модемы, кабели и порты являются устройствами связи.

Необходимые материалы

- Компьютер, удовлетворяющий тем же требованиям, которые предъявляются к рабочим станциям EntraPass Workstation. (*Смотрите в Главе 2 Рекомендуемые системные требования' на странице 10 для более подробной информации*),
- Установочный компакт-диск для приложения SmartLink с серийным номером.

Установка

1. Создать новое приложение в меню Workstation Registration (Регистрация рабочей станции). *Смотрите в Главе 2 Рекомендуемые системные требования' на странице 10 для более подробной информации* о том, как создать новое приложение,
2. Установить приложение SmartLink на компьютер (*Смотрите в Главе 2 Установка системы' на странице 14 для более подробной информации*).
3. После завершения установки приложения SmartLink необходимо выполнить настройку его конфигурации.
4. Если используется режим Message Mode (Режим сообщений), то необходимо создать инструкции, используя специальные макрокоманды. *Смотрите в Главе 5 Назначение Task Builder (конструктор команд)' на странице 204 для более подробной информации о создании команд*.

Настройка приложения SmartLink

Настройку конфигурации выполняют на обычной рабочей станции EntraPass или на любой рабочей станции EntraPass Workstation, используемой для настройки конфигурации (то есть установленной на том же компьютере, на котором установлено приложение сервера). В зависимости от режимов, которые будут использованы для работы с модулем SmartLink: сообщения (Messages) или команды (Commands), необходимо соответствующим образом настроить рабочую станцию.

Запуск приложения SmartLink

1. На компьютере с установленным приложением SmartLink вызвать меню **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass > SmartLink > SmartLink**. Приложение SmartLink будет запущено. Для получения более подробной информации о приложении SmartLink следует обратиться к руководству **SmartLink Specifications Manual** DN1327.

Нагрузка на сеть

Использование сетевых ресурсов можно подразделить на несколько категорий:

Сообщения:

- Сообщения, генерируемые на сервере, могут содержать:
  - Минимум: 128 байт + (число рабочих станций и приложений SmartLink * 32 байта)
  - Максимум: 128 байт + (число рабочих станций * 416 байт)
- Сообщения, генерируемые рабочей станцией, шлюзом и т.п. содержат по 56 байт.
- Использование фотографий (владельцев карт) увеличивает трафик сети. Этот параметр в значительной степени зависит от числа рабочих станций, использующих данную опцию, и от числа карт в системе, а также от числа транзакций, приходящихся на каждую карту.

Перезагрузка:

Поскольку повторные загрузки шлюза выполняются время от времени и оказывают незначительное влияние на сеть, их влияние на общий трафик сети можно не учитывать.

Функции	Байты	Примечания
Система	256	-
Контроллеры	# * 32	Где # = 0 to 128
Двери	# * 32	Где # = 0 to 256
Реле	# * 16	Где # = 0 to 2048
Входы	# * 16	Где # = 0 to 2048
Дополнительные выходы	# * 16	Где # = 0 to 512
Области	# * 32	Где # = 0 to 100
Тревожные разделы	# * 64	Где # = 0 to 100
Группы контроллеров	# * 32	Где # = 0 to 100
Группы дверей	# * 80	Где # = 0 to 100
Группы реле	# * 320	Где # = 0 to 100
Группы входов	# * 320	Где # = 0 to 100
Группы уровней доступа	# * 80	Где # = 0 to 100
Уровни доступа	# * 640	Где # = 0 to 248
Расписания	# * 64	Где # = 0 to 99
Карты	# * 16	Где # = 0 to 32,000
Праздничные дни	# * 64	-
Параметры событий	# * 16	Где# = 0 to 50,000

Ручные операции:

Существуют два типа ручных операций:

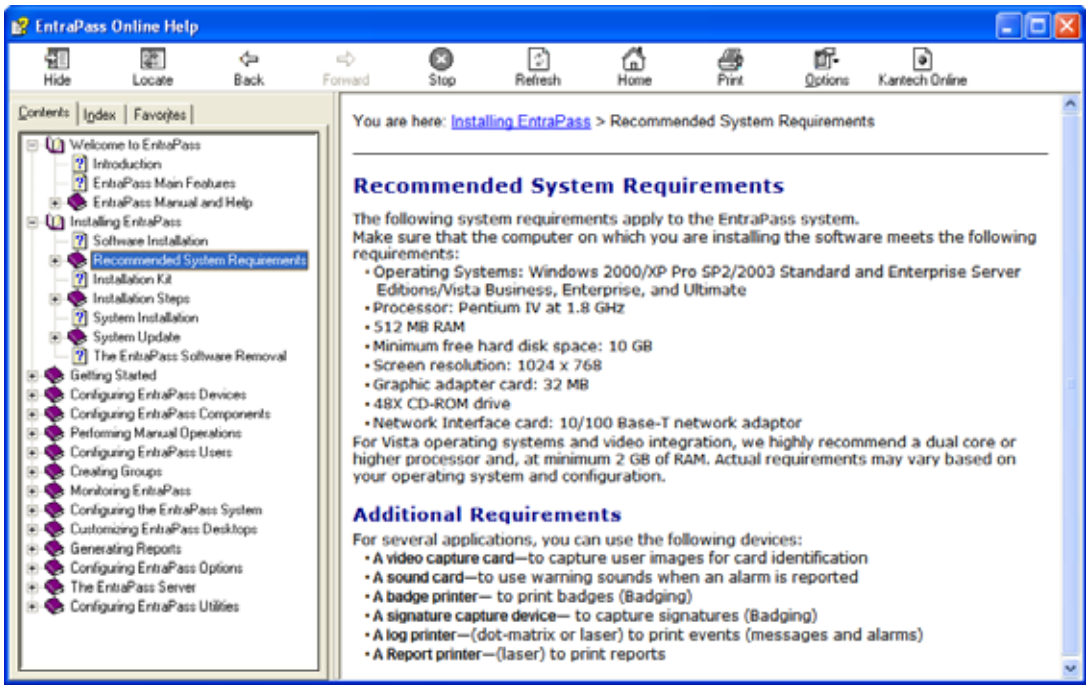
- Операции, используемые для выполнения функций, например, разблокировки двери. Эти операции, используемые время от времени, как правило, не связаны с передачей большого объёма информации.
- Операции, используемые для восстановления компонента или для запроса списка карт. Операции такого типа используются довольно часто, но как правило, не оказывают значительного влияния на трафик сети. Например, для запроса статуса двери отправляется только 16 байт, а принимается 64 байта.

EntraPass Online помощь

Получение Online помощи

1 У вас там два пути вызова EntraPass Online помощи:
   - Нажатие на кнопки (**? Help**) (Помощь).

   - Из меню Windows нажмите **Start** (Пуск) **> All Programs** (Все программы)**> EntraPass Global Edition > Server > English Help**.



Глава 17 • Анимированные иконки

Анимированные иконки указывают статус физических или логических компонентов в окнах программ системы EntraPass. Они отображают статус компонентов в режиме реального времени и имитируют движение, показывая серию изображений, связанных с этим компонентом. Эта глава предназначена для тех, у кого возникают трудности с определением статуса компонентов по анимированным иконкам.

Тревожная система

Иконки тревожной системы индицируют состояние тревожной системы на графическом рабочем столе (Desktop (APM)> Graphic desktop (Рабочий стол графических схем)) или в меню “Operation” (Управление).

