ENTRAPASS™

CORPORATE EDITION

Высокоэффективная комплексная система безопасности и контроля доступа

Справочное руководство

KANTECH™

DN1415-0810 / версия 4.01

Защита авторских прав © 2008 Холдинг *Tyco International*. Все права защищены. все спецификации верны на момент публикации брошюры и могут быть изменены без предварительного уведомления. Названия EntraPass, Kantech и логотип Kantech являются зарегистрированными товарными знаками холдинга Tyco International.

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

Особенности системы EntraPass 2

Руководство и справочная система EntraPass 5

Пользование справочным руководством 5

Обращение к справочной системе 5

Техническая поддержка 6

Архитектура системы 7

Глава 2 • Установка программного обеспечения 9

Системные требования к компьютеру 10

Сервер EntraPass WebStation 10

Дополнительные требования 10

Комплект установки 11

Порядок установки 12

Установка программного обеспечения EntraPass 12

Добавление дополнительных компонентов/функций 12

Установка системы 13

Регистрация системы 22

Регистрация системы 22

Дополнительные компоненты системы 25

Редактирование сведений о компонентах системы 28

Присвоение описательных имен приложениям 28

Связь с сервером EntraPass 29

Установление связи с сервером 29

Обновление системы 30

Перед обновлением программного обеспечения 30

Обновление программного обеспечения 30

Удаление программного обеспечения EntraPass 34

Глава 3 • Начало работы 37

Начало и окончание сессии 38

Запуск основного сервера EntraPass 38

Запуск программы Gateway 40

Запуск рабочей станции EntraPass Workstation 41

Получение сведений о статусе соединения с рабочей станцией 44

Изменение свойств рабочего пространства 44

Восстановление свёрнутых окон на рабочем столе 45

Автоматическая установка (Express Setup) 46

Автономные обслуживающие программы системы 47

Диалоговые панели инструментов EntraPass 48

Основные функции 50

Поиск компонентов 50

Окно расширенного режима поиска (Extended Selection Box) 53

Выбор компонентов 53

Выбор пути для хранения файлов 55
Порядок выбора определённого сайта или шлюза 55
Вывод на печать списка или отчёта 55
Отображение связей между компонентами 56

Глава 4 • Системные устройства 59

Конфигурация приложений EntraPass 60

Настройка конфигурации приложения EntraPass 61
Описание общих параметров (раздел General) 61
Описание параметров безопасности (раздел Parameters) 62
Описание рабочего пространства (раздел Workspace) 64
Описание параметров управления сообщениями (раздел Messages) 65
Описание параметров управления тревогами (раздел Alarms) 66
Описание сетевых тревог (раздел Network Alarms) 68
Описание параметров электронных отчётов (E-Mail Reports) 68
Настройка конфигурации приложения Шлюз (Gateway) 69
Описание общих параметров шлюза (раздел General) 70
Настройка интерфейса Oracle/MS-SQL (CardGateway) 70
Создание баз данных сервера вручную 73
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 86

Настройка конфигурации шлюза Corporate Gateway 87

Настройка конфигурации сайтов 91

Настройка таймаутов соединения 92
Настройка конфигурации соединения типа Direct RS-232 (прямое через RS-232) 92
Настройка конфигурации соединений типа Kantech IP Link или KT-400 Ethernet (только для шлюзов Corporate Gateway) 93
Настройка конфигурации соединения типа Ethernet Polling (опрос) 96
Настройка конфигурации соединения типа Dial-Up (RS-232) Modem (Связь через модем по коммутируемой линии) 97

Настройка конфигурации контроллеров 101

4-дверный Ethernet-контроллер KT-400 101
Особенности 101
Описание общих параметров (General) для контроллеров Kantech 102
Настройка конфигурации контроллера KT-100 104
Настройка конфигурации контроллера KT-200 105
Описание модулей расширения контроллеров KT-200 105
Описание дополнительных устройств для контроллера KT-200 105
Настройка контроллеров лифтов KT-2252 106
Настройка контроллеров лифтов REB-8 108
Описание реле REB-8 109
Настройка конфигурации контроллера KT-300 110
Настройка конфигурации модулей Combus с контроллером KT-300 111
Настройка конфигурации 4-дверного Ethernet-контроллера KT-400 113
Настройка конфигурации модулей расширения к контроллеру KT-400 115
Выбор типа срабатывания реле статуса (только для шлюзов Corporate Gateway) 122
Описание дополнительных функций контроллера 122
Описание локальных зон контроля для контроллера KT-400 124
Описание связей с этажами лифта для контроллера KT-400 125
Установление связей шаблонов (Pattern) с дверьми и номерами этажей 125

Сообщения контроллера о переполнении буфера событий 126

Конфигурация дверей (Door) ... 127
Описание общих параметров дверей (раздел Door) ... 127
Описание функций дверной кнопочной панели для контроллеров KT-100 и KT-300 ... 130
Для контроллеров KT-400 ... 130
Описание функций контактных датчиков открытия двери ... 132
Описание функций кнопки REX (Запрос на выход) ... 133
Описание функций взаимной блокировки дверей ("Ловушка") ... 134
Описание дверей лифта ... 135
Настройка событий дверей (раздел Door Events) ... 136
Описание функций для KT-100, KT-300 и KT-400 (только для шлюзов Corporate Gateway) ... 137
Настройка интерфейсов внешних охранных панелей ... 138
Конфигурация реле (раздел Relay) ... 142
Описание реле ... 142
Конфигурация входов (раздел Input) ... 143
Описание входов ... 143
Описание реле и входов ... 145
Описание входа для двери лифта ... 146
Настройка удалённого оповещения о событиях ... 147
Конфигурация выходных устройств ... 148
Описание общих параметров выходов (раздел Output) ... 148
Установление связей событий с дополнительными выходами ... 149
Глава 5 • Интеграция с системами видеонаблюдения ... 151
Конфигурация видеосервера ... 152
Настройка параметров связи видеосервера ... 152
Повышение уровня защищённости видеосерверов ... 154
Описание видеохранилища EntraPass Video Vault ... 155
Описание камер наблюдения ... 157
Описание камеры (раздел Camera) ... 157
Описание предустановок и маршрутов ... 158
Описание событий для записи камерой ... 159
Порядок выбора событий и расписаний для записи камерой ... 159
Установление связи камеры с иконкой ... 160
Описание видеоокон ... 162
Описание общих параметров видеоокон ... 162
Создание и редактирование видеоокон ... 165
Изменение видеоокна ... 165
События, инициирующие включение-выключение видеозаписи ... 167
Описание параметров инициирующих событий ... 167
Параметры записи (Recording Parameters) ... 169
Настройка параметров записи ... 169
Настройка параметров останова записи ... 170
Список видеособытий (Video Event List) ... 172
Порядок работы со списком видеособытий Video Event List ... 172
Поиск видеособытий ... 172
Воспроизведение видеофрагментов ... 178
Привязка ключевых кадров к видеозаписям ... 180

Экспортирование видеофайлов 181
Защита видеозаписей паролем 182
Воспроизведение видеофайлов 184
Просмотр видеозаписей в окне Video Playback 184
Записи, выполняемые в данный момент (Current Recording) 186
Просмотр текущих записей 186
Рабочий стол видеонаблюдения (Video) 188
Вывод на экран окна видеонаблюдения 188
Просмотр экспортированных видеофайлов 190
Просмотр видеохранилища EntraPass Video Vault 191
Просмотр видеофрагментов из архива видеохранилища EntraPass Video Vault 191
Глава 6 • Описания 193
Описание расписаний (раздел Schedule) 194
Описание расписания 195
Создание двухдневного интервала 196
Описание этажей (Floors) 197
Описание графических схем 198
Описание компонентов графических схем (раздел Graphic) 198
Создание фонового изображения для графического окна 201
Создание связей системных компонентов с графическими иконками 202
Описание праздников (раздел Holidays) 203
Глава 7 • Операции 205
Панель инструментов в окне Operation 205
Панель инструментов в меню Operation 205
Контекстное меню окна Operation 206
Окно статусов компонентов (Status) 206
Операции со шлюзом при работе в ручном режиме 208
Выбор шлюза 208
Выполнение жёсткой перезагрузки 209
Повторная загрузка данных шлюза 209
Операции с сайтами при работе в ручном режиме 210
Выполнение операций с сайтами при работе в ручном режиме 211
Сообщения о статусе соединения, доступные в списке меню 211
Операции с контроллерами при работе в ручном режиме 213
Выбор контроллера 214
Выполнение мягкой перезагрузки контроллера 214
Выполнение жёсткой перезагрузки контроллера 214
Повторная загрузка контроллера в ручном режиме 215
Загрузка прошивки контроллера вручную 215
Разблокировка клавиш считывателя вручную 215
Сброс счётчиков карт внутри и вне охраняемой территории или всех карт в локальной зоне контроля 215
Подсчёт числа карт внутри и вне охраняемой территории 215
Сброс счётчиков карт входящих и выходящих посетителей или всех карт в локальной зоне контроля 216
Операции с дверями при работе в ручном режиме 217
Выбор двери или группы дверей 218
Блокировка двери вручную 218

Разблокировка двери вручную 218
Временная разблокировка двери 218
Перезагрузка расписания двери 219
Разрешить использование считывателя карт на двери 219
Запретить использование считывателя карт на двери 219
Операции с дверями лифтов при работе в ручном режиме 220
Выбор двери лифта 221
Блокировка доступа на этажи через двери лифта 221
Разблокировка доступа на этажи через двери лифта 221
Временная разблокировка доступа на этажи через двери лифта 222
Перезагрузка расписания лифтовой двери 222
Разрешить доступ на этаж из лифта 222
Запретить доступ на этаж из лифта 223
Операции с реле при работе в ручном режиме 224
Выбор реле 224
Деактивация реле вручную 225
Активация реле вручную 225
Временная активация реле 225
Перезагрузка расписания реле 225
Операции с входами при работе в ручном режиме 226
Операции с входами при работе в ручном режиме 226
Ручной возврат входа в нормальное состояние 227
Прекращение мониторинга входа 227
Временное прекращение мониторинга входа (шунтирование) 227
Глава 8 • Пользователи 229
Описание карт (раздел Card) 230
Выпуск новой карты 230
Выпуск новой карты в режиме усиленного администрирования пользователей 231
Создание новых карт с помощью функции "Сохранить как..." 234
Выпуск карт с помощью функции "Групповая загрузка" (Batch Load) 234
Просмотр и проверка индивидуальных кодов 234
Просмотр карт с одинаковым кодом 235
Работа с идентификационными картами 236
Изменение карты 236
Поиск карты 236
Удаление карты 236
Индивидуальная настройка названий информационных полей идентификационной карты 236
Задание уровней доступа владельцам карт 238
Задание уровня доступа для владельца карты 238
Описание дополнительных функций карт 239
Добавление комментариев к карте 240
Ограничение числа использований карты 241
Привязка к картам фотографий и подписей 241
Импортирование фотографии из файла 242
Получение фотографии с видеокамеры 242
Импортирование подписи из файла 244
Добавление подписи с помощью устройства оцифровки подписей 245

Работа с фотографиями и подписями 246
Вырезание части изображения 246
Редактирование фотографии/подписи 249
Печать электронных пропусков 250
Выбор принтера электронных пропусков 250
Предварительный просмотр и печать электронных пропусков 251
Создание электронных пропусков 253
Создание шаблона электронного пропуска 253
Описание свойств для макета электронных пропусков 254
Редактирование макета пропусков 255
Изменение числа сторон идентификационных карт 255
Изменение цвета фона 257
Добавление объектов в макет пропусков 258
Вставка информационных полей карты 259
Выравнивание объектов в макете шаблона 261
Изменение свойств информационных полей карты 261
Изменение свойств изображений 263
Добавление объектов со статическим текстом 265
Добавление штрихкодов 266
Изменение свойств штрихкодов 268
Добавление текущей даты 268
Добавление изображения 271
Добавление других объектов 273
Добавление геометрических форм 274
Проверка уровня доступа карты 275
Печать идентификационных карт 277
Печать карт 277
Отображение последних транзакций с картой 281
Просмотр последних транзакций с картой 281
Описание групп доступа для идентификационных карт 283
Описание уровней доступа 284
Описание карт посетителей 285
Создание карты посетителя при создании новой карты 285
Создание карты посетителя при помощи шаблона карт 285
Описание типов карт 286
Создание нового типа карт 286
Описание разовых пропусков 287
Создание разового пропуска 287
Создание нового разового пропуска с помощью функции "Сохранить как..." 288
Операции с группами (Batch Operations) 289
Выполнение операций с группой карт 289
Импорт и экспорт файлов CSV 291
Использование уже настроенного шаблона 291
Создание нового шаблона для импорта/экспорта данных 292
Экспорт идентификационных карт 293
Импорт идентификационных карт 296
Исправление ошибок импорта/экспорта 298
Глава 9 • Группы 301
Создание групп контроллеров 302
Создание групп дверей 303

Создание групп реле 304
Создание групп входов 305
Создание групп уровней доступа 306
Создание групп этажей 307
Глава 10 • Статус системы 309
Список соединений 310
Просмотр списка соединений системы 310
Статус текста 312
Вывод на экран статусов компонентов 312
Цифровой статус (Numerical Status) 314
Графический статус (Graphic Status) 315
Просмотр статуса контроллера 315
Статусы видеосерверов 317
Просмотр статуса видеосерверов 317
Разрешение/запрет создания видеоархивов 317
Статусы баз данных 318
Статусы сервера (Server State) 320
Глава 11 • Системные настройки 321
Описание операторов 322
Создание нового или изменение настроек уже созданного оператора 322
Описание уровней безопасности пользователей 326
Создание/Изменение уровней доступа операторов 326
Описание регистрационных прав оператора 327
Как скрыть информационные поля карты 329
Выбор специальных кнопок для управления в режиме видеонаблюдения 330
Описание рабочего пространства 331
Использование фильтров для рабочего пространства 331
Выбор учётных записей 331
Выбор приложений EntraPass 332
Описание шлюзов и сайтов 334
Описание контроллеров 335
Описание дверей 336
Описание реле 337
Описание входов 338
Задание уровней доступа 338
Описание типов идентификационных карт 339
Описание групп доступа для идентификационных карт 340
Описание отчётов 341
Описание графических схем 343
Описание рабочего пространства 343
Задание уровней безопасности 344
Описание видеосерверов 345
Ограничение доступа для определённых камер наблюдения 346
Описание окон видеонаблюдения 348
Описание событий 348

Описание параметров событий 350
Описание параметров событий 350
Создание связей 353
Просмотр связей 354
Удаление и восстановление связей 354
Вывод на печать параметров событий 355
Описание команд 357
Описание команд 357
Описание команд SmartLink 358
Добавление в макрос SmartLink команд управления электронной почтой 359
Добавление в макрос SmartLink команды для отправки сообщения на пейджер 361
Описание фильтров сообщений 363
Описание события для фильтра сообщений 363
Описание структуры базы данных 367
Просмотр компонентов базы данных 367
Глава 12 • Рабочие столы EntraPass 369
Индивидуальная настройка рабочего пространства 370
Создание временного рабочего пространства 370
Изменение свойств экрана 372
Индивидуальная настройка специальных рабочих столов 373
Индивидуальная настройка рабочего стола оператором с полным доступом 373
Индивидуальная настройка рабочего стола для оператора с доступом "только для чтения" 374
Передача индивидуально настроенного рабочего стола 375
Рабочий стол сообщений (Message Desktop) 377
Просмотр и сортировка системных событий 377
Индивидуальная настройка параметров отображения событий на рабочих столах сообщений (Message Desktop) 378
Выполнение разных задач с системными сообщениями 380
Рабочий стол фотографий (Picture) 384
Изменение свойств окна Pictures 384
Рабочий стол избранных сообщений (Filtered Messages Desktop) 386
Настройка рабочего стола избранных сообщений (Filtered Messages Desktop) 386
Рабочий стол архивных отчётов (Historical Report Desktop) 387
Настройка рабочего стола архивных отчётов (Historical Report Desktop) 387
Создание и редактирование архивных отчётов на рабочем столе 388
Отображение статуса архивного отчёта в реальном времени 388
Воспроизведение архивных видеозаписей из списка сообщений на рабочем столе 390
Рабочий стол тревог (Alarms Desktop) 391
Описание рабочего стола тревог (Alarms Desktop) 392
Просмотр тревожных сообщений системы 393
Автоматическое отображение рабочих столов тревог 395
Подтверждение тревог/событий 397
Порядок подтверждения тревожных сообщений 398
Подтверждение тревоги в окне рабочего стола тревог 399
Рабочий стол команд (Instruction Desktop) 400
Просмотр команды к тревожному сообщению 400

Рабочий стол графических схем (Graphic Desktop) 402
Просмотр графических схем на рабочем столе Graphic Desktop 402
Рабочий стол сетевых тревог (Network Alarms Desktop) 404
Просмотр сетевых тревог 404
Рабочий стол видеонаблюдения (Video Desktop) 406
Описание рабочего стола видеонаблюдения 406
Порядок работы с рабочим столом видеонаблюдения 406
Статусы видеосерверов 408
Просмотр полного статуса видеосерверов 408
Глава 13 • Отчёты 411
Описание быстрых отчётов (Quick Report) 412
Описание быстрого отчёта 412
Описание архивных отчётов 415
Описание отчёта по умолчанию "All Events" (Все события) 415
Описание архивного отчёта с индивидуальными настройками 416
Описание компонентов для архивного отчёта с индивидуальными настройками 417
Описание дополнительных функций карт для архивного отчёта с индивидуальными настройками 418
Описание отчёта об использовании идентификационных карт 419
Настройка расписания автоматических отчётов 421
Дополнительные настройки автоматического отчёта 422
Описание выходного формата отчёта 423
Отчёты по учёту рабочего времени 424
Выполнение запроса архивных отчётов 425
Запрос отчёта о событиях 427
Отчёты, отправляемые по электронной почте 428
Настройка отчёта для отправки по электронной почте 428
Отправка отчётов на рабочие станции при помощи интерфейса SmartLink 430
Описание отчётов по учёту рабочего времени 431
Описание отчётов по учёту рабочего времени 431
Запросы отчётов по учёту рабочего времени 434
Как вручную запросить отчёт по учёту рабочего времени 434
Операции с базой данных по учёту рабочего времени 435
Добавление транзакции в базу данных по учёту рабочего времени 435
Статусы отчётов (Report State) 438
Просмотр отчётов 439
Отображение отчёта на экране 439
Предварительный просмотр архивных отчётов 440
Предварительный просмотр отчётов по учёту рабочего времени 441
Глава 14 • Опции системы EntraPass 443
Выбор формата карты по умолчанию 444
Описание формата представления идентификационных карт 444
Смена аутентификационного пароля 446
Порядок изменения аутентификационного пароля 446
Выбор языка интерфейса системы 447
Выбор языков для работы с системой 447

Выбор и настройка принтеров **448**
Выбор и настройка принтера журналов (Log Printer) 448
Выбор и настройка принтера отчётов (Report Printer) 449
Выбор и настройка принтера электронных пропусков (Badge Printer) 449
Изменение даты и времени системы **451**
Конфигурация мультимедийных устройств **452**
Выбор звукового сигнала тревоги 452
Описание параметров оцифровки изображений 453
Настройка устройства оцифровки подписей 454
Настройка системных параметров **456**
Параметры сервера (Server) 456
Журналы сервера (Server Logs) 456
Пространство на диске (Disk Space) 456
Резервный сервер (Redundant Server) 457
Окончание сеанса и бездействие (Logout and Idle) 457
Расписание (Schedule) 458
Диагностика (Diagnostic) 459
Сетевые тревоги (Network Alarm) 459
Индикация статусов на иконках (Icon Status) 460
Данные регистрации для работы в режиме службы (Service Login Information) 460
Параметры прошивки (Firmware) 460
KT-100 461
KT-300 461
KT-400 462
Kantech IP Link 462
Параметры изображений (Image) 463
Фотографии и электронные пропуска 463
Графические схемы (Graphic) 464
Параметры отчёта (Report) 465
CSV 465
Пространство на диске (Disk Space) 465
Формат имён пользователей (User Name Format) 466
Параметры видеонаблюдения (Video) 467
Параметры (Parameters) 467
Захват изображения (Snap) 468
Параметры времени (Time) 469
Параметры доступа (Credentials) 470
Карты (Card) 470
Рабочая станция и сервер 471
Кнопки на панели инструментов 471
Планировщик заданий по созданию резервных копий (Backup Scheduler) **472**
Настройка резервного копирования, когда сервер EntraPass работает в режиме службы 472
Настройка расписаний для автоматического создания резервных копий системной базы данных **475**
Специальные сообщения (Custom Messages) **477**
Настройка специальных сообщений 477
Регистрация системы (System Registration) **478**
Проверка баз данных на сервере и рабочей станции **479**
База данных сервера 479
База данных на рабочей станции 479
Глава 15 • Сервер EntraPass **481**
Запуск сервера **482**

Список соединений сервера (Connection list) 484
Просмотр приложений, подсоединённых к серверу 484
Просмотр системного журнала (System Log) 484
Просмотр системных ошибок (System Errors) 485
Резервные копии 487
Создание резервных копий типа D, A и T 487
Восстановление данных (D, A и T) 489
Использование утилит сервера 491
Выбор другого языка системы 492
Глава 16 • Системные утилиты 493
Database Utility (Утилита базы данных) 494
Работа с меню Database utility 495
Проверка целостности базы данных (Verify Database Integrity) 496
Обновление полей базы данных (Update Database Fields) 496
Проверка индекса базы данных (Verify Database Index) 497
Проверка ссылок базы данных (Verify Database Links) 497
Проверка структуры базы данных (Verify Database Hierarchy) 497
Проверка архивных файлов базы данных (Verify Database Archive Files) 497
Проверка файлов по учёту рабочего времени (Verify Time & Attendance Files) 497
Проверка файлов видеособытий (Verify Video Event Files) 498
Замена описаний (Swap Descriptions) 498
Очистка базы данных (Clean the Database) 498
Восстановление файлов по последней транзакции с картой (Rebuild Card Last Transaction Files) 498
Видеохранилище (EntraPass Video Vault) 499
Установка видеохранилища EntraPass Video Vault 499
Запуск видеохранилища EntraPass Video Vault 500
Работа с архивированными видеофрагментами 501
Редактор языков (Vocabulary Editor) 504
Установка редактора языков (Vocabulary Editor) 504
Перевод словаря системы на другой язык 504
Интегрирование пользовательского языка в систему EntraPass 508
Распространение нового словаря между пользователями 510
Обновление словаря системы 510
Обновление словаря системы 513
Программа автоматической установки Express Setup 514
Настройка конфигурации сайта на шлюзе Corporate Gateway при помощи программы Express Setup 514
Настройка конфигурации контроллера при помощи программы Express Setup 519
Порядок описания реле 520
Порядок описания входов 521
Порядок описания дополнительных выходов 521
Программа просмотра быстрых отчётов (Quick Report Viewer) 522
Диагностика по методу "запрос-ответ" (PING Diagnostic) 524
Рабочая станция – программа конфигурации 525
Утилита переноса данных (Migration Utility) 526
Переход с версии Special Edition к версии Corporate Edition 526

Порядок переноса базы данных из версии Special в версию Corporate 527
Интерфейс шлюза 528
Запуск шлюза Gateway 528
Повторная загрузка данных шлюза Gateway 528
Интерфейс MS/SQL 530
Установка программы MS/SQL Interface 530
Настройка конфигурации программы CardGateway 530
Запуск программы CardGateway 531
System configuration (Конфигурация системы) 532
Database (База данных) 532
Transaction Report (Отчёт о транзакциях) 532
Транзакции 532
Схема 533
Интерфейс SmartLink 534
Настройка конфигурации приложения типа SmartLink 534
Запуск приложения SmartLink 534
Нагрузка на сеть 535
Сообщения: 535
Повторные загрузки: 535
Ручные операции: 535
Глава 17 • Анимированные иконки 537
Контроллеры 538
Статус неизвестен 538
Потеря напряжения в сети питания переменного тока контроллера 538
Отсутствует связь с контроллером 538
Связь с контроллером в норме (всё нормально) 538
Статус контроллера пока неизвестен 538
Контроллер перезагружается, сбой в питании 539
Контроллер перезагружается, сбой в питании, тревожный статус противовзломного реле 539
Контроллер перезагружается, противовзломное реле в статусе тревоги 539
Противовзломное реле контроллера в состоянии тревоги 539
Повторная загрузка прошивки контроллера 539
Двери 540
Дверь взломана 540
Дверь взломана (считыватель отключён) 540
Дверь закрыта и заблокирована 540
Дверь закрыта и заблокирована (считыватель отключён) 540
Статус двери неизвестен 540
Дверь открыта слишком долго 540
Дверь открыта слишком долго (считыватель отключён) 541
Дверь открыта и разблокирована вручную 541
Дверь открыта и разблокирована вручную (считыватель отключён) 541
Дверь открыта и разблокирована по расписанию 541
Дверь открыта и разблокирована по расписанию (считыватель отключён) 541
Предтревожное состояние двери при слишком долгом открытии 541
Предтревожное состояние двери при слишком долгом открытии (считыватель отключён) 542
Дверь ещё открыта, хотя расписание уже не действует 542
Дверь ещё открыта, хотя расписание уже не действует (считыватель отключён) 542

Дверь разблокирована оператором 542
Дверь разблокирована оператором (считыватель отключён) 543
Дверь разблокирована по расписанию 543
Дверь разблокирована по расписанию (считыватель отключён) 543
Дверь лифта разблокирована и закрыта 543
Реле 544
Реле активировано событием 544
Реле временно активировано событием 544
Реле активировано по входу 544
Реле временно активировано по входу 544
Реле активировано оператором 544
Реле временно активировано оператором 544
Реле активировано по расписанию 545
Реле деактивировано 545
Статус реле неизвестен 545
Входы 546
Вход с тревожным статусом – не контролируется 546
Вход с тревожным статусом – шунтирован (отключён от мониторинга) оператором 546
Вход с тревожным статусом – контролируется 546
Вход с тревожным статусом – контролируется оператором 546
Вход с нормальным статусом – не контролируется 546
Вход с нормальным статусом – шунтирован (отключён от мониторинга) оператором 546
Вход с нормальным статусом – контролируется 547
Вход с нормальным статусом – контролируется оператором 547
Статус входа неизвестен 547
Сайты и шлюзы 548
Сайт контроллера: 548
Статус сайта пока неизвестен 548
Сайт контроллера подключён 548
Сайт контроллера подключён и находится в состоянии повторной загрузки данных (Reload Data) 548
Сайт контроллера – нет связи 548
Шлюз: 548
Шлюз – нет связи 548
Шлюз в состоянии повторной загрузки данных (Reload Data) 548
Шлюз – обрыв связи во время повторной загрузки данных 549
Связь со шлюзом в норме (всё нормально) 549
Проблемы со шлюзом 549
Проблемы со шлюзом во время повторной загрузки данных 549
Шлюз (программный интерфейс шлюза): 549
Шлюз в норме – есть связь 549
Шлюз в состоянии повторной загрузки данных (Reload Data) 550
Шлюз – нет связи 550
Приложения EntraPass 551
Статус приложения пока неизвестен 551
Приложение пытается установить связь 551
Приложение – нет связи 551
Прочее 551
Инициализация базы данных 551
Данные недоступны 551
Статус недоступен 551
Статус выхода пока неизвестен 552
Статус неизвестен 552
Обнаружена ошибка 552

Неизвестный компонент 552
Индекс 553

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.

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 персонального вызова (пейджерами), системами жизнеобеспечения, электронной почтой и пр.
- Резервный сервер для обеспечения дополнительной безопасности (приобретается отдельно)
- Подключение к сетевому интерфейсу Kantech IP Link
- Совместимость с KT-100, KT-200, KT-300 и KT-400
- Автоматическая установка (Express Setup)
- Локальный запрет повторного прохода, взаимодействие между контроллерами открывания и закрывания дверей и функция DayPass (Разовые пропуска) для временных посетителей
- Управление лифтами
- Встроенная функция изготовления электронных пропусков
- Интерактивные поэтажные планы здания
- Конфигурируемые оператором "рабочие столы"
- Программа CardGateway (опция)
- Технология использования нескольких считывающих устройств
- Установление связи с внешней системой оповещения о тревоге
- Учёт рабочего времени
- Возможность передачи отчётов по электронной почте
- Визуальная диагностика
- Функция *Video Integration* для интеграции видеосигналов с цифровыми системами видеонаблюдения Intellex® DVMS и видеорегистраторами EDVR компании American Dynamics
- Отображение видеоизображения в реальном времени, воспроизведение видеозаписей, локальная регистрация и сохранение видеозаписей по событиям
- Создание видеоархивов в видеохранилище EntraPass Video Vault
- Редактор языков

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.

NOTICE TO USERS: Unauthorized and/or illegal use of this system may constitute a felony or a misdemeanor under federal, state, provincial, or local laws. Tampering with, and/or attempt to tamper with, electronic monitoring or security devices, is a violation of the law. By using this SOFTWARE PRODUCT, you agree to the provisions of the Agreement.

Особенности системы EntraPass

SmartLink. EntraPass позволяет разрабатывать интегрированные решения, используя различные интеллектуальные устройства, в том числе CCTV мультиплексоры, системы персонального вызова (пейджеры) с буквенно-цифровой индикацией, автоматизированные системы рассылки электронных сообщений, системы жизнеобеспечения, ЖК-панели, коммутаторы с видеоматрицами и др., путём использования RS-232 или сетевого соединения между рабочей станцией EntraPass SmartLink и внешним 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, предотвращая многократный ввод одних и тех же данных.

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 или сливается с резервного сервера.

Kantech IP Link. Система EntraPass совместима с интерфейсом Kantech IP Link, который обеспечивает безопасное Ethernet-соединение, выступая в качестве опрашивающего устройства, и 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, что даёт дополнительное преимущество при обновлении сайтов, 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 относится к семейству Ethernet-контроллеров, предназначен для управления открытием и закрытием до 4-х дверей и для организации IP-связи с удалёнными ветвями системы.

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

- **KT-MOD-REL8**: релейный модуль расширения, 8 реле общего назначения или для управления лифтами. Допускает шлейфовое подключение устройств, что позволяет подключить 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 на один контроллер KT-400. Допускает шлейфовое подключение 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, до 16 выходов 12 В пост. тока, с открытым стоком. Используется для управления лифтами (при необходимости, приобретается дополнительное оборудование). Допускает шлейфовое подключение до 16 модулей KT-MOD-OUT16 на каждый контроллер KT-400, то есть до 256 внешних выходов.

Автоматическая установка (Express Setup). Программа "Express Setup" позволяет 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 аппаратного обеспечения и схем соединений; установщику остаётся лишь внести индивидуальные изменения, необходимые для определённого сайта.

EntraPass WebStation. Программное обеспечение EntraPass WebStation предназначено для управления идентификационными картами с удалённых станций и используется вместе с другими продуктами EntraPass. Кроме того, EntraPass WebStation обеспечивает выполнение ряда операций в ручном режиме, генерирует отчёты о работе дверей, реле и входов, о происшедших событиях (в форматах .PDF, CSV, XLS, TXT), а также создаёт веб-представления. Интерфейс программы идеально подходит для предоставления функций управления идентификационными картами персоналу службы безопасности, секретарям и руководителям и не требует полной загрузки рабочей станции EntraPass. EntraPass WebStation предусматривает возможность одновременного подключения нескольких пользователей, число которых зависит от выбранного пакета ПО.

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-PC4204 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 нанимателям, и таким образом удаётся ограничить доступ владельцев идентификационных карт на определённые этажи.

Встроенная функция изготовления электронных пропусков. Система EntraPass оснащена программными средствами для создания и изготовления электронных пропусков. Данная функция позволяет загружать фотографии и подписи сотрудников, а также с помощью соответствующих устройств оцифровывать изображения и помещать на карты при печати электронных пропусков.

Интерактивные планы этажей. EntraPass позволяет загружать и выводить на экран графические схемы высокого разрешения, созданные при помощи систем САПР (с конвертацией в формат .jpg or .bmp), то есть позволяет работать с графическим представлением системы, не требуя серьёзной подготовки операторов. 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 конфигурируемых рабочих столов. На этих рабочих столах располагаются окна с сообщениями о событиях, фотографиями пользователей, избранные события, видео и графика высокого разрешения, а также тревожные команды. 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, включая отложенную постановку на охрану. Это позволяет легко интегрировать EntraPass с внешними охранными панелями.

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.

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. Можно привязать запись к событиям, относящимся к нарушению порядка доступа, и записать изображения, передаваемые с одной или с нескольких камер наблюдения (не более 16 камер), одновременно в разных системах Intellex. Кроме того, в системе EntraPass доступно использование предустановок, управление настройками телеметрии поворотных камер, режимы вывода последовательности кадров и вывод изображений с камер наблюдения на экран, разбитый на ячейки 1x1, 2x2, 3x3, и 4x4. К каждой камере можно обращаться напрямую щелчком по её пиктограмме на поэтажном плане. Пользовательский интерфейс программ EntraPass Global и EntraPass Corporate позволяет настраивать параметры изображения для работы с цифровым видео.

Видеохранилище EntraPass Video Vault. Этот инструмент позволяет автоматически сохранять все видеофрагменты, полученные с охранных систем Intellex или 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.

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.**

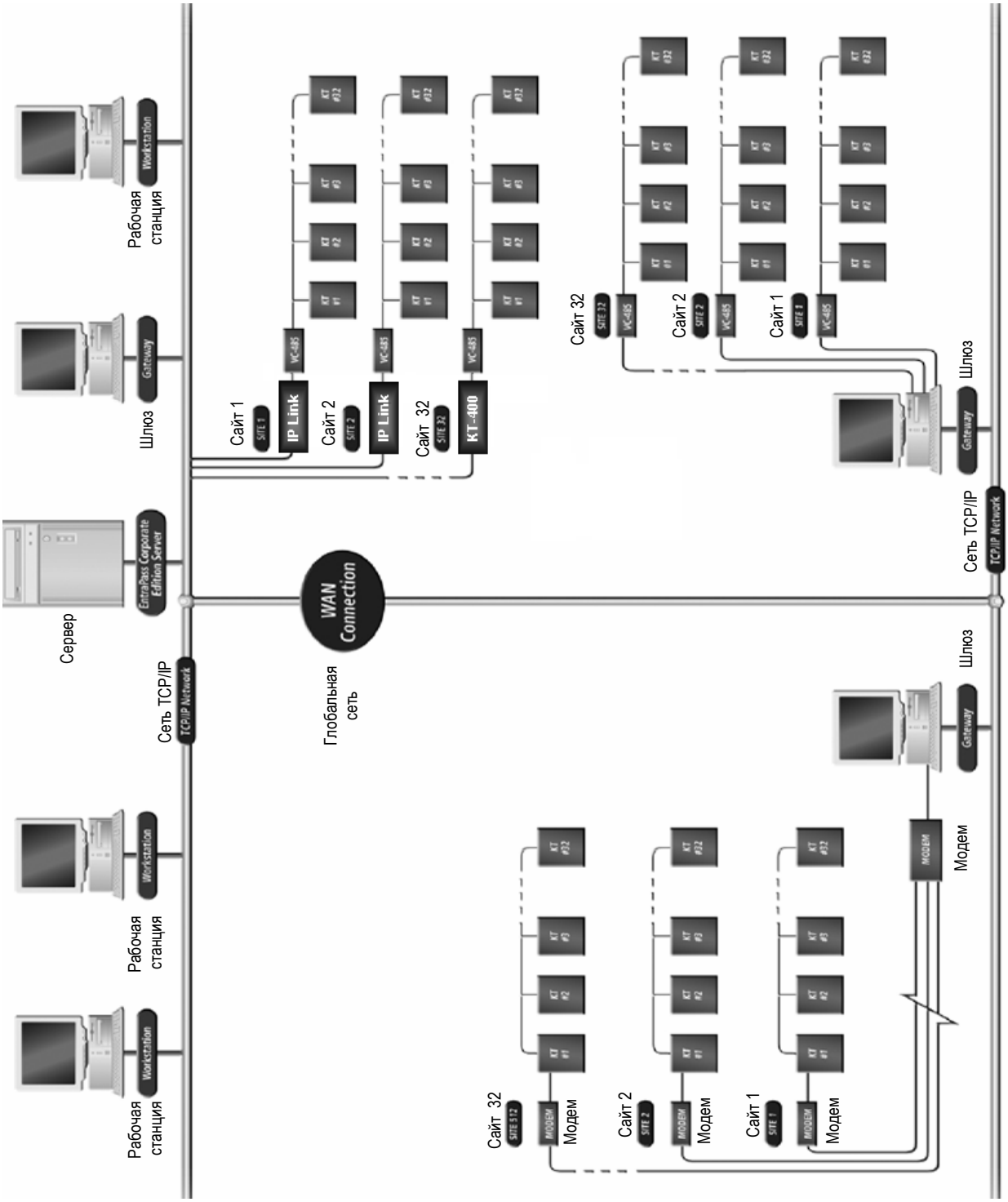
Для обращения к справочной системе можно воспользоваться клавишей **Help**, доступной во всех окнах программы. Кроме того, при нажатии на правую кнопку мыши на экране появляется всплывающее меню для быстрого вызова команд или файл справки к активному окну.

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)	Адрес электронной почты
бесплатный по Северной Америке 1 888 222 1560 (GMT -05:00)			
США и Канада	тел.: 1 450 444 2030 факс: 1 450 444 2029	от 8:00 до 20:00	kantechsupport@tycoint.com
Латинская Америка (GMT -03:00)			
Аргентина	тел.: 011 5411 4717 2929 тел.: 011 5411 4717 1320 тел.: 011 5411 4717 5525 факс: 011 5411 4717 1060	от 9:00 до 18:00	ingenieria@tycoint.com
Азия: (GMT +08:00)			
Сингапур	тел.: 011 65 6319 9820 факс: 011 65 6319 9821	от 8:30 до 18:00	swhuin@tycoint.com
бесплатный по Европе 1 800 CALL TYCO / 1 800 2255 8926 (GMT +01:00)			
Бахрейн	800 04127	от 8:00 до 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 10 190 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 тел.: 011 31 475 352 722 факс: 011 31 475 352 725		

Архитектура системы



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.

Системные требования к компьютеру

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 SP2/2003 Standard и Enterprise Server Editions/ Vista Business, Enterprise и Ultimate
- 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
- Графическая плата: 32 Мб
- Привод CD-ROM: 48X
- Сетевая интерфейсная плата: сетевой адаптер 10/100 Base-T

Для использования функции интеграции с видеонаблюдением (*Video Integration*) 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 2003 Standard и Enterprise Servers, XP Pro SP2 и Business, Enterprise, Ultimate
- Установка самых последних пакетов обновления Windows и высокоприоритетных 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 Reference Manual*", DN1709.

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 журналов** - (матричный или лазерный) для печати событий (сообщений и тревог)
- **Принтер отчётов** - (лазерный) для печати отчётов

Комплект установки

Установочный комплект EntraPass состоит из компакт-диска CD-ROM и справочного руководства DN1415 (*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 приложение Сервер (Server) и 2 дополнительных приложения Рабочая станция (Workstation)
- 1 приложение Шлюз (Corporate Gateway)
- Интерфейсы SmartLink и SmartLink Network
- Программа просмотра отчётов (Report Viewer)
- Редактор языков (Vocabulary Editor)
- Программа обнаружения устройств (KT-Finder)

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

- 6 дополнительных приложений Рабочая станция (максимум 20 +1)
- 40 приложений Шлюз (Corporate Gateway)
- Приложение Зеркальная база данных на резервном сервере
- Приложение Видеохранилище (Video Vault)
- Интерфейс Oracle/MS-SQL для программы интерфейса MS/SQL
- Соединения для веб-станции EntraPass WebStation

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

Порядок установки

Мастер установки InstallShield Wizard проведёт Вас шаг за шагом через все этапы установки. Вам требуется лишь ввести код установки **System Installation Code** (указан на компакт-диске) и следовать инструкциям, отображаемым на экране.

Установка программного обеспечения EntraPass

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).
3. Установить первые компоненты, входящие в комплект установки (5 приложений 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 пользователя. Если произошла автоматическая разрегистрация, пользователи должны ввести 20-значный пароль в жёлтом окне, отображаемом в нижней части экрана.*

WARNING: recommends that this entire system be reinstalled, tested on a regular basis. However, despite frequent testing, and due to, but not limited to, unlimited tampering by unscrupulous individuals, it is possible that the entire SOFTWARE PROGRAM may fail to perform as expected.

Добавление дополнительных компонентов/функций

Для того чтобы добавить дополнительные компоненты/функции к системе, следует выполнить 4 действия. Это можно сделать двумя способами:

1. Воспользоваться установочным компакт-диском для единовременной инсталляции всех дополнительных компонентов, или добавить некоторые из них через окно регистрации сервера или рабочей станции.
2. Обратиться в компанию Kantech для получения или регистрации серийного номера компонентов/опций **Option Serial Number** (указан в сертификате опций (Option Certificate)) и получить код подтверждения регистрации (Registration Confirmation Code).
3. Ввести код подтверждения регистрации (**Registration Confirmation Code**) в окне регистрации и активировать опцию.
4. Установить компонент или опцию с помощью кода установки **Installation Code** (если это применимо). Код установки генерируется системой и отображается в окне регистрации.

ПРИМЕЧАНИЕ. *В случае установки нового компонента/опции на компьютер, не имеющий установленного приложения типа Рабочая станция (EntraPass Workstation) (и только в этом случае) следует установить связь между этим компьютером и сервером EntraPass Server.*

WARNING: recommends that this entire system be reinstalled, tested on a regular basis. However, despite frequent testing, and due to, but not limited to, unlimited tampering by unscrupulous individuals, it is possible that the entire SOFTWARE PROGRAM may fail to perform as expected.

Установка системы

1 Перед началом установки следует убедиться, что ни одно приложение EntraPass не запущено в данный момент времени.

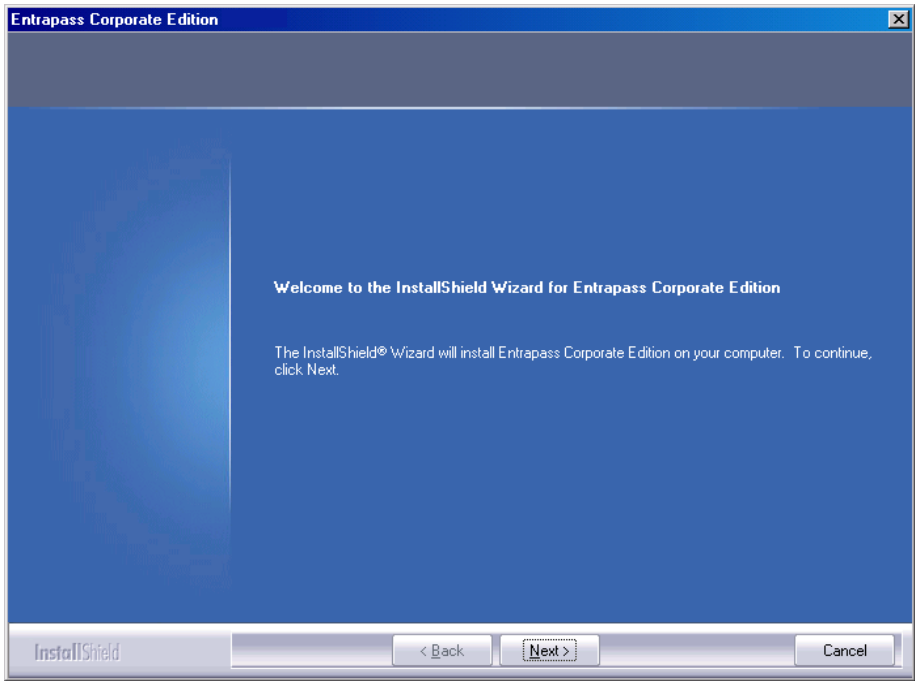
2 Установите компакт-диск в привод CD-ROM компьютера. Если в настройках компьютера разрешён автоматический запуск, программа инсталляции запускается автоматически. Если этого не произошло, следует войти в меню Start > Run и запустить файл D:\Setup.exe (где D: - имя CD-ROM привода).

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.*

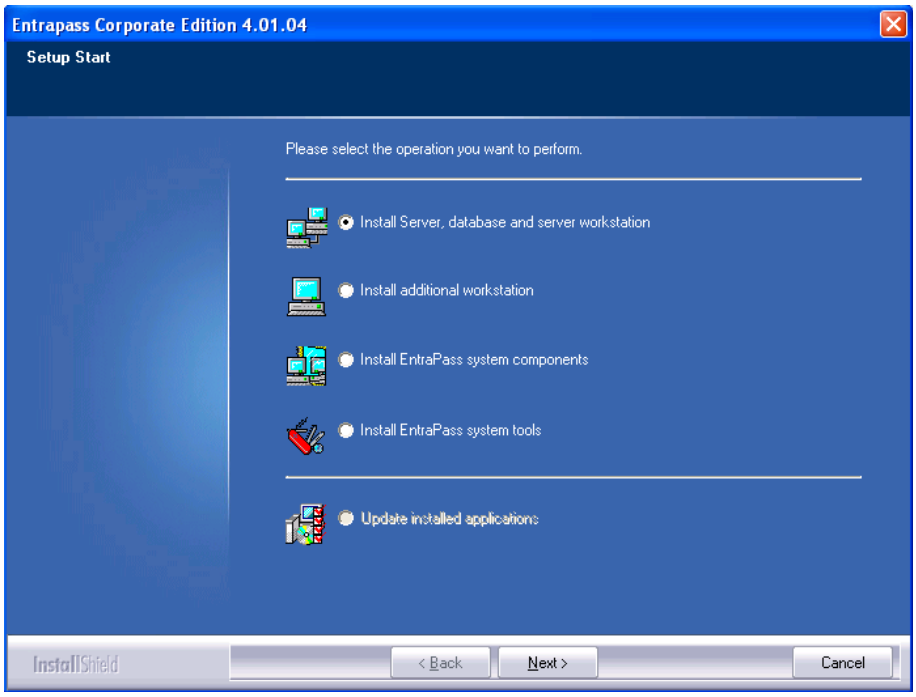
4 Нажать **OK.** При этом откроется окно приветствия.



- 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.

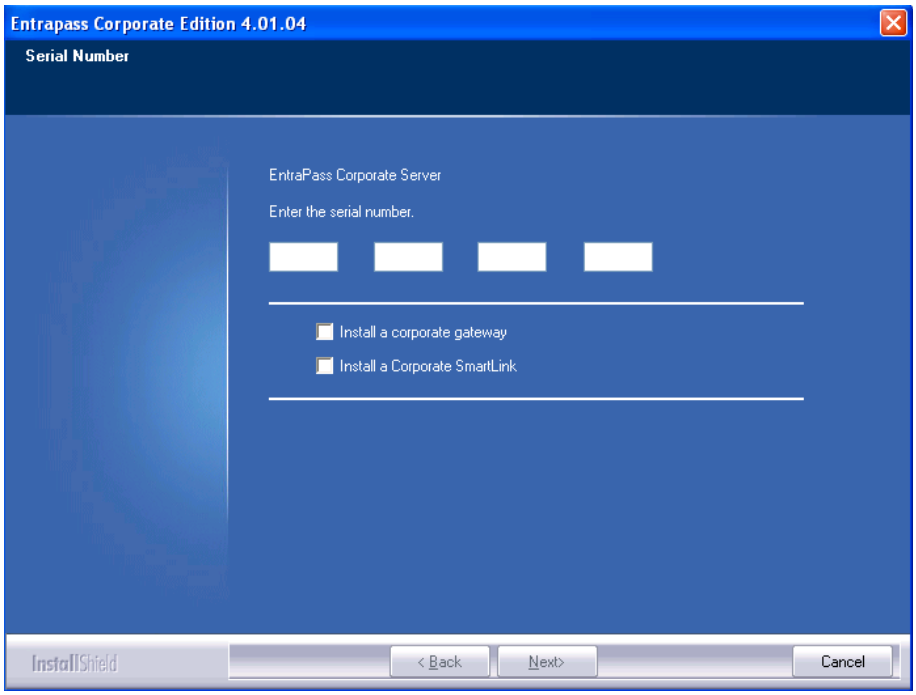
5 Нажать **Next** для продолжения процесса установки ПО. При этом откроется окно Setup Start (Начало установки).



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.

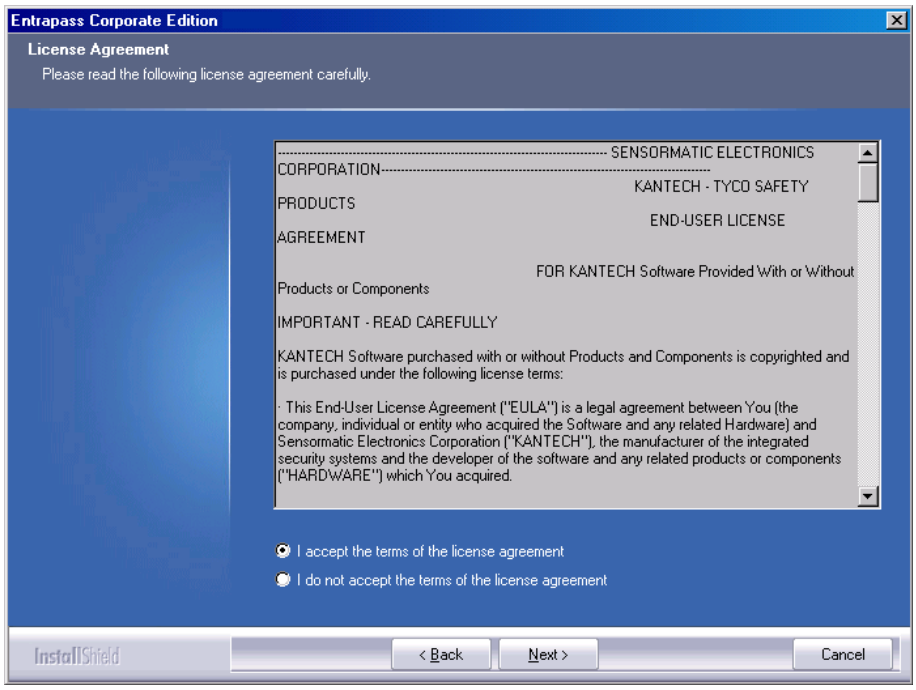
- **Install Server, Database and Workstation** (Установить сервер, базу данных и рабочую станцию). Эта опция служит для установки системы EntraPass Corporate Edition. Этот пункт будет неактивным, если перечисленные компоненты уже установлены.
- **Install Additional Workstation** (Установить дополнительную 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, в частности, шлюзов (Gateways), веб-станций (WebStations), интерфейса SmartLink, видеохранилища (Video Vault), интерфейса Oracle/MS-SQL и зеркальной базы данных (Mirror Database), а также резервного сервера (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 видеонаблюдения (Video Viewer), сетевого интерфейса SmartLink Network Interface и др. Этот пункт будет неактивным, если перечисленные компоненты уже установлены на этом компьютере.
- **Update Installed Applications** (Обновить установленные приложения). Этот пункт будет неактивным, если система ещё не установлена. Порядок обновления подробно описан *в разделе "Обновление системы" на стр. 30.*

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



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

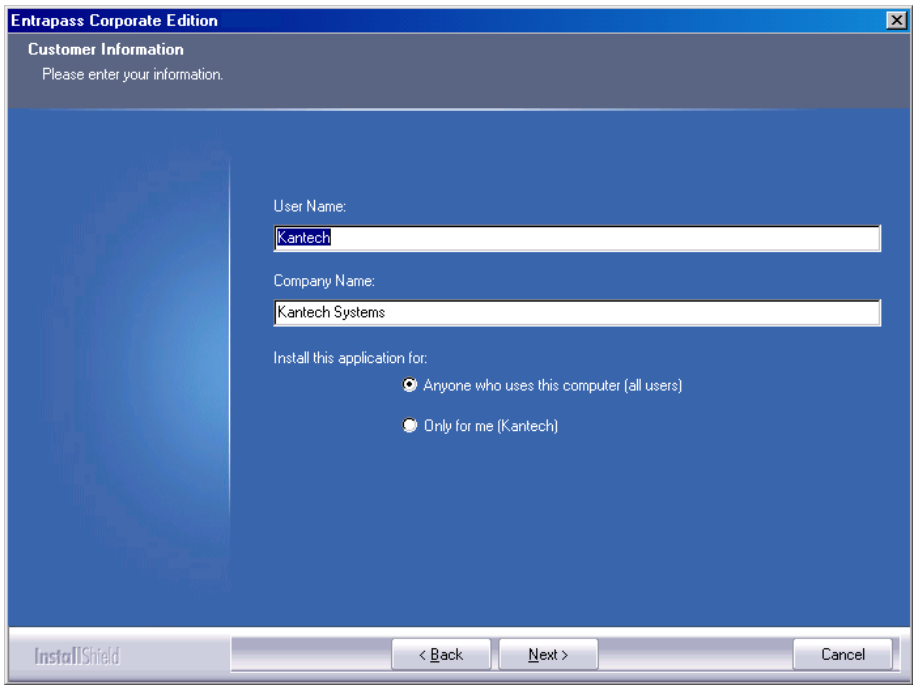
9 Нажать **Next** для продолжения работы. На экране появится Лицензионное соглашение с конечным пользователем ПО.



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...**

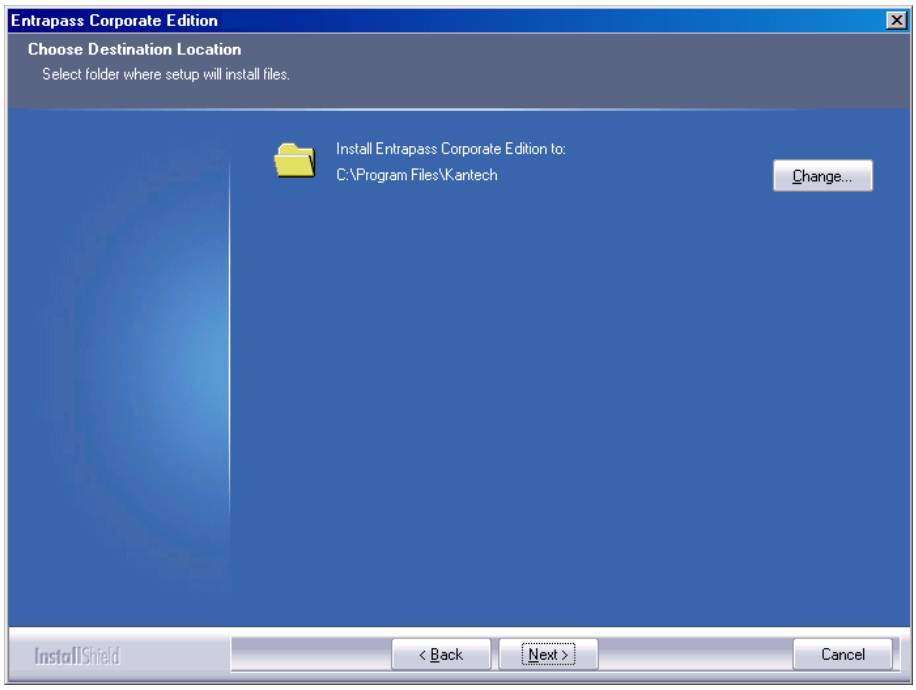
11 Нажать **Next** для продолжения работы. На экране появится окно Customer Information (Сведения о покупателе).



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

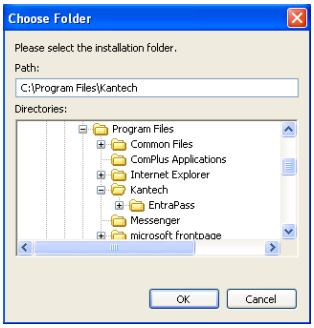
13 Ниже следует указать уровень доступа. Опция "**Anyone** who will use this computer" – доступ любому пользователю данного компьютера. Опция "**Only** for me" – доступ только для того пользователя, который в данный момент зарегистрировался в системе.

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

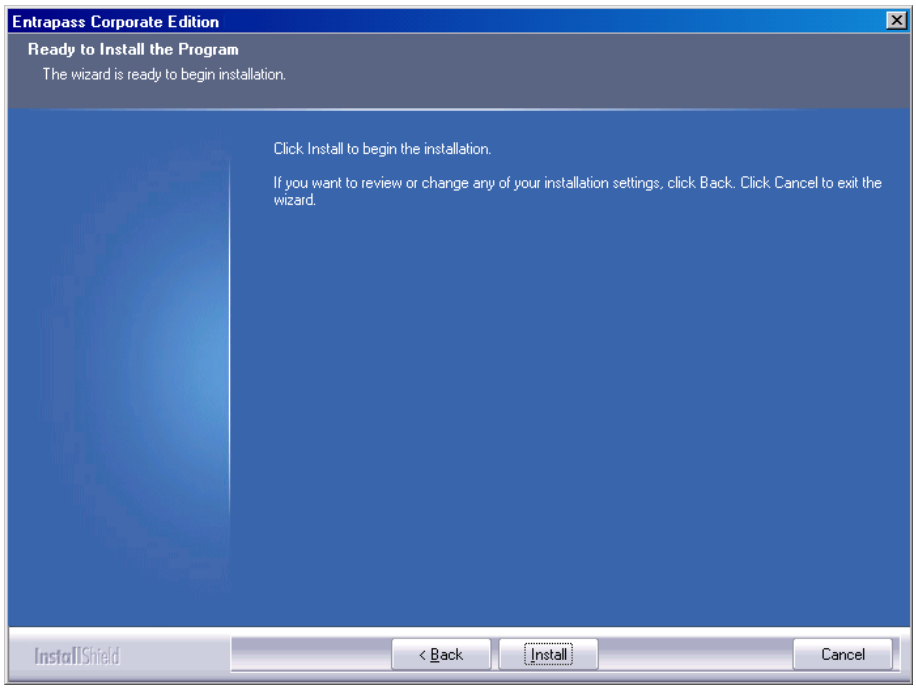


15 Пользователь может выбрать путь по умолчанию и нажать **Next** или указать другой путь.

- 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.

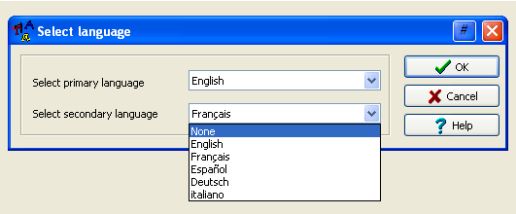


16 Нажать **Next** для продолжения работы. Откроется окно Ready to Install the Program (Готовность к установке программы).



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

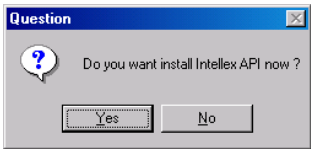
18 Во время установки необходимо будет указать два языка в полях **Select primary language** (Основной язык) и **Select secondary languages** (Дополнительный язык). Это меню служит для выбора языка, который используется при построении базы данных, а также языков, используемых при работе с системой EntraPass.



19 Нажать **OK**. Установка продолжается.

20 Во время установки пользователю будет предложено установить:

- **Intellex API,**
  - Если API (программный интерфейс Intellex) ещё не установлен, нажмите **Yes** и следуйте инструкциям.
  - Если API уже установлен, нажмите **Yes** (смотрите ***примечание***).

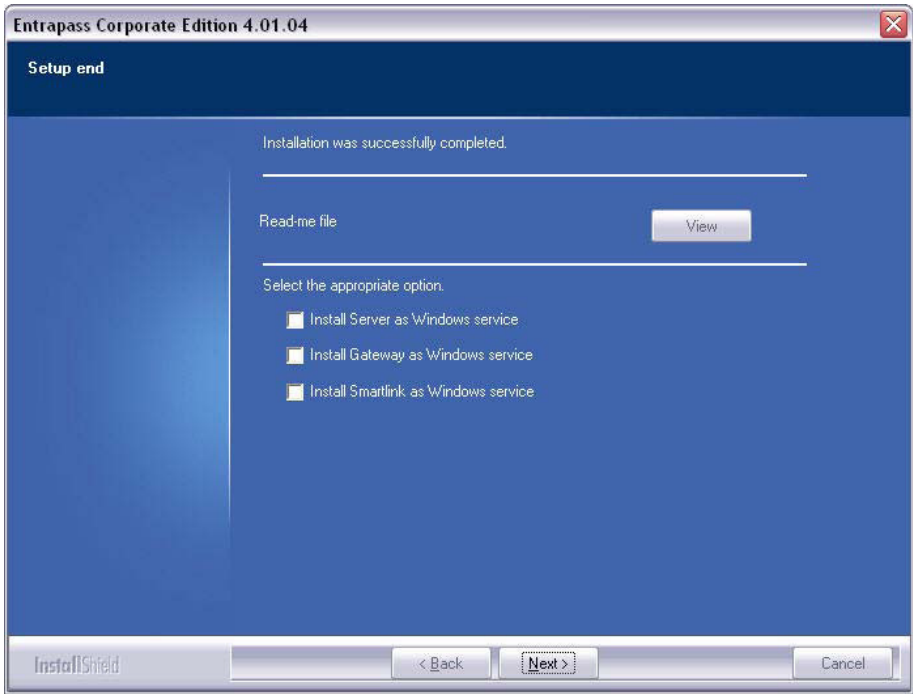


ПРИМЕЧАНИЕ. Если требуется установить **EDVRBridgeService**, то установку **Intellex API** нужно выполнить даже если интерфейс уже был установлен во время предыдущей инсталляции программы. Интерфейс **Intellex API** служит для работы с видеорегистраторами типа EDVR, в то время как **EDVRBridgeService** используется для интеграции видеосигнала с видеорегистраторами Intellex VDR. Установку **EDVRBridgeService** следует выполнять с компакт-диска.

- **EDVRBridgeService,**
  - Если EDVRBridgeService ещё не установлен, необходимо запустить программу установки с компакт-диска и следовать инструкциям.
  - Если EDVRBridgeService уже был установлен, необходимо открыть панель управления (Control Panel), деинсталлировать программу и затем снова установить её с компакт-диска.

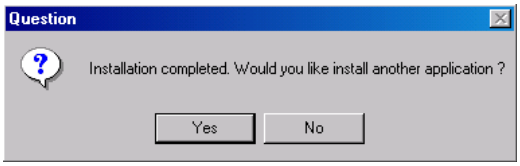
- **EntraPass WebStation,**
  - Если программа WebStation ещё не установлена, нажмите Yes и следуйте инструкциям.
  - Если WebStation уже установлена, нажмите No.

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.



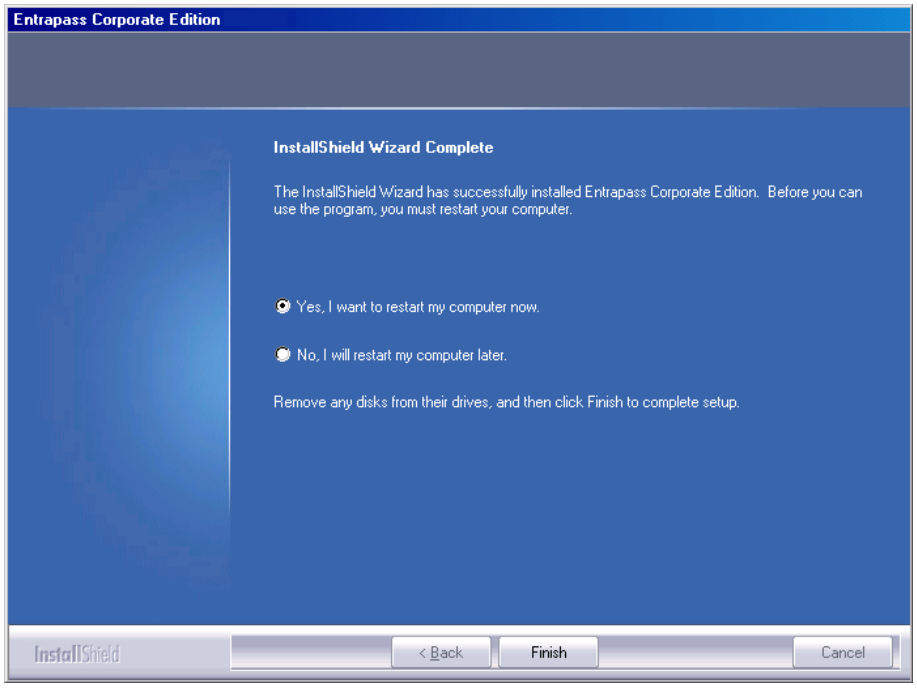
22 Нажать **Next** для продолжения работы. Система проверит, есть ли другие доступные для установки приложения или утилиты. При их обнаружении на экране появится соответствующее сообщение.

- 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 (смотрите раздел "Регистрация системы" на стр. 22).*

- 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 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.*

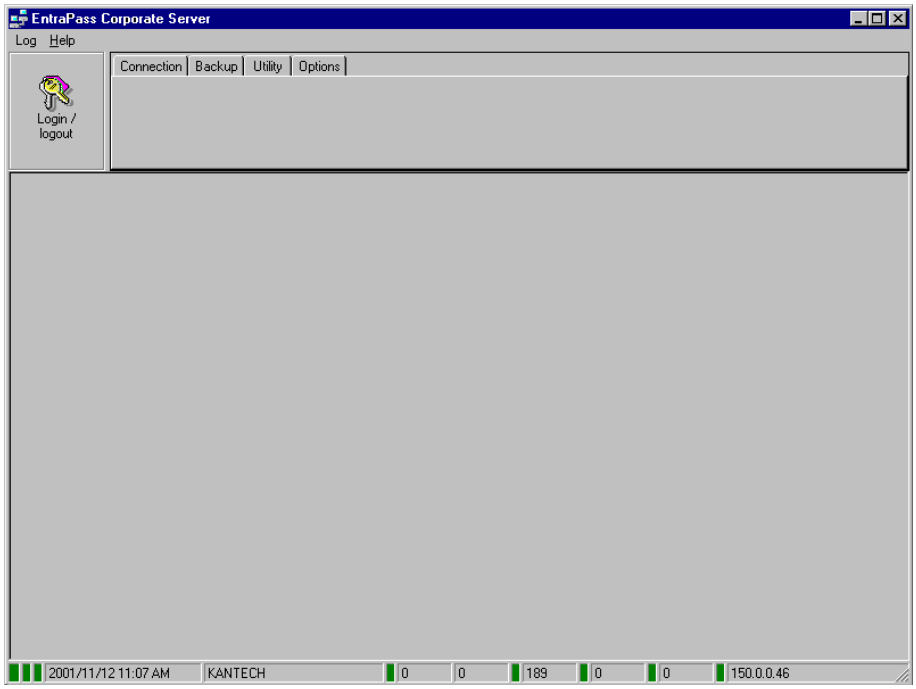
26 Следующим шагом будет обращение в службу технической поддержки Kantech для получения кода регистрации для разных компонентов системы. Следуйте инструкциям в следующем разделе руководства.

Регистрация системы

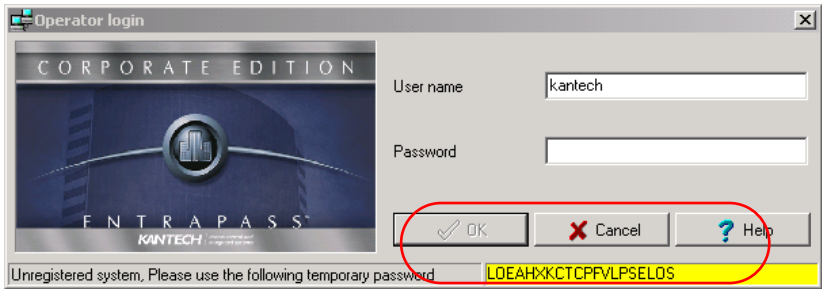
Рекомендуется как можно быстрее зарегистрировать систему, чтобы пользователи получили возможность установить дополнительные опции и работать с программой без ограничений. Фактически система функционирует даже без регистрации, но в усечённом варианте, только с 10-ю идентификационными картами. Кроме того, 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

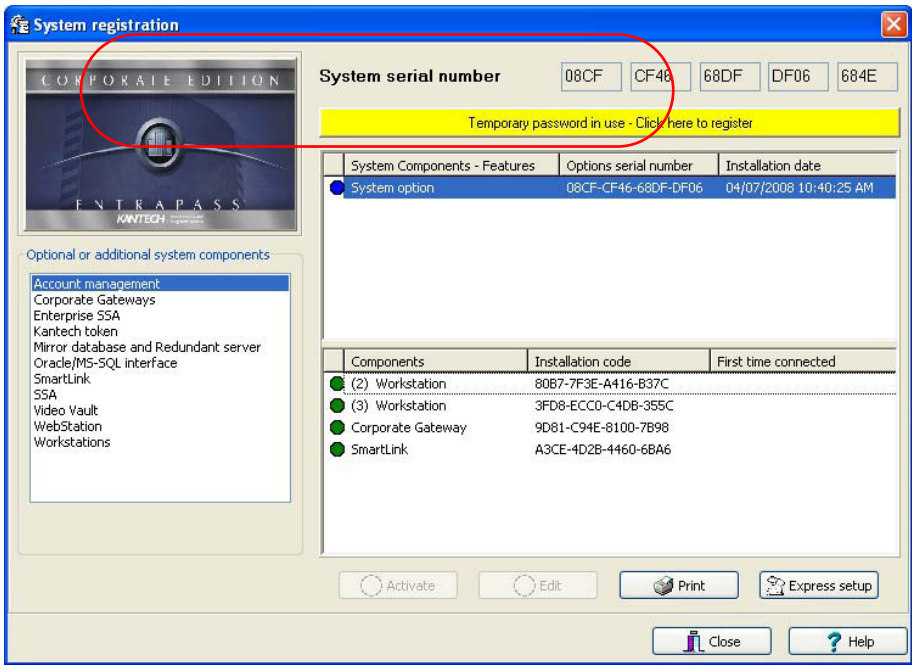
1 Запустить сервер щелчком мыши по ярлыку **Server** на рабочем столе. Или для запуска сервера использовать меню "Пуск" (Start)в среде Windows®: **Start** > **EntraPass Corporate Edition > Server > Server.**



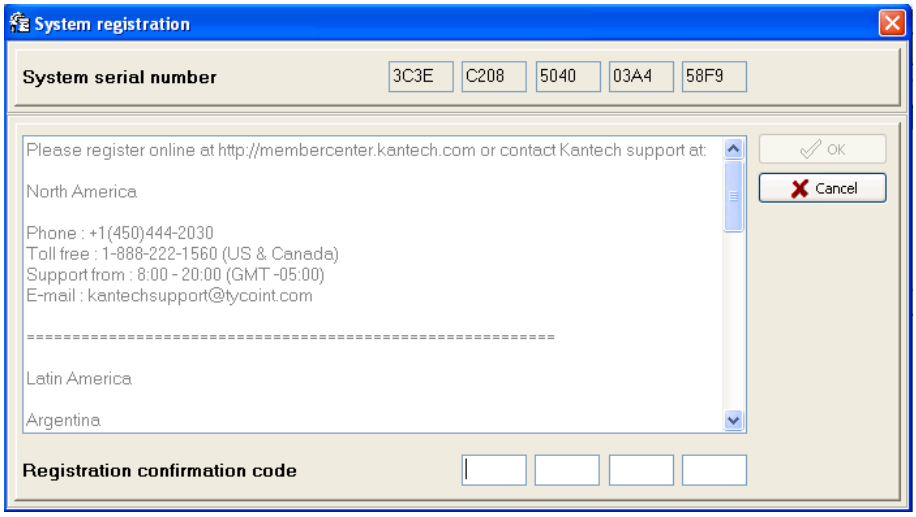
2 Нажать кнопку Login / Logout. Открывается окно Operator Login (Регистрация оператора).



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.

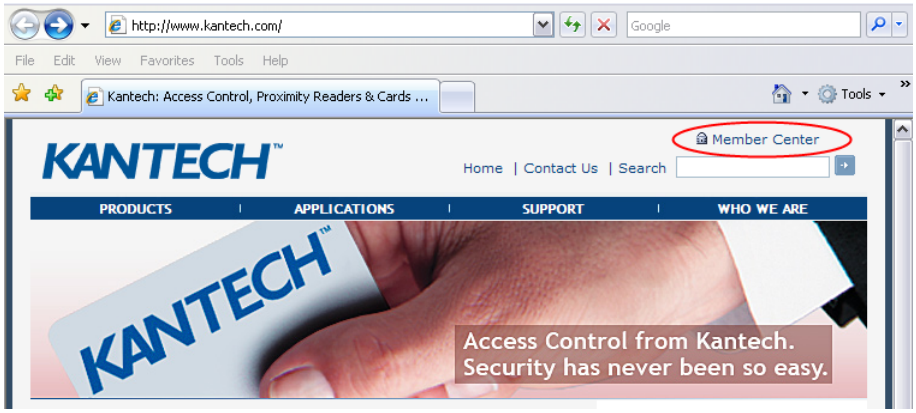


4 Нажать жёлтую кнопку **Temporary password in use (...),** чтобы зарегистрировать систему. Кнопка отображается лишь в только что установленных программах. Открывается окно регистрации System registration.



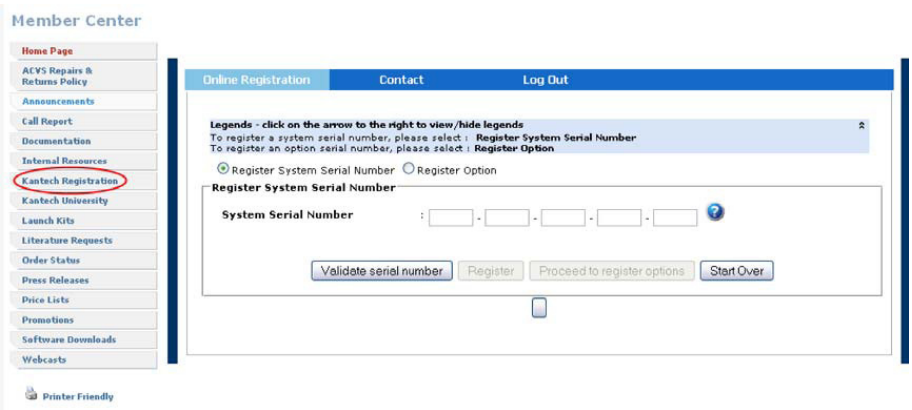
ПРИМЕЧАНИЕ. *Существует два способа регистрации новой системы: онлайновая регистрация на сайте www.kantech.com и получение кода регистрации в местной службе технической поддержки Kantech.*

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.

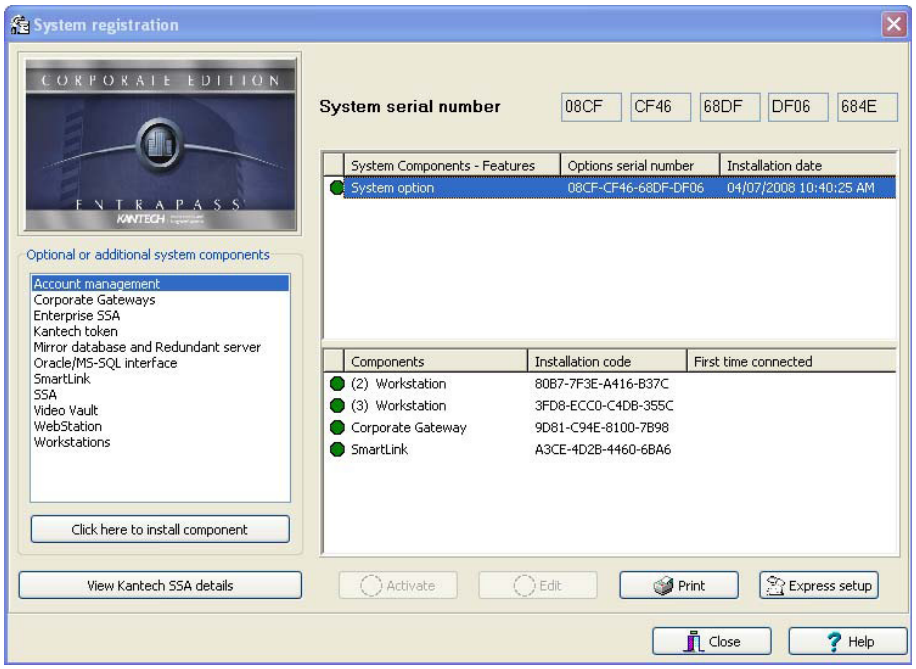
ПРИМЕЧАНИЕ. *В случае выхода из главного окна сервера без регистрации на экране появляется окно Change Authentication Password (Смена аутентификационного пароля). После регистрации системы это окно больше не отображается.*

Дополнительные компоненты системы

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.

Первые два приложения типа Рабочая станция и первое приложение типа Шлюз можно установить без обращения в службу технической поддержки Kantech. Они входят в установочный комплект.

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.

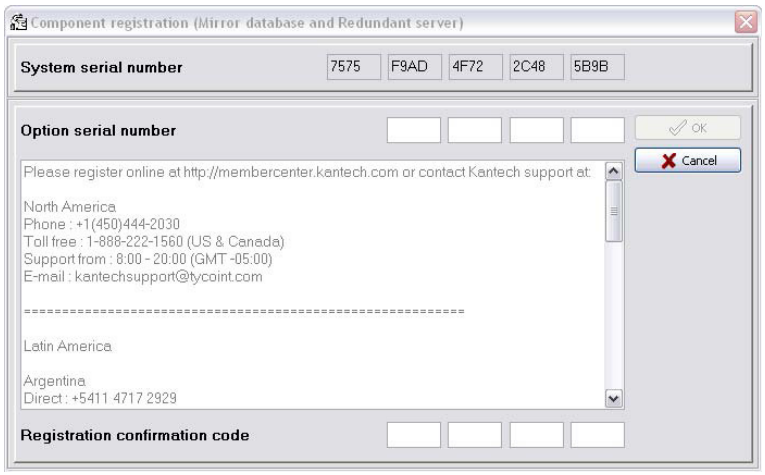


ПРИМЕЧАНИЕ. *В комплекте с сервером EntraPass поставляются три приложения типа Рабочая станция (Workstation) и одно приложение типа Шлюз (Corporate Gateway). Одно приложение типа Рабочая станция устанавливается автоматически во время установки сервера. Оно используется для настройки конфигурации. Оно 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, дополнительного шлюза) рекомендуется настроить их сайты при помощи программы автоматической установки Express Setup.*

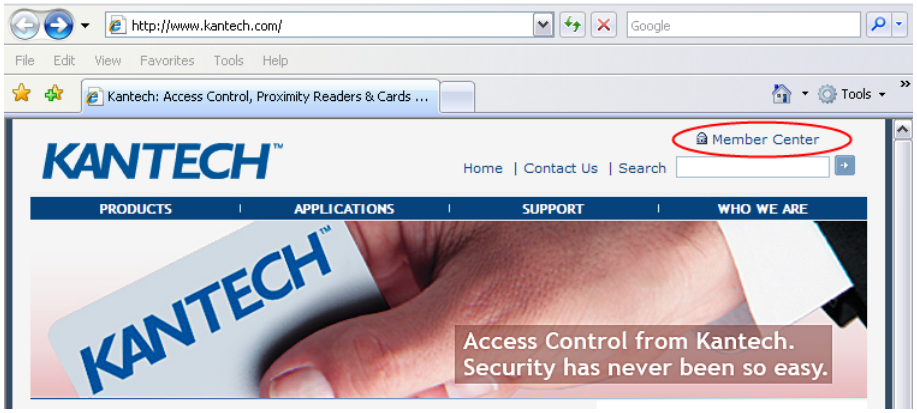
3 В окне System registration (Регистрация системы) указать, какой компонент будет устанавливаться. Затем на панели слева нажать кнопку **Click here to install component** (Нажмите для установки компонента). Открывается окно Component registration (Регистрация компонента), в скобках указывается название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



4 Указать серийный номер компонента в поле **Option Serial Number** (серийный номер указан в сертификате Option Certificate).

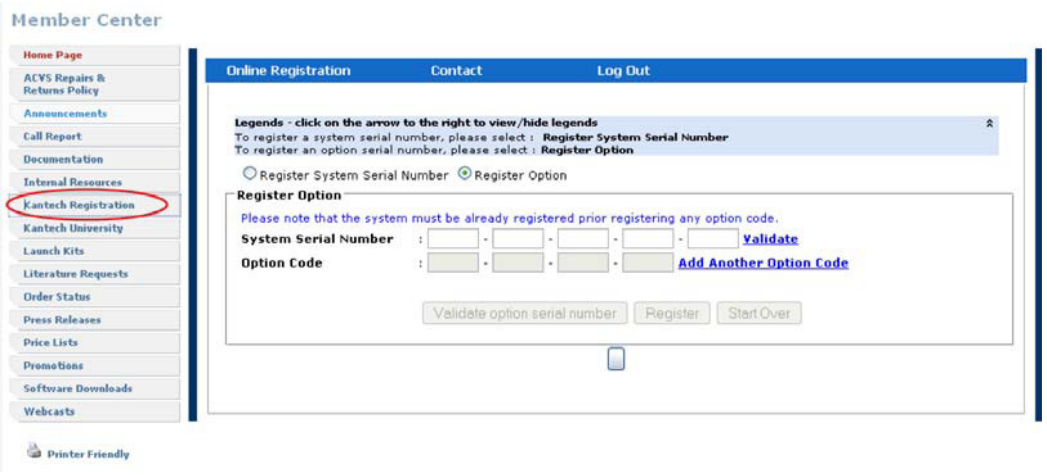
ПРИМЕЧАНИЕ. *Существует два способа регистрации нового компонента: онлайновая регистрация на сайте* ***www.kantech.com*** *и получение кода регистрации в местной службе технической поддержки Kantech.*

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).*

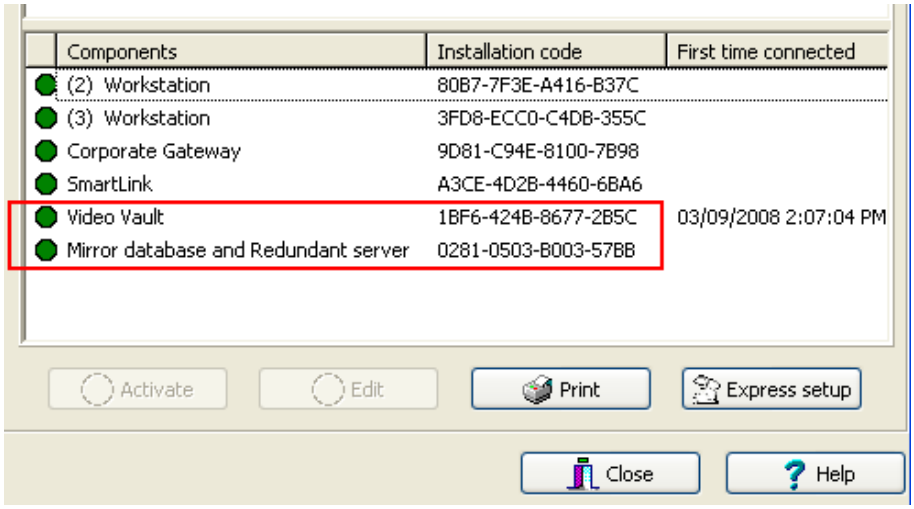
6 Выбрать раздел **Kantech Registration** (Регистрация Kantech).



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 достоверны.

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.*

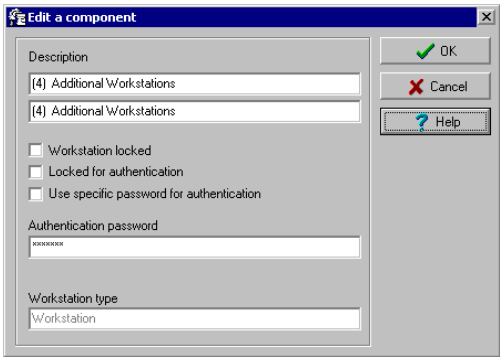


Редактирование сведений о компонентах системы

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).

Присвоение описательных имен приложениям

1. В окне регистрации выбрать приложение и нажать кнопку **Edit.** При этом открывается окно редактирования (Edit a component).
2. В поле **Description** (Описание) указать описательное имя 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 данное приложение на компьютер и использовать его только для получения системных сообщений.
   - **Locked for authentication** (Блокировать аутентификацию). Выбрать эту опцию, чтобы компьютер, на котором установлено приложение EntraPass, не отправлял свои данные аутентификации на сервер.



   - **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).*

ПРИМЕЧАНИЕ. *В среде Managed Access в диалоговом окне редактирования компонента (Edit component) будет отображаться только поле Descriptions для изменения имени основной учётной записи.*

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 рабочей станцией и сервером EntraPass.

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

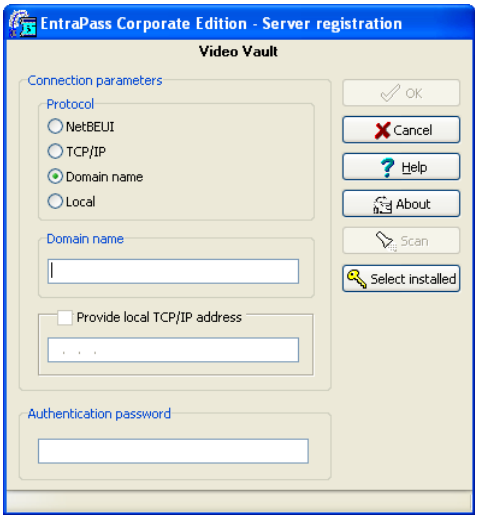
Установление связи с сервером

1 В меню Пуск (Start) в операционной среде Windows® войти в меню **All Programs** (Все программы) **> EntraPass Corporate Edition** > **EntraPass application** (Приложение EntraPass) > **Register to Server** (Зарегистрировать на сервере). Или запустить приложение EntraPass, чтобы система автоматически запустила программу регистрации, когда приложение попытается подсоединиться к серверу без регистрации.

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 уже созданных имён компьютера можно воспользоваться кнопкой **Scan** (Поиск)**.**
- **TCP/IP**. TCP/IP адрес компьютера, на котором установлено программное обеспечение 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 на компьютере, где установлено программное обеспечение EntraPass Server. При этом адрес берётся с сервера.



3 Поставить флажок напротив пункта **Provide local TCP/IP address,** 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 рабочих станций на сервере EntraPass Server.

Обновление системы

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 программного обеспечения

1. Создать **полную резервную копию базы данных системы.** Более подробные сведения по резервному копированию даны *в разделе "Резервное копирование" на стр. 487.*
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.**

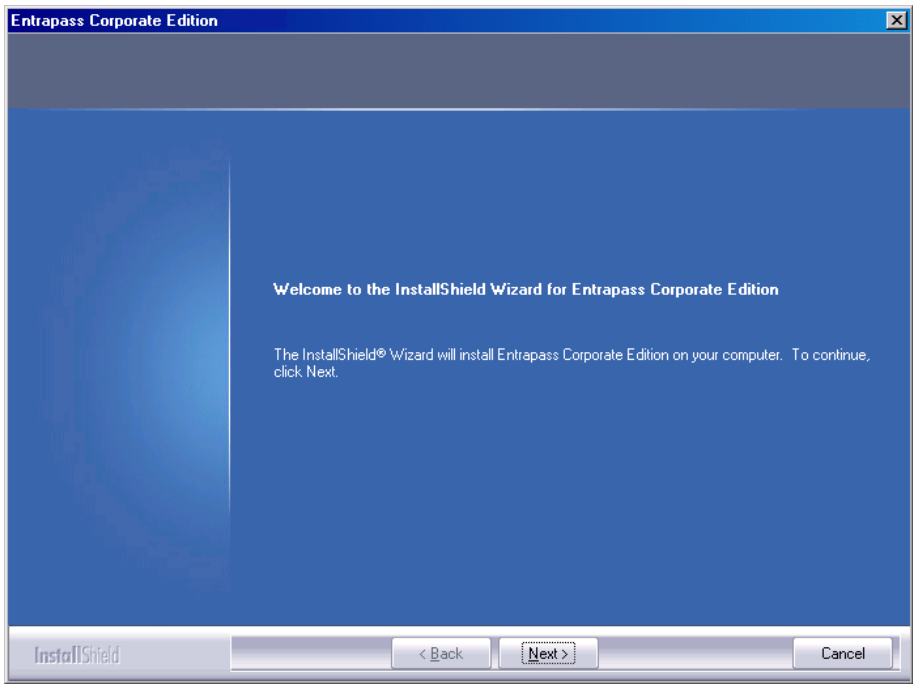
ПРИМЕЧАНИЕ. *Обновление следует выполнять на **всех** приложениях. После окончания обновления **НЕ СЛЕДУЕТ СРАЗУ ЗАПУСКАТЬ** резервный сервер и зеркальную базу данных.*

4. Сначала необходимо убедиться, что база данных системы (смотрите раздел "Утилита базы данных" на стр. 494) не содержит 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. *Подробнее см. "Сервер EntraPass", стр. 481.*

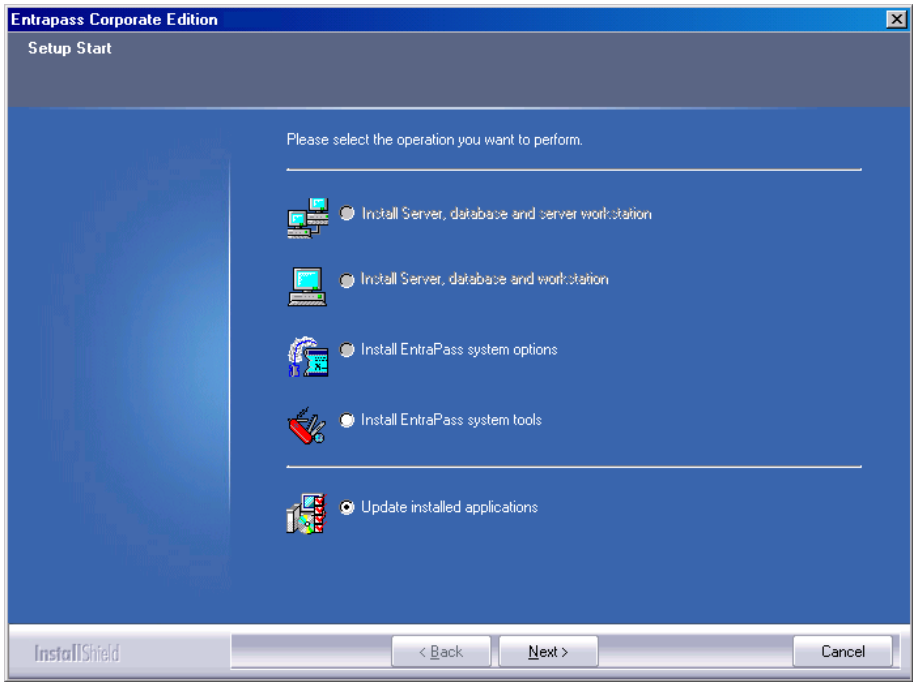
Обновление программного обеспечения

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.

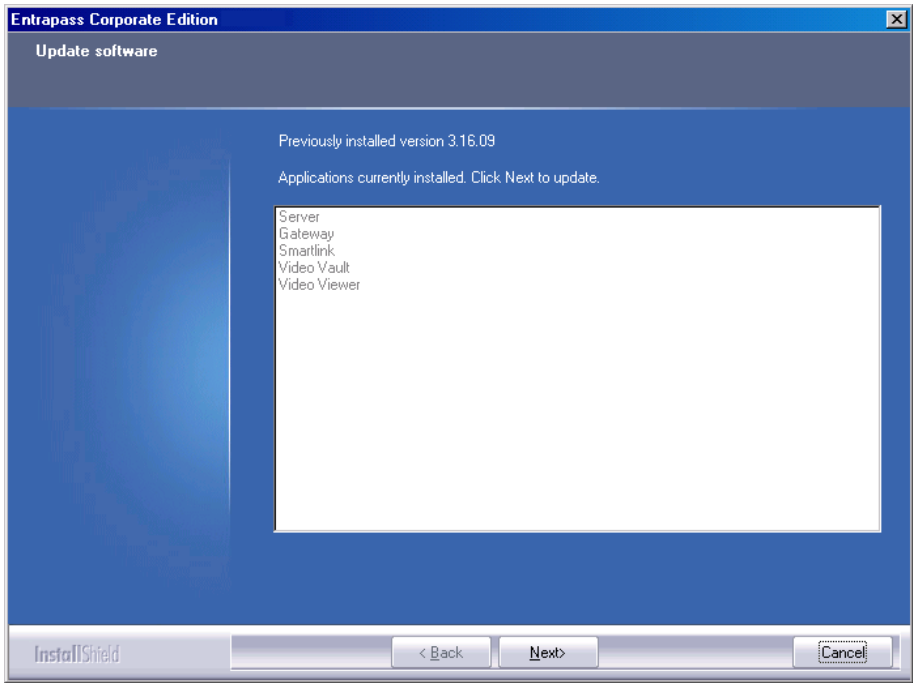
2 Нажать **Next** для продолжения работы. При этом откроется окно приветствия.



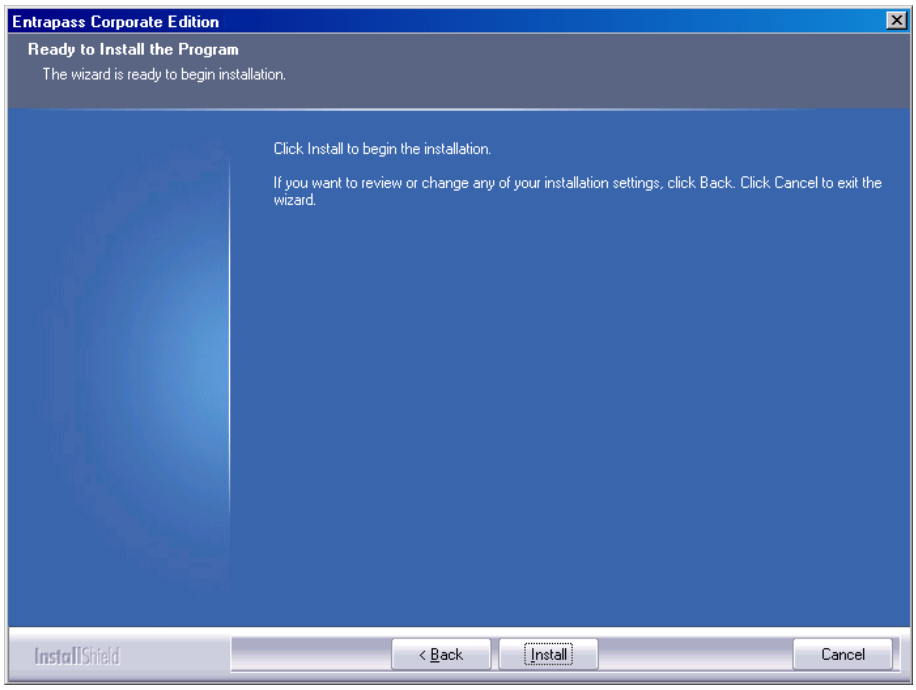
3 Нажать **Next** для продолжения работы. При этом откроется окно Setup Start (Начало установки).



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.

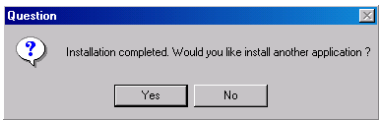


5 Нажать **Next** для продолжения работы. Начинается обновление, и все программы, установленные к данному моменту на этом компьютере, будут обновлены.



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).

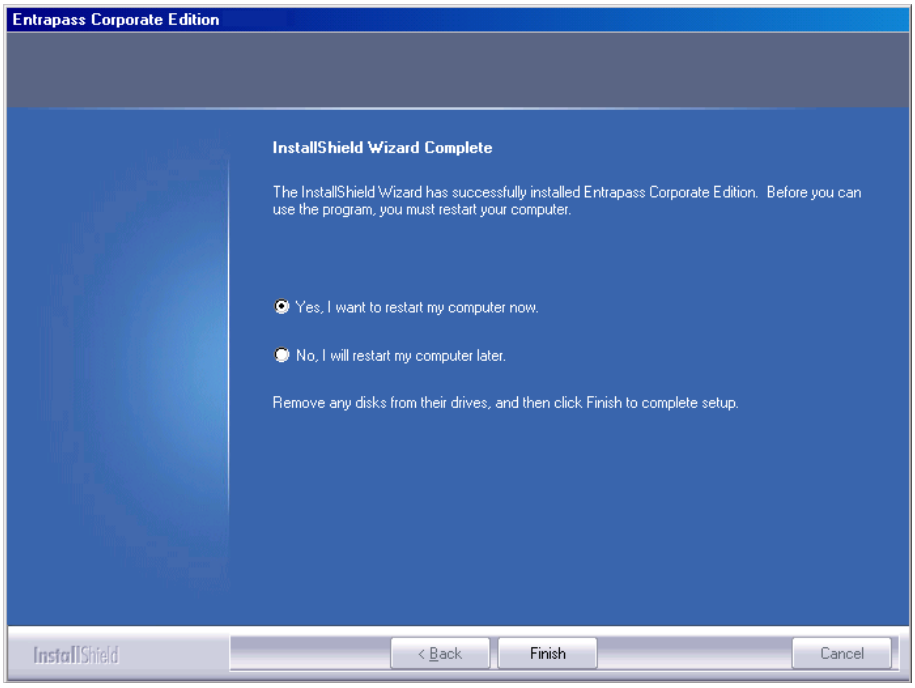
7 Нажать **Next** для продолжения работы. Система проверит, есть ли другие доступные для установки приложения или утилиты. При их обнаружении на экране появится соответствующее сообщение.



- 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 (смотрите раздел "Регистрация системы" на стр. 22).

- Чтобы завершить установку, нажать **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, раздел "Перед обновлением программного обеспечения", стр. 30.*

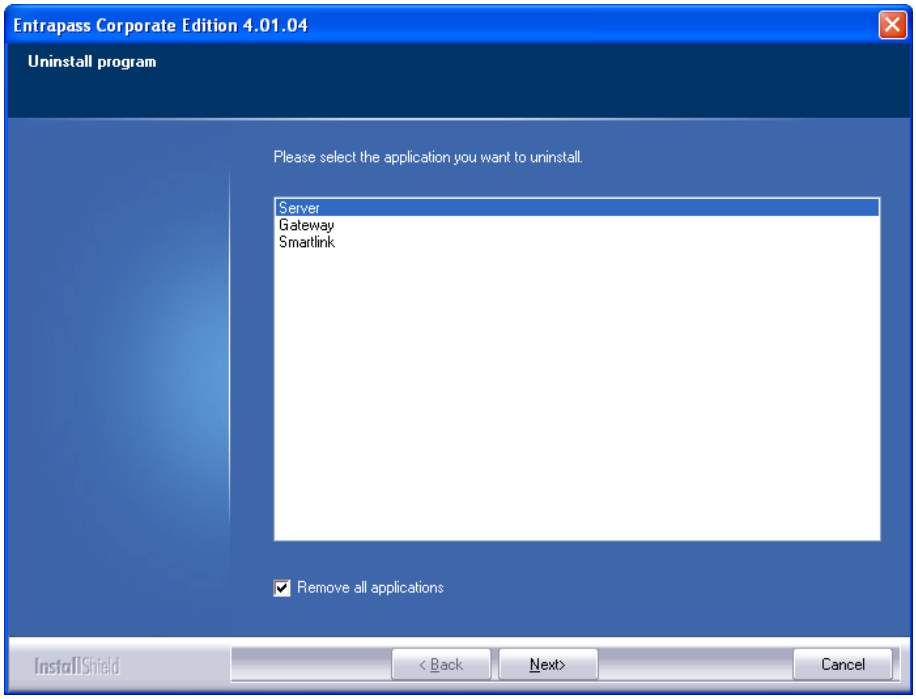
Удаление программного обеспечения EntraPass

Чтобы удалить программное обеспечение EntraPass с компьютера, следует запустить опцию **Add/Remove Programs** (Добавить/Удалить программы) с панели управления (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.

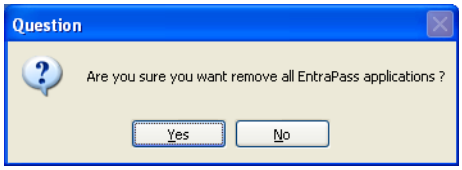
3 Выбрать из списка программу, которую необходимо удалить, и нажать Remove. На экране появляется диалоговое окно программы деинсталляции.



4 Указать, какое приложение необходимо удалить. Чтобы полностью деинсталлировать систему EntraPass, установить флажок в поле **Remove all applications** (Удалить все приложения)**.**

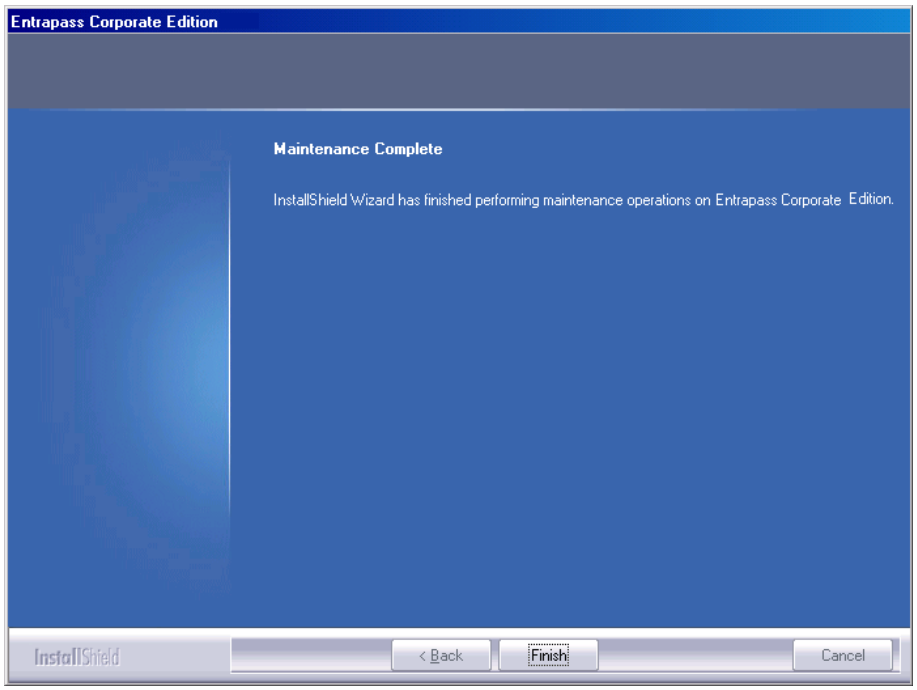
5 Нажать **Next** (Далее) для продолжения работы.

6 Чтобы начатый процесс был продолжен, необходимо подтвердить своё желание выполнить его.



- Нажать **Yes** (Да)**,** чтобы продолжить процесс деинсталляции.
- Нажать **No** (Нет), чтобы отменить деинсталляцию.

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



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

9 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. Сервер представляет собой специализированный компьютер, включённый в сеть, который организует доступ к базе данных системы управления. Он получает и отправляет данные через шлюзы.

Шлюзы получают информацию с сайтов 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 несмотря на отсутствие возможности подключения CardGateway к резервному серверу все события будут храниться в буфере, пока соединение с основным сервером не будет восстановлено.*

Программа позволяет оператору одновременно запускать шлюз и рабочую станцию щелчком мыши по ярлыку Gateway-Workstation на рабочем столе.

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 Corporate Edition** > **Server** / **Workstation** (Сервер/Рабочая станция), где в качестве приложения EntraPass может использоваться только приложение Рабочая станция (**Workstation**), Шлюз (**Gateway**) или любая самостоятельная утилита системы. Кроме того, для запуска программы можно воспользоваться ярлыком EntraPass на рабочем столе.

2 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.

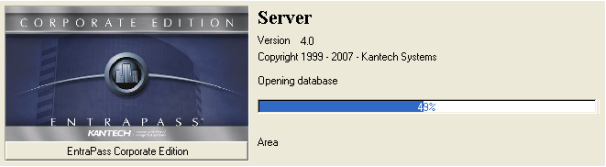
ПРИМЕЧАНИЕ. *Сначала следует запустить сервер EntraPass. Если запустить рабочую станцию раньше сервера, система предложит зарегистрировать рабочую станцию на сервере, даже если она уже была зарегистрирована. Если приложение уже было зарегистрировано, нужно просто запустить сервер.*

Запуск основного сервера EntraPass

Сервер EntraPass используется для следующих целей:

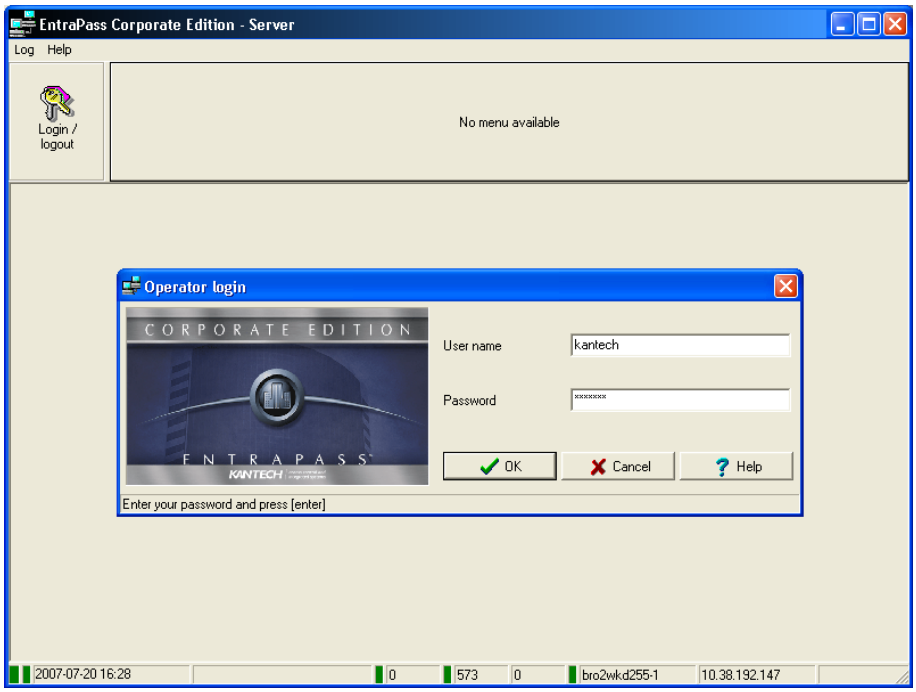
- отображение всех приложений, подключенных к серверу, журналов системных событий и ошибок
- регистрация новых подключений (приложения типа Рабочая станция, Шлюз, клиентские приложения типа интерфейса SmartLink, видеохранилища Video Vault, программы просмотра отчётов Report Viewer и др.)
- создание резервных 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 Запустить 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.