Тревожная система в тревоге

Эти анимированные иконки появляются, когда тревожная система в тревоге. Отображается в следующих окнах программы:

- В окне сообщений, когда требуется подтверждение.
- Окно“Operation” (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система поставлена на охрану

Эта анимированая иконка появляется, когда тревожная система поставлена на охрану. Отображается в следующих окнах программы:

- в окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система поставлена на охрану с тревогой по входу (принудительная постановка на охрану)

Эта анимированная иконка появляется когда происходит постановка на охрану и одна из областей в тревоге. Система будет позволять вам ставить на охрану в режиме принудительной постановки. Иконки будут отображать тревогу по входу:

- в окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система в режиме задержки постановки на охрану

Эта анимированная иконка появляется, когда система находится в режиме задержки постановки на охрану (ожидая подтверждения с запросом на постановку на охрану при попомщи входа). Отображается в следующих окнах программы:

- в окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система снята с охраны

Эта анимированная иконка появляется когда, тревожная система снята с охраны. Отображается в следующих окнах программы:

- В окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система в режиме задержки на вход

Это анимированная иконка появляется, когда тревожная система находится в режиме задержки на вход. Отображается в следующих окнах программы:

- В окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Тревожная система в режиме задержки на выход

Эта анимированная иконка появляется в режиме задержки на выход. Отображается в следующих окнах программы:

- В окне Manual Operation (Ручное управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Состояние тревожной системы еще не известно

Эта анимированная иконка появляется, когда состояние тревожной системы неизвестно. Отображается в следующих окнах программы:

- В окне “График” (Desktop (APM)> Graphic desktop (Рабочий стол графических схем)), когда состояние тревожной системы неизвестно.

Тревожная система в режиме отложения

Эта анимированная иконка появляется, когда тревожная система находится в режиме отложения. После того, как эта задержка истечет, система будет инициировать задержку на выход и пытаться вновь поставить систему на охрану (если не установлено расписание о запрете постановки на охрану). Отображается в следующих окнах программы:

- В окне Operation (Управление)
- Desktop (APM)> Graphic desktop (Рабочий стол графических схем).

Контроллеры

Анимированные иконки контроллеров указывают статус контроллера двери в окне графики (Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)) или в окне “Operation” (Управление).

Статус неизвестен

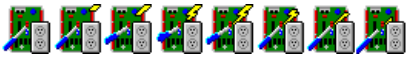
Эта иконка появляется в том случае, когда приложение EntraPass не получило информацию о статусе компонента после четырёх (4) попыток. Отображается в следующих окнах программы:

- Окно "Operation" (Управление): тревоги, области, туры охранников, двери, двери лифтов, реле, входы, повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Потеря напряжения в сети питания переменного тока контроллера

Иконка появляется в случае возникновения перебоя в питании контроллера. Отображается в следующих окнах программы:

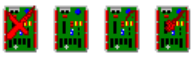
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- меню Operation (Управление) > Controller Reset (Перезагрузка контроллера), Controller AC failure (Сбой в питании контроллера) и Tamper Switch in “alarm” (тревога по тамперу)



Эта иконка отображается, когда возникает сбой в питании контроллера и тревога по тамперу контроллера. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем
- Operation (Управление) > Controller Reset (Перезагрузка контроллера)

Отсутствует связь с контроллером



Иконка появляется, когда нет связи с контроллером. Отображается в следующих окнах программы:

- Меню “Operation” “Управление” — “Область”, “Туры обхода охранника” и окна “Controller Reset” (Сброс контроллера).
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Связь с контроллером в норме (всё нормально)

Эта иконка указывает на наличие нормальной связи с контроллером. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Controller Reset (Перезагрузка контроллера)

Статус контроллера пока неизвестен

Иконка появляется в том случае, когда статус контроллера ещё неизвестен. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Контроллер перезагружается, сбой в питании

Иконка появляется в тех случаях, когда контроллер находится в состоянии перезагрузки и в сети питания отсутствует напряжение. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset (Перезагрузка контроллера)

Контроллер перезагружается, сбой в питании, тревога по тамперу

Иконка появляется в тех случаях, когда контроллер находится в состоянии перезагрузки, в сети питания отсутствует напряжение, и тревога по тамперу. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Controller Reset (Перезагрузка контроллера)

Контроллер перезагружается и тревога по тамперу

Эта иконка показывает, что контроллер находится в состоянии перезагрузки и тревога по тамперу. Отображается в следующих окнах программы:

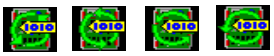
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Controller Reset (Перезагрузка контроллера)

Тревога по тамперу

Тревога по тамперу. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > (Перезагрузка контроллер, тампер в тревоге).

Повторная загрузка прошивки контроллера



Иконка появляется, когда загружается прошивка контроллера. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Controller Reset (Перезагрузка контроллера)

KT-400 проблема контроллера

Появляется, когда возникают проблемы с контроллером KT-400. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Controller (Контроллер)

Двери

Анимированные иконки дверей указывают статус дверей в графическом окне (на рабочем столе) или в окне “Operation” (Управление).

Принудительно открыта дверь

Иконка появляется в тех случаях, когда дверь находится в открытом состоянии, но доступ к этой двери не был предоставлен, и не было получено разрешение на выход. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери), Elevator Door (Двери лифтов)

Дверь принудительно открыта (считыватель отключен)

Иконка появляется в тех случаях, когда дверь находится в открытом состоянии, хотя доступ к этой двери не был предоставлен, и не было получено разрешение на выход, и считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Door (Двери), Elevator Door (Двери лифтов

Дверь закрыта и заблокирована

Иконка показывает, что дверь находится в закрытом состоянии и заблокирована. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери)

Дверь закрыта и заблокирована (считыватель отключён)

Иконка показывает, что дверь находится в закрытом состоянии и заблокирована, а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

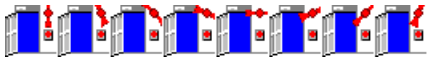
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери)

Статус двери неизвестен

Эта иконка появляется в том случае, когда статус двери ещё неизвестен. Отображается в следующих окнах

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Дверь открыта слишком долго



Иконка показывает, что дверь находится в открытом состоянии дольше, чем это допустимо в соответствии с установленным значением параметра “Open time” (Длительность открытия двери). Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери), Elevator Door (Двери лифтов)

Дверь открыта слишком долго (считыватель отключён)

Эта анимированная иконка показывает, что дверь находится в открытом состоянии дольше, чем это допустимо в соответствии с установленным значением параметра “open time” (Длительность открытия двери), а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери), Elevator Door (Двери лифтов)

Дверь открыта и разблокирована вручную

Иконка показывает, что дверь находится в открытом состоянии и разблокирована оператором. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов)

Дверь открыта и разблокирована вручную (считыватель отключён)

Иконка показывает, что дверь находится в открытом состоянии и разблокирована оператором, а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов)

Дверь открыта и разблокирована по расписанию

Иконка показывает, что дверь находится в открытом состоянии и разблокирована в соответствии с расписанием. Отображается в следующих окнах программы:

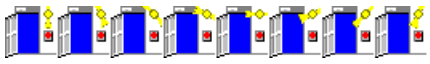
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов)

Дверь открыта и разблокирована по расписанию (считыватель отключён)

Иконка показывает, что дверь находится в открытом состоянии и разблокирована в соответствии с расписанием, а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов) .

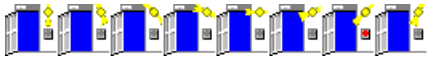
Предтревожное состояние двери при слишком долгом открытии



Иконка показывает, что дверь находится в открытом состоянии более половины времени, допустимого для оставления двери открытой. Отображается в следующих окнах программы

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов) .

Предтревожное состояние двери при слишком долгом открытии (считыватель отключён)



Иконка показывает, что дверь находится в открытом состоянии более половины времени, допустимого для открытия двери (Open time), а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) > Elevator Door (Двери лифтов) .

Дверь ещё открыта, хотя расписание уже не действует

Иконка показывает, что дверь находится в открытом состоянии, а расписание разблокировки уже не действует. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Дверь ещё открыта, хотя расписание уже не действует (считыватель отключён)

Иконка показывает, что дверь находится в открытом состоянии, хотя расписание разблокировки уже не действует, а кроме того, считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Дверь разблокирована оператором

Иконка показывает, что дверь разблокирована оператором (вручную). Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Door (Двери) > Elevator Door (Двери лифтов)

Дверь разблокирована оператором (считыватель отключён)

Иконка показывает, что дверь разблокирована оператором (вручную), а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Дверь разблокирована по расписанию

Иконка показывает, что дверь разблокирована в соответствии с расписанием. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Дверь разблокирована по расписанию (считыватель отключён)

Иконка показывает, что дверь разблокирована по расписанию, а считыватель находится в отключённом состоянии. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Дверь лифта разблокирована и закрыта

Иконка показывает, что дверь лифта находится в закрытом состоянии и разблокирована. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Door (Двери) / Elevator Door (Двери лифтов) .

Реле

Анимированные иконки реле указывают статус реле в графическом окне (на рабочем столе) или в окне “Operation” (Управление).

Реле активировано тревогой в тревожной системе

Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем) для реле, которое активируется тревогой в тревожной системе.
- Operation (Управление) > для реле, которое активируется тревогой в тревожной системе.

Реле активировано функциями тревожной системы

Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем) для реле, включенное при помощи функции трвожной системы.
- Operation (Управление) > для реле, включенное при помощи функции трвожной системы.

Реле активировано при помощи задержки тревожной системы

Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем) для реле, включенное при помощи задержки тревожной системы.
- Operation (Управление) > для реле, включенное при помощи задержки тревожной системы.

Реле активировано по событию

Эта иконка показывает, что срабатывание реле вызвано событием. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле временно активировано по событию

Иконка показывает, что реле временно активировано, и его срабатывание вызвано событием. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле активировано по входу

Эта иконка показывает, что произошло срабатывание реле по входу. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле временно активировано по входу

Иконка показывает, что реле временно активировано, и срабатывание произошло по входу. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле активировано оператором

Иконка показывает, что реле активировано оператором. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле временно активировано оператором

Иконка показывает, что реле временно активировано оператором. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле активировано по расписанию

Иконка показывает, что реле активировано в соответствии с расписанием. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Реле деактивировано

Иконка показывает, что реле деактивировано. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Relay (Реле)

Relay status unknown

Иконка показывает, что статус реле ещё неизвестен. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Входы

Анимированные иконки этого типа служат для указания статуса входов в графическом окне (на рабочем столе) или в окне “Operation” (Управление).

Тревога по входу – вход не контролируется

Иконка показывает, что вход находится в состоянии тревоги, а расписание мониторинга входа не достоверно. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу - вход контролируемый

Иконка показывает, что вход находится в состоянии тревоги, и расписание мониторинга входа верно. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу в ручном режиме — вход неконтролируемый

Иконка показывает, что вход находится в состоянии тревоги в ручном режиме, а расписание мониторинга входа не достоверно. Вход не контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу в ручном режиме — вход контролируемый

Иконка показывает, что вход находится в состоянии тревоги в ручном режиме, а расписание мониторинга входа верно. Вход контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу в ручном режиме на время— вход контролируемый

Иконка показывает, что вход находится в состоянии тревоги в ручном режиме временно, а расписание мониторинга входа верно. Вход контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу - вход не контроллируется

Иконка показывает, что вход находится в состоянии тревоги, а расписание мониторинга входа не верно. Вход не контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу – шунтирован оператором/замаскирован

Иконка показывает, что вход находится в состоянии тревоги и этот вход зашунтирован/замаскирован оператором:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу - вход контроллируется

Иконка показывает, что вход находится в состоянии тревоги, а расписание мониторинга входа верно. Вход контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу - вход контроллируется оператором

Иконка показывает, что вход находится в тревожном состоянии и контролируется оператором (продолжающиеся мониторинг). Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Вход с нормальным статусом – не контролируется

Иконка показывает, что вход находится в нормальном состоянии, а расписание мониторинга входа не достоверно. Вход не контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Тревога по входу – шунтирован оператором

Иконка показывает, что вход находится в нормальном состоянии и отключён от мониторинга (шунтирован/замаскирован) оператором. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Вход в нормальном состоянии – вход контролируется

Иконка показывает, что вход находится в нормальном состоянии, и расписание мониторинга входа достоверно. Вход контролируется. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Вход в нормальном состоянии – вход контролируется оператором

Иконка показывает, что вход находится в нормальном состоянии и контролируется оператором (продолжающиеся мониторинг). Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Input (Входы)

Статус входа неизвестен

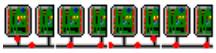
Эта анимированная иконка появляется на рабочем столе “Graphic” (Графические схемы), если статус входа ещё не определён.

Лучи/Сайты и Шлюзы

Анимированные иконки этого типа указывают состояние сайта/луча или шлюза в окне графических схем (на рабочем столе) или в окне “Operation” (Управление).

Луч контроллера:

Статус луча пока неизвестен



Иконка появляется в том случае, когда статус луча ещё неизвестен. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Луч с контроллерами подключён

Иконка показывает, что луч подключён и связь в порядке. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Reload data (Повторная загрузка данных)

Луч с контроллерами подключён и находится в состоянии повторной загрузки данных “reload data”

Иконка показывает, что сайт подключён и имеет состояние повторной загрузки данных. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Reload data (Повторная загрузка данных)

Луч с контроллерами – нет связи

Иконка показывает, что луч не подключён, и с ним нет связи. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Управление) > Reload data (Повторная загрузка данных)

Шлюз:

Шлюз – нет связи

Иконка показывает, что со шлюзом нет связи. Отображается в следующих окнах:

- Окно "Operation" (Управление): двери, двери лифтов, реле, входы, повторная загрузка данных шлюза
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Шлюз в состоянии повторной загрузки данных (Reload Data)

Иконка показывает, что на шлюзе выполняется повторная загрузка данных. Отображается в следующих окнах:

- Окно "Operation" (Управление): двери, двери лифтов, реле, входы, повторная загрузка данных шлюза
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Шлюз – обрыв связи во время повторной загрузки данных

Иконка показывает, что во время повторной загрузки данных произошла потеря связи со шлюзом. Отображается в следующих окнах:

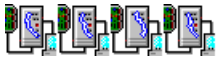
- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Связь со шлюзом в норме (всё нормально)

Эта иконка указывает на наличие нормальной связи со шлюзом. Отображается в следующих окнах:

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Проблемы со шлюзом



Иконка появляется, когда нет связи со шлюзом. Отображается в следующих окнах:

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Проблемы со шлюзом во время перезагрузки

Иконка показывает, что во время перезагрузки отсутствует связь со шлюзом. Отображается в следующих окнах:

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Шлюз (Программный интерфейс Шлюза):

Шлюз в норме – есть связь

Иконка показывает, что связь со шлюзом в порядке. Отображается в следующих окнах

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Шлюз в состоянии повторной загрузки данных (Reload Data)

Иконка показывает, что на шлюзе выполняется повторная загрузка данных. Отображается в следующих окнах:

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Шлюз – нет связи

Иконка показывает, что со шлюзом нет связи. Отображается в следующих окнах:

- Окно "Operation" (Управление): повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем

Шлюз—Перезагрузка прошивки на KT-NCC

Когда система производит автоматическое обновление прошивки на KT-NCC. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем
- Окно "Operation" (Управление)

Приложения EntraPass

Состояние приложения пока неизвестен

Иконка показывает, что статус приложения ещё неизвестен. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Приложение пытается установить связь

Иконка появляется, когда приложение рабочей станции обращается к серверу. Отображается в следующих окнах:

- Окно запуска Startup

Приложение – нет связи

Иконка показывает, что с рабочей станцией нет связи. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Окно "Operation" (Управление): тревоги, области, туры обхода охранником, двери, двери лифтов, реле, входы, повторная загрузка данных шлюза

Прочее

Инициализация базы данных

Иконка появляется, когда рабочая станция проверяет базу данных. Отображается в следующих окнах:

- Окно запуска Startup

Данные недоступны

Эта анимированная иконка предназначения для отображения переходного режима. Она показывает, что запрашиваемая информация в текущий момент недоступна.