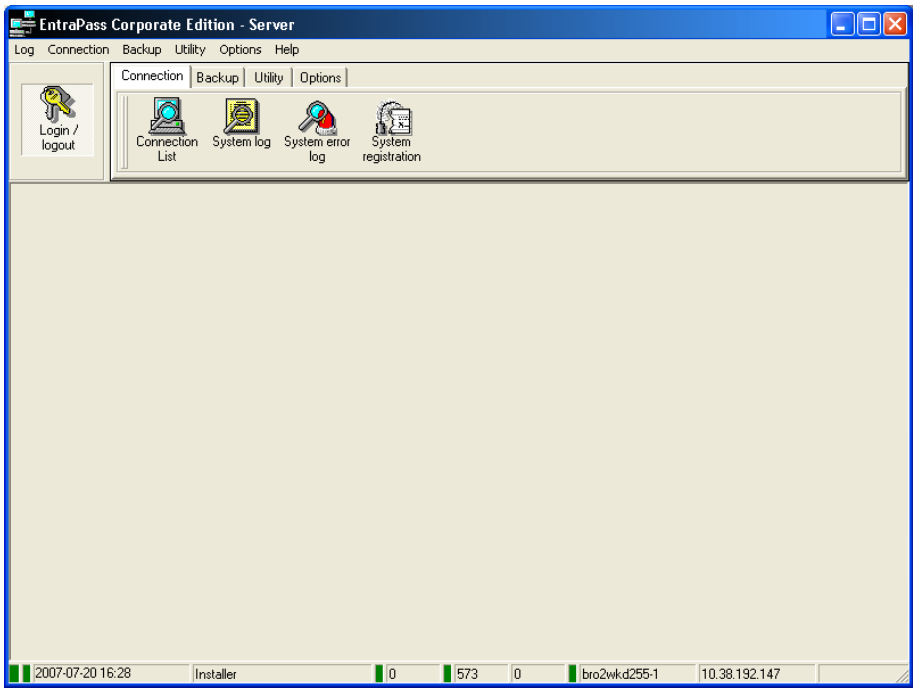


4 В открывшемся окне ввести имя пользователя (**User name**) и пароль (**Password**). По умолчанию в качестве имени пользователя используется "kantech". Имя не чувствительно к регистру. Пароль по умолчанию – kantech (нижний регистр). (Пароли чувствительны к регистру.)

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). Более подробная информация приведена в разделе "Описание уровней безопасности" на стр. 326.*

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.*

5 После правильного ввода регистрационных данных на экране появляется главное окно сервера EntraPass Server с активной панелью инструментов. Выбрать нужную закладку или войти 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.*

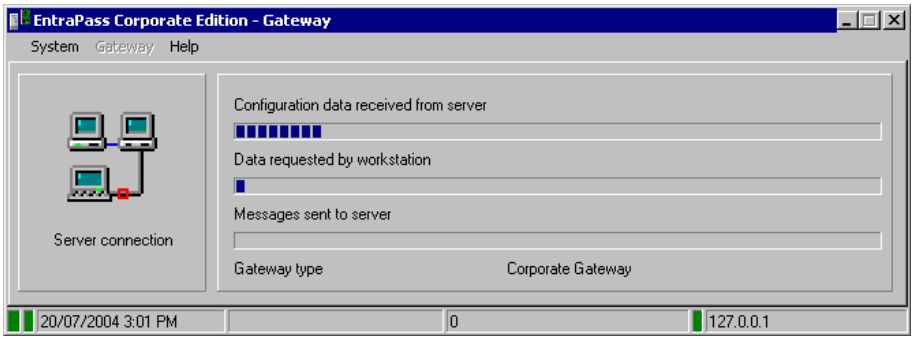
6 Установить курсор на флажок статуса (закрашенный прямоугольник) для отображения всплывающей подсказки. Первые два цветных прямоугольника в строке состояний отображают статус открытия и статус блокировки базы данных на сервере.

- 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 на доступность базы данных.

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; они указывают следующее:
   - **Configuration data received from the server** (Параметры конфигурации, полученные с 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.
   - **Messages sent to server** (Сообщения, отправляемые на сервер) – сообщения, передаваемые с контроллера на сервер.

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.

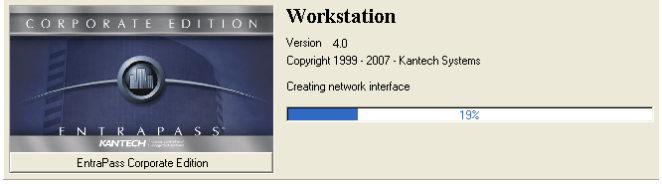
ПРИМЕЧАНИЕ. *Индикаторы состояния отображают статус соединения. Первый индикатор состояния показывает текущий статус соединения с сервером. Красный цвет означает, что связи между сервером и шлюзом нет. Эта ситуация возникает, если сервер не подключен (можно запустить его потом). В строке состояний также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

Запуск рабочей станции EntraPass Workstation

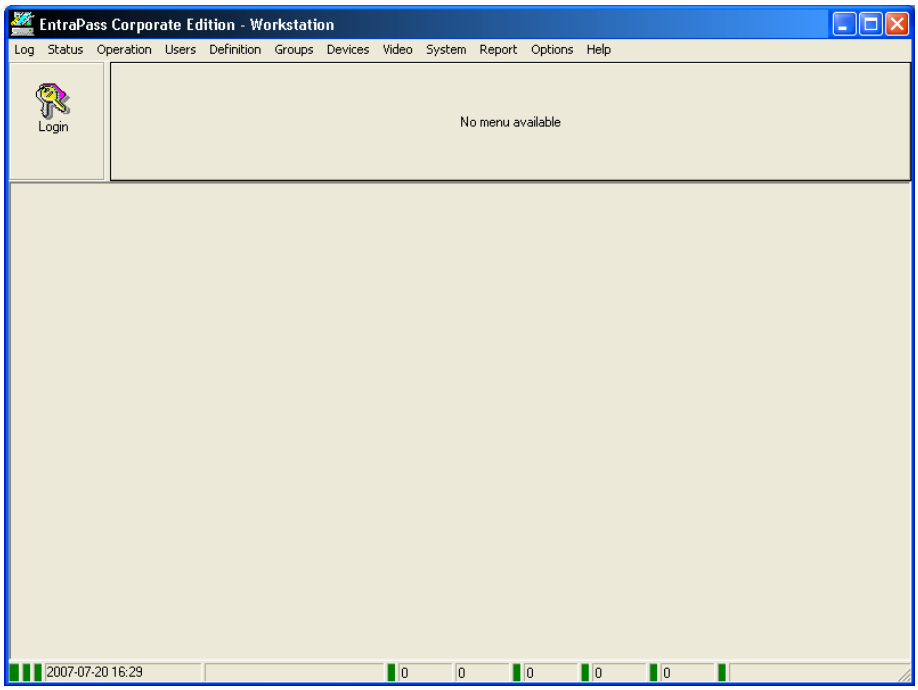
Рабочая станция EntraPass представляет собой компьютер, на котором установлено приложение EntraPass, предназначенное для мониторинга системы. С помощью этого приложения операторы получают доступ и возможность программирования базы данных и компонентов системы. Перед запуском программного обеспечения EntraPass Workstation следует убедиться, что сервер подключен к сети. Во время запуска приложение рабочей станции 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.

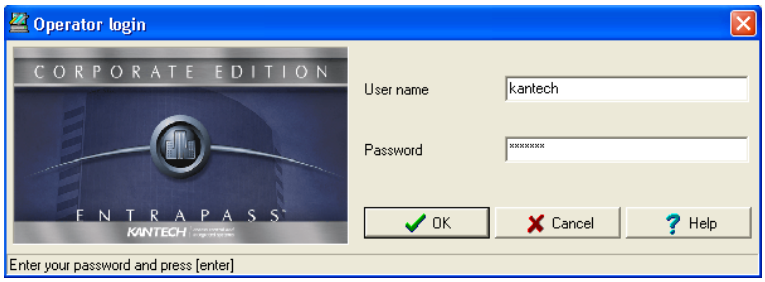


2 На экране появляется главное окно программы EntraPass Workstation.



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.*

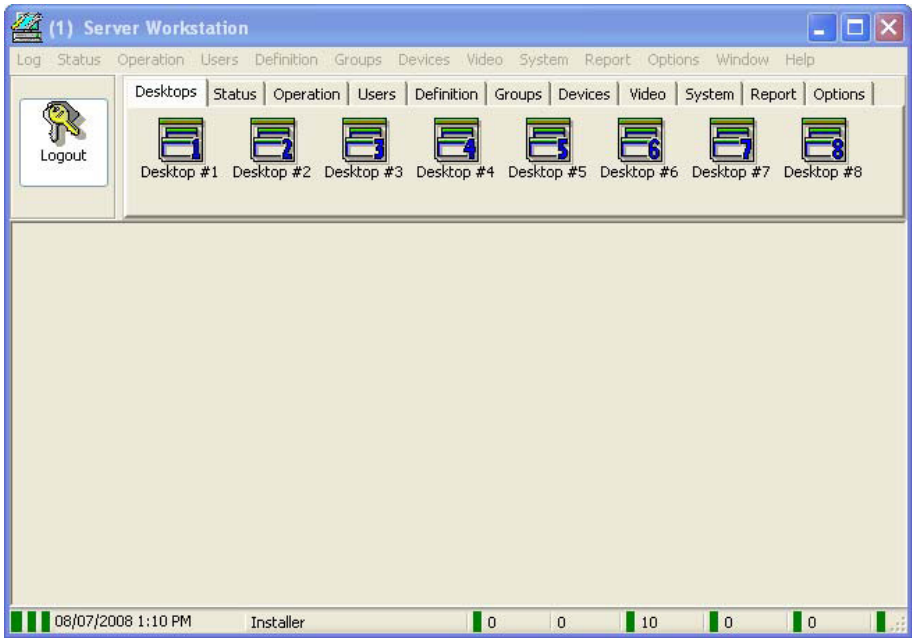
3 Нажать кнопку **Login**/**Logout** на панели инструментов для открытия окна регистрации оператора.



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. *Если используются заводские настройки, оператор не имеет возможности зарегистрироваться одновременно на нескольких рабочих станциях. При необходимости можно настроить систему таким образом, чтобы оператор мог одновременно выполнить несколько входов в систему, смотрите раздел 11 "Создание или изменение данных оператора", стр. 322. Однако у оператора есть возможность одновременно зарегистрироваться на сервере и на рабочей станции.*



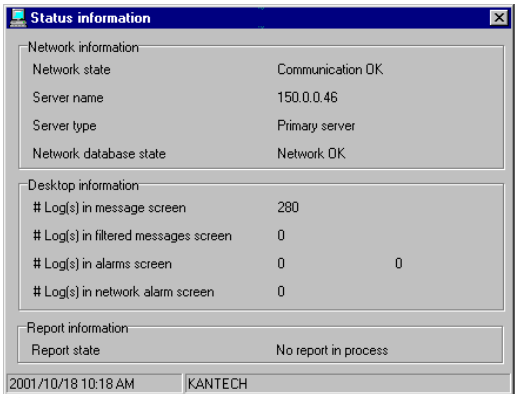
Получение сведений о статусе соединения с рабочей станцией

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, элементы на рабочем столе тревог, 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 статусе).



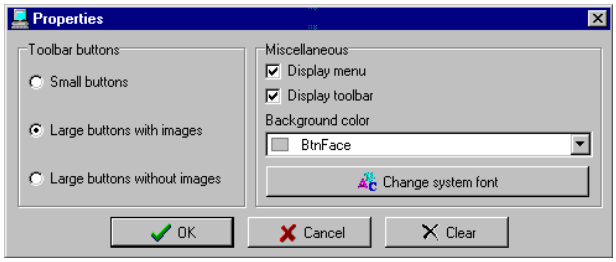
ПРИМЕЧАНИЕ. *Настоятельно рекомендуется выходить из программ EntraPass по кнопке* ***Login/Logout.*** *Это необходимо для корректного закрытия баз данных системы.*

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.

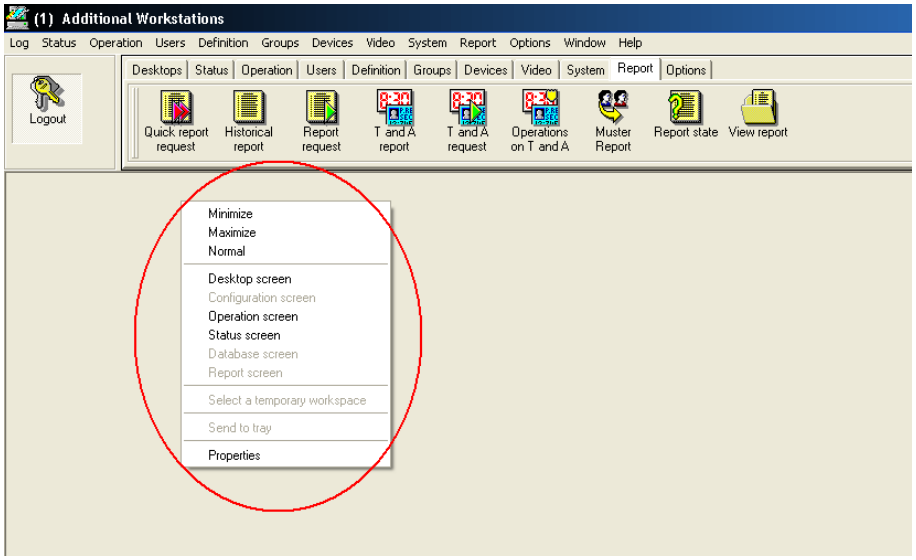
Восстановление свёрнутых окон на рабочем столе

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 для выполнения различных операций и окон статусов, 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.**

Автоматическая установка (Express Setup)

Express Setup позволяет устанавливать конфигурацию компонентов системы, включая сайты и контроллеры, а также устройства, связанные с этими компонентами (например, двери и входы). Программирование благодаря использованию этой утилиты сведено к минимуму, а установщики имеют возможность тестирования установки и компонентов системы.

Программу можно использовать для настройки сайта или для описания контроллеров, прикреплённых к определённому сайту. При использовании утилиты для выбора конфигурации сайта есть возможность привязать этот сайт к шлюзу. Кроме того, утилита позволяет быстро настроить сайт, используя минимум сведений о конфигурации подключённых к нему контроллеров.

Для запуска Express Setup из меню Start (Пуск) Windows® следует выбрать **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Corporate Edition** > **Server** > **Express Setup** или щёлкнуть по пиктограмме **Express Setup** в одном из окон рабочей станции EntraPass Workstation.

Если утилита используется для выбора конфигурации контроллера, она 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 описания контроллера.

ПРИМЕЧАНИЕ. *Чтобы запустить программу Express Express Setup, нужно зарегистрироваться на сервере. 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 "Программа "Express Setup" на стр. 514*.

Автономные обслуживающие программы системы

В систему EntraPass входит ряд автономных обслуживающих программ, 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 реиндексации архивных файлов, обновления полей базы данных, проверки архивных файлов, проверки целостности базы данных, проверки индекса базы данных, проверки ссылок и иерархии базы данных. Выполняется во время выключения сервера.
- **Express Setup** (Автоматическая установка). Программа служит для выбора конфигурации всех компонентов, имеющих отношение к шлюзу, включая тип используемых считывателей карт, способ соединения, число сайтов, число контроллеров на каждом сайте 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, управляющего открытием и закрытием до 4-х дверей, а также контроллера сетевой 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"). Служит для диагностики 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 EntraPass.
- **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 автономным обслуживающим программам EntraPass изложены *в разделе"Утилиты системы" на стр. 493.*

Диалоговые панели инструментов EntraPass

Основные кнопки, встречающиеся на панелях инструментов EntraPass, показаны ниже. Они позволяют быстро получить доступ к системным функциям. Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. 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 сайта, 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, оставив исходный компонент неизменным. 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, сайтам 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 приведена в разделе "Отображение связей компонентов" на стр. 56.
	Кнопка **Find** (Поиск) служит для поиска определённого объекта или компонента в базе данных системы с помощью специальной символьной строки. Более подробная информация приведена *в разделе "Поиск компонентов" на стр. 50.*
	Кнопка **Express Setup** (Автоматическая установка) позволяет установщикам и системным администраторам настраивать устройства, задавая настройки по умолчанию.
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 достоверно выполненного сохранения. Система предложит подтвердить выполнение операции.

Кнопка	Описание
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) 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.
Правая кнопка мыши	**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:

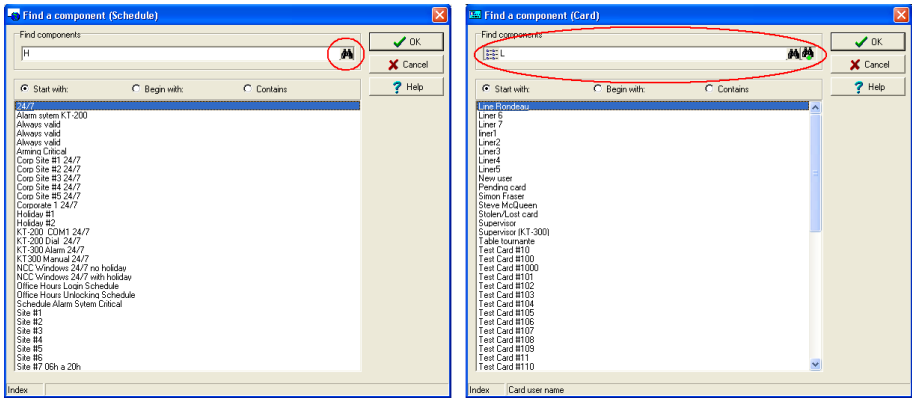
- Поиск компонентов
- Выбор компонентов
- Вывод на печать списков или отчётов
- Просмотр связей между компонентами

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.



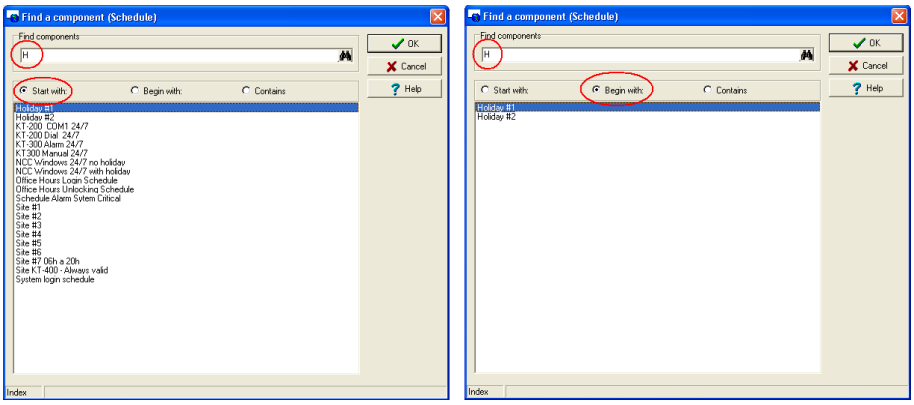
Слева изображено меню поиска компонентов, справа меню поиска карт.

Кнопки	Описание
	Поиск в базе данных компонентов или карт.
	Поиск в базе данных изображения, соответствующего карте, выбранной из списка.

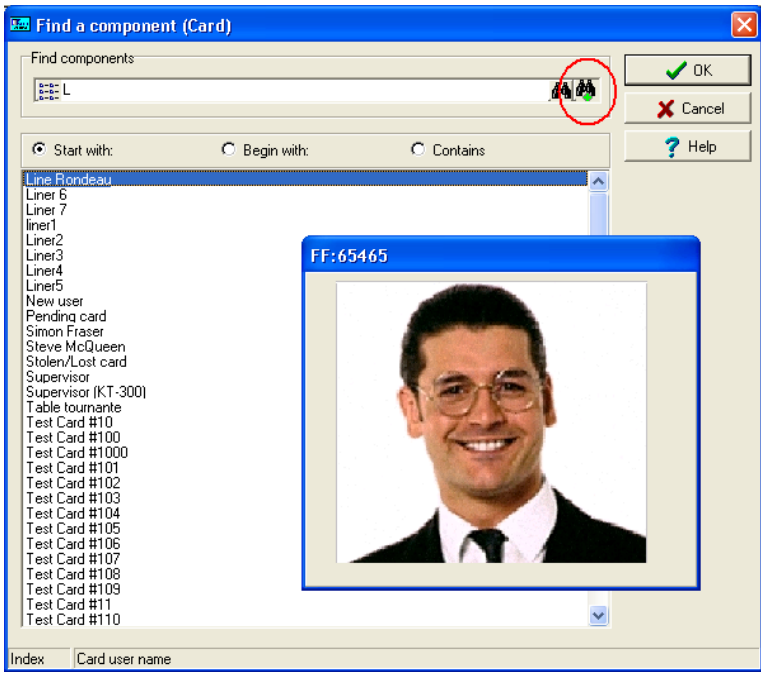
Кнопки	Описание
	Открыть меню, чтобы выбрать параметр, по которому необходимо осуществить поиск карты (номер карты, имя владельца, информационные поля карты и др.).

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 в списке карте, следует использовать кнопку поиска с изображением бинокля и знаком плюс.

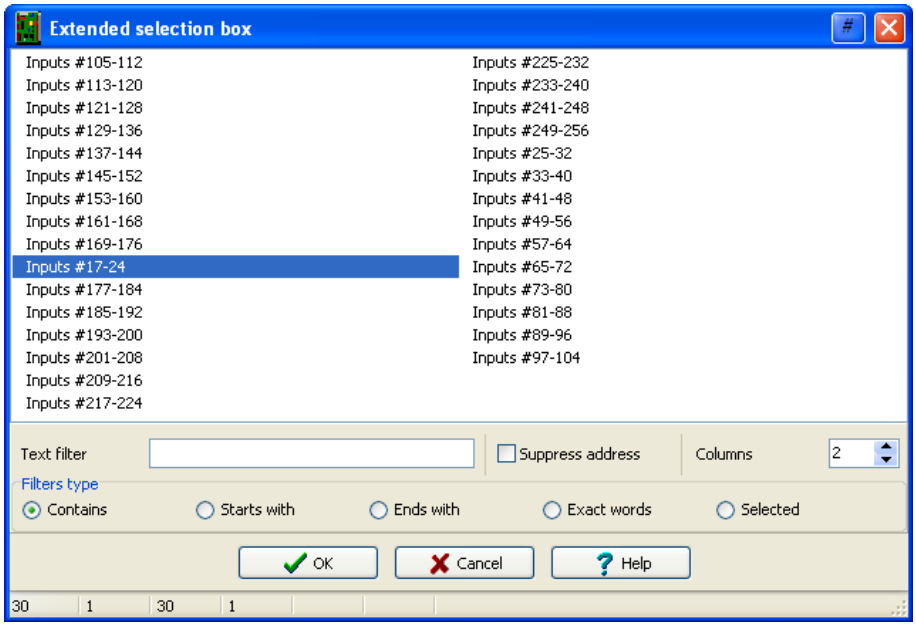


4 Для отмены поиска в процессе выполнения следует нажать кнопку **Cancel** (Отмена).

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. Эта функция доступна для таких компонентов, как приложения, контроллеры и двери, в тех случаях, когда для них предусмотрены выпадающие списки. В этом случае при помещении курсора на выпадающий список открывается окно-подсказка.



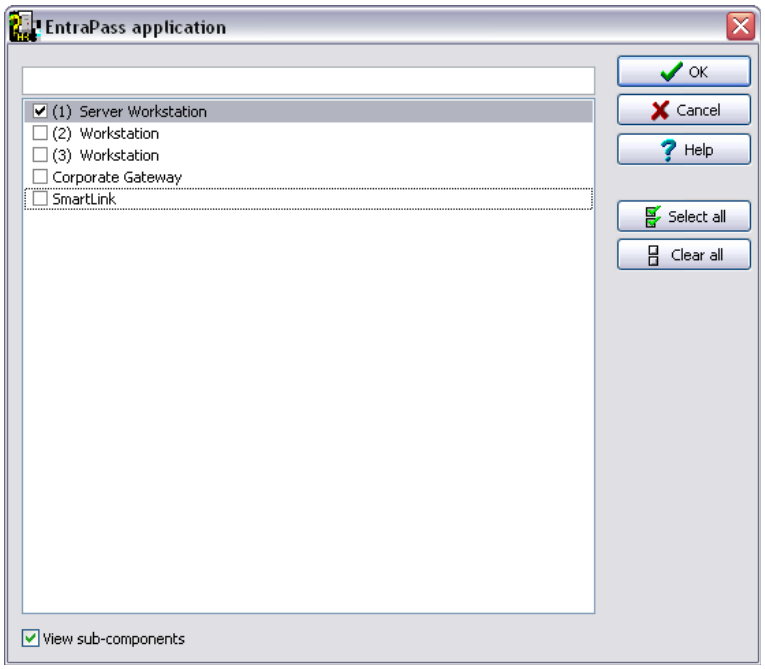
- В окне расширенного поиска предусмотрено использование следующих фильтров (**Filters types**):
- Contains (Содержит...)
- Starts with (Начинается с...)
- Ends with (Оканчивается на...)
- Exact words (Точное совпадение)
- Selected (Выделенное)
- В поле **Text filter** (Текстовый фильтр) следует указать, какие слова должен содержать искомый объект.
- Поле **Suppress the address** (Опустить 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

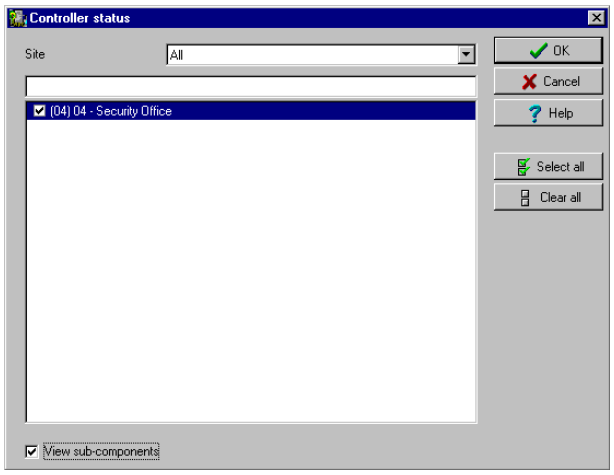
Функция Select Components (Выбор компонентов) позволяет выделить один или несколько компонентов системы. В зависимости от ситуации применяется тот или иной способ выделения.

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). 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.

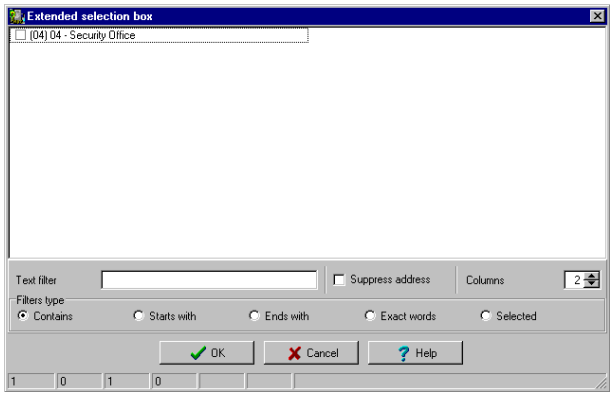
4 Если необходимо выделить все компоненты, следует воспользоваться кнопкой **Select all** (Выделить все). Чтобы снять выделение со всех компонентов, рекомендуется использовать кнопку **Clear all** (Очистить все). Для возврата к предыдущему экрану меню без внесения изменений и без выделений следует нажать 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 открывается окно расширенного режима поиска (Extended Selection Box).



6 В окне Extended Selection можно указать число колонок для удобного отображения всех компонентов. Чтобы сократить список, следует воспользоваться текстовым фильтром (**Text Filter**).



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

Выбор пути для хранения файлов

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, 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 сайта или шлюза

Система EntraPass даёт возможность связать определённый компонент с определённым шлюзом/сайтом. Например, можно указать праздничные дни для определённого сайта или шлюза.

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

2 Двойным щелчком мыши выбрать сайт/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), если такая кнопка имеется.
3. Если поставить флажок в поле **Print empty fields** (Выводить на печать пустые поля), 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 твёрдой копии отчёта или списка
- Сохранение отчёта или списка для дальнейшего использования в программе **Quick Viewer** или загрузка уже созданного отчёта. Более подробная информация об этой программе приведена *в разделе "Программы быстрого просмотра отчётов", стр. 522.*

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.*

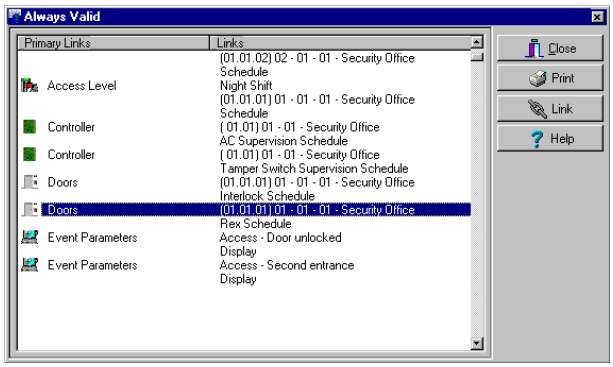
Отображение связей между компонентами

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.*

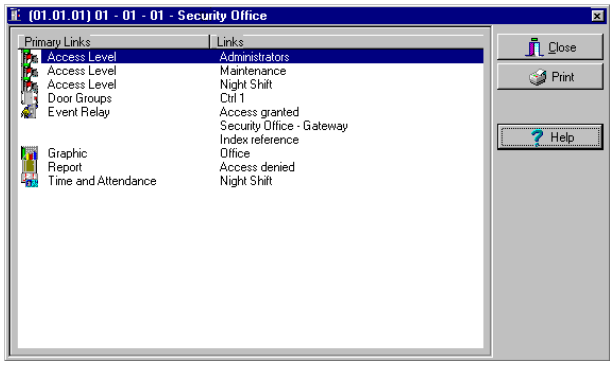
1 В любом окне меню выбрать компонент и нажать кнопку **Link** (Связь). На экране появятся все компоненты, связанные с выделенным объектом.

2 Пиктограммы, расположенные слева от компонентов, указывают их тип. Например, если выделить расписание **Always valid** (Достоверное всегда) в меню задания расписания Schedule 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 Door.* 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" используется на уровне доступа администратора (Administrator); пользователям с этим уровнем доступа разрешёно пользоваться этой дверью.

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

Глава 4 • Системные устройства

После установке оборудования и программного обеспечения системы необходимо настроить системные устройства доступа. Сюда входят программные компоненты (приложения EntraPass, шлюзы Gateways, интерфейс SmartLink, резервный сервер с базой данных и видеохранилище EntraPass Video Vault), а также физические компоненты (контроллеры, реле, двери и др.).

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, сайтов или контроллеров. 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 разделе "Программа автоматической установки" на стр. 514.*

ПРИМЕЧАНИЕ. *В случае интеграции с системами видеонаблюдения (функция Video Integration) 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, сайт, 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 (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:

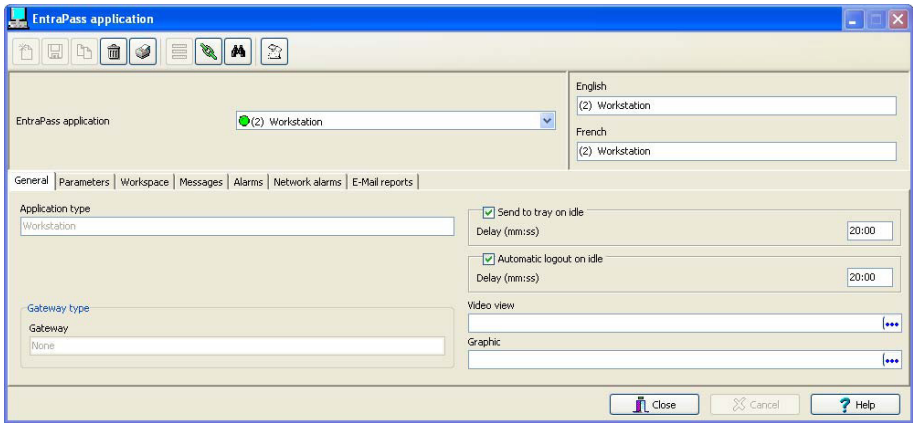
- Приложение Рабочая станция
- Приложение Сервер
- Одно приложение Corporate
- а также ряд утилит, включая редактор языков (Vocabulary Editor), Express Database и др.

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 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 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 приложения EntraPass.



ПРИМЕЧАНИЕ. *В зависимости от типа приложения (Application Type) в окне EntraPass Application отображаются разные параметры. Например, если тип приложения – рабочая станция (Workstation), то отображаются закладки* ***Workstation*** *(Рабочая станция)****, Gateway*** *(Шлюз) и* ***Site*** *(Сайт). 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** 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 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.

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

Описание общих параметров (раздел General)

Под закладкой **General** 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.

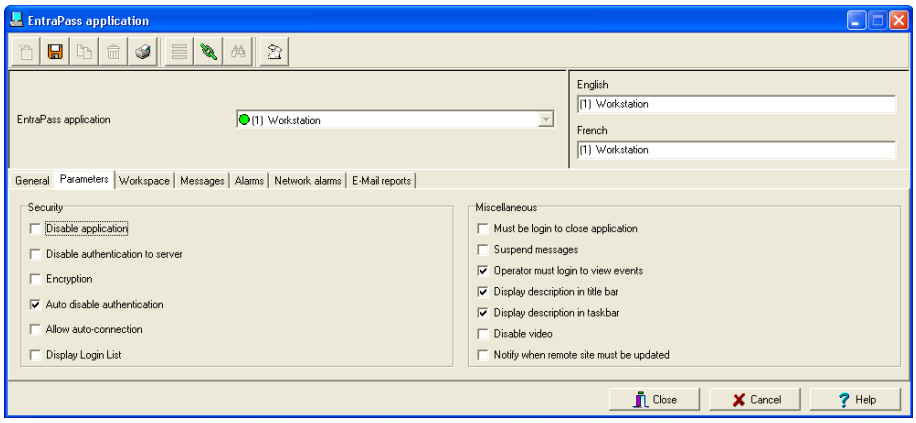
2 Если разрешено видеонаблюдение, то появляется поле **Video view** (Видеоокно). В таком случае следует выделить ячейку видеоокна, в которой следует отображать описываемый компонент. Подробнее о настройке видеоокон смотрите *раздел "Описание видеоокон" на стр. 162.*

3 В списке **Graphic** (Графические схемы) можно выбрать графический план для данного приложения, если необходимо. Подробные сведения об иллюстрациях приведены *в разделе "Описание графических схем" на стр. 198.*

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:

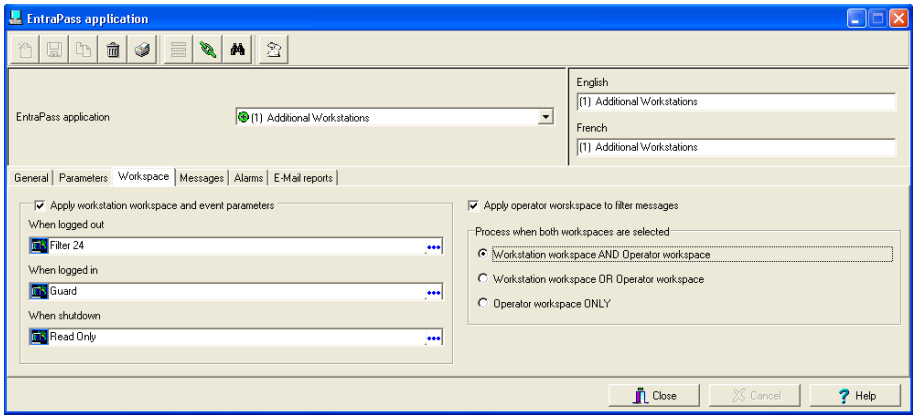
- **Disable application** (Запретить приложение). При выборе этой опции оператор не сможет запустить приложение. Эту опцию следует назначать с осторожностью.
- **Disable authentication to server** (Запретить аутентификацию на сервере). Если поставить флажок, то приложение нельзя будет зарегистрировать 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 не активной (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** (Отключить 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 системные сообщения.
- **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 видеособытий (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 сайтов). При установке флажка напротив этой опции система будет посылать уведомление перед обновлением удалённых сайтов. Операторы будут получать уведомление по модемной связи при каждом изменении данных, имеющих отношение к сайтам (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.

WARNING: Unauthorized use of this entire system for commercial broadcast on a regular basis, however despite frequent testing, and due to, but not limited to, errors or omissions in operating or electrical description, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.

Описание рабочего пространства (раздел Workspace)

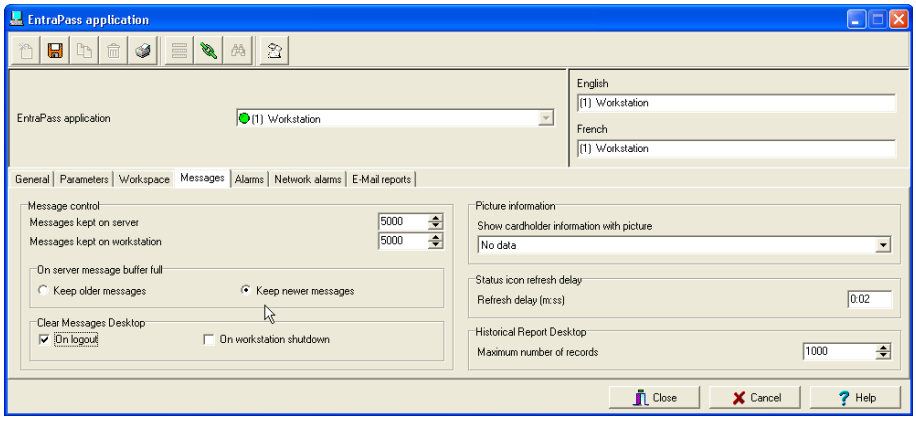
Закладка **Workspace** (Рабочее пространство) служит для выбора конфигурации рабочего пространства и параметров событий, которые будут применяться для конкретной рабочей станции, что позволяет создавать географические привязки в системе EntraPass. Эта функция позволяет описать, как должна работать рабочая станция.



- **Apply workstation workspace and event parameters** (Применять рабочее пространство рабочей станции и параметры событий). Разрешает выполнить описание рабочего пространства рабочей станции, чтобы отображать сообщения о событиях.
- **When logged out** (После завершения сеанса). Применить выбранные правила рабочего пространства, когда на рабочей станции нет зарегистрированных пользователей.
- **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). Выбрать рабочее пространство, у которого выше уровень в иерархии.
- **Operator workspace ONLY** (ТОЛЬКО рабочее пространство оператора). Рабочее пространство оператора имеет приоритет выше, чем пространство рабочей станции.

Описание параметров управления сообщениями (раздел Messages)

1 Под закладкой **Messages** (Сообщения) собраны параметры, описывающие порядок обработки сообщений, если рабочая станция подключена (или нет) к серверу.



ПРИМЕЧАНИЕ. *Рабочие столы сообщений следует настроить в меню описания рабочих столов (Desktop). Подробнее смотрите раздел Рабочие столы EntraPass на стр. 369.*

2 В меню управления сообщениями Messages необходимо выполнить следующие настройки:

- Указать, сколько сообщений 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 сообщений на каждую рабочую станцию EntraPass (по умолчанию 5 000).
- Указать, сколько сообщений должно **храниться на рабочей станции**. Каждая рабочая станция EntraPass может хранить максимум 100 000 сообщений. По умолчанию установлено 5 000 сообщений.

ПРИМЕЧАНИЕ. *Рабочая станция EntraPass всегда сохраняет самые свежие события. Для просмотра давних событий следует обратиться к архивным отчётам. Подробнее порядок обращения к отчётам описан в разделе Отчёты на стр. 411.*

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 и архивирует новые.
- **Keep newer messages** (Сохранять новые сообщения). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет новые сообщения и архивирует старые. Сообщения обрабатываются в порядке поступления.

4 В разделе **Clear Message Desktops** (Очищать рабочие столы сообщений) 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.).

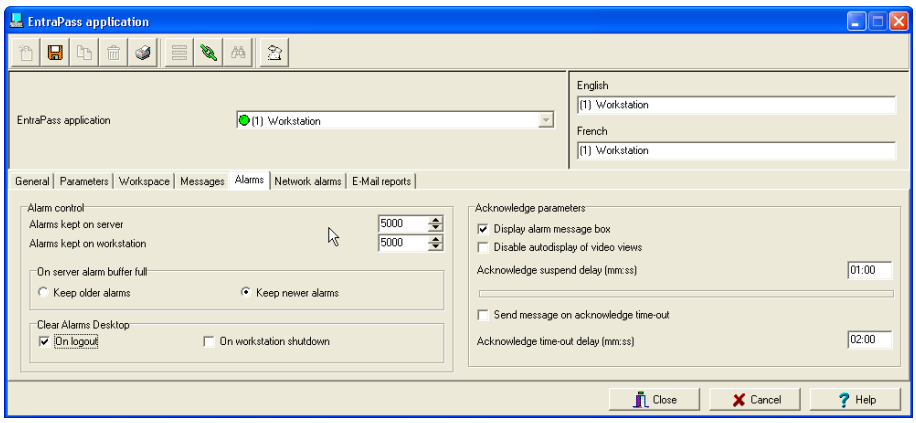
ПРИМЕЧАНИЕ. *По умолчанию в этих полях отображаются надписи “card information #1” ... “card information #10”. Эти надписи можно заменить другими по своему желанию. Более подробная информация об изменении надписей в информационных полях идентификационной карты приведена в разделе "Индивидуальная настройка названий информационных полей идентификационной карты" на стр. 236.*

6 В разделе **Status icon refresh delay** (Задержка обновления пиктограммы статуса) указать интервал обновления статуса 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. Максимальное число 200 000.

Описание 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 тревог следует настроить в меню описания рабочих столов Desktop. Подробнее смотрите раздел "Рабочие столы EntraPass" на стр. 369.*

2 В меню Alarms 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 5 000).

- 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 самые свежие события. Для просмотра давних событий следует обратиться к архивным отчётам. Подробнее порядок обращения к отчётам описан в разделе Отчёты на стр. 411.*

3 Указать, какие тревоги (старые или новые) следует оставить на сервере после заполнения всех доступных ячеек памяти:

- **Keep older alarms** (Сохранять старые тревоги). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет старые тревоги и архивирует новые.
- **Keep newer alarms** (Сохранять новые тревоги). Если рабочая станция EntraPass работает автономно, а буферная память сервера заполнена, сервер сохраняет новые тревоги и архивирует старые. Обработка тревог выполняется в порядке поступления.

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)

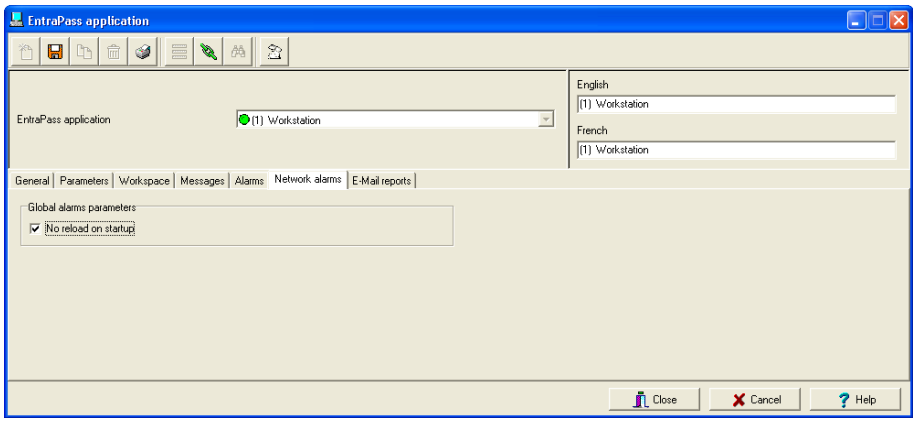
5 Кроме того, можно настроить параметры подтверждения (Acknowledgement parameters). Чтобы окно для подтверждения появлялось даже при работе в другом приложении, следует поставить галочку в поле **Display alarm message box** (Показывать окно тревожных сообщений). В этом случае необходимо также указать время, на которое можно отложить подтверждение получения (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. Действительно, видеоокна, предназначенные для сигнализации тревог и прикреплённые к компонентам системы, автоматически появляются на экране при переключении компонента в тревожный режим.

7 Если выделить опцию **Send message on acknowledge time-out** (Послать сообщение, если подтверждение отсутствует), то во всех случаях, когда от оператора не получено подтверждение, 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 разделе "*Рабочие столы EntraPass" на стр. 369.*

Описание сетевых тревог (раздел 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 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.

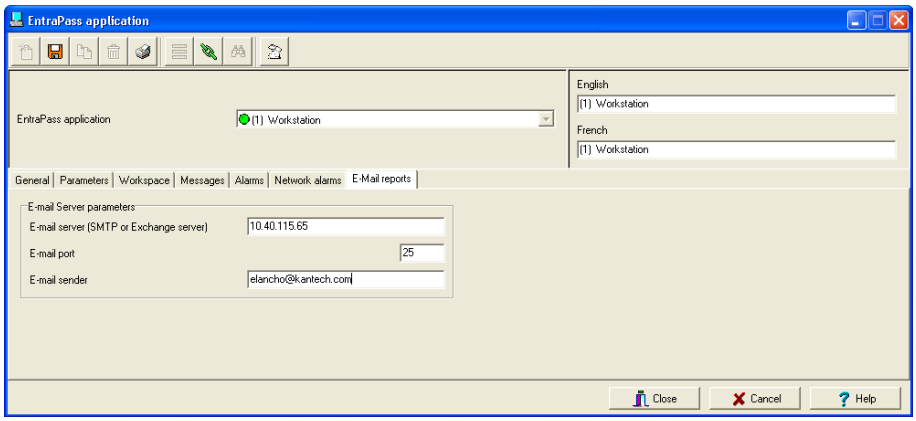
ПРИМЕЧАНИЕ. *Повторную загрузку системных тревог выполняют на рабочем столе Network Alarms (Сетевые тревоги). Для этого следует открыть рабочий стол, правой кнопкой мыши щёлкнуть на одном из пунктов, чтобы вызвать контекстное меню, и выбрать в меню пункт* ***Refresh*** *(Обновить). Эту опцию можно использовать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

Описание параметров электронных отчётов (E-Mail Reports)

Система EntraPass предоставляет своим пользователям возможность получать и отправлять отчёты по электронной почте. Электронные письма можно отправлять в двух форматах: rpf (report pack files - упакованные файлы отчётов) и CSV (comma separated values – значения, разделённые запятыми).

- **Файлы формата rpf.** Это сжатые файлы отчётов. Открываются по двойному щелчку мыши. Для просмотра rpf-файлов необходимо установить новую версию пакета рабочей станции EntraPass Workstation или программу просмотра отчётов Report Viewer (Окно настройки), которые можно найти на установочном компакт-диске или на сайте компании Kantech (www.kantech.com).
- **Файлы формата CSV.** Эти файлы можно просматривать в Excel или при помощи любого текстового редактора файлов.

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.

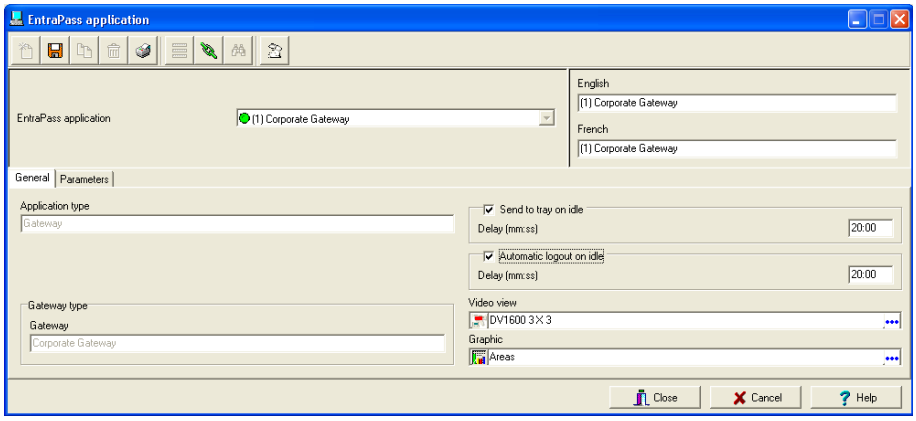
ПРИМЕЧАНИЕ. *Чтобы просмотреть отчёты, сформированные системой EntraPass, на компьютерах, на которых не установлена эта система, следует установить на них специальную программу просмотра отчётов* **Report Viewer**. *Для установки этой утилиты необходимо открыть окно настройки программы на установочном компакт-диске: Installation CD-ROM > Setup window.*

Настройка конфигурации приложения Шлюз (Gateway)

Шлюз EntraPass перерабатывает информацию, полученную с контроллера или сайта, и передаёт преобразованные данные на сервер, который, в свою очередь, отправляет их определённому приложению EntraPass. Кроме того, он преобразует данные, полученные с рабочей станции EntraPass, и передаёт их контроллерам. Таким образом, шлюз взаимодействует с сайтами и с приложением EntraPass. Приложение типа Шлюз позволяет управлять сайтами контроллеров, подключенными к шлюзу. При этом в системе может быть до 40 шлюзов Corporate Gateways.

Описание общих параметров 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) смотрите в разделе "Конфигурация приложений EntraPass" на стр. 60.

3 Настройка параметров безопасности для шлюзов описана в разделе "Описание параметров безопасности в разделе Parameters" на стр. 62.

Настройка интерфейса Oracle/MS-SQL (CardGateway)

Интерфейс Oracle/MS-SQL создаёт в реальном времени зеркальную копию баз данных EntraPass по идентификационным картам (таблицу идентификационных карт Card table, таблицу групп карт Card group table, таблицу типа карт Card type table и таблицу электронных пропусков Badge table) в базе данных MS-SQL или Oracle. Помимо этого, операторы имеют возможность работать с системной базой данных идентификационных карт с помощью своих программ MS-SQL или Oracle. Таким образом, можно добавлять, изменять и удалять карты или получать другие сведения о картах из базы данных EntraPass.

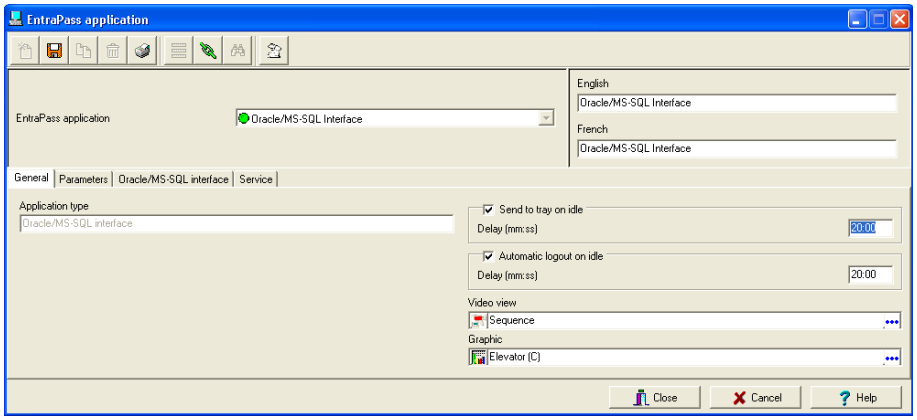
Данные идентификационных карт обновляются во всех базах данных, независимо от того, для каких целей используется программа (для изменения или для обновления базы данных). Интерфейс MS-SQL служит для передачи изменений на сервер и затем отправки их на рабочие станции.

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

Клиентское обеспечение MS-SQL или Oracle должно быть установлено на компьютере, оснащённом интерфейсом Oracle/MS-SQL. Интерфейс Oracle/MS-SQL не рекомендуется ставить на 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

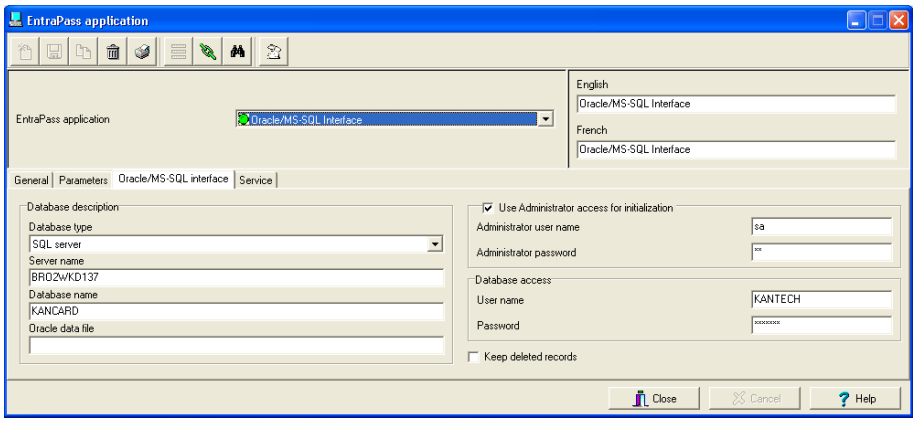
1 В строке **EntraPass application** в выпадающем списке выделить приложение Oracle/MS-SQL Interface.



2 Выполнить настройку параметров приложения, в котором установлен интерфейс Oracle/MS-SQL. Более подробные сведения по настройке смотрите *в разделе "Конфигурация приложений EntraPass" на стр. 60.*

3 Настроить параметры безопасности для интерфейса Oracle/MS-SQL под закладкой **Parameters** (Параметры). Подробнее смотрите раздел *"Описание параметров безопасности" на стр. 62.*

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: Oracle 8.0, Oracle 7.3 или 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). В случае установки флажка у пользователя будет возможность ввести достоверное 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 В 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.

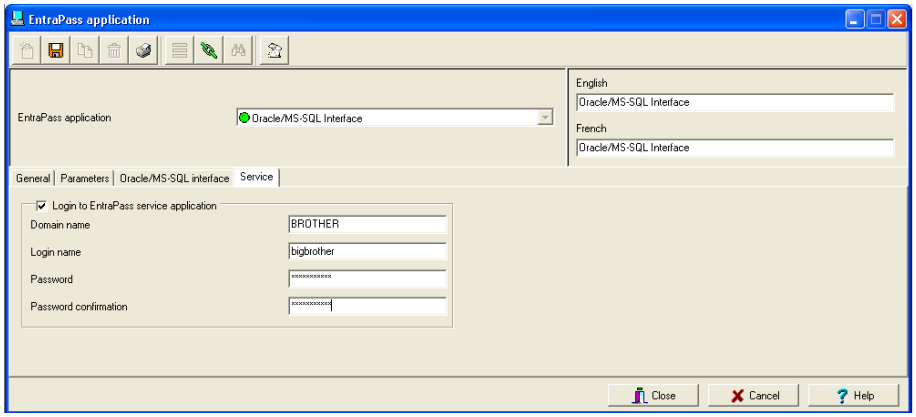
ПРИМЕЧАНИЕ. *Процедура доступа к базе данных не позволяет с помощью программы CardGateway создавать или изменять действующие параметры пользователя на сервере Oracle/SQL.*

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. *При неиспользовании данной опции 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 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 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 эту 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, которую будут затем использовать.

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 используется имя “**kantech**”.

2 Создать базу данных. По умолчанию используется имя базы “**KanCard**”.

3 Создать профиль пользователя. По умолчанию используется имя и пароль “**kantech**”.

4 Назначить для оператора kantech права доступа “**Owner**” (Владелец).

ПРИМЕЧАНИЕ. *Чтобы изменить любые настройки по умолчанию, 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 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 идентификационных карт Oracle/MS-SQL.

Если связь между зеркальной базой данных и основным сервером потеряна, база автоматически запускает резервный сервер взамен основного после окончания определённой временной задержки.

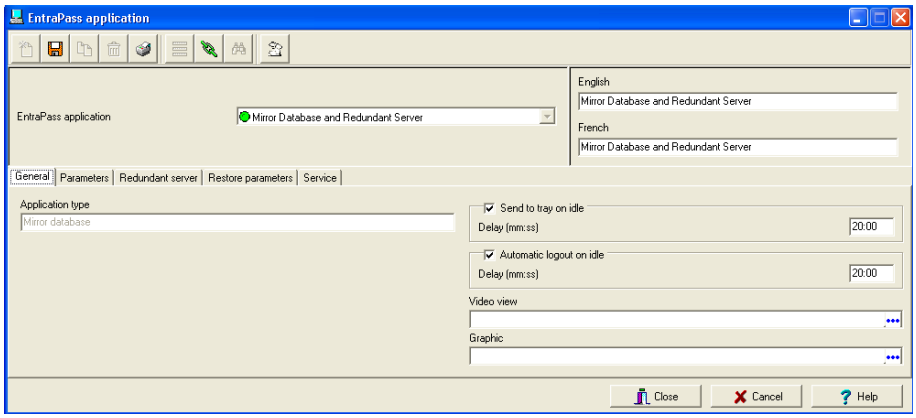
Программное обеспечение резервного сервера с зеркальной базой данных нельзя поставить на компьютер, на котором установлен сервер Entrapass. Это ПО должно быть установлено на отдельном компьютере.

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 рабочую станцию 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 безопасности (Security)

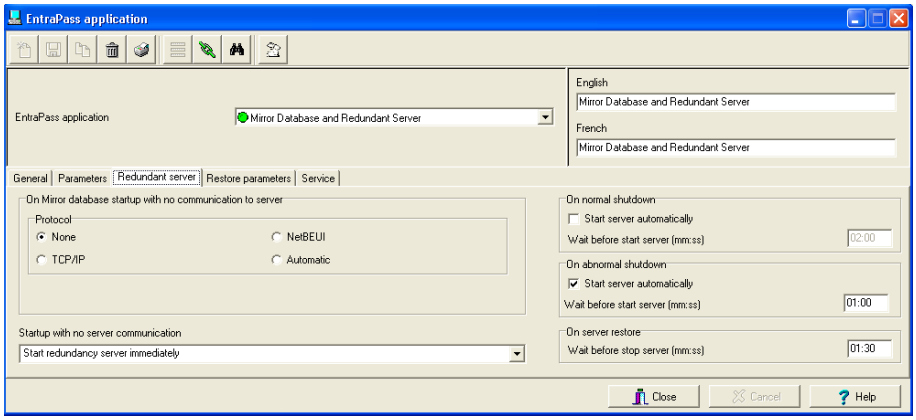
1 В выпадающем списке приложений **EntraPass application** выделить приложение "Mirror Database and Redundant Server" (Зеркальная база данных и резервный сервер).



2 Настроить параметры под закладкой **General** (Общее), следуя указаниям *раздела "Описание общих параметров" на стр. 61.*

3 Открыть закладку **Parameters** (Параметры) и настроить параметры безопасности для зеркальной базы данных и резервного сервера. Подробнее смотрите раздел "Описание параметров безопасности" на стр. 62.

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 и 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, включая DHCP сервер.*

6 Указать IP-адрес резервного сервера.

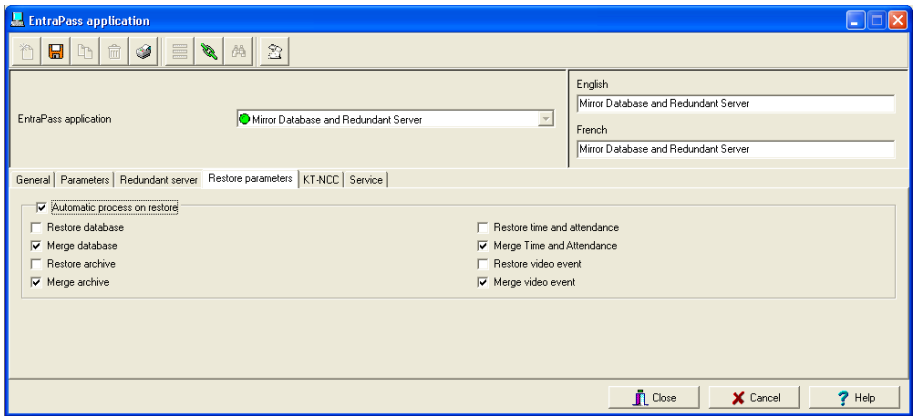
7 Выбрать действия, которые должны быть выполнены с резервным сервером в том случае, когда при запуске отсутствует связь с основным сервером (Startup with no server communication).

8 Выбрать способ запуска резервного сервера в случае выключения основного сервера: например, 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**): выбрать задержку, после окончания которой резервный сервер будет остановлен. Всё это время резервный сервер будет продолжать работать (не более 59:59 минут).

10 Открыть закладку **Restore Parameters** (Параметры восстановления) и указать необходимые действия после возобновления нормальной работы основного сервера.



- Для того чтобы автоматизировать процесс восстановления данных с резервного сервера, поставить флажок в поле **Automatic process on restore** (Автоматический процесс восстановления). После этого станут доступными остальные опции.

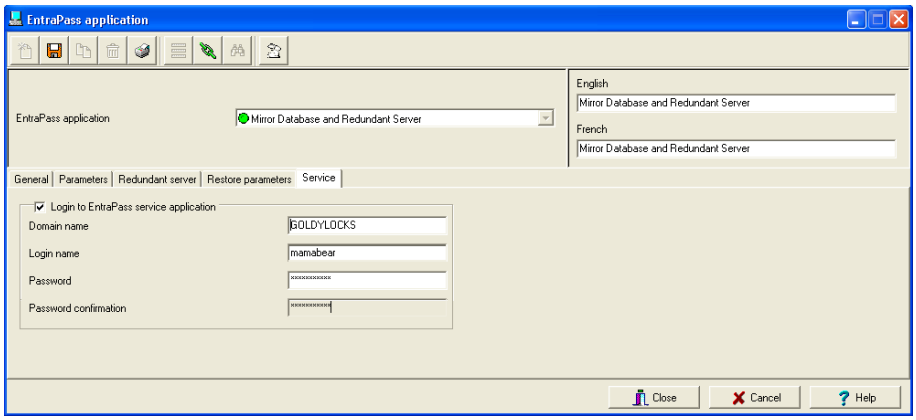
- Отметить флажками нужные опции, в зависимости от того, какие функции установлены и какие действия необходимо выполнить.

ПРИМЕЧАНИЕ. *Предусмотрено два действия:* **Restore** (Восстановить) *или* **Merge** (Объединить).

- **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.

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 от сети.*

11 Открыть закладку **Service** (Служба) и настроить параметры, необходимые для входа в систему при использовании резервного сервера и зеркальной базы данных 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).
- 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**.

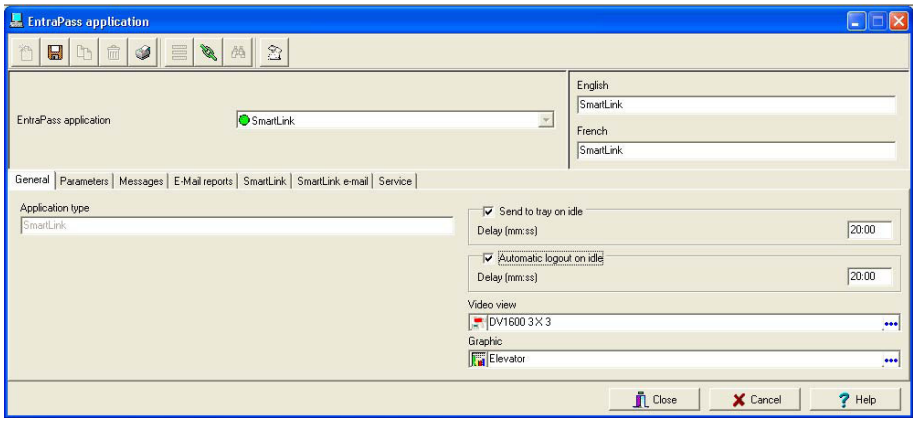
Настройка конфигурации приложения типа SmartLink

Приложение SmarkLink позволяет операторам обеспечивать взаимосвязь системы управления доступом EntraPass с любым интеллектуальным устройством, включая коммутаторы с видеоматрицами, 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 интерфейса 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 брошюре *"Справочное руководство по SmartLink"*.

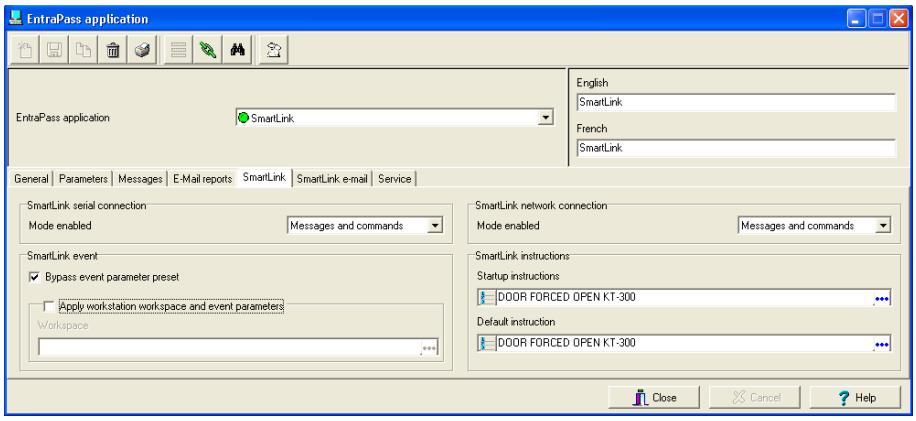
1 В выпадающем списке **EntraPass application** выделить приложение **SmartLink**.



2 Выполнить настройку параметров рабочей станции, на которой установлен интерфейс SmartLink. Подробнее смотрите раздел *"Описание параметров безопасности" на стр. 62.*

3 Настроить параметры безопасности рабочей станции SmartLink. Подробнее смотрите раздел *"Описание параметров безопасности", стр. 62.*

4 Открыть закладку **SmartLink** и настроить параметры соединения SmartLink.



5 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.

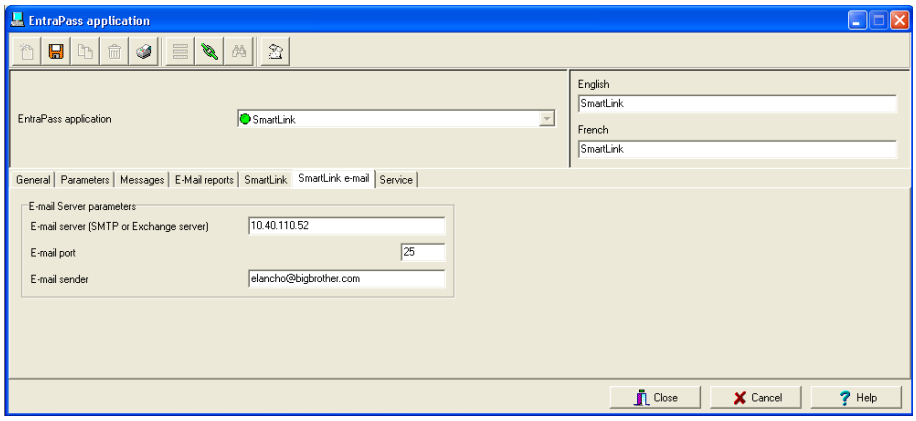
ПРИМЕЧАНИЕ. *При запуске приложения SmartLink параметры последовательного порта и сетевого соединения считываются с сервера EntraPass. Если режим сетевого соединения SmartLink указан отличным от “none”, то приложение SmartLink будет запускаться для обеспечения связи с ним клиентского приложения и использоваться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

6 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 описания 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.*

7 В разделе **SmarLink instructions** (Команды SmarLink) можно настроить команды **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 разделе "Описание команд" на стр. 357*.

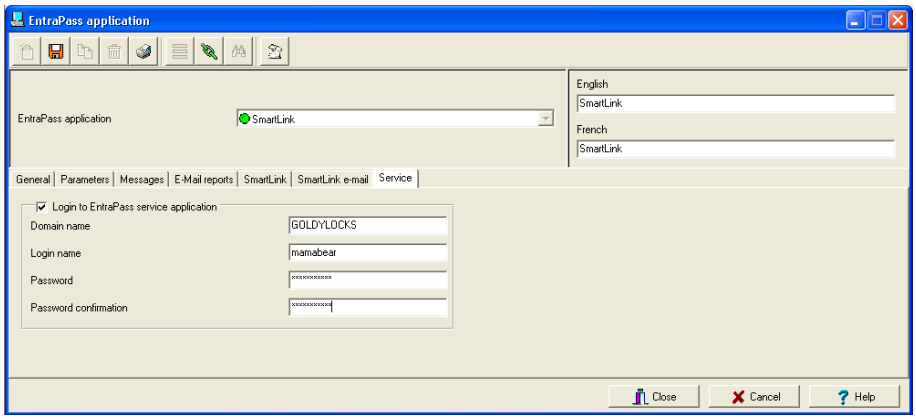
8 Открыть закладку **SmartLink e-Mail** (Электронная почта SmartLink) для просмотра и настройки параметров соединения SmartLink.



- 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.*

9 Открыть закладку **Service** (Служба) и настроить параметры, необходимые для входа в систему при использовании сервера SmartLink в режиме службы и для выдачи результатов пользователю.

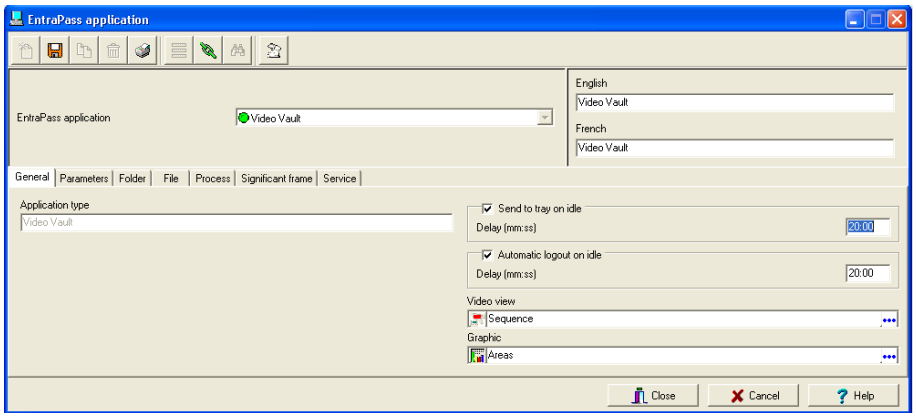


- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login to EntraPass service application** (Регистрационные данные для работы приложения в режиме службы).
- Для интерфейса SmartLink ввести имя домена в поле **Domain name** и имя пользователя в поле **Login name**.
- Указать пароль 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 (Video Integration), 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 видеохранилища изложены *в разделе "Добавление дополнительных компонентов/функций" на стр. 12.* Детали работы с приложением EntraPass Video Vault смотрите *в разделе "Видеохранилище EntraPass Video Vault" на стр. 499.*

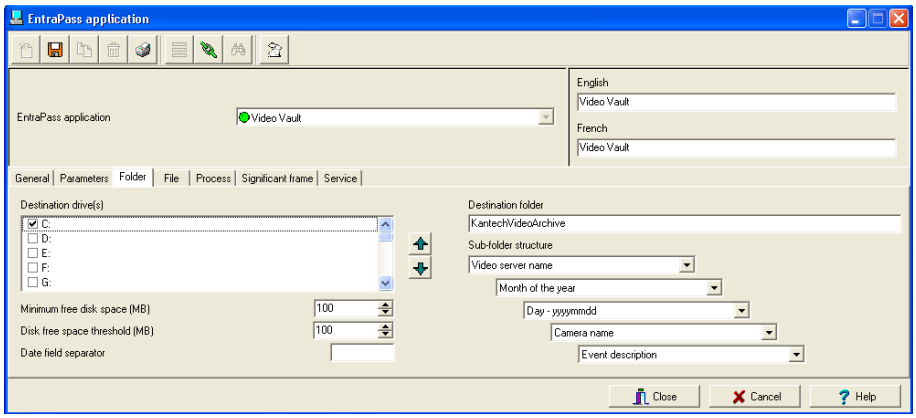
1 В выпадающем списке **EntraPass Application** выделить приложение EntraPass Video Vault.



2 Настройку общих параметров приложения EntraPass Video Vault выполнить, как описано в разделе "Описание общих параметров" на стр. 61.

3 Настройку параметров безопасности видеохранилища выполнить, как описано в разделе "Описание параметров безопасности" на стр. 62.

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**).



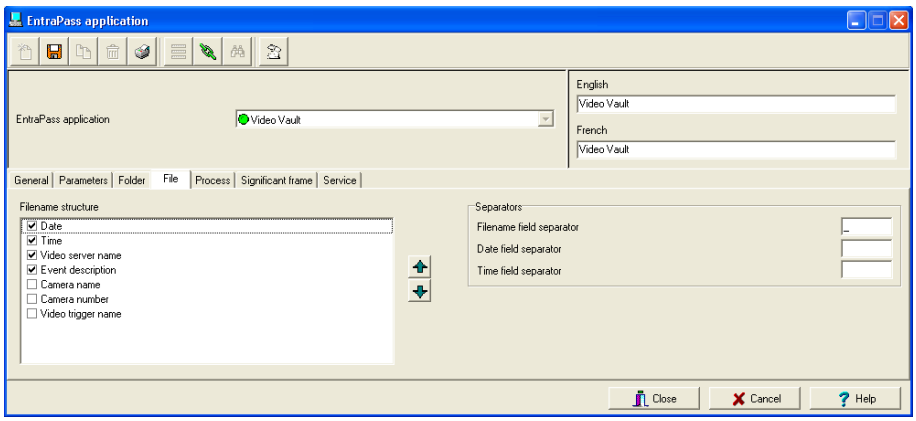
- **Destination drive(s)** (Целевой(ые) диск(и)). Список дисков, на которых будут храниться видеозаписи. Видеофрагменты будут записываться, в зависимости от доступного места на дисках, на всех выбранных дисках по порядку.

ПРИМЕЧАНИЕ. *Целевые 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.
- **Disk free space threshold, MB** (Граница свободного пространства, Мб). Максимальное занятое файлами пространство на диске, по достижении которого система посылает сообщение, что видеохранилище заполнено.
- **Date field separator** (Разделитель полей даты). 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. Всего предусмотрено 5 уровней вложенных папок.

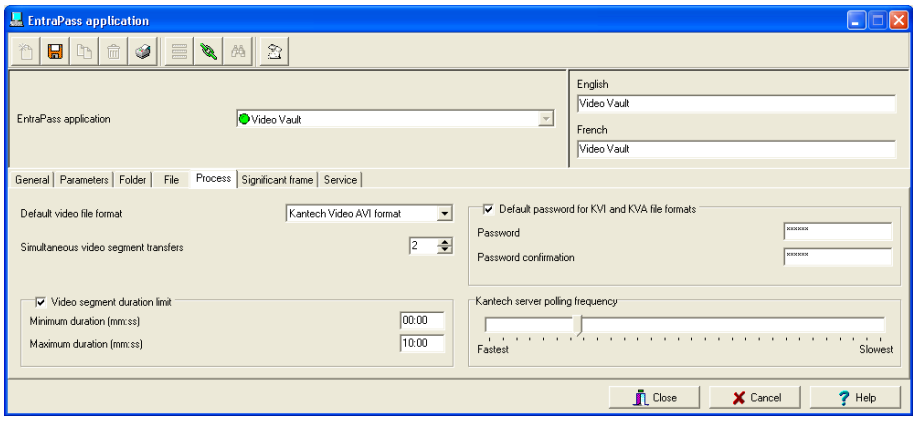
5 Открыть закладку **File** (Файл) для выбора способа присвоения имён файлов.



- **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. Видеорегистраторы серии EDVR работают с файлами формата AVI. 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.

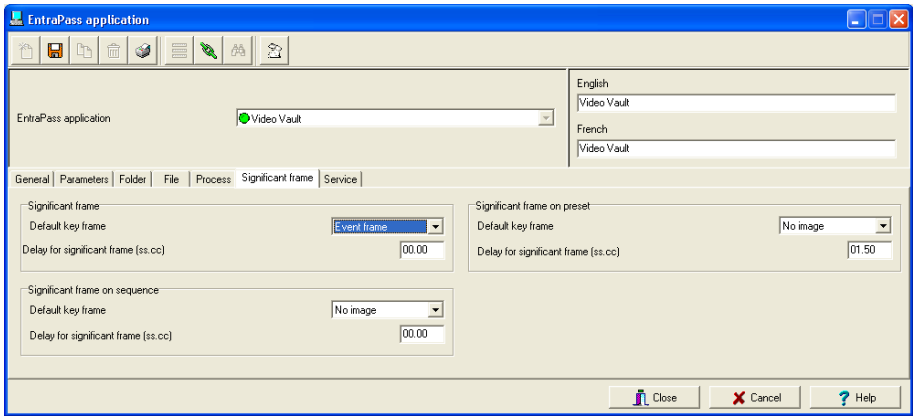
ПРИМЕЧАНИЕ. *Чем больше число одновременно извлекаемых файлов, тем больше должна быть пропускная способность сети. Поскольку при передаче видеоданных затрачивается значительная часть сетевых ресурсов, рекомендуется обратиться к администратору сети для оптимизации этих настроек.*

- **Video segment duration limit** (Ограничение длительности видеофрагмента). Необходимо задать допустимую минимальную и максимальную длительность архивируемых видеофрагментов. После установки флажка в данном поле на экране становятся активными поля ввода минимальной (Minimum) и максимальной (Maximum) длительности видеоданных. Данная функция, в частности, позволяет 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:



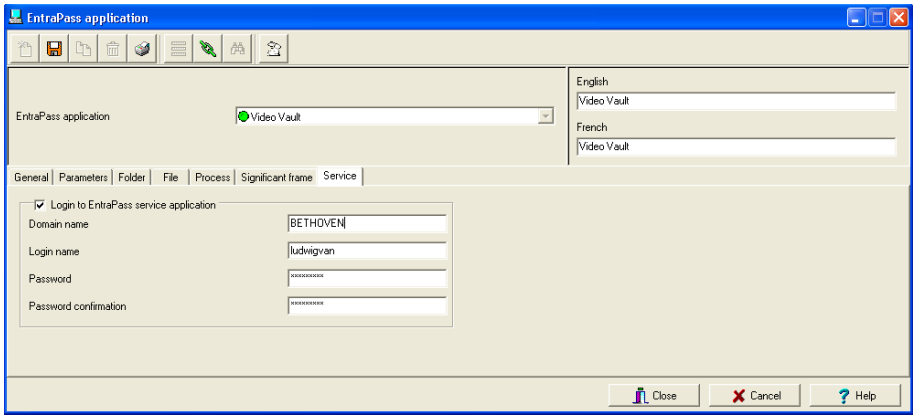
Significant Frame (Ключевой кадр). Наиболее представительный неподвижный кадр видеофрагмента. Ключевой кадр служит обобщением видеофрагмента. Его можно использовать как пиктограмму, например, при поиске определённой видеозаписи.

Significant Frame on Sequence (Ключевой кадр при использовании шаблона). Эта функция используется только с купольными камерами, которые настроены на определённый маршрут движения, для которого необходимо выбрать наиболее представительный из всех кадров видеофрагмента.

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

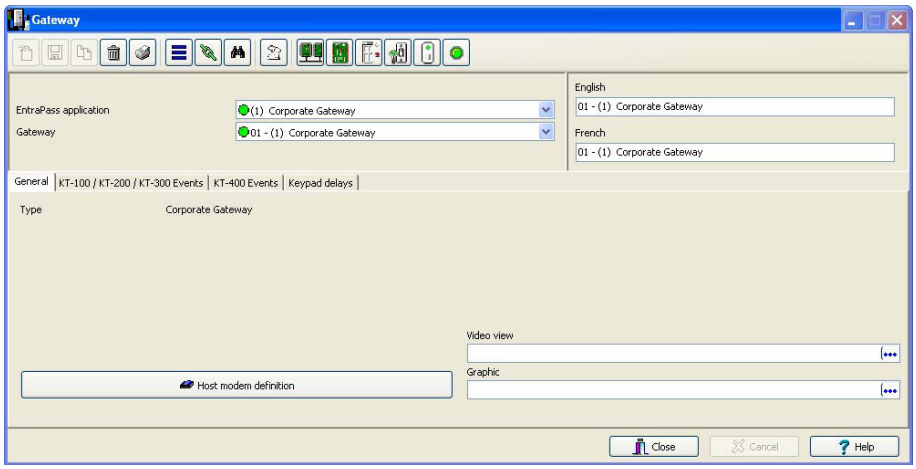
Шлюзы EntraPass перерабатывают информацию, полученную с контроллера или сайта, и передают преобразованные данные на сервер. Кроме того, шлюзы преобразуют данные, полученные с сервера, и передают их контроллерам. Приложение шлюза можно установить на отдельном компьютере или интегрировать его с другой рабочей станцией EntraPass. Ниже в таблице приведены характеристики шлюзов Corporate Gateway.

Параметры	Corporate Gateway
Число шлюзов	41
Локальные сайты	32 сайта с последовательными портами и USB
Оперативно доступные удалённые сайты	512 сайтов с интерфейсом Kantech IP Link* и контроллерами KT-400
Модемы на хост-сайте для передачи по коммутируемой линии	по 32 на каждом шлюзе
Удалённые сайты со связью по коммутируемой линии	по 512 на каждом шлюзе
Число контроллеров на каждый шлюз	всего 17 408 (по 32 KT на шлюз)
Число считывателей/кнопочных панелей на каждый шлюз	34,816
Число событий для включения/выключения таймера	29

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

Настройка конфигурации шлюза Corporate Gateway

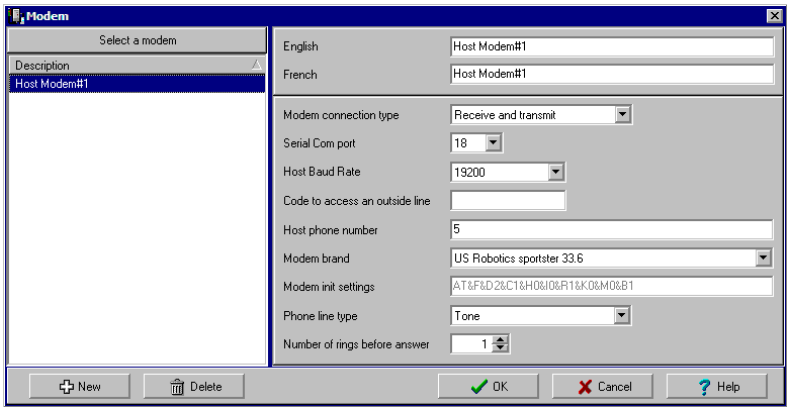
1 Открыть закладку **Devices** (Устройства) и нажать иконку **Gateway** (Шлюз).



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

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 Gateway подсоединён к первому контроллеру удалённого сайта через модем, то необходимо нажать кнопку описания модема **Host Modem** и настроить параметры связи для модема.

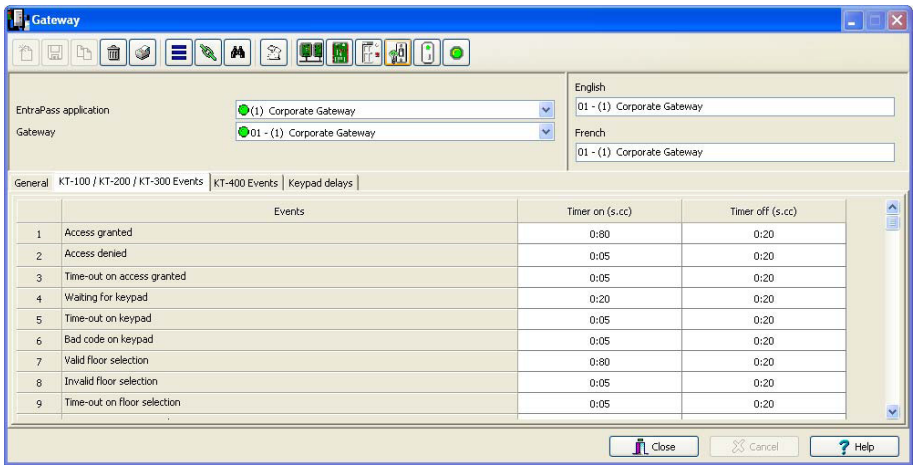


- Для того чтобы добавить модем в общий список, следует нажать кнопку **New** (Создать).

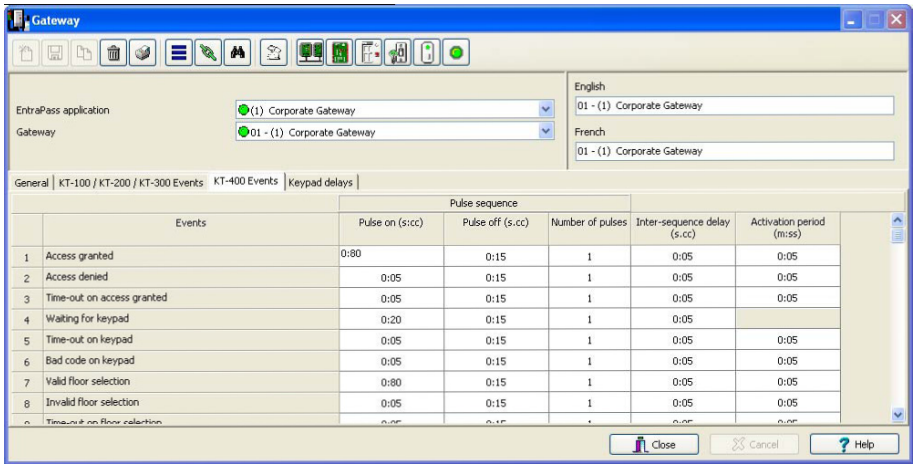
- Указать все необходимые значения параметров, как на иллюстрации выше, и нажать **OK** для возврата в меню **Device** (Устройство).

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. Таким образом, 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**) светодиода для каждого события. Версия Corporate Gateway позволяет настроить таким образом до 29 событий.



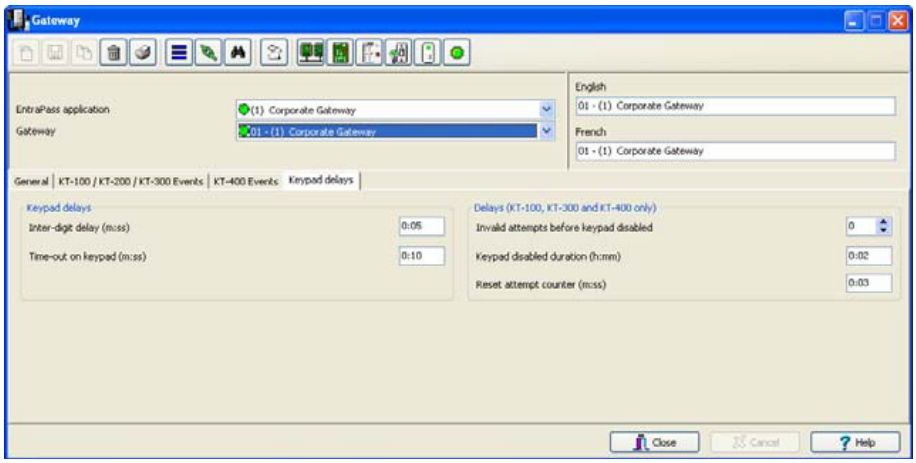
ПРИМЕЧАНИЕ. *Приложение Corporate Gateway поддерживает до 41 шлюза.* Ниже в таблице приведены все события, допустимые в версии Corporate Gateway.

Access granted (Доступ разрешён)	Request to exit denied (Запрос на выход запрещён)	Door unlocked (Дверь разблокирована)
Access denied (Доступ запрещён)	Arming request granted (Запрос для постановки на охрану разрешён)	Reader disabled (Считыватель отключён)
Time-out on access granted (Таймаут на разрешение доступа)	Arming request denied (Запрос для постановки на охрану запрещён)	Door armed (Дверь поставлена на охрану)
Waiting for keypad (Ожидание нажатия клавиши) – *прим. 1*	Postpone granted (Отсрочка разрешена)	Waiting for a second card (Ожидание второй карты) – *прим. 2*
Time-out on keypad (Таймаут нажатия клавиши)	Postpone denied (Отсрочка запрещена)	Time-out on waiting for a second card (Таймаут ожидания второй карты)
Bad code on keypad (Неверный код клавиши)	Door opened (Дверь открыта)	Access denied - Waiting for a second card (Доступ запрещён - Ожидание второй карты)
Valid floor selection (Достоверный выбор этажа)	Door forced open (Дверь взломана)	Access denied - Reader locked (Доступ запрещён – Считыватель заблокирован)
Invalid floor selection (Недостоверный выбор этажа)	Pre-alarm door opened too long (Предтревожное состояние двери при слишком долгом открытии)	Exit delay (Задержка выхода)
Time-out on floor selection (Таймаут выбора этажа)	Door open too long (Слишком долгое открытие двери)	Entry delay (Задержка входа)
Request to exit granted (Запрос на выход разрешён)	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 в* ***п. 6*** *на стр. 99.*

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. 113****.*

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



- 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 своих персональных данных на кнопочной панели.

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 (только для KT-100, KT-300 и KT-400)** указать **число неудачных попыток, после которых кнопочная панель 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 конфигурации сайтов

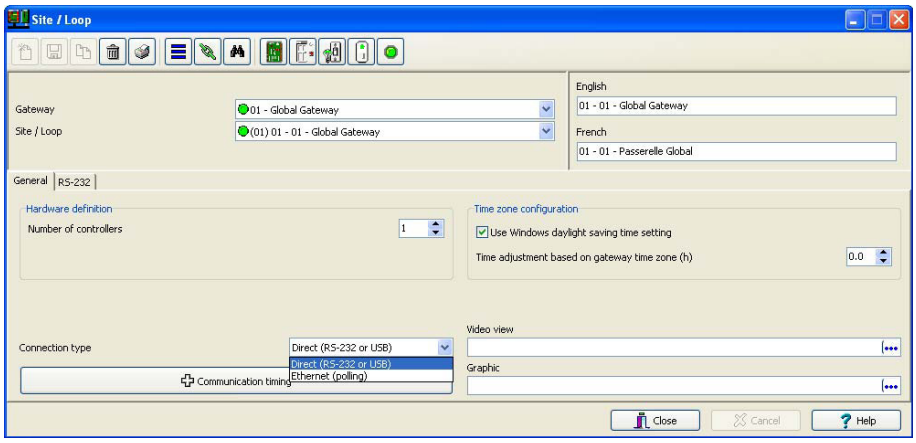
Сайт состоит из контроллеров, подключённых к одному и тому же последовательному порту. Данная система может поддерживать работу, максимум, 32 локальных сайтов на каждом шлюзе Corporate Gateway. Кроме того, EntraPass позволяет пользователям добавить до 512 удалённых сайтов со связью по коммутируемой линии на каждом шлюзе Corporate Gateway.

Сайты Corporate Gateway состоят из контроллеров KT-100, KT-200, KT-300 и KT-400.

В зависимости от выбранного типа соединения в окне EntraPass Site отображаются разные параметры. Например, если выбран тип соединения через порт RS-232, появляется закладка **RS-232** для настройки соответствующего последовательного порта и скорости передачи данных. Если используется тип соединения по коммутируемой линии, то в окне настройки сайтов появляются три дополнительных закладки для настройки конфигурации модема.

Всего предусмотрено пять типов соединения: прямое "Direct (RS-232 / USB)", безопасное "Secure IP (KT-400)", безопасное "Secure IP (Kantech IP Link)", опрос "Ethernet (polling)" и по коммутируемой линии через модем "Dial-Up (RS-232) modem".

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



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

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

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

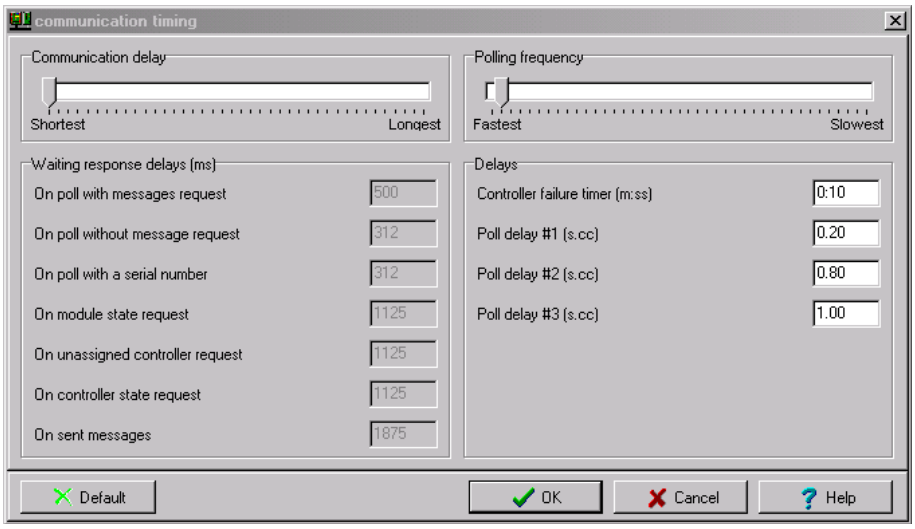
- В разделе **Hardware definition** (Описание оборудования) указать число контроллеров на сайте. На каждом сайте может быть подключено до 32 контроллеров. При вводе значения, превышающего максимально допустимую величину, система будет использовать число 32.
- В разделе **Daylight saving time options** (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 сайтом осуществляется по модему, необходимо указать разницу во времени между географическим местом расположения шлюза и сервера EntraPass в поле **Time adjustment based on Gateway timezone, h** (Установка времени по часовому поясу шлюза, часов). 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.
- В списке **Connection type** (Тип соединения) выбрать способ соединения между компьютером и шлюзом. От этого зависит, какие закладки отображаются в окне настройки.

Настройка таймаутов 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!

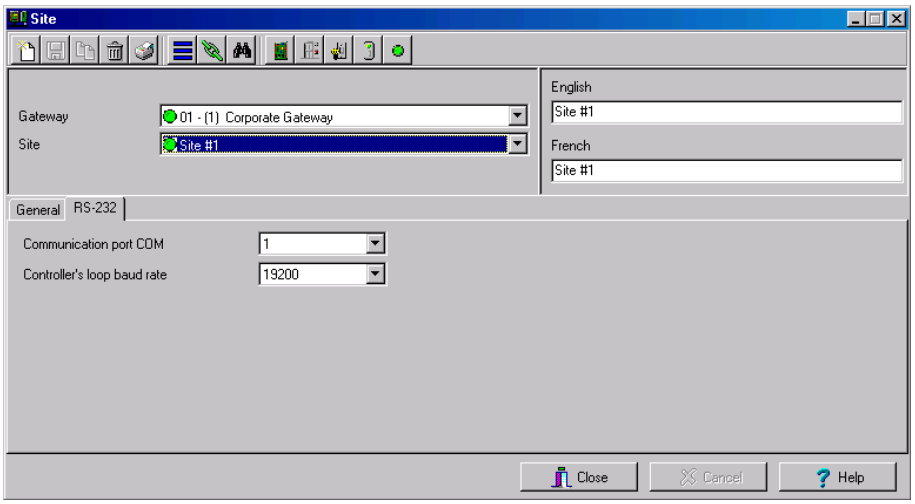
Окно Communication timing отображает значения параметров по умолчанию. Эти значения должны оставаться неизменными, если только иное не указано изготовителем (Kantech).



Настройка конфигурации соединения типа Direct RS-232 (прямое через RS-232)

Этот тип соединения используется в системах EntraPass версии Corporate Edition для соединения шлюзов Corporate через порт RS-232.

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 соединений типа Kantech IP Link или KT-400 Ethernet (только для шлюзов Corporate Gateway)

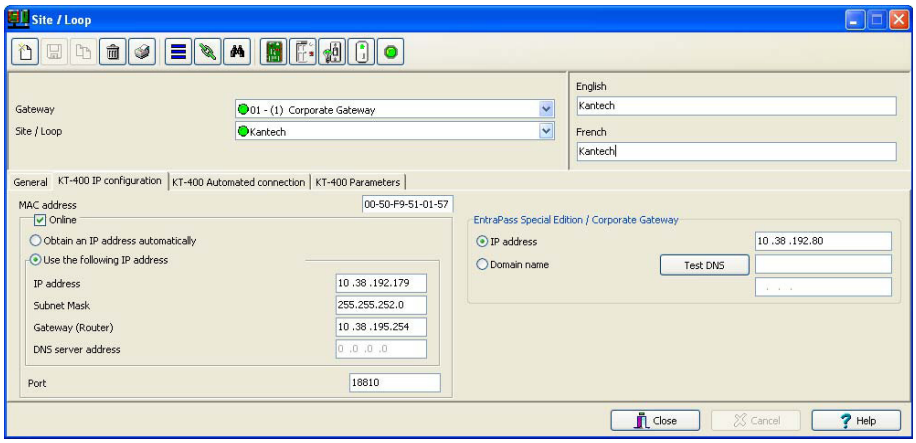
Этот тип соединения используется в системах EntraPass версии Corporate Edition для соединения через модуль Kantech IP Link или через 4-дверный Ethernet-контроллер KT-400.

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

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

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

1 Если в выпадающем списке **Connection type** под закладкой **General** указан тип соединения Secure IP (IP Link) или Secure IP (KT-400), то появляются три дополнительных закладки: IP Link или KT-400 IP Configuration (Конфигурация IP Link или KT-400 IP), IP Link или KT-400 Automated connection (Автоматическое соединение IP Link или KT-400), а также IP Link или KT-400 Parameters (Параметры IP Link или KT-400).

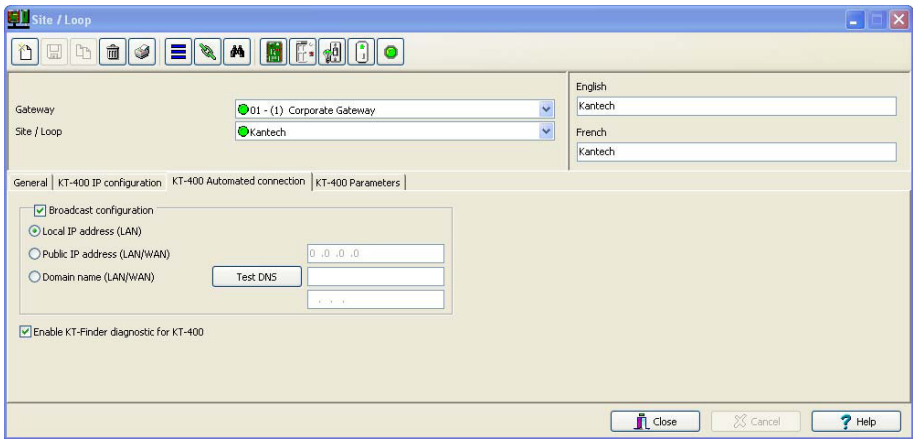


- **MAC Address** (MAC-адрес). В этом поле необходимо указать MAC-адрес устройства. Первые 6 знаков в поле MAC-адреса (00-50-F9) должны остаться неизменными.
- Поставить флажок в поле **Online** (Подключить).
- **Obtain IP address automatically** (Получить IP-адрес автоматически). Эту опцию следует использовать при настройке устройства с зарезервированным 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.
- По умолчанию для данного устройства автоматически назначается порт **18810.** Его не следует изменять, за исключением случаев, когда IP-устройство подключено удалённо, например, через WAN.
- В разделе **EntraPass Special Edition / Corporate Gateway IP address** указывают следующие параметры:
- **IP Address** (IP-адрес). Указать IP-адрес компьютера, на котором установлен шлюз.
- **Domain Name** (Имя домена). Если IP-адрес шлюза неизвестен, можно вместо него указать доменное имя, предоставленное системным администратором.

ПРИМЕЧАНИЕ. *Здесь следует указать либо IP-адрес, либо доменное имя. Вводить данные в оба поля не требуется.*

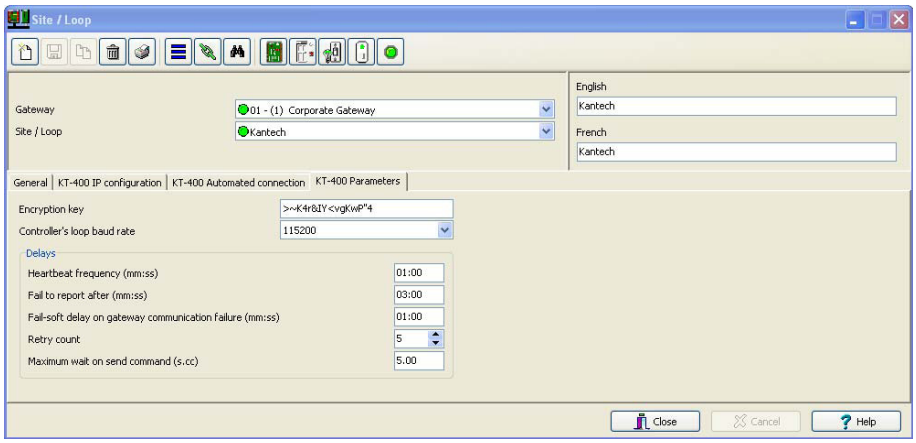
- **Test DNS** (Тест **DNS**). После ввода доменного имени следует нажать кнопку **Test DNS.** При этом в поле **IP address** должен отобразиться соответствующий IP-адрес.

2 Если используется подключение через WAN, следует перейти к закладке **KT-400** или **IP Link automated connection** (Автоматическое соединение KT-400 или IP Link).



- В поле **Broadcast configuration** (Конфигурация широковещательного запроса) обязательно должна стоять галочка!
- **Local IP Address** (Локальный IP-адрес), **LAN.** Автоматически назначается IP-адрес модуля Kantech IP Link.
- **Public IP Address** (Публичный IP-адрес), **WAN**. Этот IP-адрес предоставляется провайдером Интернет-услуг. Соответствует IP-адресу удалённого сайта.
- **Domain Name** (Доменное имя), **WAN.** Эта информация должна быть предоставлена системным администратором. Соответствует IP-адресу удалённого сайта.
- **Enable KT-Finder Wizard** (Сделать доступным мастер обнаружения устройств KT-Finder). При желании использовать KT-Finder в качестве инструмента для настройки и отладки, пользователь должен отметить флажком эту опцию.

3 Перейти к закладке **KT-400** или **IP Link Parameters** (Параметры KT-400 или IP Link) и настроить параметры безопасности и параметры связи.



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

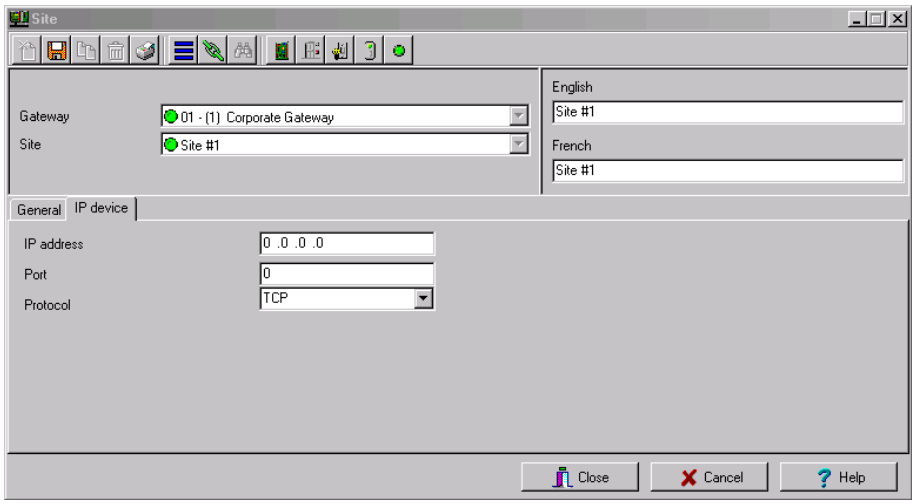
ПРИМЕЧАНИЕ. *Для контроллеров KT-200 максимальная скорость передачи данных составляет 19200.*

- В меню **Delay** (Задержки) необходимо выполнить следующие настройки:
- **Heartbeat frequency (mm:ss)** (Частота контрольных сообщений). В этом поле следует указать частоту, с которой модуль Kantech IP Link должен отправлять на шлюз сигнал для проверки связи (от 1:00 до 59:59).
- **Fail-soft delay on gateway communication failure, mm:ss** (Задержка включения безопасного режима при потере соединения со шлюзом, мин:сек). В этом поле следует указать время задержки, по окончании которого модуль Kantech IP Link будет считать, что связь с контроллером потеряна и контроллер работает в безопасном режиме.
- **Retry Count** (Число попыток). Число попыток (от 1 до 15) установить связь между модулем Kantech IP Link и контроллером с указанным выше интервалом задержки, по истечении которых связь будет считаться потерянной.
- **Maximum wait on send command** (Максимальное время ожидания команды). Если необходимо, указать максимальное время задержки, в течение которого шлюз ожидает подтверждение от модуля IP Link о получении команды с рабочей станции EntraPass.

Настройка конфигурации соединения типа Ethernet Polling (опрос)

Этот тип соединения можно использовать в системах EntraPass версии Corporate Edition для шлюзов Corporate Gateway при установлении связи со шлюзом по сети (Lantronix).

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 терминального сервера.

В поле **Protocol** необходимо выбрать протокол связи:

TCP, если сайт 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.

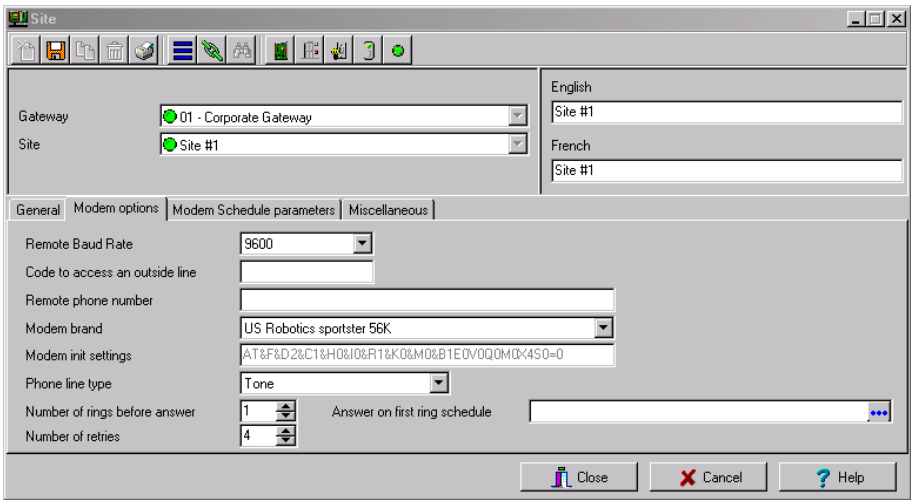
UDP (протокол пользовательских дейтаграмм), использует IP-протокол для отправки дейтаграмм из одного Internet-приложения в другое. Является протоколом "без установки соединения", так как не требует организации прямого соединения для обмена данными. Если настраиваемый сайт использует этот протокол, следует 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 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 сайтом) должен оставаться неизменным. При возникновении вопросов по поводу тех или иных настроек модема следует обращаться к системному администратору, обслуживающему данное оборудование.*

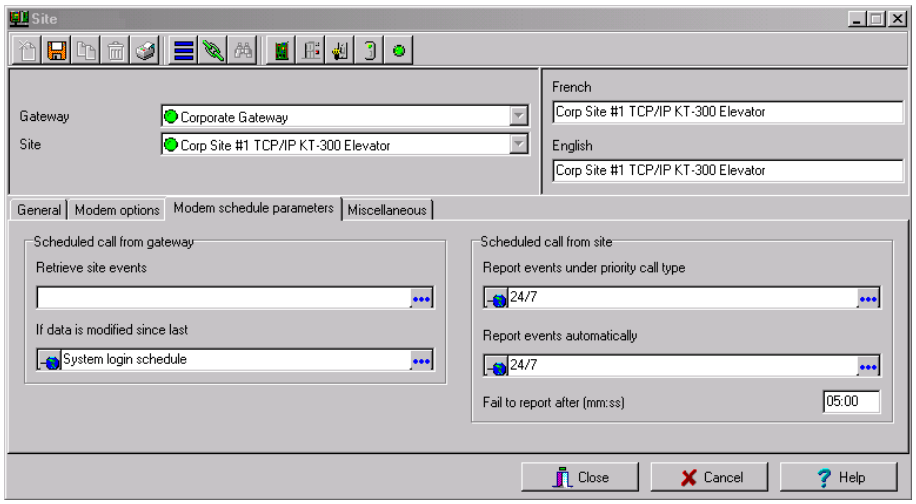
- В поле **Code to access an outside line** указать код для доступа к внешней линии (если используется).
- Введите телефонный номер удалённого сайта в поле **Remote phone number**.