Статус недоступен

Эта анимированная иконка предназначения для отображения переходного режима. Она показывает, что запрашиваемый статус компонента в текущий момент недоступен. е.

Статус выхода пока неизвестен

Иконка показывает, что статус выхода ещё неизвестен. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Статус неизвестен

Эта иконка появляется в том случае, когда рабочая станция не получила информацию о статусе компонента после четырёх (4) попыток. Отображается в следующих окнах:

- Окно "Operation" (Операции): тревоги, области, туры обхода охранником, двери, двери лифтов, реле, входы, повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Обнаружена ошибка

Иконка появляется в случае обнаружения определённой ошибки. Отображается в следующих окнах:

- Окно "Operation" (Операции): тревоги, области, туры обхода охранником, двери, двери лифтов, реле, входы, повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Неизвестный компонент

Иконка показывает, что указанный компонент не существует. Отображается в следующих окнах:

- Окно "Operation" (Операции): тревоги, области, туры обхода охранником, двери, двери лифтов, реле, входы, повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем) t.

Алфавитный указатель

3rd party hardware
Configuration 168
DLL integration 496

A

Abort report if free space lower than (MB) 491
Access
Levels
Create groups 352
Disarming 179
Primary access level 291
Privileged access level (dual custody) 151
Schedule 277
Schedule
Tenants 342
Acknowledging alarms
Acknowledge schedule 428
Using the alarm message box 69
Activate relay temporarily 162
Advanced schedule capability 482
Alarm
Message box 69
Response time 161
Alarm Systems
Arming procedure 273, 274
Definition 177
Disarming procedure 179, 274
Postpone procedure 274
Animated icons
Alarm systems 560
Controllers 562
Doors 564
Relays 568
Anti-passback
Жесткий запрет повторного прохода 130
Areas
Definition 187
Passback type 187
Authentication
Password Modification 472

B

Background
Web page 197
Backlight delay (KTES) 138
Backup 509
Автоматический 500
Папка назначения 500
Планировщик по расписанию 498, 499
Раздельные файлы 500
Самораспоковывающиеся архив 500
Тип backup 500
Badging 4
Creating a badge 304
MCI 295
Видео изображение 295
Вставить изображение из буфера 295
Захват видеоизображения 493
Извлечь изображение из файла 295
Редактирование макета пропусков 305
Bandwidth
Video 479
Battery trouble (KTES) 140
Broadcasting/Посылка широковещательного запроса 257
Buffer (KTES) 140

C

Camera
Definition 224
Card
Access group
Definitions 324
Access levels to cardholders 291
Assign a picture 295
Assigning a Picture from a File 295
Card access group 291
Card format 470
Card number 286
Change card format
Decimal 470
Create a day pass 329
Create card types 328
Creation date 287
Database fields
Supervisor parameters 409
Default card format 470
Definition 284
Enhanced user management 494
Format Selection 470
Information fields 285
Keep picture on desktop 374
Last transaction files
Rebuild 519
Last transactions 322
Management
WebStation 494
Modifications count 285
Passback option 294
Print a list of cards 319
State 293
Use count options 294
Use reports
Schedule mode 446
Validate card access 317
CardGateway
Mirror Database and Redundant Server 74
Oracle/MS-SQL Interface 72
Cardholders

Access Levels 291
Checking Server and Workstation Databases 504
Communication protocol 105
Communication timing 103
Component links
Display 58
Configuration
3rd party hardware 168
Controllers 110
Doors 143
EntraPass Gateways 85
External Global Gateway 32
Mirror Database and Redundant Server 74
Oracle/MS-SQL Interface 72
Sites/Loops 102
Contact
Interlock 149
Controllers
Configuration 110
controller local area
KT-400 130
Create groups 348
Express setup 539
Local area 144
Loop baud rate 104, 534
Loop RS-232 configuration 92
Reset 260
Status (graphic view) 361
Corporate gateway
Configuration 86
Express Setup 533
Corporate шлюз
Dual шлюзы 65, 86
Credentials
Enhanced user management 494
CSV Import/Export 333
Exporting procedure 335
Импорт идентификационных карт 337
Создание нового шаблона 333
Custom language
KTES 524
Custom Messages 502

D

Database
Checking 504
Logical components (view) 435
Structure 434
Utility program
Swap descriptions 518
Verify Database hierarchy 518
Verify Database links 517
Verify Time & Attendance files 518
Date and time on separate fields 490
Day Pass Definition 329
Daylight saving time 103
Decimal 470
Definition
Day Pass 329
Graphic 195
Host modem 86
Delays
Before unshunt 163
DEOL
Двойной оконечный резистор 163
Desktops
Alarms 384
Alarms desktop
Display instruction screen 390
Purge deleted log 386
Filtered messages 380
Messages desktop
Message type 373
Status bar
Server 506
Dial-up modem 107
DirectX Отключение 479
Disabling
Card readers 266
Video 66
Disk free space threshold
Server 480
Video Vault 81
Disk space
Video Vault 81
Displaying component links 58
DLL integration
3rd party hardware 496
Doors 63
Create groups 349
Elevators 149
Events 152
Open reading 147
Return to schedule 263, 266
REX options 147
Unlock reading 147
Команда Переключить/Toggle 211
Dual шлюзы
Global шлюз 65, 86
Duress
Duress on access denied 139
Duress on access granted 139
Keypad duress key 139

E

Edit system components 27
Elevators
Cab
Doors 144
Control
Unlock schedules (elevator floors) 150
Controllers 115

Create floor groups 353, 354
Create floors 192
Doors 149
REB-8s 116
E-mail
Максимальное количество событий для стандартного отчета 491
Email
Options 70
Reports 70
Task builder 207
Enabling
Arming request schedule 155
Card readers 266
Duress function on KTES keypad 155
Fail-soft delay (KTES) 136
Video capture 478
Encryption 66
End-of-line
KT-400 110
KTES 136
KT-MOD-INP16 module 125
Override default 162
Enhanced user management
Credentials 494
Enter network tag 210
EntraPass
Configuring 64
Запуск APM 45
Запуск сервера 42
Ethernet polling 534
Ethernet опрос
Настройка 106
Event trigger
Task builder 204
Events
Buffer
Controller 109
Color 428
Doors 152
Parameter definition 426
Print parameters 430
Expansion Modules
Configuring 124
Exported Video 251
Express Setup 49, 531
Controllers 538
KTES 539
Настройка конфигурации сайта/луча на шлюзе Corporate 533
Express setup
Контроллеры 538
Extended number of ring before answer (KTES) 135
Extended selection box 54
Extended talk time (KTES) 135

F

Fail-safe
Doors 143
Fail-secure
Doors 143
Find user timeout delay (KTES) 139
FIPS 470
Floor
Confirmation 118
Definition 192
Group 354