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 (цифровой).
- В поле **Number of rings before answer** указать число звонков вызова, предшествующих ответу модема. Эта опция действует во всех случаях, когда расписания звонков не используются.
- Указать число попыток в поле **Number of retries**. Это число вызовов, которые предпринимает модем, прежде чем положить трубку.
- Настроить опцию **Answer on first ring schedule** (Расписание ответа на первый звонок), то есть временной интервал, в течение которого модему сайта разрешено отвечать на один звонок.

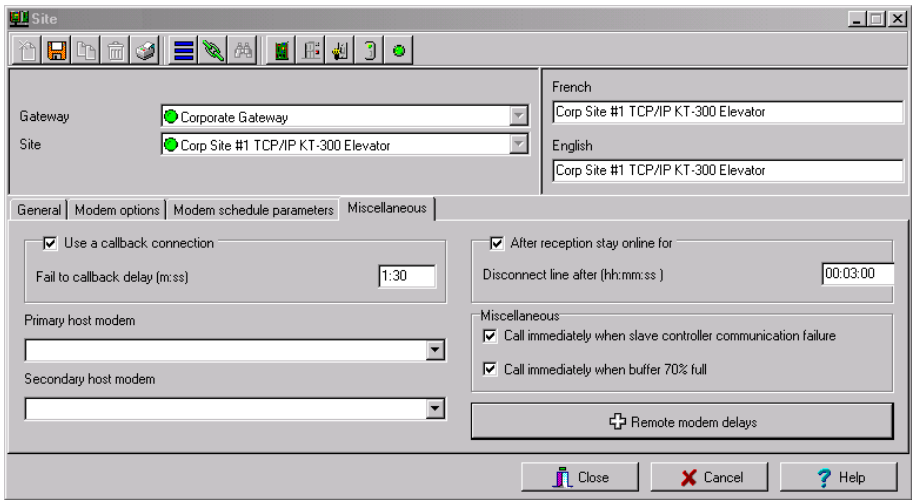
2 Перейти к закладке **Modem Schedule parameters** (Параметры расписания модема) для настройки временных интервалов подключения шлюза или сайта к удалённым сайтам или шлюзам (через модем) с целью выполнения определённых задач. Sheduled call from gateway – Вызов по расписанию со шлюза, Sheduled call from site – Вызов по расписанию с сайта.



- Нажать кнопку **Retrieve site events** (Извлечь события сайта), чтобы открыть окно выбора расписания. Выбрать расписание, наиболее соответствующее требованиям поставленной задачи. Более подробные сведения о задании расписаний изложены *в разделе "Описание расписаний" на стр. 194.*
- 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 откажется от попыток сделать сообщение.

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 обратное соединение), 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.).
- 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, входные зоны, реле и устройства вывода). Для описания контроллеров можно использовать меню настройки конфигурации шлюза или сайта, а также меню описания 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	Двери	Реле	Входные зоны	Дополнительные 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

4-дверный Ethernet-контроллер KT-400

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 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.

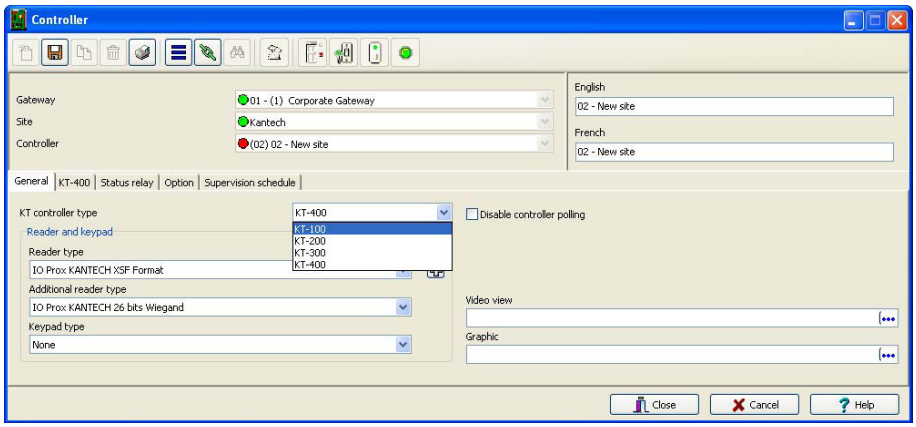
Особенности

- До 256 входов (16 входов на плате контроллера, с высокобезопасным решением для двусторонней линии с использованием резистора)
- До 256 выходов
- Четыре реле формы C на плате контроллера
- 16 выходов считывателя на плате контроллера
- 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, без необходимости использования внешних Ethernet-устройств
- Автоматическое обнаружение порта
- Для считывателей, замков и других устройств предусмотрен блок аварийного питания на аккумуляторах, что обеспечивает беспрерывную работу и сокращает время и материальные затраты на установку, так как отпадает необходимость использования внешнего источника питания.
- Может выступать в качестве главного IP-контроллера в сети RS-485

- Совместимость с контроллерами Kantech KT-100, KT-300 и (KT-200 на отдельной ветви)
- Отдельный противовзломный вход (Tamper Input)
- Питание внешнего запирающего устройства (опция)
- Четыре конфигурируемых выхода на каждый считыватель
- Встроенная конфигурация веб-страниц
- Несколько опций для выбора конфигурации (IP, RS-485 и RS-232)
- Низкая нагрузка на пропускную способность сети
- Визуальные индикаторы статуса (светодиоды)
- Более строгий контроль и наблюдение
- Локальный запрет повторного прохода через контролируемую территорию
- 100 000 идентификационных карт на каждый контроллер и 20 000 сохранённых событий при работе в автономном режиме
- Время активации при временных действиях и событиях

Описание общих параметров (General) для контроллеров Kantech

1. В меню **Devices** (Устройства) **>** **Controller** (Контроллер) выбрать шлюз, связанный с сайтом контроллера.
2. В выпадающем списке **Site** (Сайт) указать сайт, 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 только для контроллеров типа KT-100, KT-300 и KT-400.*

- 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).

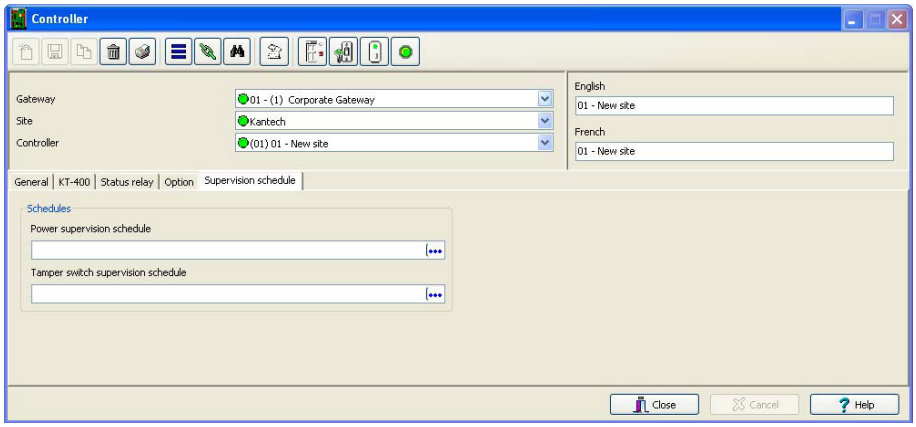
ПРИМЕЧАНИЕ. *Иконка* **New reader driver** *(Новый драйвер считывателя) позволяет пользователю установить свой драйвер для определённого контроллера. Помимо этого, данная кнопка служит для добавления драйвера в таблицу Reader+ Driver, из которой его можно будет использовать и в следующий раз при добавлении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



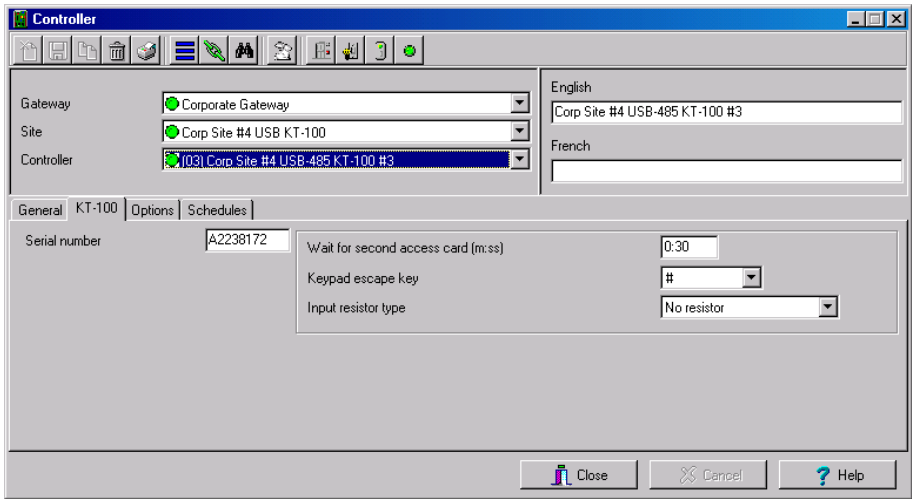
- Выбрать наиболее удобные расписания в разделе **Schedules** для нового контроллера:
- Для контроллеров KT-100 или KT-300 доступен только список **Power supervision schedule** (Расписание контроля подачи питания).
- Для контроллеров KT-200 или KT-400 доступно два списка **Power supervision schedule**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

6 Нажать кнопку **Save** (Сохранить).

Настройка конфигурации контроллера KT-100

После того как общие параметры настроены, появляется закладка **Controller type** 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 В 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 **Input resistor type** (Укажите тип резистора) выбрать, какой тип резистора используется в данной системе. По умолчанию установлено **Single resistor** (Один резистор). 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 приведены в разделе "Описание дополнительных функций контроллера" на стр. 122.*

Настройка конфигурации 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.*

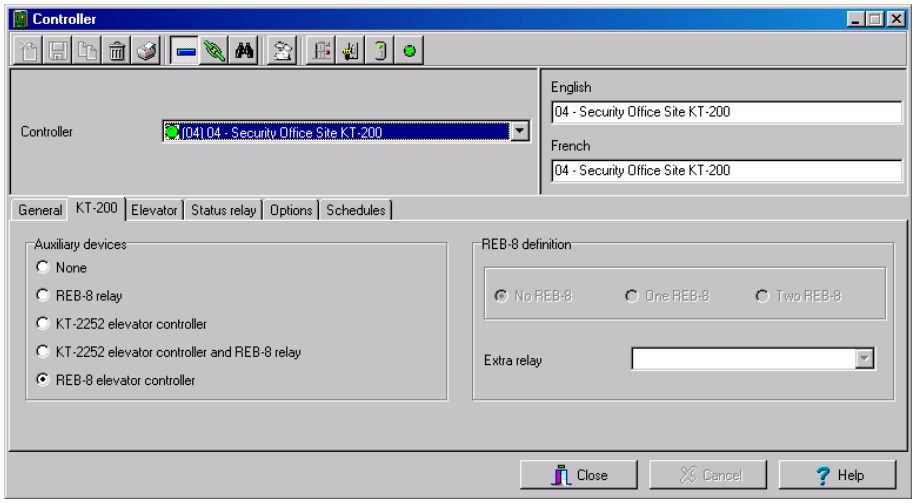
Описание модулей расширения контроллеров KT-200

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 открытие дверей на соответствующих этажах.

Описание дополнительных устройств для контроллера KT-200

1 В окне описания 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).

- Отметить флажком опцию **KT-2252 elevator controller and REB-8 relay** (Контроллер лифта KT-2252 и реле REB-8), если KT-2252 используются как контроллеры лифтов, а REB-8 как реле на одном и том же контроллере дверей. К этому контроллеру можно подсоединить не более четырёх устройств KT-2252.
- 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.

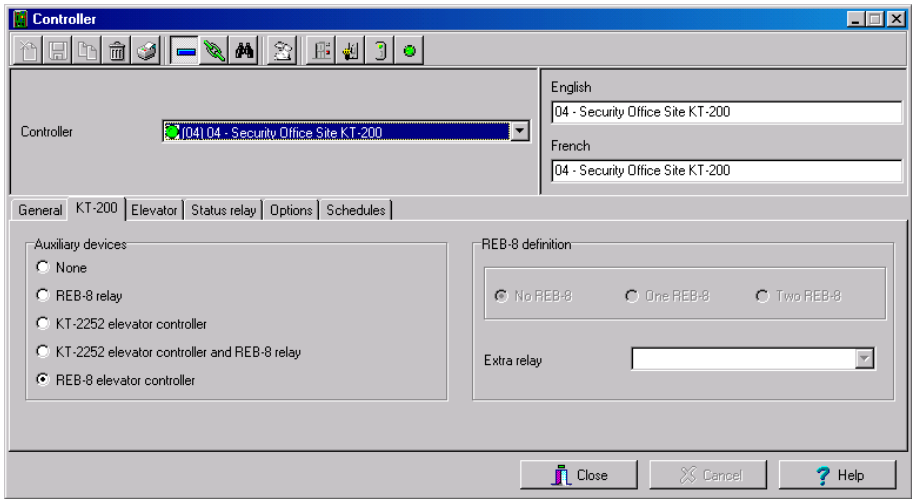
ПРИМЕЧАНИЕ. *Если в настройках отмечено использовать контроллер для управления лифтами, то за закладкой KT-200 появляется закладка Elevator (Лифт).*

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

Настройка контроллеров лифтов KT-2252

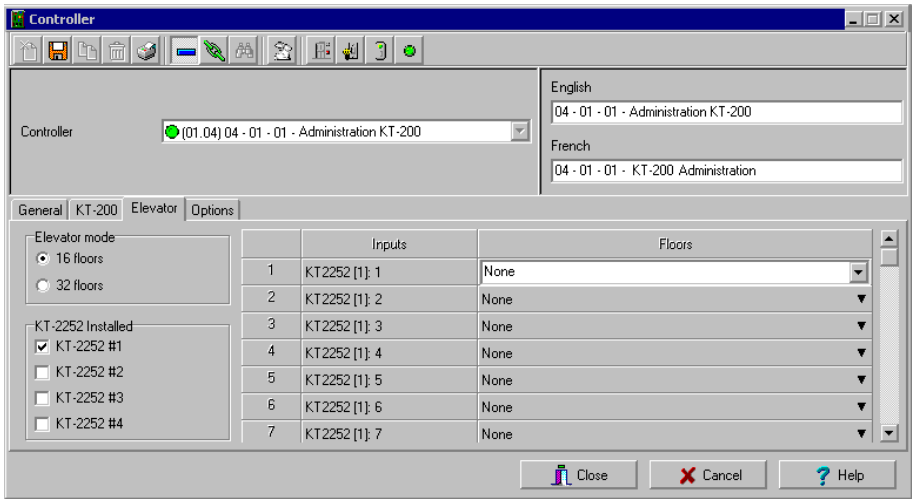
Закладка **Elevator** (Лифты) служит для настройки и описания дополнительных устройств, используемых с контроллером KT-200 для управления лифтами. В зависимости от установленной платы расширения и отмеченных флажком опций в окне Elevator отображается раздел **REB-8 Installed** или **KT-2252 Installed**.

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** (Лифты).

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

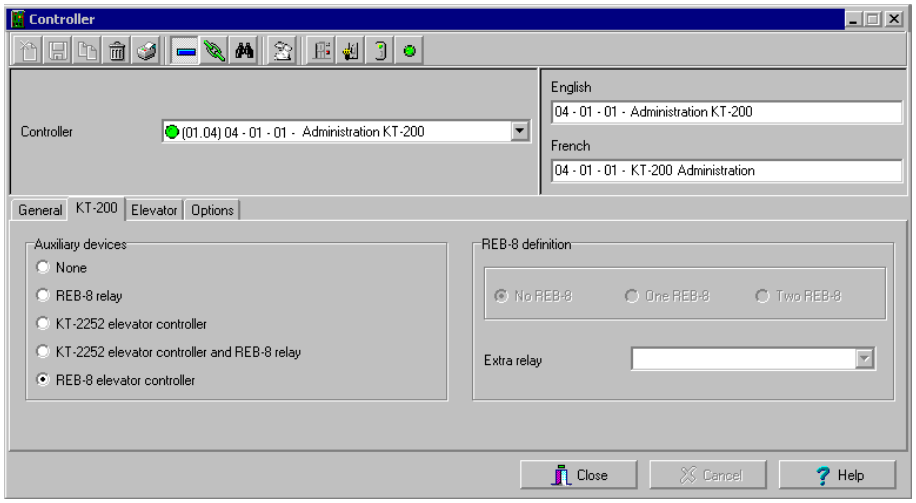
6 В колонке **Floors** (Этажи) указать число этажей, связанных с терминалами контроллера KT-2252.

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

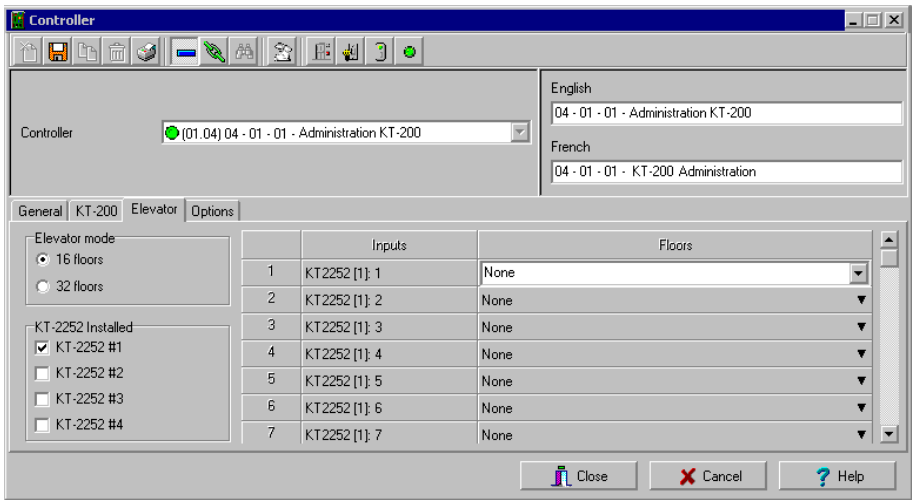
Настройка контроллеров лифтов REB-8

Релейные модули расширения REB-8 можно использовать в качестве бюджетного альтернативного механизма 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**, 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	от 1 до 8	Каб. 1
2	от 9 до 16	Каб. 1
3	от 1 до 8	Каб. 2
4	от 9 до 16	Каб. 2

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

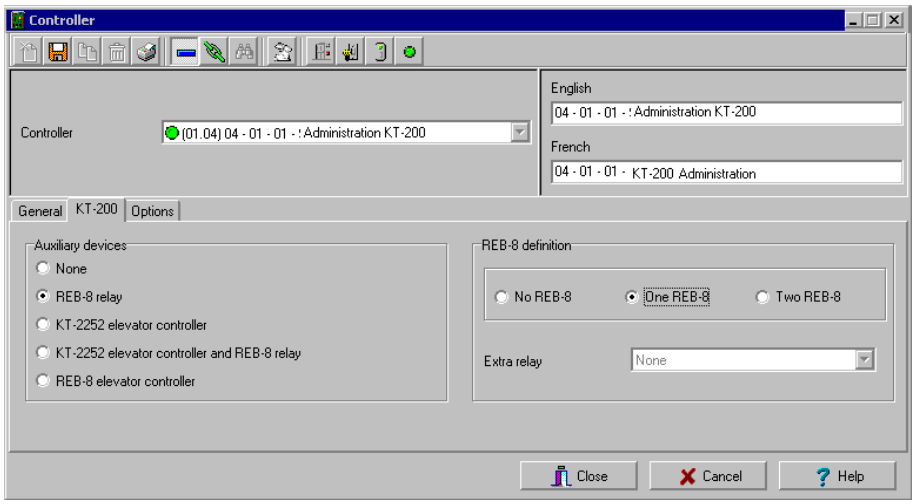
4 В колонке **Floors** (Этажи) указать число этажей, связанных с терминалами контроллера REB-8. Подробные сведения по описанию этажей и групп дверей смотрите *в разделе "Конфигурация дверей" на стр. 127*.

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

Описание 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 использовать 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 описания **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).

5 Открыть закладку **Status relay** (Реле статуса), 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

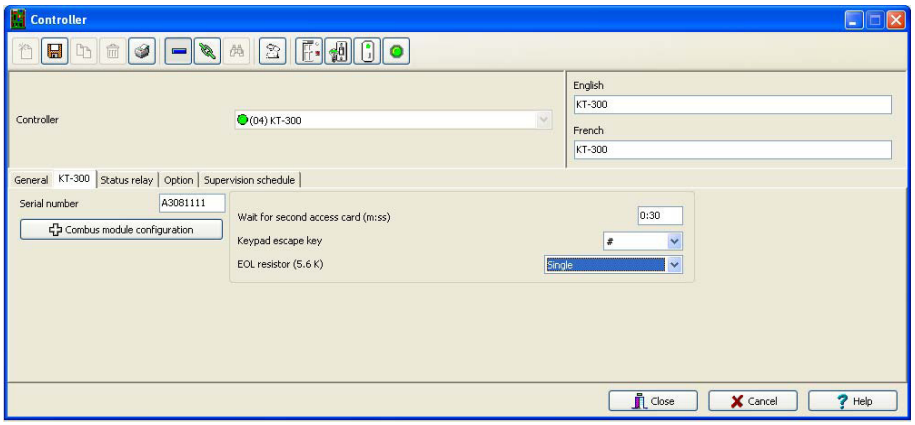
Slave controller communication failure – обрыв связи с ведомым контроллером

Настройка конфигурации контроллера KT-300

KT-300 постоянно отслеживает состояние аккумуляторного модуля питания и сообщает о низком заряде / отсутствии аккумуляторных элементов питания. 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** (Сайт) 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.

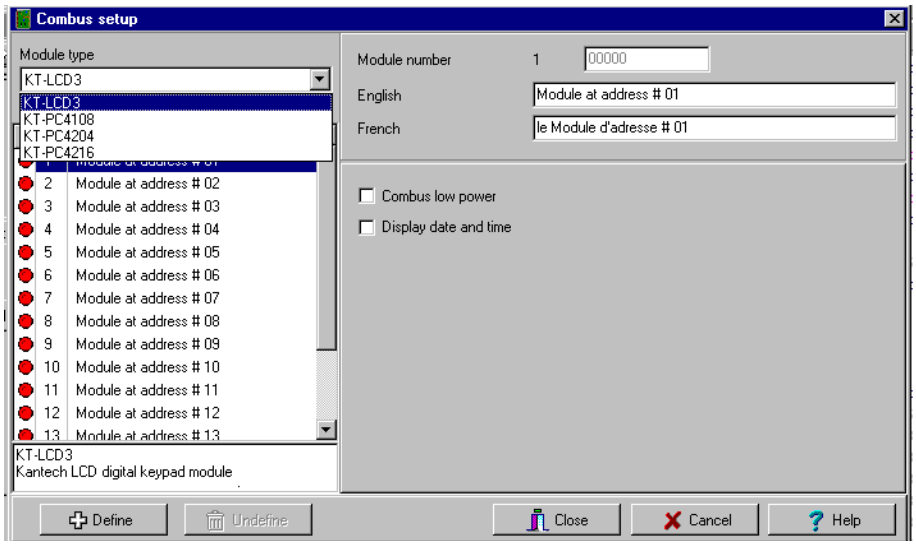
5 В выпадающем списке **Resistor type** (Тип резистора) выделить тип резистора. По умолчанию установлено **Single resistor** (Один резистор). В случае возникновения длинного звукового сигнала следует проверить число резисторов, установленных в системе.

Настройка конфигурации модулей Combus с контроллером KT-300

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

- KT-PC4108 (8-зонный входной модуль расширения). Имеет вход для подключения контакта противовзломной сигнализации (tamper contact).
- KT-PC4116 (16-зонный входной модуль расширения). Имеет вход для подключения контакта противовзломной сигнализации.
- KT-PC4204 (4-релейный модуль расширения с блоком питания). Имеет вход для подключения контакта противовзломной сигнализации, а также встроенный блок питания 12 В пост., 1 А для полевых устройств.
- KT-PC4216 (16-зонный выходной модуль расширения). Используется для управления лифтами (при необходимости, приобретается дополнительное оборудование).
- KT3-LCD (32-символьный ЖК-дисплей Kantech). Отображается *зелёным* (норма), *красным* (сбой в подаче питания) или *жёлтым* (неисправность).

1 Если на контроллер KT-300 установлен модуль 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** (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 противовзломное реле (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*** *(Энергосберегающий режим Combus) и* ***Display date and time*** *(Отображение даты и времени) контроллер KT-300 будет сообщать о включении энергосберегающего режима, а также отображать дату и время.*

Ниже в таблице представлены функции, доступные для каждого модуля:

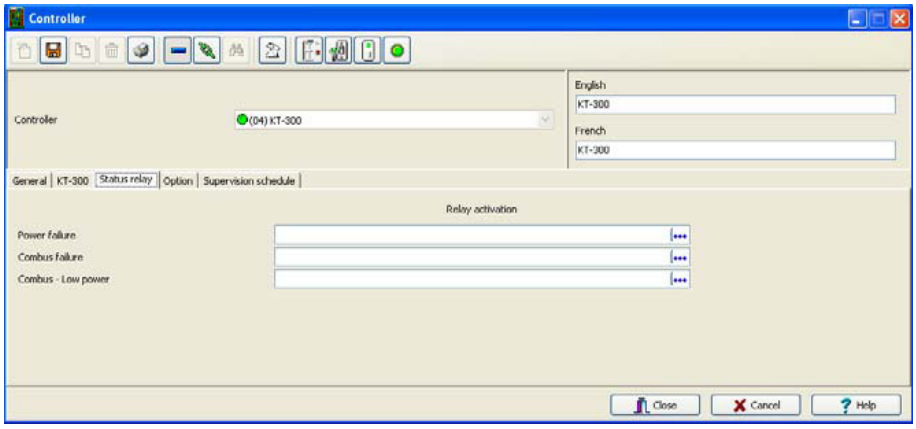
Тип модуля Combus	Функции	Дополнительные функции
KT3-LCD	Энергосберегающий режим Combus, отображение даты и времени	Нет дополнительных функций
KT-PC4108	Противовзломная сигнализация, энергосберегающий режим Combus	модуль на 8 входов
KT-PC4116	Противовзломная сигнализация, энергосберегающий режим Combus	модуль на 16 входов

Тип модуля Combus	Функции	Дополнительные функции
KT-PC4204	Противовзломная сигнализация, энергосберегающий режим Combus, разряженные аккумуляторы, сбой в подаче питания, пониженная дополнительная мощность	Используется как реле (1-4)
KT-PC4216	Противовзломная сигнализация, энергосберегающий режим Combus	Используется в качестве выходов

6 Отметить флажком опцию **Combus low power** (Энергосберегающий режим Combus), чтобы контроллер KT-300 сообщал о включении энергосберегающего режима.

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

8 После завершения настройки модуля Combus следует нажать **Ok** и вернуться в раздел KT-300 status relay (Реле статуса KT-300).



9 В разделе **Local activation relay** (Реле локализованной активации) выбрать реле, срабатывающие в ответ на сбой питания (**Power failure**), неисправность модуля Combus (**Combus failure**) и энергосберегающий режим Combus (**Combus low power**). Чтобы назначить определённое реле, следует нажать кнопку с многоточием и выбрать реле (одно или группу).

ПРИМЕЧАНИЕ. *Чтобы настроить реле локализованной активации, следует настроить реле в разделе (**Devices** > **Relays**), и затем выделить реле, предназначенные для локализованной активации.*

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

ПРИМЕЧАНИЕ. *Более подробная информация приведена в разделе "Настройка конфигурации сайтов" на стр. 91.*

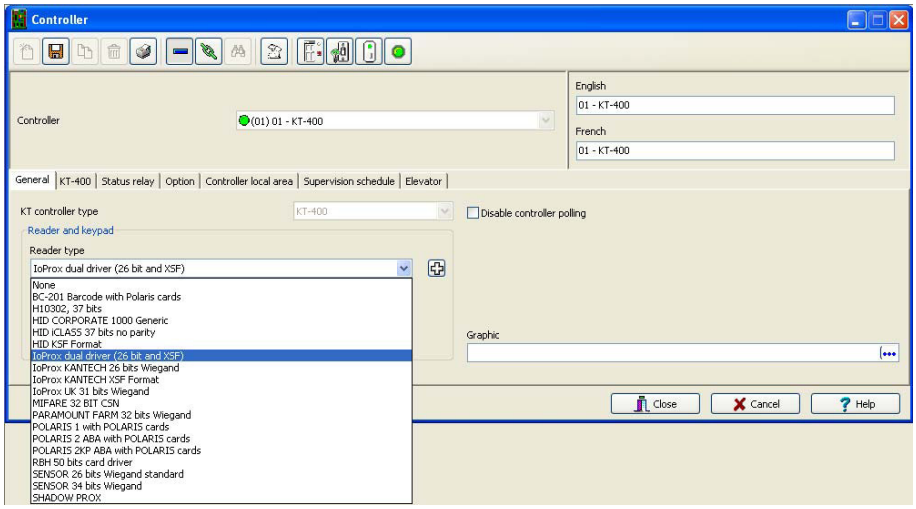
Настройка конфигурации 4-дверного Ethernet-контроллера KT-400

Контроллер KT-400 постоянно отслеживает статус сети питания переменного тока и состояние аккумуляторного модуля питания 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).

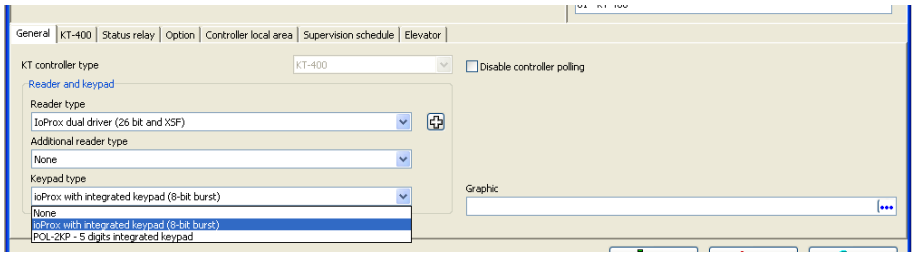
Выходы питания имеют электронную защиту от коротких замыканий и бросков напряжения. Цепи запирающих устройств также оснащены системой защиты от коротких замыканий и от разрыва цепи.

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

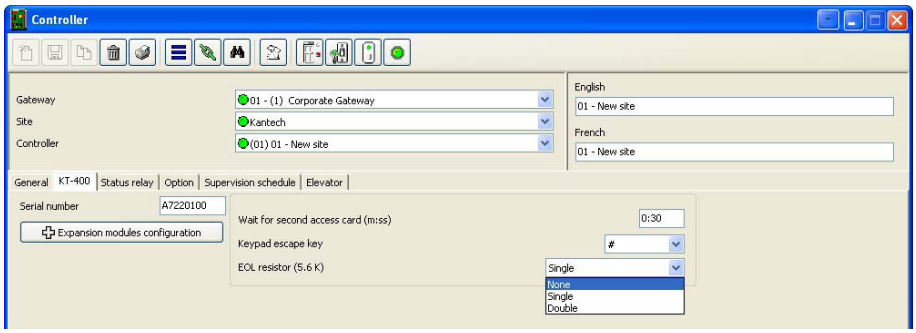
1 В меню **Devices** (Устройства) > **Controller** (Контроллер) открыть закладку **General** (Общие параметры) и выбрать тип считывателя в поле **Reader type(s)**.



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 конфигурации 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.

ВНИМАНИЕ! *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-M0D-INP16	Входы контроллера (до 256) и/или входы лифта (до 64 на одну дверь лифта)
KT-M0D-0UT16	Выходные реле (до 256) и/или выходы лифта (до 64 на одну дверь лифта)
KT-MOD-REL8 (***Прим.***)	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.*

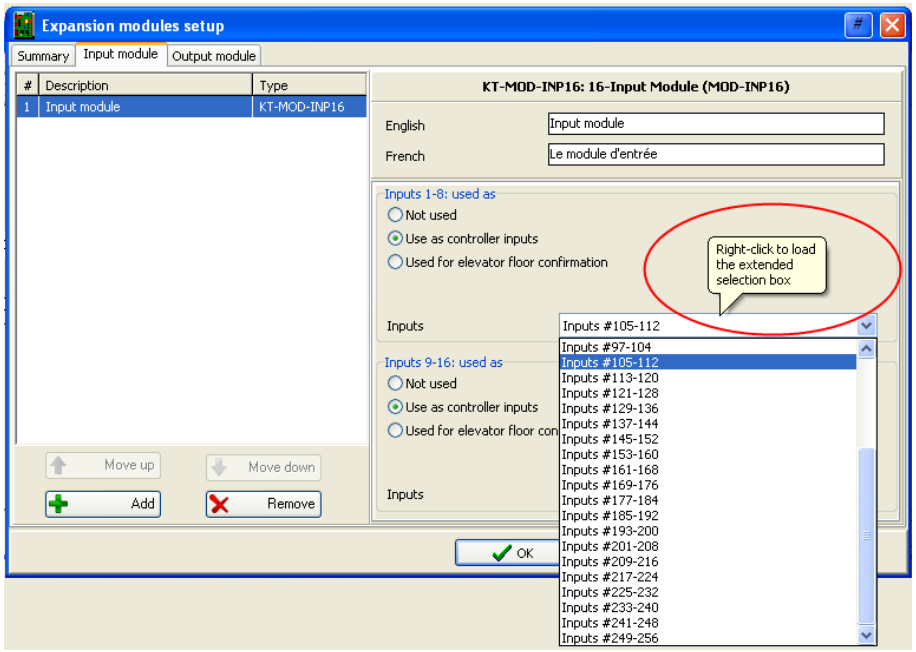
1 Если на контроллер KT-400 установлен(ы) модуль(и) расширения, следует нажать кнопку **Expansion module configuration** (Конфигурация модуля расширения). При этом открывается окно настройки модулей расширения **Expansion modules setup**.

Если необходимо:	**то следует перейти к:**
настроить входной модуль KT-MOD-INP16	п. 2.
настроить выходной модуль KT-MOD-OUT16	п. 4.
настроить выходной модуль KT-MOD-REL8	п. 5.
изменить конфигурацию уже установленного модуля расширения	п. 6.

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 перед внесением изменений необходимо тщательно проверить, какой из них будет использоваться в данном случае. Назначить имена модулей в соответствующих полях для каждого применяемого языка и выделить необходимые опции.

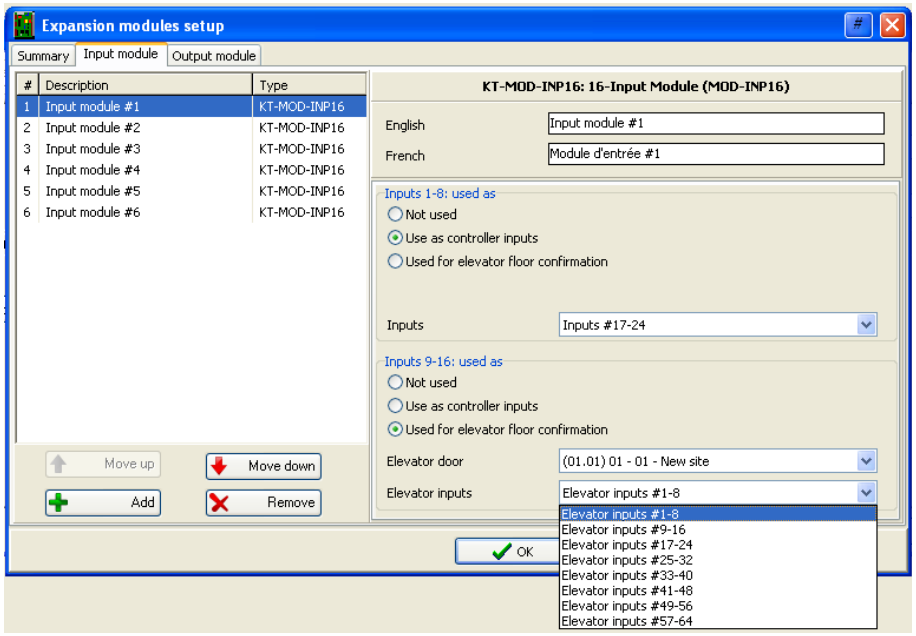
ПРИМЕЧАНИЕ. *Входы контроллера 1-16 зарезервированы для входов на KT-400.*

Пример назначения входов 1-8 в качестве входов контроллера (Controller Inputs)



3 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 изложена в разделе "Использование расширенного режима поиска" на стр. 52.

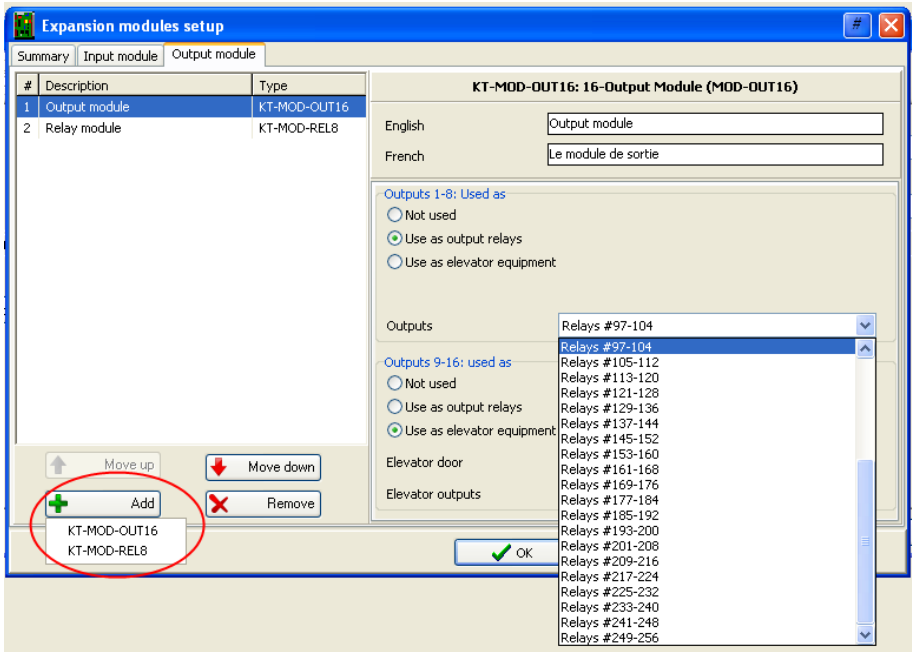
Пример назначения входов 9-16 в качестве входов лифта (Elevator Inputs)



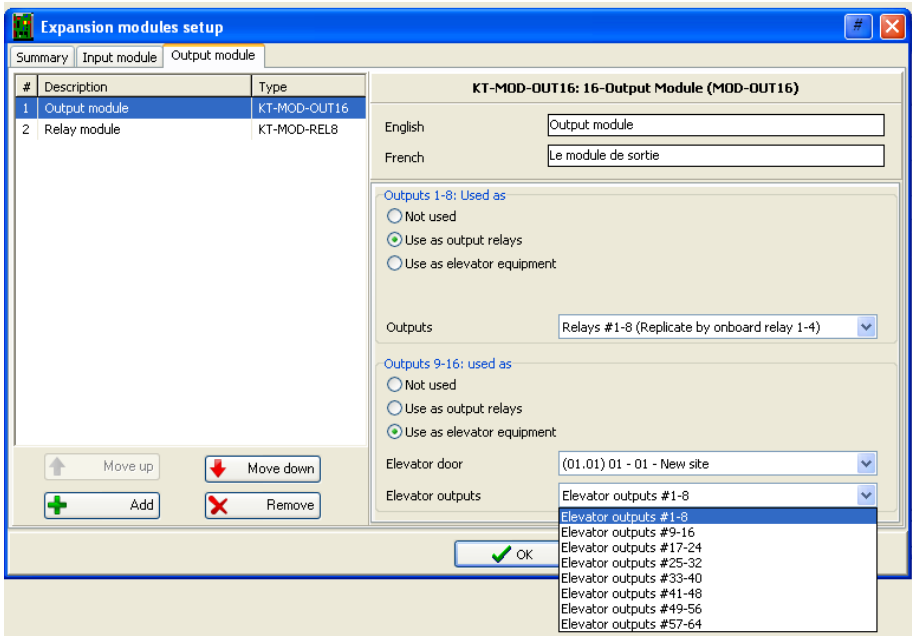
ПРИМЕЧАНИЕ. *Эти списки взаимоисключают друг друга. Нельзя выбрать один и тот же вход в меню* ***Inputs*** *и в меню* ***Elevator inputs****, так как получится дублирование, которое система не поддерживает. Например, входы 17-24 (****Inputs # 17-24****) нельзя выбрать дважды. С другой стороны, эта концепция 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).*

4 Чтобы добавить модуль KT-MOD-OUT16, 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 выходов 1-8 в качестве выходных реле (Output Relays)

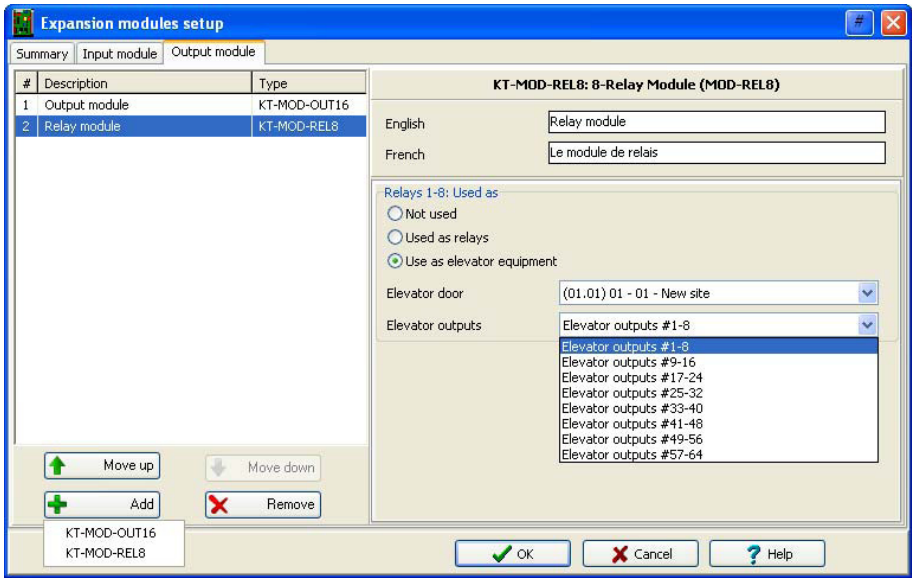


Пример назначения выходов 9-16 в качестве выходов лифтов (Elevator Outputs)

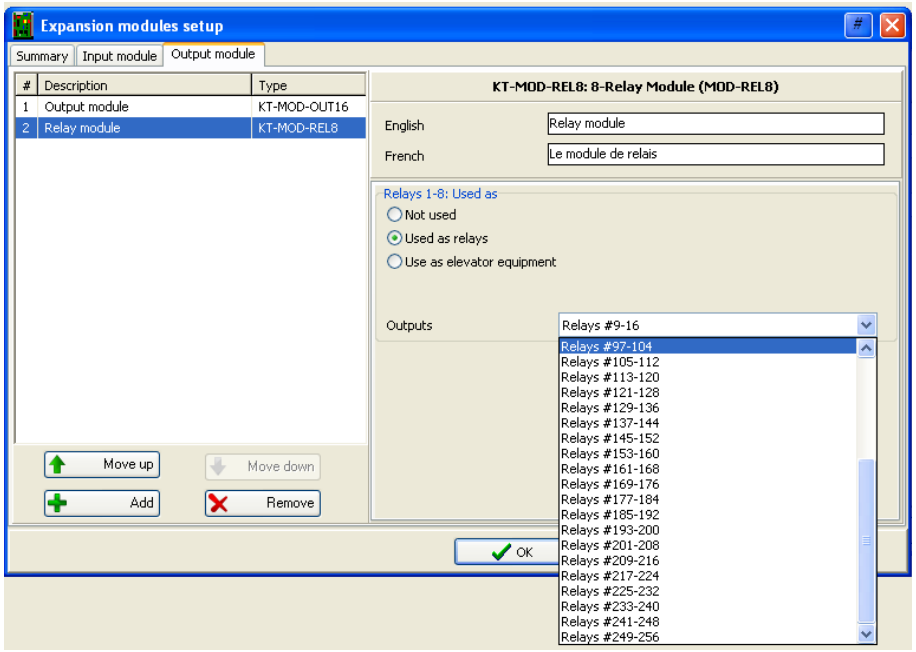


5 Чтобы добавить модуль KT-MOD-REL8, выбрать закладку **Output Module** (Выходной модуль) и нажать кнопку **Add** (Добавить). После этого на экране открывается новое меню, в котором можно выбрать, какой выходной модуль добавить. Назначить имена модулей в соответствующих полях для каждого применяемого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

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

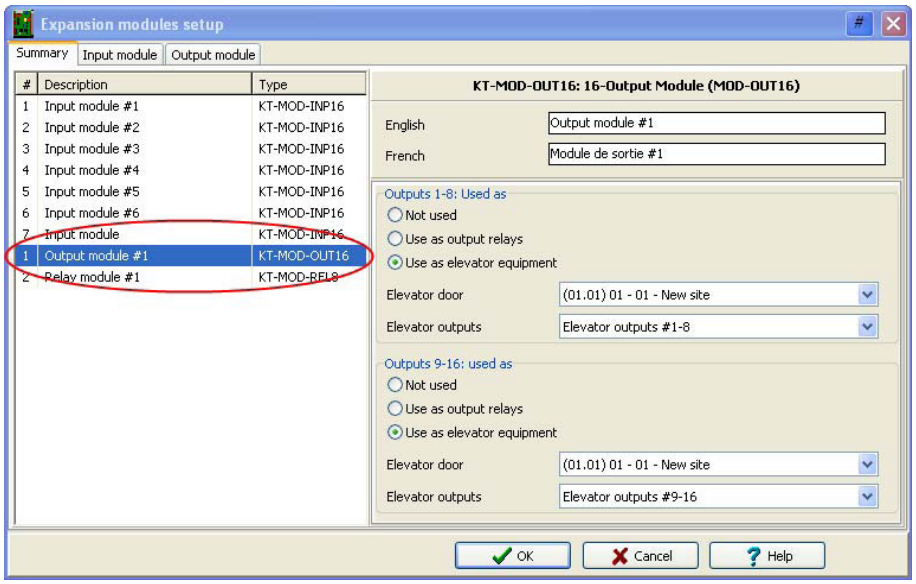


Пример назначения реле 1-8 в качестве реле (Relays)

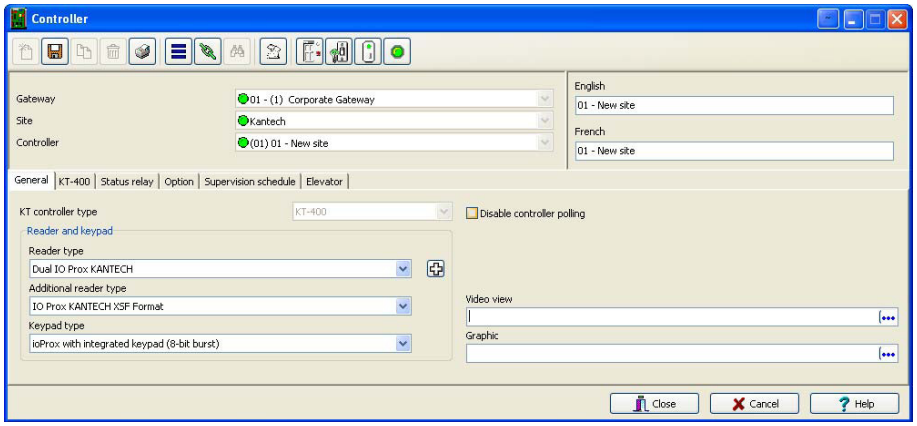


ВНИМАНИЕ! К настоящему моменту контроллеры KT-400 выпускаются с 4 реле. Рекомендуется заранее рассчитать, сколько реле потребуется, чтобы часть из них не оказались лишними (если только они не запланированы в качестве резервных). **6** Открыть закладку **Summary** (Сводка), которая позволяет изменять любые параметры. Выделить модуль, который необходимо изменить, в левой колонке и изменить его параметры в правой части окна.

Пример изменения уже установленного модуля расширения



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



ПРИМЕЧАНИЕ. *Более подробная информация приведена в разделе "Настройка конфигурации сайтов" на стр. 91.*

Выбор типа срабатывания реле статуса (только для шлюзов Corporate Gateway)

1 Открыть закладку **Status relay** (Реле статуса), чтобы запрограммировать реле (одно или группу) на срабатывание при возникновении определённого события.

Power failure – сбой питания

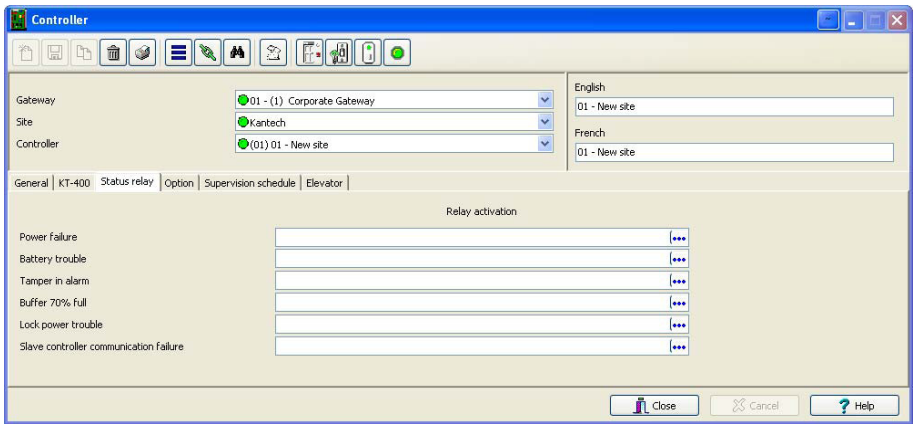
Battery trouble – разряжен аккумулятор

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



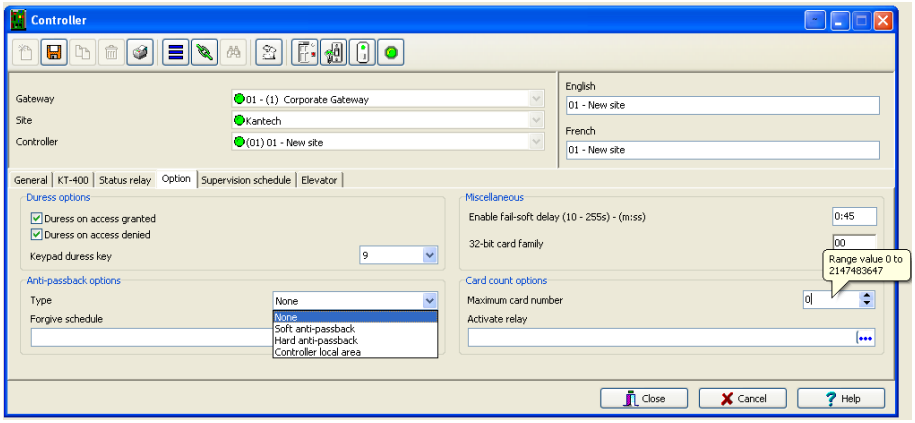
Описание дополнительных функций контроллера

Под закладкой **Option** (Опции) находятся следующие функции контроллера:

- Anti-passback – запрет повторного прохода (для синхронизации считывателей входа/выхода)
- Duress function – функция "принуждение" (для использования тревожной кнопки)
- Card count options – функции счётчиков 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 тревожной кнопки (тихая тревога).

- **Duress on access granted** (Принуждение, доступ разрешён) – разрешает использовать тревожную кнопку, если доступ разрешён.
- **Duress on access granted** (Принуждение, доступ запрещён) – разрешает использовать тревожную кнопку, даже если доступ запрещён.

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

ПРИМЕЧАНИЕ. *Для дополнительного повышения безопасности в этом меню можно выделить обе опции.*

Функция запрета повторного прохода доступна только для конфигурации Corporate Gateway.

4 Функция **Anti-passback options** (Запрет повторного прохода) доступна 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 (или выходе) более одного раза, не пользуясь соответствующим считывателем на выходе(входе). При этом на рабочий стол сообщений будет отправлено только 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.

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 перед включением безопасного режима, 10-255 сек, мин: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.

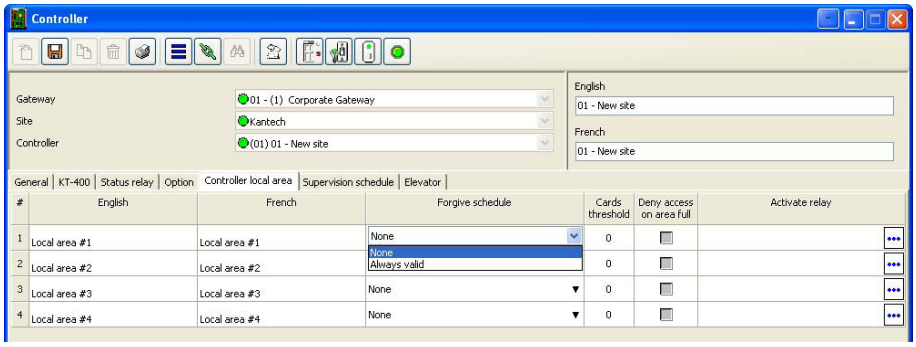
9 Систему можно настроить таким образом, что при достижении максимально допустимого числа карт будет срабатывать одно реле (**Activate a single relay**) или группа (**Group of relays**). Чтобы выбрать одно или группу реле, следует нажать кнопку с многоточием.

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).*

Описание локальных зон контроля для контроллера KT-400

ПРИМЕЧАНИЕ. *Функция* ***Controller local area*** *доступна только в конфигурации KT-400 на шлюзах Corporate Gateways и в системе EntraPass Special Edition.*

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 нужную опцию: None – не использовать, Always valid – достоверно всегда.

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.

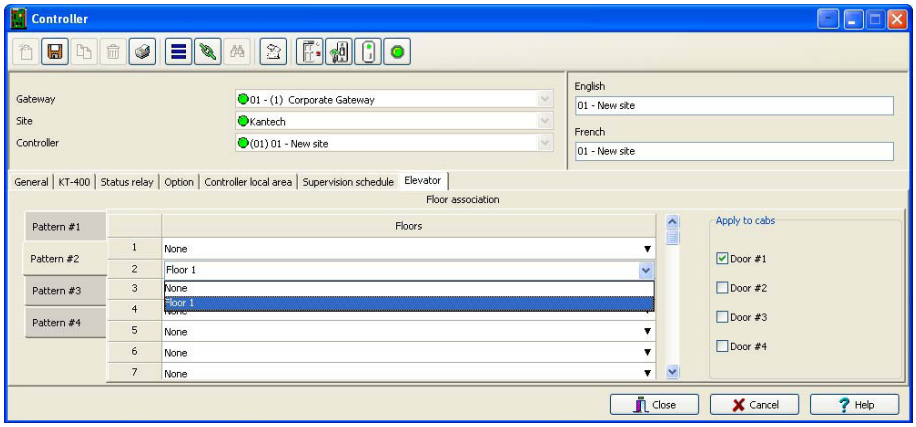
Описание связей с этажами лифта для контроллера KT-400

ПРИМЕЧАНИЕ. *Закладка **Elevator** (Лифт) отображается только в том случае, когда в закладке **KT-400** модули расширения настроены как входы или выходы для лифтов, смотрите раздел "Модули расширения к контроллеру KT-400" на стр. 115.*

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 описать привязки по этажам.



2 В закладке **Elevator** нажать **Pattern #2**, и выделить флажком необходимые номера дверей (**Door**).

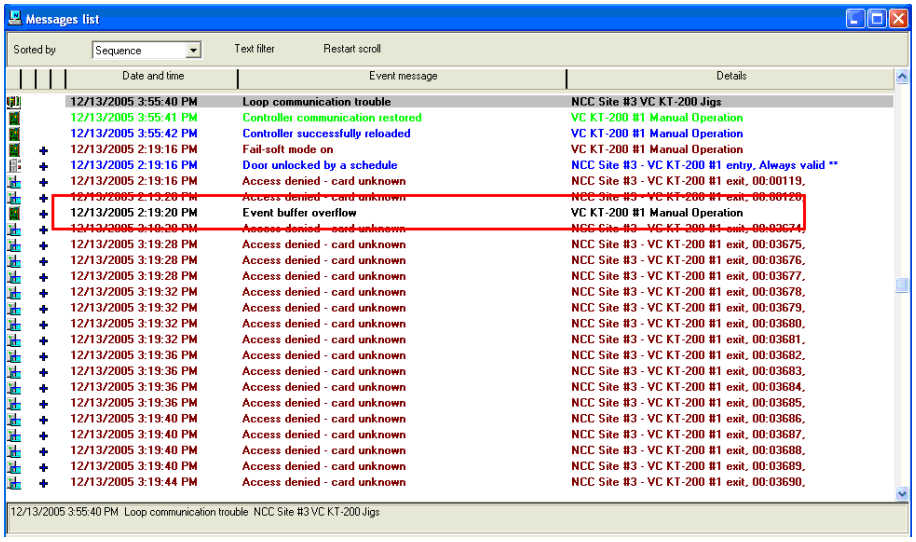
3 В выпадающем списке **Floors** (Этажи) выделить соответствующий пункт или номер этажа для привязки к номеру двери и номеру шаблона.

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 примере выделенное сообщение об ошибке “*Event buffer overflow*” является 50-м по счёту из самых старых событий контроллера, отправленных в список событий.

Конфигурация дверей (Door)

Это меню служит для описания 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. Функция двери зависит от настроек программного обеспечения.

Контролируемая дверь может быть всегда заперта или открыта в определённое время (по расписанию). Традиционными запирающими устройствами служат электронные защёлки и электромагнитные замки.

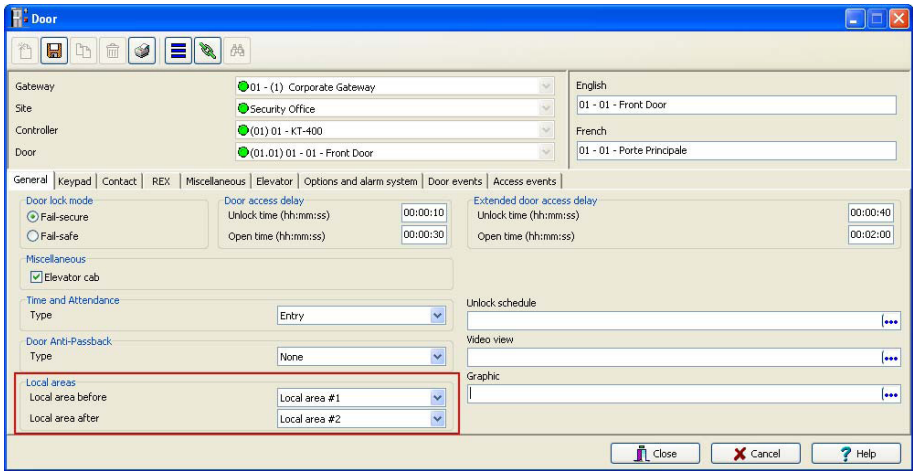
Любая дверь может быть оснащена одним или двумя считывателями карт, по одному устройству с каждой стороны. В дверях с двумя считывателями считыватель, установленный снаружи, считается "входным", а считыватель на выходе называется "выходным".

Описание общих параметров дверей (раздел Door)

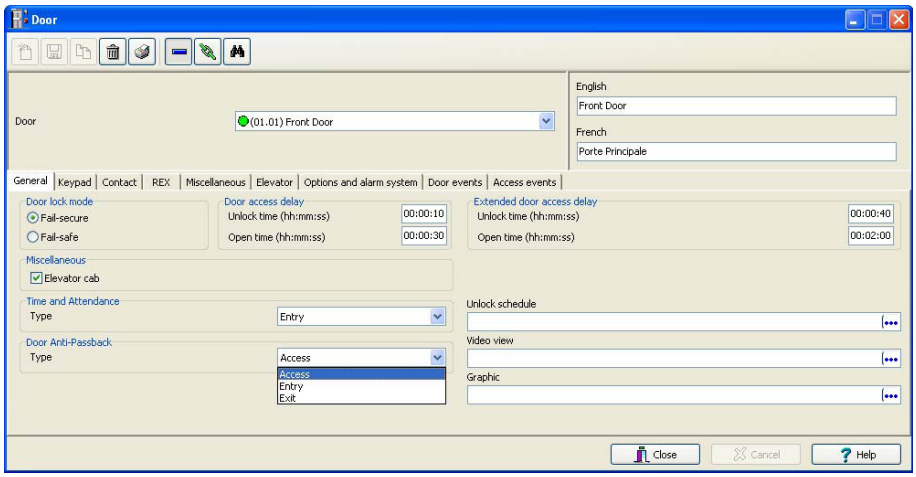
ПРИМЕЧАНИЕ. *При использовании системы с контроллерами типа KT-300 время указывается в формате ч:мм:сс и диапазон может быть настроен от 00:00:01 до 9:06:07. При использовании системы KT-400 время указывается в формате чч:мм:сс, а диапазон может быть настроен от 00:00:01 до 04:15 (255 сек) для KT-100, 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).

Так выглядит окно настройки только **для контроллеров типа KT-400 с выделенной функцией Controller Local Area** (Локальные зоны контроля).



Так выглядит окно настройки для контроллеров **KT-400 без использования функции Controller Local Areas**:



2 В окне **Door** выделить шлюз (**Gateway**) для просмотра сайтов контроллера, прикреплённых к определённому шлюзу, затем выделить сайт (из выпадающего списка сайтов **Site**) 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 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.

6 В поле **Time and Attendance type** указать тип учёта рабочего времени:

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 (если эта дверь оснащена контактным датчиком открытия).

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).

Если опция "Controller Local Areas"	**то** следует перейти к:
не выделена	**п. 7**.
выделена	**п. 9**.

7 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).
- **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).

8 Перейти к **п. 11.**

***ПРИМЕЧАНИЕ. Опции None**, **Soft anti-passback** и **Hard anti-passback** доступны только для контроллеров **KT-400** с выделенной функцией **Controller Local Area** (Локальные зоны контроля).*

9 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 она 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).

10 Описать зоны **Local area before** (Предыдущая локальная зона) и **Local area after** (Следующая локальная зона). Эти пункты меню доступны только в случае использования функции **Controller Local Area** (Локальные зоны контроля).

11 Указать дополнительную задержку доступа к двери **Extended door access delay**:

- **Unlock time (hh:mm:ss)** – длительность разблокировки (чч:мм:сс). Это время, в течение которого дверь остаётся незапертой после удачного считывания действительной карты или удачного 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 приведена в разделе *"Описание входа для двери лифта" на стр. 146.*
- **Open time (hh:mm:ss)** – длительность открытия (чч:мм:сс). Это время, в течение которого дверь может оставаться открытой после удачного 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.

12 Опция **Extended door access delay (hh:mm:ss)** – увеличенное время доступа, чч:мм:сс – позволяет оставлять дверь открытой более длительное время без срабатывания тревоги для прохода людей с ограниченными возможностями. Для использования данной опции должны быть указаны интервалы для разблокировки и открытия двери (**Unlock time** и **Open time**). 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.

13 **Unlock Schedule** (Расписание разблокировки двери) позволяет отпирать дверь в определённое, заранее указанное время.

14 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. *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.*

Описание функций дверной кнопочной панели для контроллеров KT-100 и KT-300

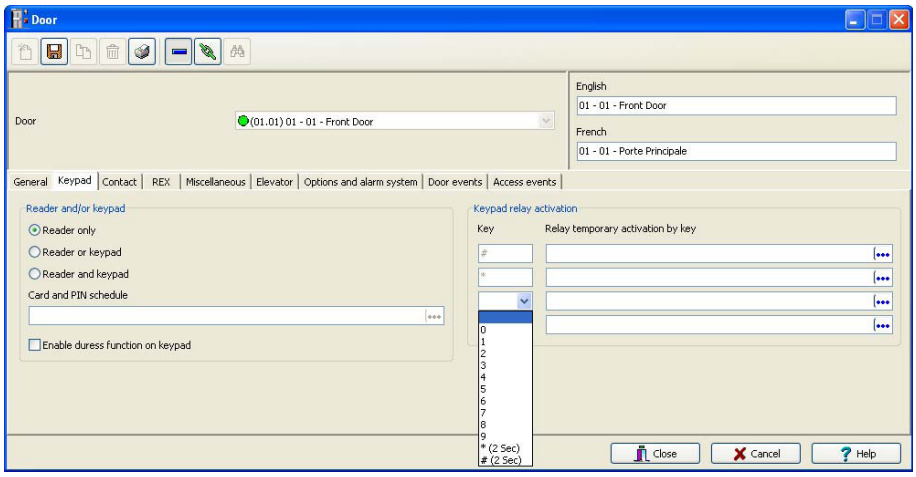
Предусмотрена возможность настройки срабатывания реле при нажатии клавиш * или # на кнопочной панели двери. Эта опция доступна только для контроллеров типа KT-100 (с прошивкой версии 1.04 и выше) и KT-300 (с прошивкой версии 1.16 и выше).

Для контроллеров KT-400

Предусмотрена возможность настройки срабатывания одного или группы реле при нажатии определённой клавиши на кнопочной панели двери.

ПРИМЕЧАНИЕ. *Закладка **Keypad** (Клавиши) доступна только при условии настройки типа кнопочной панели в поле **Keypad type** (Тип кнопочной панели) при настройке связей контроллера с дверями, смотрите пункт "Указать тип кнопочной панели в поле Keypad type (при её наличии)." на стр. 114. 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** (Клавиши).



2 Указать способ управления дверью:

- **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 недостаточно безопасным 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” достоверно. 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 действительной 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.

5 Выбрать клавишу(и) активации реле (**Keypad relay activation**):

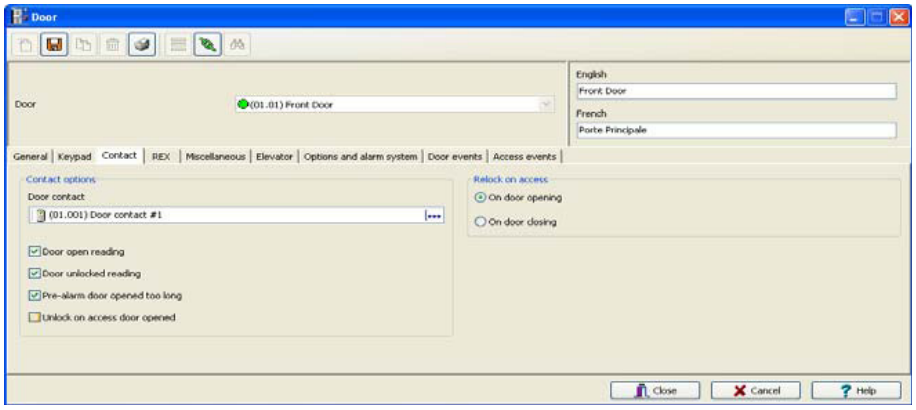
- **Для контроллеров KT-100 и KT-300**: в дверях, оснащённых кнопочной панелью или считывателем с кнопочной панелью, предусмотрена возможность настройки срабатывания реле при нажатии клавиш * или #. Если эта функция активна, пользователи могут активировать реле простым нажатием определённой клавиши.

- **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.

Описание функций контактных датчиков открытия двери

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 ("ловушка") и др.

1 В окне **Door** (Двери) открыть закладку **Contact** (Контактные датчики).



2 Выбрать контактный датчик двери из списка **Door contact.**

ПРИМЕЧАНИЕ. *В контроллерах KT-200 вход №1 (контактный датчик) и №2 (кнопка запроса на выход) оптимизирован для двери №1 контроллера , в то время как входы №9 (контактный датчик) и №10 (кнопка запроса на выход) оптимизированы для двери №2 того же контроллера. Вход, используемый для контактного датчика открытия 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 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). Или сообщения “Access granted - Door open” (Доступ разрешён – дверь открыта).
- **Door unlocked reading** (Считывание при незапертой двери) – позволяет считывать карты, если дверь отперта вручную оператором или по достоверному 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.
- **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.

- **Unlock on access door opened** (Отпирать во время доступа при открытой двери) – позволяет системе отпирать замок при обращении к открытой двери.

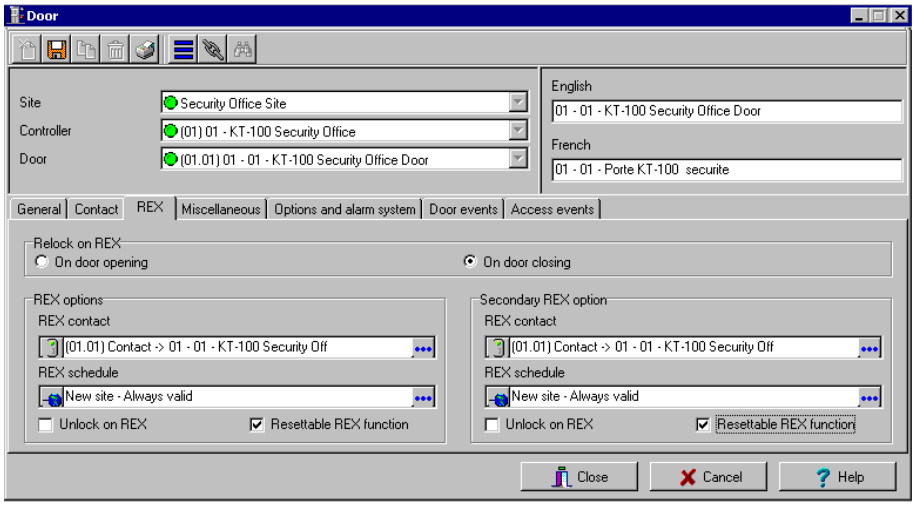
4 Выбрать соответствующую опцию "Запирать во время доступа" в поле **Relock on access**. Предусмотрена возможность запирания при открытии двери (**On door opening**) или при её закрытии (**On door closing**).

Описание функций 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 заблокировала замок после разрешения доступа
- **On door closing** (при закрытии двери) – чтобы система заблокировала замок после закрытия двери



2 В разделах **Rex options** и **Secondary Rex options** 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 сигналы запроса на выход, поступающие на соответствующий контакт. Эта опция действует только для дверей, оснащённых контактами REX.
- **Unlock on REX** (Отпирать 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 взломана).

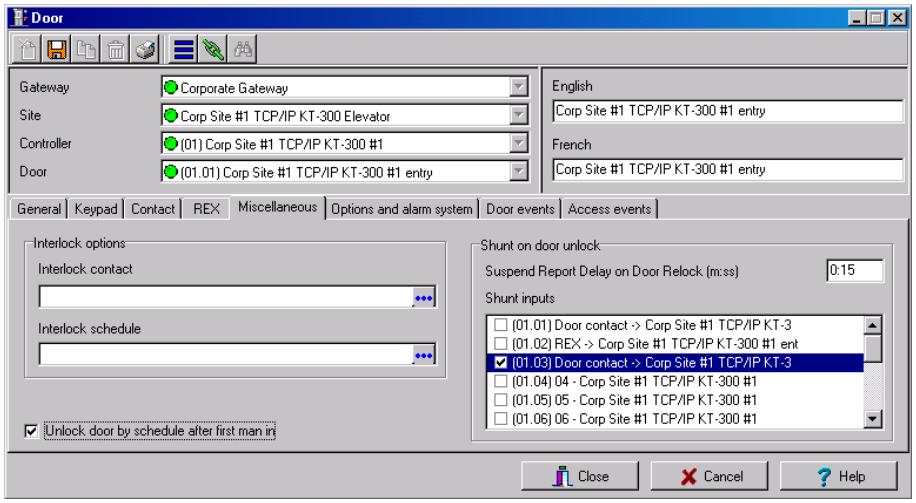
- **Resettable REX function** (Сбрасываемая функция "запрос на выход") – время разблокировки сбрасывается при успешном запросе на выход. Времена открытия и разблокировки двери указывают в меню описания двери (**Devices** > **Door** > **General**). Эта опция рекомендуется для дверей в проходах с интенсивным 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 взломана).

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 контактного датчика открытия двери.*

Описание функций взаимной блокировки дверей ("Ловушка")

Программа позволяет настроить параметры взаимной блокировки ("Ловушка") между двумя дверями для синхронизации времени открытия/закрытия этих дверей. Функция взаимной блокировки дверей называется также "ловушка". 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.

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.

3 В списке **Interlock contact** (Контакты блокировки) выбрать первый вход для системы взаимной блокировки. Выбранный вход должен быть *контактным датчиком открытия второй двери (Door contact)*.

4 Вернуться к выпадающему списку **Door** (Двери) и выбрать вторую дверь с функциями взаимной блокировки; затем указать контакт блокировки для этой двери. Им должен быть контактный датчик первой двери *(Door contact)*.

5 Выбрать расписание блокировки 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 ("ловушка") не поддерживаются контроллером типа KT-100.*

6 Отметить флажком, если необходимо, опцию **No lock by input when lock by alarm system armed** (Не запирать по входному сигналу, если дверь заперта постановкой на охрану с охранной панели).

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.

8 В поле **Suspend report delay on door relock, hh:mm:ss** (Задержка перед запиранием двери, чч:мм:сс) должно быть указано время, в течение которого мониторинг выбранных входов не будет выполняться, если дверь отперта. Возможность шунтирования (прекращения мониторинга) контактного датчика двери не предусмотрена, так как система будет шунтировать его автоматически.

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.**

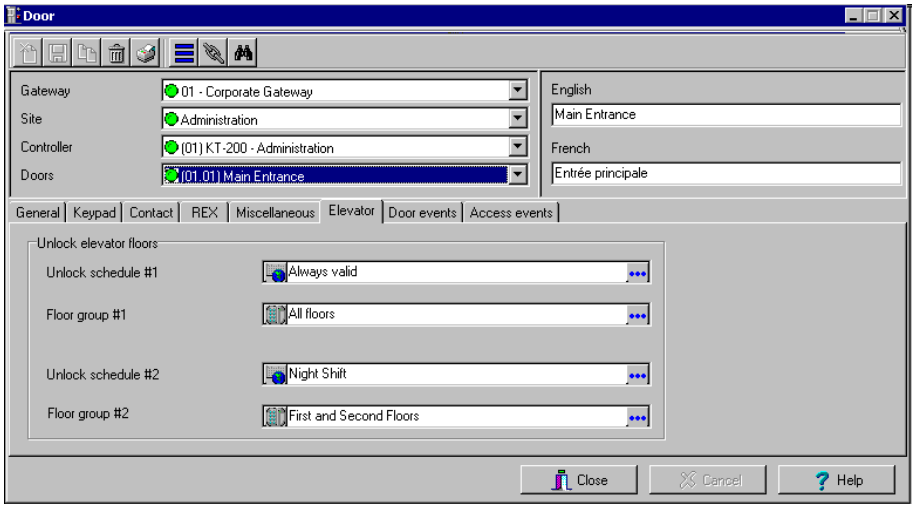
10 предоставлено пользователям.

ПРИМЕЧАНИЕ. *Меню Shunt input (Шунтируемые входы) отображается по-разному, в зависимости от того, какая система используется: KT-300 или KT-400.*

Описание 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, Schedules**).

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.

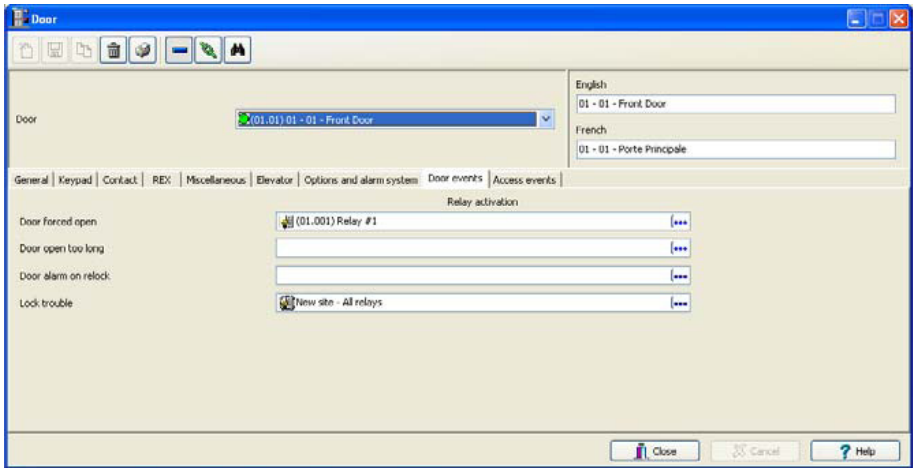
Важные примечания:

- Расписание разблокировки двери **Unlock schedule,** настраиваемое в меню описаний дверей **Door** (закладка **General**) будет БЛОКИРОВАТЬ 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 смотрите в разделе "Описание модулей расширения KT-200" на стр. 105.*

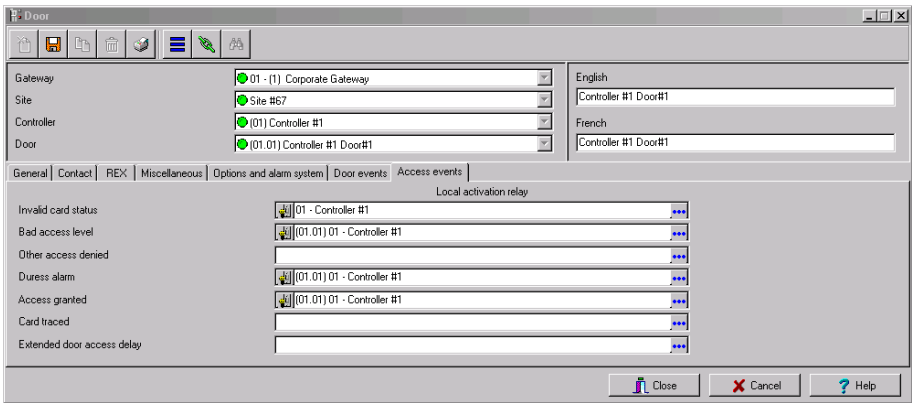
Настройка событий дверей (раздел Door Events)

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.



2 Указать реле, которые будут срабатывать локально при таких событиях, как **Door forced open** (Дверь взломана), **Door open too long** (Дверь слишком долго открыта), **Door alarm on relock** (Сигнализация двери при запирании) или **Lock Trouble** (Проблемы при запирании).

3 После окончания настройки всех событий открыть закладку **Access events** для настройки реле (или группы реле для KT-400), которые должны срабатывать при прочих событиях.



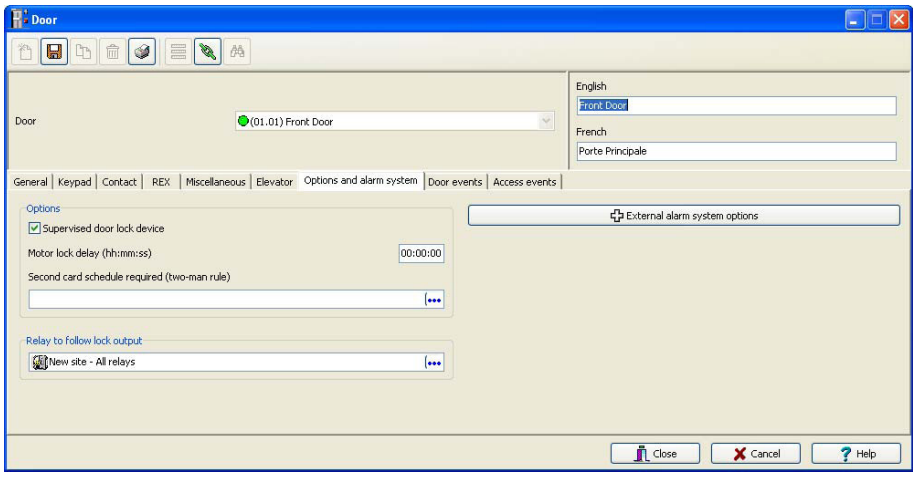
ПРИМЕЧАНИЕ. *Система EntraPass предоставляет возможность настроить реле, которое будет срабатывать при использовании функции* ***Extended delay*** *(Увеличенное время доступа). Для использования этой функции необходимо соответствующим образом запрограммировать карту пользователя. Функция* ***Extended door access delay*** *(Увеличенное время доступа) доступна только в контроллерах типа KT-100, KT-300 и KT-400.*

4 Указать реле (или группу реле для KT-400), которые будут локально срабатывать при возникновении следующих событий: **Invalid card status** (Статус недействительной карты), **Bad access level** (Неверный уровень доступа), **Other access denied** (Другой доступ запрещён), **Duress alarm** (Тревога "принуждение"), **Access granted** (Доступ разрешён) и **Card traced** (Карта отслежена).

Описание функций для KT-100, KT-300 и KT-400 (только для шлюзов Corporate Gateway)

Описанный ниже раздел отображается только в конфигурации контроллеров KT-100, KT-300 или KT-400 со шлюзами Corporate gateway.

1 Открыть закладку **Options and alarm system** (Опции и охранные панели).



- **Supervised door lock device** (Контролируемое 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) – 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, то если выход замка будет деактивирован 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 для второй карты из списка **Second card schedule required, two-man rule** (Расписание для второй карты, доступ по разрешению двух должностных лиц, действующих согласованно).
- **Relay to follow lock output** (Реле для отслеживания выхода замка) – доступно только для контроллеров KT-400. Отслеживает статус выхода замка.

ПРИМЕЧАНИЕ. *В конфигурации с использованием контроллеров KT-100, KT-300 или KT-400 и шлюзов Corporate Gateway система позволяет обеспечивать взаимосвязь с внешней охранной панелью.*

Настройка интерфейсов внешних охранных панелей

Описанный ниже раздел меню доступен только в конфигурации контроллеров KT-100, KT-300 или KT-400 со шлюзами Corporate gateway.

Контроллеры KT-100, KT-300 и KT-400 обеспечивают взаимосвязь с любой внешней охранной панелью.

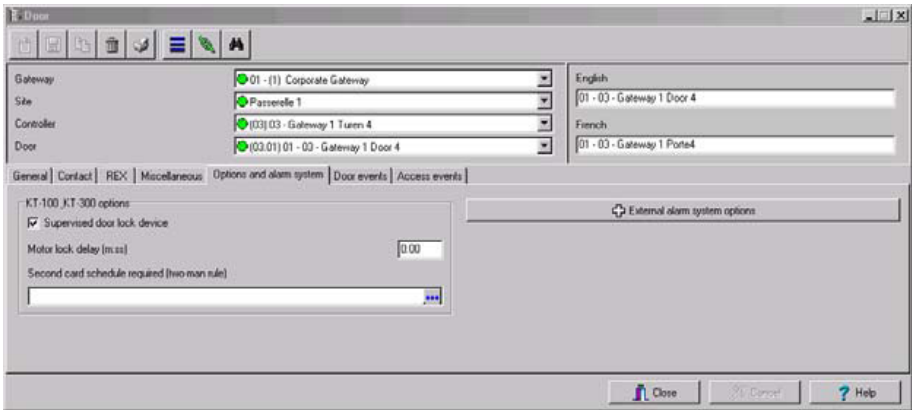
При добавлении этих контроллеров Kantech к действующей охранной системе владельцы карт получают возможность ставить (снимать) систему на охрану путем простого предъявления действительной идентификационной карты у входной/выходной двери. Применение кнопочной панели повышает защищённость системы, поскольку в этом случае помимо предъявления карты требуется ввести идентификационный код.

Существует пять способов постановки/снятия с охраны внешней охранной панели, включая отложенную постановку на охрану:

- По действительной карте, считываемой устройством постановки на охрану;
- По специальному коду, набранному на кнопочной панели;
- Нажатием клавиши на кнопочной панели;
- Нажатием клавиши, подключённой к определённому входу;
- По расписанию постановки/снятия с охраны (автоматически).

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** (Вход запроса). Этот вход становится активным при поступлении запроса о постановке на охрану внешней охранной панели.

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).

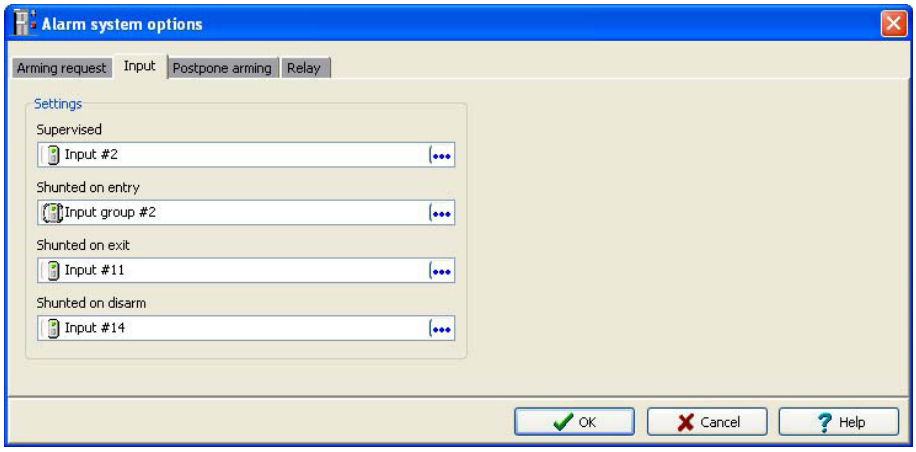
5 Чтобы повысить степень защищённости охранной панели, предусмотрены следующие опции:

- **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 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 статусу входа) – предотвращает постановку на охрану при тревожном статусе 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 система работает в обход охранной панели. **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.

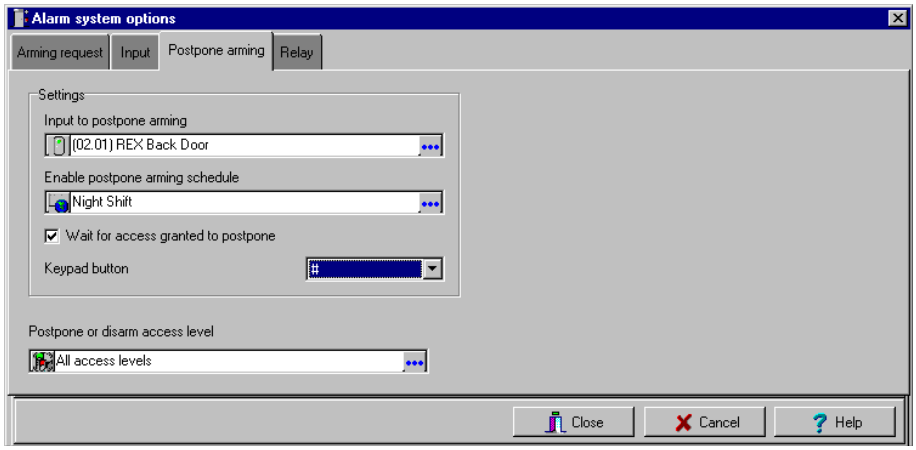
7 Указать вход, который будет использоваться для функции **External alarm system panel status**. Когда этот вход имеет статус "норма" (normal), охранная панель считается поставленной на охрану.

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.



- 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 **Postpone arming** (Отложенная постановка на охрану) выбрать вход для отложенной постановки на охрану в поле **Input to postpone arming**.

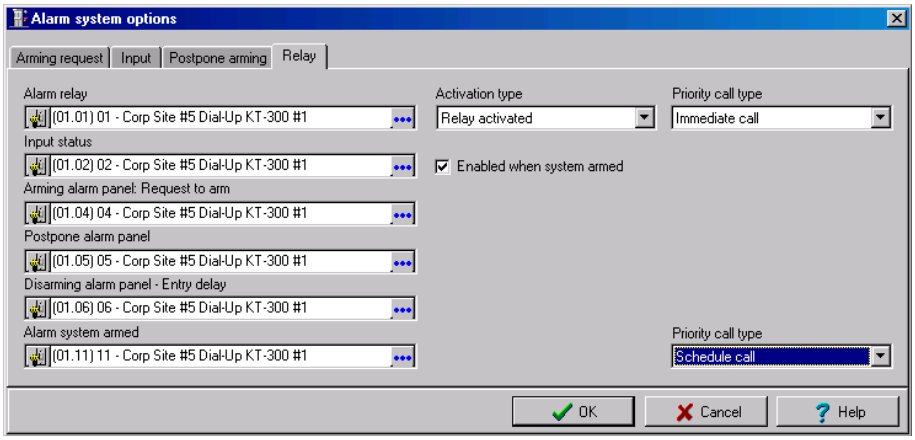


10 Указать расписание в поле **Enable postpone arming schedule.**

11 При необходимости поставить флажок в поле **Wait for access granted to postpone** (Ожидать разрешения 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 постановки/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 статус входа для реле внешней сигнализации.



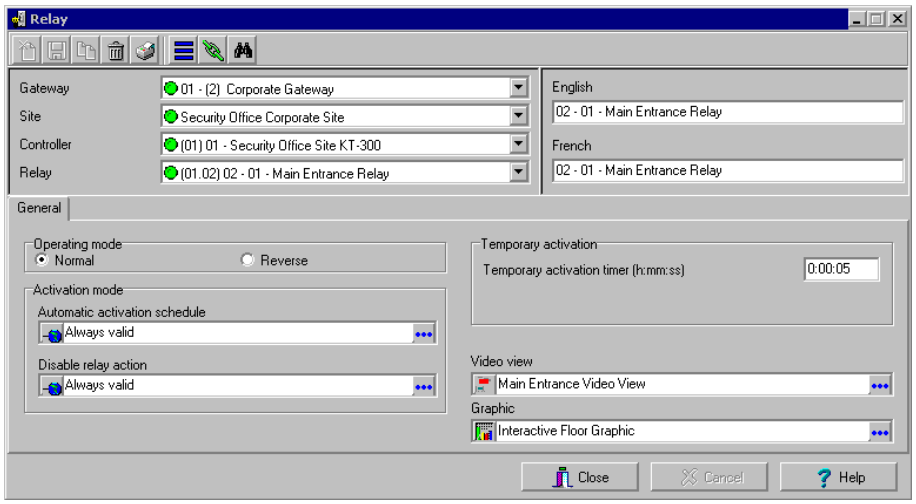
ПРИМЕЧАНИЕ. *После выбора тревожных реле в поле* ***Alarm relay*** *появляется доступ к полю* ***Activation type,*** *где можно указать тип активации реле. Они могут быть активированы постоянно или временно.*

Конфигурация реле (раздел Relay)

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.

Описание реле

1 Открыть закладку **Devices** (Устройства) и нажать иконку **Relay** (Реле).



2 Указать в поле **Gateway** шлюз, в поле **Site** сайт 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 (находится не под напряжением) и замыкается (срабатывает) по команде оператора, при возникновении события или по расписанию системы.
- **Reverse** (Обратный) – реле нормально замкнуто (находится под напряжением) 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.

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 Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплено реле.

Конфигурация входов (раздел Input)

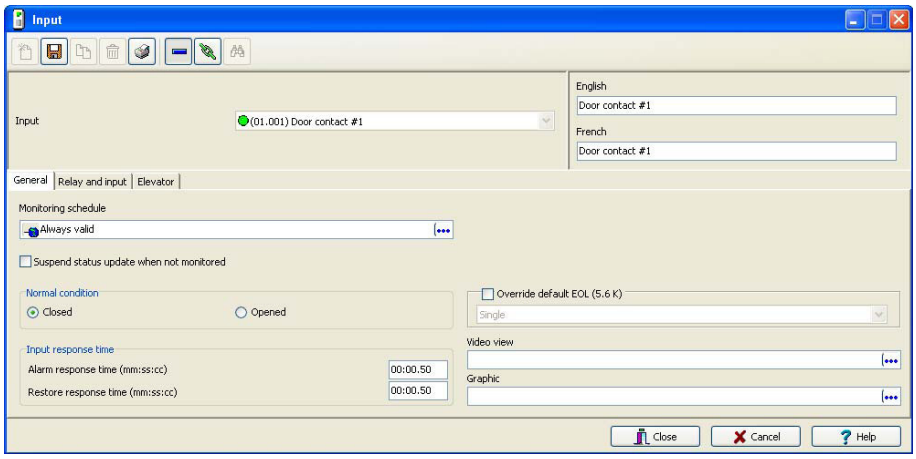
Контроллеры дверей контролируют статусы точек входа, в том числе контактные датчики открытия дверей, устройства взаимной блокировки, детекторы движения, датчики температуры, сигнальные устройства, разные устройства запроса на выход (REX), а также другие реле с сухими контактами. Число контролируемых устройств зависит от типа контроллера: 4 точки входа у KT-100, 16 у KT-200, 8 встроенных точек входа (а всего 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** (контактный датчик) и **№2** (устройство запроса на выход) оптимизирован для двери №1 контроллера, в то время как входы №9 (контактный датчик) и №10 (устройство запроса на выход) оптимизированы для двери №2 того же контроллера. Вход, используемый для контактного датчика открытия или для кнопки запроса на выход (REX), НЕ ДОЛЖЕН иметь расписание "мониторинга" в меню "Описание входов".
- **Для контроллеров KT-100.** Вход №1 предназначен для контактного датчика двери, а вход №2 для устройства запроса на выход.
- **Для контроллеров KT-300.** Вход №1 служит для подсоединения контактного датчика двери №1, а вход №2 для устройства запроса на выход на двери №1 того же контроллера. Вход №3 используется для контактного датчика на двери №2, а вход №4 для устройства запроса на выход на двери №2 того же контроллера.
- **Для контроллеров KT-400. Вход №1** используется для контактного датчика на двери №1, а вход №2 для устройства запроса на выход на двери №1 (REX Door #1) того же контроллера. Вход №5 служит для контактного датчика на двери №2, а вход №6 для устройства запроса на выход на двери №2 контроллера. Вход №9 предназначен для контактного датчика двери №3, а вход №10 для устройства запроса на выход для двери №3 контроллера. Вход №13 используется для контактного датчика двери №4, а вход №6 для устройства запроса на выход для двери №4 контроллера.

Описание входов

Входные устройства можно настроить через меню **Controller** (Контроллер) или меню **Devices** (Устройства).

1 Открыть закладку **Devices** (Устройства) и нажать иконку **Input** (Входы).



2 Указать шлюз в поле **Gateway**, сайт 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 контактного датчика открытия 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**).

6 По умолчанию опция **Controller report input state when not supervised** (Контролер сообщает статус неконтролируемого входа) не выделена. Это помогает поддерживать минимальный трафик обмена данными. Однако при необходимости можно выделить эту опцию.

7 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). Максимальное время для обоих параметров, alarm response и alarm restore, составляет 10:55:35.

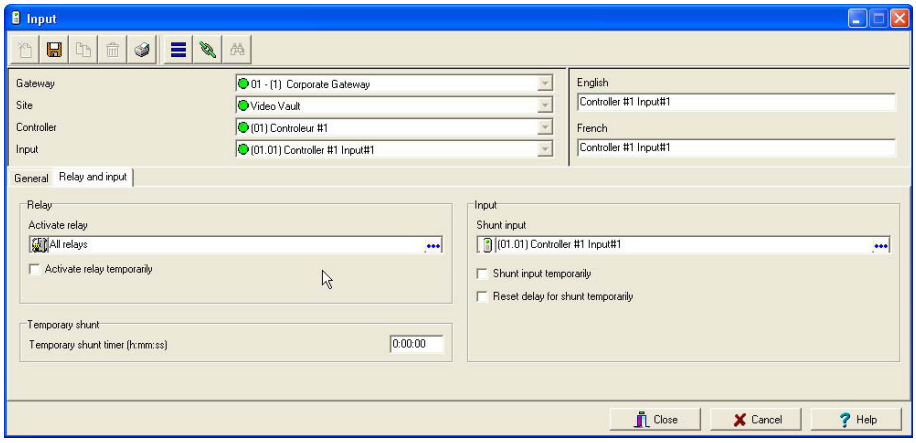
- **Alarm response time, mm:ss:cc** (Время отклика при переходе в статус тревоги) – задержка, после окончания которой система формирует событие об изменении статуса входа на тревожный.
- **Restore response time, mm:ss:cc** (Время отклика при возвращении прежнего статуса) – задержка, после окончания которой система формирует событие о возвращении прежнего статуса (только Corporate Gateways).

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.*

8 Указать при необходимости в поле **Graphic** графическую схему и в поле **Video view** видеоокно, к которому прикреплён вход.

Описание 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** указать одно или группу реле, которые будут срабатывать при активировании настраиваемого входа.

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.

ПРИМЕЧАНИЕ. *При установке таймера на ноль (0:00:00) реле точно отслеживает статус входа.*

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).

ПРИМЕЧАНИЕ. *Для того чтобы система правильно обрабатывала задержку возврата при временном шунтировании, опция* ***Temporary Shunt Timer*** *(Таймер временного шунтирования) должна быть настроена в меню описания входа, который будет сбрасывать эту задержку. Например, если вход 1 временно шунтирует вход 2, то таймер* ***Temporary Shunt Timer*** *должен быть также указан в описании входа 2.*

5 В списке **Shunt input** (Шунтируемые входы) выбрать вход, мониторинг которого не будет выполняться, пока указанный вход активирован.

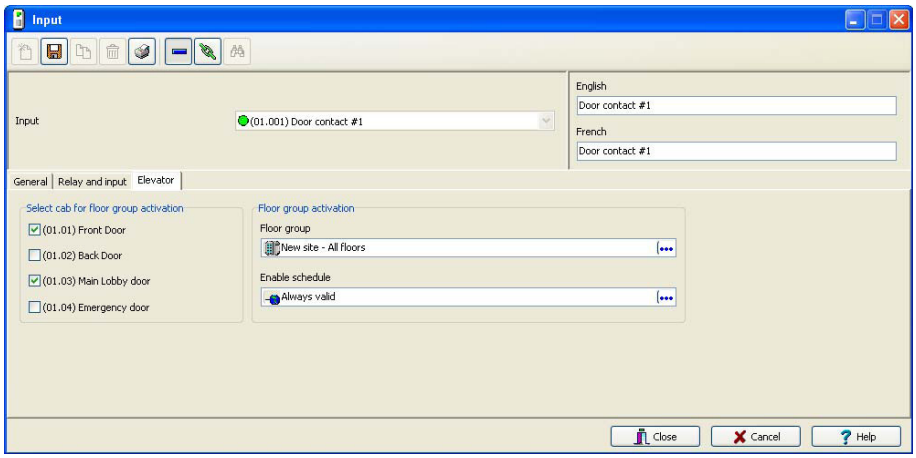
ПРИМЕЧАНИЕ. *В случае восстановления входа или возвращения его в нормальное состояние шунтируемый вход так же вернётся в нормальное состояние. Система сформирует событие “Input shunted by input” (Вход шунтируется по входу). Когда вход вернётся в нормальное состояние, будет сгенерировано событие “Input unshunted by input” (Вход перестал шунтироваться по входу).*

Описание входа для двери 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 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".*

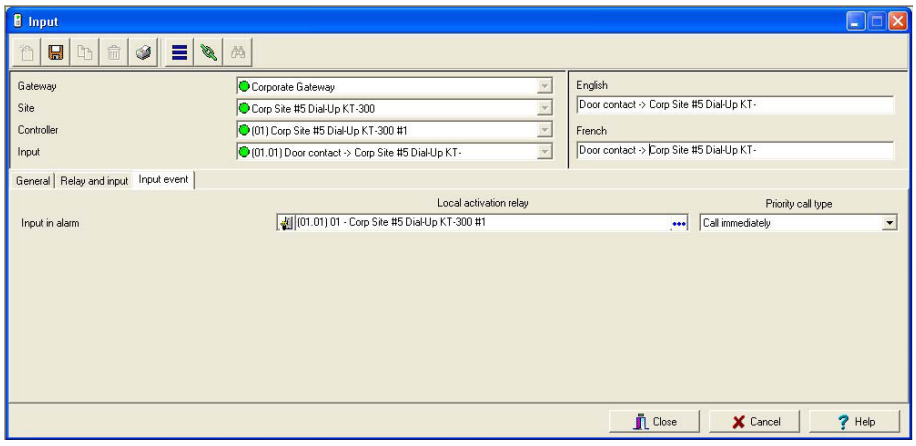
2 В разделе **Select cab for floor group activation** (Выбрать кабину для активации группы этажей) указать кабину, прикреплённую к данному входу.

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

1 Открыть закладку **Input event** (События входа).



2 В списке **Local activation relay** (Реле локальной активации) выбрать одно или группу реле, которые будут срабатывать при переключении этого входа в статус тревоги (при активировании входа).

ПРИМЕЧАНИЕ. *Группы реле доступны только при использовании контроллеров KT-400.*

3 В разделе **Priority call type** (Тип приоритетного вызова) указать тип вызова, наиболее полно отвечающий сообщению о событии, активирующем настраиваемый вход.

ПРИМЕЧАНИЕ. *Чтобы опция **Priority call type** стала доступной, в поле **Site connection type** (Тип соединения сайта) должен быть указан **Modem** (Модем). Более подробная информация приведена в разделе "Настройка конфигурации соединения типа Dial-Up (RS-232) Modem" на стр. 97.*

Конфигурация 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.

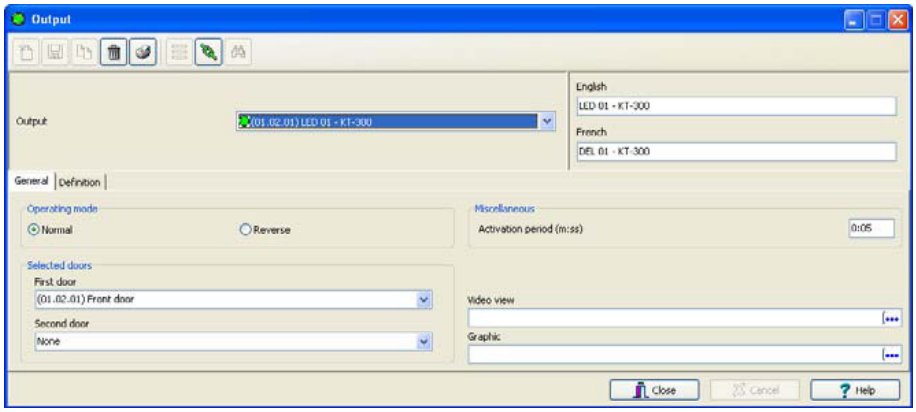
Электрические выходы имеют конфигурацию с открытым коллектором. В деактивированном состоянии они создают разомкнутый контур (не подсоединены к заземлению), а в активированном состоянии соединены на землю.

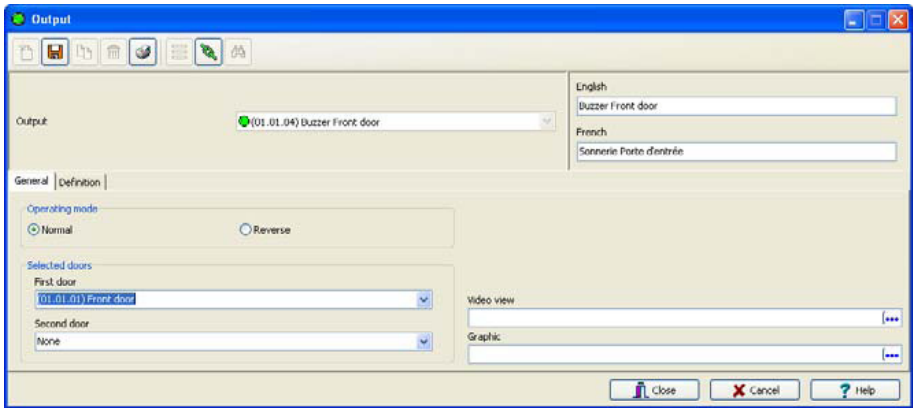
Выходные устройства можно настроить через меню Controller (Контроллер) или меню Gateway (Шлюзы).

Описание 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: шлюз, сайт, контроллер для выхода.

3 В выпадающем списке **Output** (Выходы) выделить выход, конфигурацию которого необходимо настроить.

4 Указать режим работы выходного устройства в поле **Operating mode** (Рабочий режим):

- **Normal** (Стандартный) – выход заземляется при активации.
- **Inverse** (Обратный) – выход размыкается (не заземляется) при активации.

5 В разделе **Selected doors** (Выбранные двери) указать, какая дверь будет использоваться для настраиваемого выхода.

- **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.*

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.

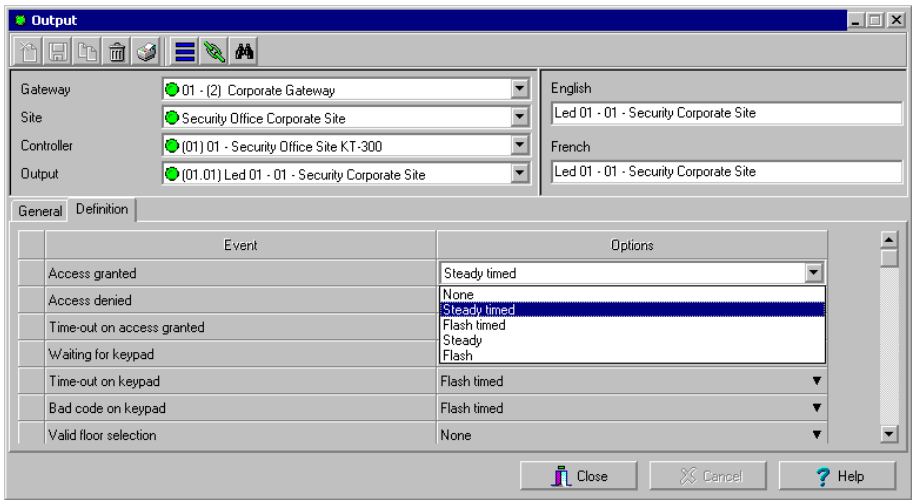
ПРИМЕЧАНИЕ. *Эта опция недоступна для контроллеров KT-400.*

ПРИМЕЧАНИЕ. *В случае интеграции с системами видеонаблюдения (функция Video Integration) 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 (рабочая станция, сайт, шлюз, контроллер и др.).*

Установление связей событий 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** (Описания), чтобы установить связь события двери с дополнительным выходом.



2 В колонке **Options** (Опции) привязать событие к статусу выхода.

- **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 вернётся в нормальное состояние.
- **Flash** (Мигание) – настраиваемый выход будет мигать, он будет оставаться активным, пока не вернётся в нормальное состояние.

ПРИМЕЧАНИЕ. *Задержки включения-выключения для выходов указывают при описании шлюза. Подробнее смотрите раздел "Настройка конфигурации шлюзов EntraPass" на стр. 86. События для включения-выключения таймера зависят от типа выбранного шлюза.*

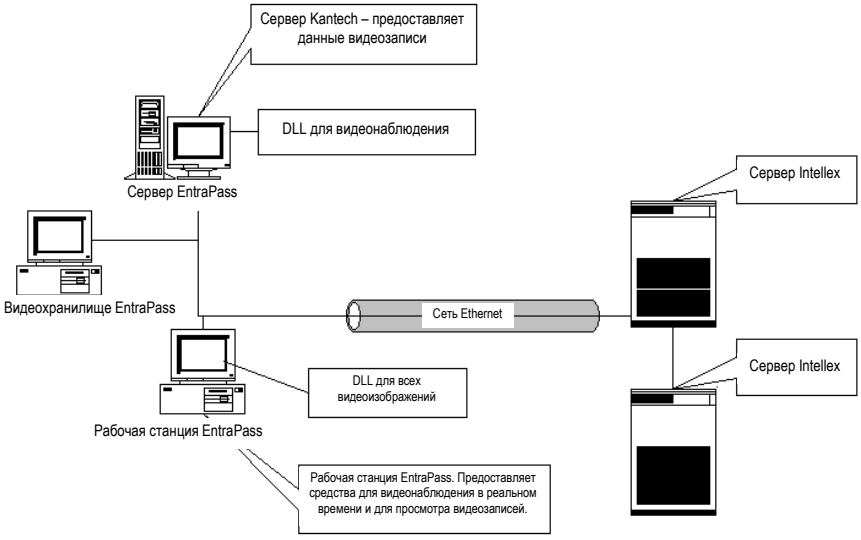
Глава 5 • Интеграция с системами видеонаблюдения

В ответ на общую тенденцию возрастания роли видео в системах контроля доступа в конфигурации EntraPass Corporate 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 и параметры видеонаблюдения, 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). 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

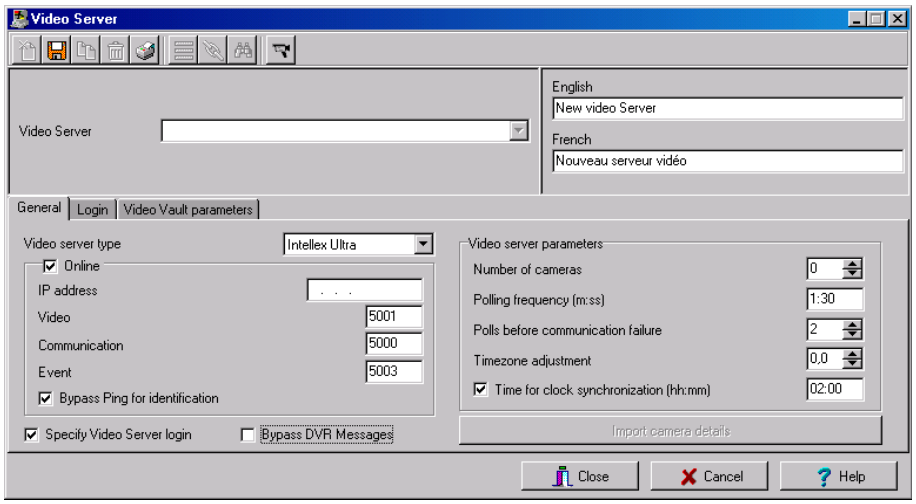
Видеосервер подключается к системе EntraPass через особый IP-адрес. Видеосервер собирает, хранит и раздаёт видеоданные на рабочие столы EntraPass для видеоконтроля и наблюдения. Доступ к видеоданным может осуществляться с любой рабочей станции EntraPass (с соответствующими правами доступа) по сети.

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 для настраиваемого видеосервера.

ПРИМЕЧАНИЕ. *Используемая в настоящий момент версия программного обеспечения интегрируется с системами видеонаблюдения Intellex® и видеорегистраторами EDVR 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 слежения (4, 8 или 16) в зависимости от выбранной модели (LT-4, LT-8 или LT-16). Кроме того, EntraPass поддерживает* EDVR-4, EDVR-9 и EDVR-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** (Сообщать видеосерверу регистрационные данные), 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.

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.

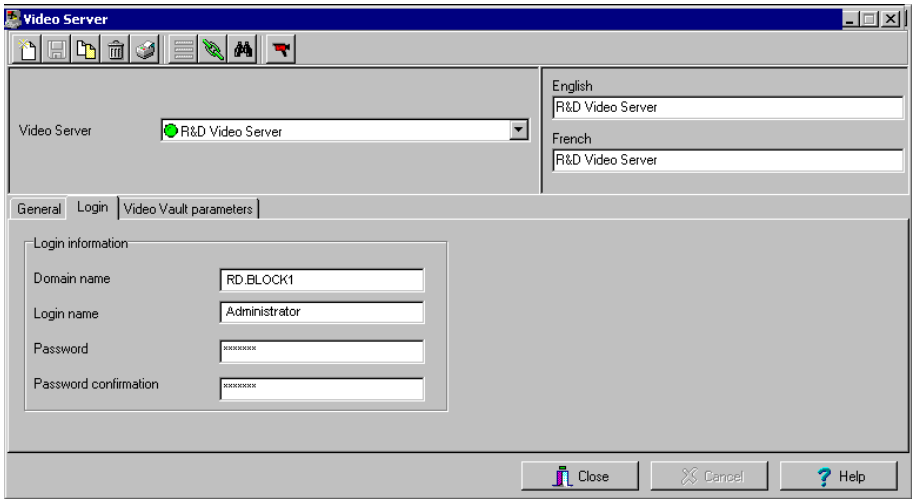
ПРИМЕЧАНИЕ. *Сервер EntraPass служит эталоном времени. Сервер Intellex будет рассчитывать время по времени сервера EntraPass. Например, если на сервере EntraPass установлено время 3:00, а на сервере Intellex 2:00, то для правильного отображения информации о событии на сервере Intellex необходимо скорректировать 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 параметрах безопасности видеосервера рекомендуется связаться с администратором сети.*

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:

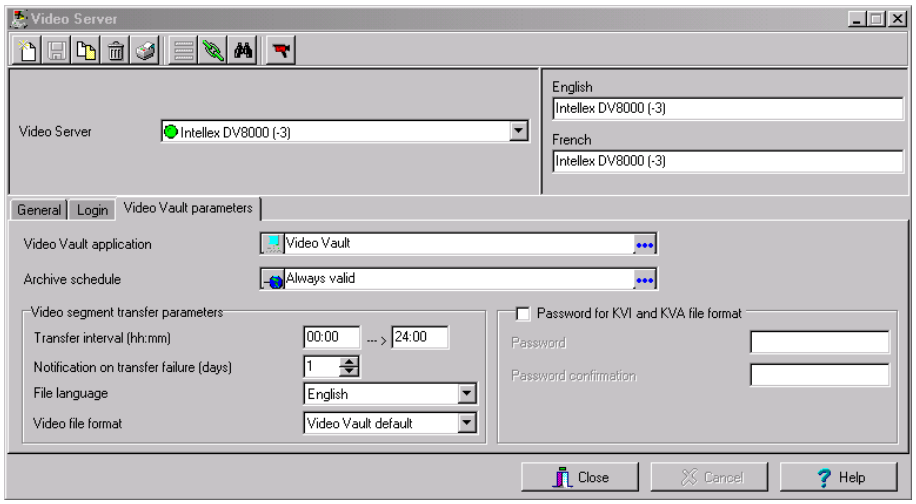
- **Domain Name** (Имя домена). Указать имя домена, используемое видеосервером Intellex.
- **Login name** (Регистрационное имя). Указать регистрационное имя, используемое для доступа к серверу Intellex.
- **Password** (Пароль). Указать пароль для контроллера домена.
- **Password confirmation** (Подтверждение 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.

Описание видеохранилища EntraPass Video Vault

Закладка **Video Vault parameters** (Параметры видеохранилища) содержит такие настройки, как расписание для создания архива и частота передачи данных для видеохранилища, если это приложение активировано в системе EntraPass и настроено на совместное использование с другими приложениями EntraPass.

- Более подробные сведения по установке видеохранилища изложены в разделе "Добавление дополнительных компонентов/функций" на стр. 12.
- Настройка приложения видеохранилища EntraPass Video Vault подробно описана в разделе "Настройка конфигурации приложения Видеохранилище EntraPass Video Vault" на стр. 80.
- Детали работы с приложением EntraPass Video Vault смотрите в разделе "Видеохранилище EntraPass Video Vault" на стр. 499.

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:

- **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, дней). 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, 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**: select the format for the video file that will be retrieved:
- **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 на видеорегистраторах типа EDVR, с помощью Windows Media Player или любой другой программы для просмотра файлов AVI. На клиентском компьютере обязательно должен быть установлен EDVR Bridge.
- **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.

Описание камер наблюдения

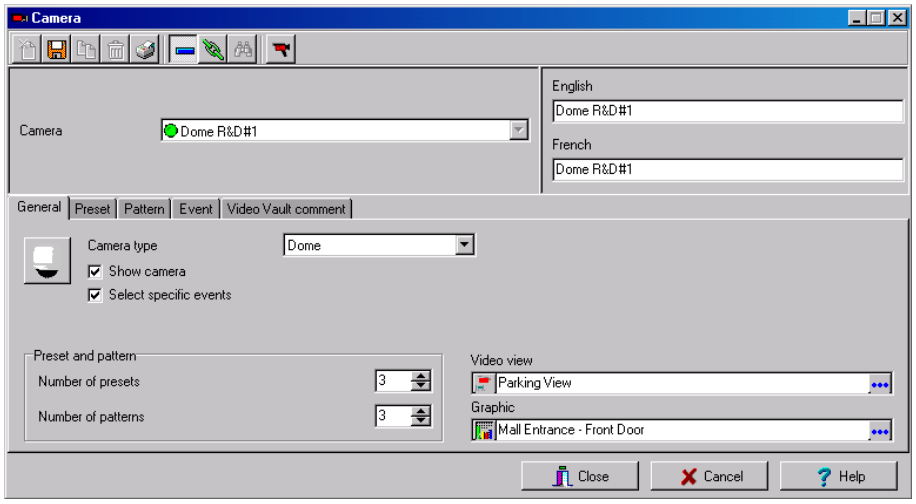
В системе EntraPass предусмотрена возможность назначения имён камерам, предустановкам и маршрутам движения камер для облегчения идентификации объектов на рабочем столе видеонаблюдения (Video) и при поиске видеособытий. При описании камеры наблюдения указываются следующие параметры:

- Тип (неповоротная или купольная)
- Предустановки (для купольных камер)
- Маршруты (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).*

Описание 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** (Описания 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 для записи (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.

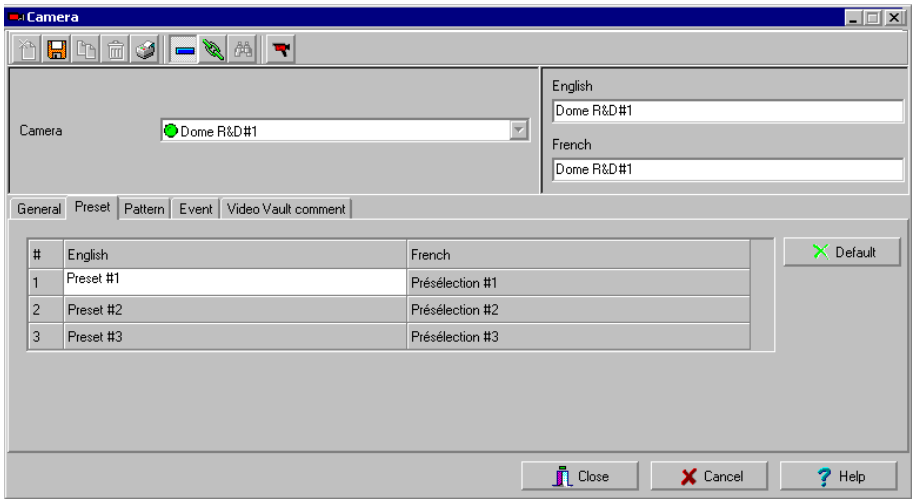
6 С помощью кнопок вверх/вниз настроить число предустановок и маршрутов движения выбранной камеры (если она купольная). После этого в окне **Camera** появятся закладки **Preset** (Предустановки) или **Pattern** (Маршруты).

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.

Описание предустановок и маршрутов

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.*

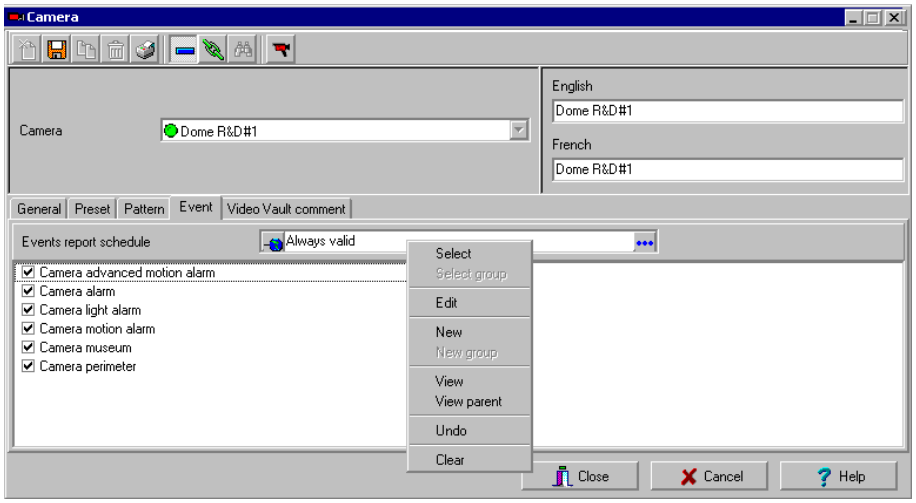
Описание событий для записи камерой

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 все выбранные события. А при указании ограниченного временного интервала будут передаваться только те 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.

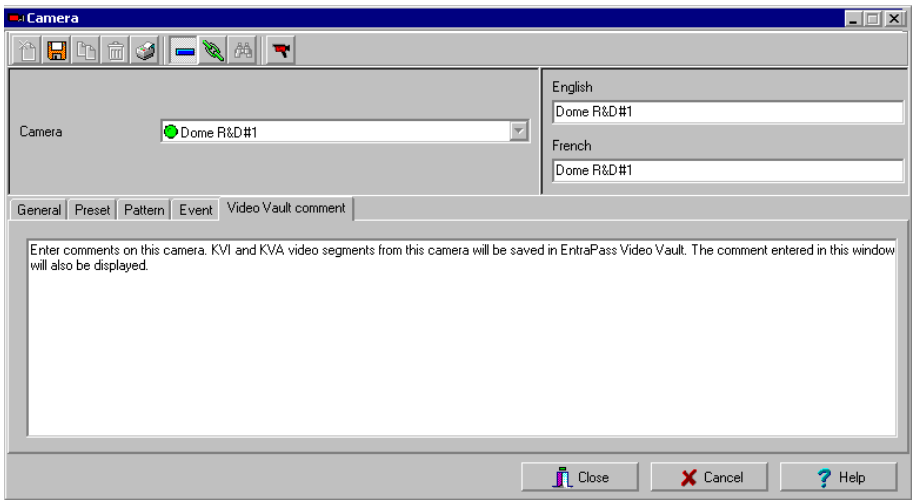


2 Выбрать расписание для передачи сообщений о событиях камеры. На сервер EntraPass будут отправляться только те события, которые будут записаны в указанный интервал времени. При нажатии на правую кнопку мыши в окне выбора расписания всплывает контекстное меню, позволяющее оператору создать новое расписание или выбрать одно из уже созданных. Порядок настройки расписания *смотрите в разделе "Описание расписания" на стр. 195*.

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 сообщает обо всех событиях, сигнализирующих о движении.
- **Camera alarm** (Сигнализация камеры). Камера сообщает о любом изменении на контролируемой территории.
- **Camera motion alarm** (Сигнализация о движении). Камера сообщает серверу EntraPass о любом движении на контролируемой территории.
- **Camera museum** (Режим музея).
- **Camera perimeter** (Сигнализация о движении по периметру). Камера сообщает серверу EntraPass о любом пересечении границ контролируемой территории.

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.

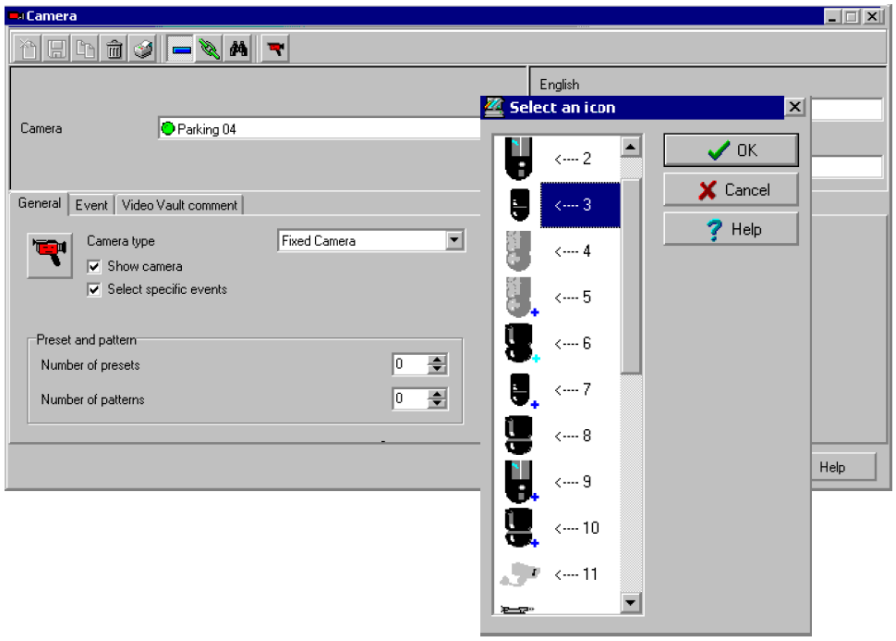


5 Записать комментарий к настраиваемой камере наблюдения и нажать кнопку **Close**, для того чтобы сохранить его и закрыть окно.

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.*

Описание видеоокон

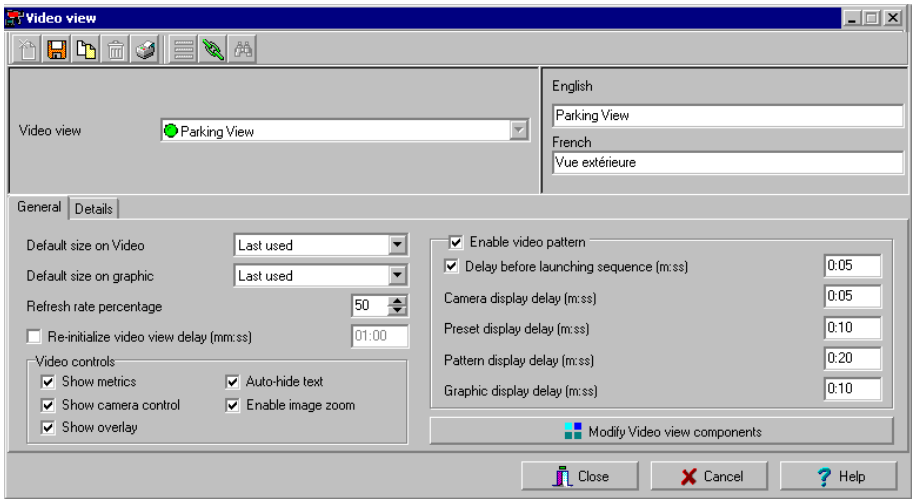
После настройки видеосервера и описания его камер наблюдения, операторы получают возможность настраивать видеоокна, отображаемые на рабочем столе видеонаблюдения.

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, шлюзы, сайты, контроллеры и др.) и видеоокнами можно установить связь. Позже, в меню описания компонентов можно назначить видеоокно, которое будет использоваться для отображения конкретного компонента.

Описание общих параметров 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 кадра: 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. При высокой степени сжатия (> 80) сжатие будет небольшим. 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 неповоротных 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 видеошаблона) становится доступной после выбора компонентов, которые будут отображаться в этом видеоокне.*

8 Поставить флажок в поле **Enable video pattern** (Разрешить использование видеошаблона), 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.

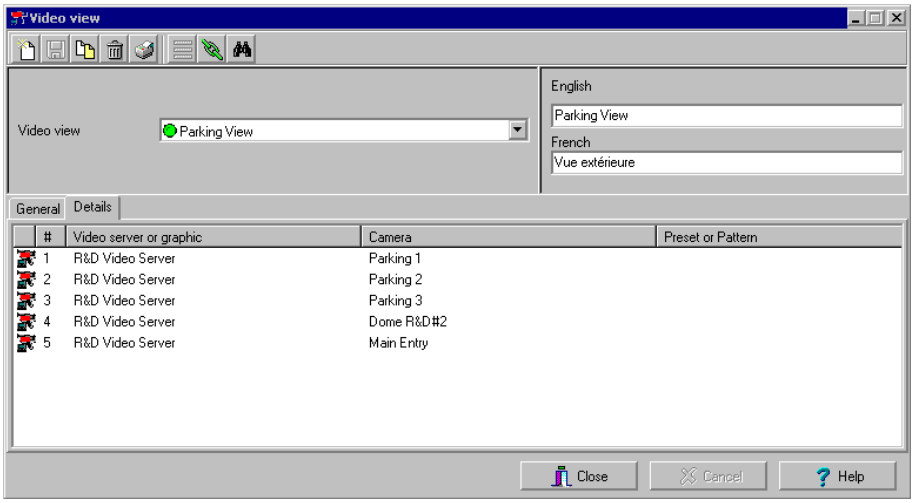
9 Отметить флажком поле **Delay before launching sequence, m:ss** (Задержка перед запуском последовательности, м:сс), чтобы указать задержку переключения перед началом последовательного вывода кадров в видеоокно.

10 Указать длительность отображения камеры **(Camera display delay)**, предустановок (**Preset display delay)**, маршрутов движения **(Pattern display delay)** и окна графики **(Graphic display delay)**.

ПРИМЕЧАНИЕ. *Эти параметры описывают длительность вывода на экран 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 секунды
Camera display delay (Длительность отображения камеры)	3 секунды
Preset display delay (Длительность отображения предустановки)	5 секунд
Pattern display delay (Длительность отображения маршрута)	10 секунд
Graphic display delay (Длительность отображения графики)	5 секунд

11 Открыть закладку ***Details*** (Подробные сведения) для просмотра данных о выделенном окне: видеосерверах (video servers), камерах наблюдения (cameras), а также (если используются) о предустановках камеры (presets) и маршрутах (patterns).



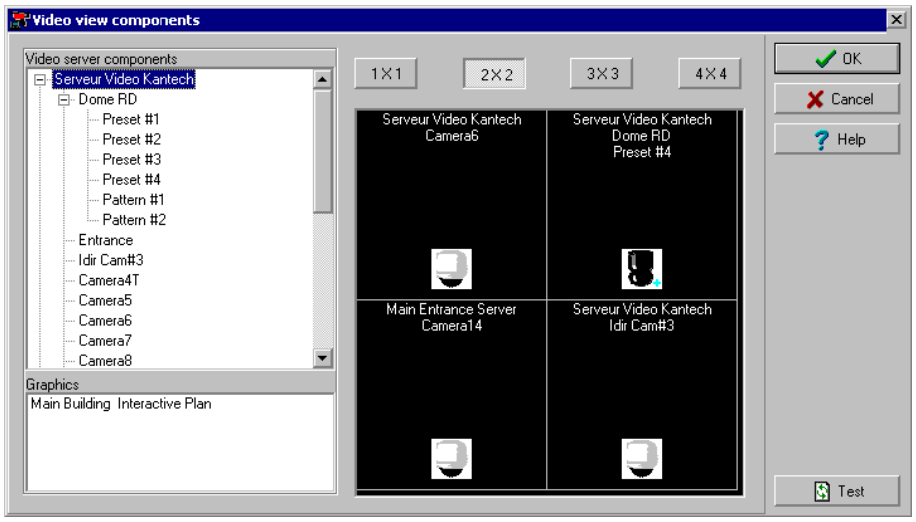
Создание и редактирование видеоокон

Использование предустановок и маршрутов движения позволяет правильно настроить автоматическую работу купольных камер. Видео, передаваемое камерами наблюдения, отображается на рабочем столе Video, предназначенном для видеонаблюдения. Предварительная настройка режимов видеонаблюдения обеспечивает оптимизацию времени наблюдения. Система EntraPass предоставляет широкие возможности выбора режима наблюдения, в зависимости от нужд пользователей:

- Одна камера наблюдения
- Несколько камер
- Несколько графических изображений 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 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 графики допускается только в одну ячейку видеоокна. Допускается вывод камер с другого видеосервера, однако источник 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.

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.

Описание параметров инициирующих событий

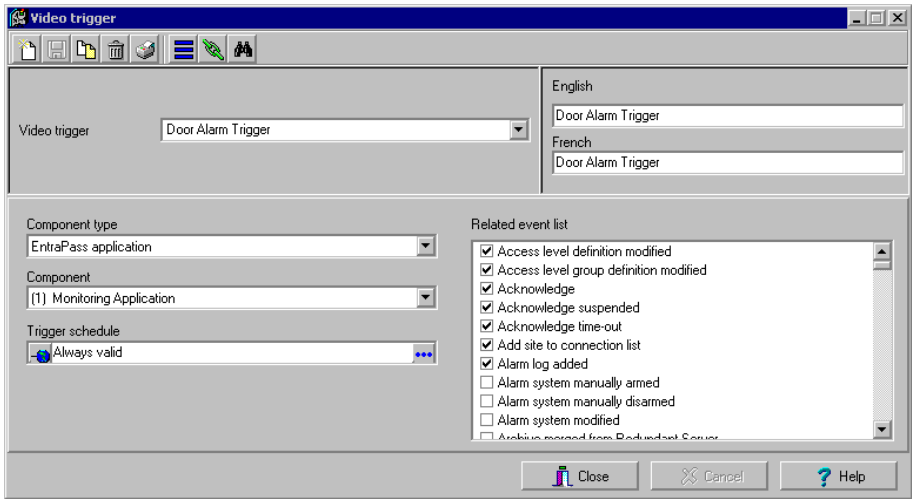
Необходимо указать следующую информацию:

- Название на двух языках
- Component type - тип компонента, используемого для инициирующего события. События связаны с компонентами системы: шлюзами, сайтами, 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 инициирующих.*

1 На панели инструментов Video нажать кнопку **Video trigger** (Инициирующие события). Откроется окно Video trigger.



2 Нажать иконку New (Создать) или выбрать уже созданное инициирующее событие, которое необходимо изменить. Назначить этому событию описательное имя.

ПРИМЕЧАНИЕ. *При попытке сохранить настройки без указания типа компонента или без назначения компонента для настраиваемого инициирующего события система выдаёт на экран предупредительное сообщение.*

3 В выпадающем списке **Component** (Компоненты) указать, какой компонент необходимо использовать для инициации записи. Это может быть контроллер двери, например.

4 В поле **Trigger schedule** (Расписание инициирующего события) указать расписание для события. При необходимости можно указать особое расписание для этого инициирующего события (**Definition** (Описания) > **Schedule** (Расписания)). Если никакого расписания для события не выбрано, событие применяться не будет.

5 В списке **Related event list** (Список связанных событий) указать одно или несколько событий, связанных с событием, инициирующим запись.

Параметры записи (Recording Parameters)

Меню **Recording Parameters** позволяет пользователям описывать параметры управления видеозаписью и создавать связи параметров записи (источник видеозаписи, камеры и пр.) с инициирующим событием. Для каждого случая записи следует указать параметры (например, источник-видеосервер, камера и др.).

Запись может останавливаться по таймеру (максимальное время записи) или по инициирующему событию, если какое-либо инициирующее событие используется для останова записи.

Для каждого типа инициирующего события должен быть указан компонент-источник. Например, для сообщения о взломе двери (Door forced) должен быть указан компонент “Door” (Дверь). Также следует указать действие (запуск или останов записи).

Система EntraPass даёт возможность связать несколько параметров записи с одним инициирующим событием. В этом случае все записи будут связаны с одним событием, и будет возможно сохранить все записанные видеофрагменты как запись одного события.

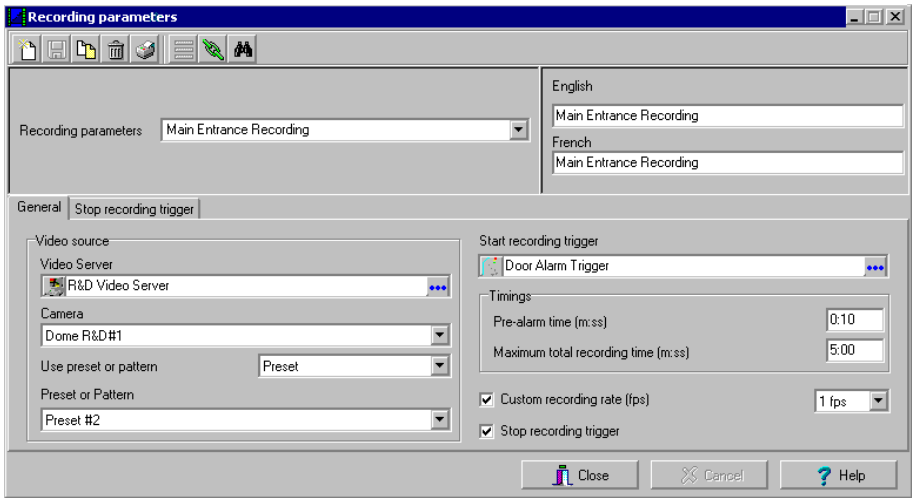
Настройка параметров записи

Окно Video record (Запись видео) позволяет настроить параметры записи видеофрагментов. 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
- Событие, инициирующее 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 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. Действительно, 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** (События, инициирующие начало записи) выбрать событие, которое необходимо связать с настраиваемыми параметрами записи. Всплывающее окно Video trigger содержит список всех инициирующих событий, описанных 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.*

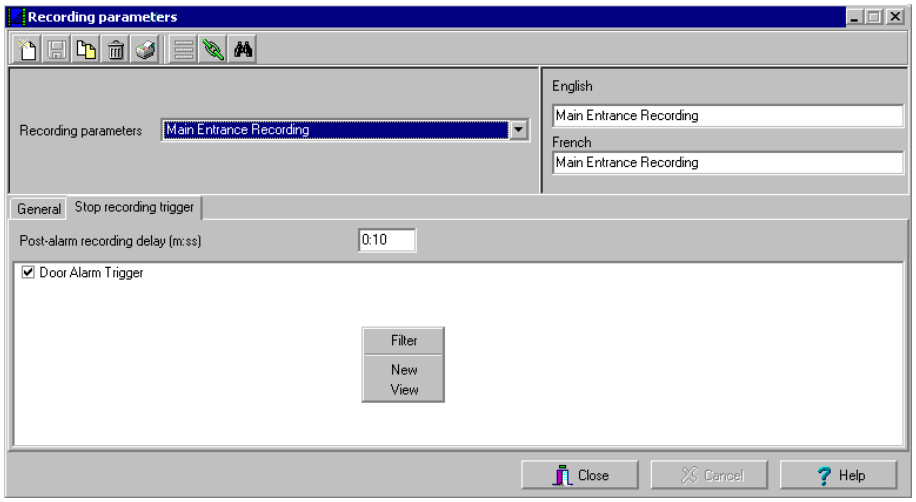
8 Стрелками вверх-вниз указать скорость записи для параметров записи. Это значение будет использоваться системой EntraPass исключительно для выбранных параметров записи. По умолчанию установлено значение 2,5 к/с. Среднее значение составляет 7,5 к/с. При установке скорости ниже этой величины на экране 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. Фактическая скорость записи каждой камеры наблюдения составляет около 30 к/с.*

Настройка параметров останова записи

Для того чтобы связать параметры записи с событием, инициирующим остановку записи, следует отметить флажком поле **Stop recording trigger** (События, инициирующие остановку записи). После этого в окне Recording parameters появится закладка **Stop recording trigger.**

1 Открыть закладку **Stop recording trigger** (События, инициирующие остановку записи).



- **Post-alarm recording delay, m:ss** (Длительность посттревожной записи, м:сс) – позволяет завершить запись по тревоге с некоторой задержкой после снятия тревоги. При установке курсора в этом поле на экране отображается допустимое значение задержки.
- **Trigger** (Инициирующее событие) – выбрать событие (одно или несколько), которое будет останавливать запись.

ПРИМЕЧАНИЕ. *Для того чтобы создать новое событие, следует щёлкнуть правой кнопкой мыши по окну, в котором отображаются инициирующие события.*

Список видеособытий (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:

- События, инициирующие включение-выключение видеозаписи
- 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 видеособытий Video Event List

В окне Video Event List отображаются все видеособытия вместе с описанием. Операторы системы EntraPass имеют возможность выполнять следующие действия:

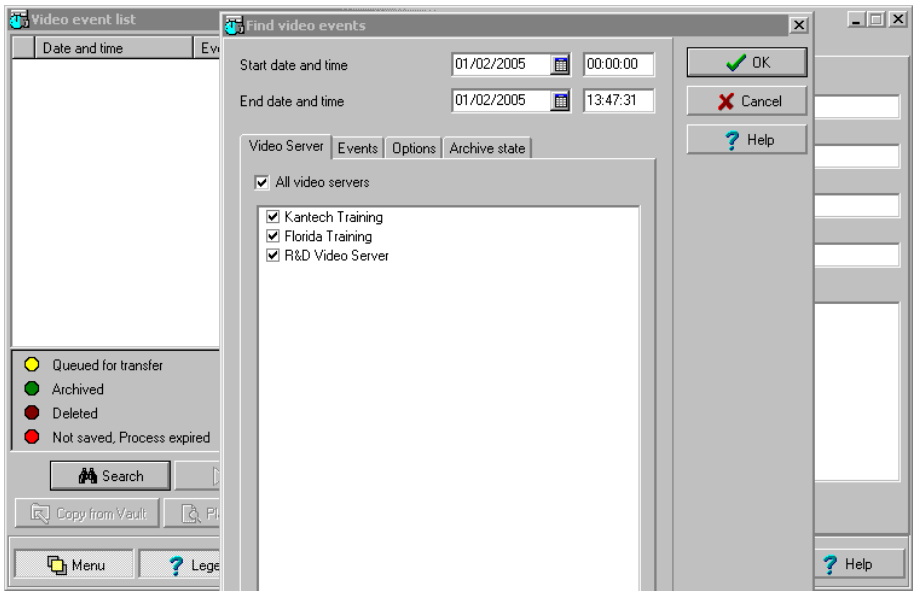
- Искать конкретное событие, связанное с видеофрагментом, по дате и времени создания этого видеофрагмента
- Просматривать записанный видеофрагмент
- Экспортировать видеофрагмент для дальнейшего обсуждения
- Просматривать или копировать видеофрагменты из видеохранилища EntraPass Video Vault
- Повторять все оборванные пересылки видеофрагментов, предназначенных для архивирования, но неудачно переданных в видеохранилище EntraPass Video Vault.

Поиск видеособытий

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 архивные события по статусу архива.

1 В окне Video Events List нажать кнопку **Search** (Поиск). Откроется окно Find video events (Поиск видеособытий).

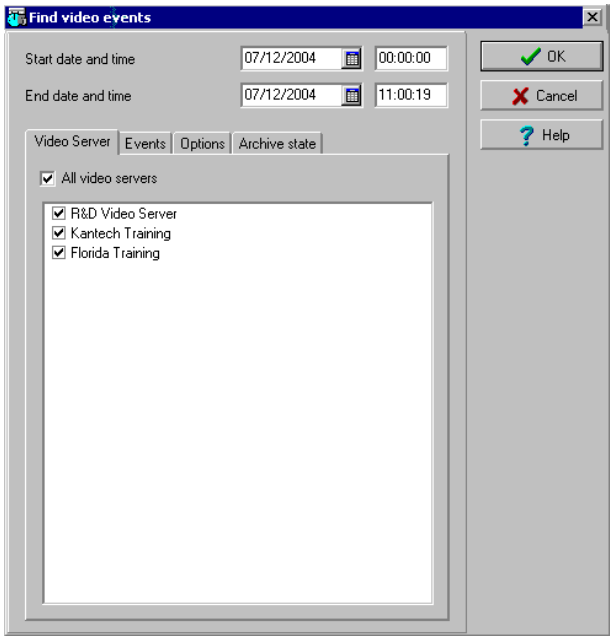


ПРИМЕЧАНИЕ. *Если кнопки* **Menu** *(Меню) и* **Legend** *(Описание) недоступны, то в этом окне не будет показываться описание и кнопки, расположенные в нижней части.*

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.

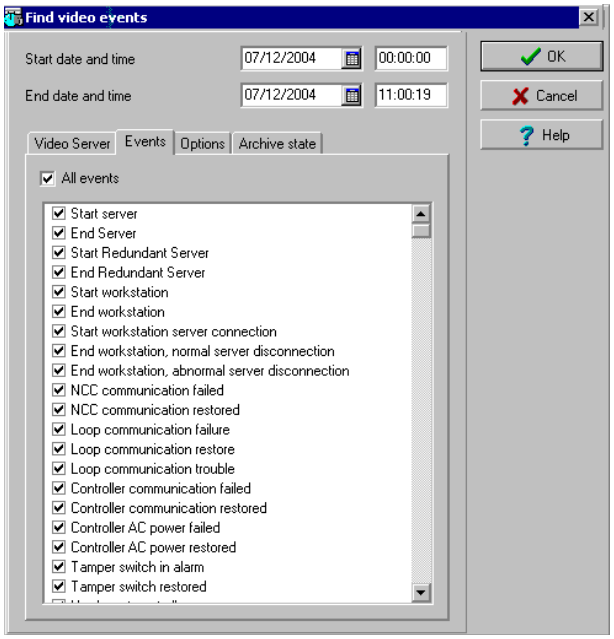
ПРИМЕЧАНИЕ. *Кнопка* **Legends** *(Описание) служит для отображения сведений о статусе видеособытий. Кнопки* ***Play*** *(Воспроизведение) и* ***Copy from Video Vault*** *(Копирование из видеохранилища) доступны в том случае, когда выбранные видеособытия уже находятся в архиве видеохранилища.*

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).

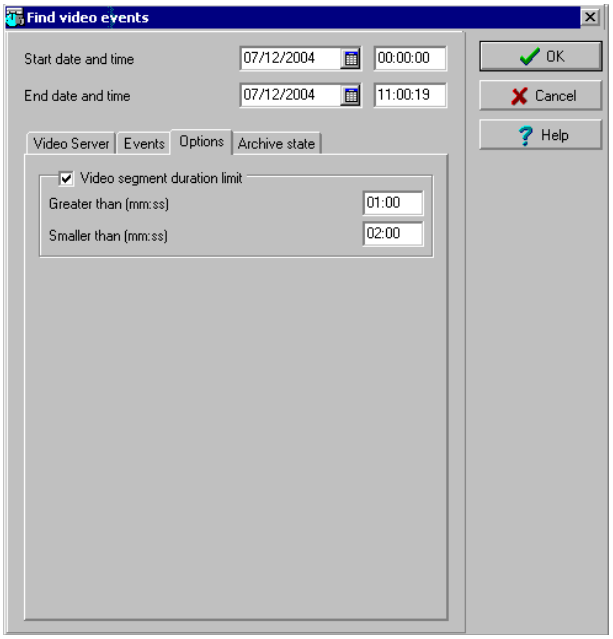


ПРИМЕЧАНИЕ. *Если событие зарегистрировано на двух и более видеосерверах, то при выделении хотя бы одного из них это событие будет включено в список.*

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.

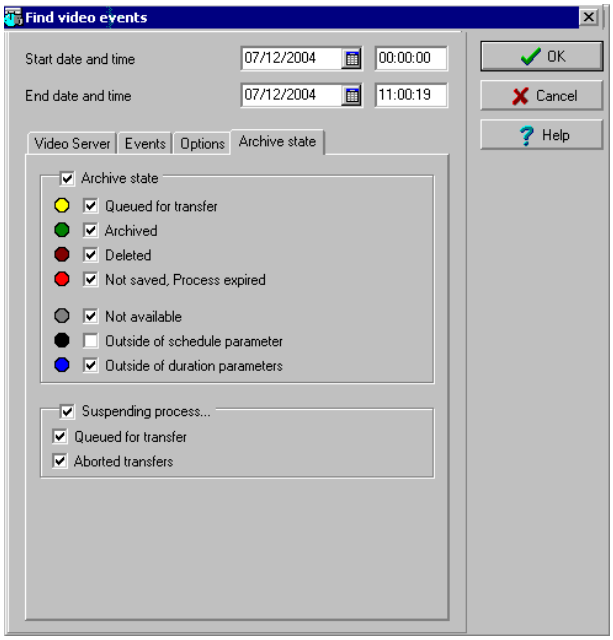


5 Открыть закладку **Options** (Опции), чтобы отфильтровать видеофрагменты по их длительности.



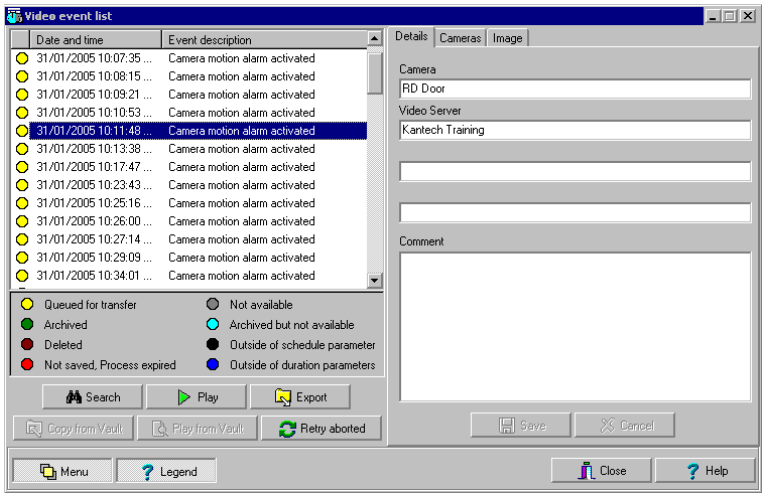
6 Поставить флажок в поле **Size filter** (Фильтровать по размеру), указать длительность в поле **Greater than, mm:ss** (Больше, чем, мм:сс) и в поле **Smaller than, mm:ss** (Меньше, чем, мм:сс). Значения этих параметров указываются в минутах и секундах. Данная функция позволяет выбрать видеофрагменты, длительность которых находится в определённом диапазоне.

7 Открыть закладку **Archive State** (Статус архива), чтобы отфильтровать события по статусу архива.



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.



ПРИМЕЧАНИЕ. *Кнопки **Play** (Воспроизведение) и **Copy from Video Vault** (Копирование из видеохранилища) доступны в том случае, когда выбранные видеособытия уже находятся в архиве видеохранилища. Архивные 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. Подробнее смотрите раздел *"Поиск видеособытий" на стр. 172.*
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** (Копирование из видеохранилища) позволяет просматривать видеособытия, хранящиеся в архиве видеохранилища.

Кнопка	Описание
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.

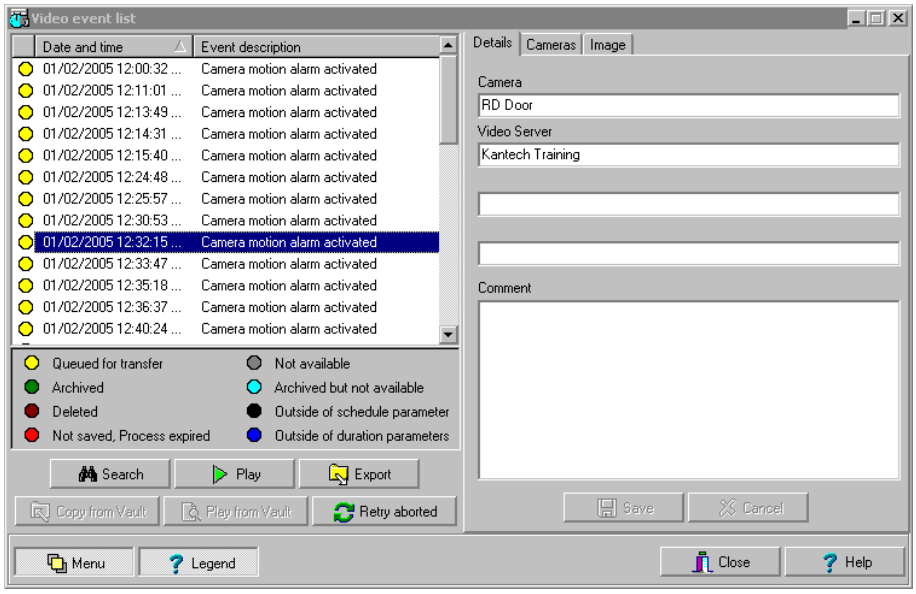
Воспроизведение видеофрагментов

Окно Video Event List разделено на две части: слева отображаются все видеособытия, отвечающие установленным критериям поиска. В нижней части окна даны описания статусов для каждого события. Кроме того, там же находятся кнопки, необходимые для выполнения различных действий с видеозаписями. Правая панель содержит три закладки:

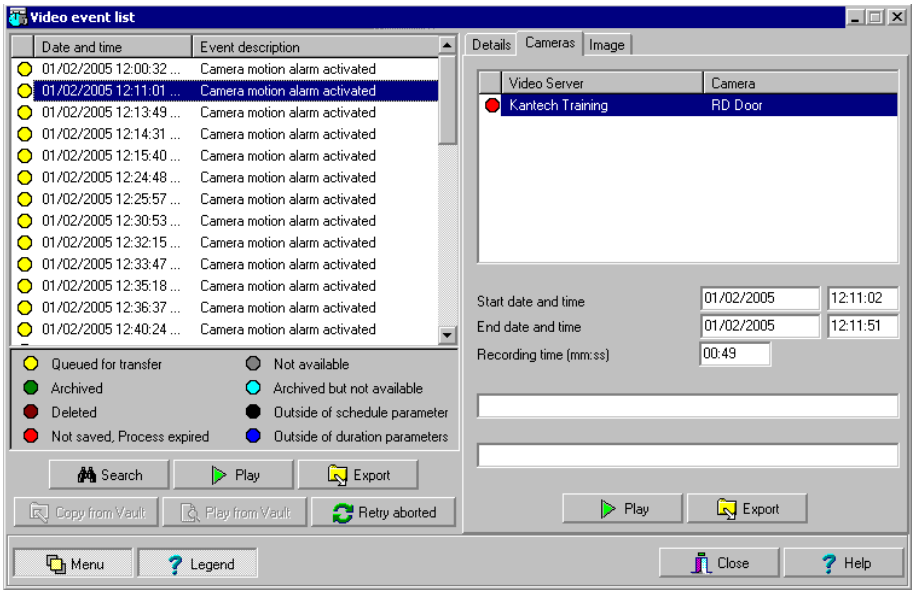
- Под закладкой **Details** (Подробные сведения) находится текстовое описание видеособытия, включая такие данные, как имя видеосервера, на котором оно было записано, имя оператора, который был зарегистрирован в системе в тот момент и др.
- В закладке **Camera** (Камеры) отображаются камеры наблюдения, связанные с выбранным событием.
- Закладка **Image** (Изображение) содержит ключевой кадр для последовательности кадров. Ключевой кадр предназначен для предварительного просмотра последовательности. 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 инициирующее запись 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.

- **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 – 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 (Video), меню **Desktop** (Рабочие столы).
- Нажать кнопку **Export** (Экспортировать) для дальнейшего использования видеофрагмента. Подробнее смотрите раздел *"Экспортирование видеофайлов" на стр. 181.*

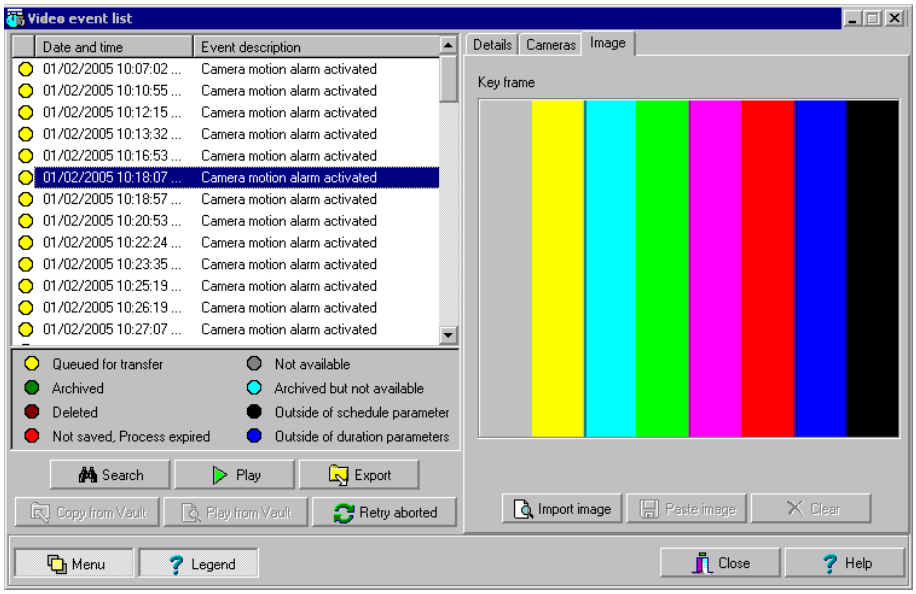
Привязка ключевых кадров к видеозаписям

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 импортирование 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) – использовать изображение из файла, ранее сохранённое или экспортированное.

- **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 видеофайлов

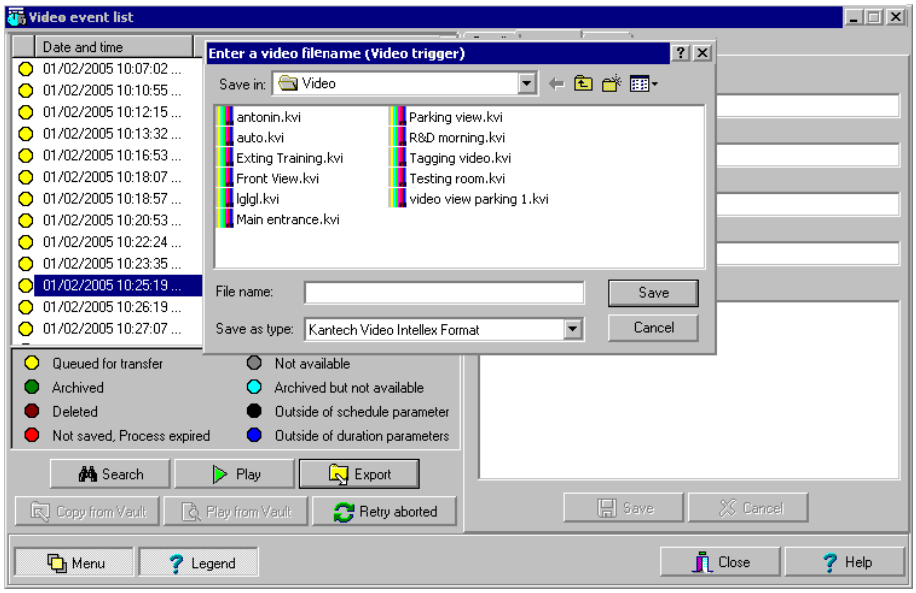
Система EntraPass экспортирует видеофрагменты в четырёх форматах, включая KVI и KVA.

- 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 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 CE\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).*

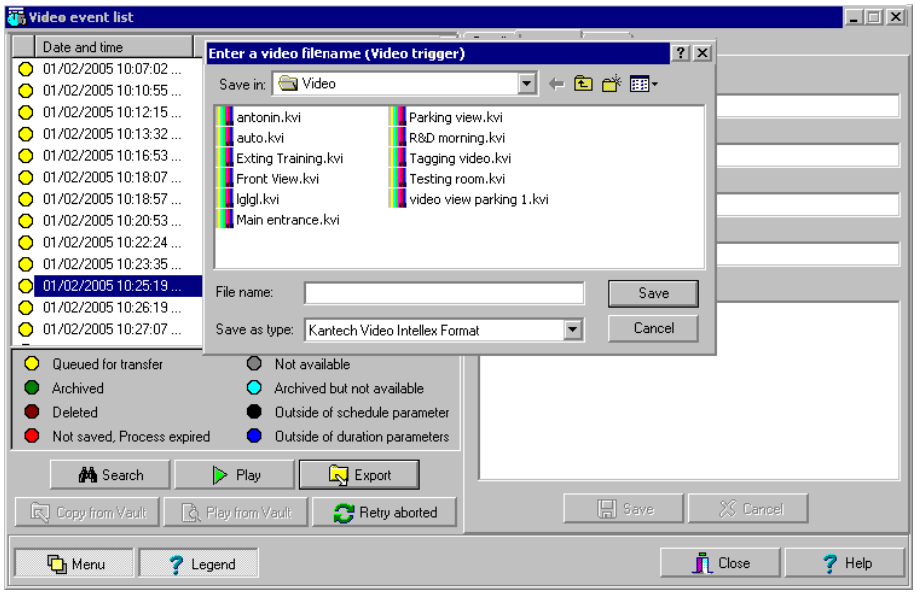
4 Нажать **Save** (Сохранить), чтобы закрыть окно Enter filename. После этого открывается окно Description and password (Описание и пароль).

Защита видеозаписей паролем

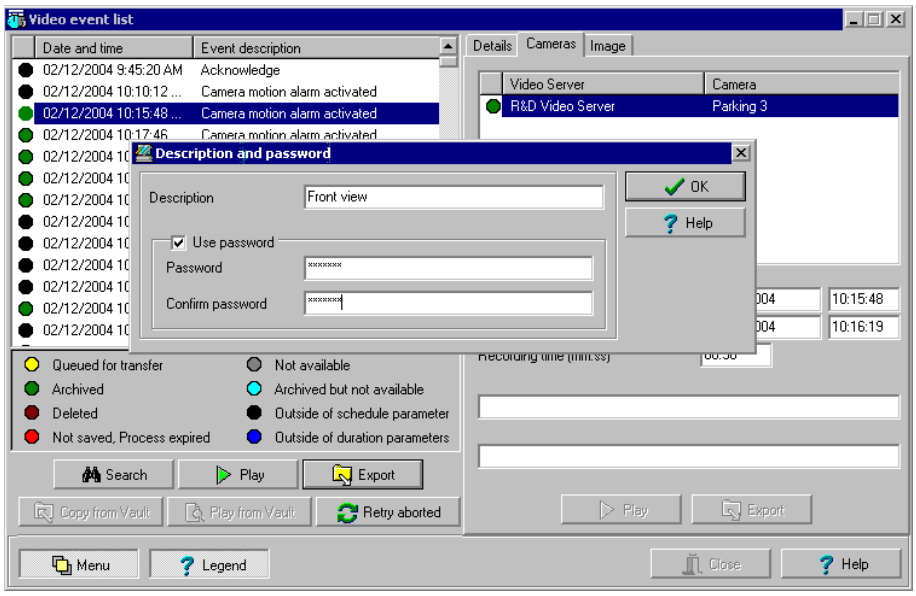
Экспортированные видеофайлы можно защитить паролем. В таком случае для просмотра видео пользователи должны будут ввести пароль.

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.

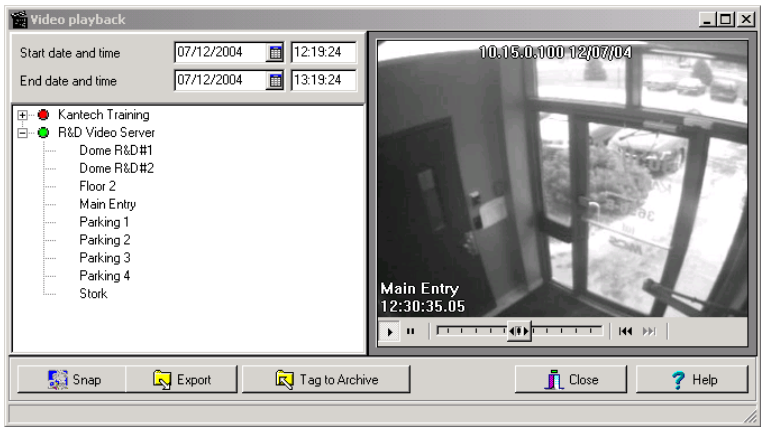
Воспроизведение видеофайлов

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 видеозаписей 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.



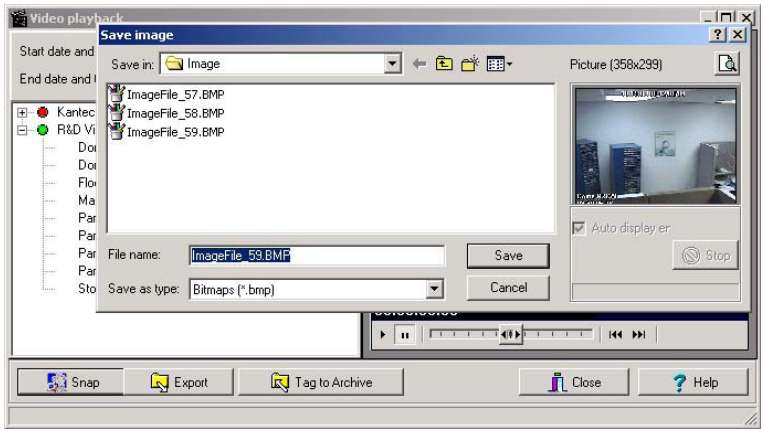
2 На панели слева выбрать камеру и перетащить в окно справа. Воспроизведение выполняется для указанного времени начала и окончания. На панели справа внизу расположены кнопки воспроизведения, паузы, останова, быстрой прокрутки вперёд/назад.

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 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_CE\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.

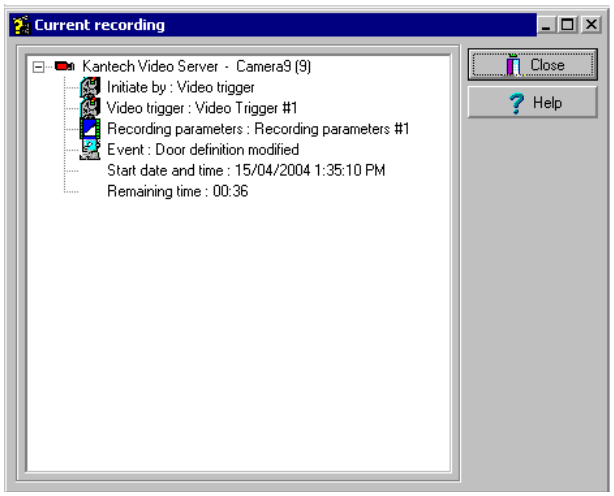
Записи, выполняемые в данный момент (Current Recording)

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:

- по инициирующему событию
- по команде оператора
- 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
Инициирующее событие	• 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

Чем вызвана запись	Сведения
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 (Video)

Рабочий стол Video позволяет операторам наблюдать в режиме реального времени изображение, передаваемое камерами наблюдения, подключёнными к сети и настроенными соответствующим образом.

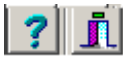
Вывод на экран окна видеонаблюдения

1 Открыть закладку **Desktop** (Рабочий стол) в главном окне приложения EntraPass. Выбрать рабочий стол **Video**. Окно видеонаблюдения Video View откроется на этом рабочем столе.

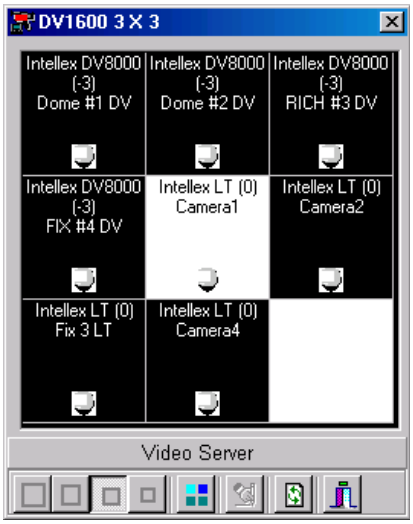
ПРИМЕЧАНИЕ. *При первом запуске рабочий стол Video откроется пустым. На экране будет сообщение “No video view selected” (Не выбрано видеоокно).*

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 мощность для его обработки. Таким образом, увеличение размеров изображения ведёт к замедлению работы.
	Эти кнопки доступны для пользователей с уровнем доступа оператора (Operator). 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 приведена *в разделе "Задание уровней безопасности" на стр. 326.*
	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 последовательный режим вывода изображений будет остановлен для вывода на экран только выбранной ячейки.



ПРИМЕЧАНИЕ. *Если вызвать 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 (для настройки положения, зума, фокуса) нажатием на иконку камеры. Доступные опции зависят от используемой цифровой системы видеонаблюдения. Подробное описание приведено в руководстве к системе видеонаблюдения.

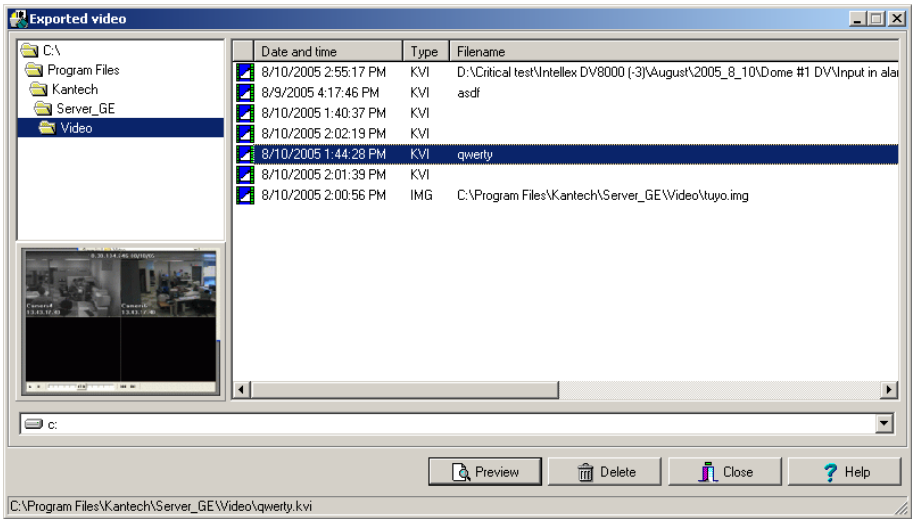
ПРИМЕЧАНИЕ. *Если купольная камера настроена на определённые маршруты движения, то изображение может передаваться по шаблону, состоящему из одного или нескольких маршрутов движения. Более подробные сведения по настройке смотрите в разделе "Описание видеоокон" на стр. 162.*

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**).

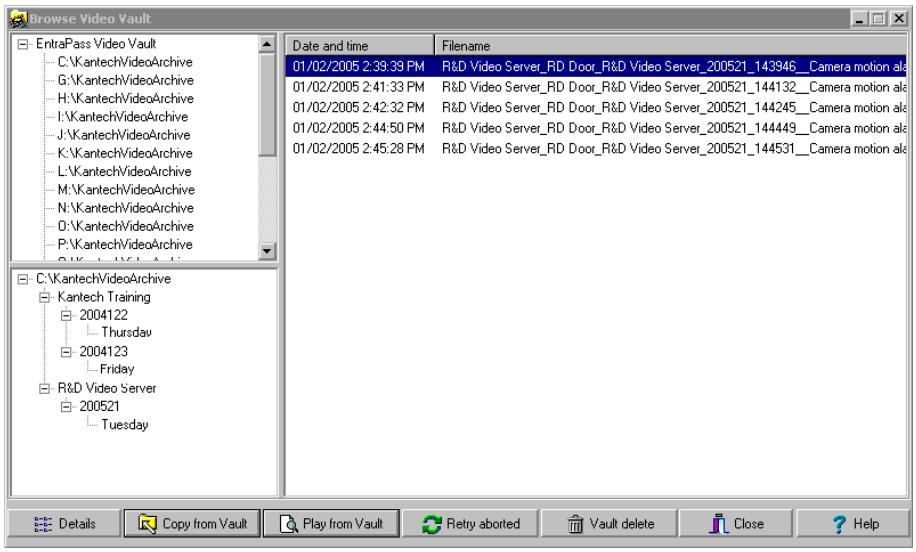
Просмотр видеохранилища EntraPass Video Vault

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 6 • Описания

Панель инструментов **Definition** (Описания) служит для описания логических компонентов системы, включая:

- Расписания
- Этажи
- Графические схемы
- Праздничные дни

Описание расписаний (раздел Schedule)

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 для каждого шлюза 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 приведена в разделе "Расписание" на стр. 458.*

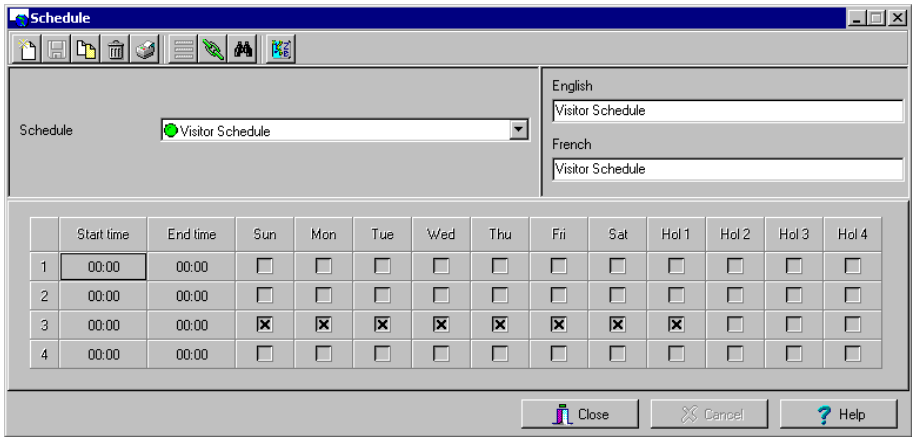
Система EntraPass поддерживает две группы расписаний:

- **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.
- **Corporate site schedules** (Расписания для корпоративных сайтов) – отдельные расписания для каждого сайта. Для каждого сайта 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).

При настройке и назначении расписания следует особое внимание уделять правильному выбору категории для этого расписания. Например, при назначении или настройке системного расписания (для рабочих станций, операторов, параметров событий, инициирующих событий) будет доступен выбор компонентов этой категории. При выборе расписаний для физических компонентов типа контроллеров, дверей, входов, их расписания будут группироваться по сайтам, если используется шлюз Corporate Gateway. Если в системе два сайта, то для каждого сайта будут две отдельные группы расписаний. Таким образом можно настроить до 99 расписаний для каждого сайта.

Описание расписания

1 В главном окне EntraPass открыть закладку **Definition** (описания). На панели инструментов **Definition** (Описания) 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). В списке* ***Gateway/ site*** *выбрать* ***Site*** *(Сайт) или* ***System schedule*** *(Системное расписание), то есть расписание, применимое к системным компонентам типа параметров событий, инициирующих событий, регистрационных данных оператора).*

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.*

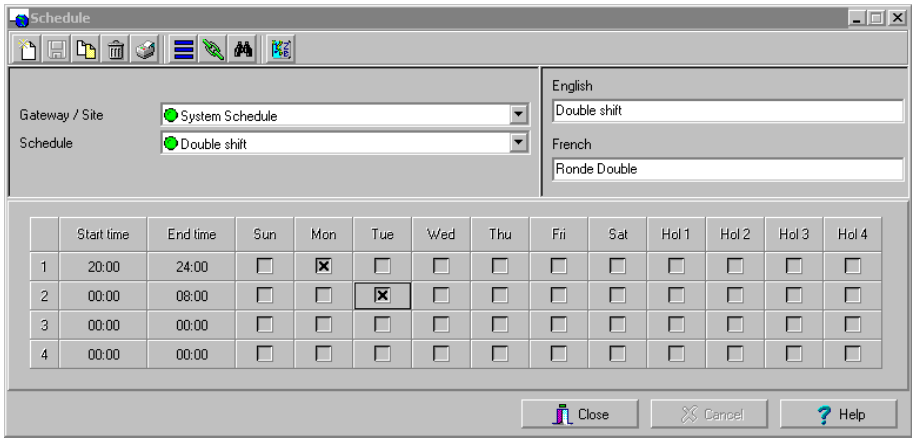
7 Указать, в какие дни недели это расписание будет достоверным. Для этого поставить галочку в поле под каждым днём недели.

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.

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;

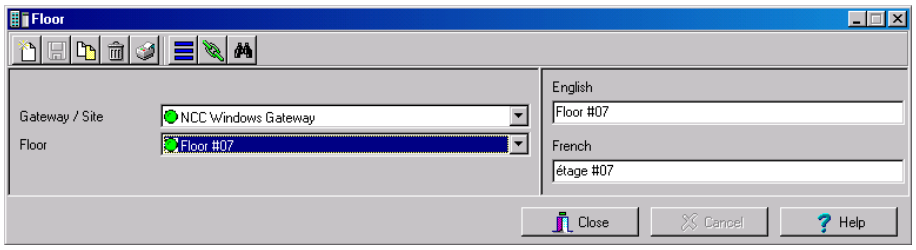


2 Второй интервал будет во вторник, с 00:00 до 08:00. Система будет рассматривать эти два интервала как единый интервал.

Описание 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** (Описания) нажать кнопку **Floor** (Этажи).



2 В выпадающем списке **Site** (Сайт) выделить шлюз/сайт, 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.

Описание графических схем

Графическая схема соответствует охраняемой территории объекта, на которой расположены компоненты (приложения EntraPass, контроллеры, входы, реле и др.).

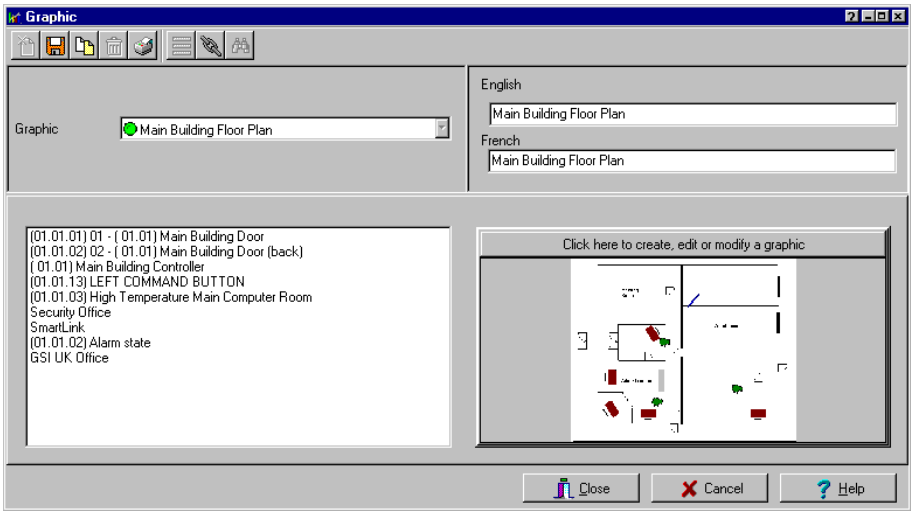
С помощью графических схем операторы могут легко определить точное место расположения компонента на сайте или увидеть статус компонентов и устройств, в том числе дверей, контактов, детекторов движения, контроллеров, прикреплённых к графическому плану системы. Операторы могут выполнять операции с изображенным на схеме компонентом (например, отпирать-запирать двери).

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-CE\Generaldata\Demobmp.*

Описание компонентов графических схем (раздел Graphic)

1 На панели инструментов Definition (Описания) нажать кнопку **Graphics** (Графические схемы).

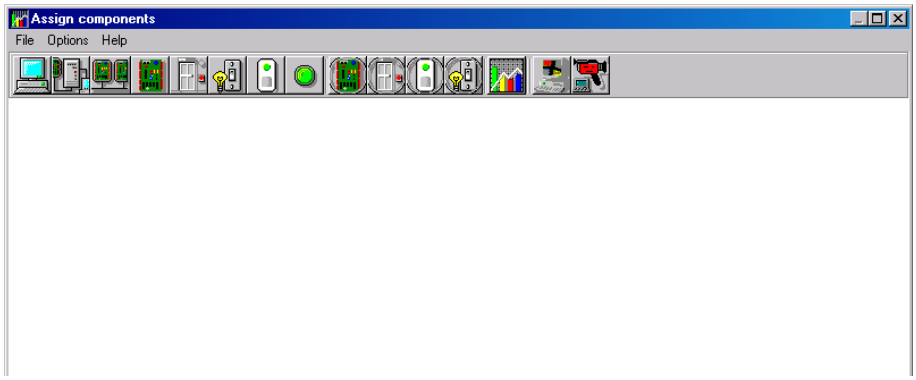


2 В выпадающем списке **Graphic** выбрать графическую схему, конфигурацию которой необходимо изменить, или нажать иконку **New** для создания новой.

3 Назначить для этой схемы новое имя (или изменить уже созданное).

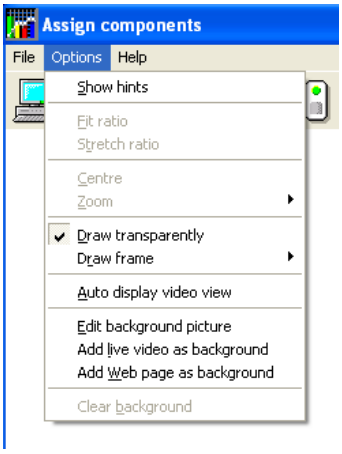
ПРИМЕЧАНИЕ. *При работе с уже созданной схемой и при создании новой все компоненты, прикреплённые к этой схеме, отображаются в левой части окна. В правой половине будет выведена сама графическая схема.*

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).



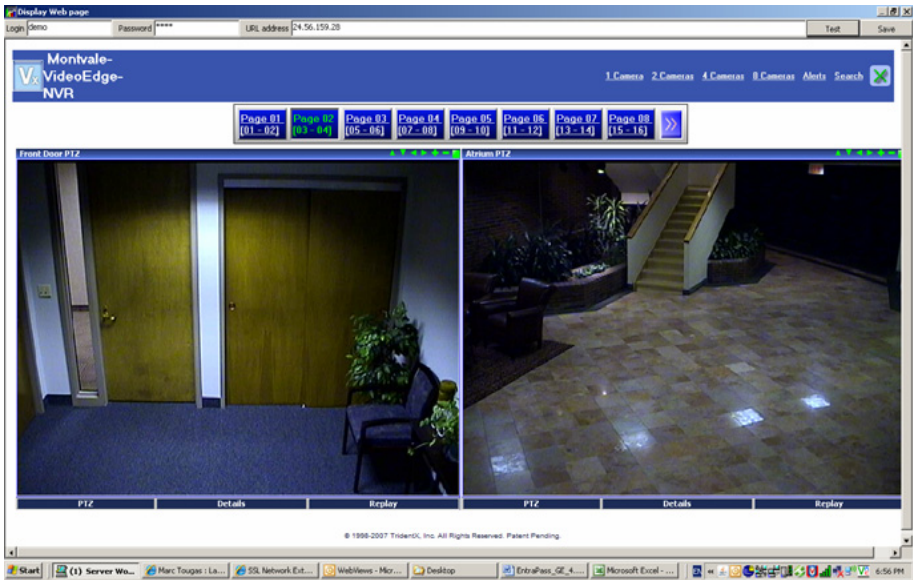
ПРИМЕЧАНИЕ. *Если в системе разрешено использование видеонаблюдения, то в меню Graphics добавляются видеокомпоненты. К этим видеокомпонентам есть доступ прямо со схемы. Если на графическую схему поместить иконку, то её статус будет отображаться при щелчке по иконке видеонаблюдения. Помимо стандартных функций предусмотрены следующие опции для определения статуса видеокомпонентов: статус подключения видеосервера, параметры видеосервера (в зависимости от изготовителя), статус камер наблюдения.*

5 Открыть меню **Options** (Опции) для выбора функций рисования. Активная функция отмечена флажком.

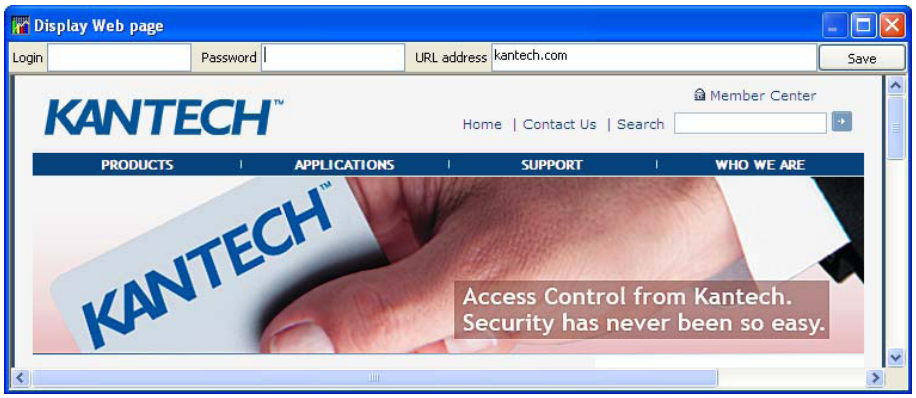


- **Show hints** (Выдавать подсказки) – отображать данные компонента (имя и адрес) при установке курсора мыши поверх изображения этого компонента.
- **Draw transparently** (Рисовать прозрачный объект) – поместить прозрачную иконку поверх фонового изображения.
- **Draw frame** (Рисовать рамку) – обвести 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.



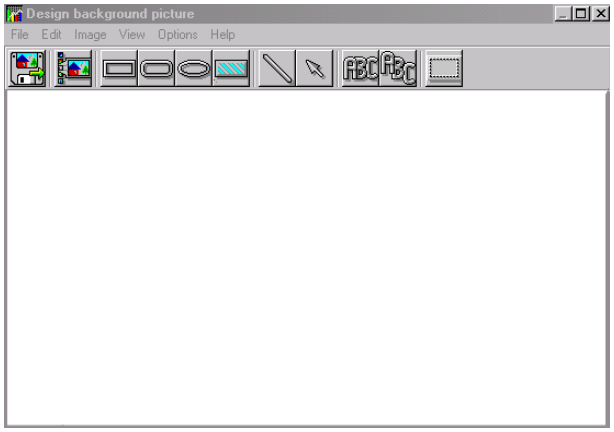
Выделить опцию **Add Web page as background** (Добавить веб-страницу, как фон), чтобы добавить на задний план веб-страницу. Для этого в поле **URL address** следует ввести адрес веб-сайта и нажать **Enter** (Ввод) на клавиатуре или нажать **Test** (Проверить). Если для доступа к веб-странице не требуется 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** (Создать фоновое изображение).

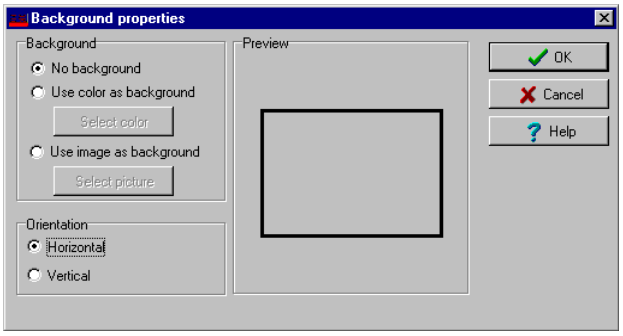


2 Использовать это окно для импортирования изображения, которое было создано в другом приложении или создать свой собственный фон при помощи инструментов для рисования.

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.



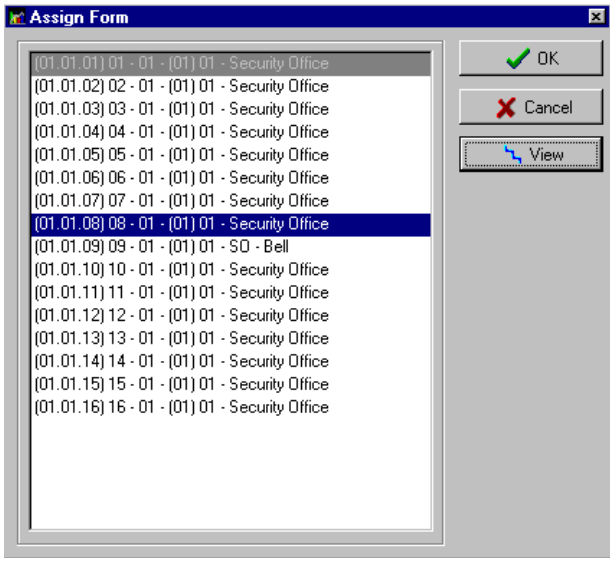
- Чтобы изменить фигуру, уже помещённую в редактируемое окно, следует щёлкнуть по ней правой кнопкой мыши, чтобы открыть меню Properties (Свойства), и внести необходимые изменения (цвет, расположение и пр.).
- Система может быть настроена таким образом, что меню Properties будет появляться сразу при 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 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.

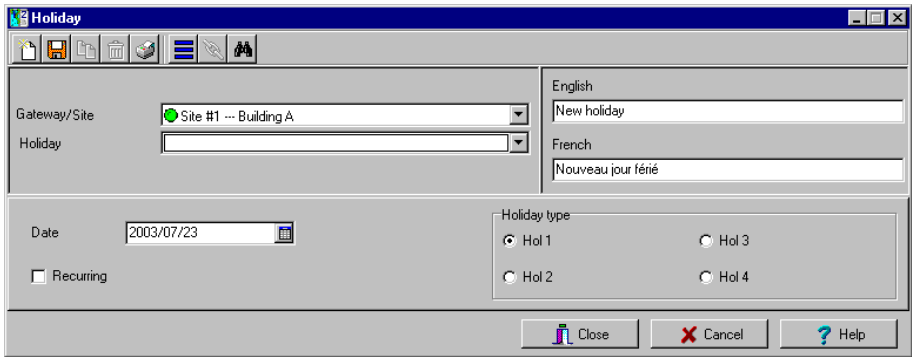
4 Нажать **OK**, чтобы вернуться в предыдущее окно.

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.*

Описание праздников (раздел Holidays)

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.).

1 Любой праздник можно отнести к одному из четырёх типов (Hol 1, 2, 3, 4). Один и тот же день может быть выходным на одном сайте и обычным рабочим днём на другом. В окне Definition (Описания) следует нажать на иконку **Holiday** (Праздники). На экране откроется окно Holiday.



2 Чтобы создать новый праздник, нажать кнопку **New** (Создать).

3 Для создания всеобщего праздника следует перейти сразу к следующему пункту. Чтобы создать праздник для определённого шлюза/сайта, 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.*

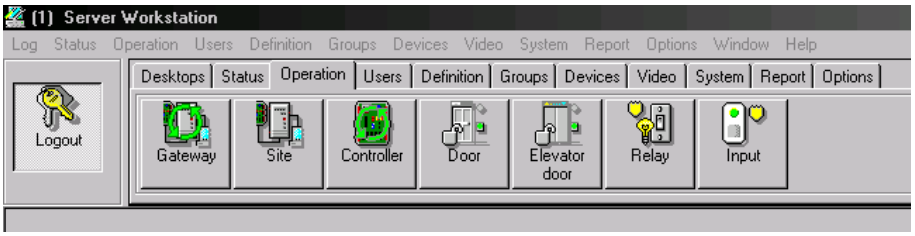
7 В разделе Holiday type (Тип праздника) указать тип описываемого праздника. Деление праздников на несколько типов повышает гибкость системы. Например, день благодарения можно назначить выходным днём для одной группы пользователей и рабочим днём для другой группы.

Глава 7 • Операции

Закладка **Operation** (Операции) содержит операции с различными компонентами системы (шлюзами, сайтами, контроллерами и т.д.), которые операторы могут выполнять в ручном режиме. Ручное управление можно при необходимости использовать для отмены расписаний или обработки специальных запросов. При выполнении операций с компонентов в ручном режиме управления у пользователя есть возможность просматривать статус выбранных компонентов в режиме реального времени. Кроме того, можно редактировать компоненты, обращаясь к ним напрямую из окна Operation.

Панель инструментов в окне Operation

Панель инструментов окна Operation (Операции) расположена в верхней части окна Workstation (Рабочая станция) и открывает доступ ко всем рабочим окнам (для работы со шлюзами, сайтами, контроллерами и т.д.), позволяя выполнять различные операции в режиме ручного управления, в частности, ручную перезагрузку или контроль работы устройств, отключение считывателей идентификационных карт и др.



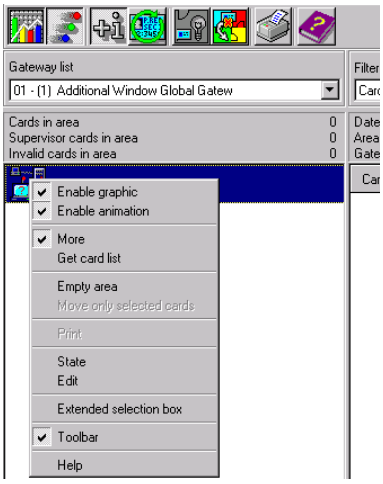
Панель инструментов в меню Operation

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



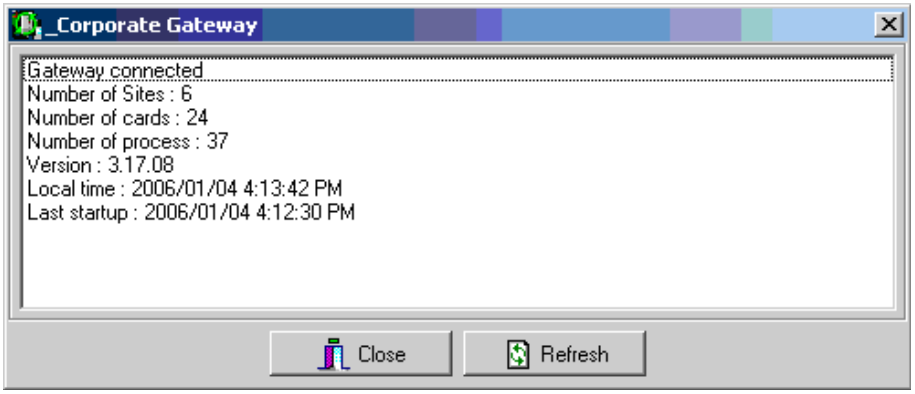
Чтобы вызвать контекстное меню, следует щёлкнуть правой кнопкой мыши в любом месте окна Operation.

Пункты контекстного меню соответствуют иконкам на панели инструментов в рабочем окне. Кроме того, при вызове контекстного меню в таких окнах, как Gateway, Site, Guard Tour State, в нём появляются три дополнительных функции:

- **State** (Статус) – вызов окна статуса, в котором содержится информация о компоненте, выбранном из списка. Подробнее смотрите раздел *"Меню статуса компонента" на стр. 206.*
- **Edit** (Редактировать) – вызов окна выбранного компонента для редактирования его данных.
- **Extended selection box** (Окно расширенного режима поиска) – окно для поиска определённого компонента.

Окно статусов компонентов (Status)

Окно, содержащее информацию о шлюзе и сайтах, открывается с помощью функции **Status** (Статус) в контекстном меню, для вызова которого следует щёлкнуть правой кнопкой мыши в соответствующем рабочем окне под закладкой **Operation** (операции).



В приведённом выше примере окно содержит сведения о шлюзе Corporate Gateway. Перечислим основные сведения, которые могут отображаться в этом окне:

Параметр	Описание
Gateway (Статус шлюза)	Показывает, есть подключение шлюза к сети или нет.
Number of sites (Число сайтов)	Показывает число сайтов для этого шлюза.
Number of cards (Число идентификационных карт)	Показывает число карт, обрабатываемых этим контроллером.
Number of processes (Число процессов)	Показывает число процессов.
Version (Версия)	Отображает версию программного и аппаратного обеспечения.
Local Time (Местное время)	Показывает текущее местное время контроллера.
Last startup (Последний запуск)	Отображает дату последнего запуска системы.

ПРИМЕЧАНИЕ. *Информация, отображаемая в окне статуса, соответствует конфигурации системы и зависит от того, из какого окна в меню Operations был сделан запрос (шлюза или сайта).*

Операции со шлюзом при работе в ручном режиме

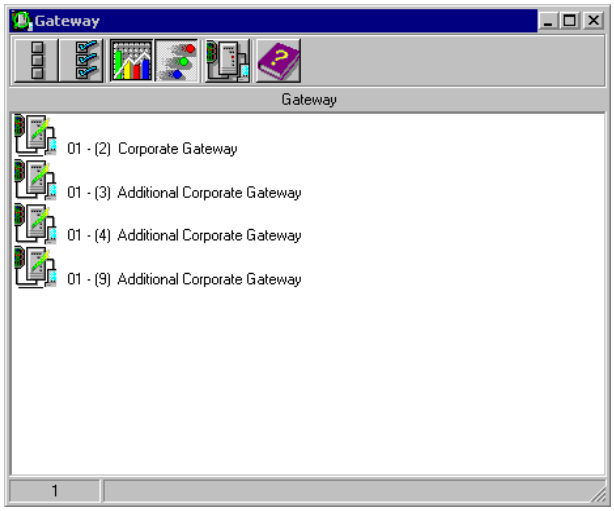
Ручной режим работы со шлюзом позволяет операторам обращаться к шлюзам для обновления и перезагрузки данных.

Кнопка	Описание
	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. Более подробная информация приведена в разделе *"Техническая поддержка" на стр. 6.*
	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.

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** (Операции) и нажать кнопку **Gateway** (Шлюза), чтобы открыть меню шлюза, содержащее все подключённые к системе шлюзы.



ПРИМЕЧАНИЕ. *Описание иконок в окне Gateway (Шлюз) приведено в главе 17 "Сайты и шлюзы" на стр. 548.*

Выполнение жёсткой перезагрузки

ПРИМЕЧАНИЕ. *Команды перезагрузки следует применять с осторожностью. Перед перезагрузкой контроллера рекомендуется проконсультироваться со службой технической поддержки. Более подробная информация приведена в разделе "Техническая поддержка" на стр. 6.*

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 полученные данные и пересылает их на все сайты и контроллеры.

ПРИМЕЧАНИЕ. *Во время выполнения повторной загрузки связь с контроллерами временно прерывается.*

1. Выбрать шлюз, требующий повторной загрузки данных.
2. Нажать кнопку **Reload data** (Повторно загрузить данные). Данные шлюза будут обновлены.

Операции с сайтами при работе в ручном режиме

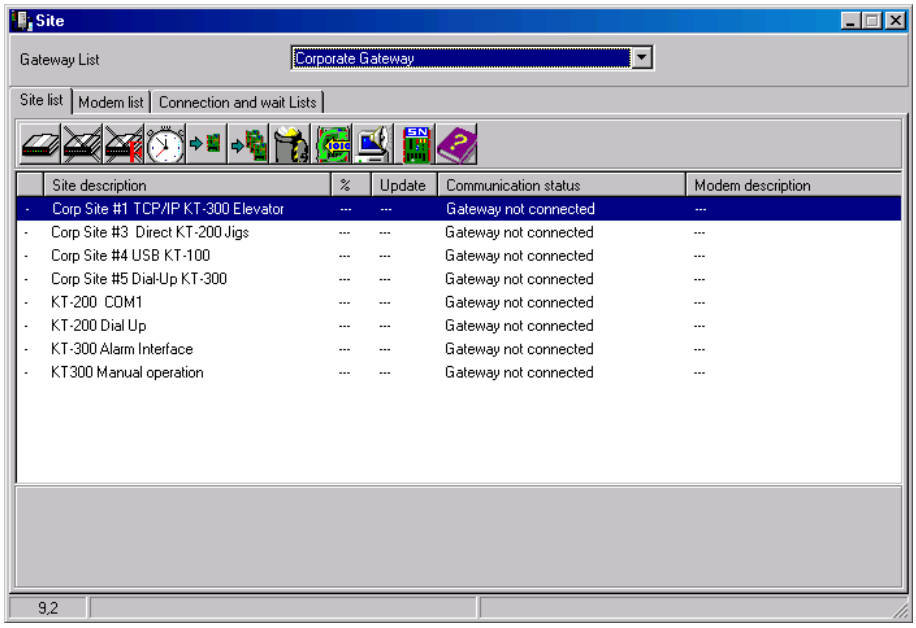
Режим ручного управления сайтами используется для опроса неприкреплённых к ним контроллеров. Например, если контроллер был добавлен в систему без указания серийного номера, то при помощи этой команды можно получить его серийный номер.

Кнопка	Описание
	Connect to remote site (Соединение с удалённым сайтом) – служит для подключения к удалённому сайту при помощи предварительно настроенного соединения по коммутируемой линии.
	Disconnect remote site (Отключение от удалённого сайта) – служит для **завершения** соединения между этой рабочей станцией EntraPass и удалённым сайтом.
	Force disconnect site (Принудительное разъединение) – 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) – служит для подключения к выбранному сайту и обновления его параметров.
	Update all remote sites (Обновить все удалённые сайты) – служит для подключения и обновления параметров на всех сайтах, начиная с первого сайта в списке.
	Remove site from connect and wait list (Исключить сайт из списка соединений) – прекратить соединение с выбранным сайтом после того, как все сайты будут 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 типа Secure IP (KT-400).

ПРИМЕЧАНИЕ. *Как правило, при наведении курсора на пиктограмму появляется текстовая подсказка. Она содержит подробные сведения о выполняемой операции.*

Выполнение операций с сайтами при работе в ручном режиме

1 В окне **Operation** (Операции) нажать иконку **Site** (Сайт), чтобы открыть окно Site. Выбрать шлюз, к которому подключен сайт.



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 сайта, он отправит на рабочий стол сообщений (Message) сообщение-подтверждение связи.

3 Оператор может посмотреть серийный номер контроллера на рабочем столе Message.

ПРИМЕЧАНИЕ. *В колонке % отображается эффективность связи с выбранным сайтом. Если эта величина невелика (например, ниже 75%), то это может указывать на плохое качество связи с сайтом. Проблемы со связью могут быть вызваны различными причинами, например, воздействием электромагнитных помех, повреждением соединительных кабелей и т.п.*

Сообщения о статусе соединения, доступные в списке меню

Сообщения в списке диалогового меню отображают статус соединения с сайтом. В примере, показанном ниже, перечислены сообщения о статусе соединения со шлюзами Corporate Gateway.

Сообщение	**Описание**
Site Communication OK (Связь с сайтом в порядке)	Все контроллеры сайта поддерживают связь со шлюзом.
Site Communication Trouble (Проблемы со связью на сайте)	Хотя бы у одного из контроллеров сайта нет связи со шлюзом.

Сообщение	Описание
Site Communication Failure (Нет связи с сайтом)	Нет связи между контроллерами сайта и шлюзом.
Site Communication Cannot be Opened (Невозможно установить связь с сайтом)	Шлюз не может открыть порт связи.

Операции с контроллерами при работе в ручном режиме

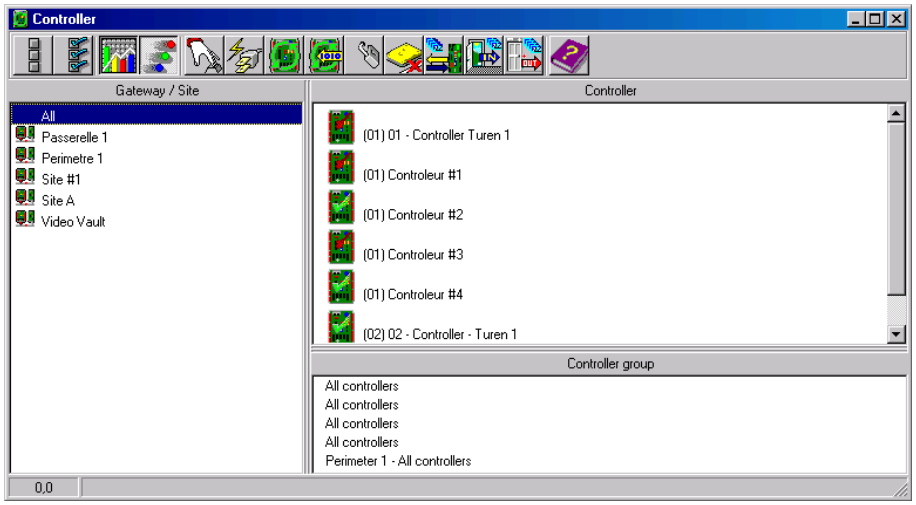
Это меню служит для выполнения различных операций по повторной загрузке и перезагрузке контроллера, а именно для мягкой и жёсткой перезагрузки, повторной загрузки и обновления прошивки.

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. Более подробная информация приведена в разделе *"Техническая поддержка" на стр. 6.*
	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-100, KT-300).
	Unlock reader keypad (Разблокировать клавиши считывателя) – позволяет разблокировать клавиши считывателя карт на контроллерах KT-100.
	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) выбрать шлюз или сайт. Контроллеры, присоединённые к этому шлюзу/сайту, 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 только один сайт или шлюз, панель со списком сайтов или шлюзов 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. Более подробная информация приведена в разделе "Техническая поддержка" на стр. 6.*

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 типа KT-100 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 снимать с блокировки клавиши считывателя идентификационных карт в системах с контроллерами KT-100, обращаясь к ним с рабочей станции.

1 В меню Controller (Контроллер) выделить нужный контроллер или группу контроллеров.

2 Нажать на панели инструментов кнопку **Unlock reader keypad** (Разблокировать клавиши считывателя).

Сброс счётчиков карт внутри и вне охраняемой территории или всех карт в локальной зоне контроля

Эта функция обнуляет счётчики идентификационных карт внутри и вне охраняемой территории.

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) 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** (Найти 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 входящих и выходящих посетителей или всех карт в локальной зоне контроля

Эта функция обнуляет счётчики идентификационных карт на входе и выходе.

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.

Операции с дверями при работе в ручном режиме

Это меню позволяет авторизованному оператору вручную изменять статус 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 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 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) – поставить дверь на охрану, то есть заблокировать дверь и активировать охранную панель, чтобы никто не мог войти в здание или в помещение.
	Disarm door (Снять дверь с охраны) – снять охрану, 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 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 (Операции), 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 статус двери.

- На панели слева показан список всех сайтов/шлюзов под заголовком **Sites/Gateways**. Выбрать все или один сайт/шлюз.
- Отдельные двери, прикреплённые к сайту/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 или шлюзов не будет отображаться в окне контроллеров.*

- Группы дверей, 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 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.

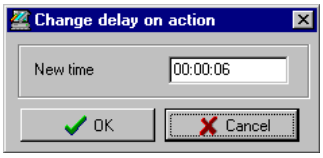
Временная разблокировка двери

Система EntraPass позволяет временно снять с блокировки дверь на определённый срок. После окончания времени задержки дверь будет снова автоматически заблокирована. Эту функцию можно использовать для предоставления доступа посетителям, которые не имеют идентификационной карты или забыли её дома.

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 контактный датчик двери, то дверь будет снова заперта сразу после получения сигнала о переходе из открытого состояния в закрытое. Для этой операции не предусмотрено никакой анимационной картинки.*

Перезагрузка расписания двери

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.

WARNING: Your life safety system has components linked via a regular cable. However, cable transport mediums, such as, but not limited to, external networking or wireless alternatives, if in place, are not SOP (NORM) PRODUCT so fall as partners as expected.

Операции с дверями лифтов при работе в ручном режиме

В ручном режиме управления операторы, обладающие необходимыми полномочиями, могут вручную ставить и снимать блокировку, в том числе временно. Это окно также отображает в режиме реального времени статус выбранной двери лифта.

Получение доступа к лифту

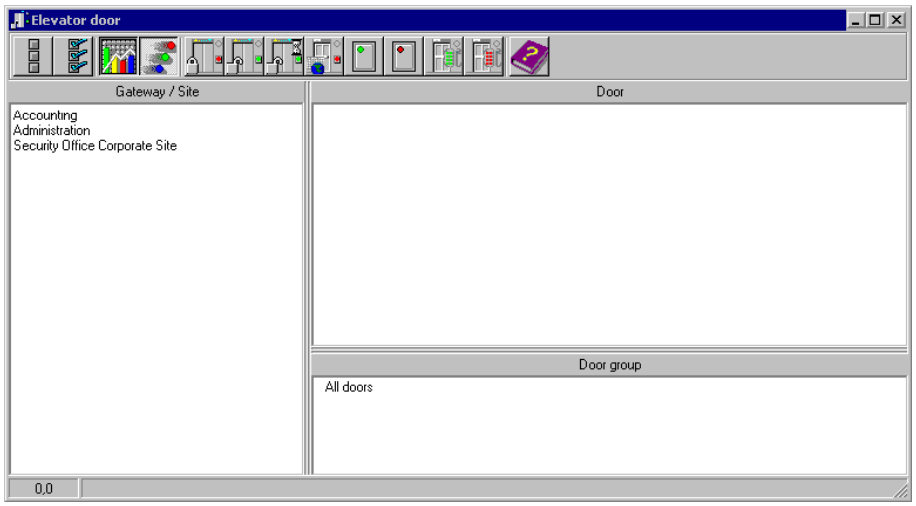
- Владелец карты нажимает кнопку "вверх-вниз". Двери лифта открываются.
- Владелец карты предъявляет свою карту считывателю (обычно уже в лифтовой кабине).
- Система проверяет, достоверно ли расписание, назначенное для указанной двери. Если да, выполняется проверка, какая группа этажей имеет привязку 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 заблокирован.
	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 из лифта) – 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** (Операции) нажать иконку **Elevator Door** (Двери лифта).



2 Нажать на кнопку **Enable animation** (Разрешить анимацию), чтобы в режиме реального времени отображался статус двери лифта.

- На панели слева показан список всех сайтов/шлюзов под заголовком **Sites/Gateways**. Выбрать все или один сайт/шлюз.
- Отдельные двери лифта, прикреплённые к сайту/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/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.

Блокировка доступа на этажи через двери лифта

1 Выбрать одну дверь лифта или целую группу.

2 Нажать на панели инструментов кнопку **Lock** (Заблокировать). Эта команда позволяет вручную заблокировать 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 доступа на этажи 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 в колонке “State” (Статус) в меню Floor group Definition (Описание группы этажей). В таком случае 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, 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 (Статус). 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.*

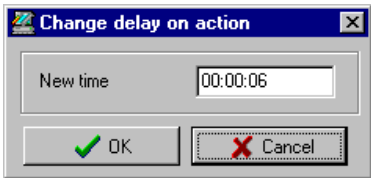
Временная разблокировка доступа на этажи через двери лифта

Система EntraPass позволяет разблокировать доступ на этаж через двери лифта на установленный срок. После окончания времени задержки дверь лифта будет снова автоматически заблокирована.

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**. 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 (Описание 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).*

Перезагрузка 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 из 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, на которые раньше не было доступа.

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** (Запретить 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 статуса 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 (Операции) 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/шлюзов под заголовком **Sites/Gateways**. Выбрать все или один сайт/шлюз.
- Отдельные реле, прикреплённые к сайту/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/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

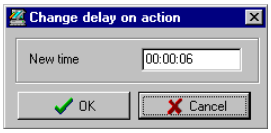
1 Выделить реле (одно или группу).

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**. 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

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 при работе в ручном режиме

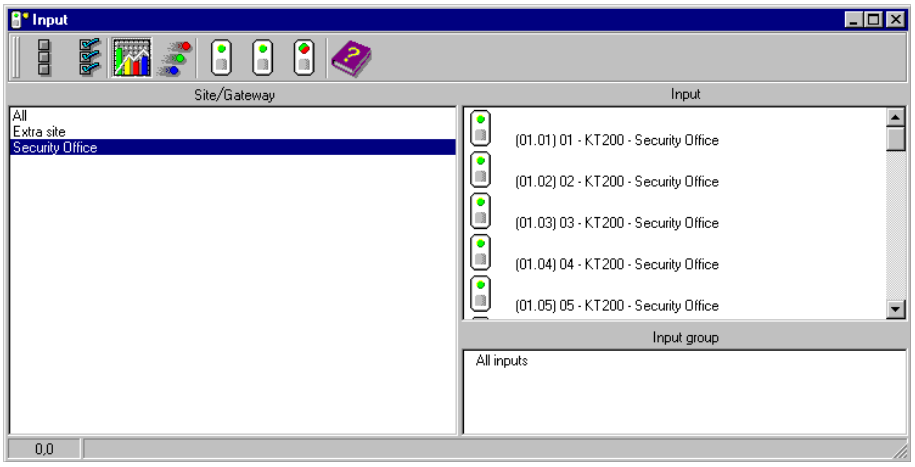
Этот раздел меню позволяет вернуть вход в нормальное состояние, прекратить мониторинг входа, выполнять мониторинг статуса определённого входа постоянно или временно шунтировать выбранный вход, если его статус, описанный в меню Device, перед этим изменился.

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 (Операции) 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/шлюзов под заголовком **Sites/Gateways**. Выбрать все (**All**) или один сайт/шлюз.

- Отдельные входы, прикреплённые к сайту/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.

Ручной возврат входа в нормальное состояние

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).

Прекращение мониторинга входа

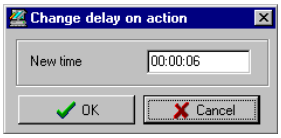
Эта команда используется для отмены мониторинга входа, независимо от его расписания (если оно настроено).

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 и нажать **OK**. Пиктограмма рядом со входом будет указывать, что его мониторинг временно отключён. В случае возникновения тревоги или физического отсоединения этого входа сообщения на рабочий стол сообщений (Message) отправляться не будут.

WARNING: Unauthorized use of this copyright material is prohibited. Subject to Intellectual Property Protection Laws, and Acts by, but not limited to, unauthorized transmitting or electronic distribution, it is prohibited. Use for this PRODUCT is not to exceed the supplied.

Глава 8 • Пользователи

Меню **Users** (Пользователи) служит для работы с базами данных по владельцам идентификационных карт. Панель инструментов в окне **Users** служит для вызова следующих функций:

- Описание 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 организация групп доступа для идентификационных карт;
- Задание уровней доступа;
- Создание шаблонов для карт посетителей;
- Описание типов карт;
- Описание и выпуск разовых пропусков;
- Изменение групп 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, чтобы использовать идентификационные карты для создания электронных пропусков.

Описание карт (раздел Card)

При описании карт необходимо указать следующие параметры: номе карты (card number), имя владельца (cardholder name), тип карты (card type), уровень доступа (access level) и статус (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) (смотрите раздел "Описание формата представления идентификационных карт" на стр. 444), то у каждой карты можно индивидуально изменить формат в меню Card (Карты). Эта опция повышает гибкость системы при использовании идентификационных карт на сайтах, 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.

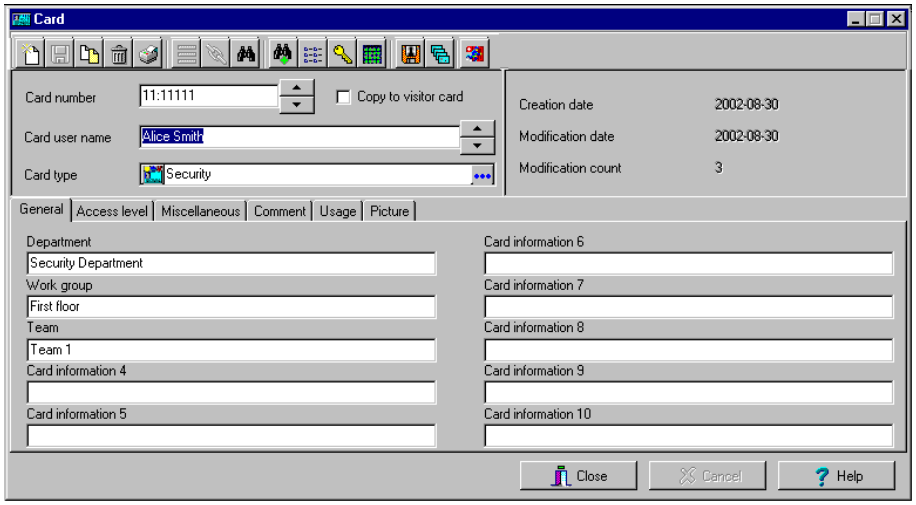
Если в меню System parameters (Системные параметры) отмечена флажком опция **Enhanced user management** (Усиленное администрирование пользователей) (смотрите раздел "Настройки регистрационных данных" на стр. 469), то описание карты будет незначительно отличаться. При использовании этого типа администрирования 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 статусу (действительная, недействительная, отложенная, потерянная/украденная).