G

Gateway
Animated icons 573
Configuration 85
Configuring 71
Data reload 256
Global
External configuration 32
Hard reset 256
Soft reset 256
Starting 44
General parameters 65
Global шлюз
Dual gateways 65
Dual шлюзы 86
Graphic
Definition 195
Icons
Assigning system components 199, 200
Printing system components and graphics 200
Groups
Access levels 352
Doors 349
Floors 353
Inputs 351
Relays 350
Guard Tours
Definition 190
End guard tour 275
Start guard tour 275
Дверь/Вход 191
Действия в ручном режиме 275
Запуск тура 275
Изменить задержку для следующего пункта 276
Изменить следующую станцию 276
Настройки задержки 191
Окончание тура 275
Предтревожная задержка 190
Разблокировать дверь 191

H

Hard anti-passback 130, 144

Hardware
Definition 103
HDD
Граница свободного пространства на диске, Мб 480
Интервал между уведомлениями, ч 481
Heater kit activated (KTES) 140
Hide PIN number (KTES) 138
Historical Reports 441
Automatic report schedule screen 446
Desktop 381
Holiday
Definition 203

I

Immediate call 140
Import/Export 333
Input module
End-of-line 125
Inputs
Abnormal condition 161
Alarm system options 156
Animated icons 570
Arming request 155
Continuous supervision 271
Create groups 351
Group 351
Normal 271
Normal condition 161
Instructions
Assign to events 428
Definition 431
Integrated component
Configuration 171
Interlock options
Mantrap 148
Interval 176
IP Link 487

K

Kantech controllers
Configuration 111
Kantech IP Link 104
Kantech Telephone Entry System
Настройка 134
Опции 136
Keypad
Enable duress function 146
Relay activation 146
Клавиша ESC 115
Опции
Двери 145
KT-100
Configuration 114
KT-200
Expansion devices 115
Дополнительных устройства 115
Настройка 115
KT-2252
Elevator controllers 115
Program 116
Контроллеры лифтов 116
KT-300
Контроллер
Конфигурация 119
Модули расширения по шине Combus
Настройка 120
KT-400
Configuring 122
Controller local area 130
End-of-line 110
Ethernet 4-х дверный контроллер 104
Ethernet four-door controller
Configuration 122
Expansion modules 124
Автономный режим 324
Модули расширения
Настройка 124
Назначение локальных областей 131
Связи с этажами лифта
Назначение 132
Уровни доступа 324
KTES
Custom language 524
End-of-line 136
Express Setup 539
Fail-soft delay 136
General parameters 134
Language and Welcome messages 137
LCD настройки 138
Options 138
Pager reporting 141
Postal lock 135
Relays parameters 139
Serial number 136
Setup Wizard 134
Supervision schedules 139
Wiegand интеграция 137
Жилец уровени администратора 142
Настройка телефонной линии 136
Настройки звонка посетителя 134
Настройки ответа жильцом 136
Опции входа под принуждением 139
События коды пейджера 141
Сообщения приветствия 137
Список Жильцов 135
KT-MOD-INP16 124
End-of-line 125
KT-MOD-OUT16 124
KT-MOD-REL8 124
KT-NCC 85
Gateway 95
Двери 150

Настройка 95

L

Language
Custom 524
KTES 137
LCD настройки (KTES) 138
Limit video bandwidth 493
Line monitoring (KTES) 136
Line Type (KTES) 136
Local area after 144
Local area before 144
Lock
Door temporarily 263
Elevator door 266
Elevator door temporarily 266
Group of doors 263
Power trouble (KTES) 140
Login
Name 402
Logout and Idle 481

M

MAC address 104
Mantrap 148
Interlock options 148
Manual Operations
Arm door 263
Disable card readers 263
Disable reader 266
Disarm door 263
Enable card readers 263
Enable readers 266
Lock door or group of doors 263
Lock elevator door 266
Temporarily lock door 266
Temporarily lock/unlock door or group of doors 263
Temporarily unlock door 266
Unlock door or group of doors 263
Unlock doors 266
Master Password
New 472
Maximum event for email report 491
Migrate to enhanced user management 495
Mirror Database and Redundant Server
CardGateway 74
Modem
Call type 153
Dial-up 107
Параметры задачи 208
Motor lock delay 154
Multimedia Devices 469, 477
Signature capture 478
Video options 478
Muster reports 354
Area group 354
Reports 460

N

NCC - Глобальные преимущества 485
NCC 8000 Шлюз
Настройка 90
Программа просмотра 92
Установка 30
Network
Alarm 483
Alarms
Desktop 395
Next character delay (KTES) 139
Number of rings before answer (KTES) 135

O

Open time 145
Operators
Allow login on server 408
Login name 402
Login schedule 404
Password 403
Options and alarm system 154
Oracle/MS-SQL Interface
CardGateway 72
Output
Device configuration 166
Override
End-of-line 162

P

Pager
Call type 152, 161
Reporting (KTES) 141
Panel
DLL integration 496
Parameters
Credentials 494
Integration 496
Parse user name 491
Passback
Type 187
Password
Change master password 472
Pictures
Transparent color position 489
PIN
Number 115, 293
Дублировать идентификационный PIN код 471
Polling (KTES) 135
Port number 534
Postal lock

Card holder used for postal activated 137
KTES 135
Power failure (KTES) 140
Power supervision schedule 114
KTES 139
Pre-alarm on door opened too long 147
Prevent arming request on input status 156
Print a log 386, 395
Print event parameters 430
Printer, see Log printer 474
Printers Selection and Configuration 474
Programming mode timeout delay (KTES) 139
Programming PIN timeout delay (KTES) 139

Q

Quick report
Send to workstations 454
Viewer 543

R

REB-8
Контроллеров лифтов
программирование 117
Реле
Назначение 118
Релейные модули расширения 115
Redundant Server
Auto-restart delay 481
CardGateway Limitations 74
Quick synchronize 481
See Mirror Database and Redundant Server 74
System parameters 481
Registration
see Workstation registration 513
Server 513
System 503
Relays
Activated 269
Activation (KTES) 139
Alarm system options 157
Create groups 350
Deactivated 269
Operation mode 158
Parameters (KTES) 139
Resetting schedule 270
Return to schedule 269
Temporarily activated 269
To follow lock output 155
Relock
Door on arming after exit delay 156
Door on request to arm 156
On access 147
On door closing 147
On door opening 147
Removing EntraPass 38
Report input in alarm when the alarm system is armed 485
Reports
Historical report 441
Muster report 460
Report state 465
Roll Call report 463
Time & Attendance report 455
Time & Attendance request 454
View report 466
Resettable REX function 148
Restrict Access 151
REX 115
Contact 148
Options
Doors 147
Primary and Secondary 148
Roll Call
Reports 463
RS-232
Настройка шлюза 91
Сериный порт для луча 534
Соединение
Настройка 103

S

Schedules
2-day continuous interval 176
Acknowledge schedule 428
End time 175
Interlock 149
Login schedule (operators) 404
Postal Lock 135
REX 148
Start time 175
Supervision 139
Unlock 145
Unlock schedule # 1 (elevator doors) 150
Secondary access levels
Cards 283
Security level
Installer 402
Read only - (View components) 407
Security parameters 65
Selecting
Applications 411
Primary language 473
Serial
Com port 208
Number (KTES) 136
Устройства для команд 209
Server
Disk free space threshold 480
Getting Started 506
IP Address 534
Login 506

Logs 480
Registration 513
Service Login Information 484
Setting Up a Badge Printer 475
Show properties on Drop 198
Site
Configuration 102
Retrieving site events 108
SmartLink
Application 77
Command builder 210
Configuring 77
Restore previous SmartLink mode 206
Save SmartLink mode 206
Send reports to workstations 454
Task builder 210
WebStation 77, 79
Меню вставки задачи для SmartLink 205
Назначение команд SmartLink при использовании 431
Отправка отчётов на рабочие станции 454
Soft anti-passback 130, 144
Software installation 9
SPI Порт
KT-400 124
SQL Interface
See Oracle/MS-SQL Interface 72
Start a session 42
Starting the gateway program 44
State (cards), see Cards 293
Status
Time out delay 484
Supervised door lock device 154
Supervisor
Parameters
Card database fields 409
Suspend messages 66
Swap descriptions 518
System
Components 27
Data 509
Date & Time 476
Modification 476
Installation 14
Language selection 473
View log 512