Данные карт 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** (Усиленное администрирование пользователей), то следует перейти к следующему разделу "Выпуск новой карты в режиме усиленного администрирования пользователей" на стр. 231.*



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 разделе "Описание типов карт" на стр. *286*.

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.*

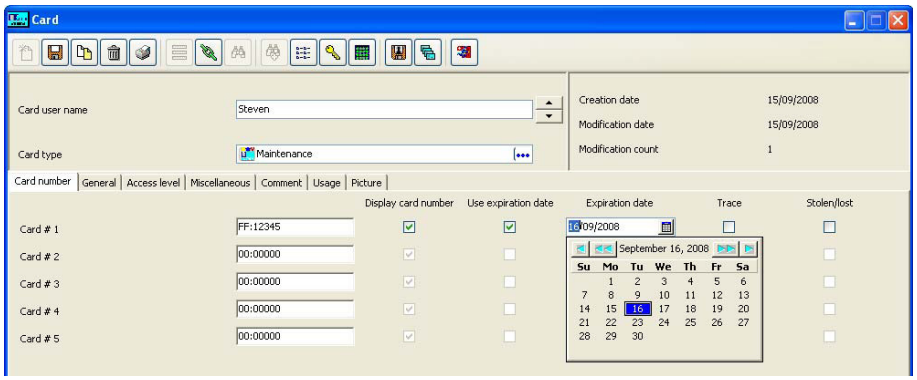
7 Заполнить поля **Card Information 1 ... 10**. Это поля для ввода информации о пользователе. Они служат для хранения дополнительных сведений о владельце карты. Например, поле №1 (Card Information 1) можно использовать для указания номера трудового договора, в поле №2 (Card Information 2) записать отдел, 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 усиленного администрирования пользователей

1 В меню **Users** (Пользователи) нажать на иконку **Card** (Идентификационные карты). Открывшееся окно Card служит для ввода/проверки основной информации о владельце карты.



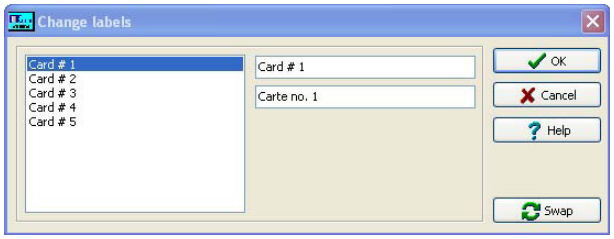
2 Нажать на панели инструментов кнопку **New** (Создать). В поле **Card user name** (Имя пользователя карты) ввести имя владельца карты. Допускается ввод имени длиной до 50 символов.

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 приведена в разделе "Описание типов карт" на стр. 286.

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.

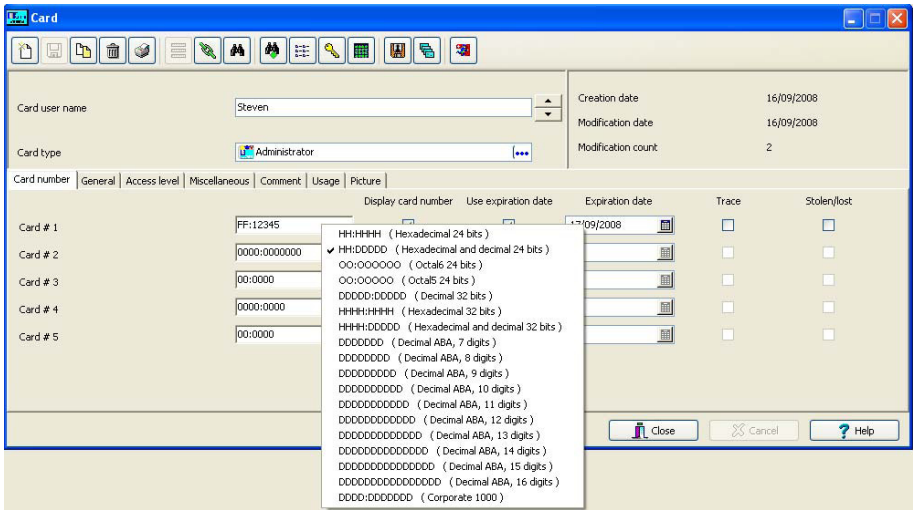


6 В поле **Card number** указать номер карты.

- Если система настроена на работу с разными форматами карт, то формат выбранной карты можно изменить нажатием на правую кнопку мыши в поле **Card number**, (смотрите раздел "Описание формата представления идентификационных карт" на стр. 444), а также можно использовать несколько форматов карт и выбрать новый формат по умолчанию для карт №1...№5. Используемый по умолчанию формат карты – HH:DDDDD (шестнадцатеричный и десятичный 24-разрядный).

ПРИМЕЧАНИЕ. *Уровень доступа (**Access Level**) применяется к пользователю, то есть ко всем его пяти картам.*

- **Если используется несколько форматов карт (Multiple Card Format).** Список всех карт отображается при нажатии на правую кнопку мыши в поле Card number.
- **Если формат карты был введён 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 пользования конкретной картой, 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.

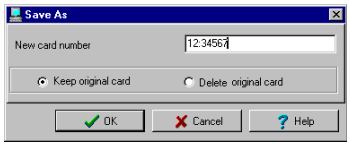
11 Выделить поле **Stolen/Lost** (Потеряна/Украдена), если карта была потеряна или украдена. Такая карта больше не будет функционировать.

12 Повторить пп. 5 ... 11 для карт **Card #2 ... Card #5**, если необходимо. Перечисленные параметры могут различаться для этих пяти карт.

ПРИМЕЧАНИЕ. *Остальные параметры в меню Card отображаются независимо от того, включён режим Enhanced user management или нет. Приведённые ниже разделы руководства проиллюстрированы на примере обычного режима работы с картами пользователей (без отображения закладки Card Number).*

Создание новых карт с помощью функции "Сохранить как..."

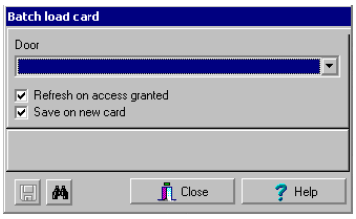
Функция **Save as** (Сохранить как...) позволяет создавать новые карты, используя уже выпущенную карту, путём внесения необходимых изменений. Например, можно изменить только имя пользователя, и оставить неизменными все остальные данные.



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.*

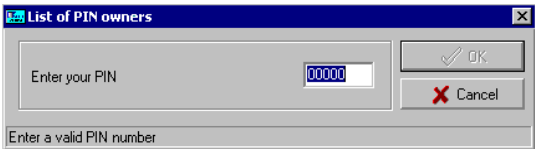
Просмотр и проверка индивидуальных кодов

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

Изменение 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 архивных данных карты

ПРИМЕЧАНИЕ. *Более подробная информация приведена в разделе "Поиск компонентов" на стр. 50.*

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.

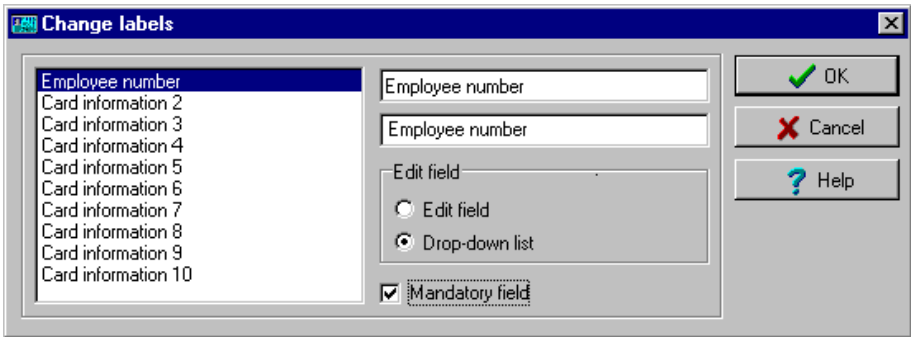
2 Нажать кнопку **Delete** (Удалить) и в появившемся окошке с предупреждением (**Warning message**) выбрать **Yes** (Да).

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.*

Задание 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.

Подробные сведения по заданию уровней доступа смотрите *в разделе "Задание уровней доступа" на стр. 284.*

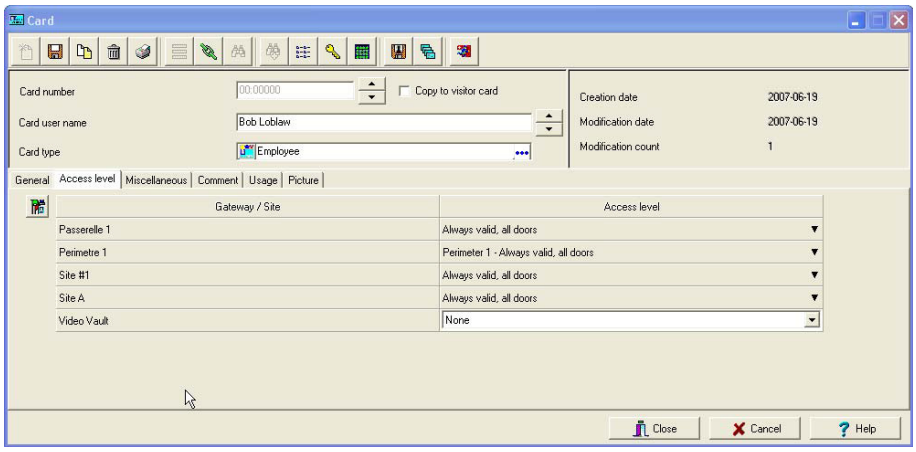
ПРИМЕЧАНИЕ. *Если изменить уровень доступа, который назначен для выбранной карты, то у пользователя карты изменится уровень доступа к дверям и изменятся расписания, связанные с этим уровнем доступа.*

Уровень доступа назначается для карты в следующем порядке:

- Создать расписания в соответствии со временем предоставления пользователю доступа к выбранным дверям;
- Назначить созданное расписание для выбранных дверей (в меню задания уровня доступа);
- Назначить для карт уровень доступа.

Задание 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), 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 и шлюзов, которым будет назначен уровень доступа.

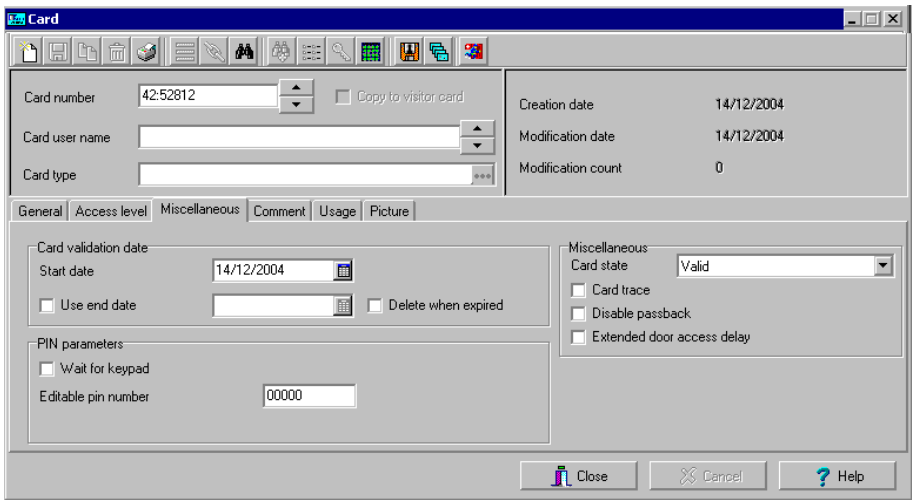
3 В списке **Access level** (Уровни доступа) выбрать уровень доступа владельца карты к дверям указанного сайта. Если владелец карты не должен иметь доступ к двери этого сайта, в этом поле следует указать **None** (Отсутствует).

ПРИМЕЧАНИЕ. *Чтобы в списке **Access level** (Уровни доступа) отображались уровни доступа, их следует создать в меню **Users** > **Access Level**.*

Описание дополнительных функций 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”.

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; а 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** > **Doors**). Кроме того, расписание действия кнопочной панели для этой двери должно быть достоверным. Более подробные сведения по настройке дверей изложены в разделе "Конфигурация дверей" на стр. 127.*

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,
- **Expired** (Просрочена) – карта с прошедшим сроком действия,
- **Pending** (Отложенная) – карта ещё не действует.

ПРИМЕЧАНИЕ. *Статус **Pending** (Отложенная) невозможно выбрать в списке **Card state** (Статус карты). Для этого следует изменить дату начала действия карты (Start date).*

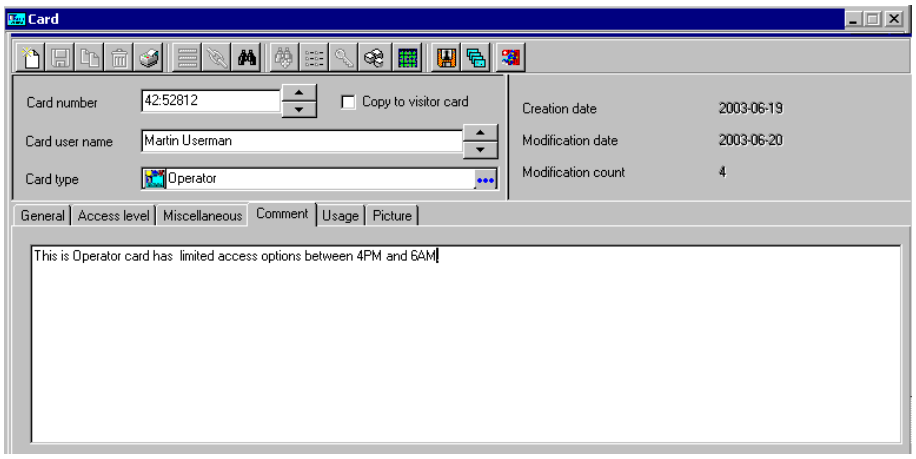
6 Отметить опцию **Card trace** (Отслеживать карту), если необходимо отслеживать пользование этой картой. При выделении этой опции каждое предъявление карты считывателю будет сопровождаться созданием события “Card traced” (Карта отслежена). По этим событиям можно, например, составить отчёт и отследить действия владельца карты.

7 Выделить опцию **Disable passback** (Запрет повторного прохода), если необходимо запретить для этой карты повторный проход, разрешённый 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.*

Добавление комментариев к карте

1 В окне Card (Карты) открыть закладку **Comment** (Комментарии).



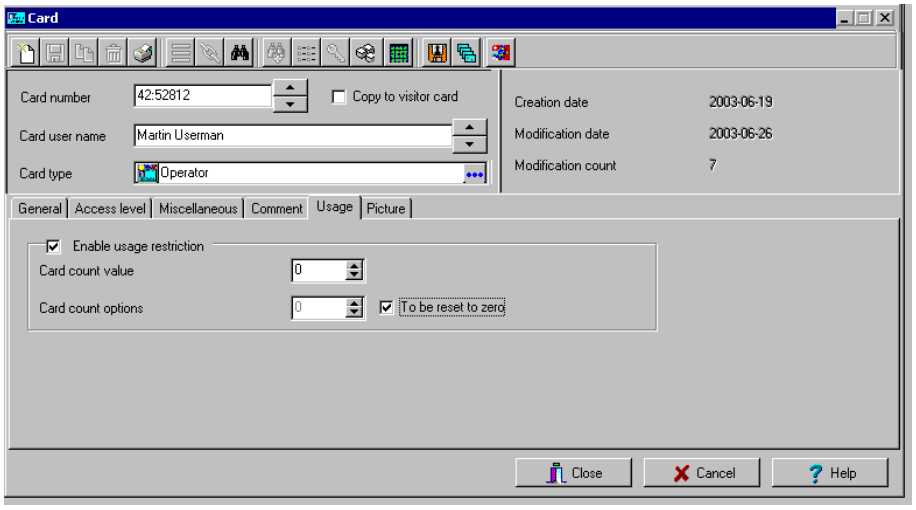
2 При необходимости ввести комментарий о владельце карты. Это поле служит для хранения в базе данных дополнительных сведений. Максимальная допустимая длина – 241 символов.

3 Нажать **Save** (Сохранить) и затем **Close** (Закрыть).

Ограничение числа использований карты

Система EntraPass позволяет 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.

ПРИМЕЧАНИЕ. *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.*

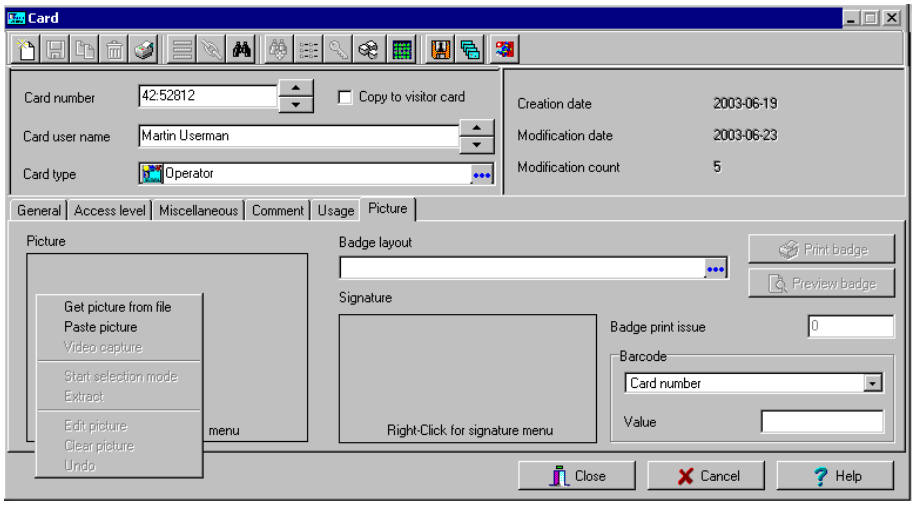
Привязка к картам фотографий и подписей

Система даёт возможность создавать связи между фотографиями с подписями и владельцами карт, а также использовать шаблоны для создания карт и изготовления 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.

Импортирование фотографии из файла

1 В меню Card (Карты) открыть закладку **Picture** (Изображения).



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.
- Paste picture (Вставить изображение из буфера) – для использования этой опции следует скопировать изображение в буфер и затем вставить его в это окно.

ПРИМЕЧАНИЕ. *Функция оцифровки видеоизображений доступна только при условии установки устройства оцифровки видеоизображений.*

3 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).

ПРИМЕЧАНИЕ. *Поддерживаются следующие форматы файлов: BMP, EMF, WMF, JPG, GIF, PNG, PCD и TIF.*

4 Выбрать путь для сохранения изображения. Выделить искомое изображение, нажать кнопку **Open** (Открыть), чтобы импортировать его в окно **Card** (Карты).

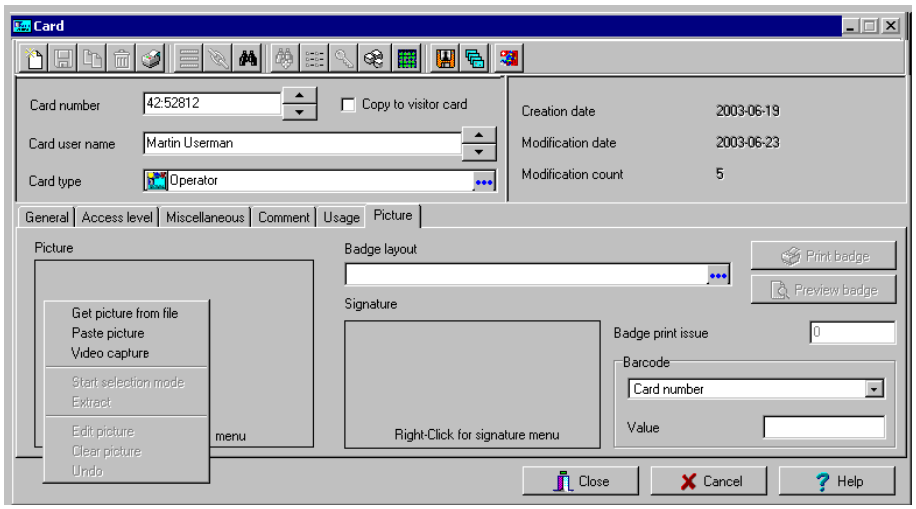
ПРИМЕЧАНИЕ. *Чтобы удалить импортированное изображение, следует щёлкнуть по нему правой кнопкой мыши, и выбрать в контекстном меню команду **Clear picture** (Удалить изображение).*

Получение фотографии с видеокамеры

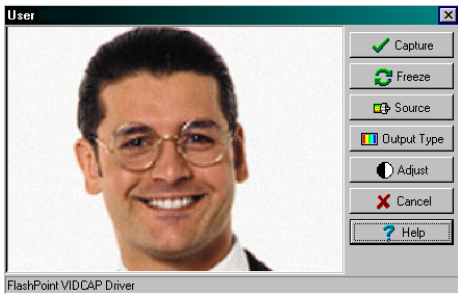
Функция оцифровки изображений доступна только при условии, что в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > закладка **Video** выделена опция **Enable video capture** (Разрешить оцифровку изображений).

ПРИМЕЧАНИЕ. *Перед оцифровкой изображений, полученных с видеокамеры необходимо правильно настроить всё оборудование. Более подробные сведения приведены в руководстве. При наличии двух и более видеосерверов следует указать, какой видеосервер 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 видеосерверов следует указать, какой видеосервер нужно использовать. Более подробные сведения по настройке видеодрайверов смотрите в разделе "Конфигурация мультимедийных устройств" на стр. 452.*

3 Нажать кнопку **Freeze** (Остановить) на понравившемся изображении, затем нажать кнопку **Capture** (Захватить), чтобы вставить и сохранить изображение на экране.

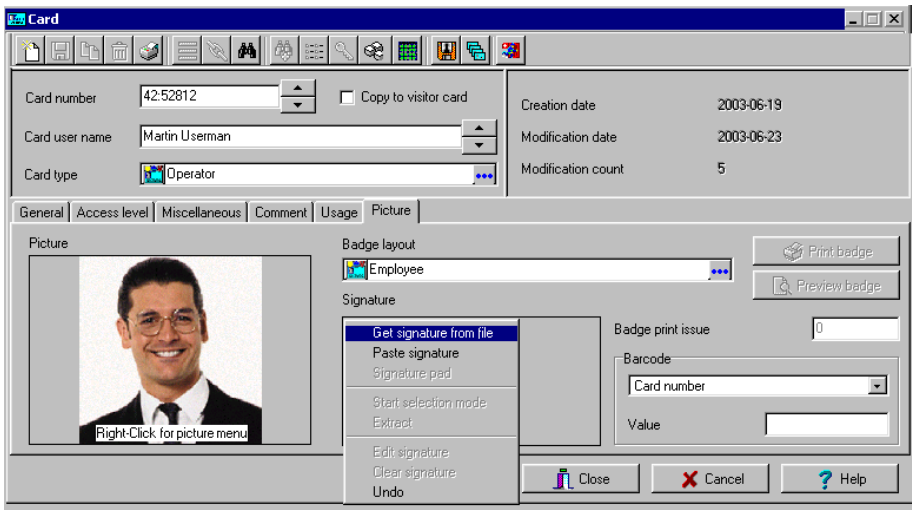
4 Для указанной карты выбрать макет электронного пропуска из списка **Badge layout** (Макет электронного пропуска). Подробные сведения по описанию макета смотрите *в разделе "Создание электронных пропусков" на стр. 253.*

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).

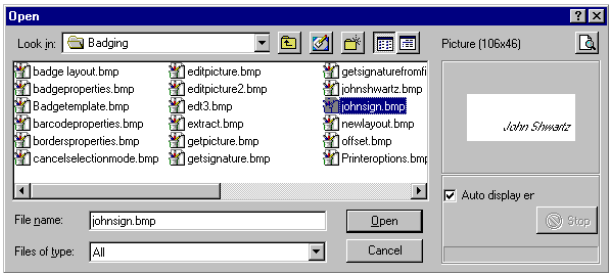
1 В меню Card (Карты) щёлкнуть по области подписи правой кнопкой мыши. Откроется контекстное меню.



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.*

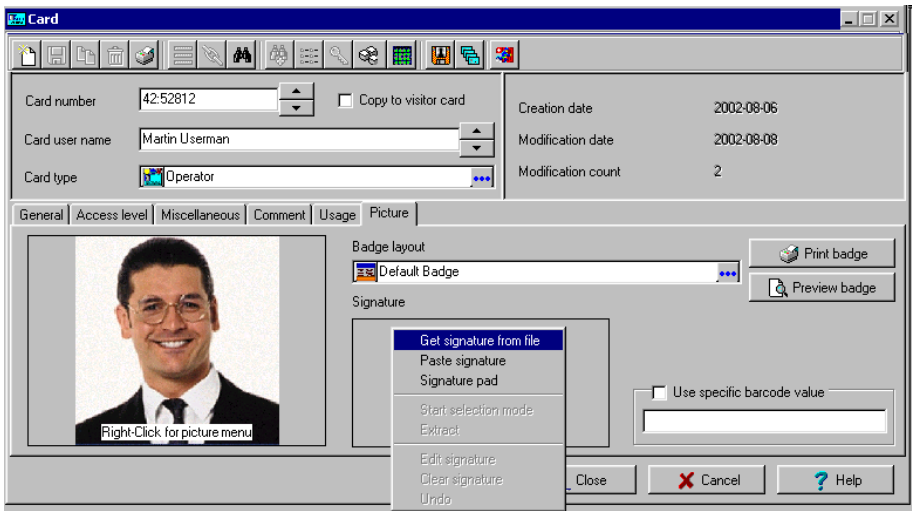


3 Выбрать файл с подписью, нажать **Open** (Открыть).

Добавление подписи с помощью устройства оцифровки подписей

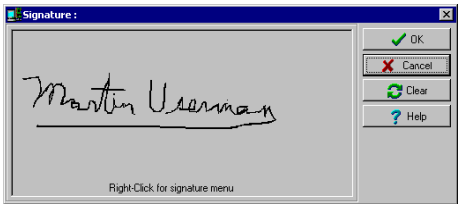
Чтобы воспользоваться этой функцией, необходимо установить и правильно настроить устройство оцифровки подписей. Устройство ввода подписей становится доступным только после того, как в меню **Options** (Опции) > **Multimedia devices** (Мультимедийные устройства) > **Signature** (Подпись) будет указано 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 "Card".



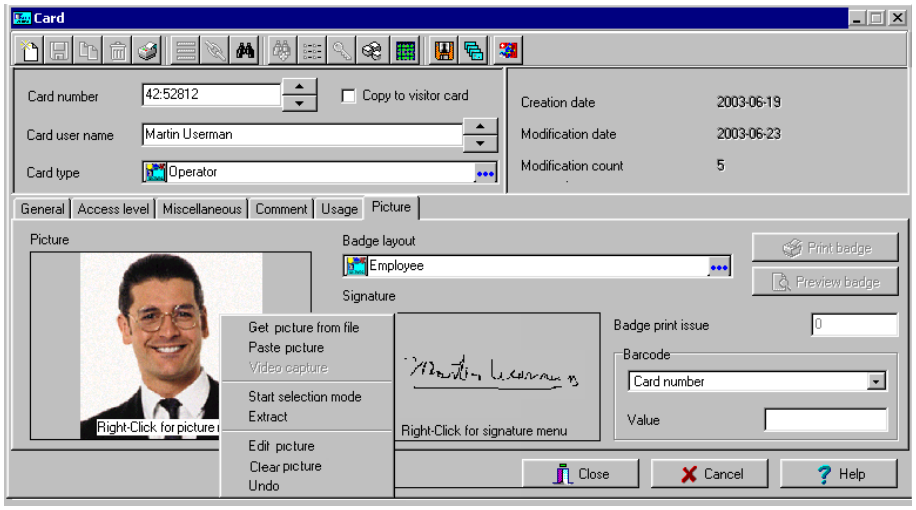
Работа с фотографиями и подписями

Встроенная функция изготовления электронных пропусков EntraPass Integrated Badging позволяет извлекать часть изображения или улучшать изображения, предназначенные для оформления идентификационных карт.

Вырезание части изображения

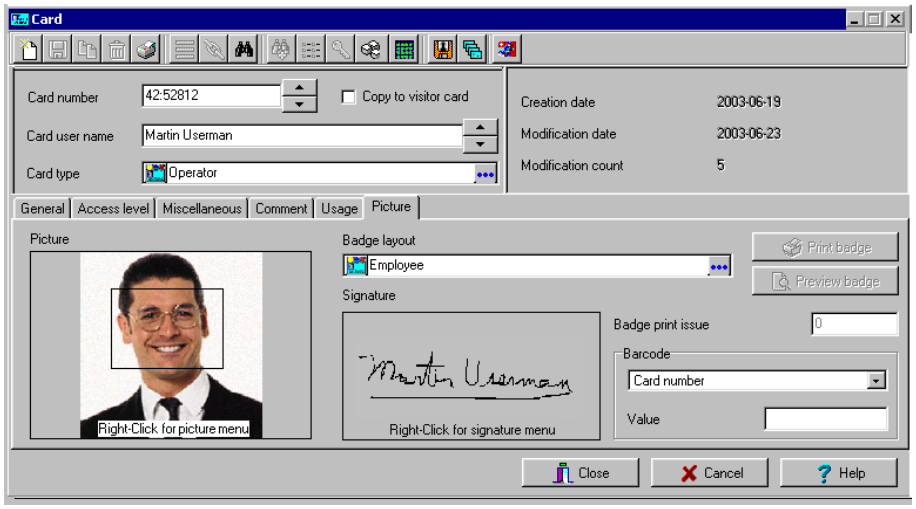
Если для оформления идентификационной карты пользователя требуется обрезать изображение (фотографию или подпись), содержащее избыточную информацию, и оставить только важные детали, то это можно сделать при помощи функции Extract.

1 Щёлкнуть правой кнопкой мыши по только что вставленному изображению.



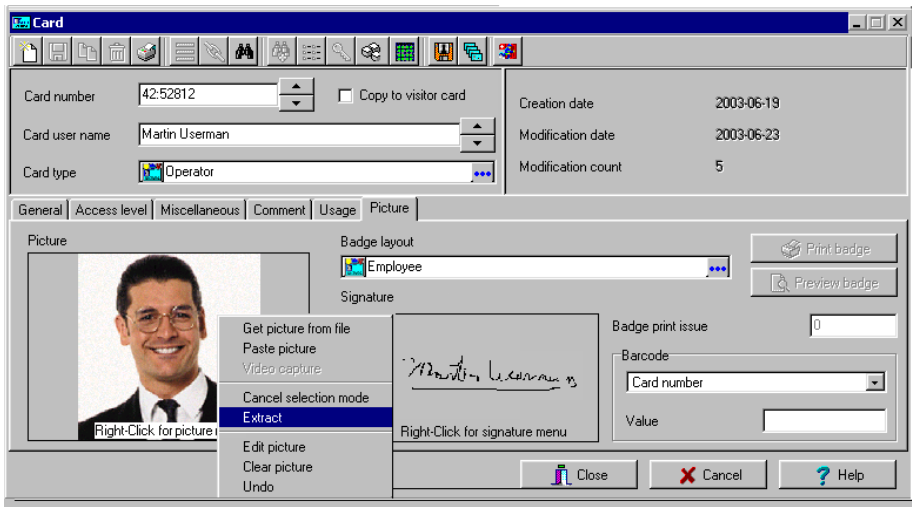
ПРИМЕЧАНИЕ. *Функция* ***Extract*** *(Извлечь) доступна сразу после перехода в режим выделения изображения (функция* **Start selection mode***). Аналогично, функция* ***Undo*** *(Вернуться назад) доступна только сразу после вставки изображения.*

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.

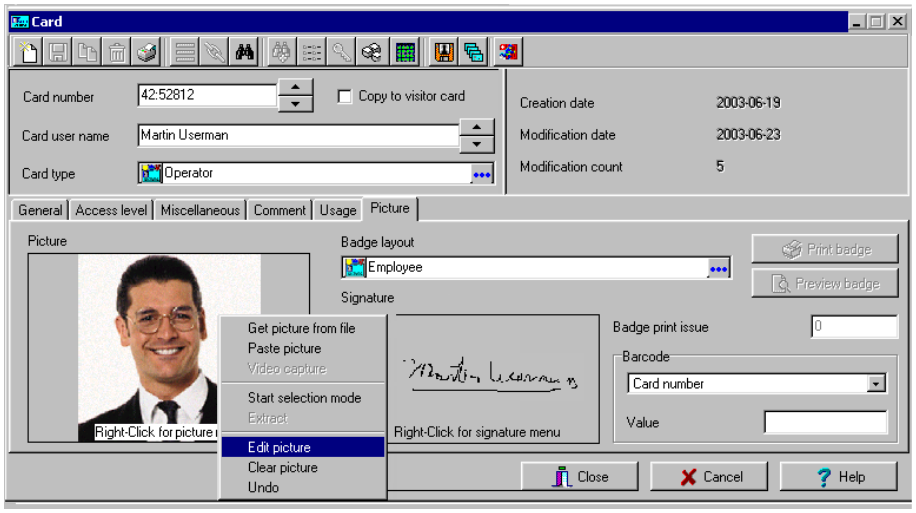


ПРИМЕЧАНИЕ. *Чтобы отменить выделение, нажать на правую кнопку мыши и выбрать в контекстном меню пункт* ***Cancel selection mode*** *(Отменить режим выделения). Выбрать пункт* ***Undo*** *(Вернуться назад) для отмены изменений. Функция* ***Undo*** *доступна только после вставки изображения.*

4 В контекстном меню выбрать функцию **Extract** (Извлечь).

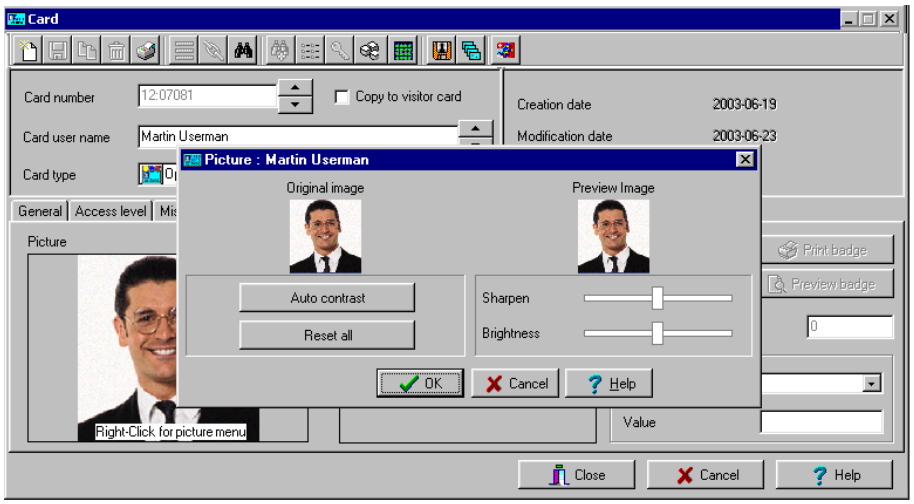
Редактирование фотографии/подписи

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 **Picture**.

5 Выбрать макет электронного пропуска из списка Badge layout (Макет электронного пропуска). Порядок создания макета смотрите *в разделе "Создание электронных пропусков" на стр. 253.*

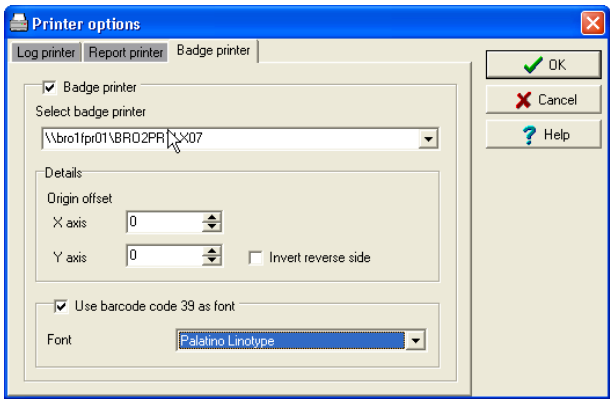
Печать электронных пропусков

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 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.

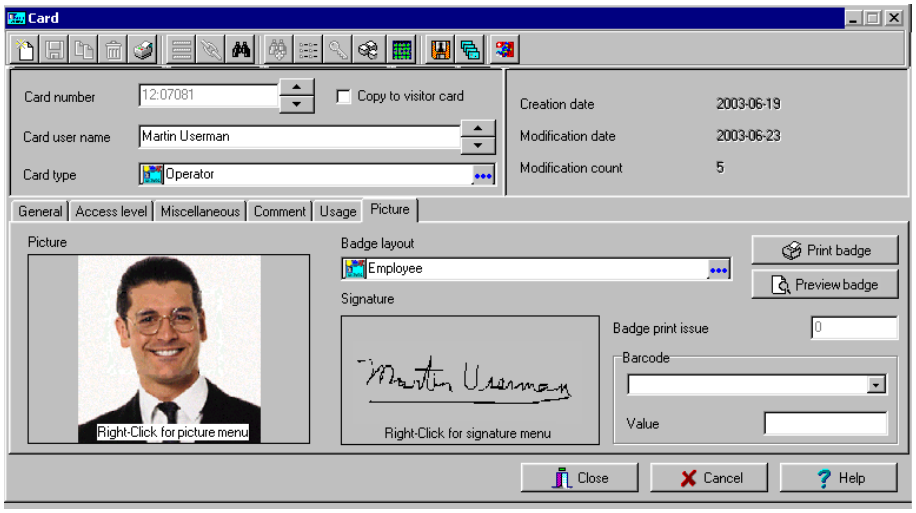
5 Настроить границы печати:

- 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

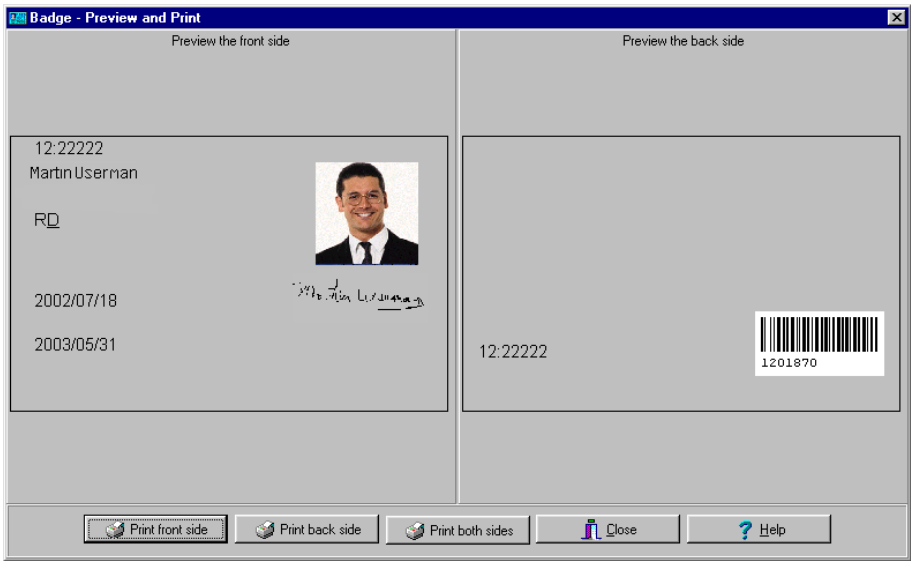
Окно **Badge - Preview and Print** (Электронные пропуска – Предварительный просмотр и печать) служит для предварительного просмотра макета электронного пропуска с заданными параметрами карты (если макет пропуска прикреплён к идентификационной карте) или с настройками по умолчанию (если макет ещё не прикреплён 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.

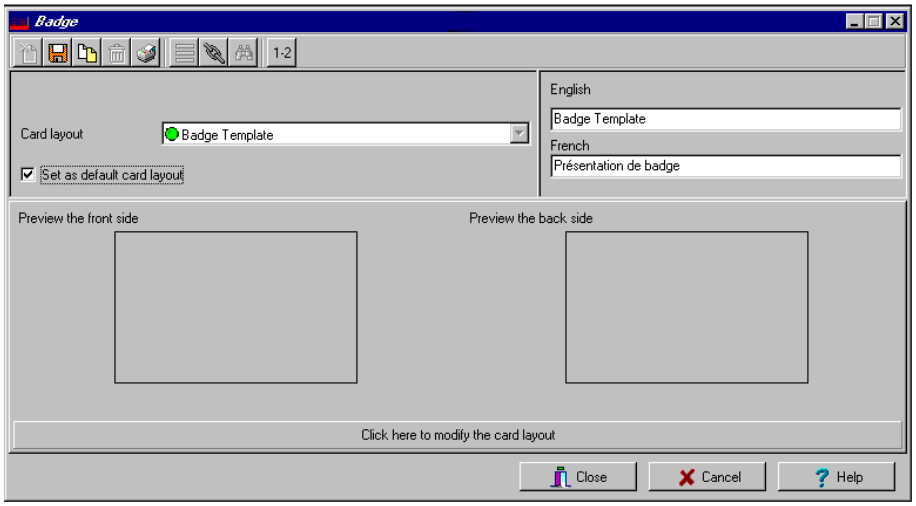
ПРИМЕЧАНИЕ. ВАЖНО! *Для того чтобы печатать электронные пропуска со штрихкодами, принтер должен быть правильно настроен. Для этого должна быть выбрана опция “black resin” (истинно чёрный цвет), иначе считыватели штрихкодов не смогут правильно определять их. При возникновении проблем с печатью или считыванием 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.

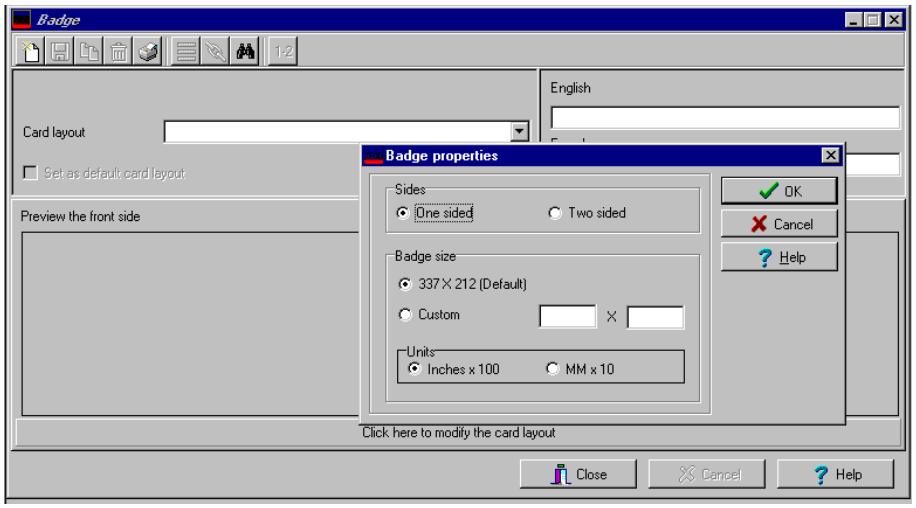


ПРИМЕЧАНИЕ. *Окно Badge содержит все инструменты, доступные в других окнах системы EntraPass: New (Создать), Save (Сохранить), Copy (Копировать), Delete (Удалить), Print (Печать), Links (Связи), Search (Поиск) (кнопка Hierarchy недоступна). Зато в этом окне есть дополнительная кнопка "1-2", которая позволяет изменять число сторон в макете пропуска.*

2 Нажать на панели инструментов кнопку **New** (Создать). Откроется окно Badge properties (Свойства электронных пропусков).

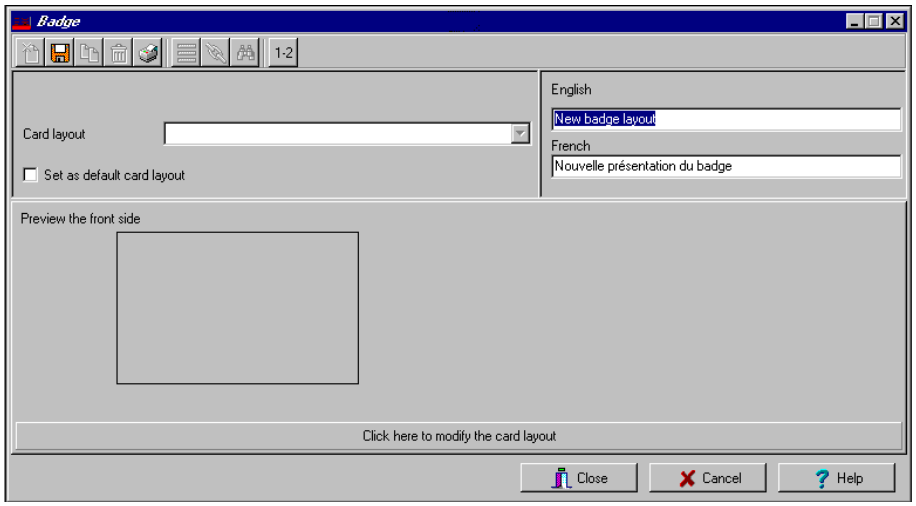
Описание свойств для макета электронных пропусков

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.

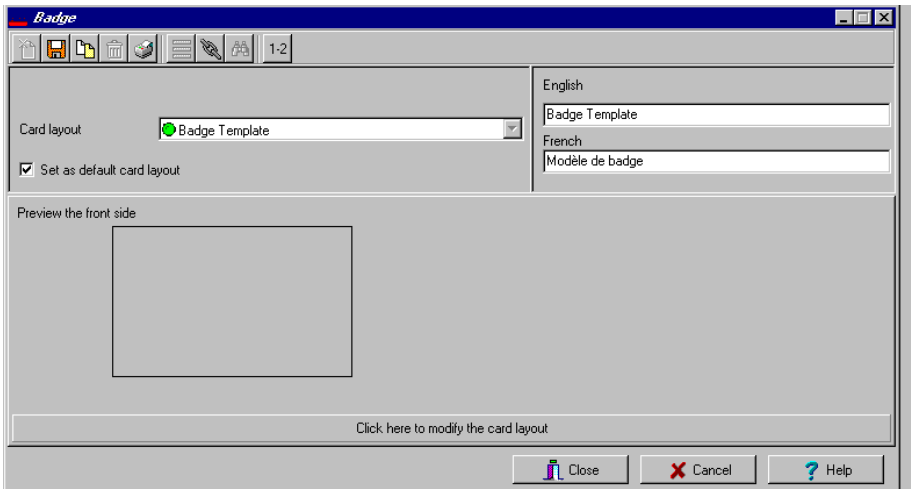
Редактирование макета пропусков

Утилита создания электронных пропусков (Badge Design) позволяет редактировать макет пропусков, делать цветной фон или использовать в качестве фона графическое изображение, изменять шрифты и пр.

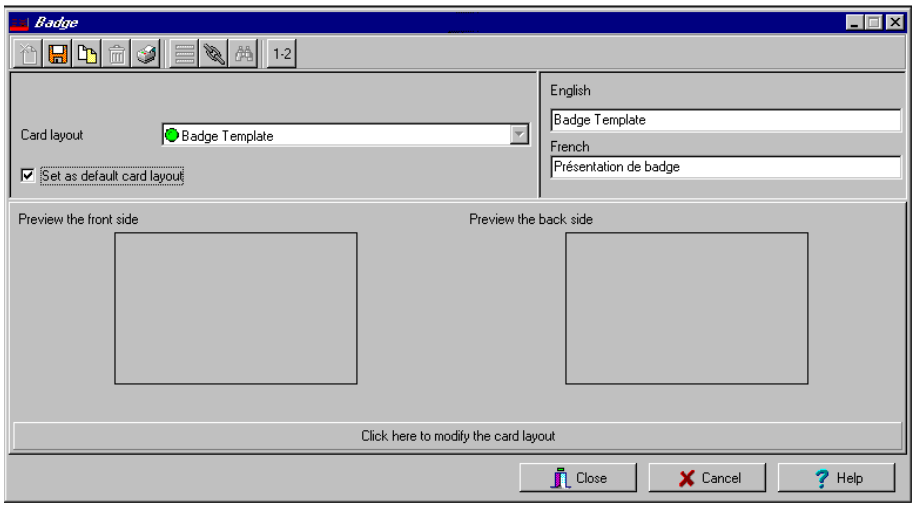
ПРИМЕЧАНИЕ. *После создания макета невозможно изменить его размеры, можно только создать новый макет. А число сторон изменять можно – следует нажать иконку* ***Sides*** *на панели инструментов окна Badge.*

Изменение числа сторон идентификационных карт

1 В окне Badge выбрать, какой электронный пропуск необходимо отредактировать.



2 В инструментах окна Badge нажать кнопку "1-2".

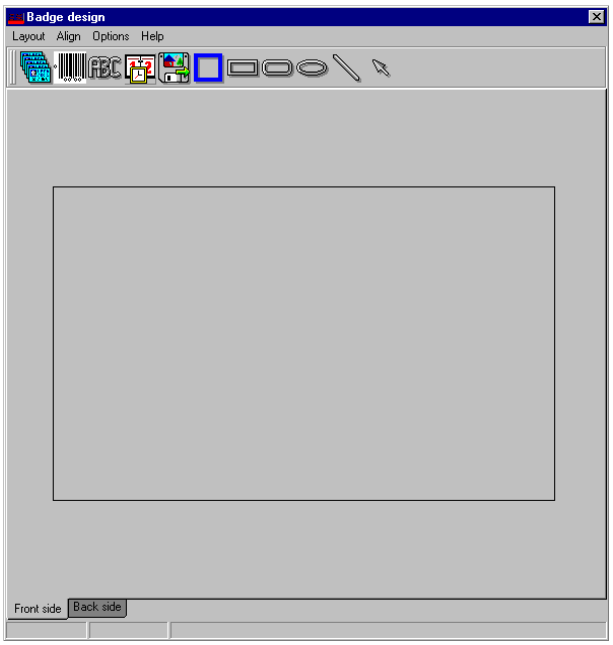


3 Нажать **Save** (Сохранить) для сохранения новых данных.

Изменение цвета фона

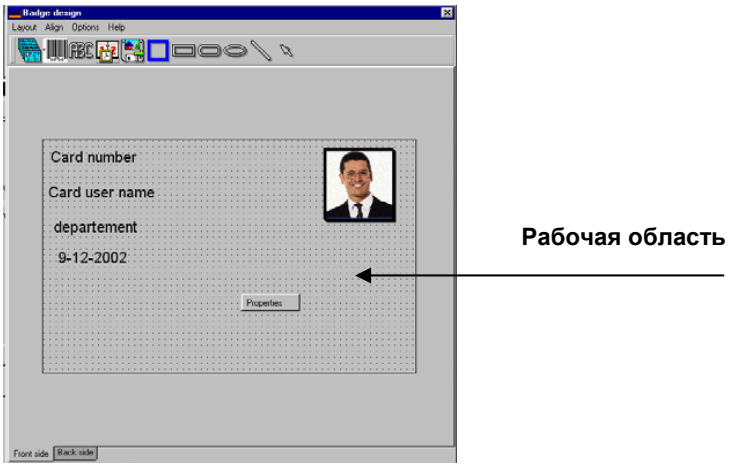
1 В окне Badge выбрать, какой электронный пропуск необходимо отредактировать.

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.*

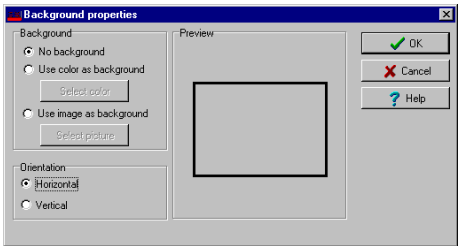
3 Чтобы изменить цветовой фон шаблона, следует нажать на правую кнопку мыши в любом месте рабочего окна. Откроется контекстное меню **Properties** (Свойства).



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) – служит для применения цветового фона ко всем разработкам.
- **Use image as background** (Использовать изображение как 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

Примитивная технология буксировки объекта мышью позволяет вставлять необходимые объекты в шаблон пропусков:

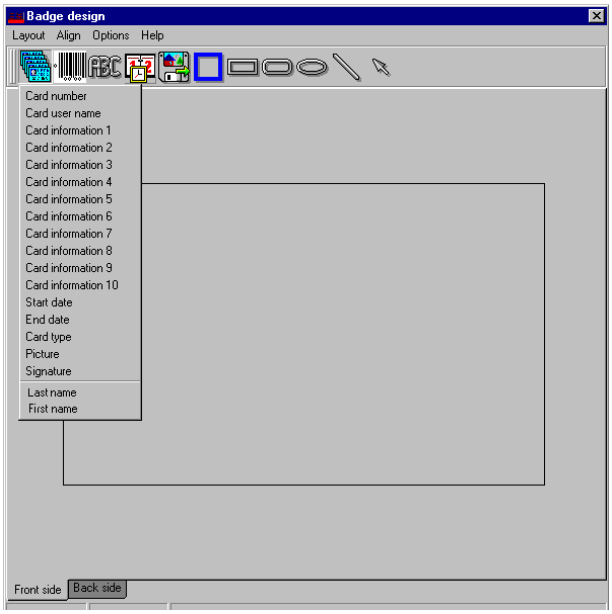
- данные в полях карты,
- штрихкоды,
- текстовые окна,
- текущая дата,
- Ранее сохранённые изображения и логотипы (формата BMP, JPG, GIF и др.),

- 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.*

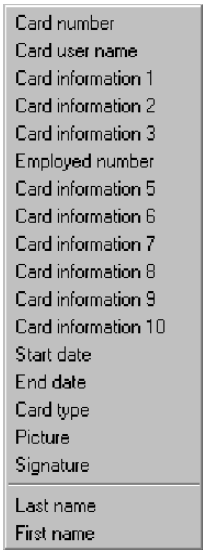
Вставка информационных полей карты

1 Чтобы добавить в шаблон электронных пропусков информационные поля карты, следует нажать на иконку **Card fields** (Поля карты). Откроется окно **Card fields.**

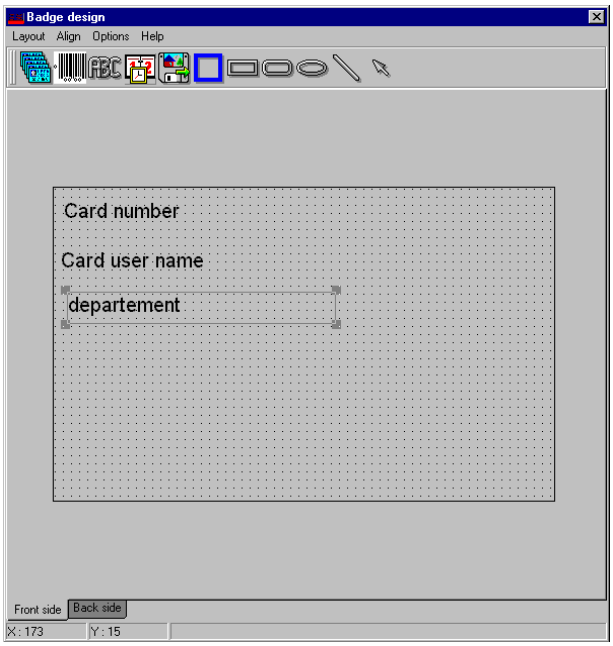


2 Для того чтобы изменить свойства объекта до перетаскивания его в рабочее окно, следует открыть закладку **Options** (Опции) в окне Badge Design (Создание пропуска) и выбрать пункт **Show properties on drop** (Показывать свойства при перетаскивании). В таком случае окно Properties будет открываться 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). Подробнее смотрите раздел "Формат имени пользователя" на стр. 466.*



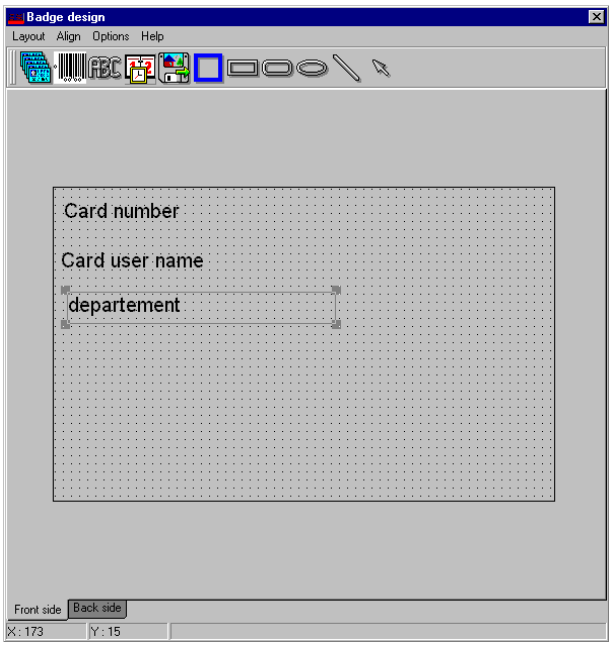
3 В контекстном меню выбрать информационное поле карты, которое необходимо добавить в макет шаблона, затем щёлкнуть в рабочей области шаблона, чтобы вставить это поле в шаблон.



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).

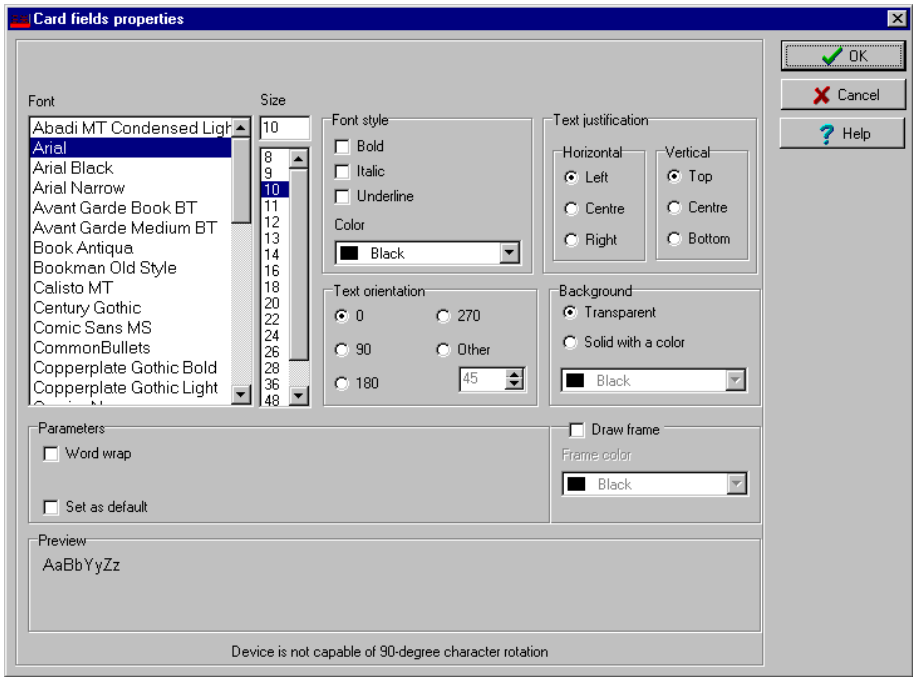
Изменение свойств информационных полей карты

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.*

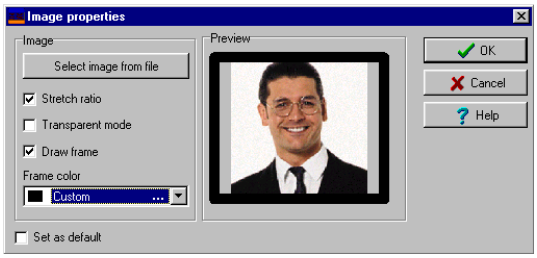
Изменение свойств изображений

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.



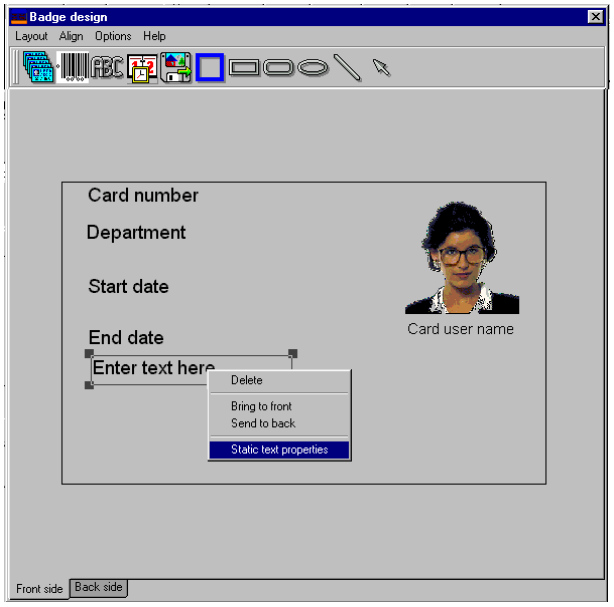
- **Stretch ratio** (Относительное растяжение) – позволяет разместить изображение в центре поля, сохраняя его оригинальные пропорции.
- **Transparent mode** (Прозрачный фон) – не использовать цветной фон,
- **Draw frame** (Нарисовать рамку) – обвести изображённый объект в рамку,
- **Frame color** (Цвет 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 объектов со статическим текстом

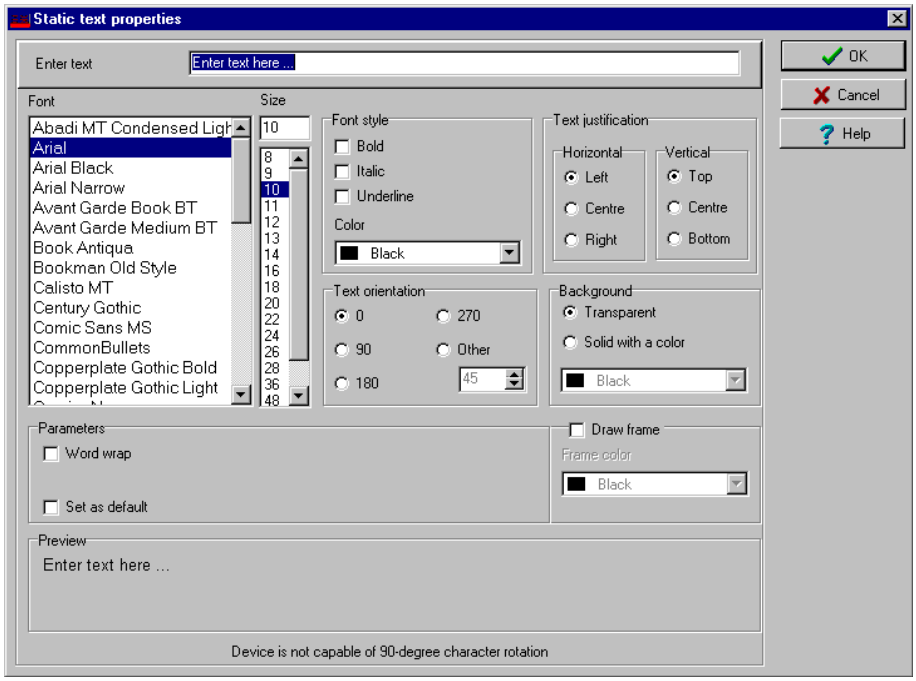
Чтобы добавить текстовый объект в шаблон пропусков, следует сначала перетащить в рабочую область текстовое окно, а потом ввести текст в окне Text properties (Свойства текста). Это же окно Text properties служит и для форматирования текста.

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 Порядок выравнивания текстовых объектов подробно описан в разделе "Выравнивание объектов в макете шаблона" на стр. 261.

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).

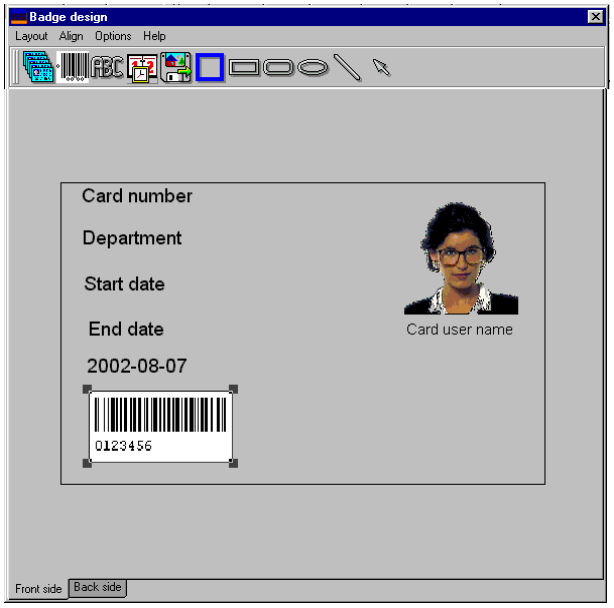


4 Ввести текст в поле **Enter text** (Введите текст); затем изменить свойства текста, если требуется. В окне предварительного просмотра (Preview) можно увидеть результаты внесённых изменений.

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.

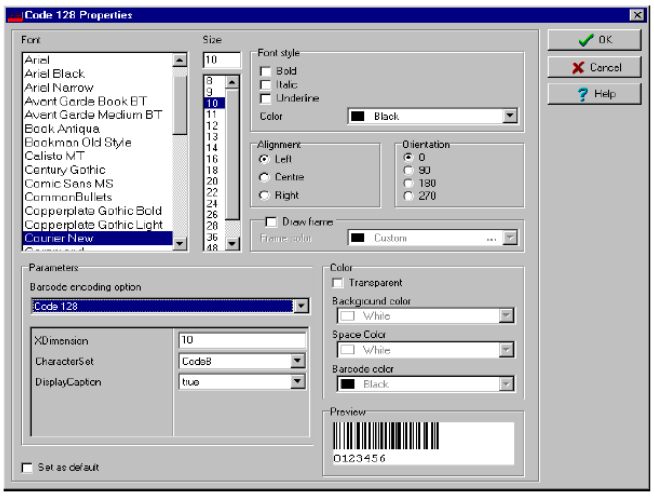
1 В окне Badge Design (Создание пропуска) нажать на иконку **Barcode** (Штрихкоды), затем щёлкнуть по рабочей области окна Badge design.



2 Для выравнивания объекта со штрихкодом смотрите указания в разделе "Выравнивание объектов в макете шаблона" на стр. 261.

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

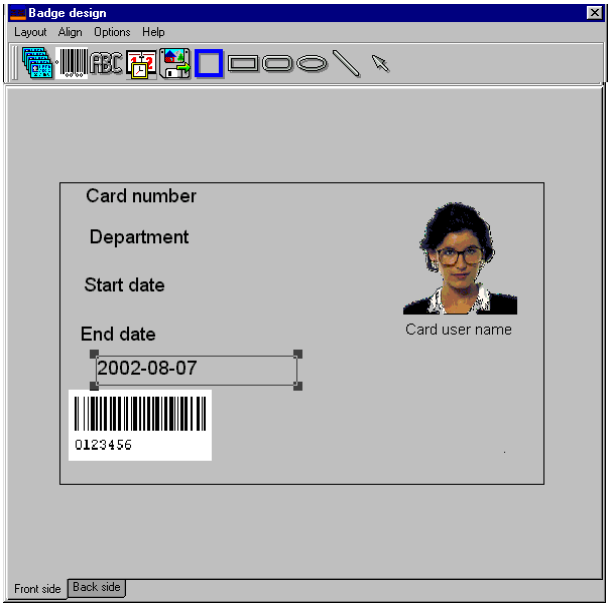
2 В открывшемся окне указать свойства штрихкодов, которые будут размещены на электронных пропусках.

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.

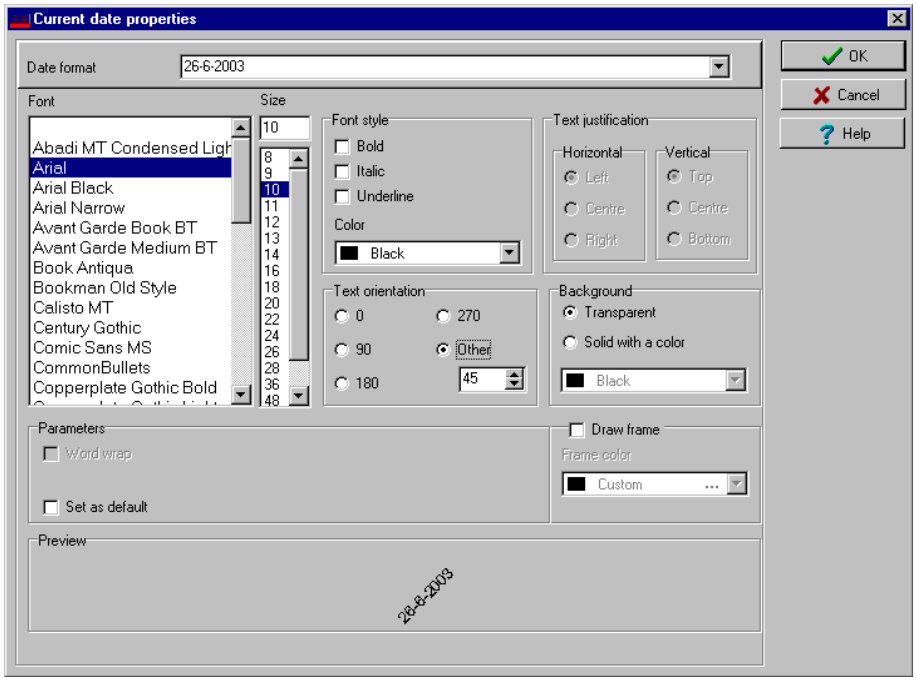
1 В окне Badge Design (Создание пропуска) нажать на иконку **Current date** (Текущая дата), затем щёлкнуть мышью в рабочей области окна.



2 Щелчком правой кнопки мыши по отображаемой дате вызвать контекстное меню.

3 Для выравнивания объекта выполните указания раздела "Выравнивание объектов в макете шаблона" на стр. 261.

4 В контекстном меню выбрать пункт **Current date properties** (Свойства текущей даты).



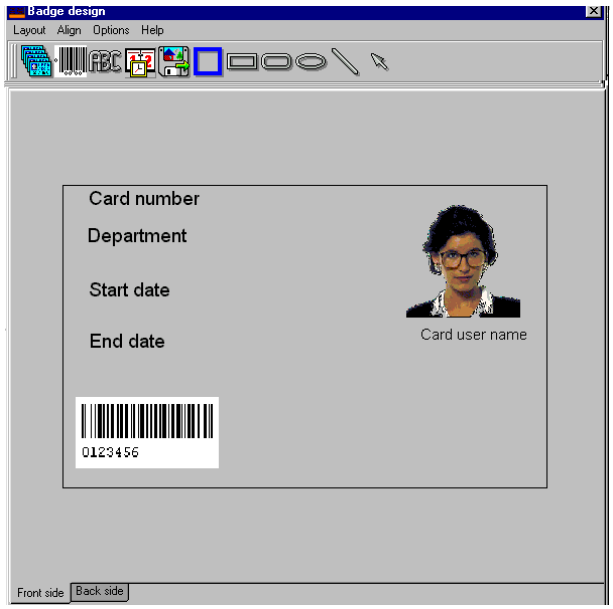
5 В окне Current date properties доступны следующие функции:

- формат даты (верхнее поле Date format).
- 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.

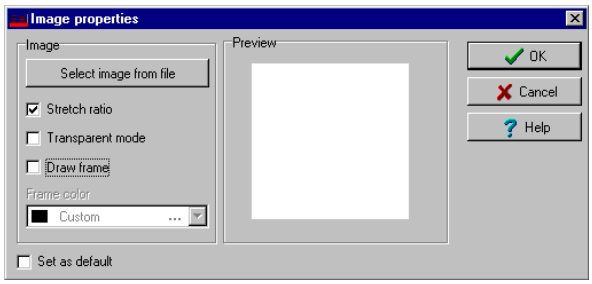
1 Для этого в окне Badge Design (Создание пропуска) следует нажать на иконку **Picture** (Изображение).

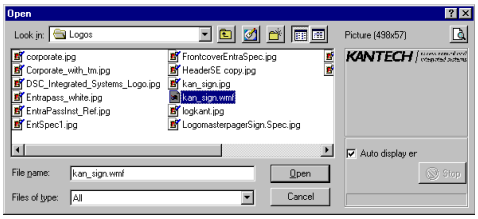


ПРИМЕЧАНИЕ. *Поддерживаются следующие форматы изображений: BMP, JPG, EMF, WMF, GIF, PNG, PCD и TIF.*

2 Вставить 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). Более подробная информация приведена в разделе *"Выравнивание объектов в макете шаблона" на стр. 261.*

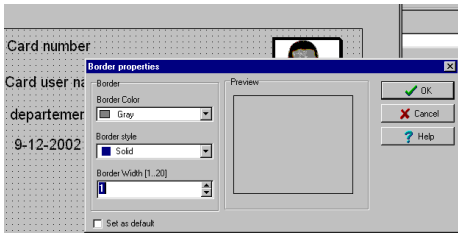
6 Для изменения свойств щёлкнуть по изображению правой кнопкой мыши. Подробнее смотрите раздел *"Изменение свойств изображения" на стр. 263.*

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.

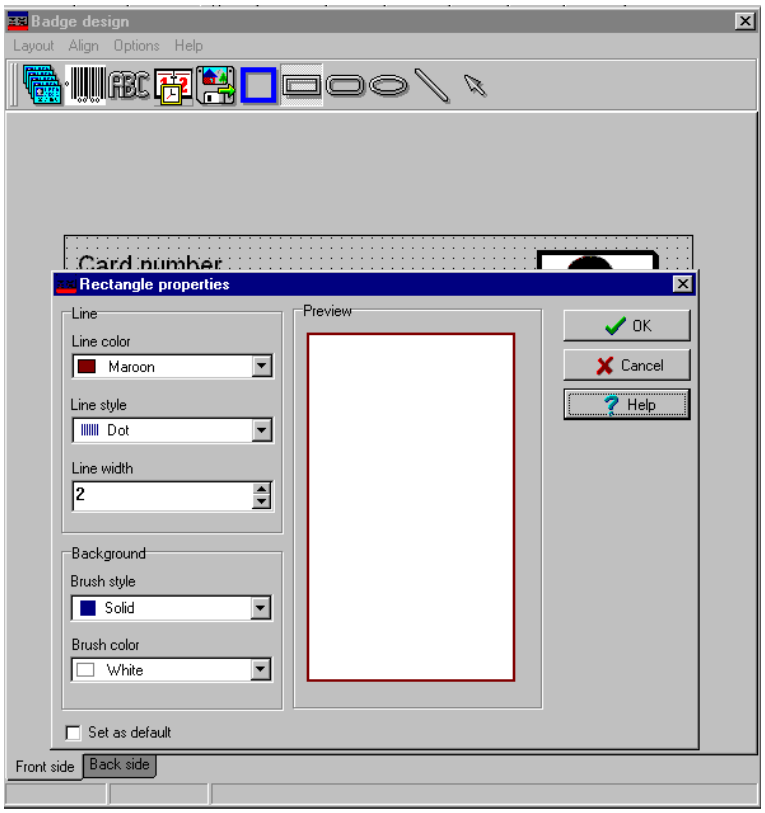
1 В окне Badge Design (Создание пропуска) выделить объект, который необходимо добавить (рядом с иконкой дискеты Diskette), затем щёлкнуть мышью в рабочей области окна. Откроется окно свойств Border properties (Свойства рамки).

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:

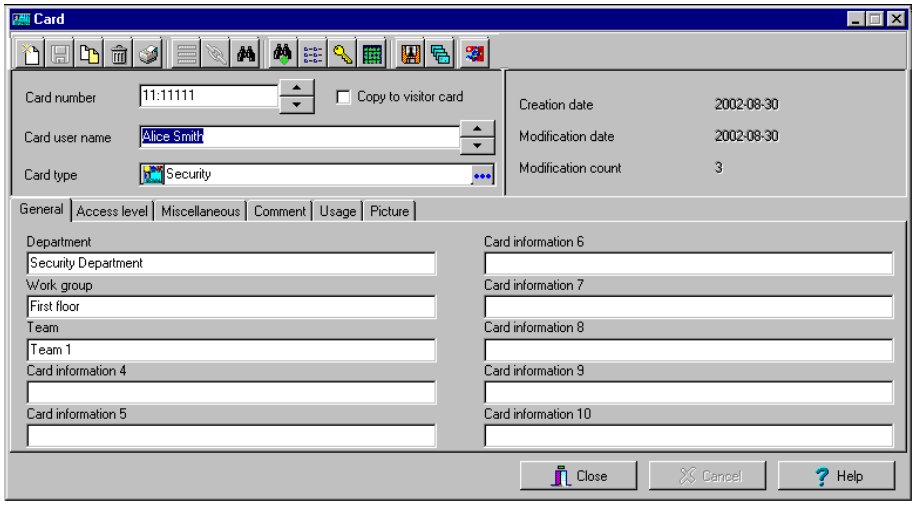
- Line color (Цвет линии),
- Line style (Стиль линии),

- Line width (Ширина линии),
- Background (Фон) – brush style (Стиль кисти) и brush color (Цвет кисти).

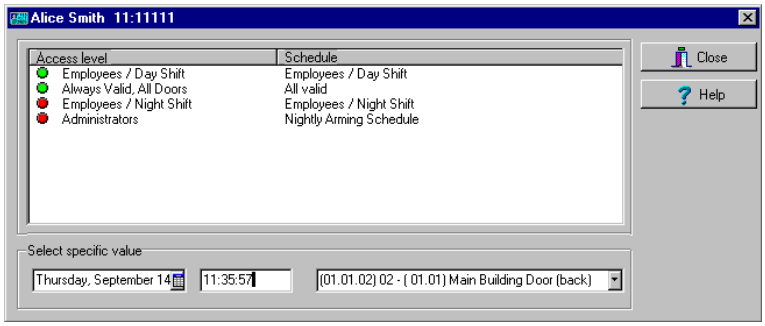
Проверка уровня доступа карты

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 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

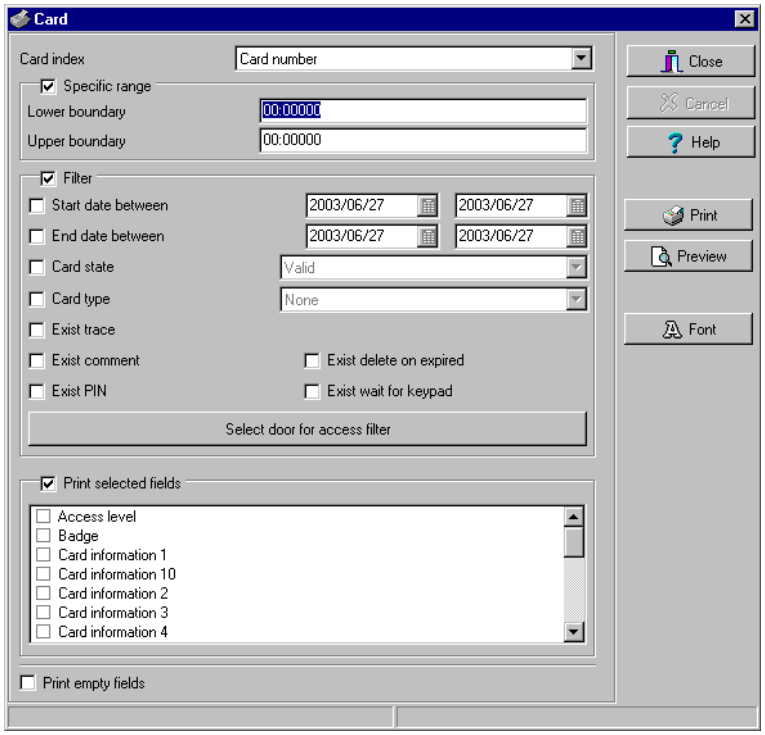
Чтобы распечатать определённую группу карт, хранящихся в базе данных, следует воспользоваться функцией Print (Печать). Для уточнения списка карт предусмотрено несколько фильтров.

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). 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.

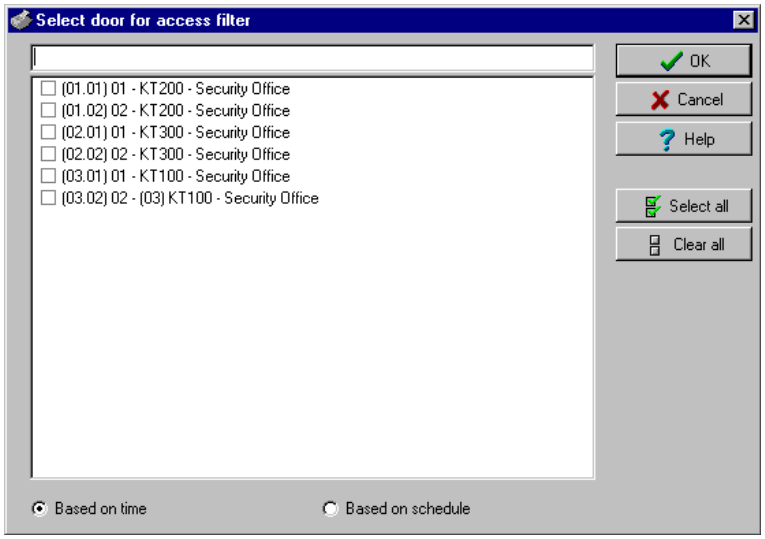
ПРИМЕЧАНИЕ. *Принтер будет печатать только те карты, которые удовлетворяют ВСЕМ критериям отбора. Например, если указано шесть критериев отбора, то карты должны удовлетворять всем шести критериям. Карты, не удовлетворяющие всем указанным критериям, не будут включены в список.*

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 активной 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).

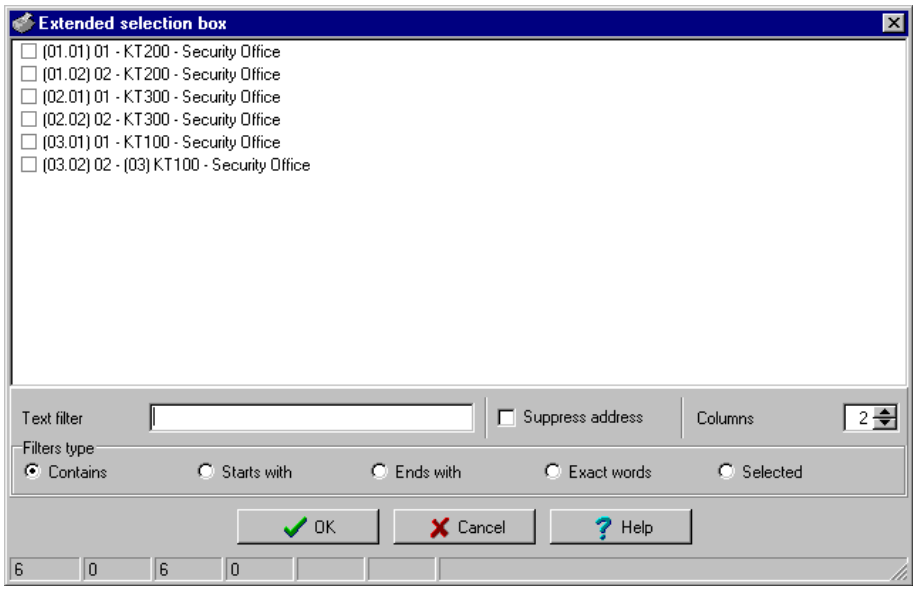
5 Если необходимо, отметить флажком поле **Print selected fields** (Выбрать поля для печати), чтобы печатать только указанные данные. Если отметить эту функцию, но не выделить флажком ни одного поля в прилагаемом списке информационных полей, то на печать будут выставлены карты, отобранные по выставленным 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

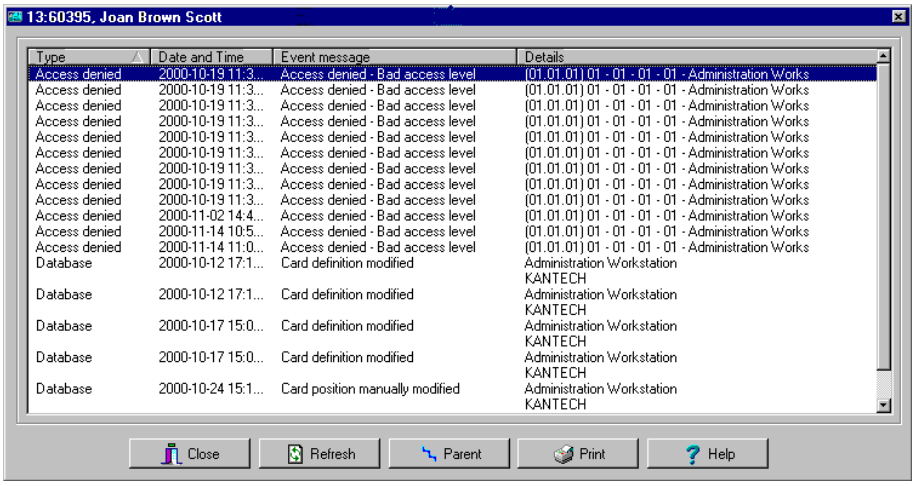
Функция **View last transactions** (Посмотреть последние транзакции) служит для просмотра последних транзакций, выполненных указанным владельцем карты. Например, в этом окне отображается “Access denied” (Доступ закрыт), как тип события, а также дата и время и сообщение о событии, которое отображается 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 события (включая 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, отправленное после возникновения события на сервер (и на соответствующую рабочую станцию EntraPass). 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, в 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. Более подробная информация приведена в разделе *"Основные функции" на стр. 50.*
- **Print** (Печать) – служит для вывода на печать точной копии информации, представленной в этом окне. Более подробная информация приведена в разделе *"Основные функции" на стр. 50.*

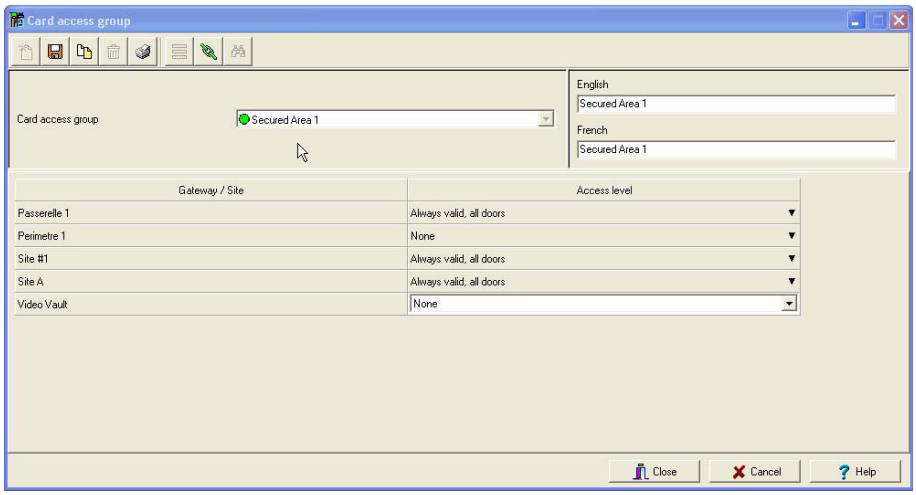
Описание групп доступа для идентификационных карт

Предварительно настроенные группы доступа для идентификационных карт позволяют быстро назначать уровень доступа для разных сайтов системы. Такую группу доступа можно вызвать во время описания карты вместо повторного ввода уровней доступа для каждого сайта.

Причём именно данные из группы доступа прикреплены к карте. Таким образом, можно изменять данные в группе доступа, не изменяя данные о доступе в описании карты.

ПРИМЕЧАНИЕ. *При импортировании идентификационных карт функцию* ***Card access group*** *(Группа доступа для карт) можно использовать для назначения уровня доступа для этих карт.*

1 В окне Card (Карты) нажать кнопку Access group (Группа доступа).



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) отображается сайт, прикреплённый к указанной группе доступа.

3 В списке **Access level** (Уровни доступа) выбрать уровень доступа к дверям указанного сайта.

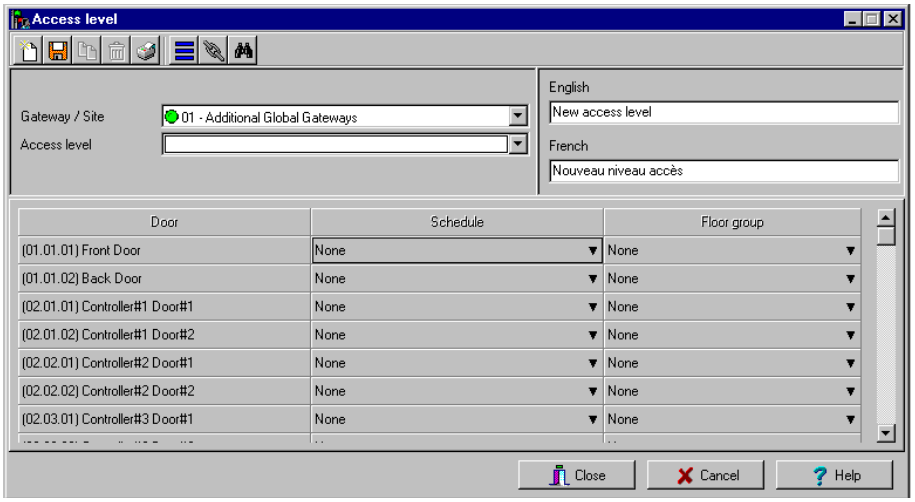
Описание уровней доступа

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 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);
- 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 описания дверей нужно перейти в меню **Devices** (Устройства) > **Sites** (Сайты) > **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 списке **Doors** (Двери) выбрать двери, к которым владелец карты должен иметь доступ.

4 В колонке **Schedule** (Расписания) указать расписание, согласно которому владельцы карт должны будут иметь доступ к выбранной двери.

5 Если необходимо, выбрать группу этажей.

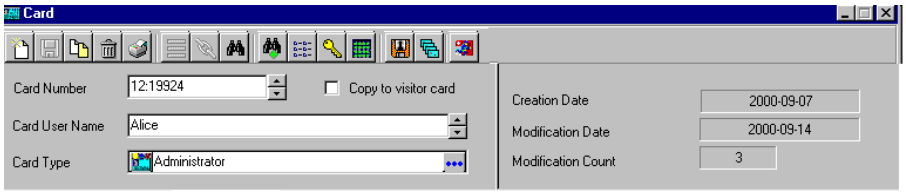
Описание карт посетителей

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 о картах посетителей, когда в системе создаётся новая карта или разовый пропуск,
- созданием новой карты посетителя.

Создание карты посетителя при создании новой карты

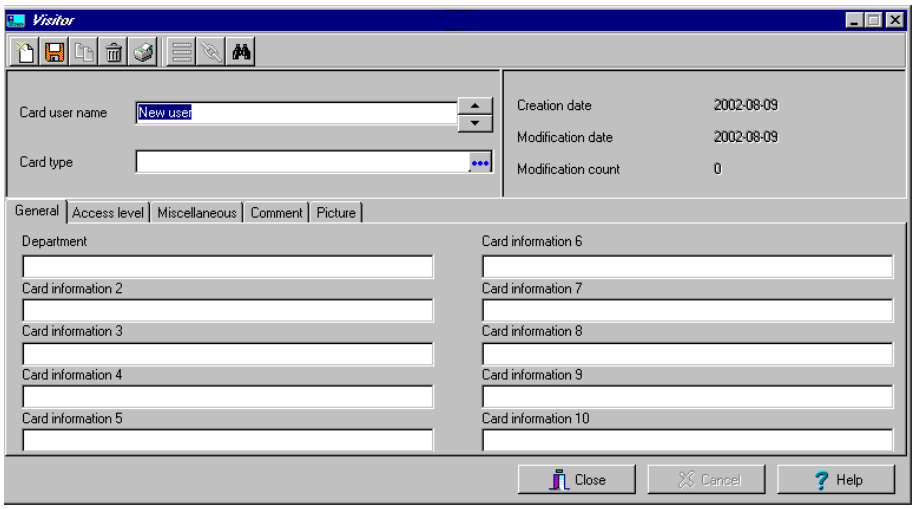
1 В окне Users (Пользователи) нажать на иконку **Card** (Идентификационные карты). Открывается окно Card.



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.

Создание карты посетителя 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. *Более подробная информация о создании разовых пропусков и карт посетителей приведена в разделе "Описание типов карт" на стр. 230. Закладка Picture (Изображение) даёт возможность размещать на картах фотографии и подписи, а также изготавливать электронные пропуска (доступна также функция предварительного просмотра).*

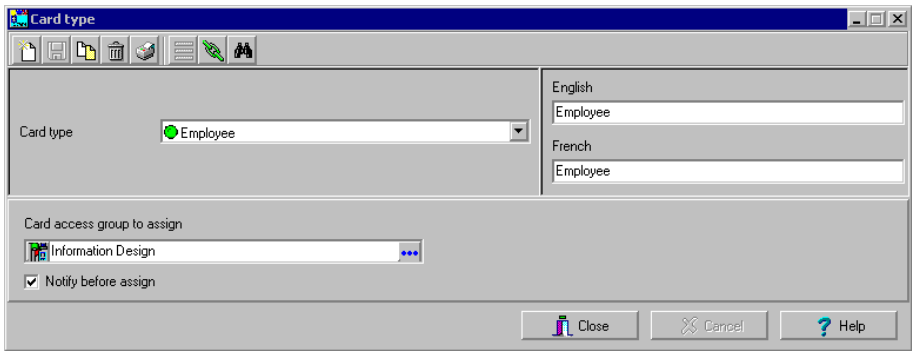
Описание типов карт

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. Более подробные сведения о группах доступа смотрите *в разделе "Описание групп доступа для идентификационных карт" на стр. 283.*

4 Порядок прикрепления владельца к определённому типу карты смотрите *в разделе "Пользователи" на стр. 229*.

Описание разовых пропусков

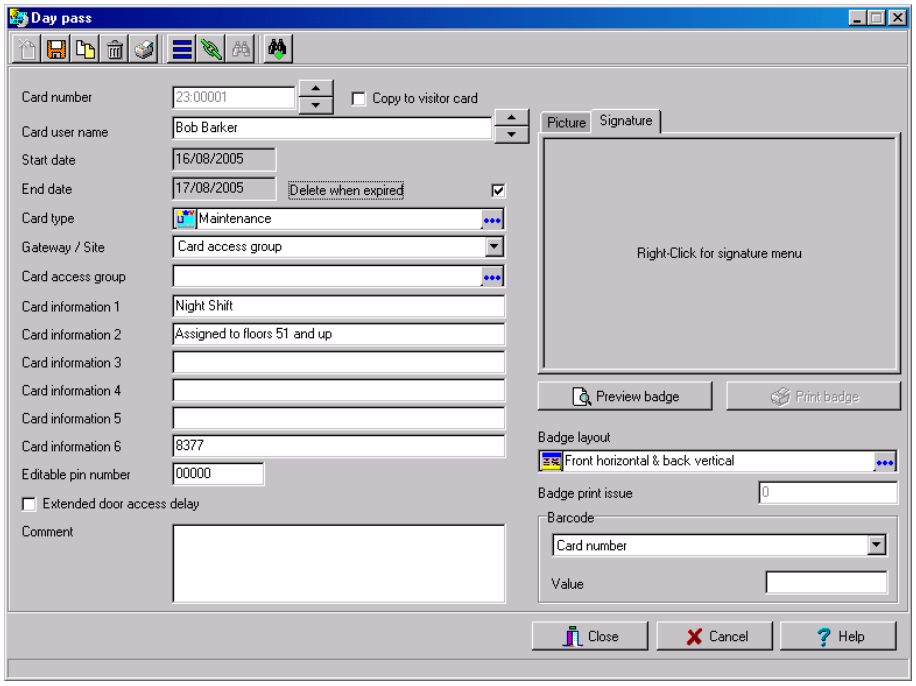
Разовые пропуска выписываются временным работникам, служащим других филиалов компании, покупателям и т. д. Эта опция позволяет быстро предоставить доступ разовым посетителям.

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” (Описание посетителей), для поиска нужного посетителя служит кнопка “Find visitor”. Кроме того, для создания нового пропуска можно использовать действующий разовый пропуск.

Создание разового пропуска

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. Более подробная информация приведена в разделе *"Пользователи" на стр. 229.*

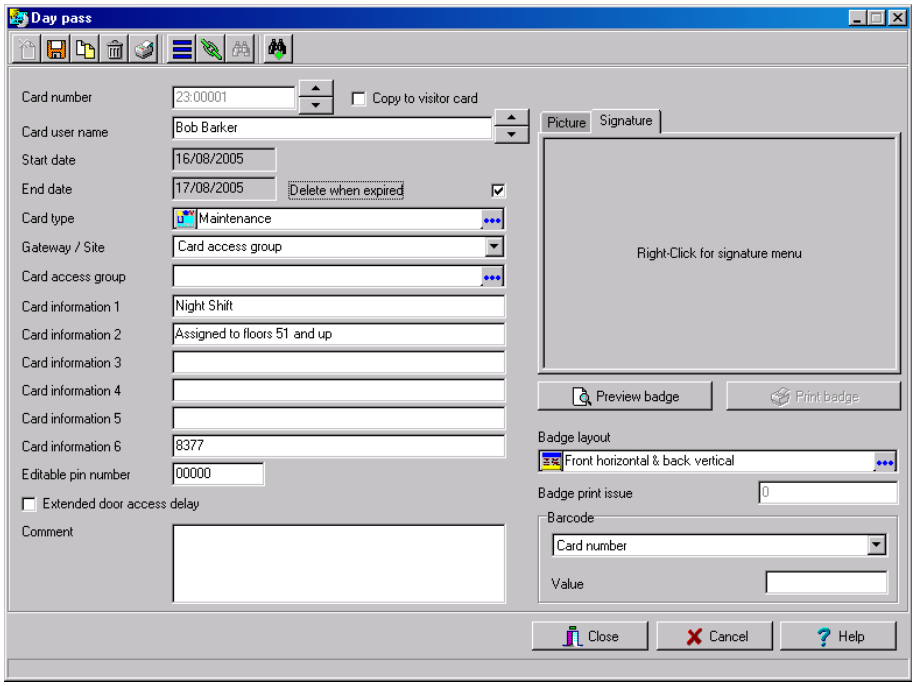
3 Отметить флажком опцию Copy to visitor card (Копировать в карты посетителей), чтобы сохранить этот разовый пропуск в базе данных посетителей.

ПРИМЕЧАНИЕ. *Более подробная информация о картах посетителей изложена в разделе "Описание типов карт" на стр. 230. 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...).

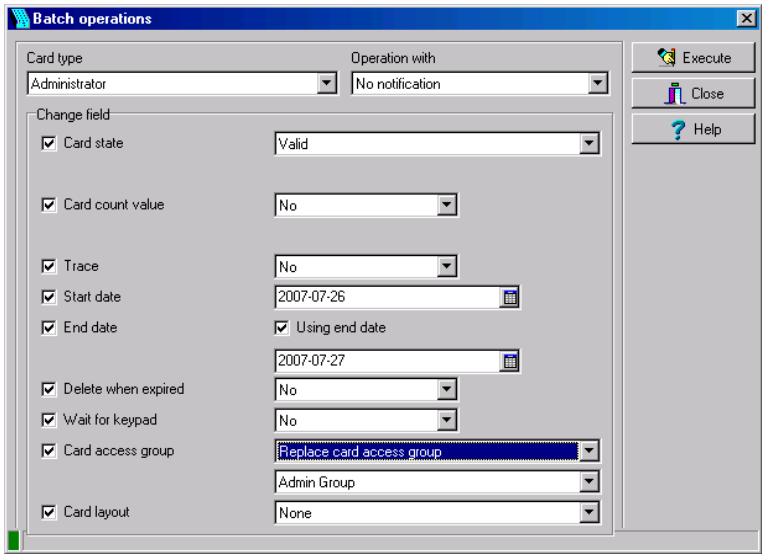
4 Система предложит назначить созданной карте новый номер.

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 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.

4 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.
- **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) – 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 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.

5 Чтобы запустить процесс, нажать кнопку **Execute** (Выполнить). Система предложит подтвердить выполнение операции.

6 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.

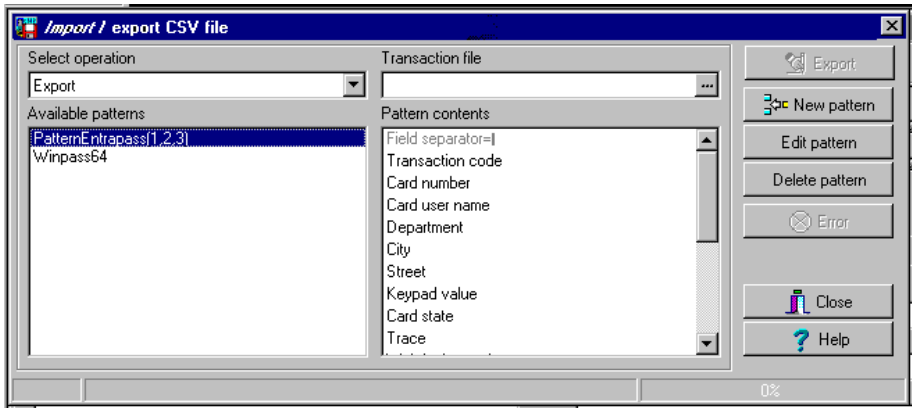
ПРИМЕЧАНИЕ. *Функция CSV Import/Export устанавливает несколько правил: формат данных у каждого поля в старой и новой базе должен совпадать. Например, поле статуса карты может содержать только три значения: 0=действительная карта, 1=недействительная карта, 2=карта потеряна/украдена.*

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).

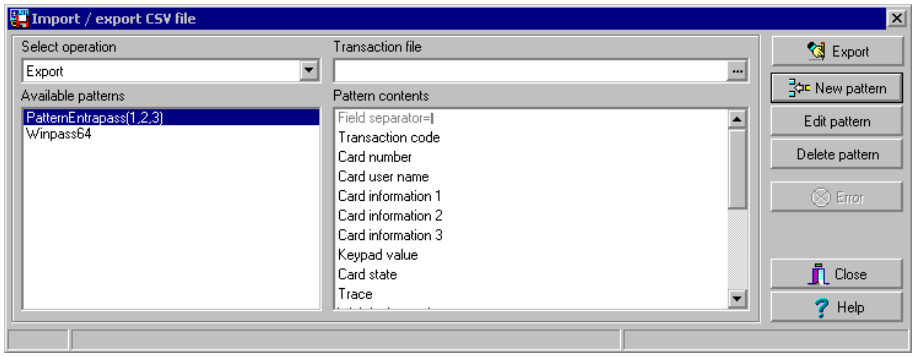
3 На панели **Available Patterns** (Доступные шаблоны) выбрать шаблон. Это зависит от настроек обновляемого программного обеспечения.

4 Чтобы изменить шаблон (при необходимости), нажать кнопку **Edit** (Редактировать).

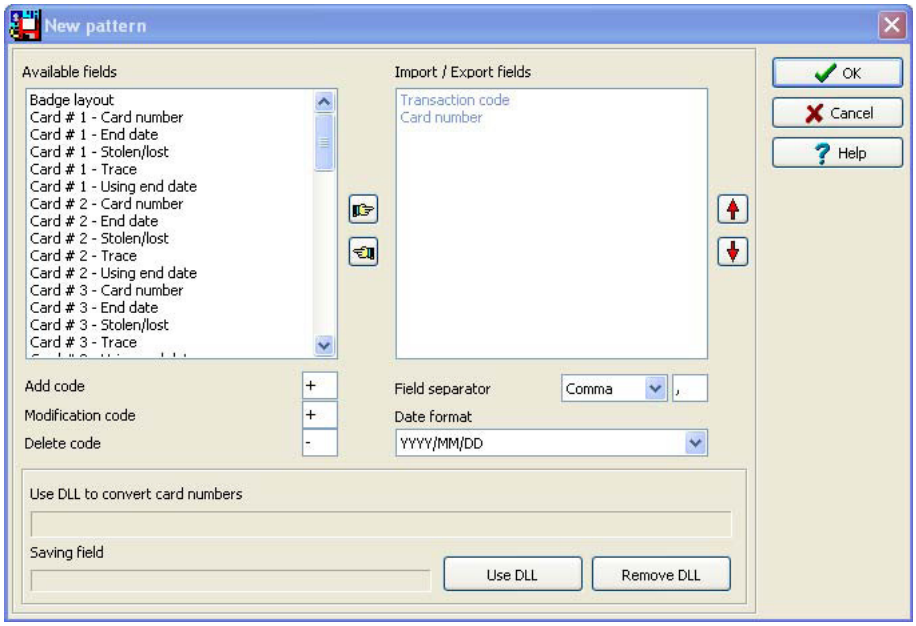
Создание нового шаблона для импорта/экспорта данных

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).

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 “+”.

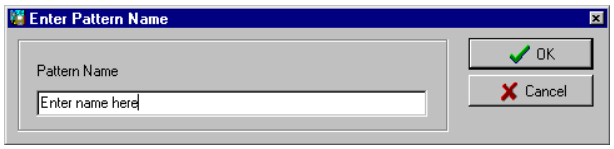
5 Выбрать **Delete code** (Код удаления). По этому коду система во время импортирования файла определяет, какую карту нужно удалить из базы данных. По умолчанию это код имеет значение “-”.

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.

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).

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.



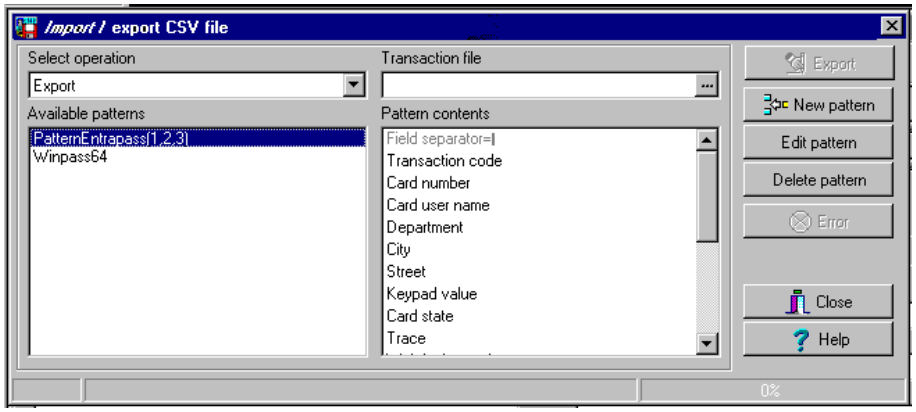
9 Указать имя нового шаблона в открывшемся окне в поле Pattern name и нажать **OK**. Система автоматически вернётся к окну Import/Export CSV file (Импорт/Экспорт CSV файлов). Только что созданный шаблон появится в списке **Available patterns** (Доступные шаблоны).

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.

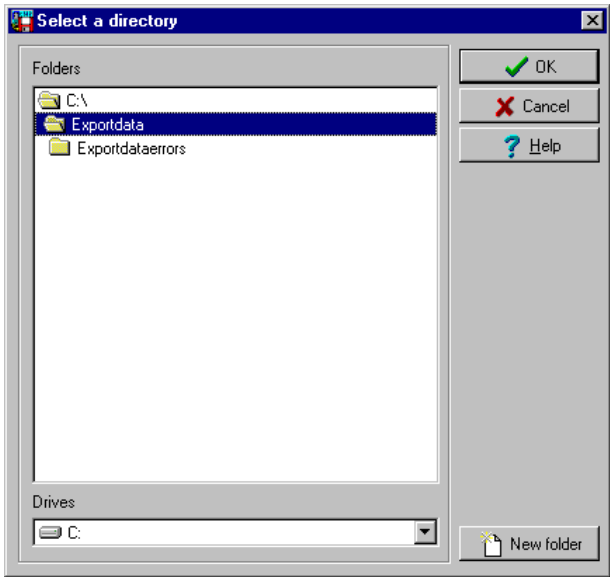
1 В меню **Users** (Пользователи) нажать на кнопку **Import/Export CSV File**. При этом должно открыться окно Import / Export CSV file (Импортирование/Экспортирование CSV файлов).



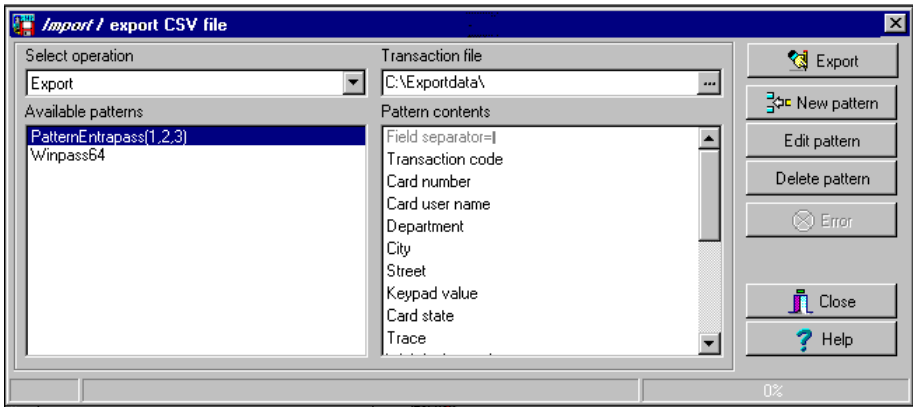
2 В выпадающем списке **Select operation** (Выберите операцию) выбрать опцию **Export** (Экспортировать).

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. (Подробная информация и указания по созданию шаблона приведена *в разделе "Создание нового шаблона для импорта/экспорта данных" на стр. 292*).

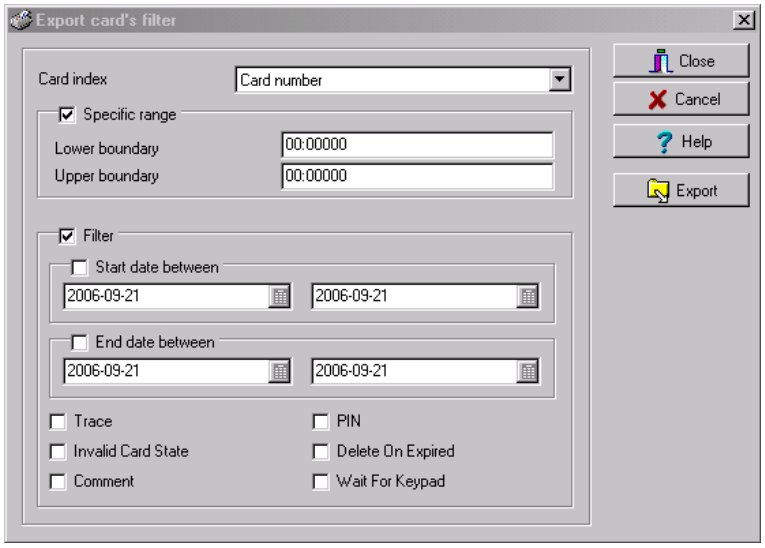
4 В поле **Transaction file** (Файл транзакции) указать путь сохранения создаваемого файла данных. Для открытия этого CSV файла можно использовать Excel, NotePad и другие программы.



5 После указания/создания папки для экспорта данных следует нажать **OK** и вернуться в окно Import/Export CSV file.

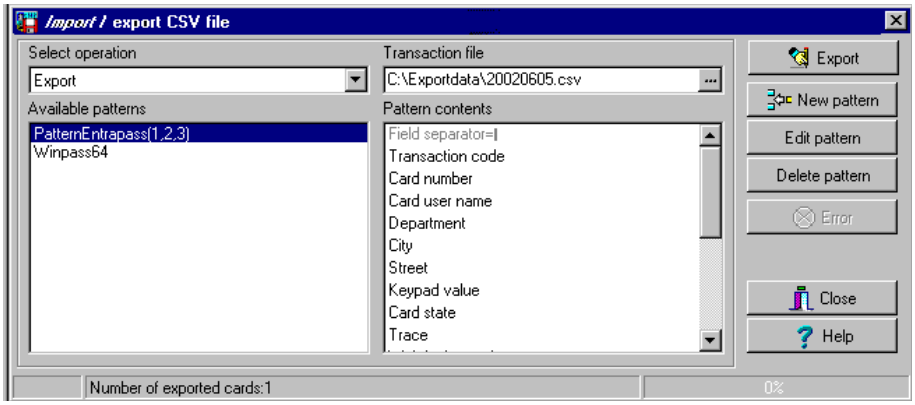


6 Нажать кнопку **Export** (Экспортировать), которая становится активной после указания пути сохранения файла. В открывшемся окне отобрать карты, предназначенные для экспорта.



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.*

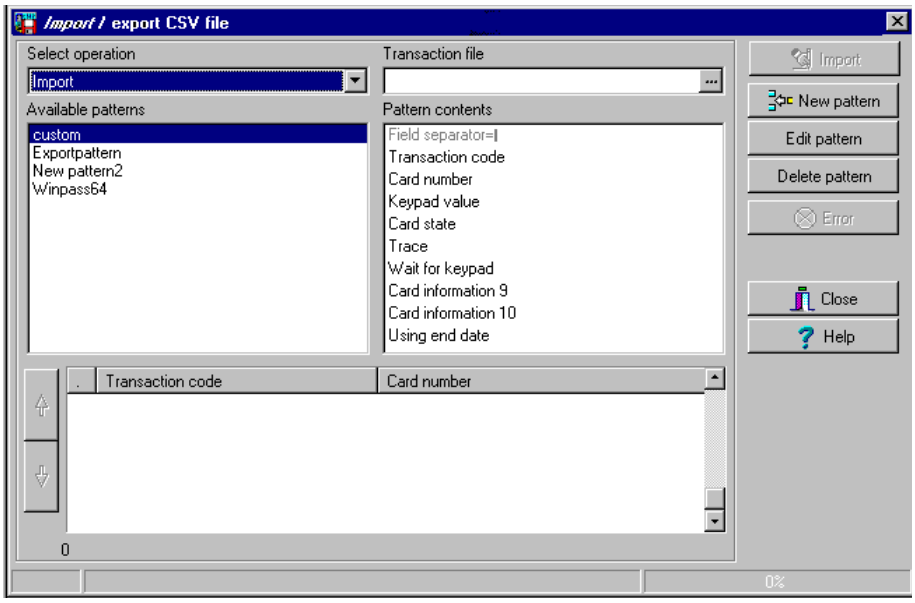
7 В окне Export Card's filter (Фильтры экспортируемых карт) отобрать карты, предназначенные для экспорта. После выделения всех необходимых полей нажать кнопку **Export** (Экспортировать). При этом должно открыться окно Import/Export CSV file.



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

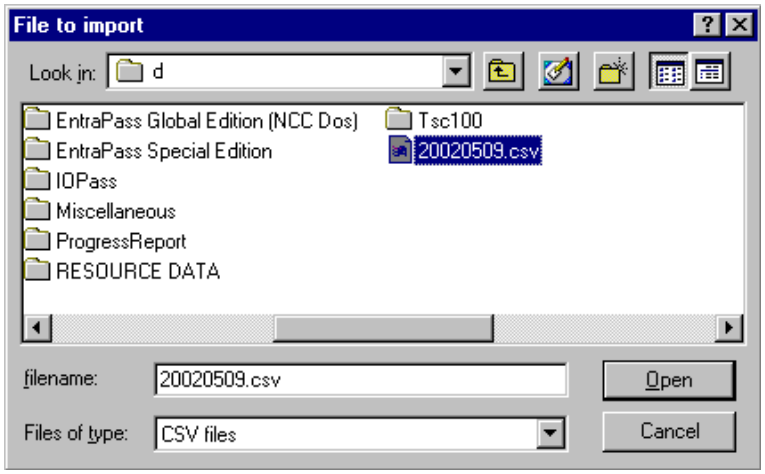
1 В меню **Users** (Пользователи) нажать на кнопку **Import/Export CSV File**. На экране появляется диалоговое окно Import/Export CSV file.



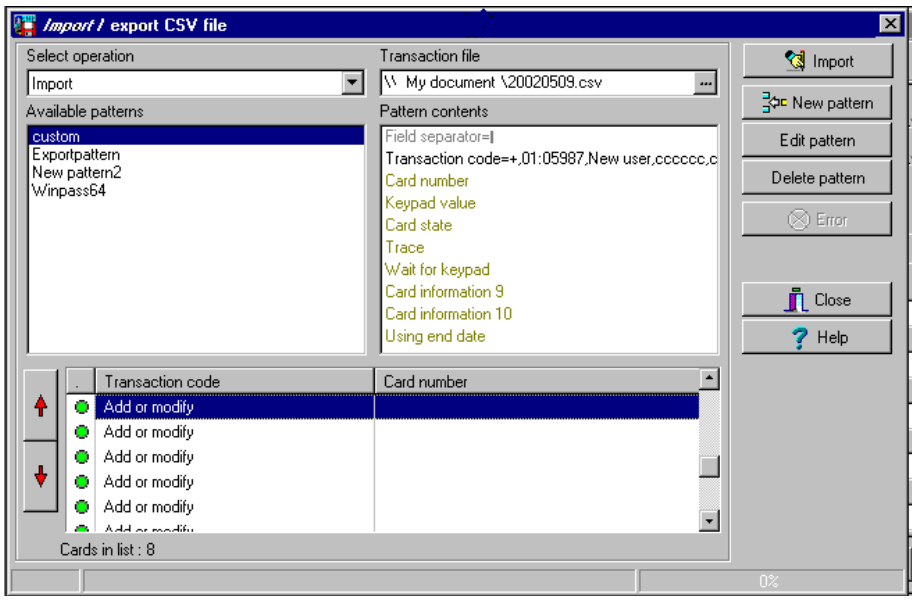
2 В выпадающем списке **Select operation** (Выберите операцию) выбрать опцию Import (Импортировать).

3 В списке **Available patterns** (Доступные шаблоны) выделить шаблон, с помощью которого необходимо импортировать данные. (Подробная информация и указания по созданию шаблона приведена в разделе *"Создание нового шаблона для импорта/экспорта данных" на стр. 292).*

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.

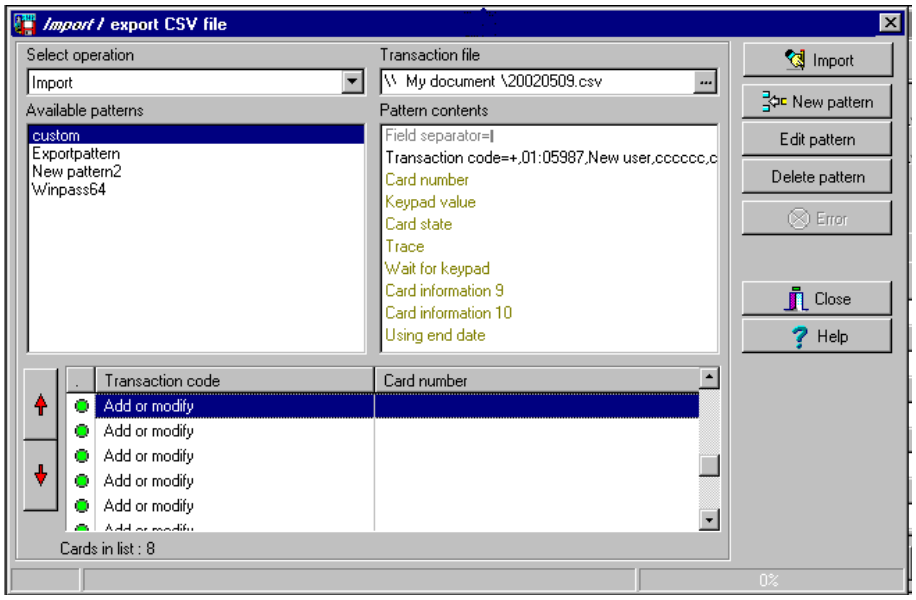
ПРИМЕЧАНИЕ. *Система сканирует файл с импортируемыми данными и отображает результаты при помощи цветового кода. Каждая позиция отображается вместе с цветовым флажком. Жёлтый или красный цвет указывает на ошибку. Ошибки часто возникают из-за несоответствия шаблонов. В этом случае необходимо выбрать другой 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 глава 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.

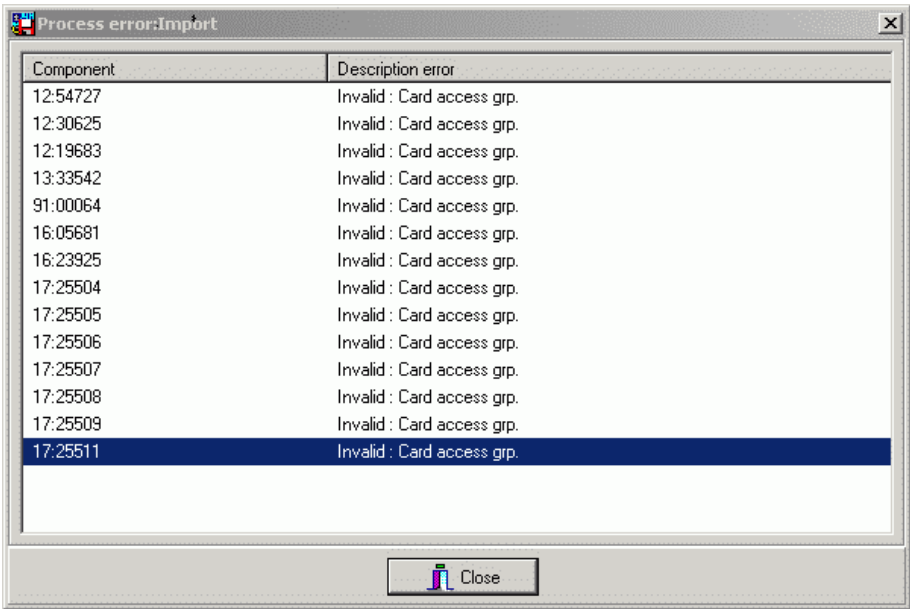


ПРИМЕЧАНИЕ. *Несмотря на то, что позиции в колонке **Transaction code** (Код транзакции) отмечены зелёным флажком, колонка **Card number** (Номер карты) осталась пустой. Это указывает на неправильное конвертирование шаблона.*

2 Нажать кнопку **Import** (Импортировать).

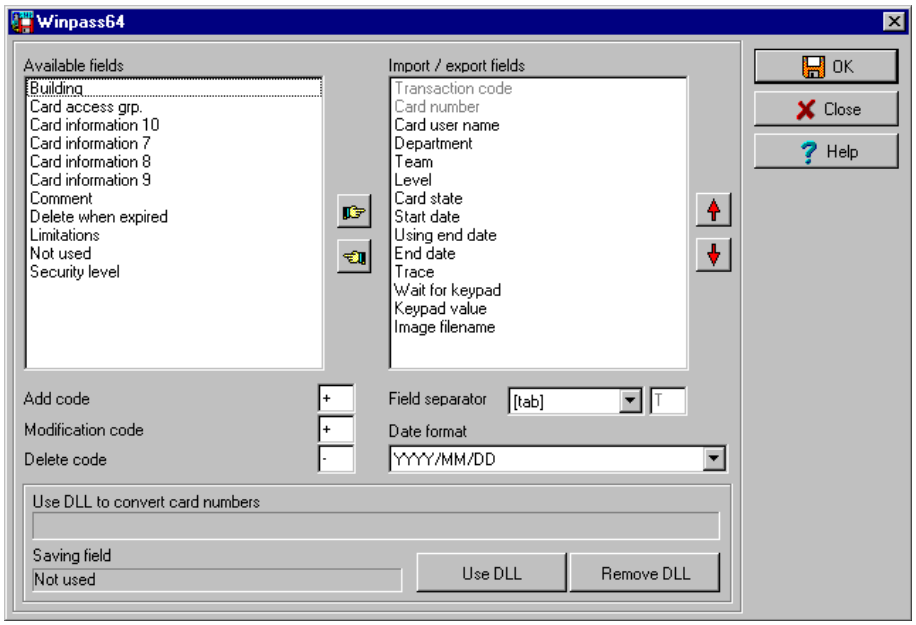
ПРИМЕЧАНИЕ. *Кнопка **Error** (Ошибки) стала активной, поскольку система обнаружила ошибки при импортировании данных.*

3 Чтобы увидеть информацию об ошибках, нажать кнопку **Error.** Окно Process error (Ошибки обработки) содержит те позиции, которые оказались неверными в используемом шаблоне.

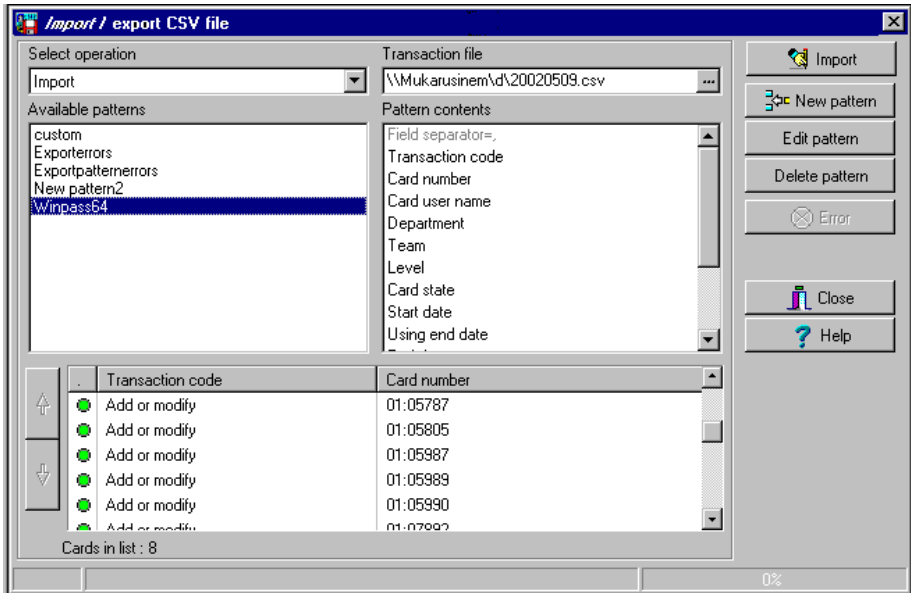


4 Нажать **Close** (Закрыть), чтобы вернуться в окно Import/Export.

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.



Глава 9 • Группы

Чтобы применять функции системы сразу к целой группе компонентов, следует объединить компоненты в группы.

ПРИМЕЧАНИЕ. *Каждый компонент системы, перед тем как включить в группу, следует описать.*

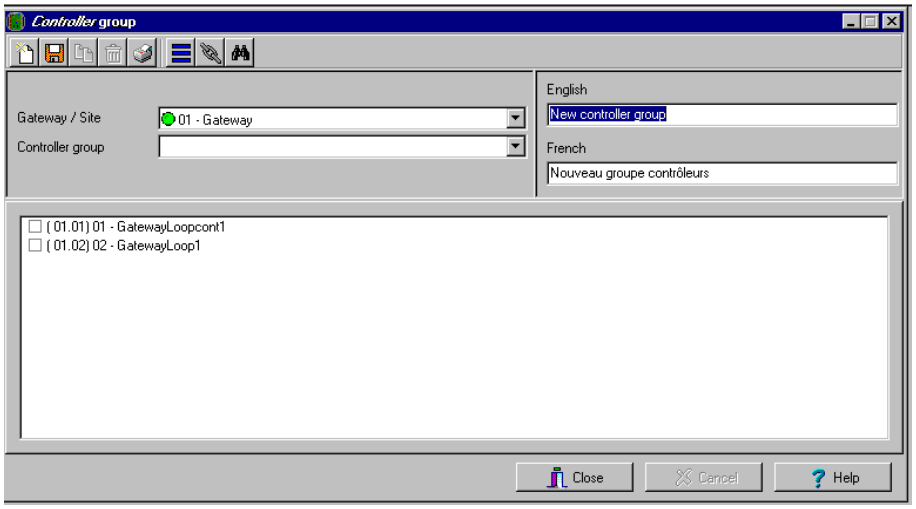
Система предусматривает создание следующих групп компонентов:

- Группы контроллеров
- Группы дверей
- Группы реле
- Группы входов
- Группы уровней доступа
- Группы этажей

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.

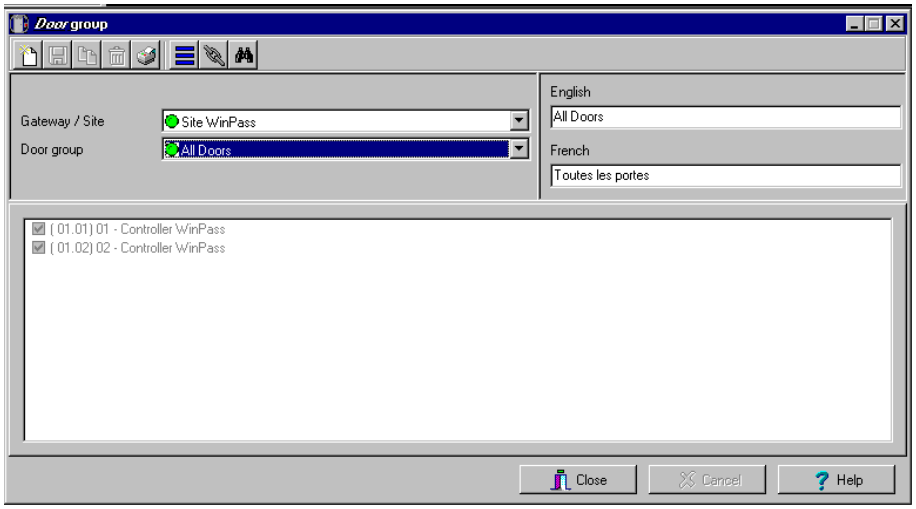
5 Из списка контроллеров, подключённых к выбранному сайту, выделить компоненты, которые должны быть объединены в группу.

ПРИМЕЧАНИЕ. *Более подробные сведения по настройке контроллеров смотрите в разделе "Настройка конфигурации контроллеров" на стр. 101.*

Создание групп 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.

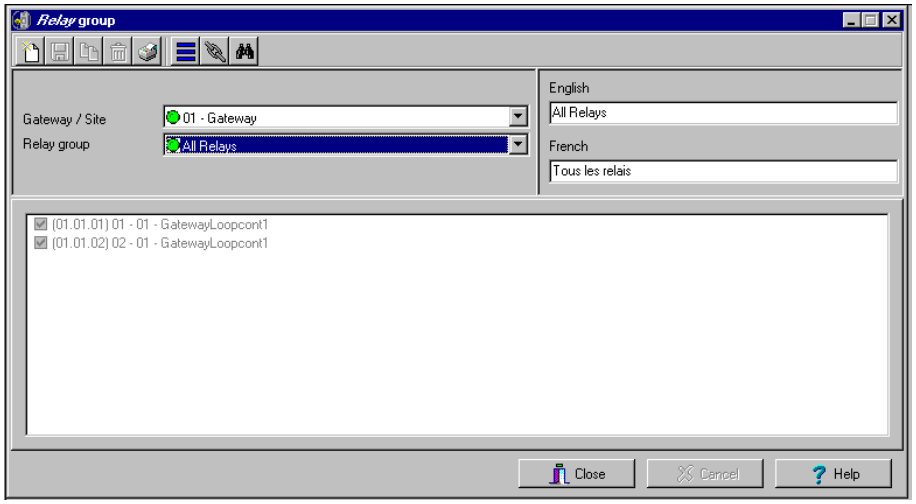
5 В списке дверей выбрать компоненты, которые должны быть включены в группу.

ПРИМЕЧАНИЕ. *Подробнее смотрите в разделе "Конфигурация дверей" на стр. 127.*

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.

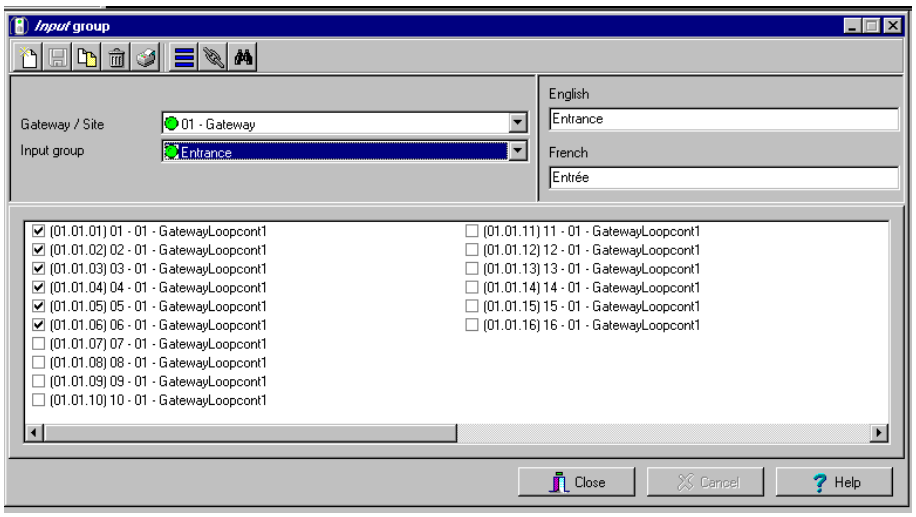
ПРИМЕЧАНИЕ. *Подробнее смотрите в разделе "Конфигурация реле" на стр. 142.*

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.

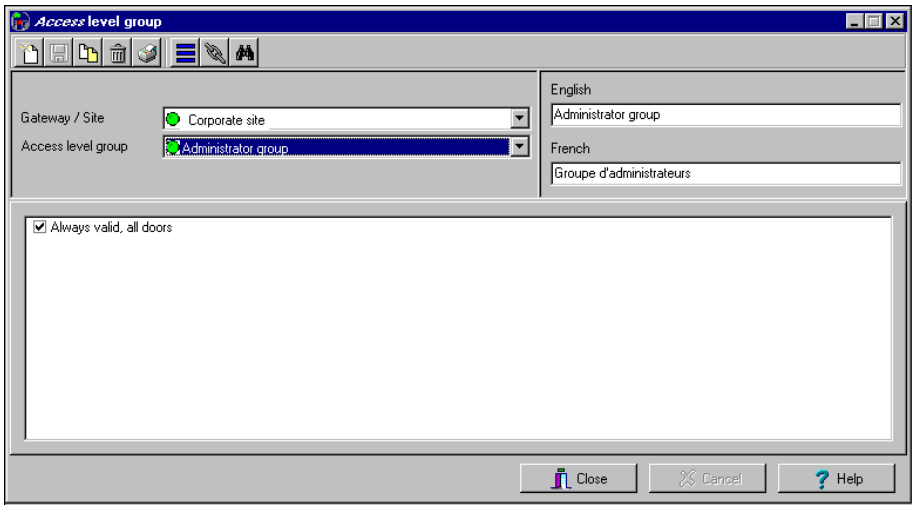
5 В списке входов выбрать компоненты, которые должны быть включены в группу.

ПРИМЕЧАНИЕ. *Подробнее смотрите в разделе "Конфигурация входов" на стр. 143.*

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.

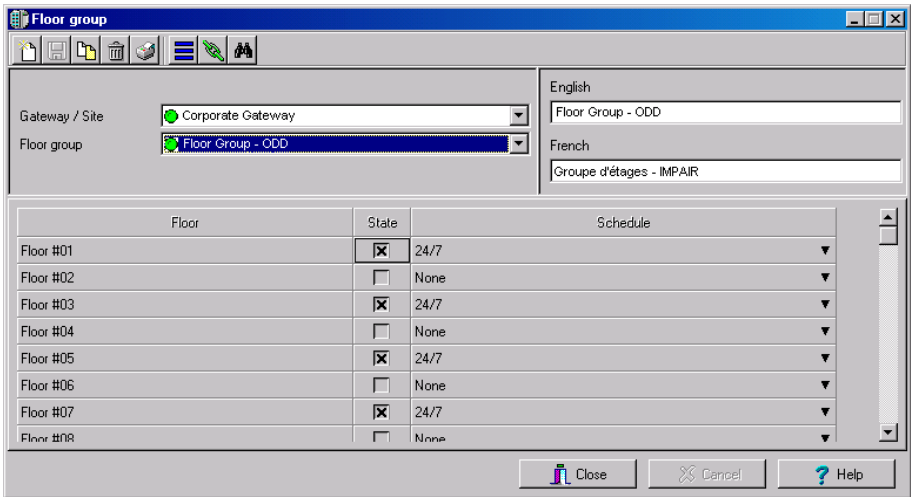
4 Нажать кнопку **New** (Создать) для создания новой группы и присвоить имя на используемых языках.

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 опускают их в считыватель, 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 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 описания входов Input > закладка Elevator),
- Владельцы карт опускают их в считыватель, чтобы получить доступ на этажи, и когда контроллер работает в автономном режиме (из-за потери связи). Для выбора будут доступны только те этажи, которые отмечены флажком “X”.

Глава 10 • Статус системы

С помощью меню **Status** операторы могут просматривать статусы 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 статистический статус всех компонентов по выбранному шлюзу. Например, можно посмотреть число входов, находящихся в тревожном состоянии.
- Кнопка **Graphic** (Графика) служит для отображения графического статуса 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.

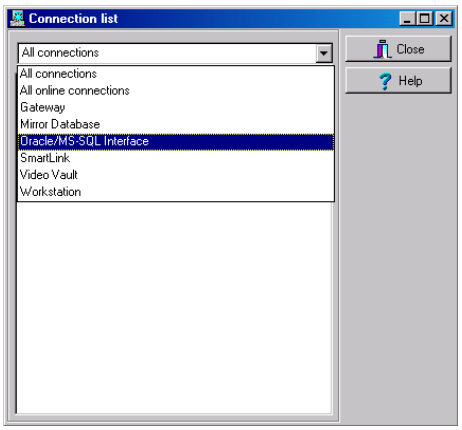
Список соединений

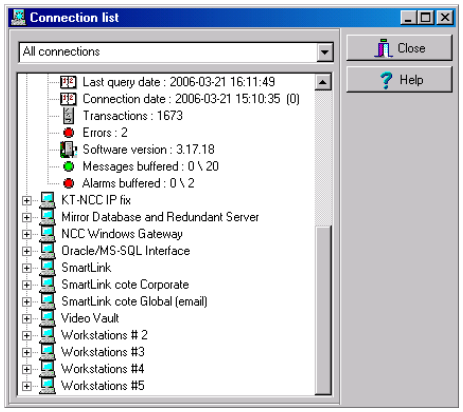
В окне Connection List (Список соединений) отображаются сведения о выделенном приложении, например, имя оператора, дата последнего запроса, локальный идентификационный номер и др. Кроме того, его можно использовать для проверки наличия связи между приложениями EntraPass и сервером.

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 ярлык 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 вызвал тревогу и др. Сведения о том, как сменить имя оператора, изложены *в разделе "Описания операторов" на стр. 322.*
- **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.

ПРИМЕЧАНИЕ. *В буферной памяти сервера может храниться до 100 000 сообщений на каждую рабочую станцию EntraPass (по умолчанию 5 000). Эти настройки можно изменить в меню описания 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 (более подробные сведения изложены в разделе "Конфигурация приложений EntraPass" на стр. 60).*

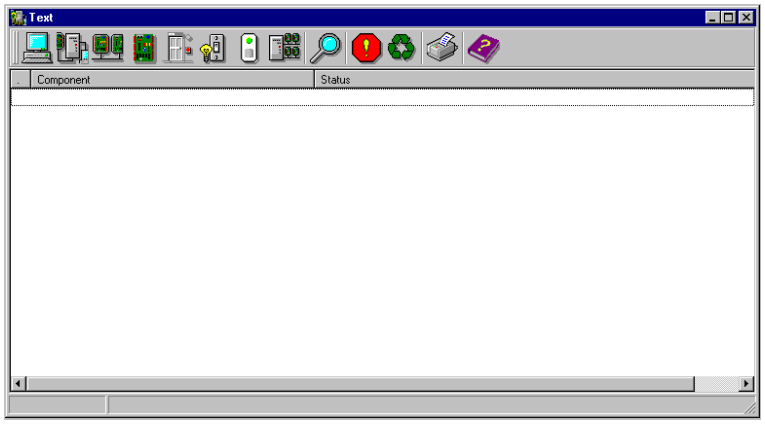
Статус текста

Окно **Text status** (Статус текста) позволяет отобразить статус 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:

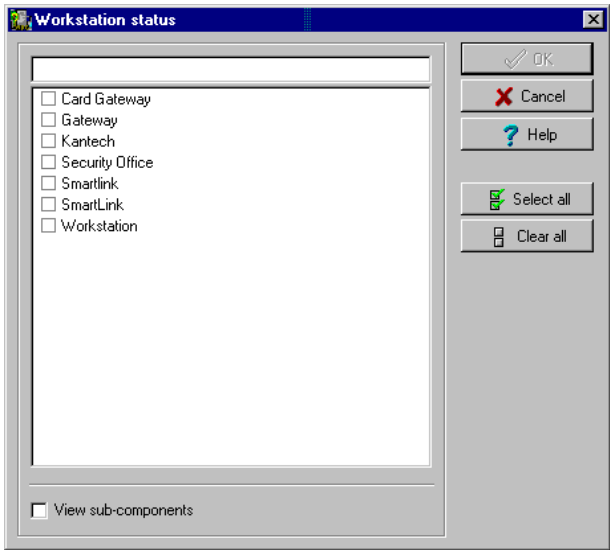
- Первые семь кнопок представляют устройства системы: Workstation (Рабочие станции), Gateway (Шлюзы), Site (Сайты), Controller (Контроллеры), Door (Двери), Input (Входы) и Output (Выходы).
- **Summary / Detailed list** (Сводка/Подробный список) – иконка лупы служит для отображения компонентов, статус 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 статуса. Функция Preview позволяет посмотреть получившийся список на экране перед выводом на печать.

Вывод на экран статусов компонентов

1 В меню **Status** (Статусы) нажать кнопку **Text Status** (Текстовый статус). 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.

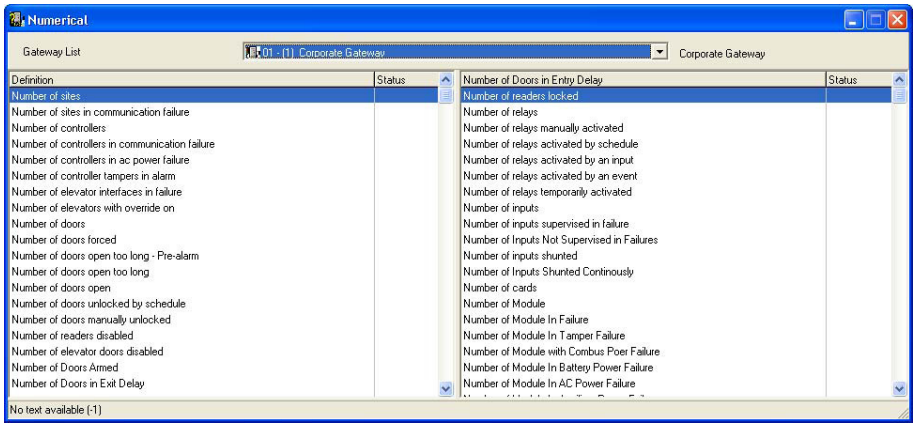
5 Для возврата к предыдущему окну с использованием выделенных опций нажать **OK.**

ПРИМЕЧАНИЕ. *Кнопка* ***Magnifying glass*** *(Экранная лупа) служит для отображения компонентов, статус которых отличается от нормы. В положении "Summary" отображаются только те компоненты, статус которых отличается от нормы. В положении "Detailed" система отображает полный статус 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 показать статус. В открывшемся окне будет показано число карт для выбранного шлюза (Number of cards), число тревожных входов (Number of inputs in alarm), число активированных вручную реле (Number of relays manually activated), число взломанных дверей (Number of doors forced open) и др. Эту функцию очень удобно использовать для определения числа описанных в системе карт.

Графический статус (Graphic Status)

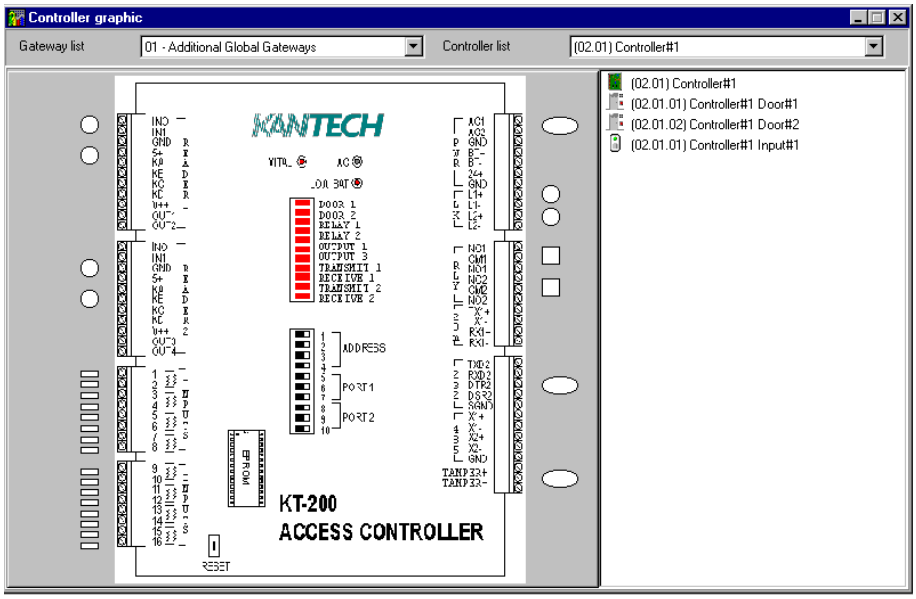
Данная функция служит для отображения графического статуса контроллера дверей, включая статус всех его компонентов (выходов, входов, подачи питания, наличия связи и пр.), в виде различных геометрических фигур разного цвета (кругов, прямоугольников и т.п.).

- 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).

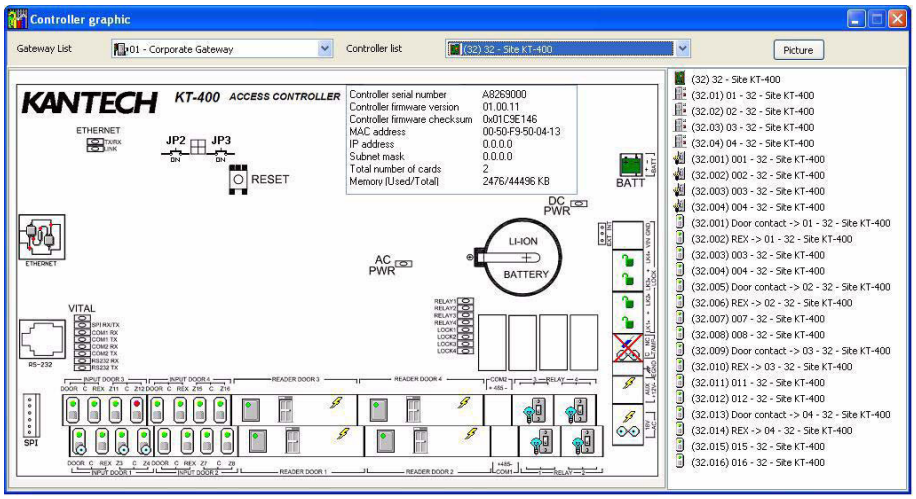
Просмотр статуса контроллера

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



ПРИМЕЧАНИЕ. *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).

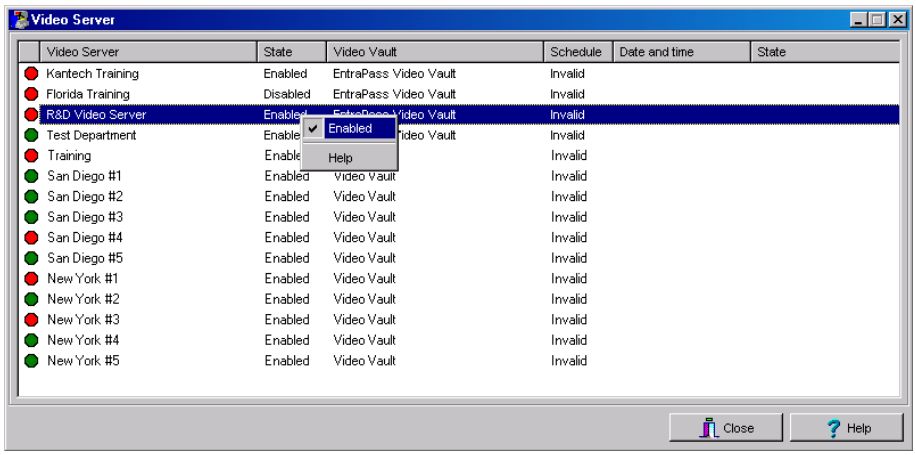
ПРИМЕЧАНИЕ. *Если на один шлюз приходится более одного сайта с контроллером, то число в скобках (xx) указывает номер контроллера, а остальные цифры обозначают номер компонента.*

Статусы видеосерверов

Эта опция используется для контроля статусов 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 статусы.

Просмотр статуса видеосерверов

1 Нажать иконку **Video Server** (Видеосерверы), предварительно открыв закладку **Status** (Статусы). В открывшемся окне Video Server будут отображаться все видеосерверы и их статусы.



- **State** (Статусы) – 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** (Статусы) – описание последней транзакции этого видеосервера с видеохранилищем EntraPass Video Vault

Разрешение/запрет создания видеоархивов

ПРИМЕЧАНИЕ. *Эта опция доступна только в случае установки видеохранилища EntraPass Video Vault.*

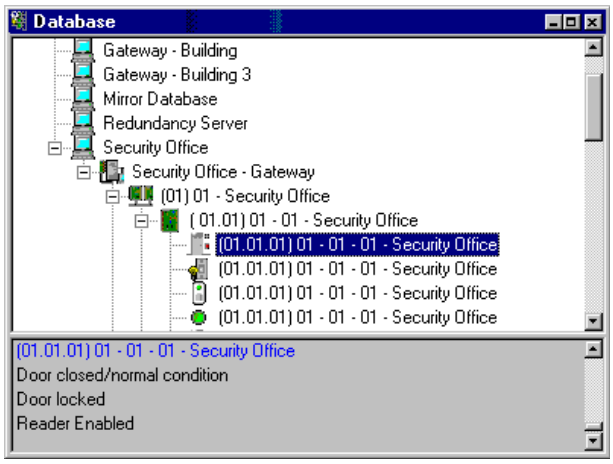
1 Правой кнопкой мыши выделить сервер, для которого требуется разрешить/запретить создание видеоархивов.

- В контекстном меню выбрать **Enable** (Разрешить), чтобы включить архивирование.
- Или выбрать в контекстном меню **Disable** (Запретить), чтобы прекратить архивирование.

Статусы баз данных

В этом окне вместе с изображением структуры базы данных показаны статусы всех её компонентов. Отображаются все приложения (не только подключенные), шлюзы, сайты 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.

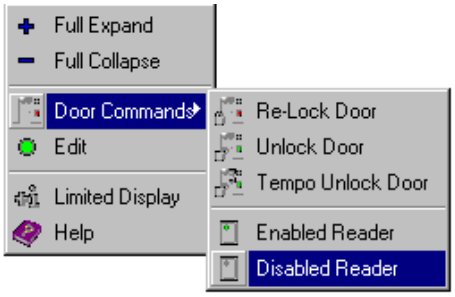


ПРИМЕЧАНИЕ. *Иконки соответствуют типу компонентов.*

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.



ПРИМЕЧАНИЕ. *Список команд в контекстном меню будет разным для разных компонентов.*

5 Внести необходимые изменения и вернуться в окно Database status. В контекстном меню, вызываемом **правой кнопкой мыши**, доступны следующие команды:

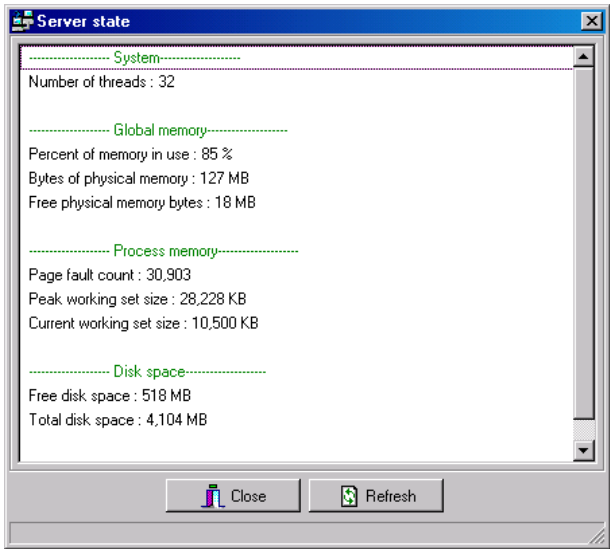
- **Full expand** (Развернуть) – эта функция позволяет полностью развернуть все ветви схемы, чтобы увидеть все компоненты. Со знаком "+" будут отображаться только те приложения, которые подключены к серверу.
- **Full collapse** (Свернуть) – эта функция позволяет полностью свернуть схему, чтобы спрятать все составляющие корневого компонента.

- **Edit** (Редактировать) – выделив включённый в схему компонент (например, вход) и вызвав меню редактирования, оператор вносит изменения в описание этого компонента в открывшемся окне описаний и 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.

ПРИМЕЧАНИЕ. *Пиктограммы, расположенные слева от компонентов, указывают их тип.*

Статусы 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 • Системные настройки

Меню **System** (Системные настройки) служит для указания настроек системных операторов, описания уровней безопасности, параметров событий, команд 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, регистрационные имена и пароли операторов системы EntraPass
- **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** (Команды) – позволяет создавать команды для тревожных сообщений и приложений SmartLink
- **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.

Описание операторов

Меню **Operator** (Операторы) служит для настройки параметров операторов, задания их уровней доступа и описания прав. Оператор отвечает 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.

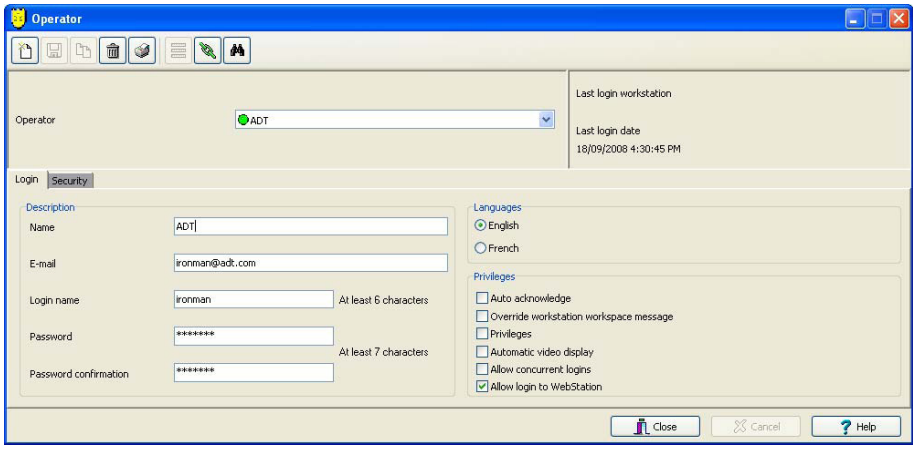
Система уже настроена на работу с тремя операторами. Все они имеют разные уровни доступа:

- 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. *Для использования других операторов необходимо изменить настройки операторов по умолчанию или создать новые записи. Более подробные сведения об уровнях доступа смотрите в разделе "Описание уровней безопасности" на стр. 326.*

Создание нового или изменение настроек уже созданного 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.

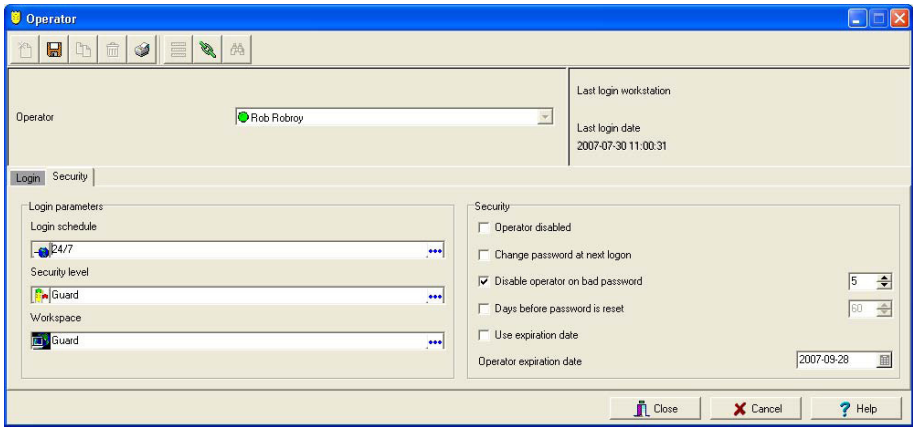
8 В разделе Privileges (Особые права):

- Если необходимо, выделить опцию **Auto acknowledge** (Автоматическое подтверждение). При выделении этой опции на рабочем столе тревог (Alarms) появляется дополнительная кнопка **Manual** (Ручной режим управления) – *смотрите раздел "Рабочие столы EntraPass" на стр. 369.* Оператор должен решить, как подтверждать события – вручную или автоматически. Это право оператора.
- Если необходимо, отметить флажком опцию **Override workstation workspace message** (Игнорировать рабочее пространство рабочей станции). В случае выделения этого поля базовая конфигурация рабочего пространства рабочей станции игнорируется, и оператор получает сообщения о событиях со всех рабочих станций и шлюзов.
- Если необходимо, отметить флажком поле **Privileges** (Особые права), чтобы для этого оператора скрытые камеры стали доступны для просмотра. Описание 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. Но если рабочий стол тревог не загружен, 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)), и если эта опция не активирована, 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 concurrent logins** - разрешить одновременно несколько входов в систему для одного оператора.
- 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** (Описания) > **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 впервые.*

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**.

ПРИМЕЧАНИЕ. *Все внесённые в профиль оператора изменения начинают действовать при следующей попытке войти в систему.*

Описание уровней безопасности пользователей

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.

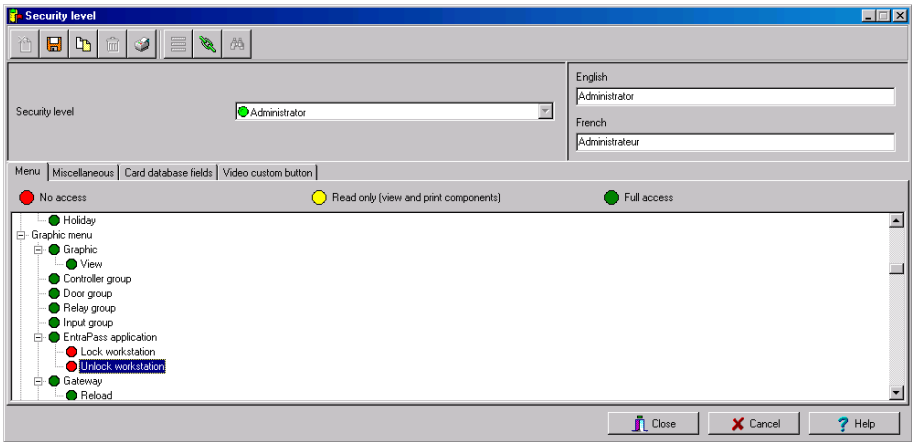
Создание/Изменение уровней доступа операторов

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)**.**

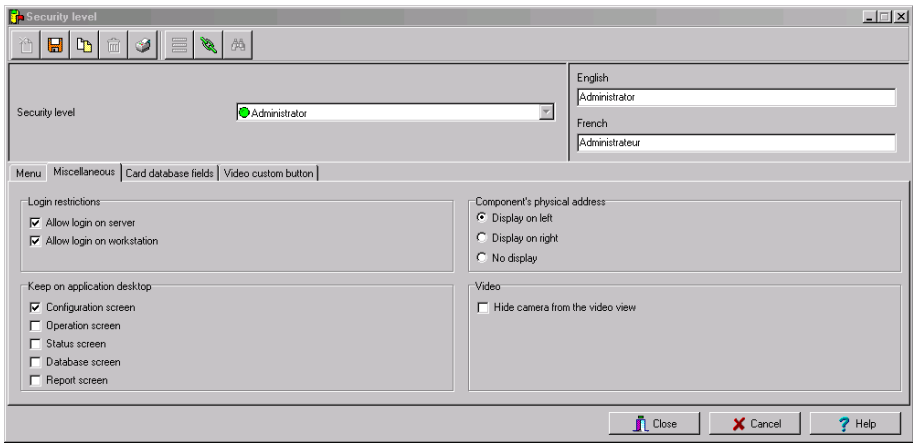
ПРИМЕЧАНИЕ. *Пользователи с правами "только для чтения" не имеют прав для вывода данных на печать в системе EntraPass.*

Описание регистрационных прав оператора

Закладка **Miscellaneous** (Прочее) содержит описание регистрационных прав операторов и параметров отображения на экране различной информации:

- В разделе "Login restrictions" можно разрешить/запретить оператору регистрироваться на рабочей станции или на сервере EntraPass.
- Раздел "Keep on application desktop" служит для выбора активных окон, которые могут находиться на рабочем столе оператора.
- В следующем разделе следует указать, отображать ли на экране физический адрес компонента (Component's physical address). Физический адрес компонента может находиться слева (on left) или справа (on right) от его имени.

1 Открыть закладку **Miscellaneous,** чтобы настроить параметры выбранного уровня безопасности.



2 В разделе **Login restrictions** (Ограничения на регистрацию) 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 системы.

3 Раздел **Keep on application desktop** 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 операций) – к этой категории относятся все пункты меню Operations и функция просмотра видеозаписей.
- **Status screen** (Окно статусов) – в эту группу входят окна меню Status (Статусы), 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.

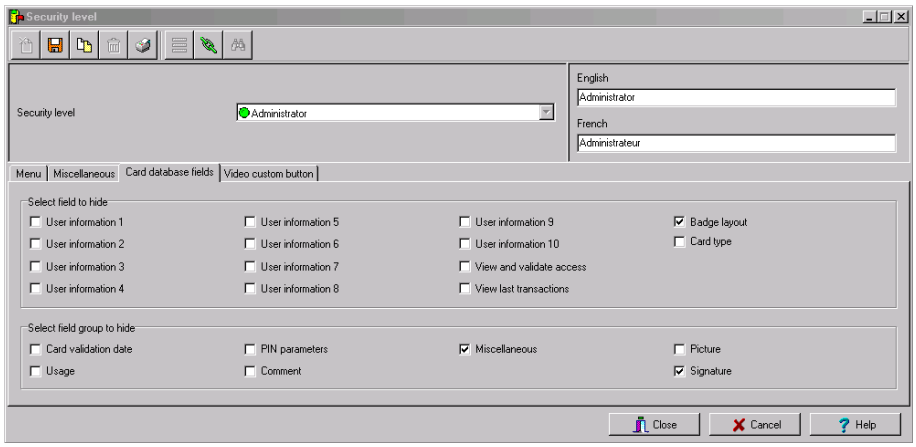
5 В случае использования функции видеонаблюдения программное обеспечение EntraPass позволяет запретить видеонаблюдение на отдельных объектах для определённых уровней доступа операторов, используя опцию **Hide camera from video views** (Скрыть камеры от видеонаблюдения).

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. Подробнее смотрите раздел "Ограничение доступа к отдельным камерам наблюдения" на стр. 346.*

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 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.



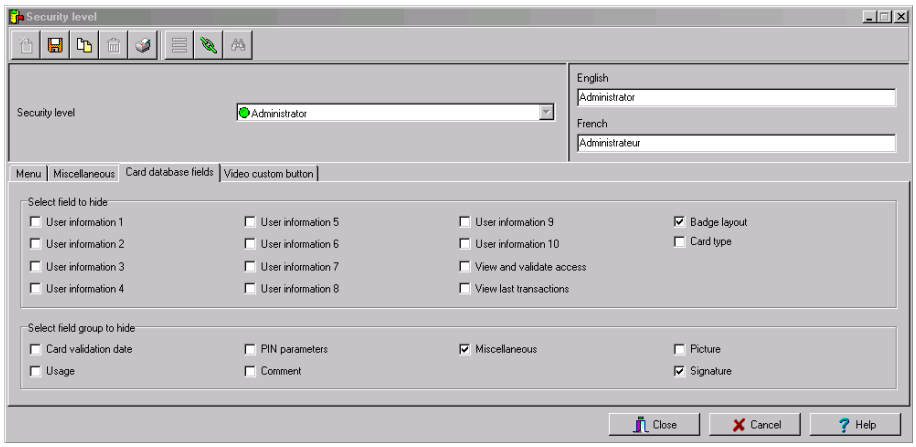
2 Указать поля (по отдельности или группами), которые должны быть скрыты для пользователей с выбранным уровнем безопасности. В приведённом выше примере операторы с уровнем безопасности Guard (Охранник), не будут видеть поля, отмеченные флажками.

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 рабочий стол видеонаблюдения добавляют 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.*

Описание 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.).

Операторы, для которых 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 впервые.*

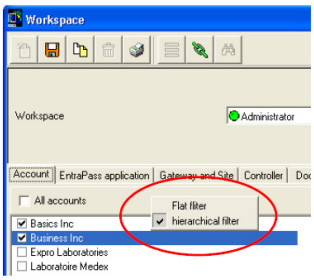
Использование фильтров для рабочего пространства

Предусмотрено два способа отбора компонентов рабочего пространства в системе EntraPass:

- **Regular filter** (Обычный фильтр) – отображаются все компоненты системы, которые было указано отображать при создании рабочего пространства. Доступна навигация по всем закладкам меню и выбор любых компонентов без разбора. Чтобы увидеть и выделить дочерний компонент (дверь, например), не требуется выделять родительский компонент (в данном случае, контроллер).
- **Hierarchical filter** (Иерархический фильтр) – компоненты в списке отображаются в зависимости от того, какой родительский компонент был выбран. Например, при выборе сайта (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. Эта опция доступна только при работе со следующими закладками: **Entrapass application** (Приложения Entrapass), **Gateway and Site** (Шлюзы и сайты), **Controller** (Контроллеры), **Door** (Двери), **Relay** (Реле), **Input** (Входы) и **Access level** (Уровни доступа).

ПРИМЕЧАНИЕ. *Если в закладке ничего не отображается, следует убедиться, что указанные компоненты действительно относятся к выбранному родительскому объекту.*

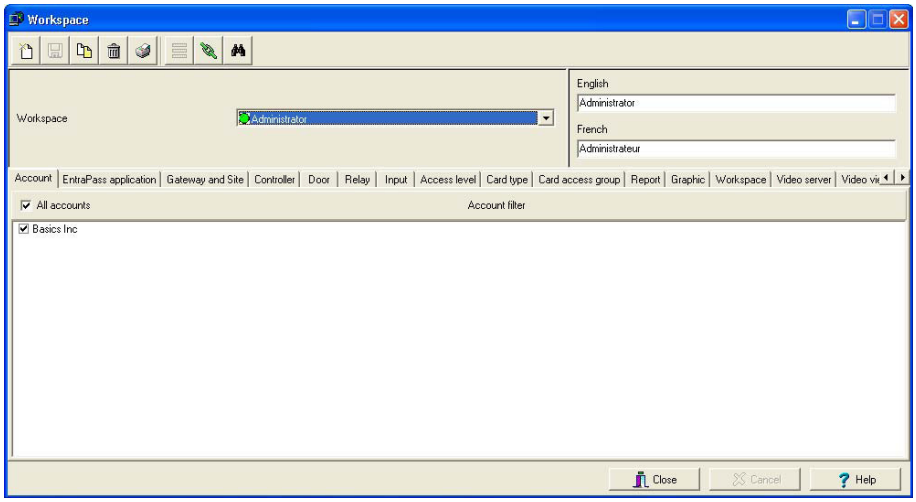
1. Для того чтобы переключиться из обычного режима отбора в иерархический или обратно, рекомендуется воспользоваться контекстным меню, которое вызывается щелчком правой кнопкой мыши по строке заголовка внутри каждой закладки окна Workspace. Активный режим отбора выделен флажком.
2. Выбранный режим отбора становится активным во всех закладках.



Выбор учётных записей

Эта функция позволяет выделить те учётные записи, которые будут доступны оператору, за которым закреплено данное рабочее пространство.

1 В выпадающем списке **Workspace** (Рабочее пространство) выбрать, какое рабочее пространство необходимо настроить или изменить.



- Чтобы создать новое рабочее пространство, следует нажать кнопку **New** (Создать) и ввести необходимые данные на используемых языках в полях справа.
- Если необходимо, выделить поле **All accounts** (Все учётные записи), чтобы сделать доступными все отображаемые на экране учётные записи для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые учётные записи из общего списка.

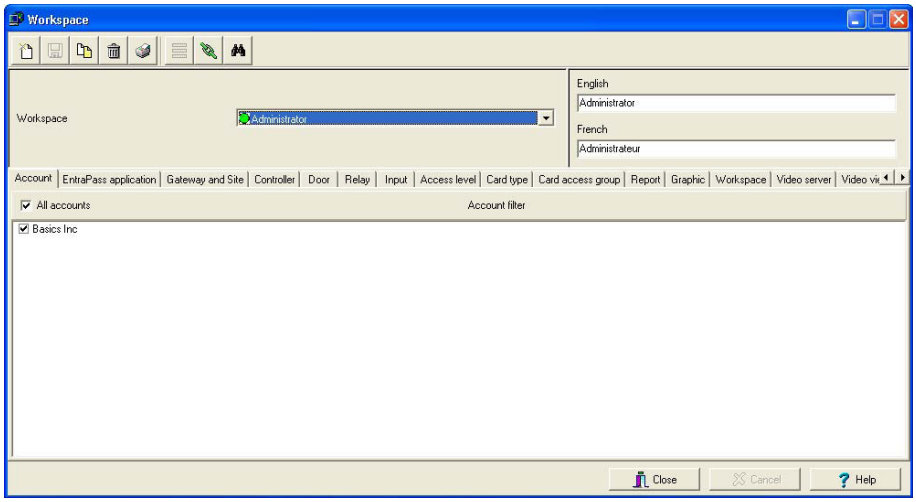
2 Сохранить внесённые изменения.

Выбор приложений EntraPass

Эта функция позволяет выделить приложения, доступные оператору, за которым закреплено данное рабочее пространство.

В приведенном ниже примере администраторы (Administrator) не будут видеть сообщения, отправленные с приложения SmartLink, потому что это приложение не включено в их рабочее пространство.

1 Открыть закладку **Workspace** (Рабочее пространство) и выбрать, какое рабочее пространство необходимо настроить или изменить.



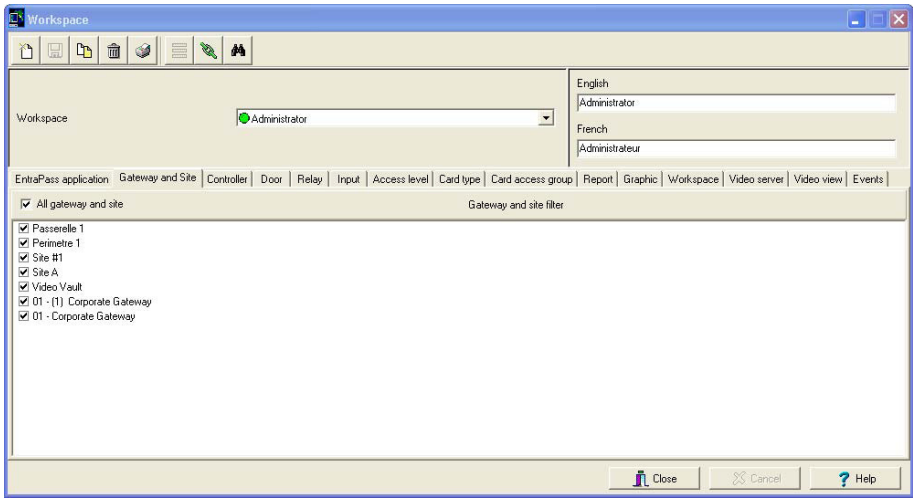
ПРИМЕЧАНИЕ. *Если для выбранного оператора разрешена опция Network alarms message desktop (Рабочий стол сообщений о сетевых тревогах), настраиваемая в меню Desktops (Рабочие столы), то на экране будут отображаться только те тревожные события, которые возникли в указанных в этом окне приложениях и компонентах 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.

Описание шлюзов и сайтов

1 Открыть закладку **Gateway and Site** (Шлюзы и сайты), чтобы выделить список шлюзов и сайтов, доступных оператору, за которым закреплено данное рабочее пространство.

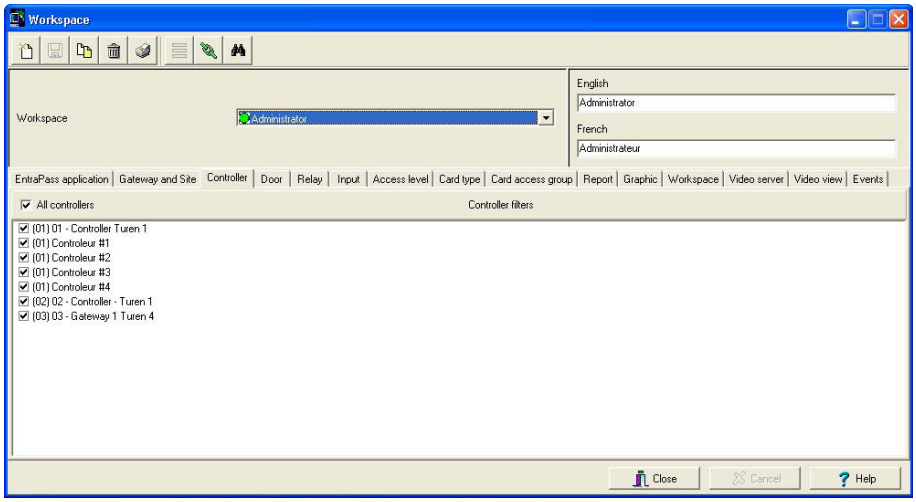


- Если необходимо, выделить опцию **All gateways and sites** (Все шлюзы и сайты), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все шлюзы и сайты, отображаемые на экране.
- Либо выделить определённые шлюзы и сайты из общего списка.

2 Сохранить внесённые изменения.

Описание контроллеров

1 Открыть закладку **Controller** (Контроллеры), чтобы выделить список контроллеров, доступных оператору, за которым закреплено данное рабочее пространство.



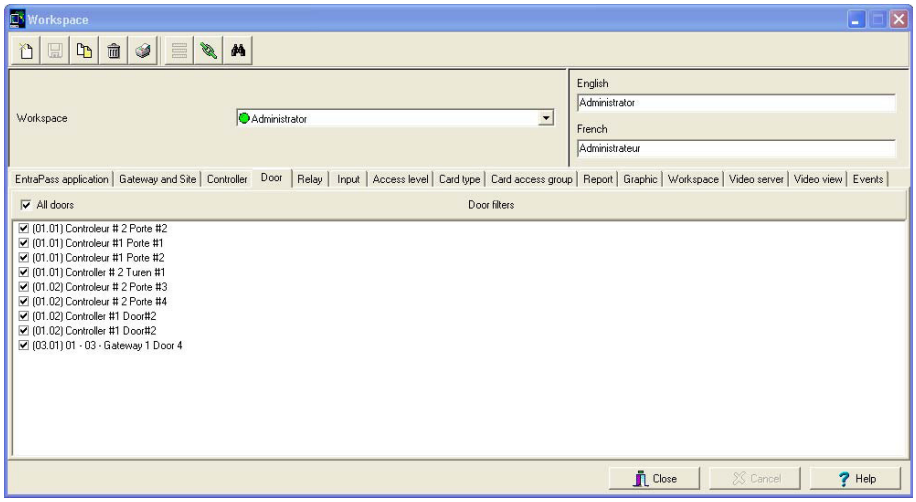
- Если необходимо, выделить опцию **All controllers** (Все контроллеры), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все контроллеры, отображаемые на экране.
- Либо выделить определённые контроллеры из общего списка.

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.*

Описание дверей

1 Открыть закладку **Door** (Двери), чтобы выделить список дверей, доступных оператору, за которым закреплено данное рабочее пространство.

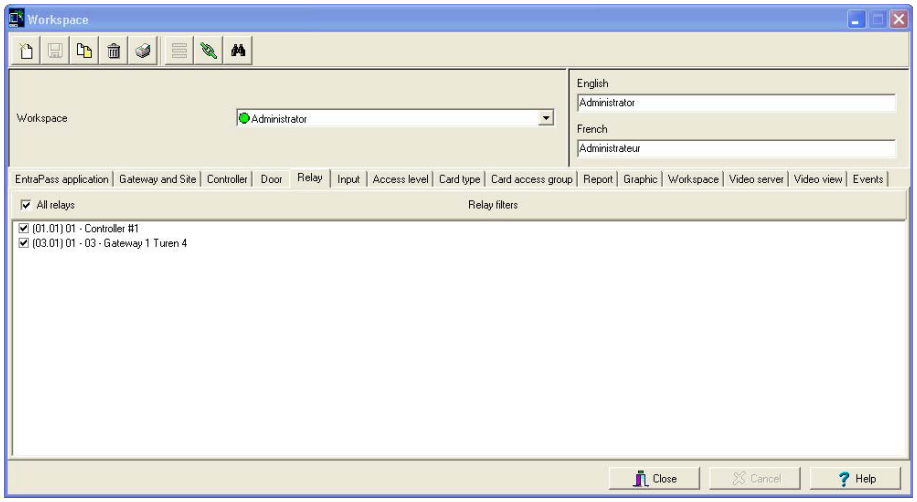


- Если необходимо, выделить опцию **All doors** (Все двери), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все двери, отображаемые на экране.
- Либо выделить определённые двери из общего списка.

2 Сохранить внесённые изменения.

Описание реле

1 Открыть закладку **Relay** (Реле), чтобы выделить список реле, доступных оператору, за которым закреплено данное рабочее пространство.

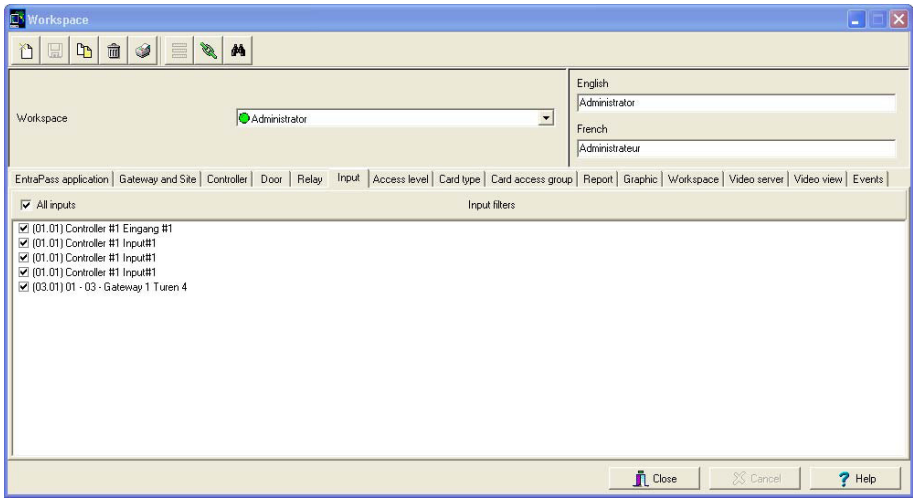


- Если необходимо, выделить опцию **All relays** (Все реле), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все реле, отображаемые на экране.
- Либо выделить определённые реле из общего списка.

2 Сохранить внесённые изменения.

Описание входов

1 Открыть закладку **Input** (Входы), чтобы выделить список входов, доступных оператору, за которым закреплено данное рабочее пространство.



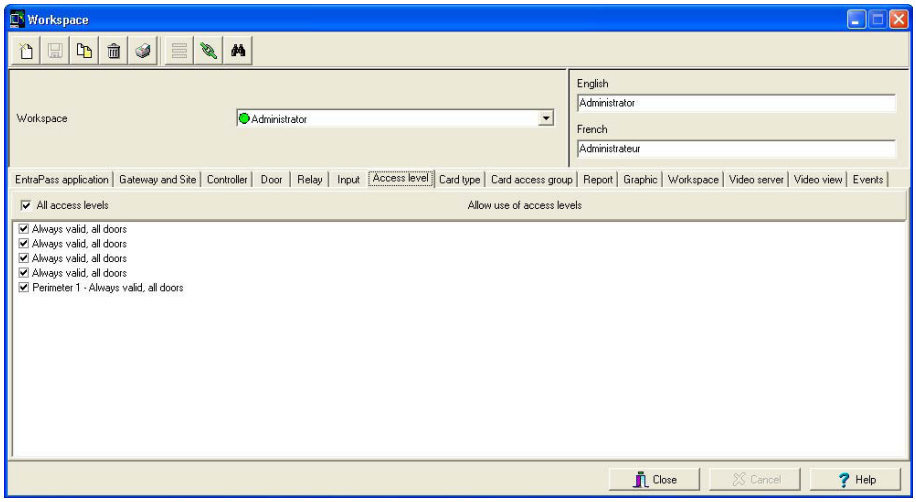
- Если необходимо, выделить опцию **All inputs** (Все входы), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все входы, отображаемые на экране.
- Либо выделить определённые входы из общего списка.

2 Сохранить внесённые изменения.

Задание 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.

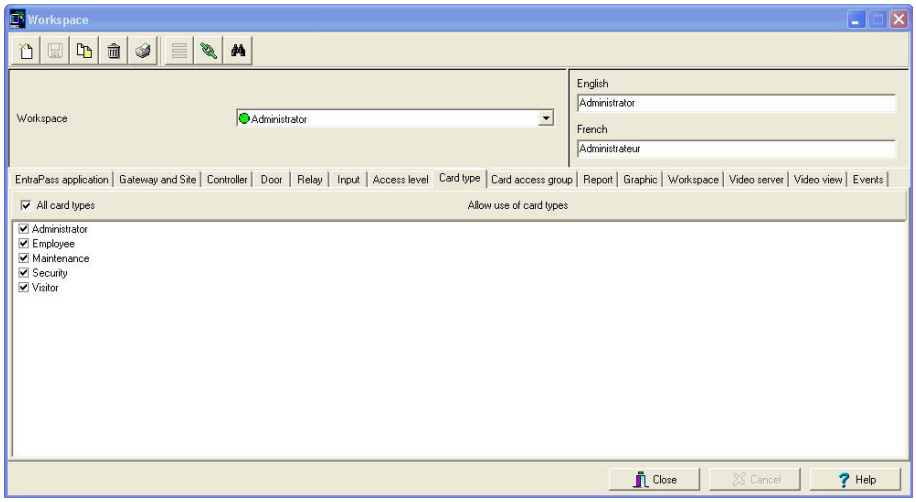
2 Сохранить внесённые изменения.

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.*

Описание 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.



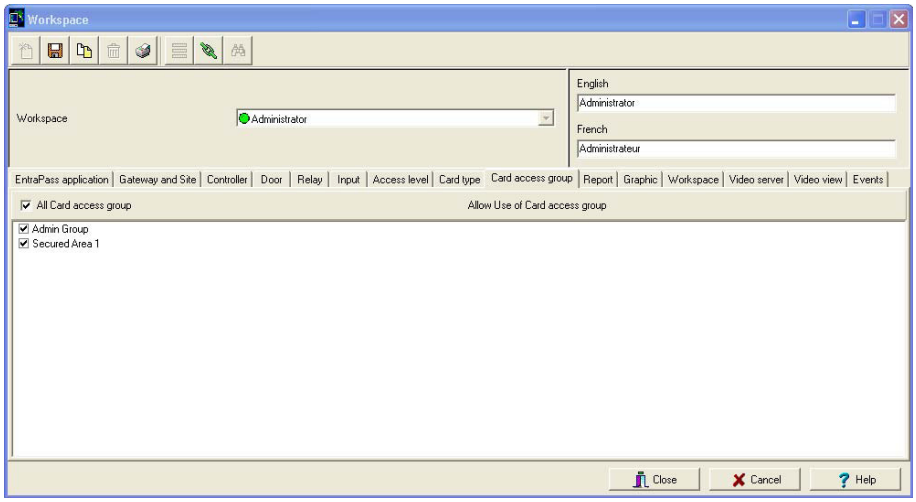
- Если необходимо, выделить опцию **All card types** (Все типы карт), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все типы карт.
- Либо выделить определённые типы карт из общего списка.

2 Сохранить внесённые изменения.

Описание 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.



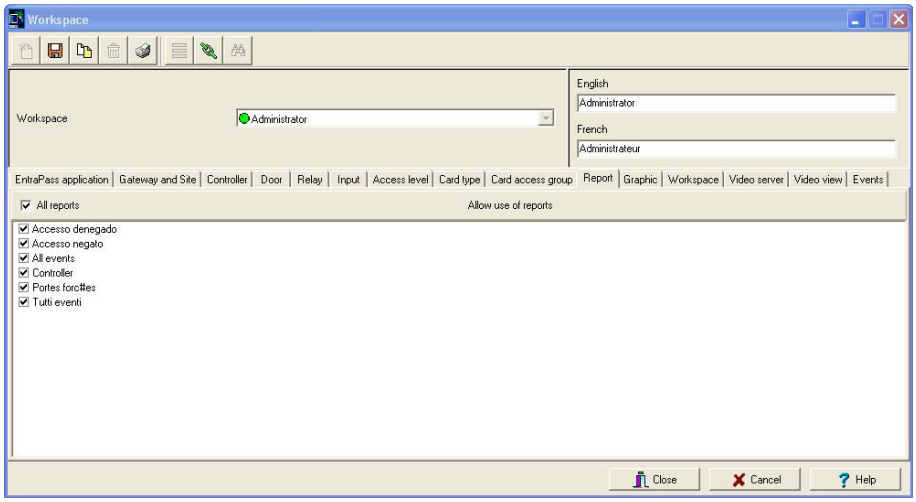
- Если необходимо, выделить опцию **All Card access group** (Все группы доступа карт), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все отображаемые на экране группы доступа карт.
- Либо выделить определённые группы доступа из общего списка.

2 Сохранить внесённые изменения.

Описание 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.

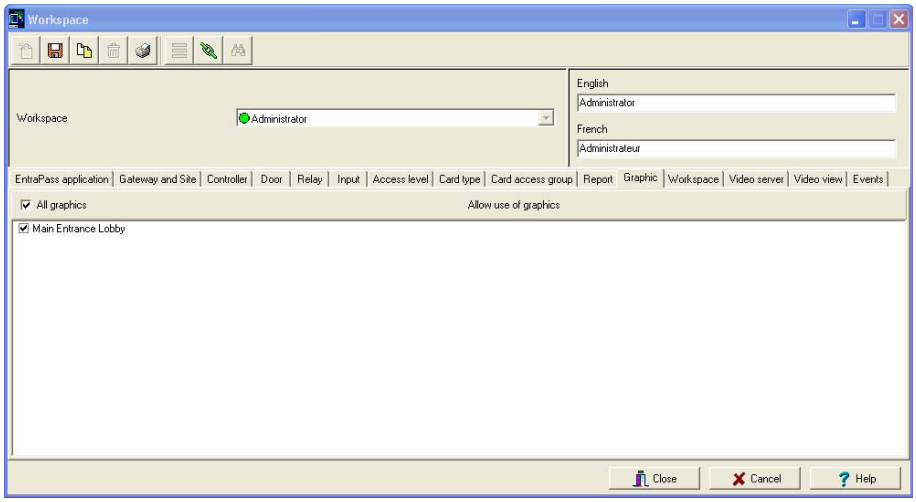


- Если необходимо, выделить опцию **All reports** (Все отчёты), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все отчёты.
- Либо выделить определённые отчёты из общего списка, отображаемого на экране.

2 Сохранить внесённые изменения.

Описание графических схем

1 Открыть закладку **Graphics** (Схемы), чтобы выделить список схем, доступных оператору, за которым закреплено данное рабочее пространство.



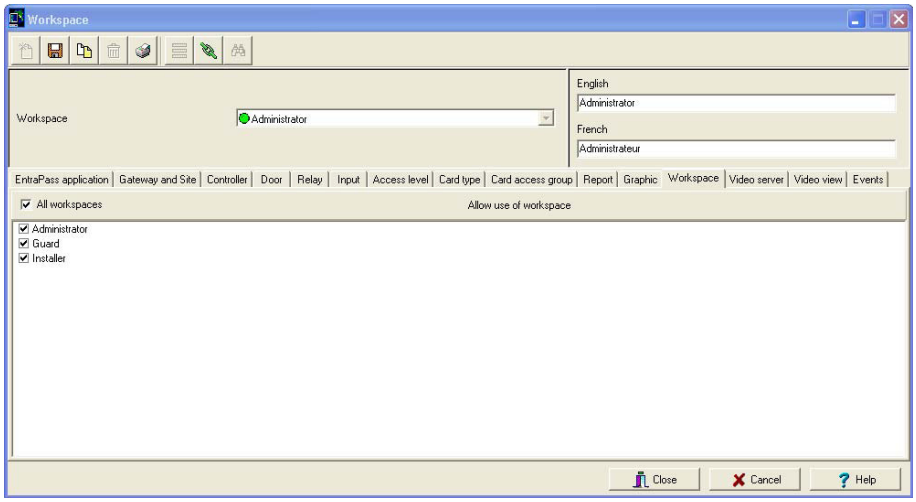
- Если необходимо, выделить опцию **All graphics** (Все схемы), чтобы оператору, за которым закреплено данное рабочее пространство, были доступны все схемы.
- Либо выделить определённые схемы из общего списка.

2 Сохранить внесённые изменения.

Описание 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.



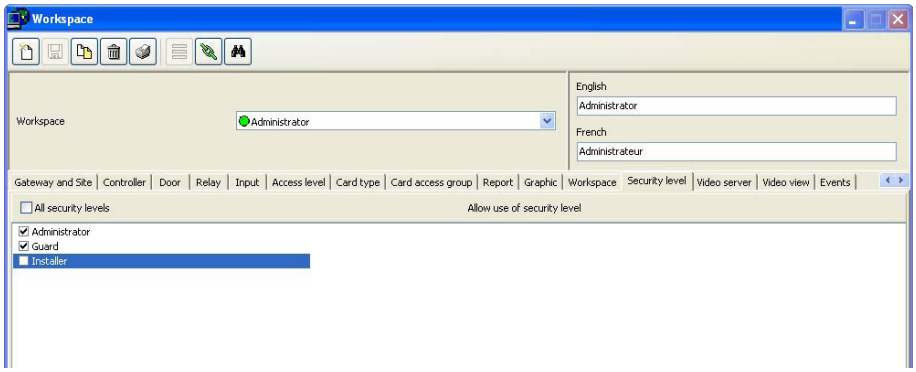
- Если необходимо, выделить поле **All workspaces** (Все рабочие пространства), чтобы сделать доступными все рабочие пространства из списка для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые позиции из общего списка.

2 Сохранить внесённые изменения.

Задание уровней безопасности

Эта функция даёт возможность системным администраторам назначать определённые уровни безопасности для выбранного рабочего пространства. В проиллюстрированном ниже примере рабочее пространство администратора доступно только пользователям, имеющим уровень безопасности **Administrator** (Администратор) и **Guard** (Охранник). А пользователи с уровнем **Installer** (Установщик) не будут иметь доступ к этому рабочему пространству. Выбранные уровни безопасности будут действовать для всех операторов, работающих в этом рабочем пространстве.

1 Открыть закладку **Security level** (Уровни безопасности), чтобы выбрать уровни безопасности для данного рабочего пространства. Если необходимо создать новый уровень безопасности, смотрите раздел "Описание уровней безопасности" на стр. 326.



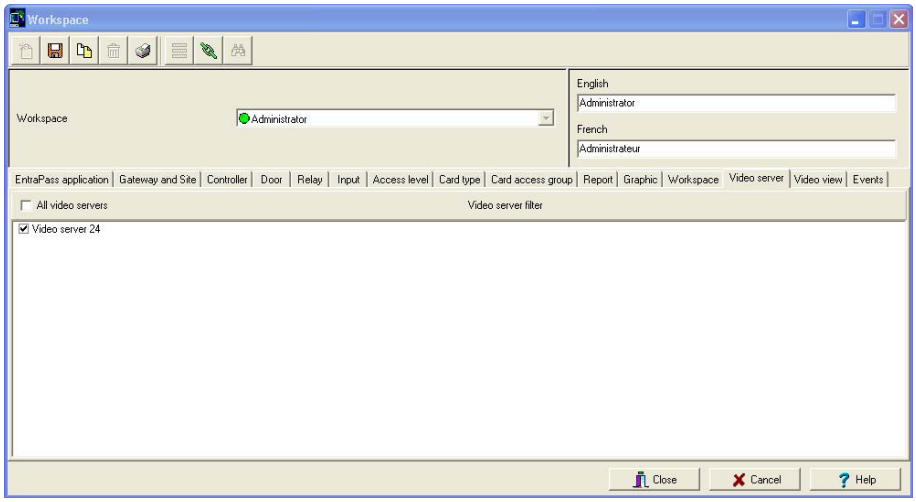
- Выбрать опцию **All security levels** (Все уровни безопасности), чтобы назначить все уровни для данного рабочего пространства.
- Либо выделить определённые уровни безопасности из общего списка.

2 Сохранить внесённые изменения.

Описание 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.*

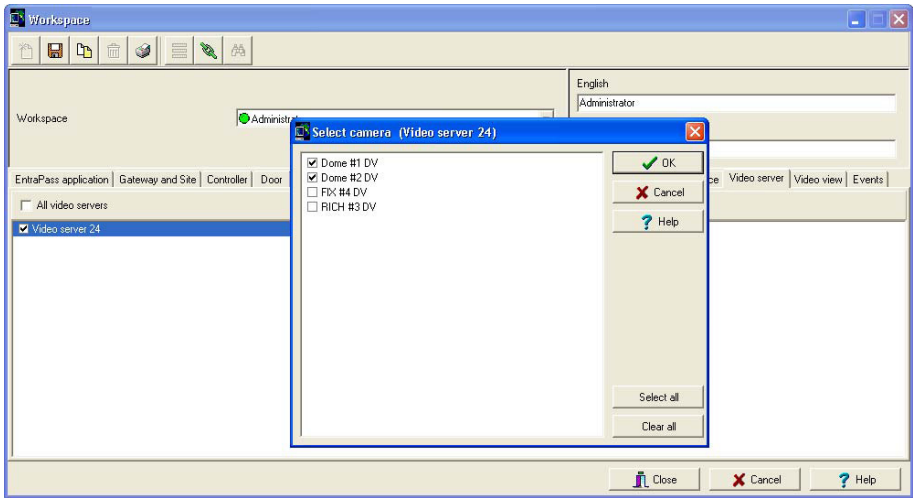
Ограничение доступа для определённых камер наблюдения

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).



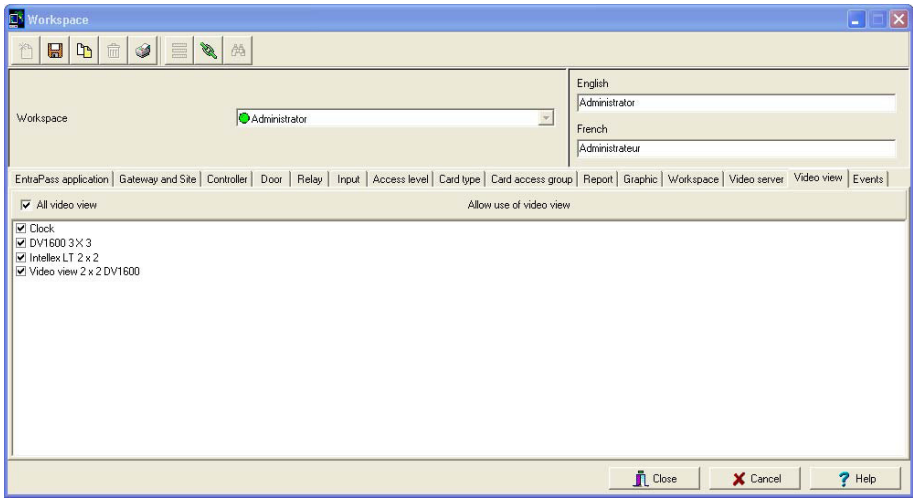
3 В окне Select camera снять выделение с тех камер, которые должны быть скрыты от наблюдения при работе в данном рабочем пространстве.

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.

Описание окон видеонаблюдения

1 Открыть закладку **Video views** (Видеоокна), чтобы выделить список видеоокон, доступных оператору, за которым закреплено данное рабочее пространство.



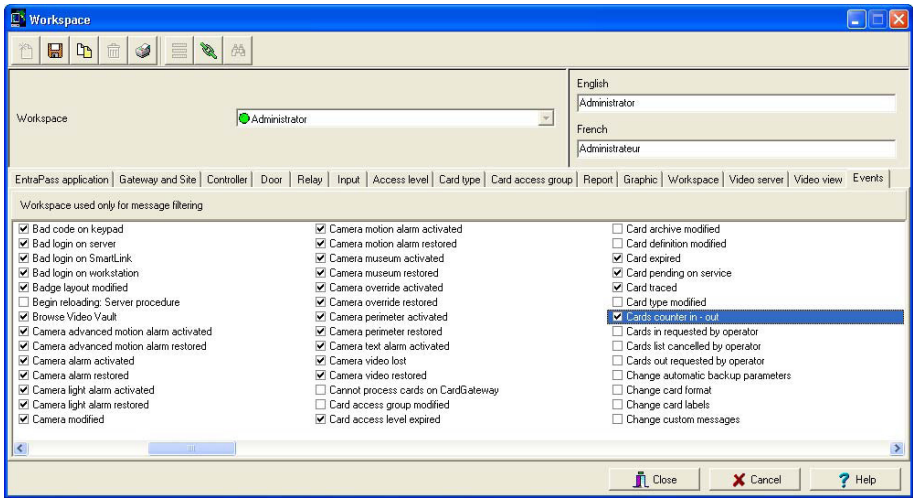
- Если необходимо, выделить поле **All video views** (Все видеоокна), чтобы сделать доступными все видеоокна из списка для оператора, за которым закреплено данное рабочее пространство.
- Либо выделить определённые видеоокна из общего списка.

2 Сохранить внесённые изменения.

Описание событий

Этот раздел меню служит для описания 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.

Описание параметров событий

Описание 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 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".

Описание 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 команд для оповещения 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.

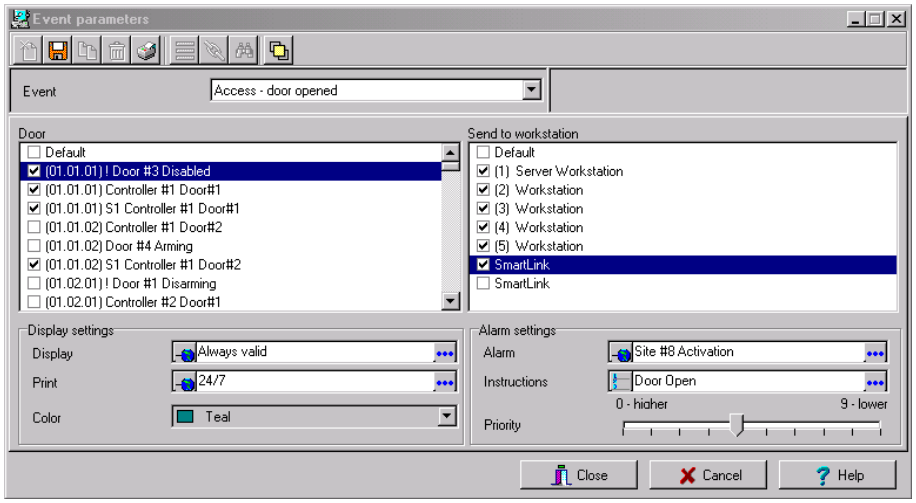
Связи по умолчанию		Замечания
Компонент	**Рабочая станция**	
Настройки по умолчанию	Настройки по умолчанию	Сообщения обо всех событиях, поступающие со всех компонентов, посылаются на все рабочие станции.
Настройки по умолчанию	Специальные настройки (Рабочая станция 2)	Сообщения обо всех событиях, поступающие 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** – 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		Замечания
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. *Специальные связи 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 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 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.*

3 В разделе **Display settings** (Параметры отображения) указать опции для отображения на экране: по умолчанию все события должны посылаться на рабочие столы сообщений (Message) на все рабочие станции EntraPass, настроенные 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.*

4 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.

5 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.

6 В меню **Alarm Settings** (Параметры тревог) необходимо выполнить следующие настройки:

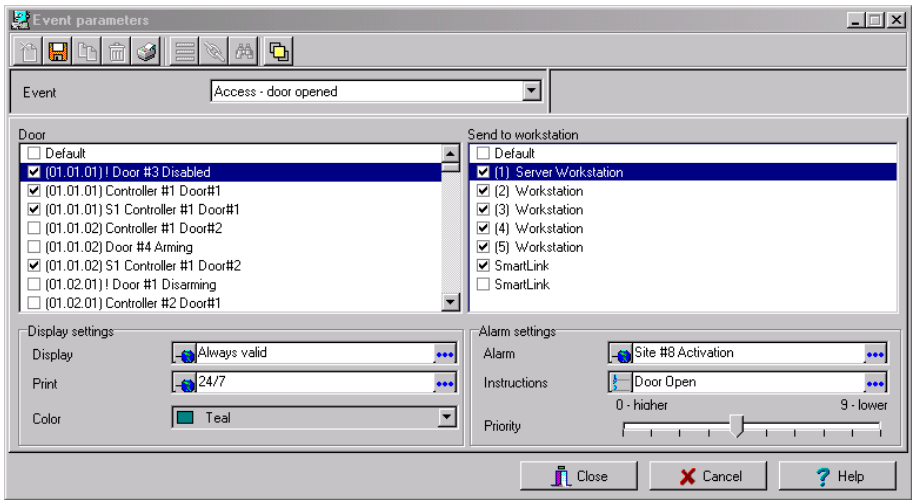
- **Alarm** (Тревога/расписание) – в период действия расписания сообщение о выбранном событии будет отправлено на рабочий стол тревог (Alarms) на выбранных рабочих станциях и будет требовать подтверждения оператора.
- **Instructions** (Команды) – выбрать команду, которая будет отправлена на рабочий стол команд (Instruction) при появлении события, требующего подтверждения. Команды будут посылаться только во время действия расписания тревог.

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.*

7 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).

Создание связей

1 В окне Event parameters (Параметры событий) выбрать событие из выпадающего списка **Event** (События). На панели компонентов (слева) выбрать компонент и затем выбрать рабочую станцию EntraPass, на которую будет отправляться сообщение о событии.

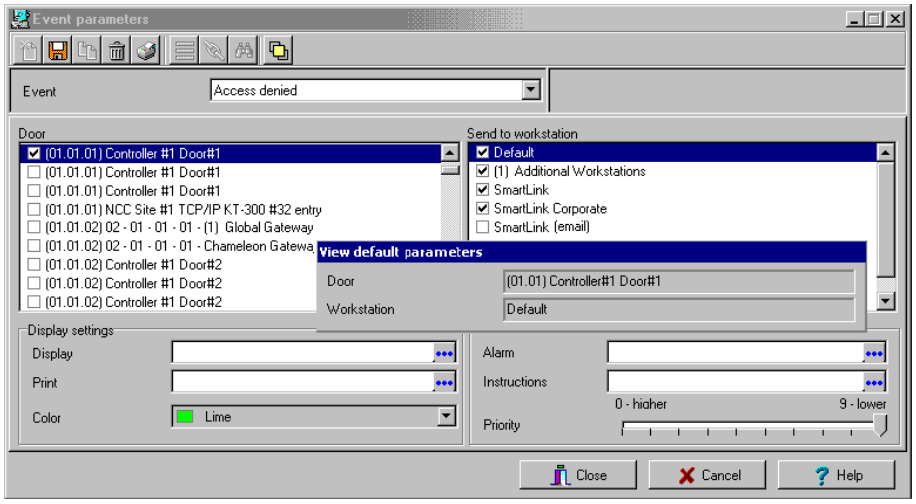


2 Нажать **Save** (Сохранить) для создания новой связи. В приведённом на иллюстрации примере сообщение о событии "*All access - Door opened" (Полный доступ – дверь открыта),* возникающем на выбранной двери, отправляется на указанную рабочую станцию (выделена на панели справа).

ПРИМЕЧАНИЕ. *Кнопка **Save** (Сохранить) становится доступной только после создания связи между выделенным событием и компонентом.*

Просмотр связей

1 На панели компонентов (слева) выбрать компонент и затем выбрать приложение EntraPass, в которое будет отправляться сообщение о событии.



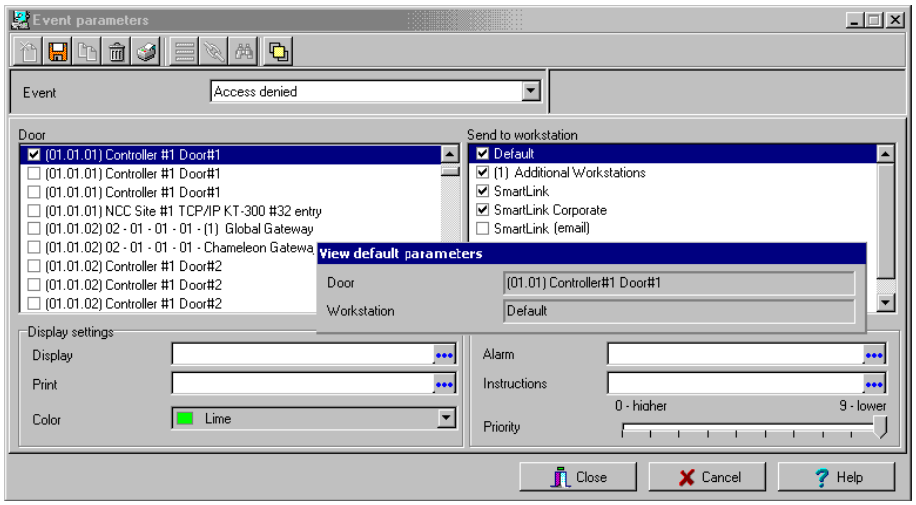
2 Нажать на панели инструментов кнопку **View association** (Посмотреть связи). В окне View default parameters (Посмотреть параметры по умолчанию) будет показано, как настроены параметры события: по умолчанию (Default) или нет.

3 Чтобы закрыть окно View default parameters, щёлкнуть по иконке **View association**.

Удаление и восстановление связей

В какой-то момент может потребоваться, чтобы сообщения о событии, связанном с определённым компонентом, перестали отправляться на рабочий стол Message на всех рабочих станциях 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 событие из списка **Event** (События), которое необходимо изменить.



2 Нажать на панели инструментов кнопку **Delete** (Удалить).

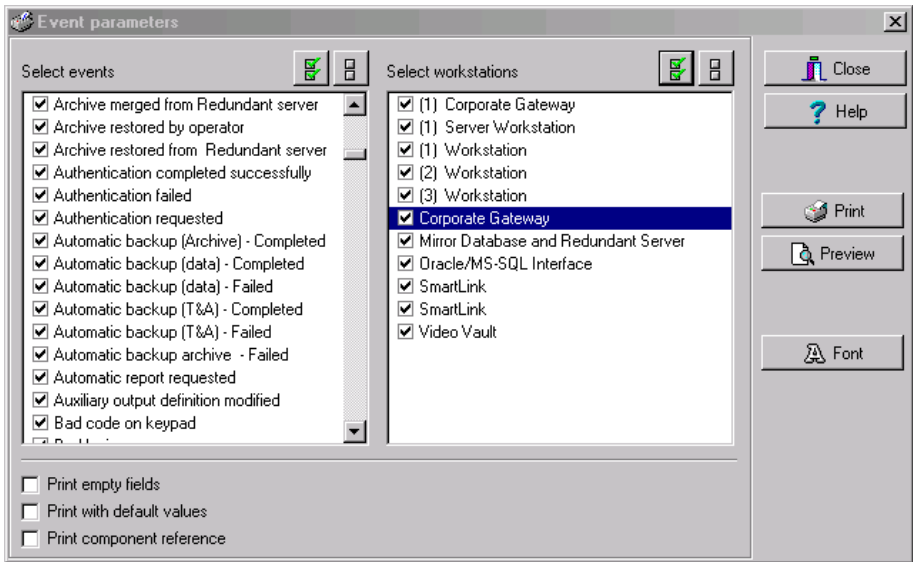
3 В окне Delete event parameters (Удалить параметры событий) выбрать одну из следующих опций:

- **Restore default** (Восстановить настройки по умолчанию) – применить заводские настройки к параметрам тревог и параметрам отображения.
- **Delete association** (Удалить связь) – 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 выбранных событий (параметры тревог и параметры отображения).

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 связи (без связей по умолчанию). Если специальные связи не назначены (компонент X и рабочая станция Y), то отчёт окажется пустым.*

- **Print components reference** (Печатать ссылки компонентов) – печатать физический адрес вместе с 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.

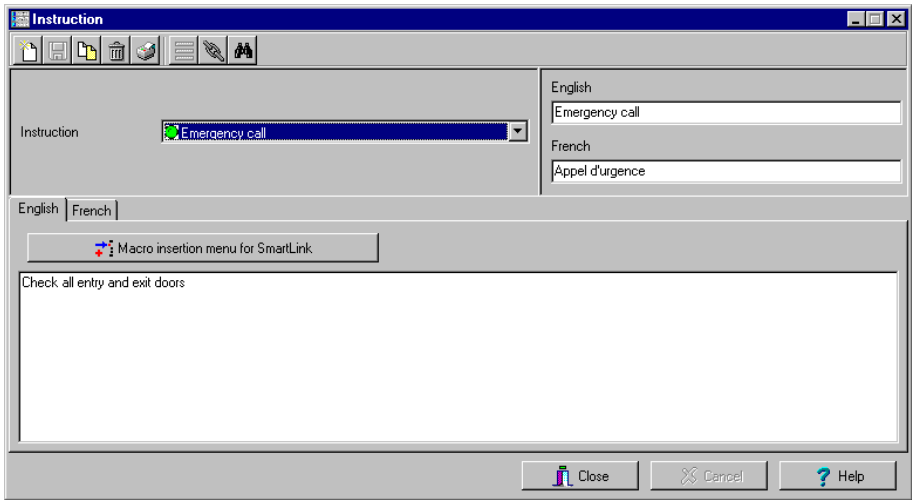
Описание команд

Этот раздел меню служит для описания команд, которые должны быть привязаны к определённым событиям. При формировании сигнала тревоги эти команды будут отображаться в окне Instruction (меню рабочих столов Desktop) для подтверждения.

Как правило, каждая строка содержит одну команду; ответные серии команд состоят из нескольких команд (строк). Таким образом удаётся обеспечить более высокую гибкость на случай, если необходимо внести изменения.

Описание команд

1 В главном окне **System** (Системные настройки) нажать на иконку **Instruction** (Команды).



2 Чтобы создать новую команду, нажать на кнопку **New** (Создать). Чтобы изменить уже созданную команду, выбрать её из выпадающего списка **Instruction.**

3 Назначить имя/идентификатор команды в соответствующих полях для каждого применяемого языка.

4 Выбрать закладку с названием одного из применяемых языков, чтобы ввести команду. Команды вводят только на *одном* выбранном языке.

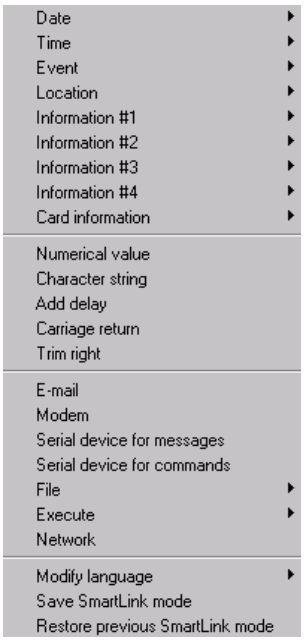
ПРИМЕЧАНИЕ. *В каждой команде можно ввести до 511 символов (включая пробелы).*

5 Чтобы связать команду с событиями, выполнить указания раздела "Описание параметров событий" на стр. 350.

Описание команд SmartLink

Меню описания команд Instruction позволяет создавать команды SmartLink. Если приложение SmartLink установлено, то пользователям доступна кнопка Macro-insertion для использования макрокоманд. Она позволяет отправлять в приложение SmartLink встроенные макрокоманды.

1 В окне Instruction нажать на кнопку **Macro insertion menu for SmartLink** (Меню макрокоманд для SmartLink) или вызвать контекстное меню правой кнопкой мыши.



ПРИМЕЧАНИЕ. *При создании серий команд для приложения SmartLink достоверными будут считаться только команды, написанные на основном языке. Подробные сведения о макрокомандах изложены в брошюре "Справочное руководство по SmartLink".*

Опции, доступные в этом меню, приведены ниже в таблице:

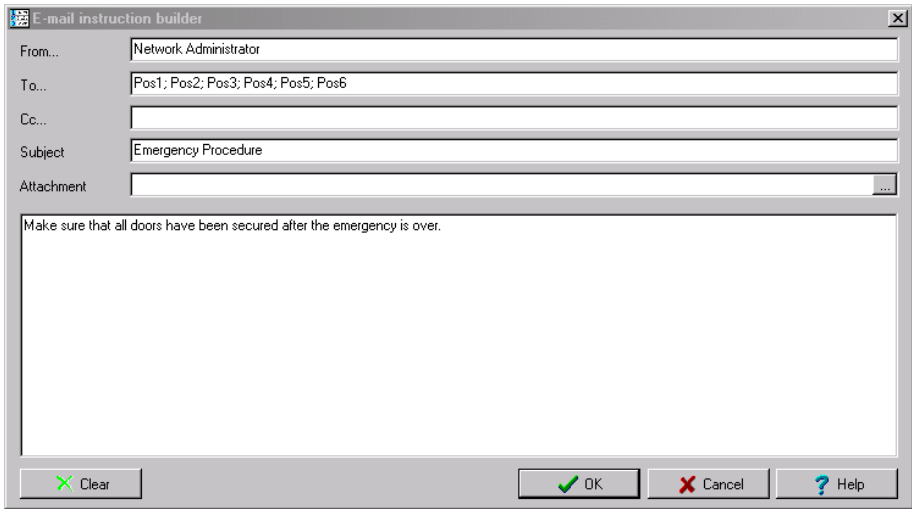
Параметр	Описание
Date (Дата)	Добавить дату в команду. Доступные опции: **Year** (год), **Month** (месяц), **Day** (день), **YYYY/MM/DD** или **MM/DD/YYY** (YYYY – год, MM – месяц, DD - день)
Time (Время)	Добавить в команду время. Доступные опции: **Hour** (часы), **Minute** (минуты), **Second** (секунды), **HH:MM:SS** или **HH:MM** (HH – часы, MM – минуты, SS - секунды).
Event (Событие)	Добавить в команду описание события. Отображается имя события (**Text**) или его номер (**Number**).
Location (Место)	Указать место, где будет действовать команда. Доступные опции: **EntraPass Application** (Приложение EntraPass), **Gateway** (Шлюз) или **Site** (Сайт).
Information #1 - 4 (Информационные поля 1 – 4)	Добавить информацию о событии. Опции, доступные в базе данных: **Index Number** (Номер индекса), **Index Text** (Описание индекса), **Component ID** (Идентификатор компонента) и **Component Text** (Описание компонента).
Card Information (Информация о карте)	Добавить в команду сведения о карте. Доступные опции: **Card Number** (Номер карты), **Card User Name** (Имя владельца), **Card Information #1 - #10** (Информационные поля карты 1 - 10) или **Comment** (Комментарий).
Numerical Value (Численное значение)	Добавить число в команду.
Character String (Строка символов)	Добавить в команду строку символов (свободный текст).
Add Delay (Добавить задержку)	Добавить в команду задержку 1/10 сек.
Carriage Return (Возврат каретки)	Добавить в команду возврат каретки.
Trim Right (Выравнивание по правому краю)	Последний символ с правой стороны команды будет удалён.
E-Mail (Электронная почта)	Добавить в команду электронный адрес, на который автоматически будет отправлено сообщение при возникновении события.