T

Talk time (KTES) 135
Talk time remaining warning (KTES) 135
Tamper in alarm (KTES) 140
Tamper switch supervision schedule (KTES) 139
Task
Insertion menu for SmartLink 204
Task Builder
Definition 204
Emailing 207
Event trigger 204
Переключить/Toggle 211
Task Builder/Конструктор команд
График 195
Task/Задача
Параметры событий 428
TCP/IP 107
Tenant
End date 342
ID length 341
PIN length 341
Tenants list 341
Creating new 341
Wiegand display format on LCD 341
Tenants list
Export/Import Wizard 343
Terminal server 107
Time & Attendance Reports 449, 455
Operations 458
Preview 467
Request 454
Select doors 455
Time base (KTES) 136
Transfer to Unknown Area 162
Tree view 59

U

UDP 107
Unlock
Door temporarily 263
Elevator door 266
Elevator door temporarily 266
Group of doors 263
On access door opened 147
On REX 148
Schedules (elevator floors) 150
Time 144
Use JPEG format for graphics 490
Use JPEG format for pictures, signatures and badges 489
User Datagram Protocol (UDP) 107
User name format 491
Users 283

V

Validate Card Access 317
Video
Bandwidth 479
Bandwidth control 479
Linking video clips with key frames 243
Playing segments 241
Server options 492
Triggers definition 233
Vault

Configuring 80
Disk free space threshold 81
File format 82
Vault definition 222

W

Wait for access granted to arm 156
Web page
Background 197
WebStation
Card number 286
Email reports 70
Enhanced user management 494
SmartLink 77
Авторизация оператора 403
Архивные отчеты 442
Одновременная авторизация 405
Отчет по использованию карт 445
WebViews
Add Web page as background 197
Graphic definition 195
What is access control? 2
Wiegand
Display format on LCD 137
Reader type 137
Интеграция (KTES) 137
Windows
Плавающие окна 59
Workspace
Defining gateways and sites 412
Defining video servers 421
Definition 66
Selecting applications 411
Workstation
Suspend messages 66

Z

Автоматически
Автоматическая остановка guard tour в конце 191
Если не используется, автоматически закончить сеанс 481
Постановка на охрану 179
Расписание активации 158
Автономный режим 434
Авторизация
Расписание 404
Активация локального реле) 164
Анимированные иконки
Другие 576
Архивные отчеты
WebStation 442
режим расписания 446
база 3
База данных
Восстановление файлов по последней транзакции с картой 519
Имя выходного файла 439
Очистка базы данных 519
Показывать системные индексы базы данных 483
Проверка файлов видеособытий 518
Путь 439
Состояние 364
Тип выходных данных 439
Безопасный режим
Сообщения о работе в безопасном режиме 374
Блокировка двери вручную 264
Быстрый backup 481
Введите 32
Вид
Roll Call 279
Иерхаический режим просмотра 59
Видео
Вывод на экран окна видеонаблюдени 249
Журнал ошибок обработки видеоданных 493
Задний фон 197
Запись событий 225
Захват видеоизображения 493
Защита видеозаписей паролем 244
Изменение видеоокна 231
Назначение общих параметров для видеоокон 228
Настройка параметров связи видеосервера 220
Отключение DirectX 492
Параметры дистанционного видеонаблюдения 492
Параметры записи 234
Перезапустить приложение видеонаблюдения 492
Перезапустить систему управления приложениями по видеонаблюдению 493
Полоса пропускания видеоканала 493
Приложение по управлению предустановками и маршрутами 492, 493
Просмотр видеофрагментов из архива 252
Просмотр записей видео 246
Список событий видео 237
Экспортирование видео файлов 243
Включение
TFTP KT-NCC обновление 488
Карта уже занята 485
Расписание режима отложение постановки на охрану 157
Считыватель двери 265
Внешняя охранная панель
Интерфейсы системы 155
Внешняя тревога
Системные опции 155
Временная активация 193
Временная блокировка при антипасбеке 151
Временная разблокировка двери 264

Вставка серийных устройств для передачи команд 209
Вторичные уровни доступа
Автономный режим работы 291
Вторичные/дополнительные уровни доступа
Автономный режим 324
Входы
KTES 161
Анимированные иконки 570
Время отклика входа 161
вход для отложенной постановки на охрану 157
Вход прерывания постановки на охрану 184
Группа дверей 164
Дверь лифта 163
Дополнительный вход для постановки на охрану 184
Контакт на вход 184
Настройка 160
Настройка удалённого оповещения о событиях 164
Операции с входами при работе в ручном режиме 271
Переключить/Toggle команда 211
Расписание мониторинга 160
Тампер и проблема 163
Тревога, уровень№1 184
Тревога, уровень№2 184
Установка продолжительного контроля входа 272
Шунтирование при снятии с охраны 184
Шунтирование/Маскирование 162
Шунтировать/Маскировать 149
Выбор
Дополнительный язык системы 473
Контроллер 260
Шлюз 256
Выбор языков для работы с системой 473
Выход
Steady timed/Ровная работа, ограниченное время 167
Выбранные двери 166
Мигание 167
Мигание, ограниченное время/Flash 167
Период активации 166
Рабочий режим 166
Ровная работа/Steady 167
Установление связей событий дверей с дополнительными выходами 167
Выходы
Общие параметры 166
График
Задача 195
Состояние (вид контроллеров) 361
Графики
Оборудование других производителей 195
Сохранять графические схемы в файл 490
Графическая схема
Дизайн заднего фона 198
назначение 196
Групповое урправление с картами
Фильтр карт 332
Группы
Контроллеры 348
Области 354
Двери
Keypad Опции 145
KT-NCC 150
Анимированные иконки 564
Блокирование двери при постановке на охрану 183
Выбор двери 264
Группа 349
Контроль двери когда система поставлена на охрану 183
Назначение взаимной блокировки дверей ("Шлюз") 148
Назначение общих параметров 143
Опции дверного контакта 146
Опции и тревожная система 155
Разблокировать дверь (guard tours) 191
Дверной контакт
Опции
Двери 146
Диагностика 483
Диагностика PING по методу "запрос-ответ" 545
Разрешить диагностику сети 483
Дизайн фонового изображение 198
Для экстренных ситуаций
Отчеты Muster 460
Добовление системных компонентов 23
Доступ
Доступ и задержки 181
События 153
Управление пользователем 169
Уровни
Вторичные/Дополнительные уровни доступа
Уровни доступа 291
Вторичные/дополнительные уровни доступа 324
Назначение 326
Плохой 153
Постановка на охрану 155, 179
Уровень доступа для постановки на охрану 181
Уровень доступа для снятия с охраны 181
Жесткий запрет повторного прохода 130
Жилльцы
Список
Опции 135
Жильцы
Импорт списка жильцов 343
Уровень администратора (KTES) 142
Установки ответа (KTES) 136
Экспорт списка жильцов 344
Житель

PIN 341
Wigand интеграция с контроллером доступа 343
Время начала 342
Второй телефонный номер 341
Имя 341
Интерфейс Wiegand для доступа 342
Первый телефонный номер 341
Период действия прав доступа для жильца 342
Расписание доступа по PIN 342
Расширенная задержка на вход 342
Расшитренный звонок 342
Скрыть жильца 342
Список жильцов
Добавление нового жильца 341
Трассировка 342
Уровень администратора 342
Язык 342
Журнал событий
Журнал ошибок обработки видеоданных 493
Задержка на вход 182
Задержка шунтирования/маскирования 149
Задержки
Вход и Выход 156
До сообщения 208
Сброс задержки для временного шунтирования 162
Задний фон
Живое видео 197
Запрет повторного прохода
Мягкий запрет повторного прохода 130
Запрещение
Запретить вход в область, когда она полная 189
Запрос на снятие с охраны 157, 184
Запуск АРМ 45
Запуск сервера EntraPass 42
Звонить незамедлительно 161
Звонить немедленно 154
Иерхаический режим просмотра
Система 59
Иконки
Анимированные иконки 559
Интегрированная панель 168
Информация о звонке 208
Исполнение жесткого сброса Шлюза 256
Карт
Фильтр 332
Карта
FIPS 470
Группа доступа
Уровни доступа 324
Дата начала 293
Добавление подписи с помощью устройства оцифровки подписей 298
Жёсткий поиск по полям карты 491
Изменение даты 285
Изменение формата карт 470
Восьмеричный 470
Десятичный 470
Шестьнадцатиричный 470
Изменить дату 287
Импортирование подписи из файла 297
Имя пользователя 284
Как скрыть информационные поля карты 409
Картодержатель для доступа, предоставленного жильцом 343
Копировать в карту посетителей 284
местоположение карты уже верно (Области) 187
Назначение типов карт 328
Назначение фотографии из файла 295
Новая 284
Номер 284
Номер карты 286
Трассировка 287
Ограничение числа использований 294
Ограничить использование 294
Ожидание kepad 293
Отложенная 293
Отчет по использованию карт
WebStation 445
Печать 319
Печать электронных пропусков 301
Показать формат карты
Назначение 470
Получение фотографии с видеокамеры 296
Поля базы данных
Уровень безопасности 409
Потеряна 287
Просрочена 294
Сохранять фотографии идентификационных карт и подписи в файл 489
Сохранять фотографии посетителей и подписи в файл 489
Трассировка 287
Удалить когда закончится срок действия 293
Украдена 287
Формат карты
Использовать несколько форматов карт 471
Карты
Показать рядом с фотографией сведения о владельце карты 68
Кнопка многоточие 60
Код доступ пользователя 171
Контроллеры
Express setup 538
Анимированные иконки 562
Жесткий сброс 261
Мягкий сброс 261
Настройка 110
Перезагрузка прошивки 261
Контроль доступа 2
Конфигурация
EntraPass АРМ 64
Лифты

Выбрать кабину для активации группы этажей 164
Дверь
Выбор 267
Закрытие этажей 267
Назначение входа 163
Запретить доступ на этаж из лифта 268
Разрешить доступ на этаж лифта 268
Луч
Порт RS-232 534
Лучи
Анимированные иконки 573
Максимальное количество в области 189
Мастер код доуступа 170
Модем
Серийный порт 208
Тип вызова 161, 164
Мультимедийные устройства
Звук тревоги 477
Устройства оцифровки подписей 478
Мультимединые устройства
Настройка устройств оцифовки подписей 478
Мягкий запрет повторного прохода 130
Назначение
E-mail параметры 453
Посетитель 327
Расписание 175
Уровни доступа 326
Назначение взаимной блокировки дверей ("Шлюз")
Двери 148
Назначение общих параметров для KTES 134
Назначение уровня доступа для владельца карты 291
Нарисовать рамку 196
Настройка
Входы 160
Реле 158
Настройка времени опроса соединения 103
Настройка временной зоны между сервером и Шлюзом 191
Настройка дополнительных выходов 92
Не звонить 140, 154
Не производить звонок 161
Не разблокировать дверь по input, когда дверь поставлена на охрану 149
Несколько сообщений для предотвращения постановки на охрану 485
Области
Активировать реле когда область открыта 189
Количество ревизоров внутри области 188
Местоположение карты уже верно 187
Нормальный passback 187
Расписание запрета повторного прохода 188
Расписание перемещения 188
Ревизор passback 187
Ревизор для открытия области 188
Ревизор должен уходить последним 188
Управление областями в ручном режиме 277
Уровень ревизора 188
Обновление системы 34
Обновление физических компонентов 256
Оборудование других производителей
Графики 195
Управление 280
Ограниченная задержка на вход 151
Одновременная авторизация
WebStation 405
Ожидать разрешения/доступа для отложенной постановки на охрану 157
Оконечный резистор
Двойной 163
Операторы
WebStation авторизация 403
Выбор языка 403
Игнорировать фильтр сообщений на АРМ 403
Назначение 402
Ограничение авторизации 407
Отключение
Активация реле 158
Запретить синхронизацию по времени вручную 492
Считыватель двери 265
Отложить отчет на незапертую дверь 149
Отображать
Показывать описание на панели задач 482
Показывать список зарегистрировавшихся 482
Отображение
Отображать описание в строке заголовка 482
Последние транзакций с картой 322
Отчет по учету рабочего времени
Запрос 457
Отчеты
Roll Call отчеты 437
WebStation 442, 445
Быстрый отчет 438
Запрос отчета 450
По учёту рабочего времени 437
Отчеты Muster
Генерация Muster отчета 462
Для экстренных ситуаций 460
Использование Muster отчета для управлением парковкой 462
Контроль группы областей 392
Отчеты Roll Call
Muster Muster 460
Отчеты Архивные
Автоматическое назначение имени файла 449
Путь назначения с результатами 449
Язык отчета 449
Отчеты архивные
Предварительный просмотр 466
Состояние 382
Способ вывода 448
Отчеты учета рабочего времени
Правило первый приход и последний уход 456
Охранная панель

Оборудование других производителей 280
Охранная сигнализация
PowerSeries 168
Доступ предоставлен пользователем 169
Код доступ пользователя 171
Код доступа Мастер 170
Охранные панели
События 427
Очистить задний фон 197
Очистить комментарии 198
Очистить тревожные сообщения 68
Очищать тревожные сообщения 69
Панель инструметов
Кнопки 495
Параметры
АРМ 495
Видео 492
Время 494
Двери 143
Изображение 488
Отчеты 490
Прошивка 485
Шлюз 484
Параметры IP устройств 106
Пароль
Изменение аутентификационного пароля 472
Мастер пароль 472
Новый пароль 472
Оператор 402
Подтверждение ввода пароля 472
Пейджер
Опции 208
Тип вызова (KTES) 140
Пейджерг
Опции (KTES)
KTES
Опции пейджера 140
Переключить/Toggle
Task Builder 211
Печать идентификационных карт 319
Плавающие окна
Рабочий стол 59
Плавующие окна
Windows 59
Повторная загрузка данных шлюза 257
Подготовка электронных пропусков 4
Подтверждение тревог
Назначение и цель 387
Поиск
Жёсткий поиск по полям карты 491
Посетитель
Назначение 327
Настройка вызова (KTES) 134
Последовательность 191
Постановка на охрану при помощи считывателя 179
Потеряна карта 287
Приложение
Данные регистрации для работы в режиме службы 498
Если не используется, отправлять в трей 482
Требовать аторизацию для закрытия приложения 482
Принтер
Выбор и настройка принтера отчётов (Report Printer) 475
Принтер журналов/лог 474
Принудительная загрузка frimeware 257
Принуждение
Опции 130
Приостановить состояние обновления когда не контроллируется 161
Пространство на диске 480
Проход по двум картам 151
Рабочая область
изменения 48
Рабочее пространство
Назначение входов 414
Назначение графических схем 419
Назначение груп доступа 418
Назначение дверей 413
Назначение дверей guard tour 416
Назначение задач в Task builder 423
Назначение компонентов для охранных панелей 424
Назначение областей 416
Назначение окон видеонаблюдения 423
Назначение отчетов 419
Назначение охранных панелей 424
Назначение приложений 413
Назначение рабочего пространства 420
Назначение реле 414
Назначение событий 425
Назначение типов карт 417
Назначение тревожных систем 415
Назначение уровней доступа 415
Уровни безопасности 420
Рабочие столы
Сообщения рабочего стола
Задержка автоматического пролистывания 375
Несколько строк 374
Оставлять на экране фотографию карты 374
Отображать сообщения (полное описание) 375
Перевести на задний план 377
Показывать панель инструментов 374
Показывать пиктограммы 374
Показывать родительский элемент 377
Показывать события жирным шрифтом) 375
Последнее сообщение сверху 375
Сохранять свойства только вручную 375
Удалить все 376
Цветовой фон сообщений 375