Параметр	Описание
Modem (Модем)	Добавить в команду сообщение, которое будет автоматически отправлено на пейджер при возникновении события.
Serial Device for Messages (Последовательный порт для сообщений)	Выбрать последовательный COM-порт (**Serial Com Port**) и указать скорость обмена данными (**Baud rate**) для отправки сообщения.
Serial Device for Commands (Последовательный порт для команд)	Выбрать последовательный COM-порт (**Serial Com Port**) и указать скорость обмена данными (**Baud rate**) для отправки команды.
File (Файл)	По команде **File** (Файл) открывается меню Select a filename (Укажите имя файла), предназначенное для выбора пути файла (или создания нового), в который при возникновении события будет записываться вся информация о событии, указанная в команде. **Close** (Закрыть) – закрыть файл. **Commit to disk** (Передать на диск) – сохранить файл на диск. Эта команда не выполняет закрытие файла.
Execute (Выполнение)	По команде **File** (Файл) открывается меню Select a filename (Укажите имя файла), предназначенное для выбора пути exe-файла, который будет использоваться вместе с макрокомандой. **Parameter** (Параметр) – открывает меню Enter Character Strings (Введите символьные строки), предназначенное для ввода строки символов, которые будут добавлены в макрокоманду. **Action** (Действие) – служит для выбора режима выполнения макроса: **Launch Hidden** (Скрыть запуск), **Launch Normal** (Нормальный запуск), **Launch Minimized** (Свернуть при запуске), **Launch Maximized** (Развернуть при запуске) или **Terminate the process** (Прервать выполнение).
Network (Сеть)	Добавить метку сети (**Network Tag**).
Modify Language (Изменить язык)	Язык команд можно изменить на английский (**English**) или французский (**French**).
Save SmartLink Mode (Сохранить режим SmartLink)	Добавить в SmartLink команду на прерывание и перевод текущего режима SmartLink в фоновый (например, отправка электронной почты). Эту команду **обязательно** следует использовать вместе с командой **Restore Previous SmartLink Mode** (Восстановить предыдущий режим SmartLink).
Restore Previous SmartLink Mode (Восстановить предыдущий режим SmartLink)	Добавить в SmartLink команду на восстановление предыдущего режима SmartLink. Эта команда **всегда** используется вместе с командой **Save SmartLink Mode** (Сохранить режим SmartLink).

Добавление в макрос SmartLink команд управления электронной почтой

При создании макрокоманды с помощью приложения SmartLink система EntraPass позволяет добавлять в неё команды управления электронной почтой.

1 Выделить уже созданную команду или создать новую, нажать кнопку **Macro insertion menu for SmartLink** (Меню добавления макросов для приложения SmartLink), выделить команду **e-Mail** (Электронная почта). На экране появится окно компоновщика команд управления электронной почтой (E-Mail instruction builder).



2 Указать электронный адрес в поле **From...** (Отправитель).

3 В поле **Too...** (Получатель) указать электронный адрес (один или несколько) адресата. Каждый адрес должен быть отделён от следующего точкой с запятой (;).

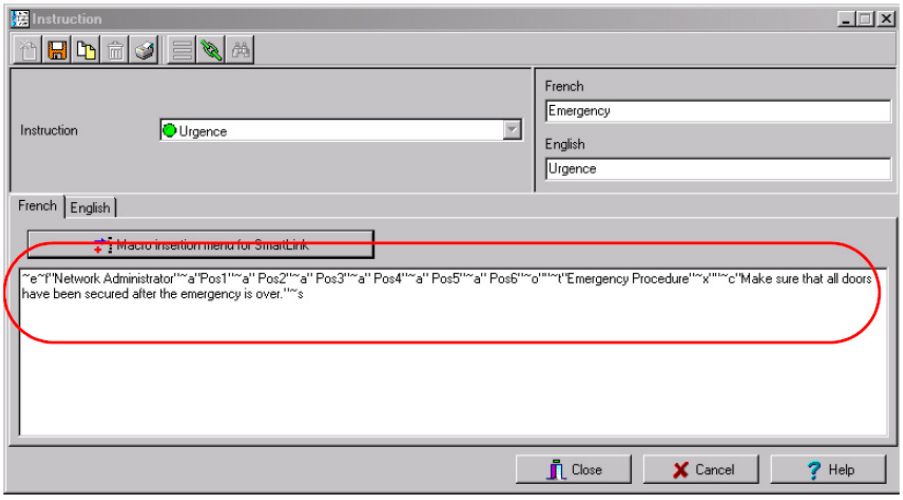
4 Если необходимо отправить копию письма другим людям, их имя следует указать в поле **Cc...** (Копия).

5 В поле **Subject** указать тему письма.

6 Чтобы прикрепить к письму файл, необходимо указать путь к этому файлу. Каждый файл должен быть отделён от следующего точкой с запятой (;).

7 Напечатать текст сообщения в большом окне.

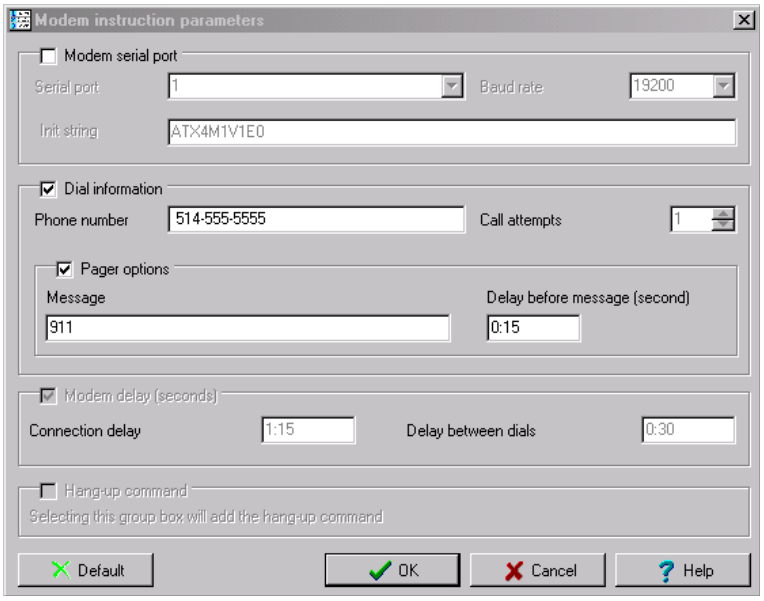
8 Нажать **OK**, чтобы прикрепить письмо к команде SmartLink. Сообщение появится в окне Instruction (Команды).



Добавление в макрос SmartLink команды для отправки сообщения на пейджер

При создании макрокоманды с помощью приложения SmartLink система EntraPass позволяет добавлять в неё команду для отправки сообщения в систему персонального вызова (на пейджер).

1 Выделить уже созданную команду или создать новую, нажать кнопку **Macro insertion menu for SmartLink** (Меню добавления макросов для приложения SmartLink), выделить команду **Modem** (Модем). На экране появится окно Modem instruction parameters (Параметры команды управления модемом).

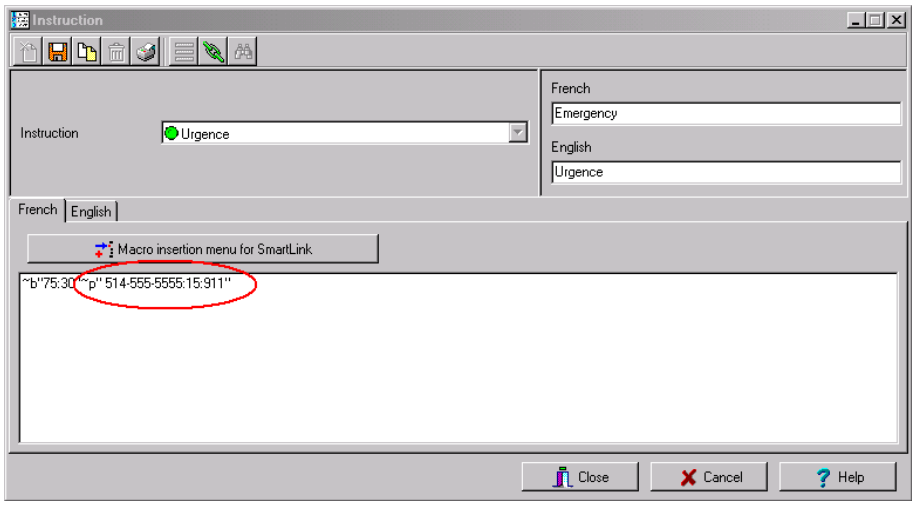


2 В поле **Modem serial port** (Последовательный порт для модема) уже должны быть введены настройки.

3 Ввести данные в раздел **Dial information** (Параметры набора), в частности, телефонный номер оператора в поле **Phone number.**

Поставить флажок в поле **Pager options** (Опции пейджера) и ввести в поле **Message** сообщение, которое будет отображаться на экране пейджера (если у него есть экран для показа сообщений). Указать в поле **Delay before message** задержку перед отправкой сообщения на пейджер.

4 Нажать **OK**. Номер телефона и текст сообщения появится в окне Instruction.



Описание фильтров сообщений

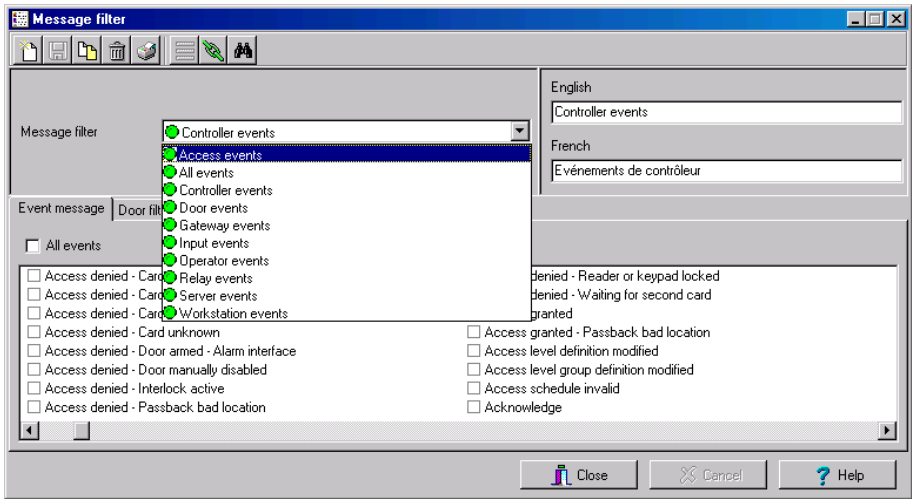
Функция Message filter (Фильтр сообщений) предназначена для описания фильтров, используемых на рабочем столе Filtered Messages (Избранные сообщения). Эти фильтры служат для определённого отбора событий.

Существует много предварительно настроенных фильтров, например: события, связанные с нарушением доступа, события на контроллере 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. *Более подробная информация приведена в разделе "Рабочий стол избранных сообщений" на стр. 386.*

Описание события для фильтра сообщений

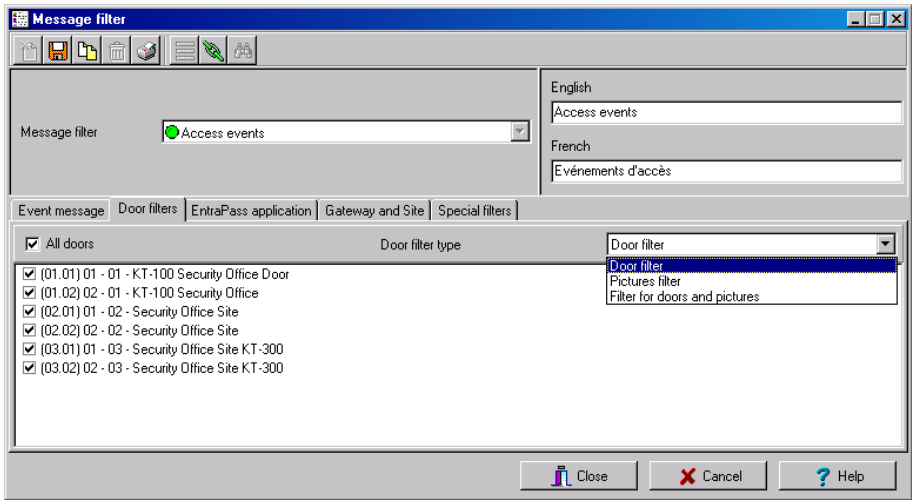
1 В главном окне System (Системные настройки) нажать на иконку **Message Filter** (Фильтр сообщений). Открывается окно Message filter.



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, с которых будут отправляться сообщения на рабочий стол Filtered Messages (Избранные сообщения). 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.

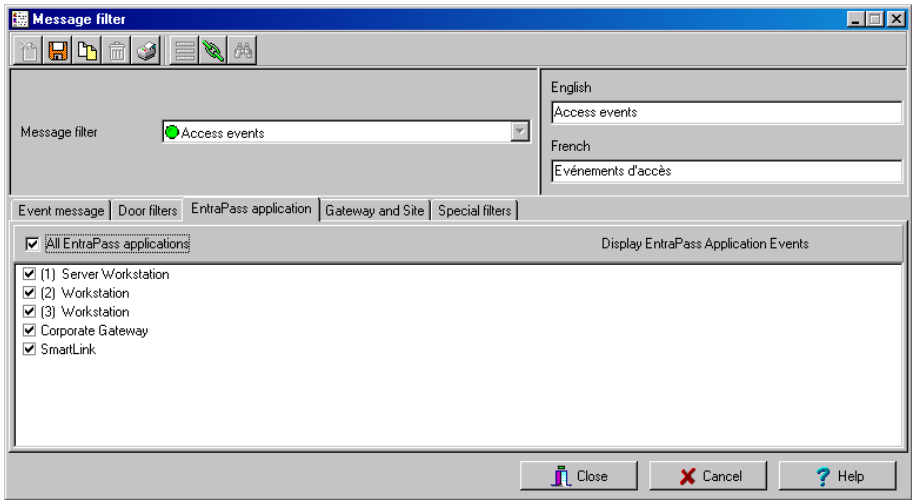


5 Выделить все двери при помощи опции **All doors** (Все двери) или выбрать определённые двери, для которых при возникновении события будет отображаться фото владельца карты.

6 В списке **Door filter type** (Типы фильтров дверей) выбрать фильтр, который будет использоваться при отборе событий, связанных с дверями:

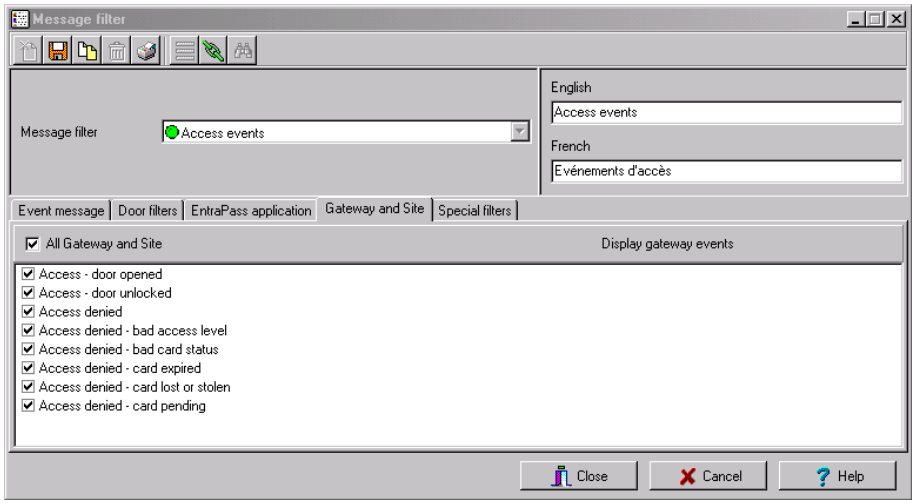
- **Door filter** (Фильтр дверей) – на рабочий стол Filtered Message (Избранные сообщения) будут отправляться только события, связанные с указанными дверями.
- **Pictures filter** (Фильтр фотографий) – на рабочий стол Filtered Message (Избранные сообщения) будут отправляться только фотографии владельцев 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 о событиях, связанных 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.

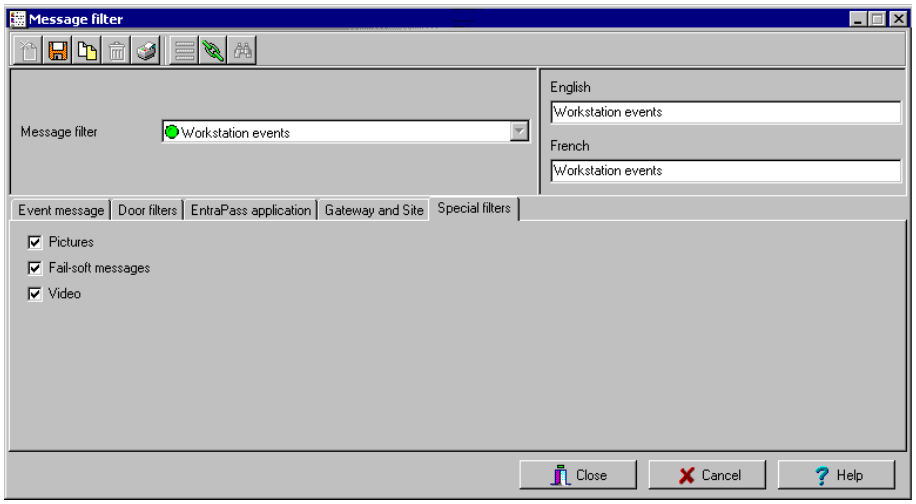
9 Открыть закладку **Gateway and site** (Шлюзы и сайты), чтобы отобрать шлюзы и сайты, с которых будут отправляться сообщения на рабочий стол Filtered Messages (Избранные сообщения).



10 Отметить флажком опцию **All events** (Все сообщения), чтобы получать сообщения о событиях, происходящих на компонентах шлюзов или сайтов. 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** (Безопасный 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.*

Описание структуры базы данных

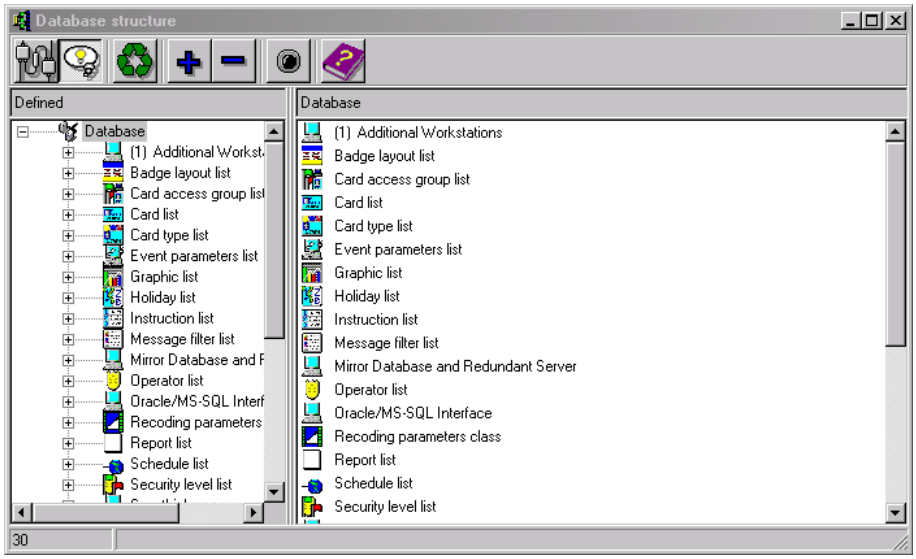
Меню Database structure (Структура базы данных) служит для просмотра базы данных системы. В нём отображается вся структура базы данных и в том числе:

- *Физические компоненты* системы (приложения EntraPass, шлюзы, сайты, контроллеры, двери, реле, входы и дополнительные выходы), а также.
- *Логические компоненты* (карты, расписания, отчёты, команды, группы 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 адресу компонента.

ПРИМЕЧАНИЕ. *Кроме того, можно указать, каким образом система должна отображать на экране физический адрес компонента. От этого зависит также способ сортировки компонентов. Более подробные сведения смотрите в разделе "Описание уровней безопасности" на стр. 326.*

Глава 12 • Рабочие столы EntraPass

Рабочие столы предназначены для получения и отображения на экране сообщений о событиях (активных 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 на экране макрокоманд 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 события системы
- Рабочий стол 4: Избранные сообщения системы и фотографии и др.
- Рабочий стол 5: Окно тревог
- Рабочий стол 6: Графические схемы
- 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:

- Команды
- 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).

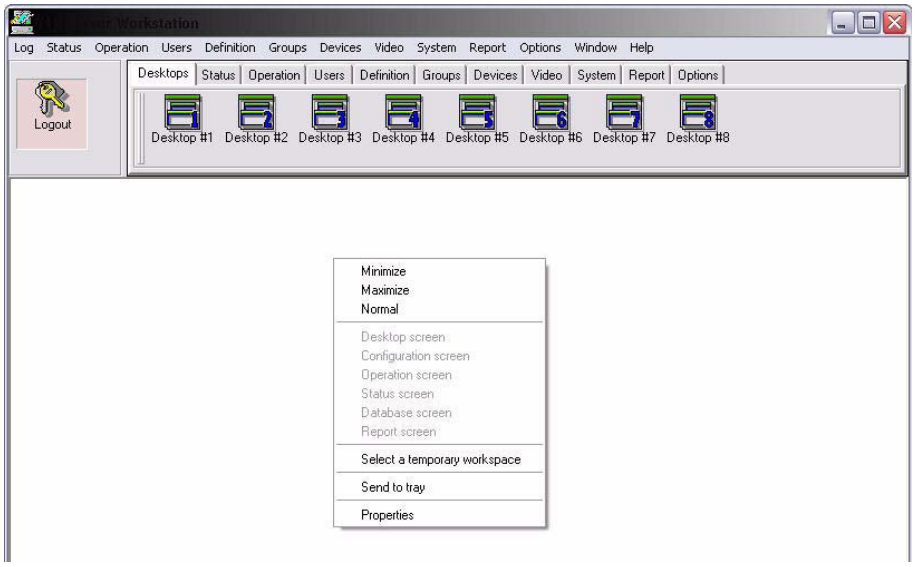
ПРИМЕЧАНИЕ. *Изменять настройки рабочих столов по своему усмотрению могут только операторы с соответствующим уровнем безопасности (доступа) (закладка* **System** *(Системные настройки) >* **Security Level** *(Уровни безопасности). У них также есть возможность разрешить операторам со статусом "Read-only" (Только для чтения) изменять настройки своих рабочих столов. Но в этом случае изменения будут действовать только в текущей сессии!*

Индивидуальная настройка рабочего пространства

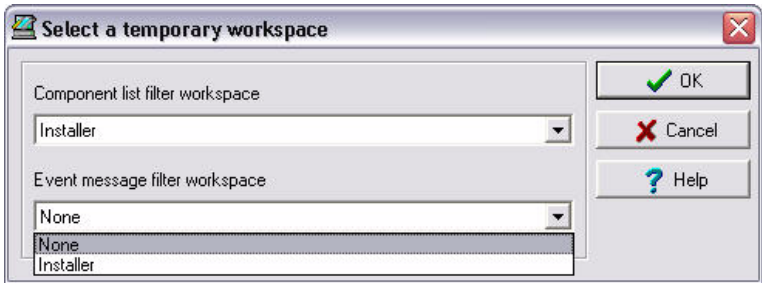
Система EntraPass позволяет операторам, имеющим соответствующие права, по своему желанию настраивать своё рабочее пространство, создавать временное рабочее пространство и изменять свойства рабочих столов. Уровни безопасности для операторов назначаются в разделе **System** (Системные настройки) > **Security Level** (Уровни безопасности).

Создание временного рабочего пространства

1 В окне Desktop (Рабочие столы) щёлкнуть правой кнопкой мыши под строкой меню.



2 Выбрать в контекстном меню пункт Select a temporary workspace (Выбрать временное рабочее пространство).



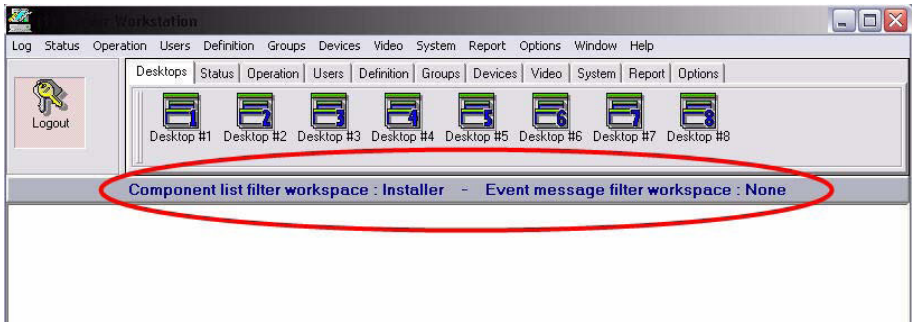
3 Указать нужное в списках **Component list filter workspace** и **Event message filter workspace**.

- **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.*

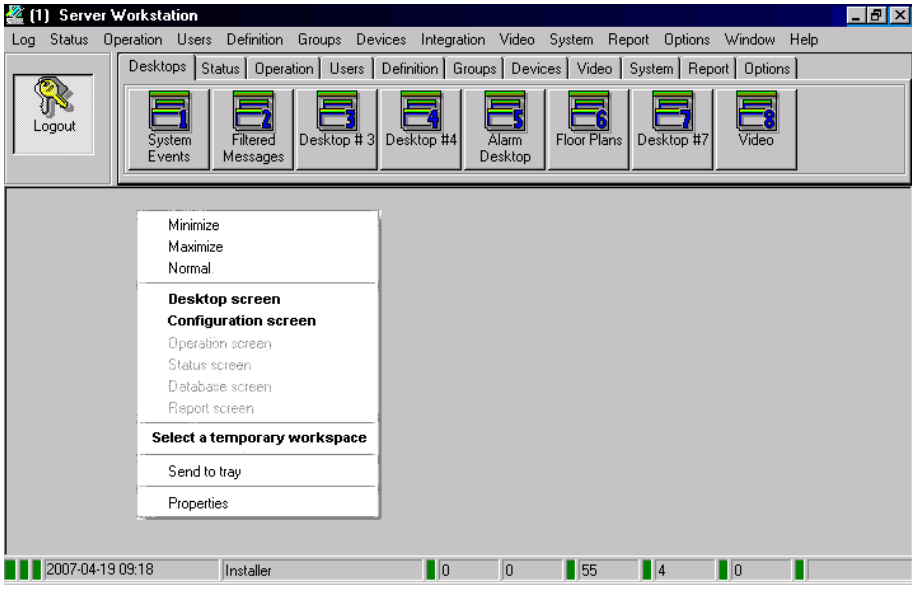
4 Нажать **OK**. На экран будет выведен заголовок временного рабочего пространства с именами используемых фильтров.



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.

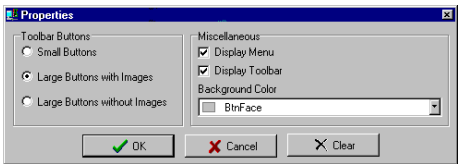
Изменение свойств экрана

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

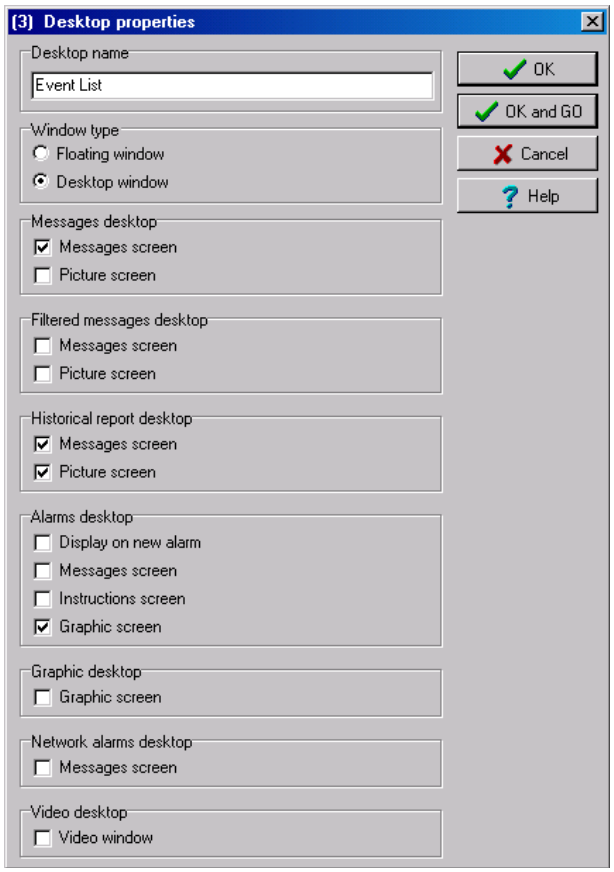
Система EntraPass позволяет операторам, имеющим соответствующие права, настраивать рабочие столы по своему желанию. Помимо этого, операторы с полным доступом могут разрешать операторам с доступом "только для чтения" индивидуально настроить свои рабочие столы. Они также могут настраивать специальные рабочие 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.

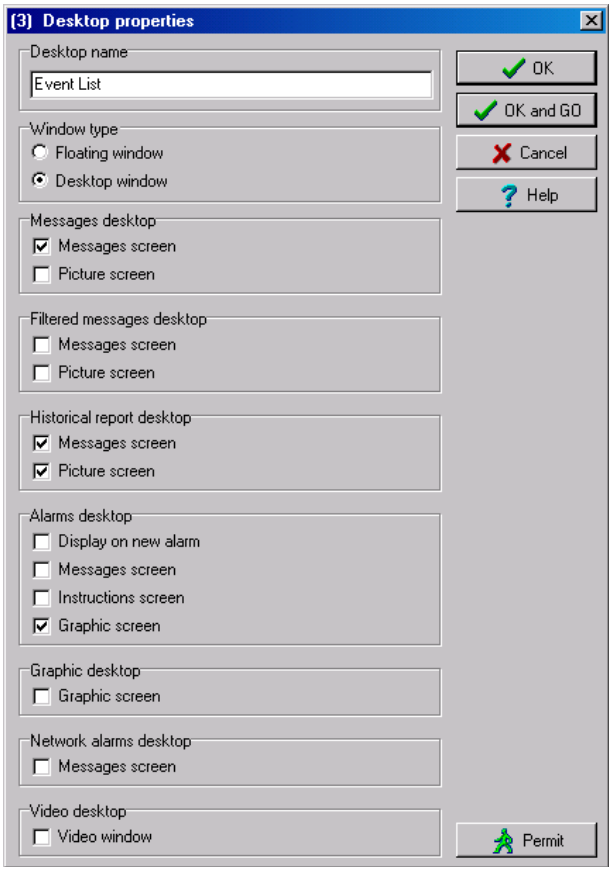
ПРИМЕЧАНИЕ. *При открытии окна рабочего стола в первый раз для правильного отображения информации может потребоваться изменить его размеры. Для этого следует установить курсор мыши на край рамки и после того как курсор превратится в двунаправленную стрелку, растянуть окно до нужного размера. После этого 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).



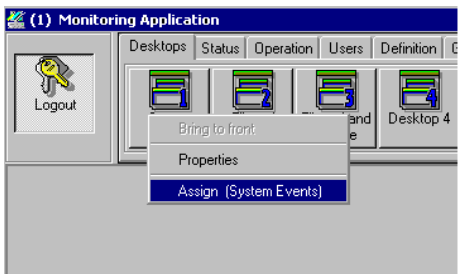
ПРИМЕЧАНИЕ. *Кнопка **Permit** (Разрешить) появляется, если зарегистрировавшийся в системе оператор имеет доступ "только для чтения". Разрешение действует только на время текущей сессии, пока оператор не выйдет из системы.*

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.

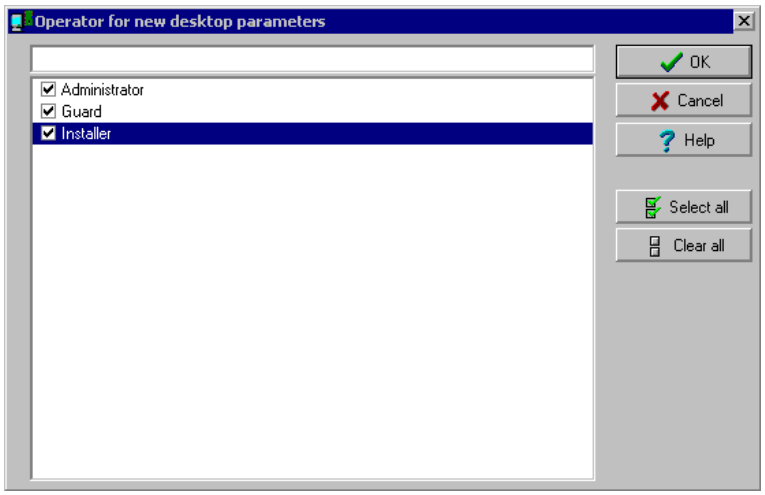
Передача индивидуально настроенного рабочего стола

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)

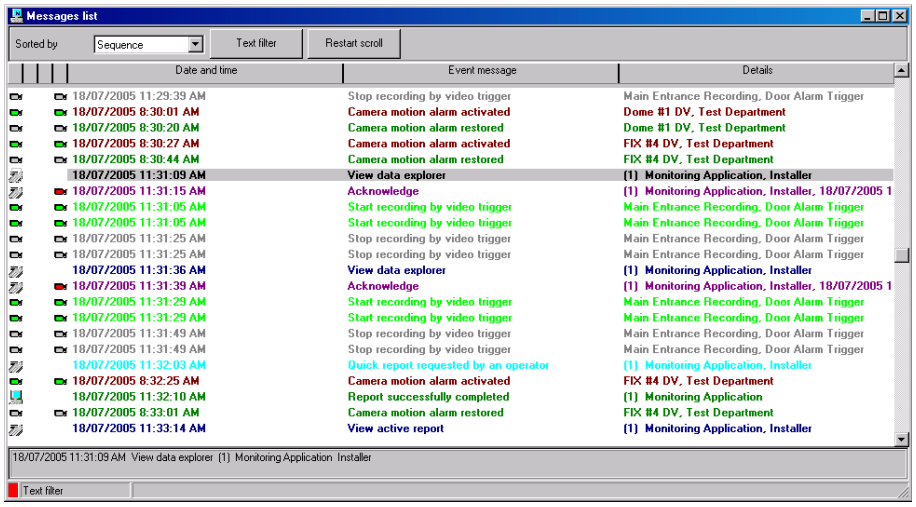
По умолчанию первый рабочий стол служит для вывода на экран сообщений и называется **Messages List** (Список сообщений). Он содержит все системные события. Каждое событие отображается вместе с особой пиктограммой, датой и временем, описанием и компонентами, связанными с этим событием (контроллерами, 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 сообщений – смотрите раздел "Индивидуальная настройка экрана событий для стола сообщений Message" на стр. 378.*

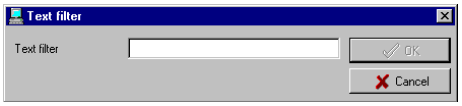
2 В окне Message list (Список событий) есть возможность изменить критерий сортировки сообщений (функция **Sorted by**). Сообщения можно сортировать по следующим критериям:

- **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) 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).*

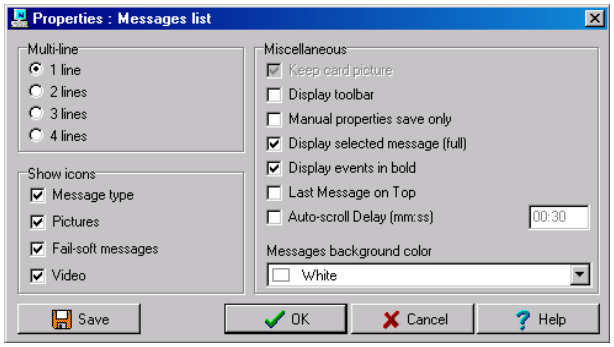
3 Кнопкой **Text filter** (Текстовый фильтр), расположенной в верхней части окна, открыть меню Text filter. В поле Text filter ввести ключевое слово, чтобы вывести на экран все сообщения из списка Message list, которые содержат это ключевое слово. Чтобы закрыть окно Text filter, нажать **Cancel** (Отмена) или закрыть окно кнопкой (X).



4 Чтобы вернуться к нормальному режиму отображения сообщений в окне Messages list, нажать кнопку **Text filter.**

Индивидуальная настройка параметров отображения событий на рабочих столах сообщений (Message Desktop)

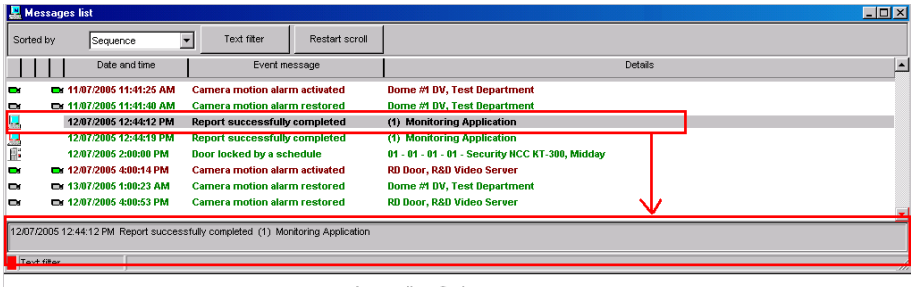
1 На рабочем столе **Message** вызвать контекстное меню щелчком правой кнопки мыши и выбрать пункт Properties (Свойства).



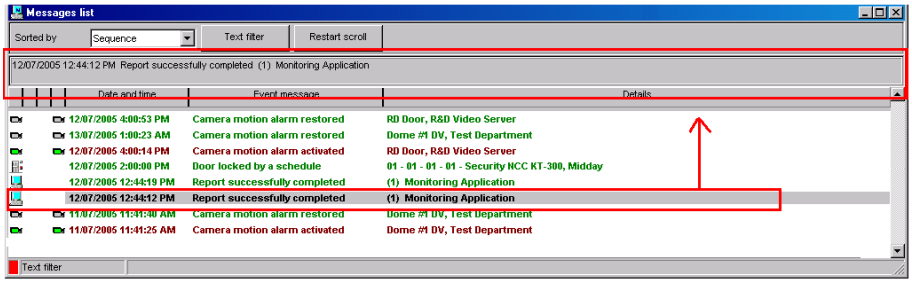
2 В окне Properties (Свойства) выбрать необходимые параметры отображения информации.

- **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 ручное 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 указанные 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.



в порядке поступления



в обратном порядке

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 списков архивных сообщений Archived Messages Lists).

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

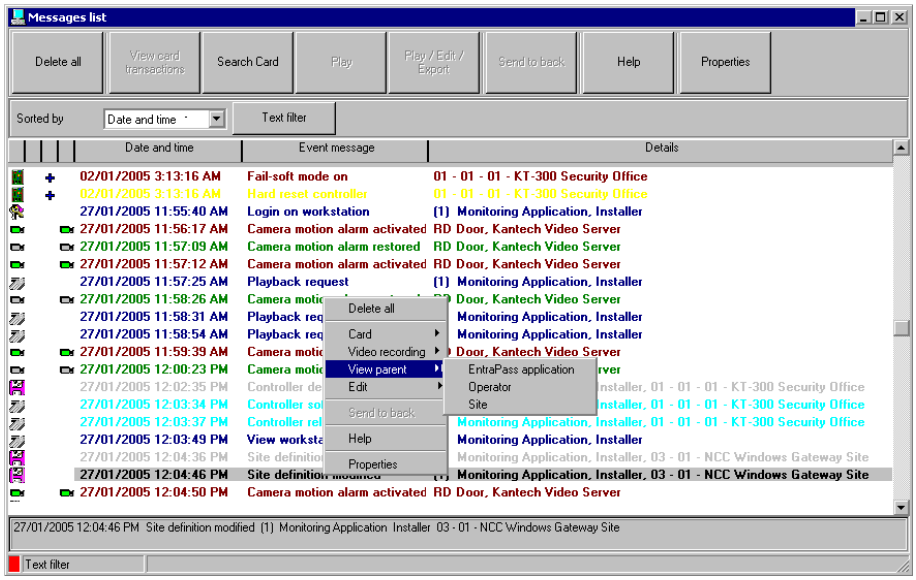
Система EntraPass позволяет выполнять самые разные задачи с системными сообщениями. А именно:

- Удаление сообщений

- Просмотр информации о карте
- Проверка статуса карты и транзакций 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. Подробнее смотрите в разделе "Рабочие столы тревог" на стр. 391.*

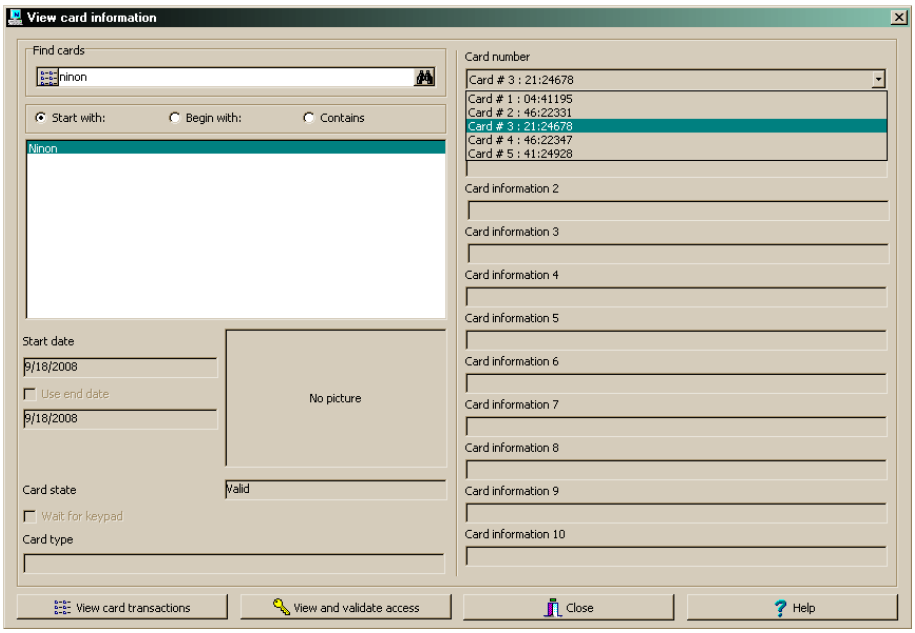
1 На столе сообщений Message вызвать контекстное меню правой кнопкой мыши.



2 Выполнить одно из следующих действий:

- **Delete all** (Удалить все) – позволяет удалить все отображаемые события.
- **Card** (Карта) – это меню содержит две функции: **View card transactions** (Просмотр транзакций 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 транзакции с нею или посмотреть и проверить уровень доступа карты.

Более подробно о проверке последних транзакций и уровня доступа владельца карты смотрите *в разделе "Описание идентификационных карт" на стр. 230.*



- **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 описание сайта) имеет связи с приложением EntraPass, оператором, зарегистрированным в системе во время возникновения события, а также с сайтом, связанным с этим событием. Данная функция позволяет редактировать любой из этих трёх компонентов, отображённых в контекстном меню.

ПРИМЕЧАНИЕ. *Если выбранное событие связано с правами доступа, а карта, из-за которой событие возникло, уже зарегистрирована в системе, то будет возможно редактировать карту. Однако если это событие типа "Access denied - card unknown" (Доступ запрещён – неизвестная карта), то карта будет создана и зарегистрирована в системе.*

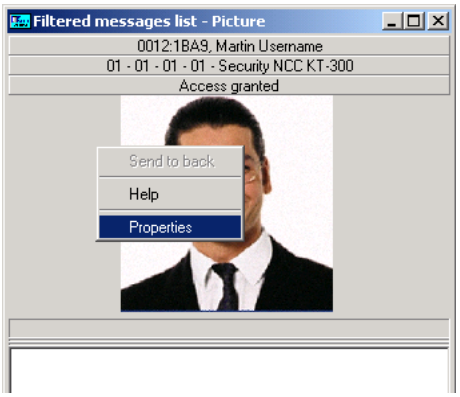
- **Send to back** (Перенести на задний план) – эта опция работает только для плавающих окон (Floating). При использовании данной опции активное окно оказывается за главным окном приложения. Чтобы вернуть его на передний план, следует щёлкнуть правой кнопкой по кнопке рабочего стола и выбрать в контекстном меню пункт **Bring to front** (Перенести на передний план).
- **Properties** (Свойства) – служит для изменения настроек для выбранного рабочего стола.

Рабочий стол фотографий (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). Более подробные сведения по настройке смотрите в разделе "Описание фильтров сообщений" на стр. 363.

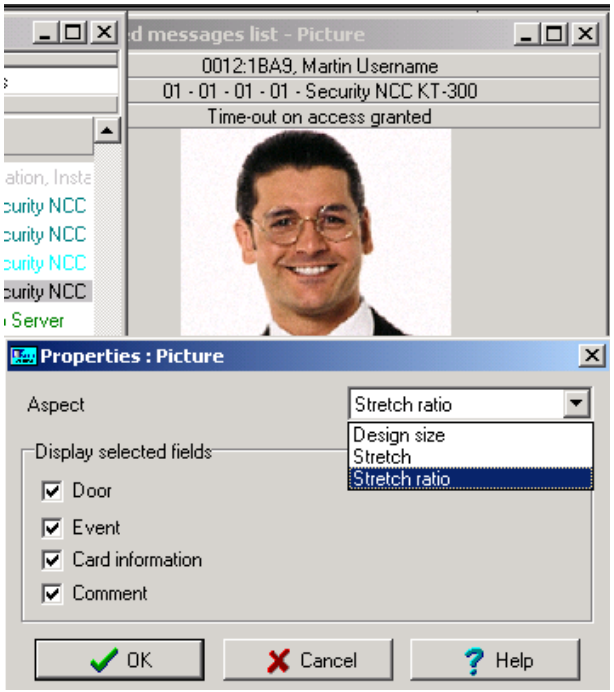
Изменение свойств окна Pictures

1 В списке избранных событий с фотографиями (Filtered Message list) выбрать событие, связанное с доступом карты, и щёлкнуть правой кнопкой мыши по фотографии владельца карты.



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).

2 В контекстном меню выбрать пункт **Properties** (Свойства).



3 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.

4 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 описании карты.

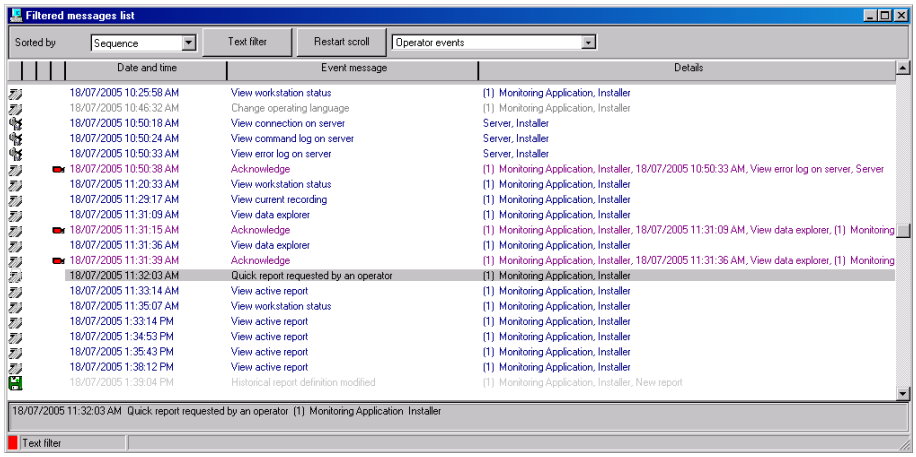
Рабочий стол избранных сообщений (Filtered Messages Desktop)

Рабочий стол Filtered Messages служит для отображения избранных 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 этому рабочему столу имя и указать его тип (окно Message (Сообщения), окно Picture (Фотографии) или оба окна вместе).



3. Настроить текстовый фильтр (**Text filter**) для отображения избранных сообщений. Более подробная информация приведена *в разделе "Рабочий стол сообщений" на стр. 377.*

Рабочий стол архивных отчётов (Historical Report Desktop)

Рабочий стол **Historical Report** (Архивные отчёты) позволяет операторам отображать события, поступающие из предварительно настроенных 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.

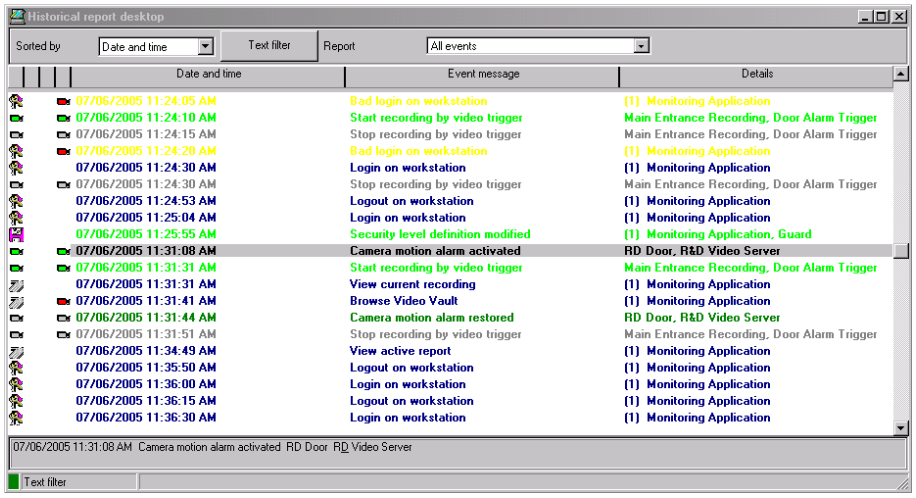
Список сообщений **Historical Report** ничем не отличается от остальных списков сообщений EntraPass, за исключением дополнительной комбинированной панели, позволяющей операторам выбирать один из предварительно настроенных архивных отчётов.

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).



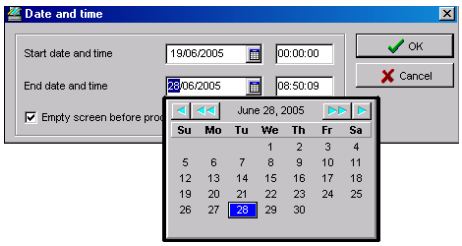
3 Выбрать критерии отбора, по которым будут отображаться архивные данные: **Date and Time** (Дата и время), **Event** (События) или **Message Type** (Тип сообщения).

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.

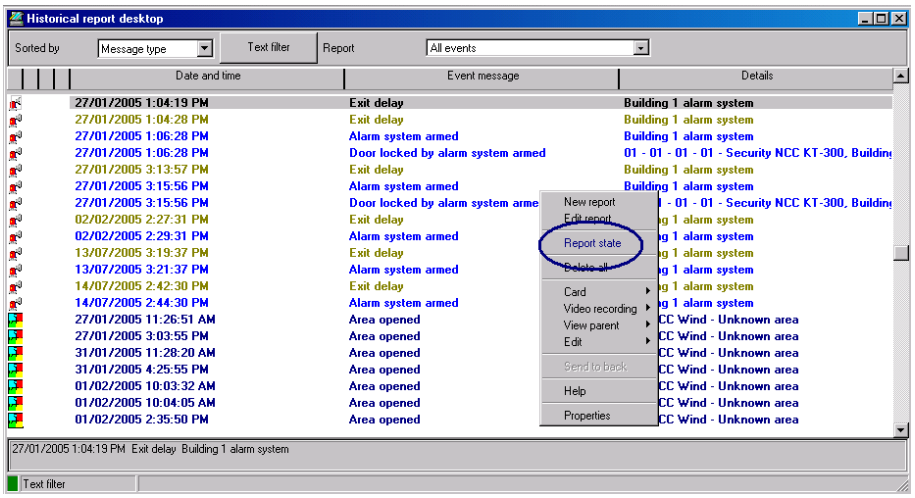
Создание и редактирование архивных отчётов на рабочем столе

- Если уровень безопасности оператора позволяет ему создавать новые отчёты, то он может войти в меню Historical Report (Архивные отчёты), используя команду **New Report** (Новый отчёт), которую следует вызвать в контекстном меню рабочего стола Historical Report Desktop. Подробнее об архивных отчётах смотрите *в разделе "Описание архивных отчётов" на стр. 415.*
- Если уровень безопасности оператора позволяет редактировать уже созданные отчёты, то он может войти в меню Historical Report (Архивные отчёты), используя команду **Edit Report** (Изменить отчёт) в контекстном меню рабочего стола Historical Report. Подробнее об архивных отчётах смотрите *в разделе "Описание архивных отчётов" на стр. 415.*

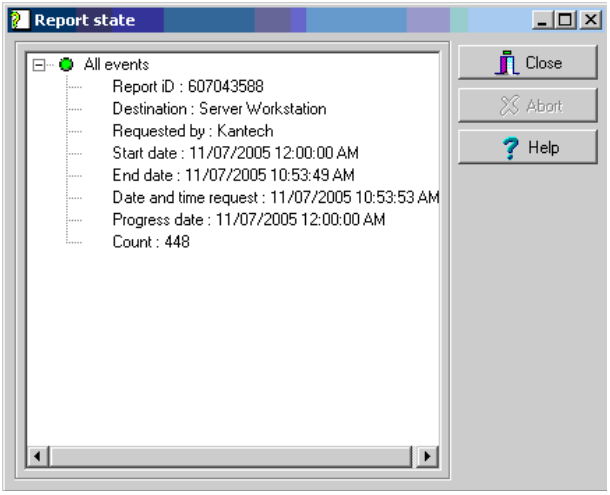
Отображение статуса архивного отчёта в реальном времени

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.



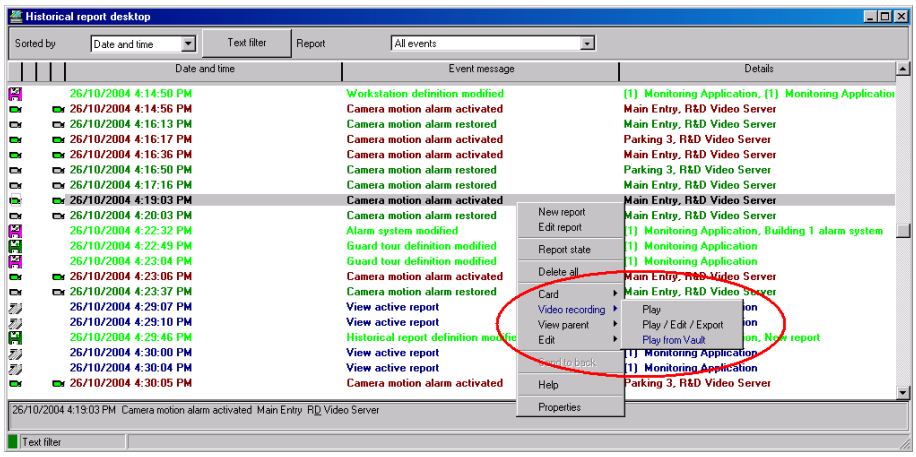
2 Выбрать пункт **Report State** (Статус отчёта). Окно Report State содержит сведения о генерации отчёта.



3 После завершения создания отчёта все данные в окне Report State исчезают. Нажать **Close** (Закрыть).

Воспроизведение архивных видеозаписей из 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.

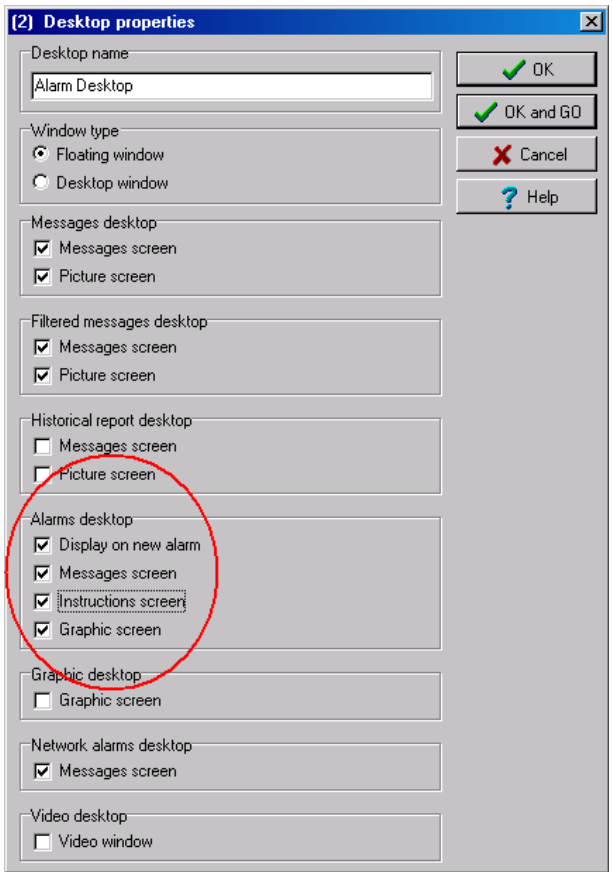
Рабочий стол тревог (Alarms Desktop)

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, команд (если их описали в настройках) и прикреплённых графических схем или видеофайлов. Новые события добавляются в конец списка тревог, если в настройках не указано иное (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. Подробнее о запрете использования функции сетевых тревог смотрите в разделе "Сетевые тревоги" на стр. 459.*

Описание 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:

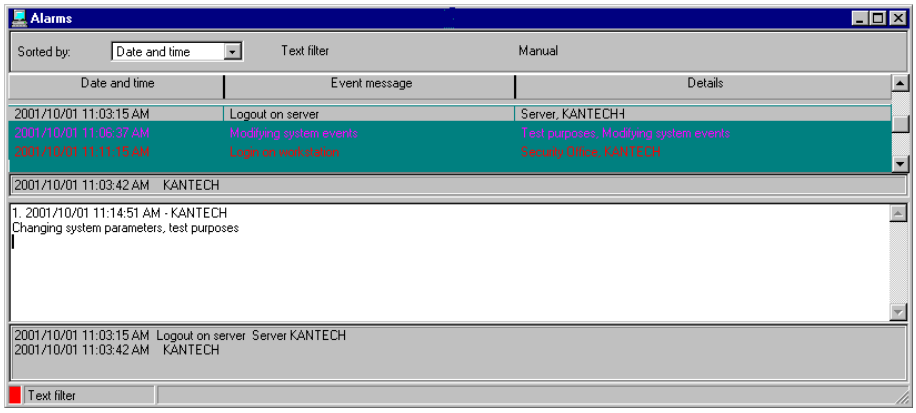
- **Display on new alarm** (Показывать при возникновении новой тревоги) – автоматически открывать рабочий стол тревог при возникновении тревоги.
- **Message screen** (Окно сообщений) – служит для просмотра и подтверждения тревог, для которых в меню описания параметров событий (**System** (Системные настройки) > **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 команд) – отображает команды, прикреплённые к событию, которое требует подтверждения (например, вызов полиции, отправка сообщения в клиентское приложение и др.). Для описания команд следует войти в меню **System** (Системные настройки) > **Instructions** (Команды). Затем можно создать связи между командами и событиями.

- **Graphic screen** (Окно графических схем) – позволяет определить место, где возникла тревога (если в системе описаны графические планы). Подробнее смотрите *раздел "Описание графических схем" на стр. 198.*

ПРИМЕЧАНИЕ. *Рабочий стол тревог можно настроить как окно сообщений (Message), окно графики (Graphic) и окно команд (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 сообщений системы

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** (Вход переведён в статус тревоги) будут сгруппированы вместе.
- **Priority** (Приоритет) – сортировка событий по приоритету, как описано в меню **Event Parameters** (Параметры событий).

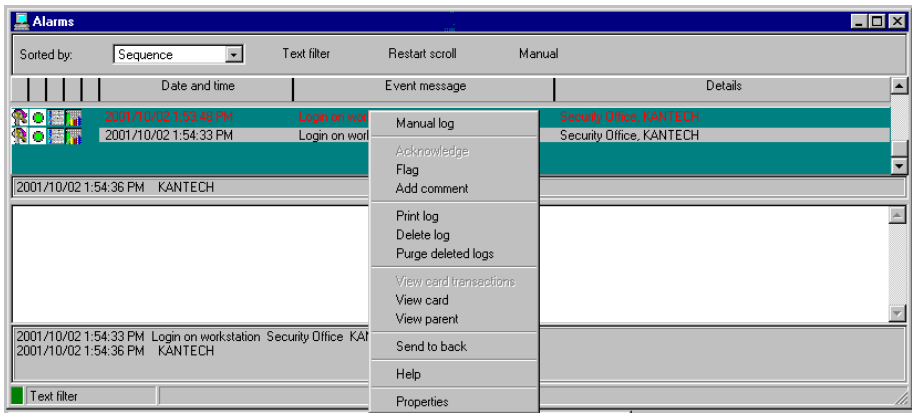
4 Правой кнопкой мыши вызвать окно Properties (Свойства), в котором необходимо активировать индикаторы статуса тревог:

- **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 (Описания операторов). Более подробная информация приведена *в разделе "Описания операторов" на стр. 322.*

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:



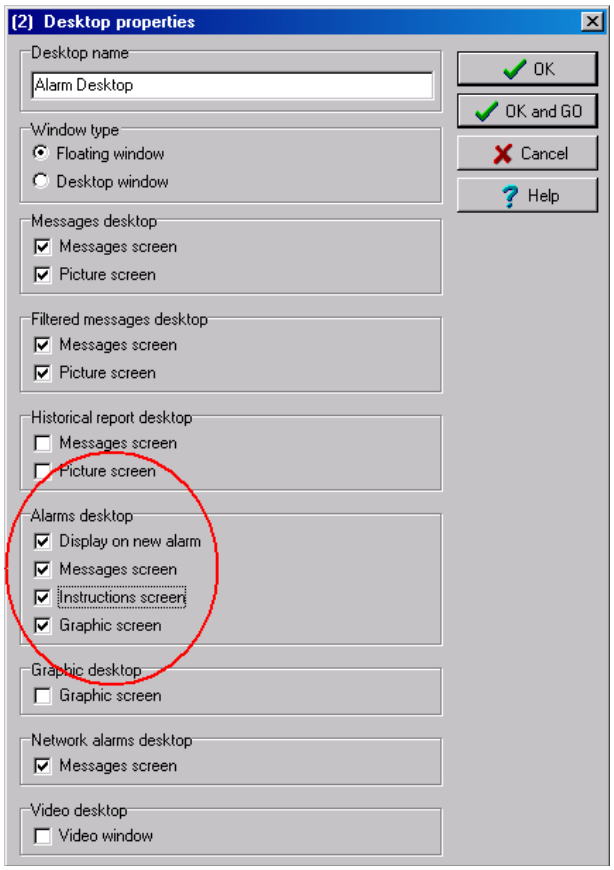
- **Manual log** (Ручная запись) – при выборе этой опции открывается окно Manual log, в котором оператор имеет возможность добавлять комментарии к событию, и следовательно, создавать события, настроенные под свои собственные требования (приоритет, подробные сведения о событии, цвет и пр.). При добавлении 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 опция выделена флажком, то при вызове стола тревог фон иконки стола становится синим, указывая, что окно тревоги и дополнительные окна будут отображаться при возникновении новой тревоги. Однако если эта опция выделена, например, при описании рабочего стола избранных сообщений (Filtered message), то при нажатии на иконку этого рабочего стола он появится на экране (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 после открытия всех этих окон (при появлении тревоги) 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 по 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 окнах-предупреждениях или в окне рабочего стола тревог.

ПРИМЕЧАНИЕ. *Систему можно настроить таким образом, чтобы тревожные сообщения отображались в сопровождении звукового сигнала. Более подробные сведения по настройке тревожных звуковых сигналов смотрите в разделе "Конфигурация мультимедийных устройств" на стр. 452.*

Опции подтверждения настраивают в меню описания приложения: **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 это видеоокно с изображением, передаваемым в реальном времени, или с видеозаписью.*

Автоматическое подтверждение

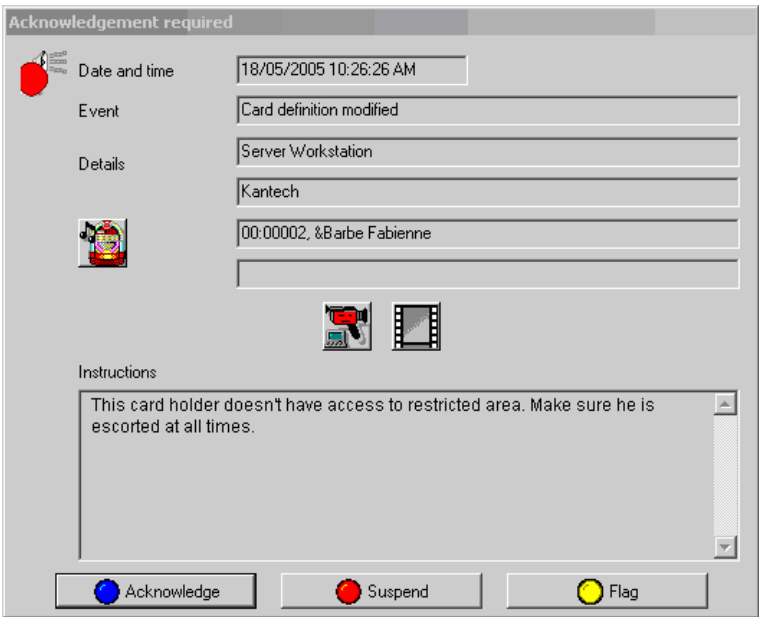
В системе предусмотрено автоматическое подтверждение тревог, без участия оператора. Эта опция активируется в меню Operator Definition (Описания операторов): **System** (Системные настройки) > **Operators** (Операторы) > **Privileges**, **Auto acknowledge** (Особые права, Автоматическое подтверждение).

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 команд, то окно с заголовком* ***Acknowledgement required*** *(Требуется подтверждение) будет отображаться без окошка с командами.*

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.

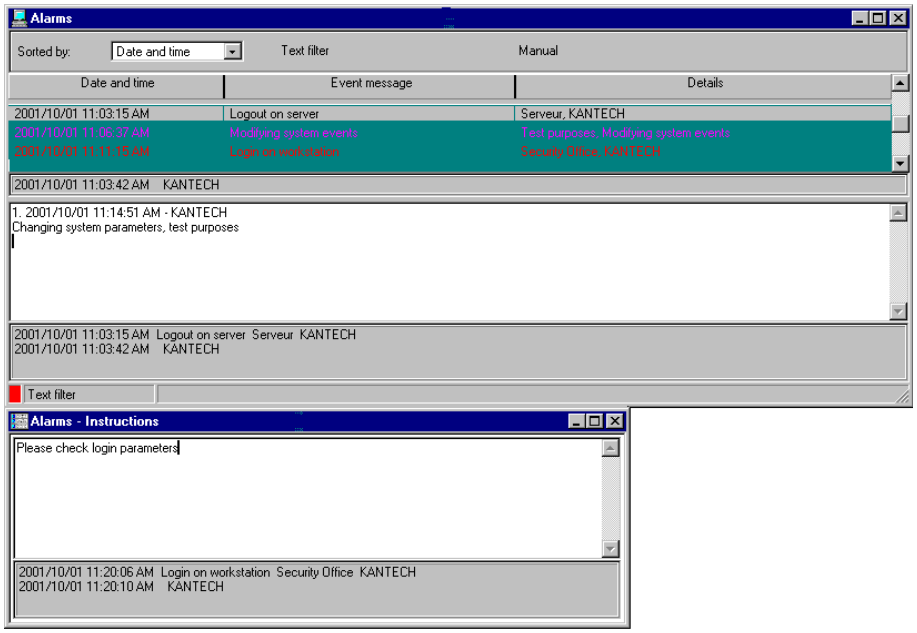
ПРИМЕЧАНИЕ. *Чтобы отметить тревожное сообщение флагом для каких-либо определённых целей, следует выделить его и щелчком правой кнопки мыши вызвать контекстное меню, в котором выбрать пункт* ***Flag*** *(Поставить флаг). Кроме того, можно просто щёлкать по этому сообщению до тех пор, пока метка не станет нужного цвета.*

Рабочий стол команд (Instruction Desktop)

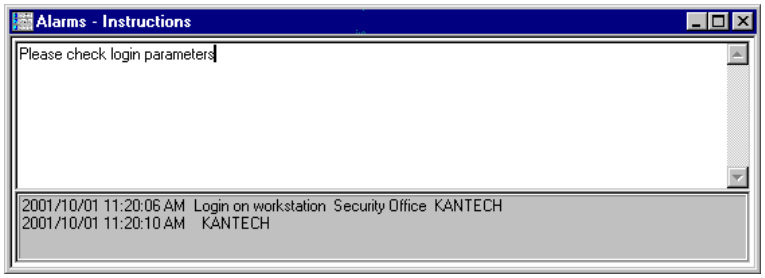
Окно команд (Instruction) показывает команды, которые необходимо выполнить при сообщении о тревоге. Команды отображаются на экране только в том случае, если эта опция разрешена в настройках параметров событий: **System** (Системные настройки) > **Event parameters** (Параметры событий), **Alarm settings** (Параметры тревог).

Просмотр команды к тревожному сообщению

1 Чтобы видеть команды к тревожным сообщениям, рабочий стол тревог (Alarms desktop) можно настроить как окно сообщений (Message) и окно команд (Instruction) или просто как окно команд. Если рабочий стол сконфигурирован как окно сообщений и окно команд, то оба окна отображаются одновременно .



2 Кроме того, чтобы вывести на экран команду 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 система настроена на работу с графическими планами). 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). Указания по настройке поэтажных планов изложены *в разделе "Описание графических схем" на стр. 198.*

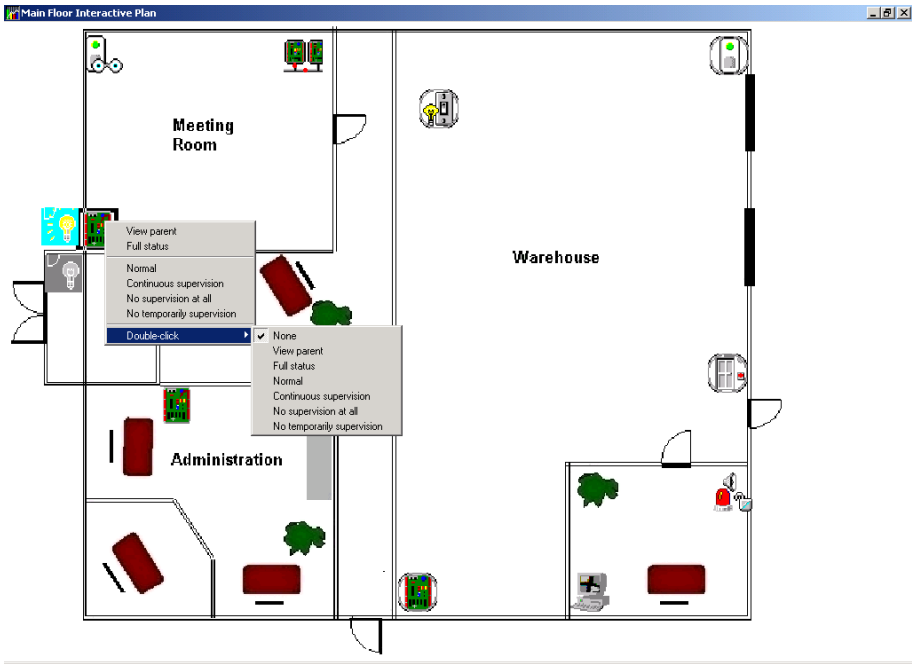
Просмотр графических схем на рабочем столе Graphic Desktop

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, какие схемы 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*** *(Описания) > **Graphics*** *(Графические схемы), окно Design (Проект), щёлкнуть правой кнопкой мыши по компоненту > выбрать пункт* ***Default dblclick*** *(Двойной щелчок по умолчанию)). Более подробные указания по созданию графических схем и использованию компонентов на схемах приведены в разделе "Описание графических схем" на стр. 198.*

Рабочий стол сетевых тревог (Network Alarms Desktop)

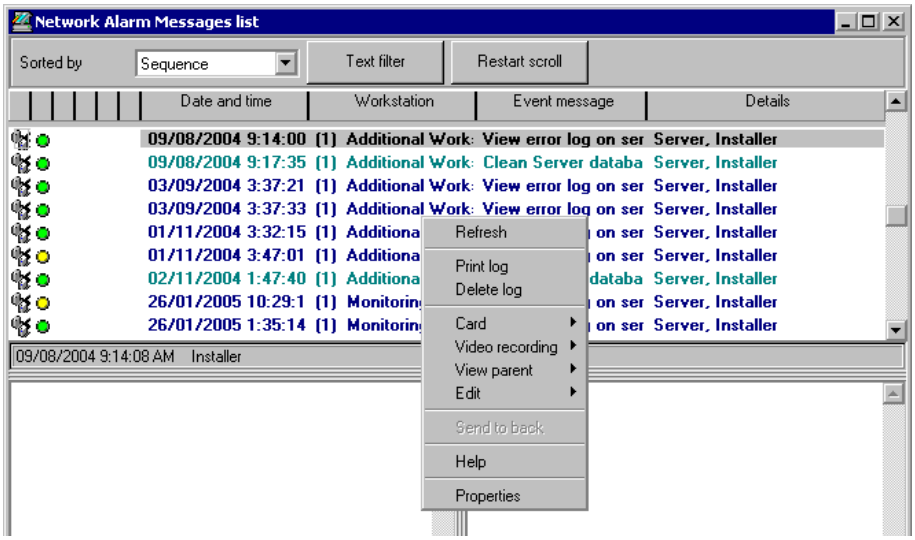
Рабочий стол сетевых тревог служит для просмотра и подтверждения *всех* тревожных событий в системе. На этом столе отображаются только события, требующие подтверждения оператора, и запрограммированные в меню **Event Parameters** (Параметры событий).

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 описания их уровня безопасности.

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 запись) – 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.

Описание 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	Описание
	Большое окно, 1024x768 пикселей

Иконка	Описание
	Среднее окно, 800x600 пикселей
	Небольшое окно, 640x480 пикселей
	Миниатюрное окно, 400x300 пикселей
	Создать новое видеоокно
	Показать панель
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).

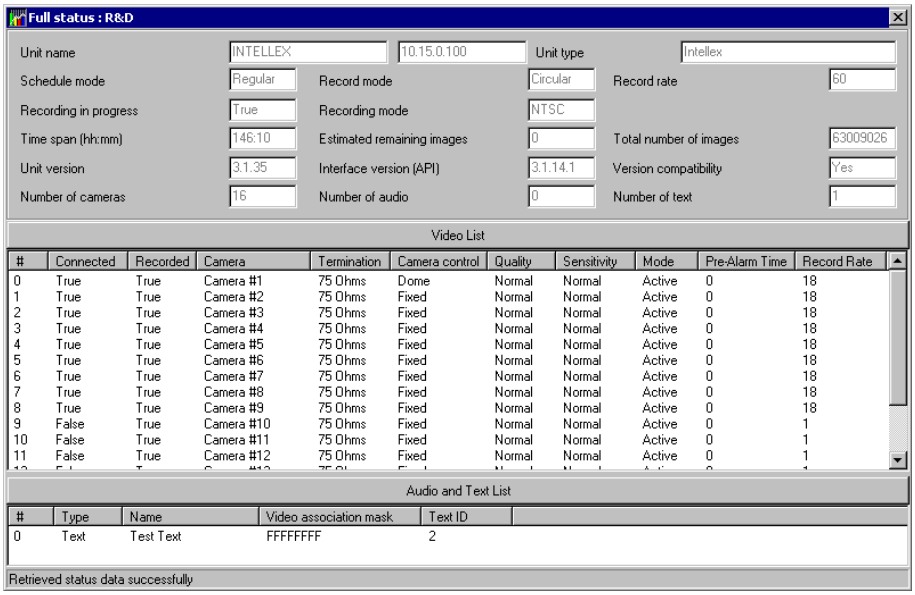
Статусы видеосерверов

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 статуса видеосерверов

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 DVMS (например, в проиллюстрированном примере "Intellex"). В соседнем поле отображается IP-адрес видеорегистратора.
Unit type (Тип устройства)	Тип устройства: Intellex, Iris (сетевой клиент) и др.

Параметр	Описание
Schedule mode (Режим расписания)	Текущий режим расписания работы удалённого устройства DVMS. 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 (Число камер наблюдения)	Число 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 DVMS. В качестве источника текстовых данных может использоваться кассовый аппарат или другое устройство.

Глава 13 • Отчёты

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 три типа отчётов:

- **Quick reports** (Быстрые отчёты) – выполняются для определённой группы событий (например, группы дверей, контроллеров и др.) и для определённого типа событий (корректные, некорректные и др.).
- **Historical reports** (Архивные отчёты) – это отчёты по архивным событиям и по использованию карт. В архивные отчёты входят архивные и избранные 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.

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.

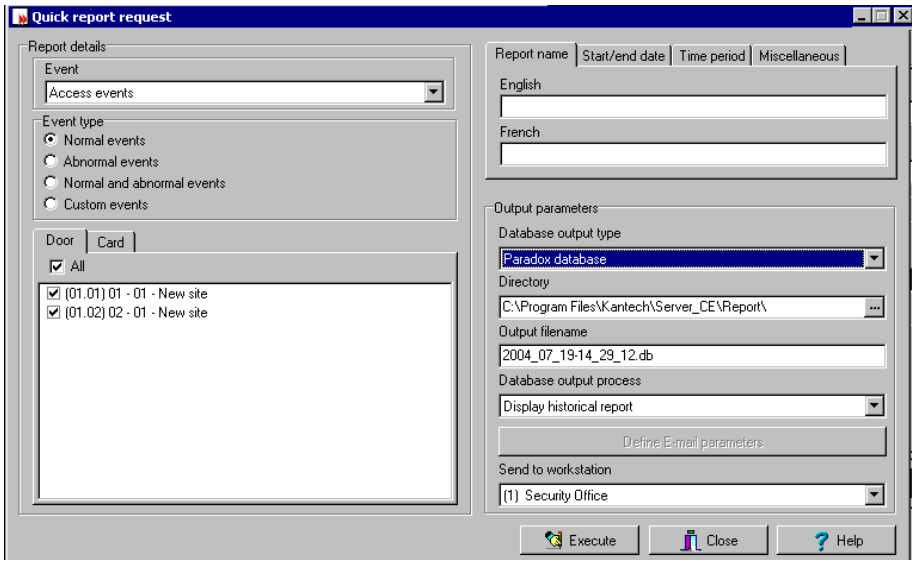
Описание быстрых отчётов (Quick Report)

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.

Описание 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).

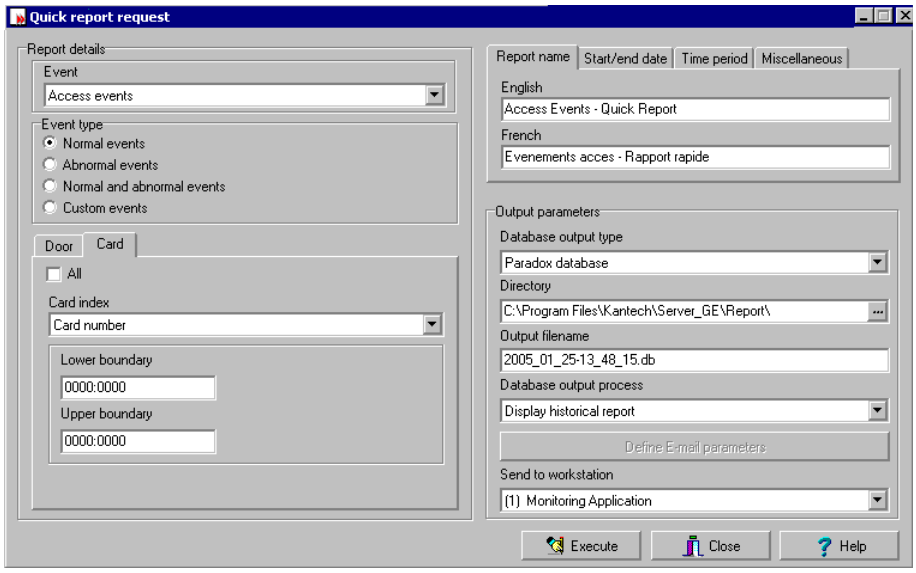
3 В опциях **Event type** (Тип событий) указать тип событий, которые должны быть включены в отчёт.

- **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), "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).
- **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\Workstation_CE\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\Workstation_CE\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 report** (Показать архивный 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 report** (Отправить архивный 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). Чтобы увидеть отчёт, открыть закладку **View report** (Посмотреть отчёт).

Описание архивных отчётов

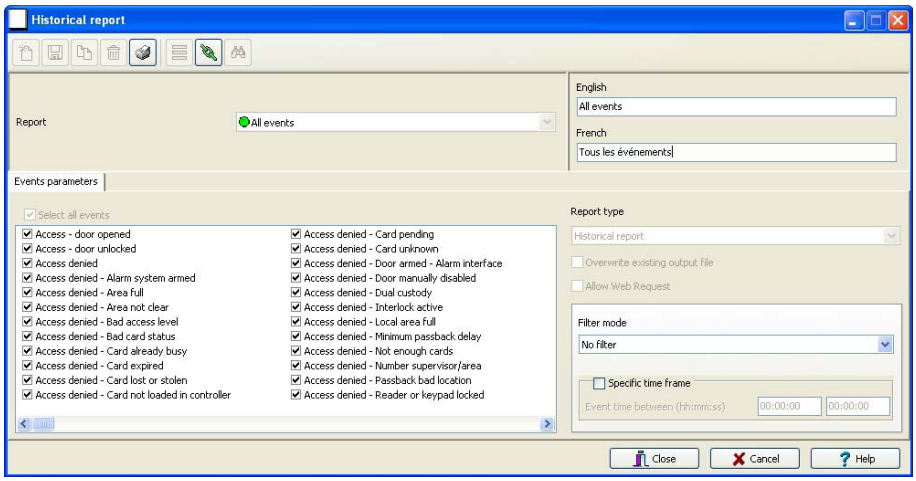
Функция описания архивных отчётов служит для индивидуальной настройки отчётов о давних событиях и отчётов об использовании идентификационных карт с индивидуальными параметрами автоматического выполнения.

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.

Описание 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.

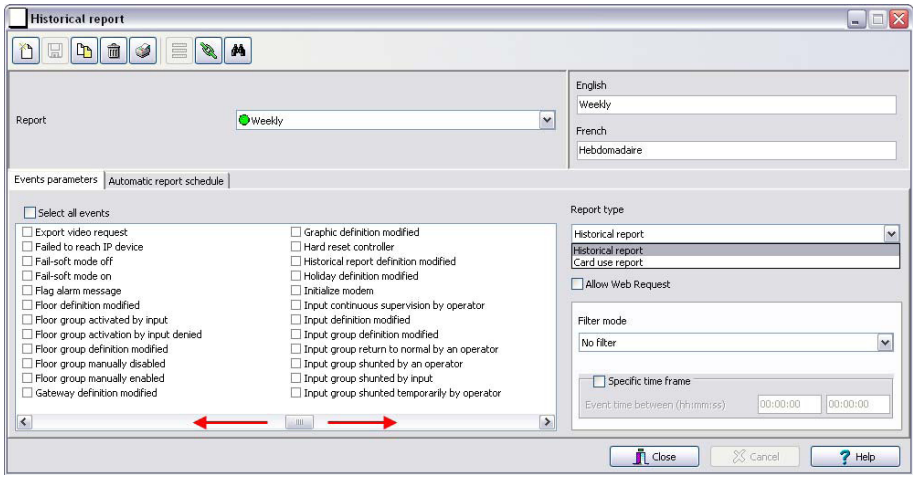
1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **Historical report** (Архивный отчёт). На экране появится окно Historical report.



2 В отчёте **All Events** доступными для редактирования будут только поля для изменения языков.

Описание 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 426 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).*

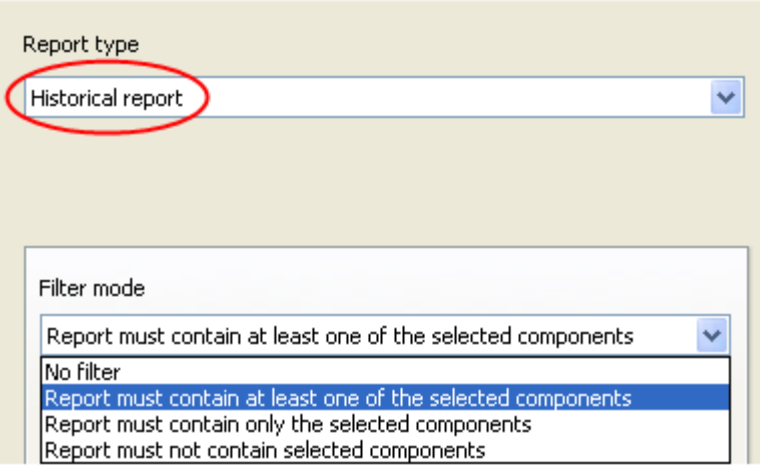
6 *Только для архивных отчётов (Historical Reports).* В случае выбора отчёта типа **Historical report** (Архивный отчёт) следует отметить флажком опцию **Specific time frame** (Определённые временные рамки). В этом случае система будет использовать при создании отчёта указанные временные рамки. В отчёт 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 Открыть закладку **Automatic report schedule** (Расписание автоматических отчётов), чтобы указать необходимые данные для создания автоматического отчёта. Подробнее об описании автоматических отчётов смотрите *в разделе "Настройка расписания автоматических отчётов" на стр. 421.*

Описание компонентов для архивного отчёта с индивидуальными настройками

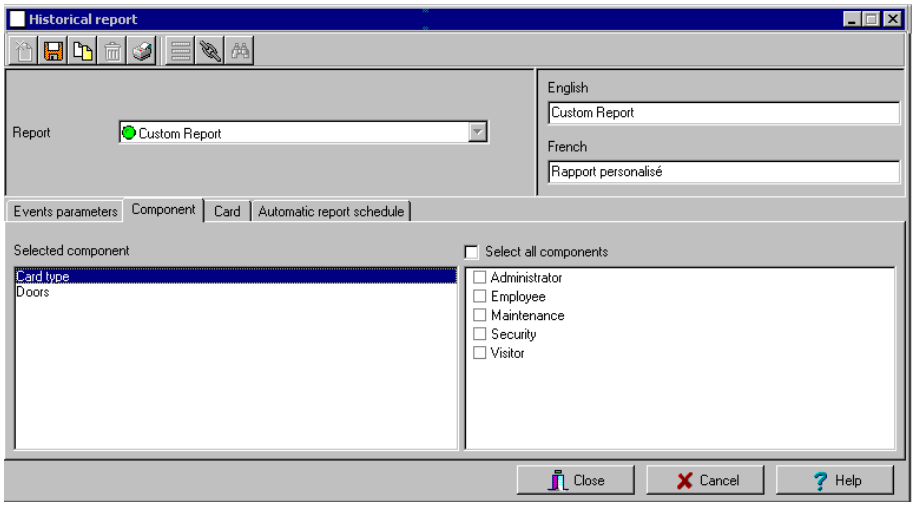
Если архивный отчёт (**Historical report**) создаётся с использованием фильтров (в выпадающем списке **Filter mode** указан фильтр), то **при выборе соответствующих событий** на экране появляются дополнительные закладки: **Components** (Компоненты) и **Cards** (Карты). Необходимо указать компоненты и 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 прямые ссылки на выбранные события.

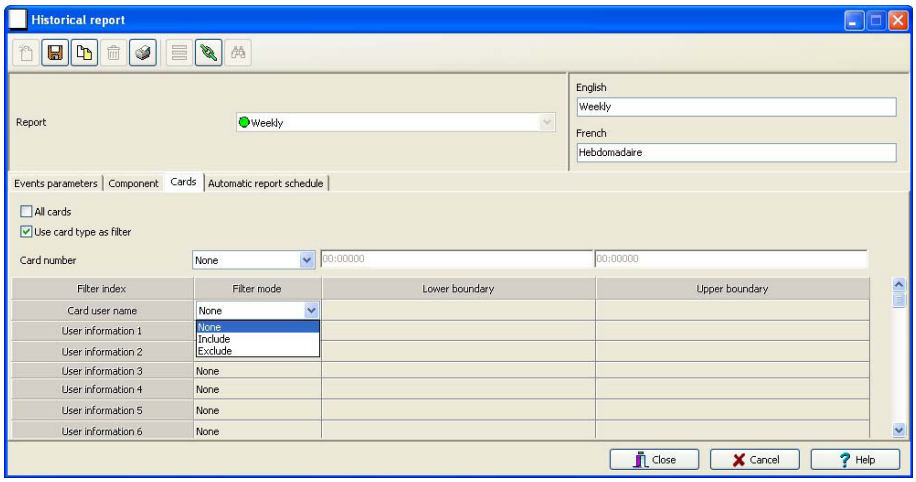


4 Указать тип события. На панели справа появятся все его составляющие. Если выделить **Card type** (Тип карты), то на панели справа будут отображаться все типы карт, описанных в системе. Если выделить Doors (Двери), то справа будут показаны все двери, используемые в системе доступа.

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).*

Описание 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.*

Описание отчёта об использовании идентификационных карт

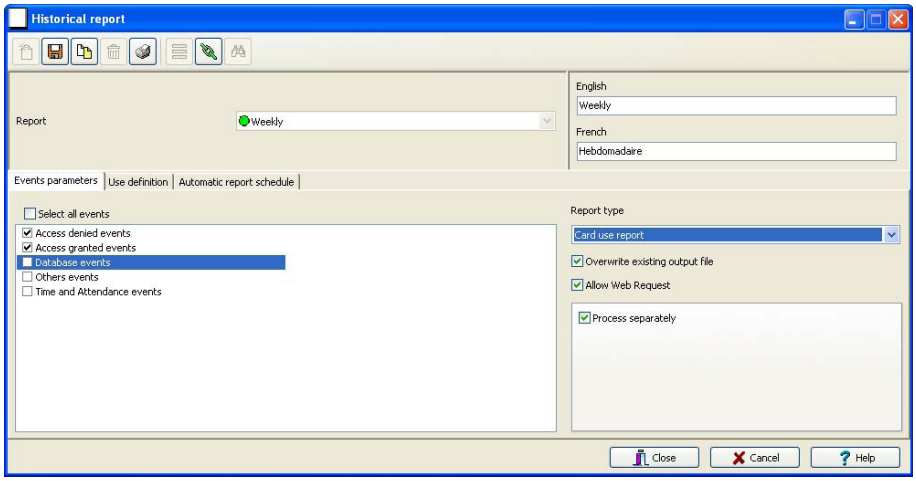
Функция Card use report служит для создания отчётов, в которых перечислены владельцы карт, создававшие/не создававшие события за последние несколько дней или начиная с некоторой указанной даты. Например, может возникнуть необходимость запросить отчёт, в который войдут события типа “Access granted” (Доступ 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 (Описание 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:

- События, вызывающие запрет доступа (проход не в том месте, не тот уровень доступа, не тот статус карты и т.д.),
- События с предоставлением доступа
- 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.

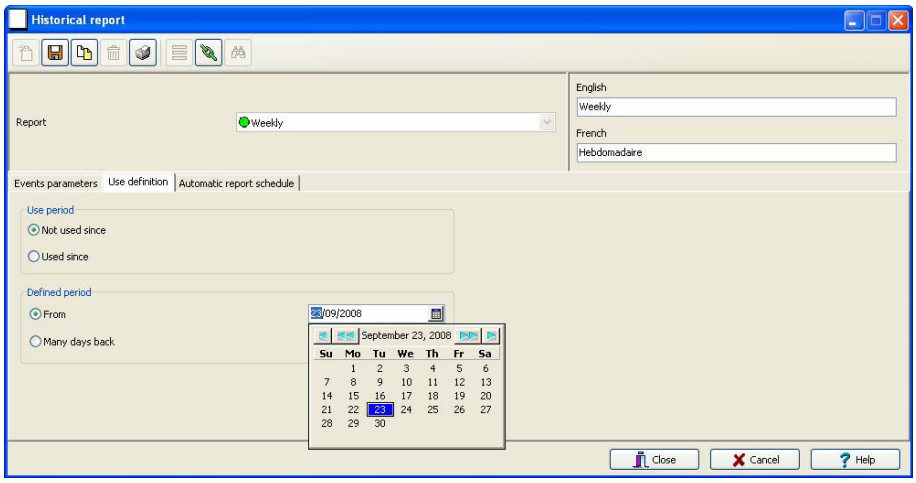
4 Отметить флажком опцию **Overwrite existing output file** (Записать поверх старого файла), чтобы система каждый раз заменяла старый файл отчёта на новый при автоматической генерации отчёта в соответствии с автоматическими настройками, указанными в разделе **Automatic report schedule** (Расписание автоматических 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** (Описания 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. Подробнее об описании автоматических отчётов смотрите *в разделе "Настройка расписания автоматических отчётов" на стр. 421.*

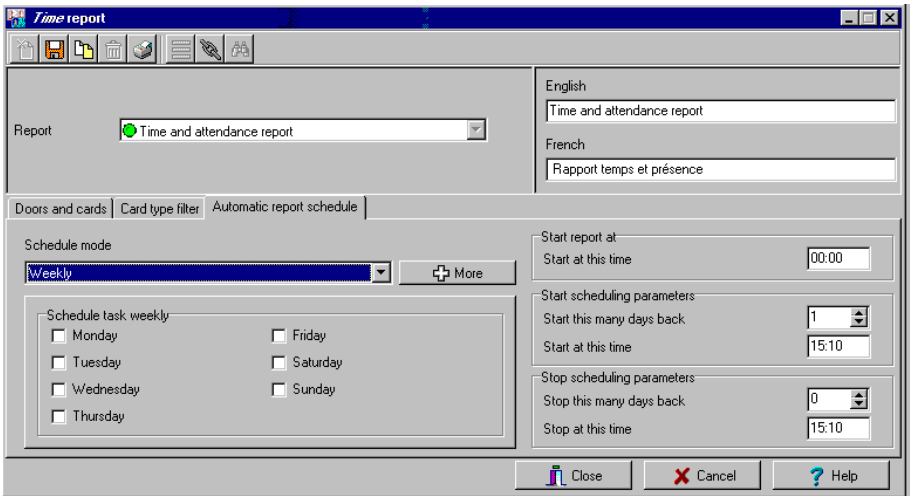
Настройка расписания автоматических отчётов

(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: 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)
- Путь для файла с результатами (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).*

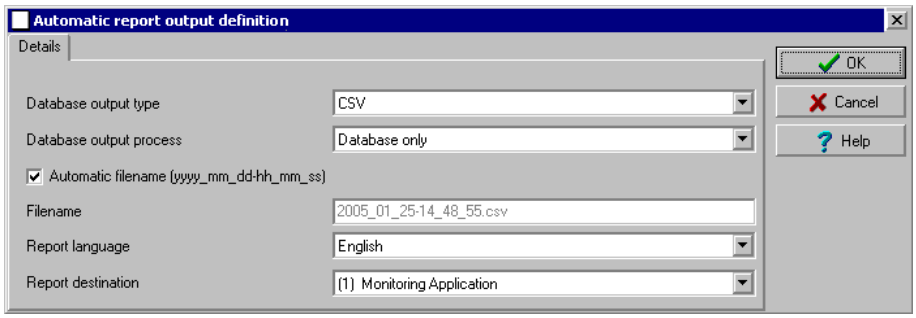
ПРИМЕЧАНИЕ. *Эти настройки будут* ***игнорироваться****, если отчёт будет запрашиваться вручную оператором.*

- **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	-
CSV	Сохраняет отчёт в файл значений с разделителями-запятыми (yourfile.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 и XtreeGold.	dBase III, IV, FoxPro, dBFast, DataBoss и Excel.	-
.csv, средство редактирования	-	-	Excel, NotePad, WordPad, др.
.rdf, средство просмотра	Средства EntraPass (Borland Database Engine)	Средства EntraPass (Borland Database Engine)	NotePad

5 В выпадающем списке **Output process** (Способ вывода базы данных) указать шаблон отчёта. Он будет использоваться вместе с запрашиваемым отчётом. Подробнее смотрите раздел *"Описание выходных форматов отчётов" на стр. 423.*

Описание 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), то отчёт будет автоматически отображаться на экране после окончания процесса генерации. Перед тем как отправить отчёт на печать, оператор может индивидуально изменить его настройки. Более подробные сведения по индивидуальной настройке отчётов смотрите *в разделе "Предварительный просмотр архивных отчётов " на стр. 440.* 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 (Посмотреть отчёт).

1 *Только 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 по датам и времени, идентификаторам транзакций, номерам карт и именам 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. Более подробные сведения по индивидуальной настройке отчётов смотрите *в разделе "Предварительный просмотр отчётов по учёту рабочего времени" на стр. 441.*

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 Только для баз данных *CSV:* если выделена опция **CSV compilation time and attendance** (Составление отчёта по учёту рабочего времени в формате CSV), то 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.

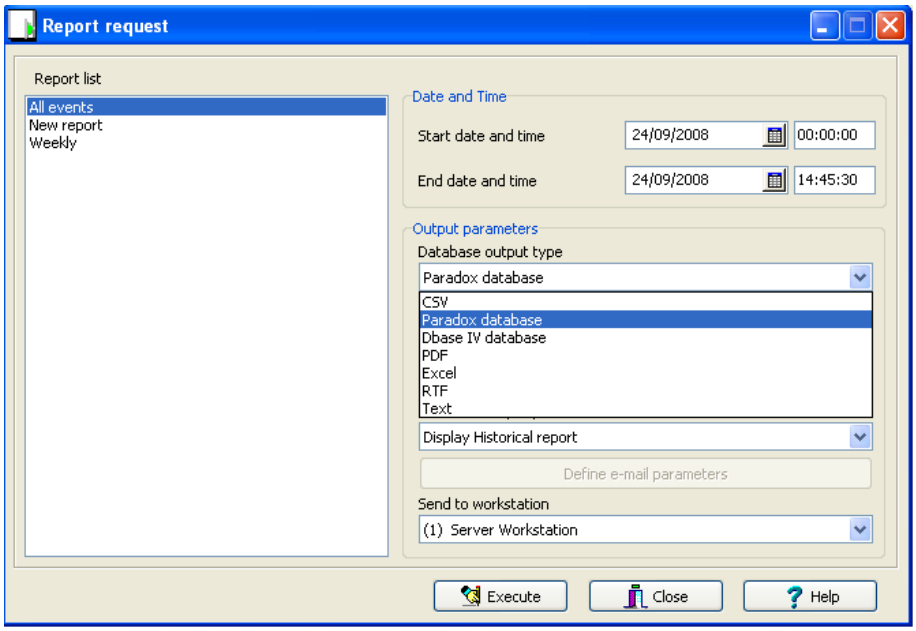
- **Automatic filename** (Автоматическое назначение имени файла) – эту функцию следует использовать для автоматического назначения даты и времени, а также имени файла. Эта функция не может быть использована вместе с опцией “Overwrite existing output file” (Записать поверх старого файла).
- **Filename** (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.

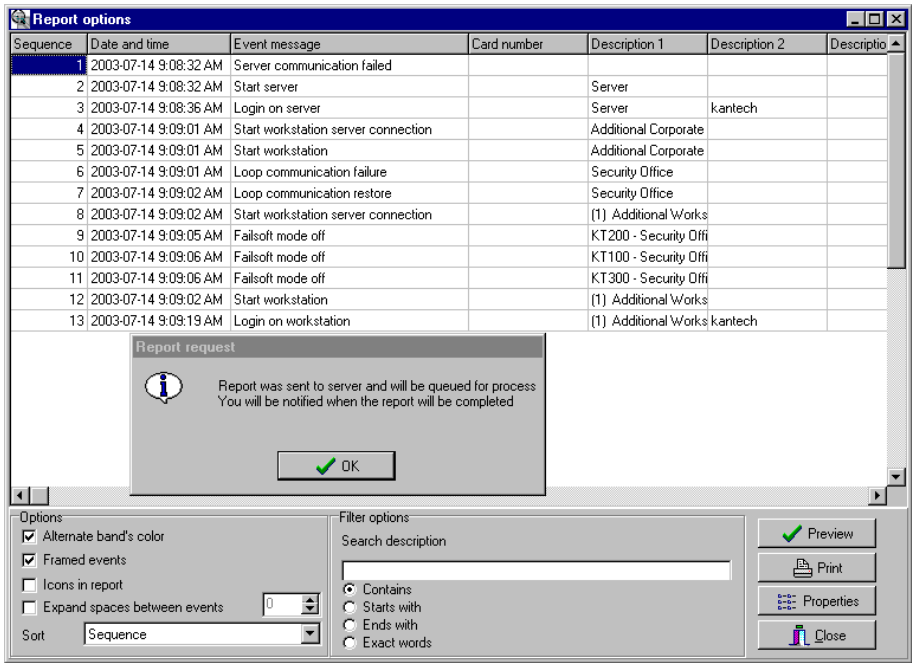


2 На панели слева (**Report list**) указать, какой отчёт должен быть выполнен.

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. Более подробная информация приведена *в разделе "Описание выходного формата отчёта" на стр. 423.*

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.



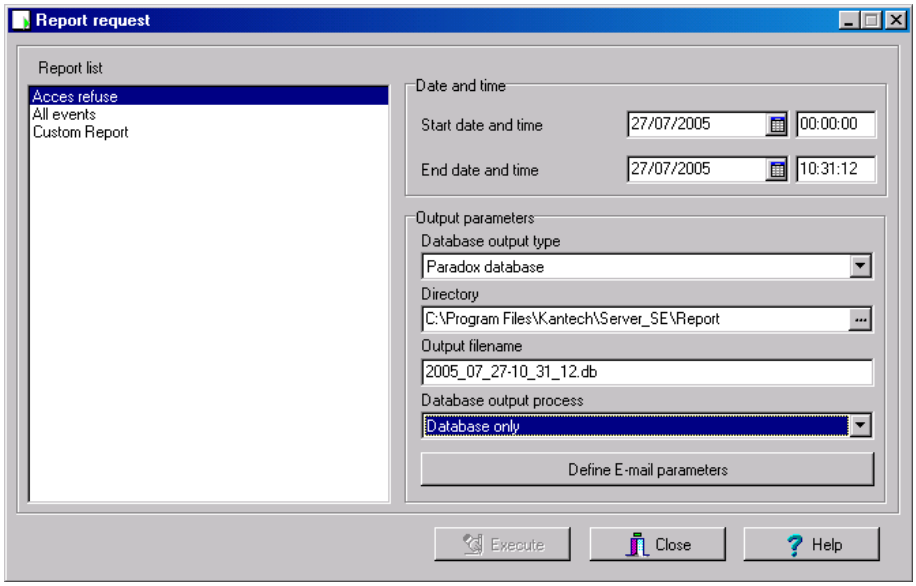
5 Нажать кнопку **Preview button** (Кнопка предварительного просмотра), чтобы настроить отчёт и установить необходимые фильтры. Повысить удобочитаемость отчёта можно, например, путём добавления полос другого цвете, обрамления событий в рамку, прикрепления к событиям иконок и др. или путём сортировки 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 формате .QRP) 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. Подробнее смотрите раздел "Описание выходного формата отчёта" на стр. 423.*

4 Чтобы увидеть статус отчёта, нажать иконку **Report state** (Статус отчёта) на панели инструментов.

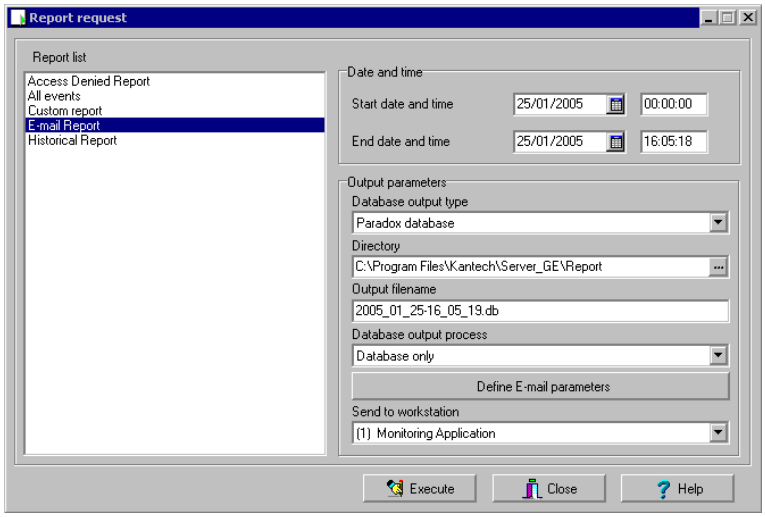
5 Нажать иконку **View report** (Посмотреть отчёт) на панели инструментов, чтобы посмотреть отчёт на экране. По умолчанию имя отчёта установлено YYYY_MM_DD_-HH_MM_SS.db (YYYY – год, MM – месяц, DD – день, HH – часы, MM – минуты, SS – секунды, .db – расширение файла).

Отчёты, отправляемые по электронной почте

Операторы системы EntraPass могут отправлять отчёты по электронной почте одному или нескольким адресатам. Функция электронной почты доступна во время описания 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 (Вызов отчёта) или T and A request (Отчёт по учёту рабочего времени).

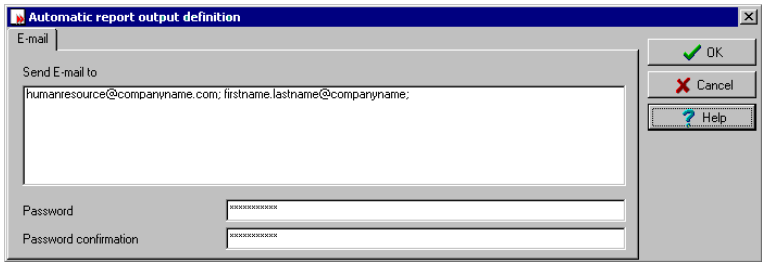


2 На панели **Report List** (Список отчётов) указать, какой отчёт необходимо отправить по электронной почте.