Рабочий стол
Воспроизведение архивных видеозаписей из списка сообщений 383
Изменение свойств окна Pictures 378
Отобразить несколько фотографий 379
Плавающие окна 59
Рабочий стол архивных отчётов 381
Рабочий стол тревог
Графические схемы 391
Печатать журнал событий 386
Печатать журнал/лог 395
Подтверждение 386
Поставить флаг 386
Удалить журнал событий 386
Удалить журнал/лог 395
Сетевые тревоги
Рабочий стол 395
Разблокировка
Отпирать дверь по расписанию после входа первого посетителя 149
Разблокировка двери вручную 264
Расписание
Звонить 154
Разблокировка 150
Расписание не снимать с охраны 181
Расписание активации 193
Расписание для второй карты, доступ по двум картам 155
Расписания 482
Дни 175
Звонки 140, 161
карта и PIN 146
Назначение 174
Печатать события 428
Расписание запрета повторного прохода 188
Расписание перемещения 188
Расписание постановки на охрану 181
Расписания Глобальные 482
Расписания луча corporate 482
Расширенная задержка на вход 145, 153
Житель 342
Расширенное окно выбора 61
Расшитренный звонок
Житель 342
Ревизор
Внутри (области) 188
Открыть область 188
Ревизор должен уходить последним 188
Уровни (Области) 188
Региональные настройки (KTES) 136
Регистрация
Сервер 503
Система 21
Редактировать фоновое изображение) 196
Режим расширенного 285
Резервный сервер 481
Реле
Активация на отложение 185
Активация при задержке на выход, задержка 185
Активация реле когда область полная 189
Активировать временно 162
Анимированные иконки 568
Выбор 269
Группы 350
Задержка на вход - реле активация 185
Настройка 158
Переключить/Toggle 211
Режим активации 159, 193
Система на охране 185
Система снята с охраны 185
Состояние прерывания постановки на охрану 185
Ручные операции
Постановка на охрану 179
Снятие с охраны 179
Сброс
Задержка для временного шунтирования 162
Смотреть контроллеры 260
Сброс двери в работу по расписанию 265
Сервер
Параметры 480
Регистрация 503
Утилиты для базы данных 516
Сеть
Регулировка/синхронизация времени 494
Система
Иерхаический режим просмотра 59
Параметры 480
Расписания 482
Регистрация 21
Снятие с охраны при помощи считывателя 179
События
Инструкции (Назначение на события) 428
Коды пейджера (KTES) 141
Назначение связки Событие/Реле 193
Отобразить (расписание) 427
Параметры
Задача/Task 428
Печатать расписание 428
Просмотр связей 428
Расписание подтверждения 428
Реле
Назначение 193
Печать 194
Удаление и восстановление связей 429
Сообщение
Настройка 68
Сообщения
Назначения (Фильтр) 432
Подключение серийного устройства 208
Рабочий стол 373
Состояние
Активация реле
Настройка 129
Иконка

Обновить задержку 69
Сохранение
Комментарии 198
Специальные символы
Сообщения приветствия 138
Считыватели
Считыватель для постановки на охрану 182
Считыватель для постановки на охрану без разблокировки двери 183
Считыватель для режима отложения 183
Считыватель для снятия с охраны 183
Таймер временного шунтирования 162
Таймер временной активации реле 158
Тампер и проблема
Входы 163
Тампер и проблемы
Назначение 163
Трассирвка
Карта 287
Трассировка
Номер карты 287
Трбования компьютера 10
Тревога
Выбор звукового фала на тревогу 477
Назначение звука тревоги 477
Уровень приоритета звукового сигнала 477
Тревоги
Автоматическое подтверждение 403
Тревоги сетевые
Использовать сетевые тревоги 483
Максимальное число записей в списке сетевых тревог 483
Тревожная система
Блокирование двери при постановке на охрану 183
Возможности 177
Задержка на постановку на охрану 182
Задержка отложения постановки на охрану 182
Звонок реле 186
Контроль двери когда система поставлена на охрану 183
Постановка на охрану, приостановка и снятие с охраны 177
Разделы 177
Считыватель для снятия с охраны 183
Тревожные системы
Анимированные иконки 560
Вход прерывания постановки на охрану 184
Детекция периметра и внутренних зон 178
Дополнительный вход для постановки на охрану 184
Задержка на вход - реле 185
Задержка на выход 182
Закрытие дверей при постановке на охрану 183
контакт на вход 184
Общие входы 178
Процедура отложения постановки на охрану 180
Процедура постановки на охрану 178
Процедура снятия с охраны в ручном режиме 274
Раздел 181
Расписание не снимать с охраны 181
Расписание постановки на охрану (авто) 181
Реле - состояние Alarm#1 186
Реле - состояние Alarm#2 186
Реле отложения 185
Ручное управление 273
Снятие с охраны, когда по расписанию действует режим “No Disarm” 179
Состояние
Система на охране 185
Задержка состояния системы 185
Система снята с охраны 185
Состояние реле для прерывания постановки на охрану 185
Состояние активации при задержке на выход, задержка 185
Состояние задержки при постановке на охрану 185
Счетчик попыток режима отложения постановки 182
Считыватель для постановки на охрану 182
Считыватель для постановки на охрану без разблокировки двери 183
Считыватель для режима отложения 183
Тревога, уровень№1 184
Тревога, уровень№2 184
Уровень доступа для постановки на охрану 181
Шунтирование при снятии с охраны 184
Трей
Данные регистрации для работы приложения в режиме службы 498
Уведомление, тревога по входу когда система поставлена на охрану 485
Уведомлять о последнем выходящем из системы 482
Удаленно
Задержка модема 109
Оповещение о событиях
Включение 164
Удаленное
Приложение 479
Украдена карта 287
Управлением парковкой
Muster отчеты 462
Уровень безопасности
Рабочее пространство 404
Уровень безопасности для оператора
Назначение для оператора 404
Уровень безопасности оператора
Поля базы данных карт 409
Уровень безопасности охранника
Ограниченный 402
Уровень доступа для отложения/снятия с охраны 157

Уровни безопасности
Назначение 406
Рабочее пространство 420
Установить прозрачный объект 196
Утилита
Восстановление файлов по последней транзакции с картой 519
Очистка базы данных 519
Утилиты
Проверка файлов видеособытий 518
Физический адрес компонента 408
Фотографии
Отобразить несколько фотографий 379
Рабочий стол 378
Шлюз
Corporate
Dual Шлюзы 65
Dual шлюзы 86
Global
Dual Шлюзы 65
Dual шлюзы 86
Настройка 93
Анимированные иконки 573
Ручное управление 256
Шунтировать вход временно 162
Этаж
группа 164
Этажи
Группа 353
Язык
Оператор 403

KANTECH™

© 2010 Tyco International Ltd. and its Respective Companies. All Rights Reserved.
www.kantech.com