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)**.**

5 Нажать кнопку **Define E-mail parameters** (Описать параметры электронной почты), чтобы открыть окно Automatic report output definition (Описание 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.*

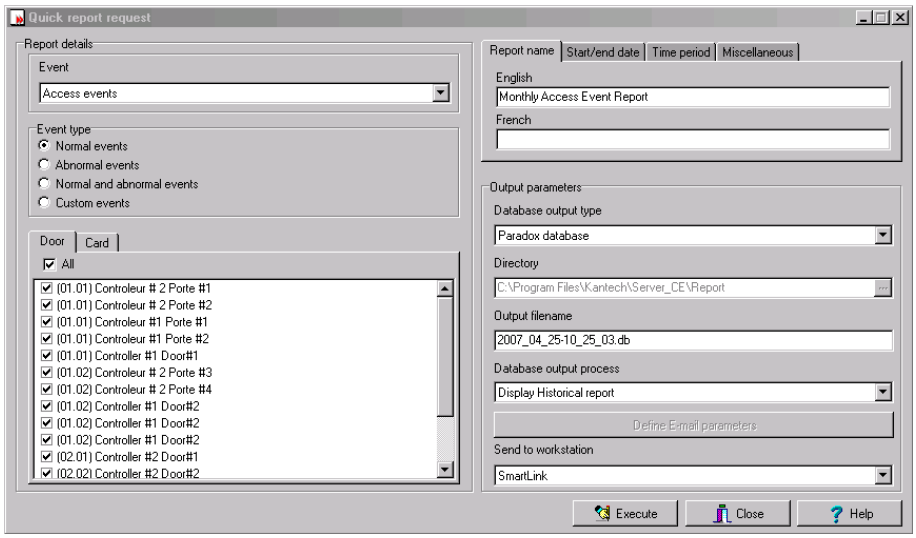
8 Нажать кнопку **Execute** (Выполнить), чтобы отправить отчёт на указанный адрес. Отчёт будет отправлен на рабочую станцию, указанную в выпадающем списке Send to workstation (Отправить на рабочую станцию), а также указанным адресатам.

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 станциях, 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.

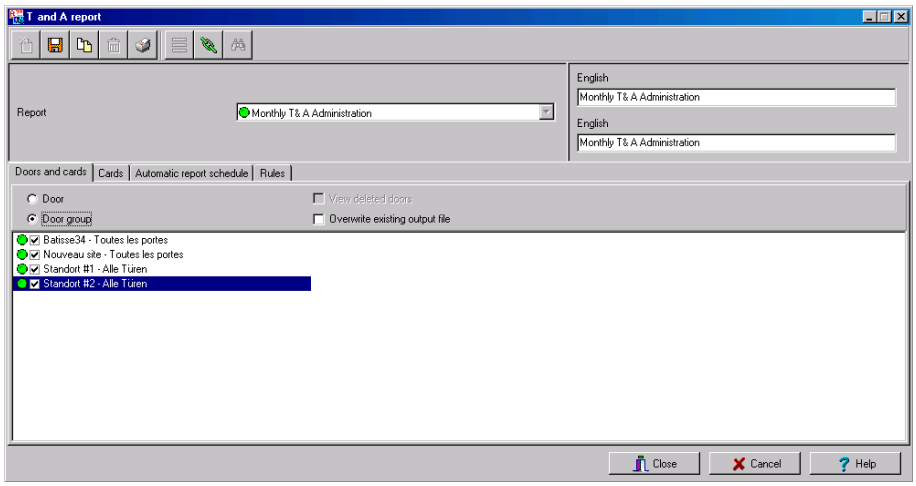
Описание отчётов по учёту рабочего времени

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****.*

Описание отчётов по учёту рабочего времени

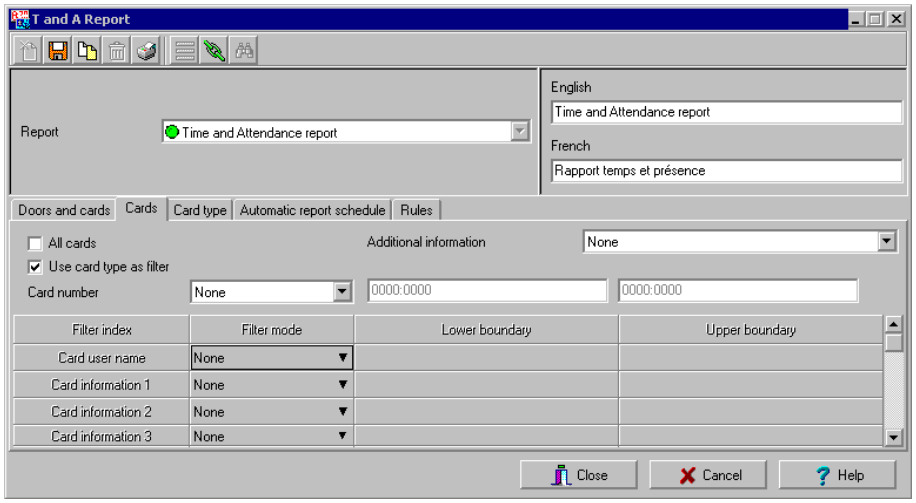
1 На панели инструментов в окне **Report** (Отчёты) нажать иконку **T & A Report** (Отчёт по учёту рабочего времени).



2 Если выбрана опция **Doors** (Двери), то на экране будут отображаться только двери, предназначенные для учёта рабочего времени (это должно быть указано в меню описания 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.

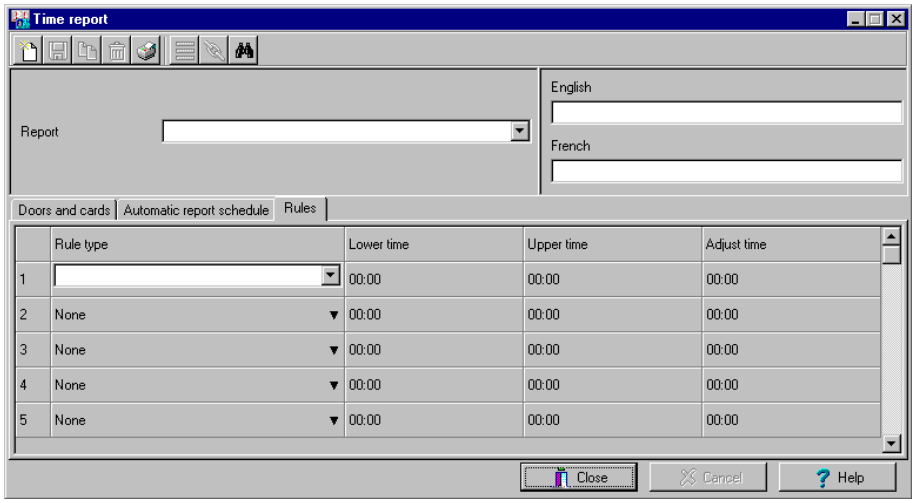
6 Чтобы добавить данные в критерии сортировки, следует выбрать параметр в выпадающем списке **Additional information** (Дополнительные сведения).

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. Подробнее об описании автоматических отчётов смотрите *в разделе "Настройка расписания автоматических отчётов" на стр. 421.*

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.



Запросы отчётов по учёту рабочего времени

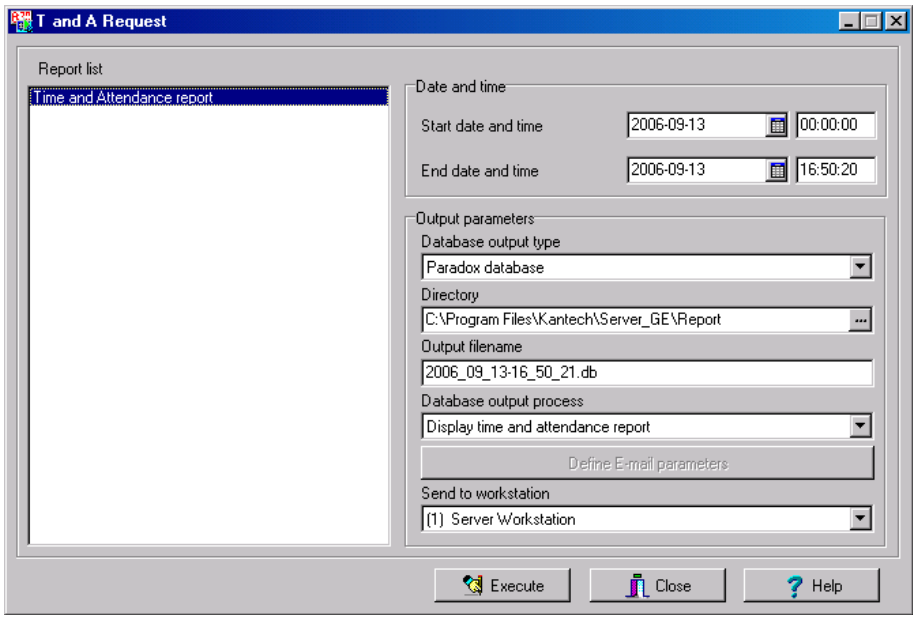
С помощью этой функции операторы могут запрашивать предварительно настроенные отчёты (Time and attendance reports), созданные при помощи меню Time and Attendance Report Definition (Описание отчёта по учёту рабочего времени). Эта функция позволяет запрашивать отчёт вручную, игнорируя автоматические настройки.

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**) указать, какой отчёт должен быть выполнен.

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).*

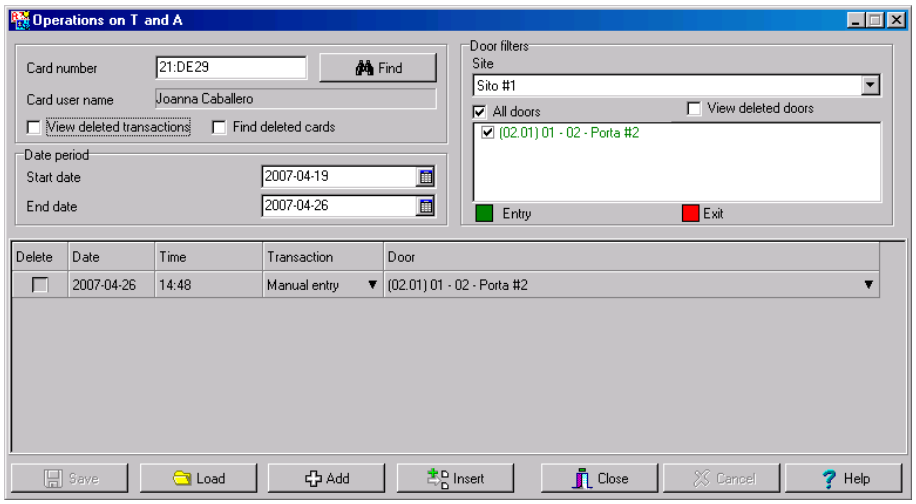
ПРИМЕЧАНИЕ. *При работе с файлами типа Paradox система выводит на экран окно предварительного просмотра отчёта. В других выходных форматах необходимо вручную запрашивать отчёт, иначе он не будет выведен ни на экран, ни на принтер. Чтобы просмотреть все сгенерированные отчёты, следует воспользоваться кнопкой View Report (Посмотреть отчёт) на панели инструментов Report (Отчёты). Подробнее смотрите раздел "Описание выходного формата отчёта" на стр. 423.*

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** (Сайт) выделить сайт/шлюз, 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 в поле Site, 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.

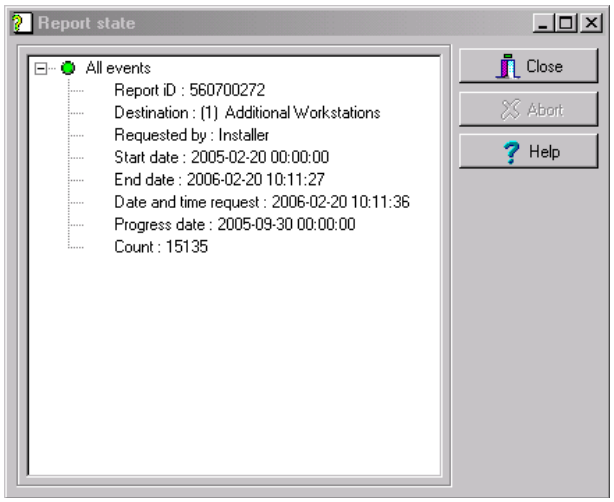
13 Чтобы вставить транзакцию в список между другими транзакциями или вместо любой транзакции, следует воспользоваться кнопкой **Insert** (Вставить).

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).*

Статусы отчётов (Report State)

Функция **Report state** предназначена для отображения списка, а также статусов всех запрошенных отчётов, которые еще находятся в очереди.



1 Для удаления/прекращения генерации отложенного отчёта следует выделить его в списке и нажать кнопку **Abort** (Прервать).

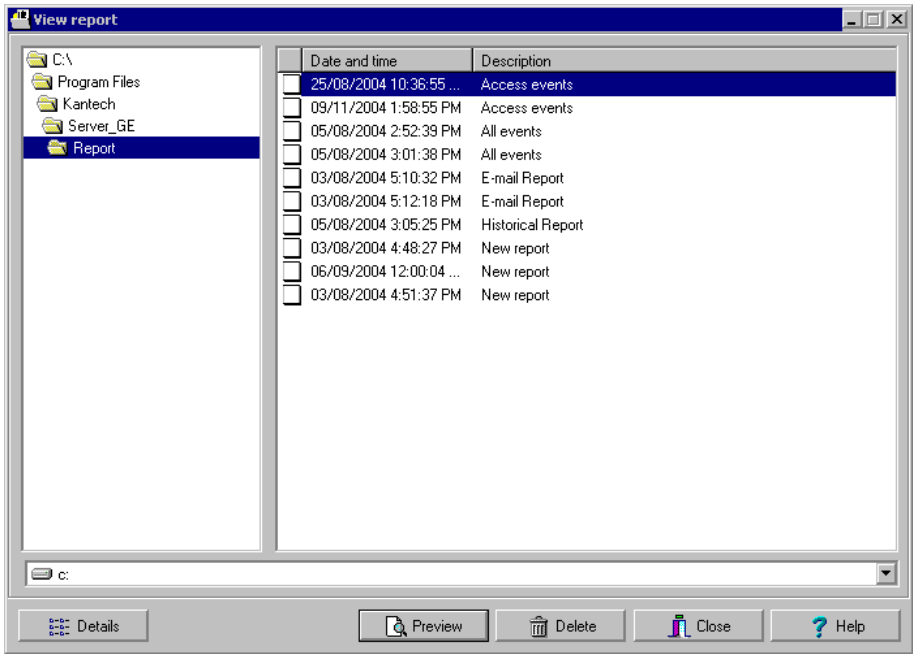
Просмотр отчётов

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.*

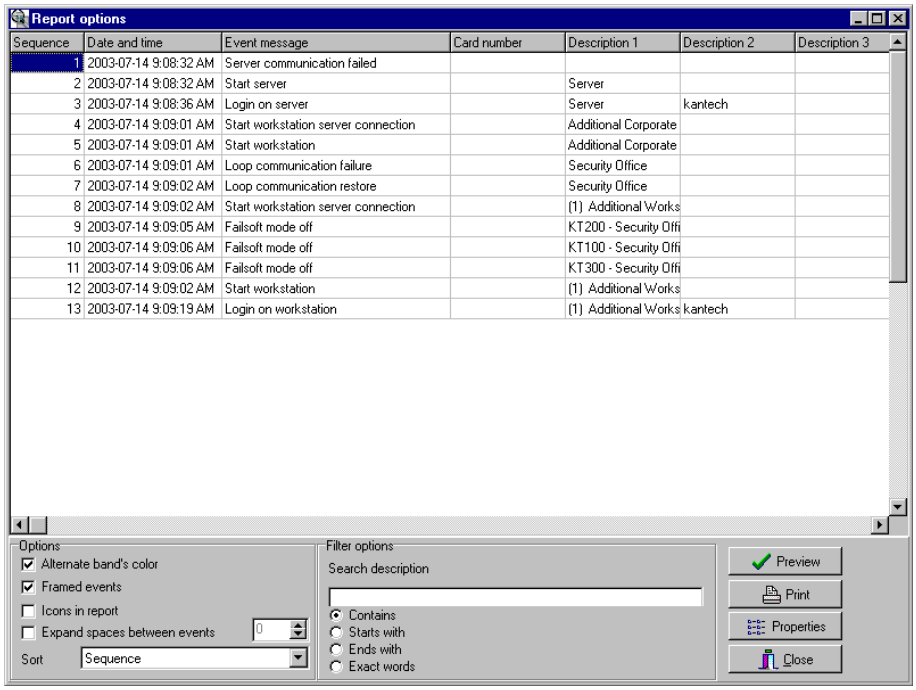
3 Чтобы увидеть информацию об отчёте, нажать кнопку **Details** (Подробные сведения). В случае нажатия кнопки **Details** на экране появляется окно Report details (Подробные сведения об отчёте), в котором отображаются данные, связанные с выделенным файлом отчёта (имя файла, заголовок, тип, дата и др.). Чтобы закрыть окно Report details, нужно снова нажать кнопку **Details**.

4 Нажать кнопку **Preview** (Предварительный просмотр), чтобы вывести отчёт в окно предварительного просмотра (Report preview).

Предварительный просмотр архивных отчётов

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). Система выведет на экран результаты отчёта. В этом окне можно сохранить отчёт (в формате .QRP) или распечатать его на принтере.

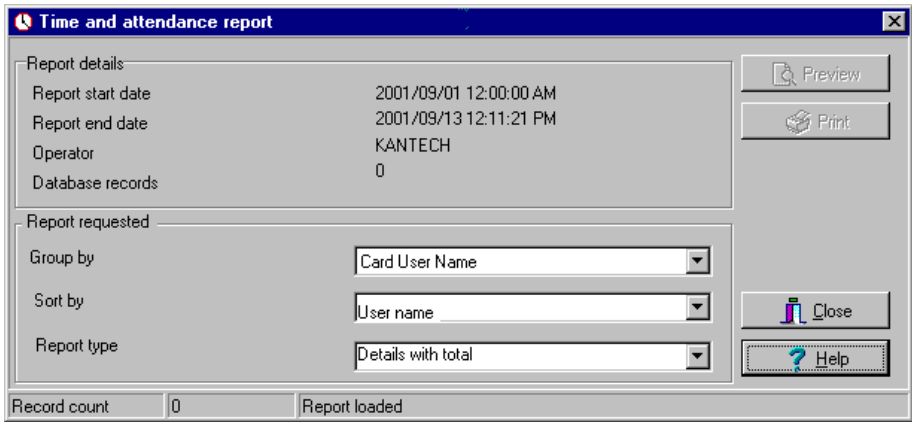
4 Нажать **Properties** (Свойства), чтобы открыть окно Reports details (Подробные сведения об отчёте).

- **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 выполнения запроса.
- **Delivered** (Выполнен...) – отображает дату и время создания и печати отчёта.
- **Requested by** (Запрошен...) – содержит имя оператора, выполнившего запрос отчёта.
- **Count** (Счётчик) – отображает число транзакций (строк), включённых в отчёт.
- **Output process** (Способ вывода) – отображает список шаблонов, которые можно использовать 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 для указанного отчёта при описании была выделена опция 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 **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):

- Выбор формата карты по умолчанию
- Изменение аутентификационного пароля
- Выбор языка
- Настройка типа принтера
- Изменение даты и времени системы
- Настройка мультимедийных устройств
- Изменение системных параметров
- Расписание автоматического резервного копирования
- Регистрация системы (эта иконка исчезает из меню рабочей станции после того, как система зарегистрирована)

Ниже перечислим утилиты, которые доступны в меню **Option** (Опции) только в приложении Рабочая станция (EntraPass Workstation):

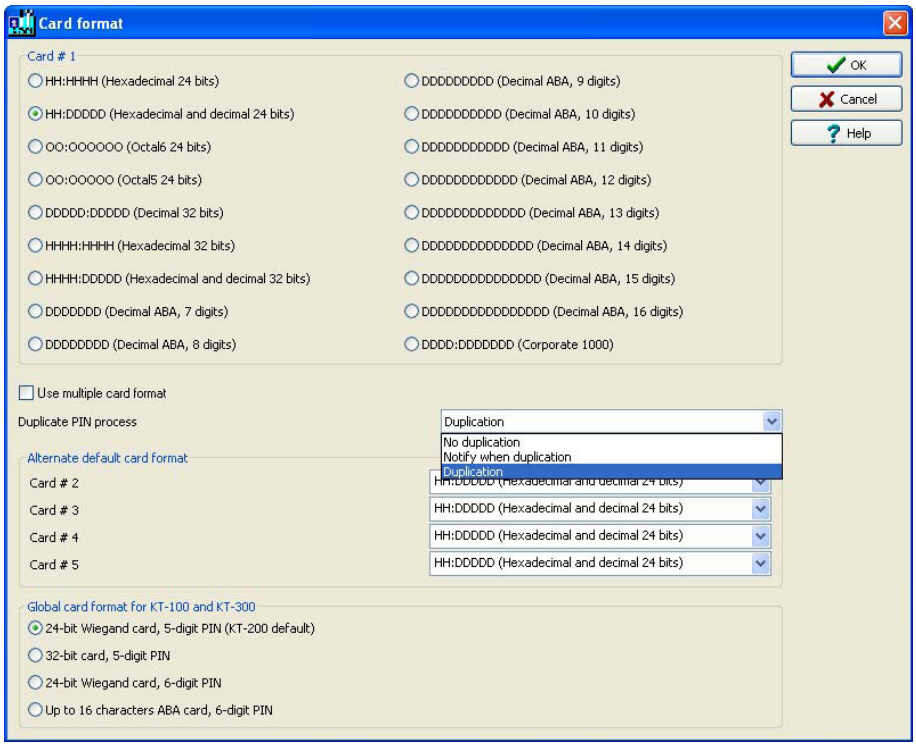
- Настройка опций принтера (принтеры журналов и электронных пропусков)
- Настройка конфигурации мультимедийных устройств (параметры тревожной сигнализации, оцифровка фотографий и подписей)
- Настройка специальных сообщений
- Полная проверка базы данных сервера
- Полная проверка базы данных рабочей станции

Выбор формата карты 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.

Описание 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.

ПРИМЕЧАНИЕ. *В будущем планируется осуществить поддержку системой EntraPass 17, 18, 19 и 20-ой системы счисления.*

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 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 дубля 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 Если была выделена опция Advanced User (Продвинутый пользователь), то теперь будет доступно поле **Card #2** (Карта №2) для выбора другого формата по умолчанию для карты №2.

6 Если была выделена опция Advanced User (Продвинутый пользователь), то п.5 следует повторить для карты №3 (**Card #3**), карты №4 (**Card #4**) и карты №5 (**Card #5**).

7 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.

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).

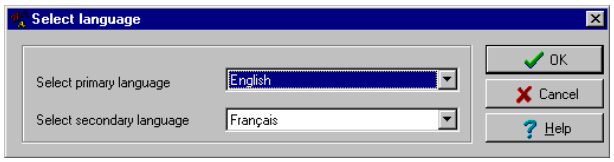
ПРИМЕЧАНИЕ. *Аутентификационный пароль отличается от пароля на доступ оператора. Аутентификационный пароль используется для аутентификации рабочих станций на сервере, а пароль оператора служит для открытия рабочей сессии.*

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 привести к разрушению базы 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

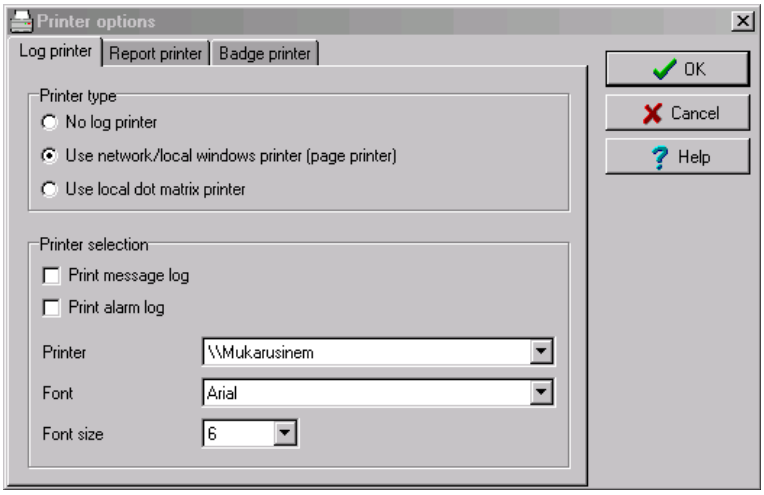
Меню **Printer options** (Опции принтера), вызываемое из меню **Options** (Опции), позволяет пользователям выбирать принтер для печати журналов событий и принтер для печати отчётов или электронных пропусков.

Выбор и настройка принтера журналов (Log Printer)

После описания событий в меню **Events parameters** (Параметры событий) можно указать, каким образом и когда операторы будут проинформированы об этих событиях. 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 печати 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, которая будет служить в качестве принтера журналов (Log printer).

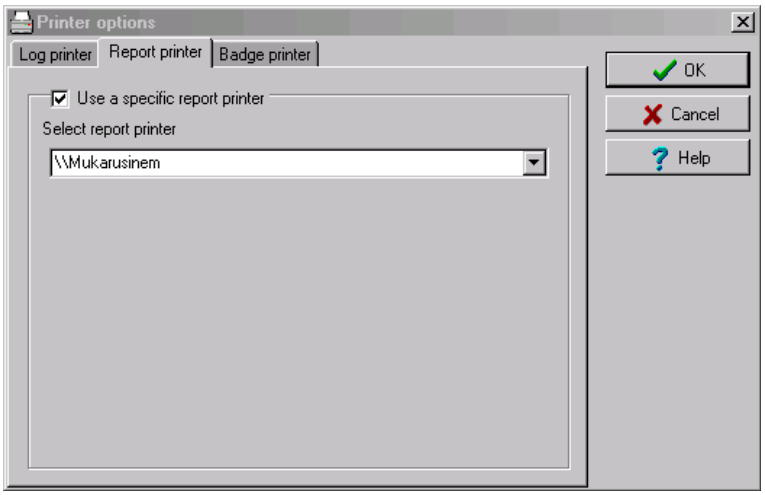
Если была выделена опция **Dot matrix printer** (Матричный принтер), то в поле **Port** следует указать порт, через который принтер подсоединяется к компьютеру. Поле **Port** (Порт) появляется в случае выделения опции Dot matrix printer.

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.

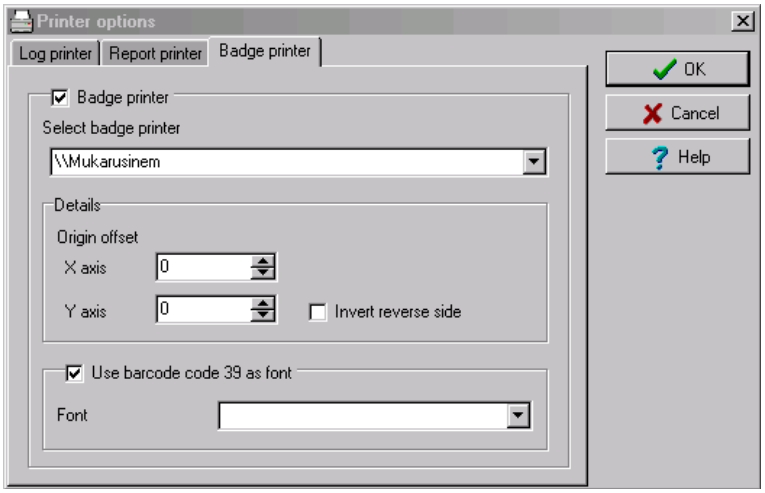
1 В окне Printer option выбрать закладку **Report printer** (Принтер отчётов).



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).

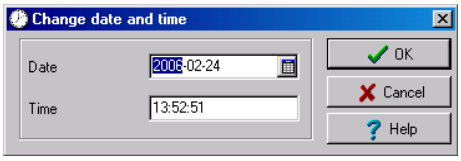
5 Если необходимо, поставить флажок в поле **Use barcode 39** (Использовать штрихкод 39) и указать шрифт в поле **Font**.

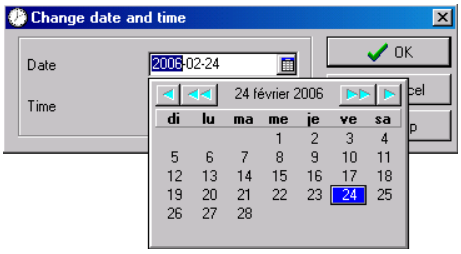
Изменение даты и времени системы

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). Подробные сведения по настройке времени сети смотрите *в разделе "Опции системы EntraPass" на стр. 443*.

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 виртуальном 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 (Описание параметров сервера). Подробности смотрите в разделе "Опции системы EntraPass" на стр. 443.*

ВАЖНЫЕ ПРИМЕЧАНИЯ: Не рекомендуется изменять время в настройках Windows®. Настоятельно рекомендуется изменять время в системе через настройки параметров сервера.

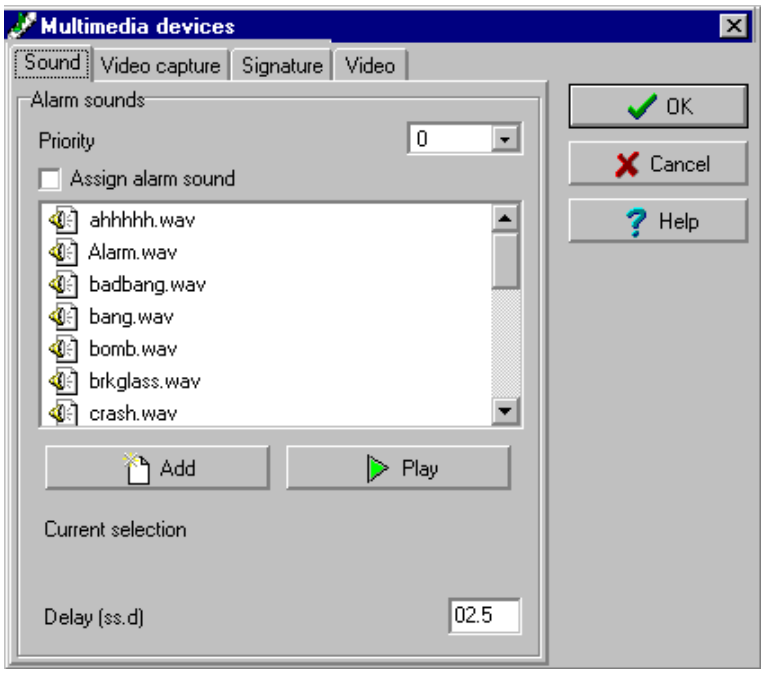
Конфигурация мультимедийных устройств

Утилита Multimedia devices (Мультимедийные устройства) позволяет настроить следующие средства мультимедиа:

- Звуковая тревожная сигнализация
- Устройства оцифровки изображений
- 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, в какой последовательности тревожные сообщения будут отображаться на рабочем столе тревог (Alarm desktop). В системе EntraPass, "0" соответствует самому высокому приоритету, "9" – самому низкому. Более подробная информация приведена в разделе "Описание параметров событий" на стр. 350.*

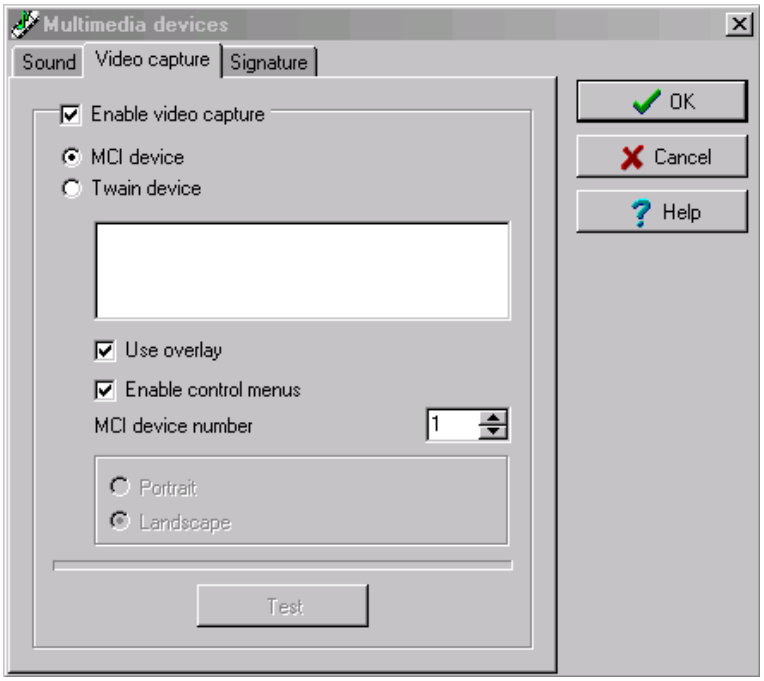
5 Нажать **Play** (Воспроизвести), чтобы прослушать звуковой сигнал. Система воспроизведёт выбранный звуковой сигнал.

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 изображений

1 В окне Multimedia devices (Мультимедийные устройства) открыть закладку **Video capture** (Оцифровка изображений).



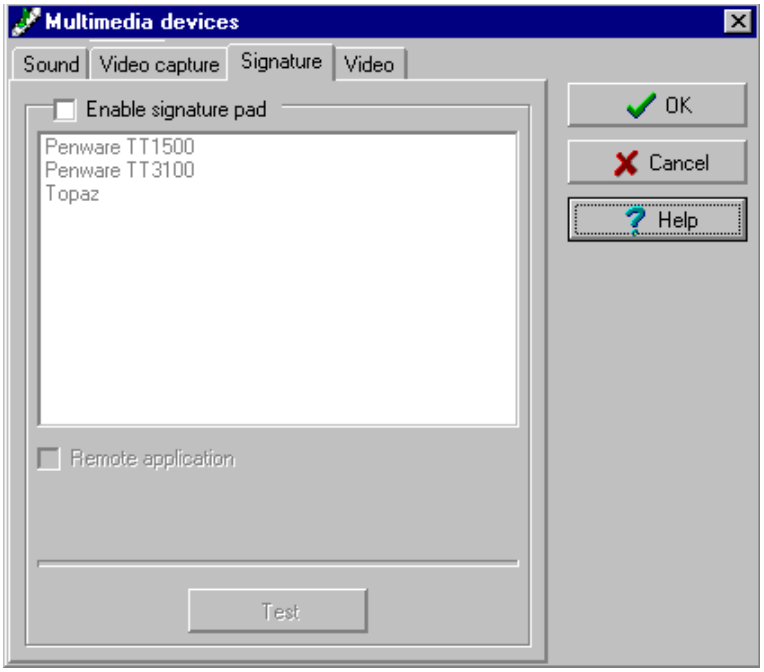
2 Поставить флажок в поле **Enable video capture** (Разрешить оцифровку изображений), чтобы разрешить использование этой функции в системе.

- **MCI device** (Драйвер MCI) – стандартные драйвера оцифровки в среде Windows®
- **Twain device** (Драйвер Twain). (Рекомендуется.)
- **Use overlay** (Использовать наложение) – эта опция используется для устройств оцифровки 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).



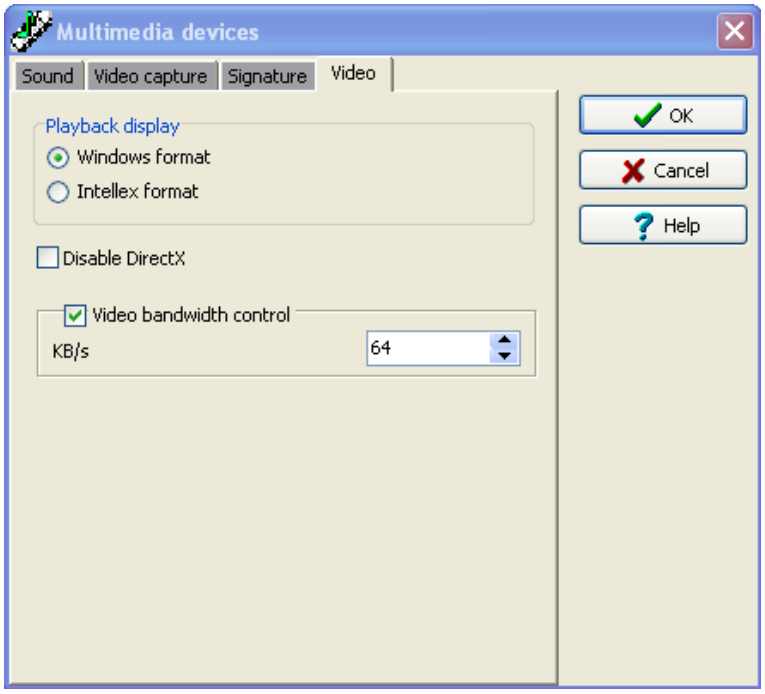
2 Выделить флажком опцию **Enable Signature pad** (Активировать устройство ввода подписей), чтобы разрешить использование такого устройства.

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.

ПРИМЕЧАНИЕ. *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 описания: Card (Карты), Visitor (Посетители) и Daypass (Разовые пропуска).*

5 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 (см. стр. 476).*

Настройка системных параметров

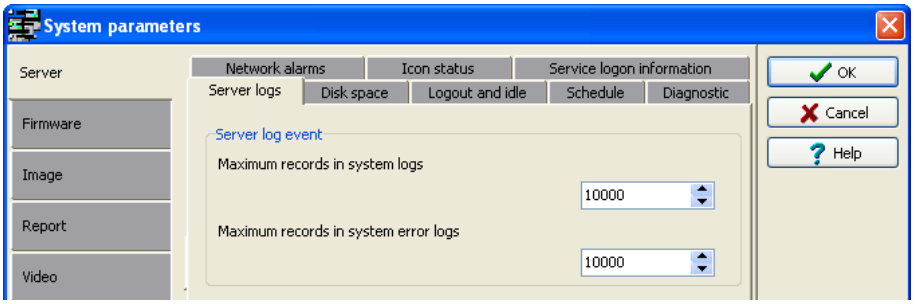
При помощи меню System parameters (Системные параметры) пользователь с правами системного администратора (System Administrator) получает возможность изменять параметры, используемые для описания системы EntraPass.

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 (Server)

Под закладкой **Server** (Сервер) собраны параметры настройки максимальных размеров журналов, функции диагностики, параметры безопасности, ограничения используемого пространства на диске, сетевые тревоги и индикация статусов на иконках.

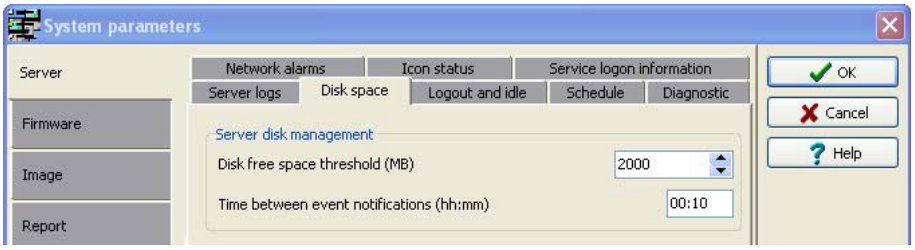
Журналы сервера (Server Logs)



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, останов 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)

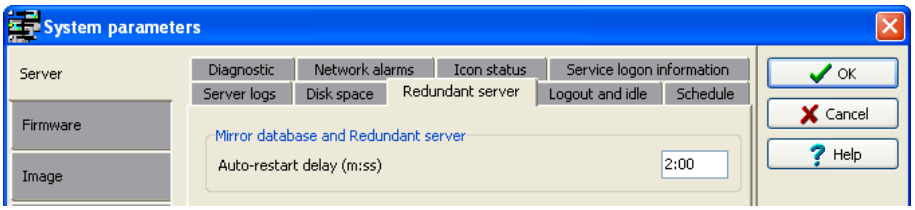
Функция Disk Space предназначена для защиты от неполадок в работе системы из-за нехватки рабочего пространства на диске. Эта функция позволяет наблюдать за свободным местом на диске в целях обеспечения оптимальной работы системы или для создания отчётов. В системе EntraPass предусмотрено прекращение 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.

Резервный сервер (Redundant Server)

ПРИМЕЧАНИЕ. *Эта опция недоступна, если в системе не установлен резервный сервер.*

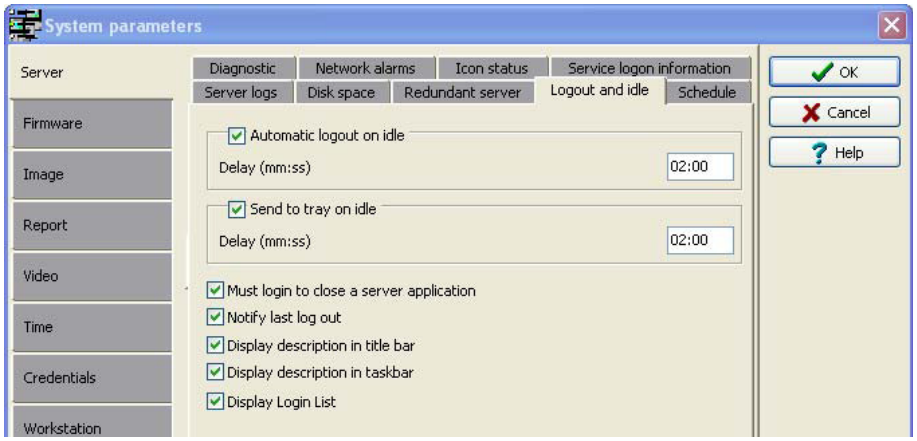


В поле Automatic restart delay (Задержка автоматической перезагрузки) можно установить задержку для зеркальной базы данных и резервного сервера. Диапазон допустимых значений: от 1:00 до 9:59.

ПРИМЕЧАНИЕ. *После запуска и загрузки основного сервера можно запустить зеркальную базу данных и резервный сервер (**Mirror Database and Redundant Server**). Даже если интерфейс MS/SQL не может соединиться с зеркальной базой данных на резервном сервере, все сообщения будут сохраняться в буфере.*

Окончание 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 регистрацию 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** (Показывать 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.*

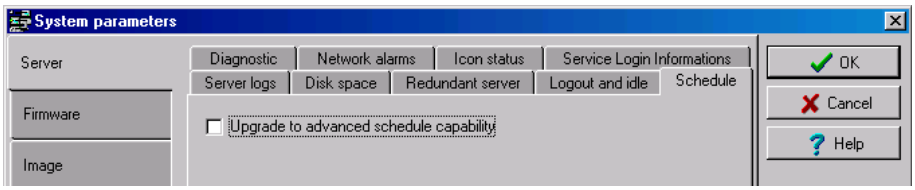
Расписание (Schedule)

Закладка **Schedule** служит для обновления структуры расписания до более совершенной модели. В усовершенствованной модели все расписания сгруппированы по шлюзам, сайтам 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.*

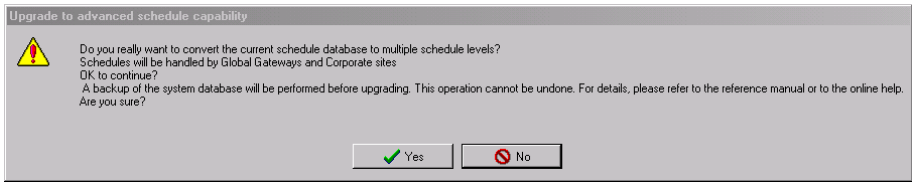
Расписания сгруппированы следующим образом:

- **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.
- **Corporate site schedules** (Расписания для корпоративных сайтов) – отдельные расписания для каждого сайта. 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.

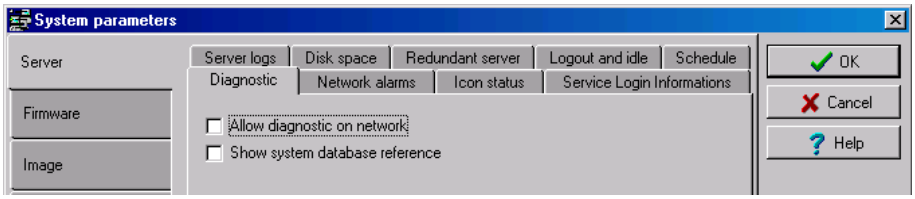
- Перед выполнением этого действия настоятельно рекомендуется создать резервную копию данных.



- После завершения процесса закладка **Schedule** исчезнет из меню System Parameter (Системные параметры).

Диагностика (Diagnostic)

Эта функция позволяет выполнять диагностику сети.

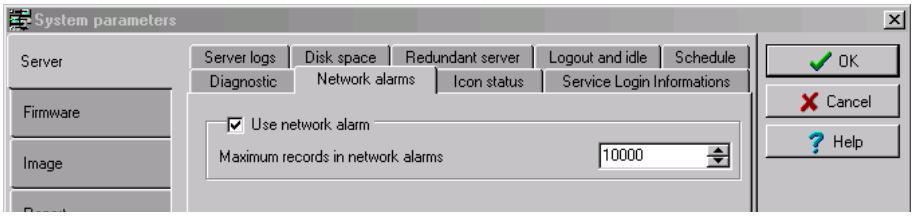


- **Allow diagnostic on network** (Разрешить диагностику сети) – разрешает использование утилиты PING (Packet INternet Groper). Эта автономная программа служит для диагностики неисправностей в сети и/или проверяет состояние маршрута следования пакета до определенного IP-адреса. Подробнее о программе PING смотрите *в разделе "Системные утилиты" на стр. 493*.
- **Show system database reference** (Показывать индексы) – 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.

Сетевые тревоги (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.



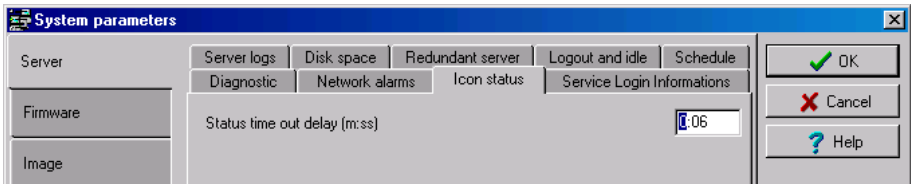
- Поставить флажок в поле **Use network alarm** (Использовать сетевые тревоги), чтобы использовать эту функцию, или не ставить флажок, чтобы запретить её использование.

- 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. Более подробная информация о сетевых тревогах приведена в разделе "Рабочие столы EntraPass" на стр. 369.*

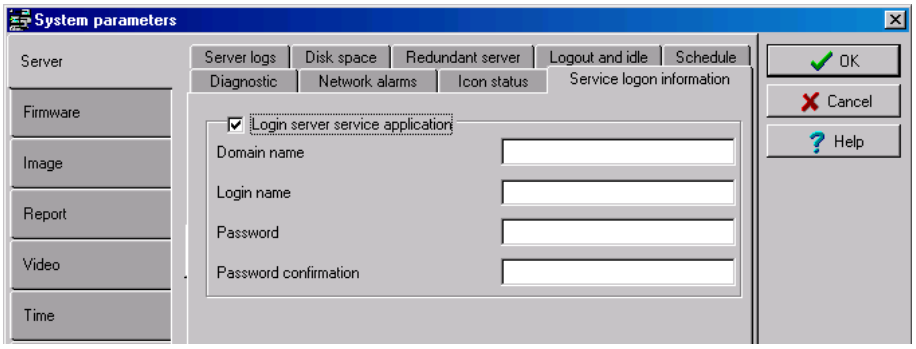
Индикация статусов на иконках (Icon Status)

Параметр **Status time out delay** (Таймаут статуса) позволяет указать задержку, после окончания которой рабочая станция пошлёт на сервер запрос о последних статусах иконок. Чем больше указанное время задержки, тем меньше частота обновления иконок, и соответственно, меньше загрузка сети. Максимальное значение параметра составляет 1 мин. 30 сек.



Данные регистрации для работы в режиме службы (Service Login Information)

Параметры, указываемые в разделе **Service Login Information,** требуются для программы **Backup Scheduler** (Планировщик заданий по созданию резервных копий). Введённые данные используются для работы сервера в режиме службы.



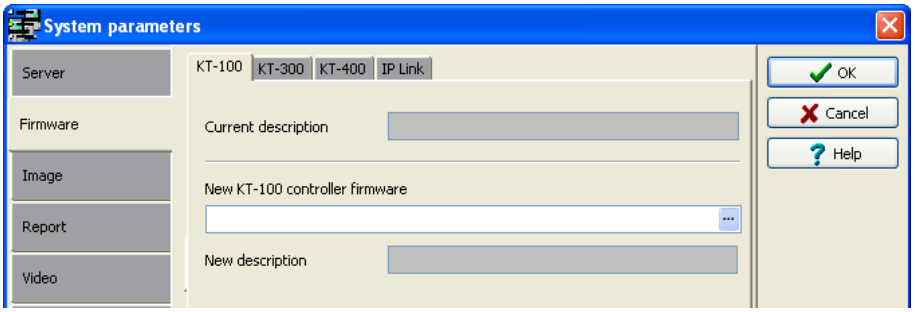
- Чтобы воспользоваться этой опцией, нужно поставить флажок в поле **Login Server service application** (Регистрационные данные для работы сервера в режиме службы).
- **Обязательно** указать имя домена или рабочей группы в поле **Domain name** и имя пользователя в поле **Login name** и дважды ввести пароль в полях **Password** (второй раз – для подтверждения).

Параметры прошивки (Firmware)

Этот раздел меню содержит всю необходимую информацию о контроллерах, шлюзах и IP-модулях, а также раздел для обновления прошивки.

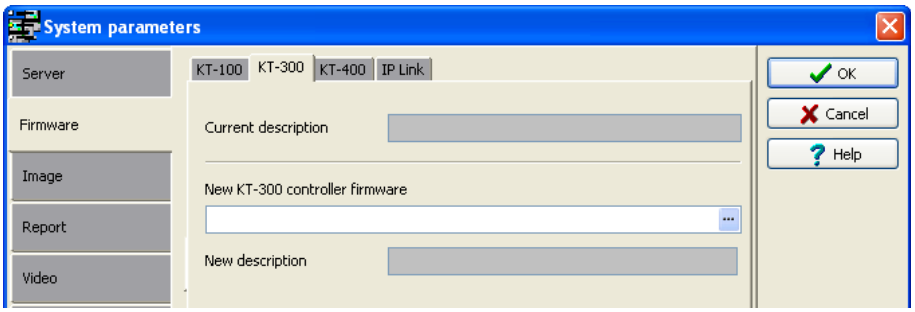
KT-100

Закладка **KT-100** указывает место размещения папки, в которой хранится прошивка для контроллеров KT-100. Эти данные будут использоваться для обновления установленных контроллеров.



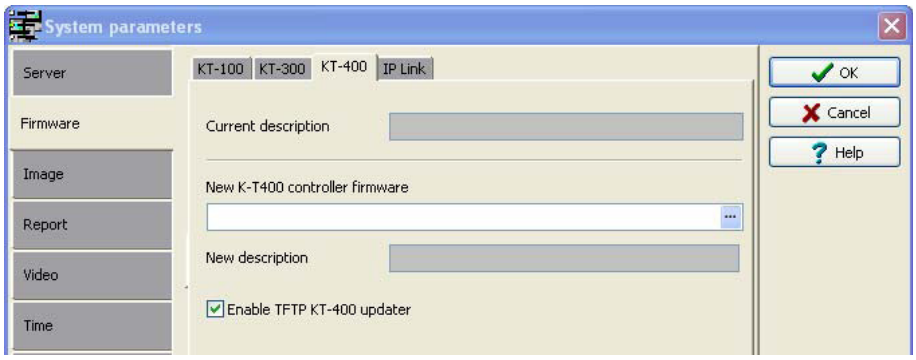
KT-300

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.



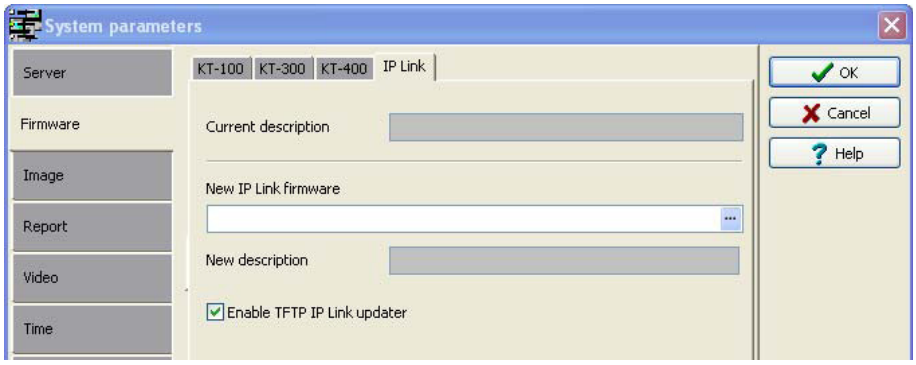
- Если в поле **Enable TFTP KT-400 updater** (Разрешить обновлять KT-400 через TFTP) поставить флажок, то операторы смогут обновлять прошивку контроллера KT-400 при помощи кнопки **Update firmware** (Обновить прошивку) в меню **Operation** (Операции) > **Site** (Сайт).

ПРИМЕЧАНИЕ. *Чтобы программа обновления прошивки (TFTP KT-400 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.

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. *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.

Параметры изображений (Image)

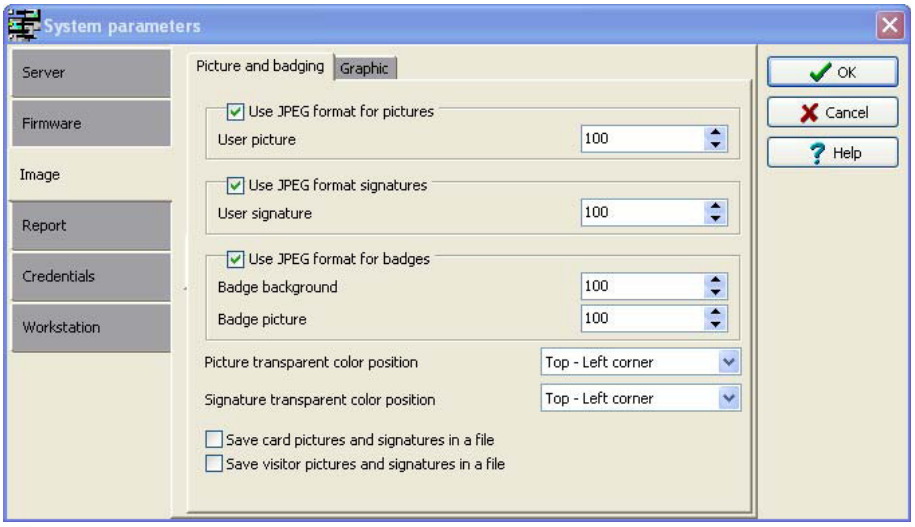
Раздел меню Image служит для описания параметров, необходимых для создания электронных пропусков. Необходимо указать уровень качества изображений для фотографий, подписей и фоновых изображений.

- 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.

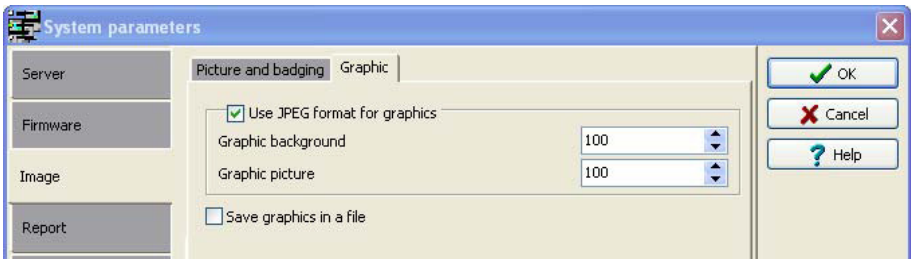
ПРИМЕЧАНИЕ. *Помните, что это может ухудшить качество изображения. Непродвинутым пользователям лучше оставить эти настройки по умолчанию.*

- 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 фотографии и подписи в поле **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_CE\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_CE\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 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_CE\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.*

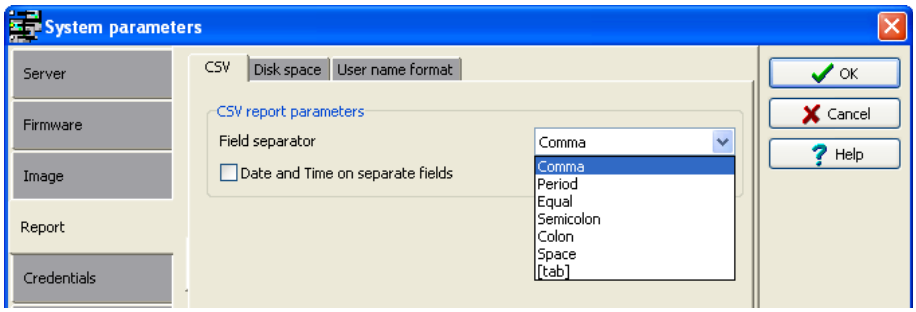
Параметры отчёта (Report)

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.

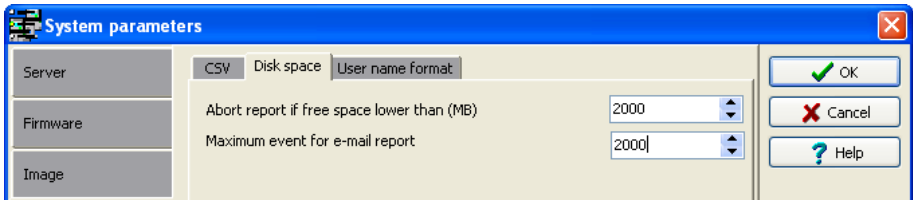


Пространство на диске (Disk Space)

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.

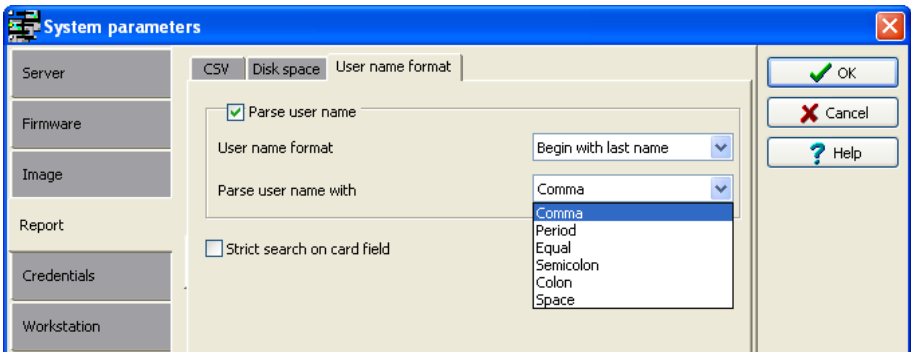
- **Abort report if free space lower than** (Прервать выполнение отчёта, если свободного места осталось менее...) – в этом поле следует указать минимальное доступное место на диске, необходимое для выполнения отчётов. Допустимый диапазон значений: от 2000 до 999 999 Мб.

- **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.



Формат имён пользователей (User Name Format)

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.

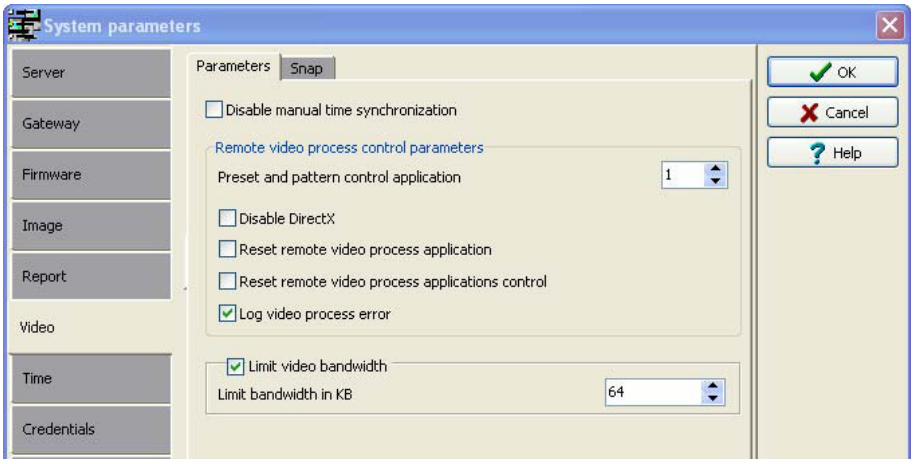
ПРИМЕЧАНИЕ. *В системе EntraPass версии 3.18 и ниже система использовала более строгий метод поиска, требовавший обязательного указания верхней и нижней границ поиска для получения результатов. Например, при составлении отчёта, в который должны быть включены все пользователи с фамилиями, начинающимися на букву A, необходимо было указать нижнюю границу "A", а верхнюю границу "AZZZZZ". Теперь для этого в обоих полях (верхней и нижней границы) достаточно указать "A".*

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, выполнение всех записей на видеосервере не прерывалось.
- 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** (Приложение 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_CE\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), смотрите стр. 455.

ПРИМЕЧАНИЕ. *Установленное значение полосы пропускания на рабочей станции не может* ***превышать*** *значение этого параметра на сервере EntraPass.*

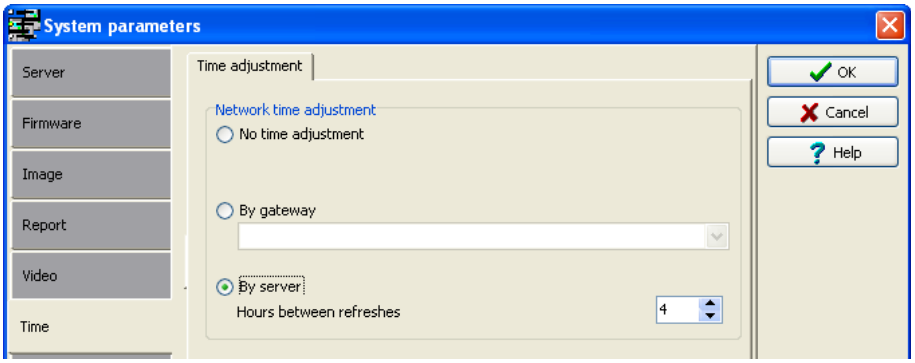
Захват изображения (Snap)

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.



ПРИМЕЧАНИЕ. *Шлюз опрашивает первый контроллер на первом сайте в 5:47 am или 05:47, в 1:47 pm или 13:47 и в 7:47 pm или 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.

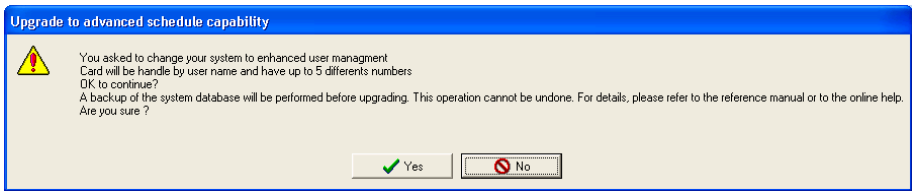
Параметры доступа (Credentials)

Карты (Card)

Под закладкой **Card** системные администраторы имеют возможность перестроить систему EntraPass и включить режим усиленного администрирования пользователей, чтобы работать с пользователями, выбирая их не только по именам, но и по номерам карт. Каждый владелец карты будет наделён именем пользователя и сможет иметь до 5 разных номеров карт. Этот режим позволяет создавать карты, не назначая номера для новых карт, смотрите раздел *"Выпуск новой карты в режиме усиленного администрирования пользователей" на стр. 231.* Эта опция используется с веб-станцией EntraPass WebStation для организации работы с картами. Более подробную информацию по работе с веб-станцией EntraPass можно получить *в справочном руководстве* (DN1709).

ВНИМАНИЕ! Переход в режим усиленного администрирования пользователей является **НЕОБРАТИМЫМ** процессом. Однако при передаче данных система создает резервную копию, с которой можно восстановить предыдущий режим работы системы.

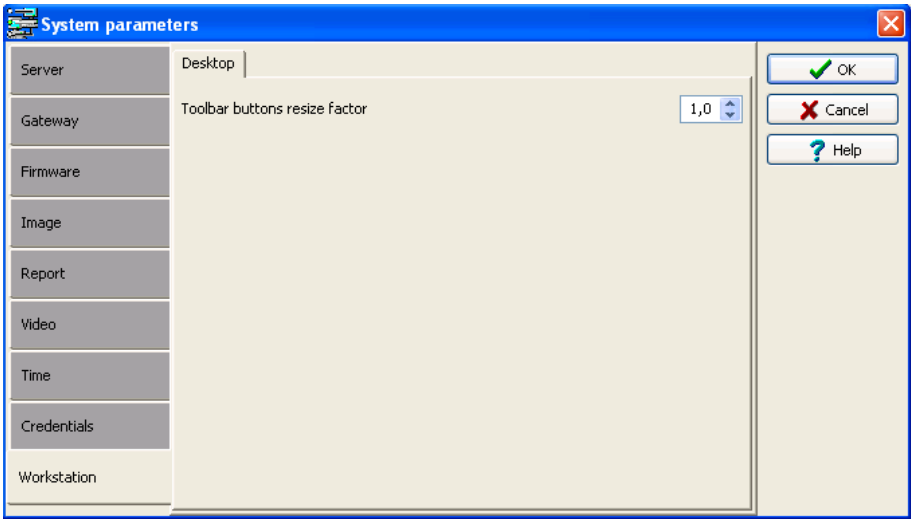
- **Migrate to enhanced user management** (Переход в режим усиленного администрирования пользователей) – установить метку, чтобы система перешла в этот режим.
- При выделении данной опции и нажатии кнопки **OK** система выдаёт на экран предупреждение о том, что данная операция необратима, пока система 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. Ниже для сравнения приведён пример минимального размера кнопки (1.0) и её максимального размера (2.5).

Default = 1.0

Maximum = 2.5

Планировщик заданий по созданию резервных копий (Backup Scheduler)

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 только неродного программного обеспечения не рекомендуется).

ПРИМЕЧАНИЕ. *По умолчанию во время создания резервных копий или восстановления файлов базы данных сервера временно недоступны (отключены). Рабочие станции не смогут изменять базы данных.*

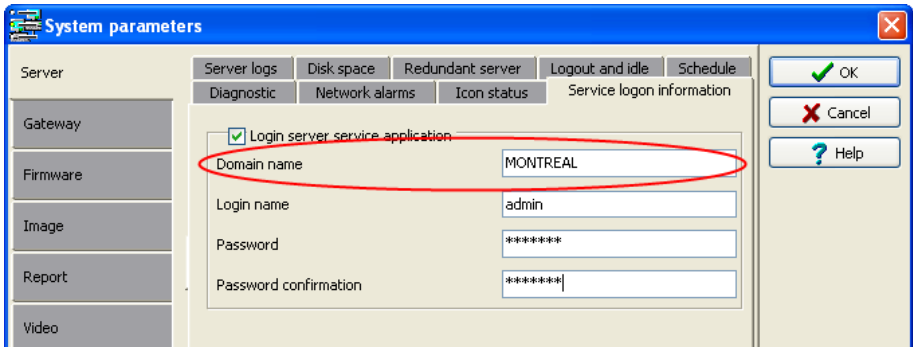
Программа-планировщик Backup Scheduler предназначена для создания расписаний резервного копирования системных данных, архивов и данных по учёту рабочего времени. Достаточно указать настройки по умолчанию, и система сделает все остальное сама!

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.**

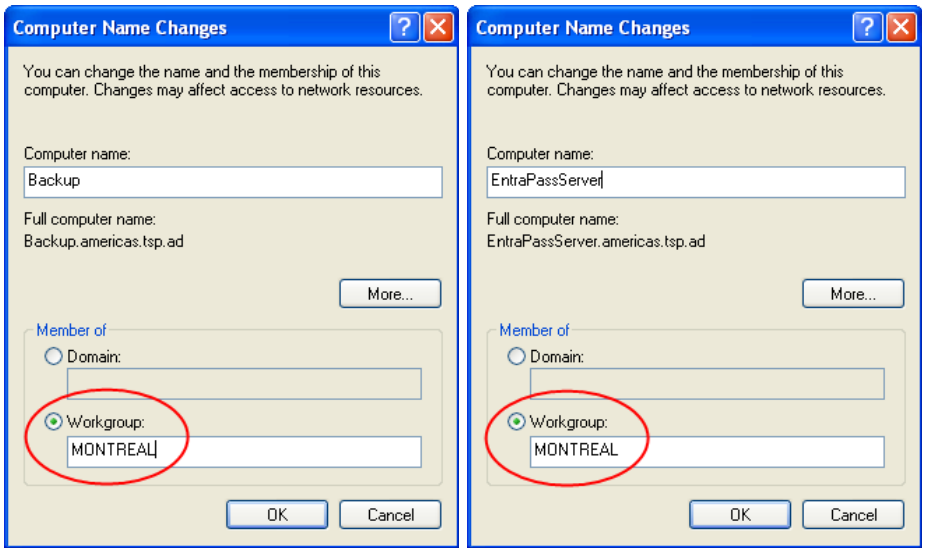
ПРИМЕЧАНИЕ. *Для выполнения описанных ниже действий на сервере EntraPass пользователь должен иметь все права администратора. При отсутствии необходимых прав или недостаточном знании средств администрирования Windows (Windows Administrative Tools) следует обращаться к администратору сети.*

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. *В поле Domain Name записывают имя рабочей группы или домена, в которые входят сервер EntraPass и резервный компьютер, как в примерах ниже.*

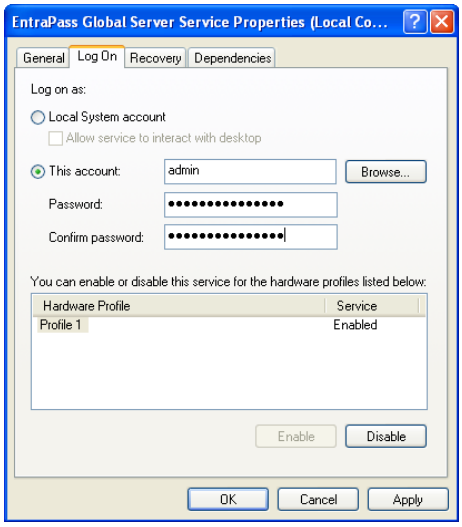


3 Нажать **OK**.

4 Войти в меню **Start** (Пуск) Windows > **Control Panel** (Панель управления) **> Administrative Tools** (Администрирование) > **Services** (Службы).

5 Открыть **EntraPass Corporate Server Service**.

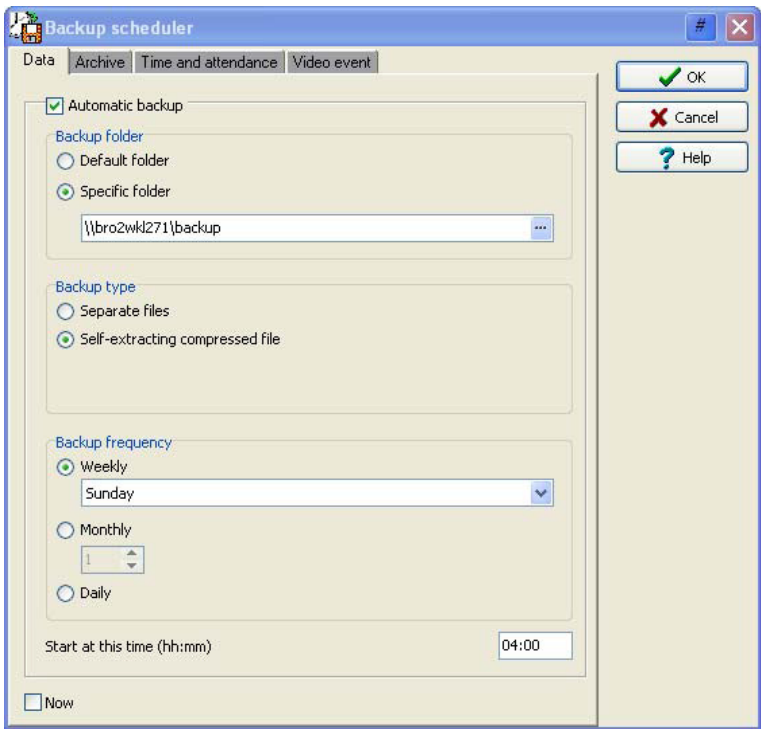
6 Открыть закладку **Logon** (Регистрация в системе), указать данные в поле **This account** (Эта учётная запись)**,** они должны совпадать с данными, указанными в **пункте 2**.



7 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.

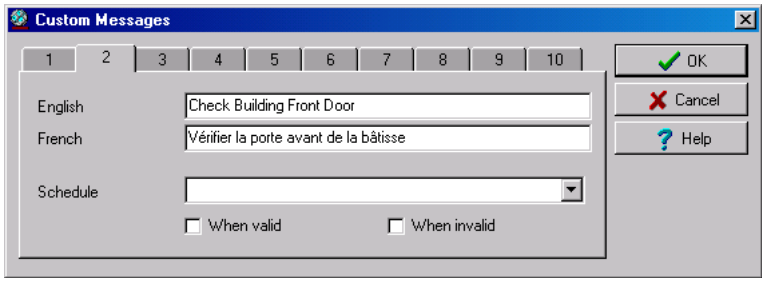
9 Нажать **OK** для сохранения.

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.

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.

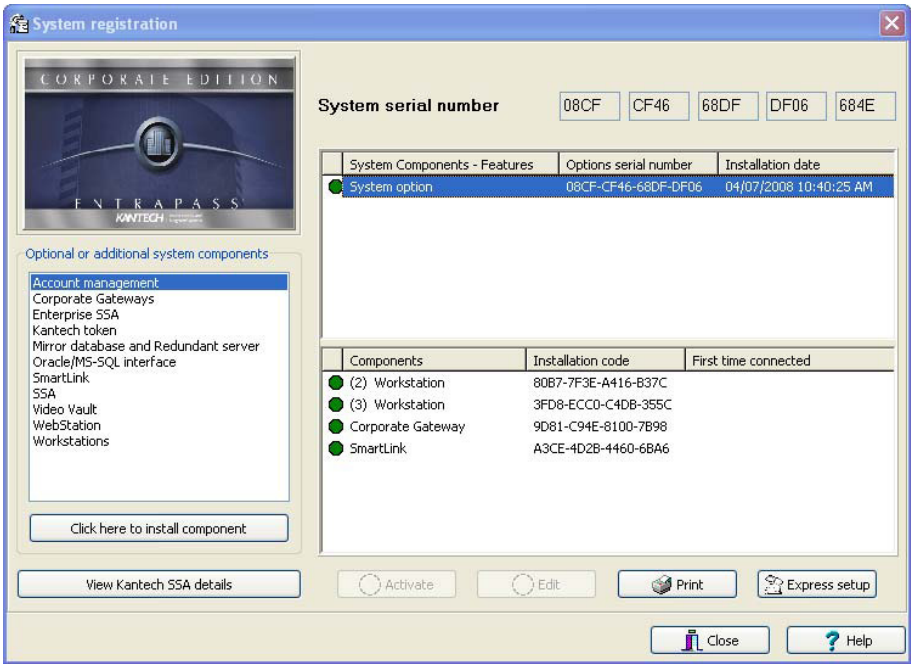
3 Указать предварительно настроенное расписание, по которому будет инициироваться специальное событие.

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)

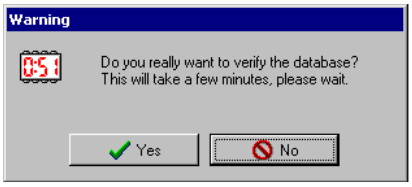
Это меню служит для регистрации новых системных приложений, например, рабочих станций, шлюзов, интерфейсов SmartLink и др., чтобы использовать их при работе с базами данных системы и чтобы установить связь между ними и сервером.



ПРИМЕЧАНИЕ. *Более подробные сведения по установке и регистрации новых приложений в разделе "Установка программного обеспечения" на стр. 9. Перед началом установки новых приложений следует убедиться в наличии правильных серийных номеров, необходимых для установки.*

Проверка баз данных на сервере и рабочей станции

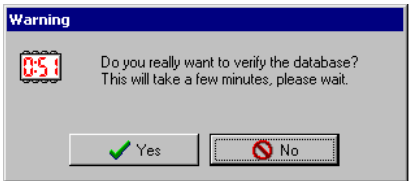
База данных сервера



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®. Более подробная информация приведена в разделе "Проверка целостности базы данных" на стр. 496.*

База данных на рабочей станции



1. На панели инструментов **Options** (Опции) нажать иконку **Workstation full database check** (Полная проверка базы данных на 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®. Более подробная информация приведена в разделе "Проверка целостности базы данных" на стр. 496.*

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 через контроллеры сайтов.

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

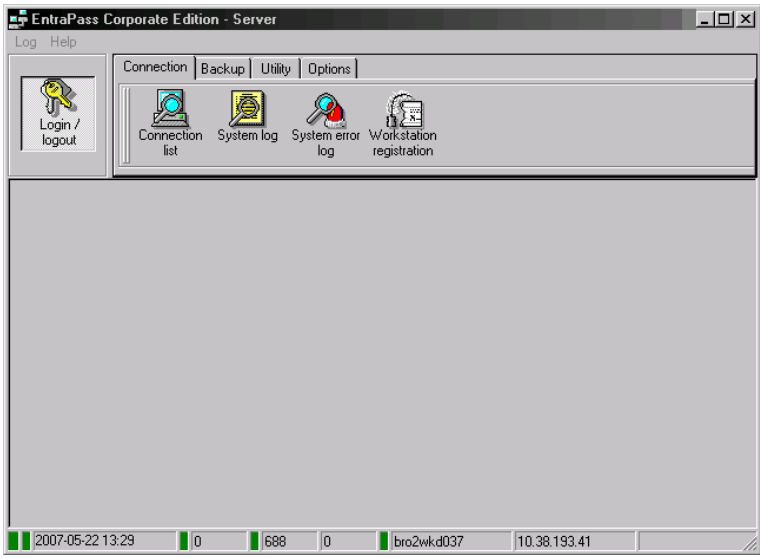
Для того чтобы получить доступ к командам управления сервером EntraPass, необходимо запустить сервер и зарегистрироваться в системе. При входе в систему операторы должны зарегистрироваться. Таким образом они получают доступ к тем разделам меню, которые соответствуют их уровню доступа, а также могут устанавливать 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 Corporate > 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. Чтобы изменить этот пароль, перейдите *в раздел "Описания операторов" на стр. 322.*

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). Более подробная информация приведена в разделе "Описание уровней безопасности" на стр. 326.*



- 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 настройки даты и времени
- 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
- Другой IP-адрес, если используется.

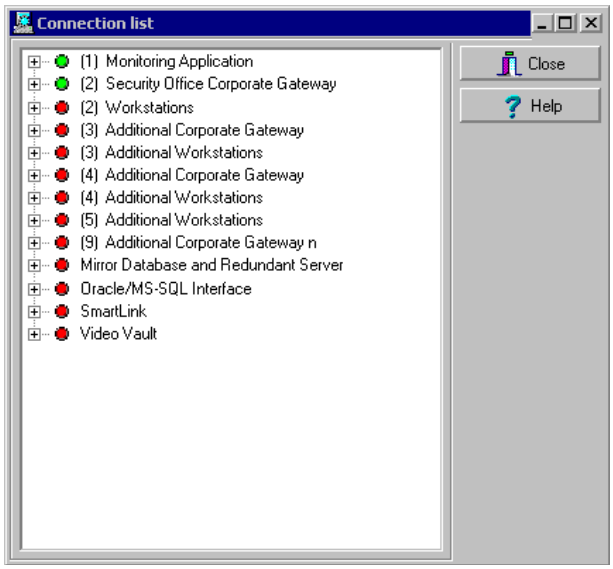
Список соединений сервера (Connection list)

Это меню позволяет операторам просматривать различные списки, отображающие текущее рабочее состояние соединения между сервером EntraPass и подключёнными к нему рабочими станциями.

Просмотр приложений, подсоединённых 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).



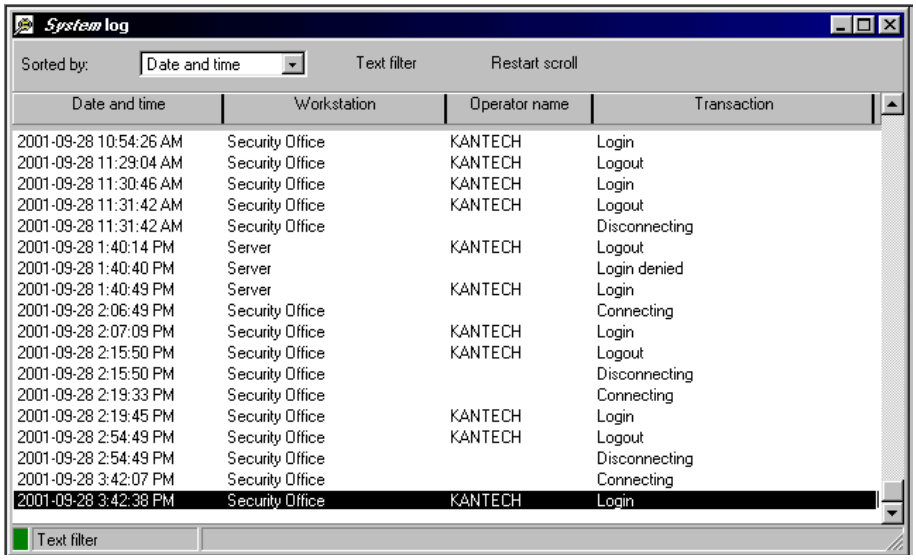
2 Чтобы просмотреть подробные сведения по каждой рабочей станции (коды регистрации, TCP/IP адреса, соединения, сообщения, хранящиеся в буфере, и др.), следует нажать знак плюса (+) рядом с названием рабочей станции.

Просмотр системного журнала (System Log)

В окне System Log отображаются все события по началу и окончанию сеанса работы операторов для всех рабочих станций, описанных в системе. В этих списках отображаются дата и время, название рабочих станций, имена операторов и типы транзакций.

В окне System Log отображаются все события по началу и окончанию сеанса работы операторов для всех рабочих станций, описанных в системе.

1 Для просмотра системного журнала следует нажать иконку **View System Log** (Посмотреть системный журнал).



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 В выпадающем списке **Sorted by** (Способ сортировки) выбрать критерии сортировки, в соответствии с которыми будут отображаться системные события:

- **Date and time** (Дата и время) – это стандартная последовательность поступления событий; при выборе другого способа сортировки стандартная последовательность поступления событий нарушается. Чтобы восстановить стандартную последовательность, нужно снова выбрать способ сортировки по дате и времени. Для этого следует также использовать кнопку “Restart scroll” (Возобновить пролистывание).
- **Operator** (Операторы) – события будут отсортированы по списку в колонке **Operator** в алфавитном порядке.
- **Workstation** (Рабочие станции) – сортировка событий выполняется в алфавитном порядке в соответствии со списком событий в колонке **Workstation**.
- **Text filter** (Текстовый фильтр) – в случае выбора этой опции откроется новое окно. В этом окне следует указать текстовую строку (например, kantech), и система будет отображать только записи, содержащие указанный текст. Чтобы вернуться к нормальному режиму отображения записей, нажать кнопку Text filter.

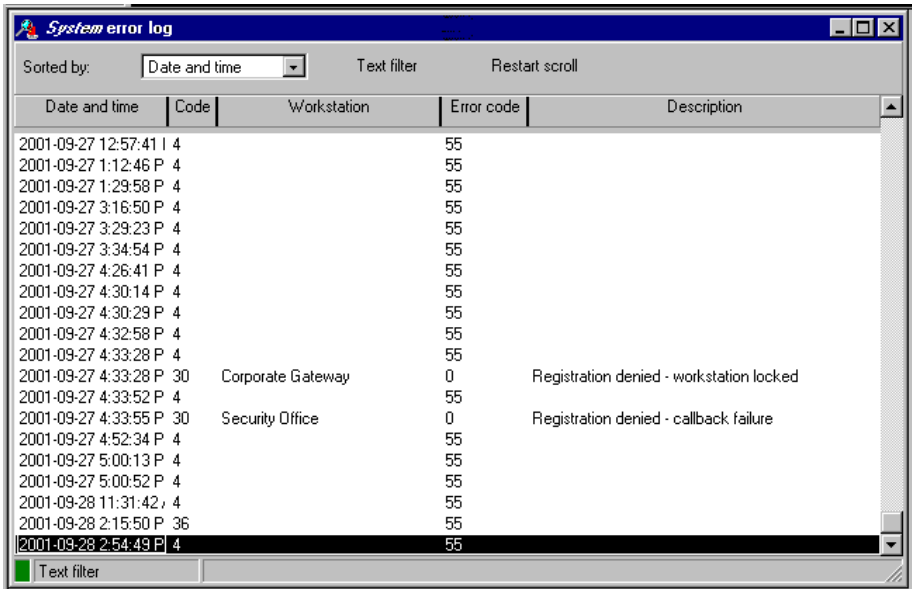
3 По желанию можно изменить цвет фона. Для этого следует вызвать контекстное меню щелчком правой кнопки мыши и выбрать цвет (Color).

4 Кроме того, можно очистить окно. Для этого следует вызвать контекстное меню щелчком правой кнопки мыши и выбрать команду **Clear** (Очистить).

Просмотр системных ошибок (System Errors)

В списках системных ошибок отображаются дата и время, название рабочих станций, номера кодов и описание.

1 Нажать иконку **View system errors** (Показать системные ошибки), чтобы посмотреть все ошибки, возникшие в системе.



2 При нажатии на правую кнопку мыши на экране появляется всплывающее меню, в котором можно вызвать команды для изменения цветового фона или очистки окна ото всех данных.

ПРИМЕЧАНИЕ. *Более подробная информация по регистрации системы приведена в разделе "Установка системы" на стр. 13.*

Резервные копии

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 установлен Сервер 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.

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.*

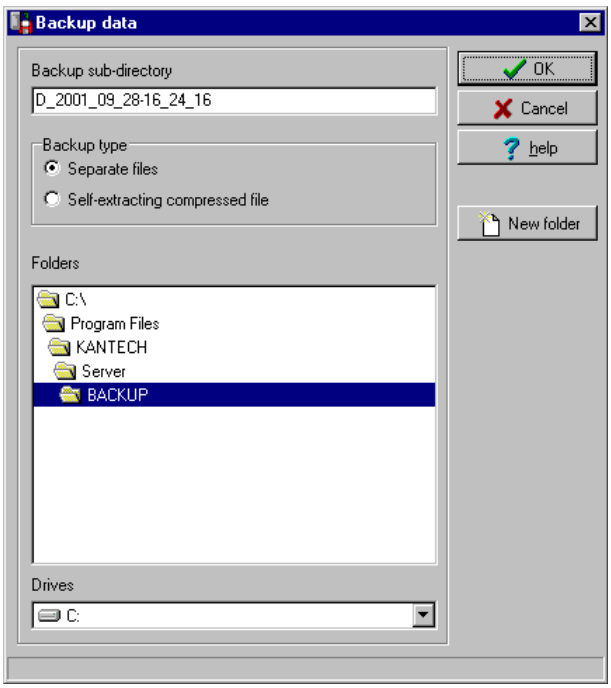
Все системны данные хранятся в файле по ссылке: C:\Program Files\Kantech\ Server_CE\XXXX. Если для создания резервных копий используется программа другого изготовителя, то рекомендуется выполнить резервное копирование всего директория Kantech и вложенных директориев.

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_CE\Data (данные) или Archive (архивы) или Time (учёт рабочего времени). Путь сохранения копии: C:\ProgramFiles\Kantech\Server_CE\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: название программы, используемой 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: название программы, используемой 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 системная кодировка EntraPass совпадает с кодировкой, использованной 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).

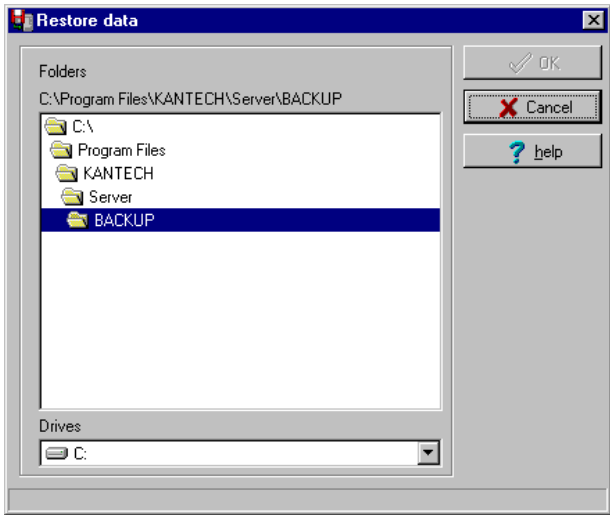
5 Нажать **OK,** чтобы запустить резервное копирование. Ход выполнения процесса копирования отображается в нижней части окна.

ПРИМЕЧАНИЕ. *Чтобы выполнять резервное копирование по расписанию или настроить автоматическое создание резервных копий, можно воспользоваться программой-планировщиком “Backup Scheduler”. Порядок настройки расписания автоматического резервного копирования описан в разделе "Опции системы EntraPass" на стр. 443. 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 всего директория Kantech и вложенных директориев.

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.



ПРИМЕЧАНИЕ. *По умолчанию система/рабочая станция восстанавливает все данные из файла C:\ProgramFiles\Kantech\Server_CE\Backup\ X_YYYY_MM_DD-h_mm_ss, где X – тип данных в папки: C:\Program Files\Kantech\Server_CE\Data (данные) или Archive (архивы) или Time (учёт рабочего времени).*

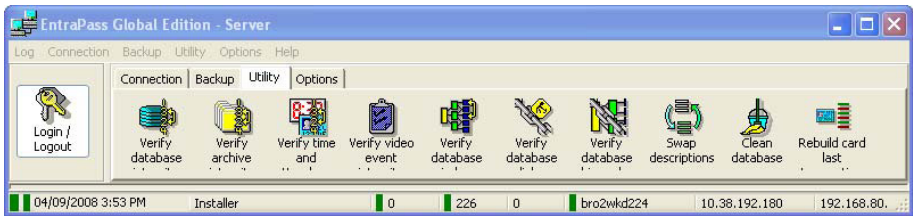
2 Чтобы изменить путь, следует воспользоваться выпадающим списком **Drives**. Нажать **OK**, чтобы запустить процедуру восстановления данных.

ПРИМЕЧАНИЕ. *Рекомендуется повторно загрузить шлюз после восстановления данных:* ***Operation*** *(Операции) >* ***Reload data*** *(Повторная загрузка данных).*

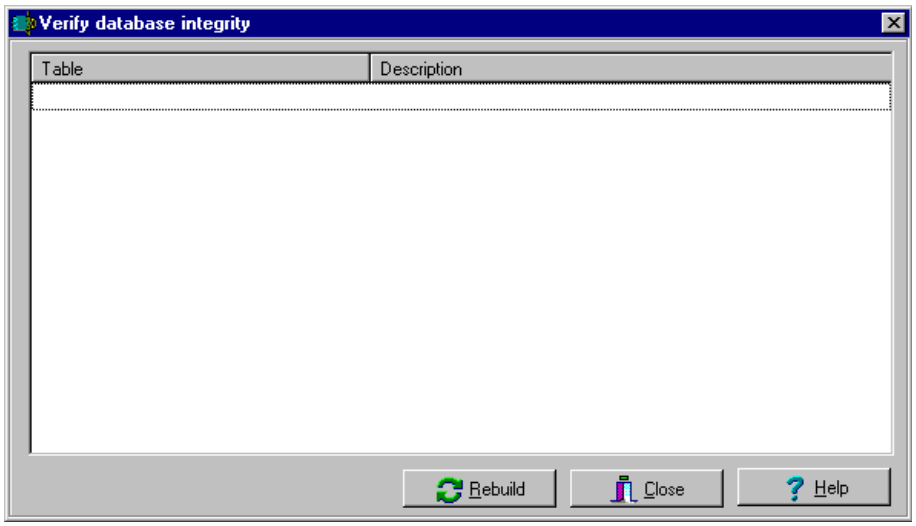
Использование утилит сервера

Это меню предназначено для проверки целостности базы данных системы и для восстановления системных баз данных. Этот раздел меню доступен также и с рабочих станций. Подробнее о системных утилитах смотрите *в разделе "Системные утилиты" на стр. 493.*

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 **Rebuild** (Восстановить). Система автоматически начинает процесс и отображает ход выполнения операции на экране.

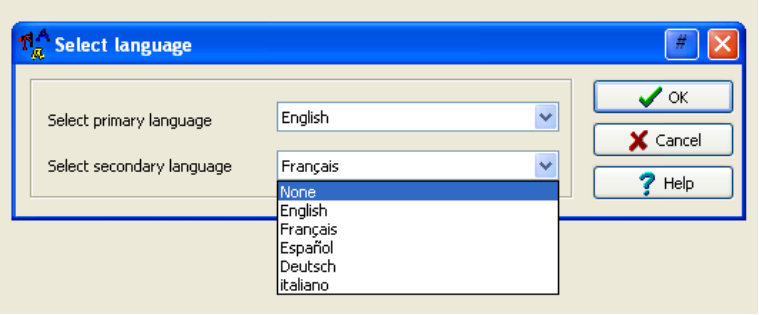
ПРИМЕЧАНИЕ. *В некоторых окна могут быть доступны только кнопки **Yes** (Да) или **No** (Нет) вместо кнопки Rebuild.*

ПРИМЕЧАНИЕ. *При запуске утилиты Clean database (Очистить базу данных), предназначенной для очистки базы данных от ранее удалённых данных, так же появляются кнопки Yes и No.*

Выбор другого языка системы

Для того чтобы индивидуально использовать при работе с системой языки по своему выбору, необходимо сначала указать основной язык, а потом дополнительный.

1 На панели инструментов **Options** (Опции) нажать иконку **Select language** (Выбрать языки).



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 (завершить сеанс работы).

4 Снова войти в систему.

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 сайтов, число контроллеров на каждом сайте 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, управляющего открытием и закрытием до 4-х дверей, а также контроллера сетевой связи KT-NCC.
- **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 настройки Setup.
- **Vocabulary Editor** (Редактор языков). Служит для перевода отображаемого на экране текста на язык, выбранный пользователем.
- **Workstation - Configuration Program** (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 по базам 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.

Database Utility (Утилита 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.

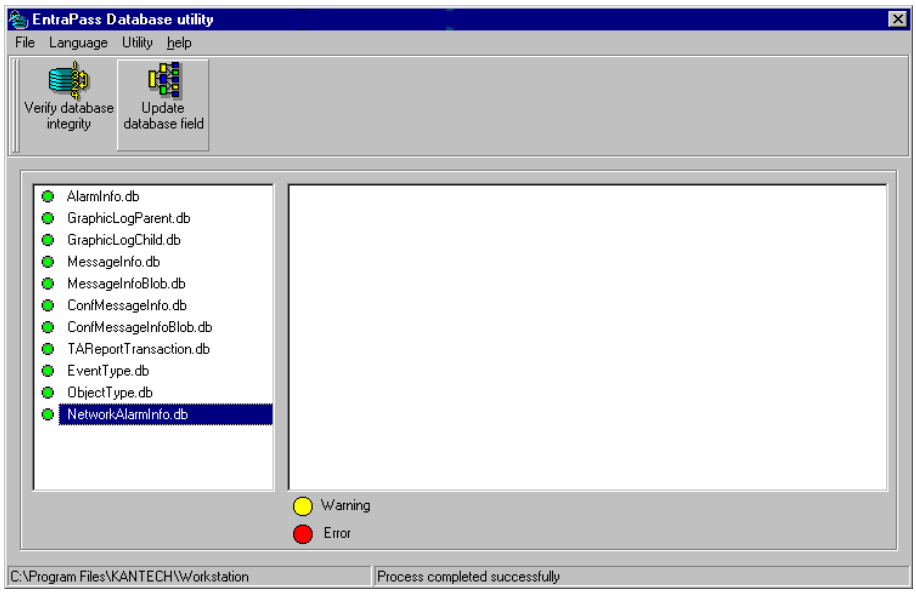
Кроме того, запуск этой программы может понадобиться, например, в случае часто повторяющихся проблем с системой. Процедуру необходимо выполнить и в случае не слишком частого использования системы, поскольку базы данных системы недоступны во время работы с базами данных.

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.

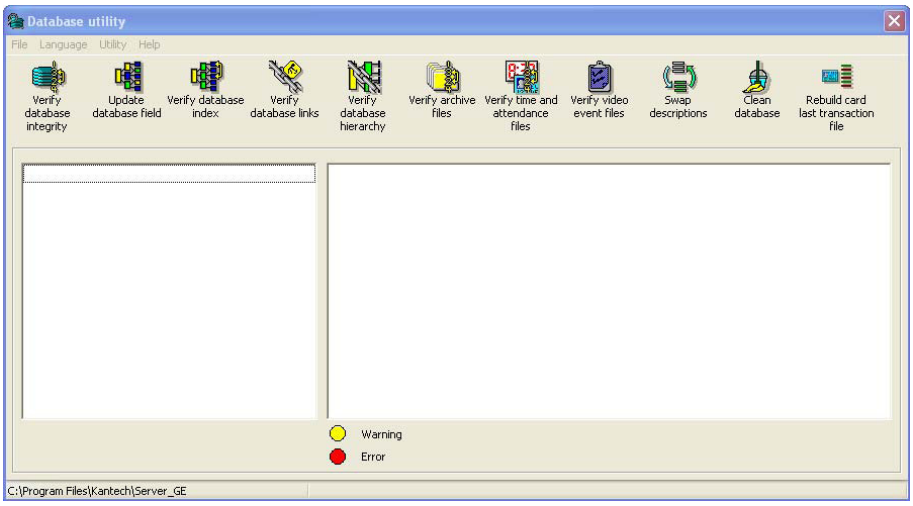
ПРИМЕЧАНИЕ. *Сервер EntraPass должен быть выключен до запуска утилиты.*

Работа с меню Database utility

1 Для запуска утилиты можно использовать иконки под закладкой **Utility** в приложении сервера EntraPass или запустить утилиты через меню **Start** (Пуск) Windows® > **All Programs** (Все программы) > **EntraPass Corporate 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 (Verify Database Integrity)

1 Нажать на панели инструментов кнопку **Verify database integrity** (Проверить целостность базы данных). Сделать выбор, какую проверку делать: быструю или полную.

- **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 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.*

Проверка архивных файлов базы данных (Verify Database Archive Files)

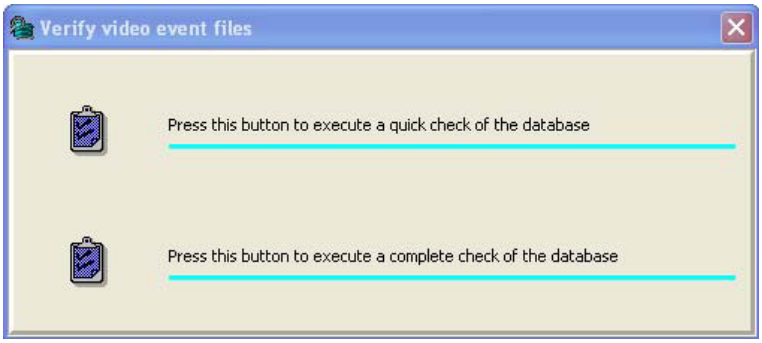
Эта функция используется для проверки архивных файлов. Она назначает новое уникальное порядковое значение для всех исходных индексов архивных файлов.

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 статуса видеосерверов, связанных с активным приложением EntraPass Video Vault
- Мониторинг журналов загрузки видеоданных
- Архивирование видеофрагментов

Видеохранилище EntraPass Video Vault обрабатывает видеофрагменты следующих типов:

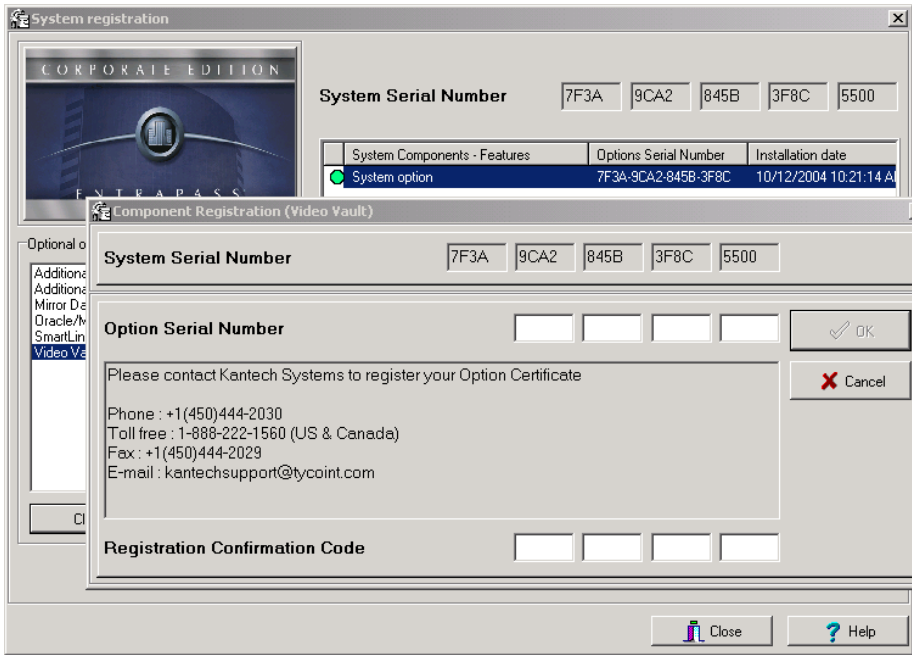
- инициированные автоматически
- инициированные вручную
- инициированные видеосервером
- экспортированные с меткой для архивирования

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 сертификат Option Certificate. Более подробные сведения по установке видеохранилища изложены *в разделе "Добавление дополнительных компонентов/функций" на стр. 12.*

1 В окне EntraPass System Registration (Регистрация системы EntraPass) выбрать пункт EntraPass Video Vault, и нажать кнопку **Click here to install component** (Нажмите для установки компонента).

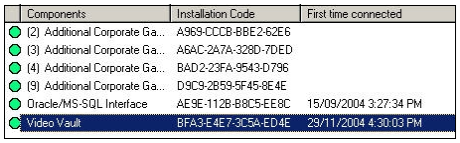


2 Указать серийный номер приложения EntraPass Video Vault в поле **Option Serial Number** (серийный номер указан в сертификате Option Certificate).

3 Ввести код **Registration Confirmation Code** (Код подтверждения регистрации), предоставленный службой обслуживания клиентов Kantech (Kantech Technical Support).

4 Нажать **OK**, чтобы закрыть окно регистрации. После завершения процедуры регистрации приложение EntraPass Video Vault будет добавлено в список компонентов (Components list) в окне System Registration.

5 Чтобы установить видеохранилище EntraPass Video Vault на любой компьютер, удовлетворяющий минимальным требованиям для приложения типа Рабочая станция EntraPass, потребуется код установки (Installation code) и установочный компакт-диск. Подробная информация о требованиях к компьютеру для работы системы изложена *в разделе "Системные требования к компьютеру" на стр. 10.*



Запуск видеохранилища EntraPass Video Vault

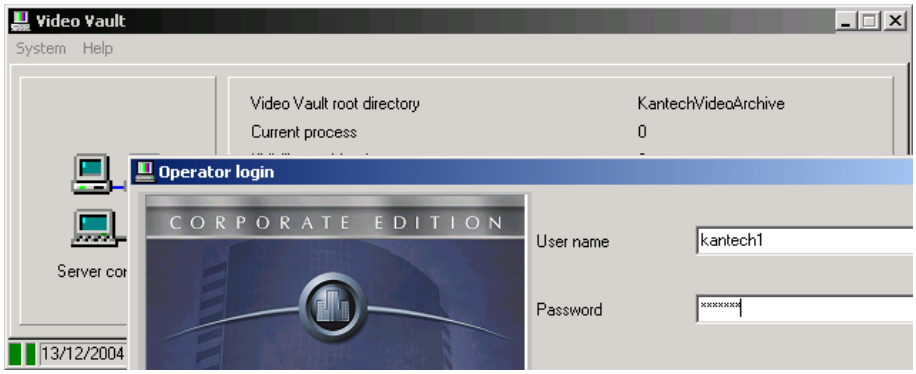
Во время запуска приложение EntraPass Video Vault пытается обратиться к серверу EntraPass. Если запуск выполняется впервые, то может потребоваться ввод IP-адреса сервера (EntraPass Server). Кроме того, необходимо помнить, что запускать видеохранилище следует только после того, как будет запущен сервер.

1 Запустить приложение EntraPass Video Vault, используя контекстное меню на рабочем столе или меню **Start** (Пуск) операционной среды Windows®.

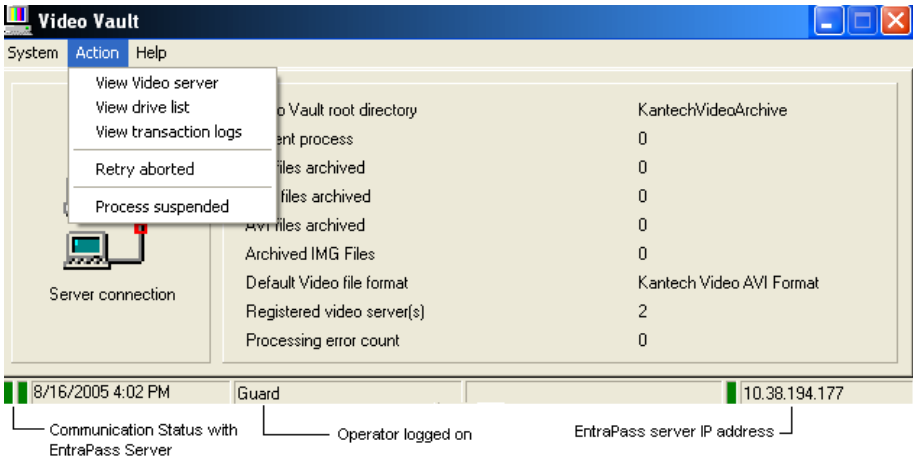
- **Video Vault root directory** (Корневой каталог видеохранилища) – папка, используемая по умолчанию для хранения видеофрагментов. Корневую папку видеохранилища указывают при настройке приложения в среде EntraPass: **EntraPass workstation application** (Приложение типа Рабочая станция) > **Devices** (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 архива.
- **(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.

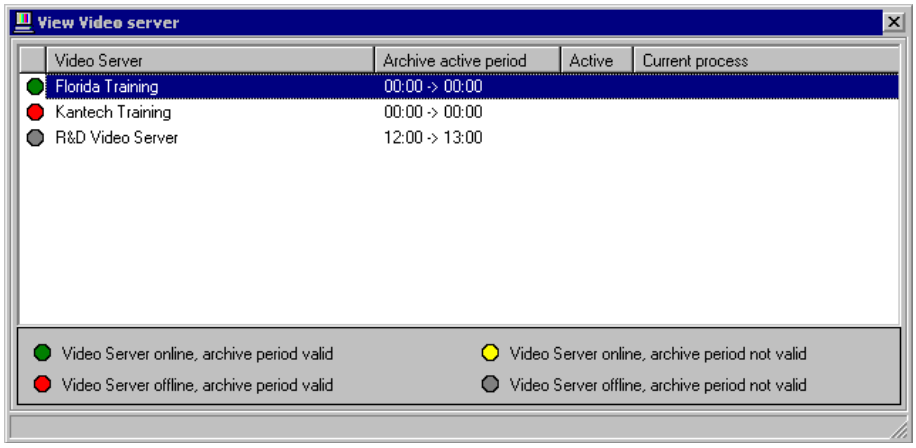


2 Указать имя пользователя в поле **User name** и пароль в поле **Password** для работы с видеохранилищем. Нажать **OK**, чтобы закрыть окно регистрации операторов Operator login. Использование одного и того же имени пользователя и пароля для одновременной регистрации в двух приложениях EntraPass недопустимо! 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.*

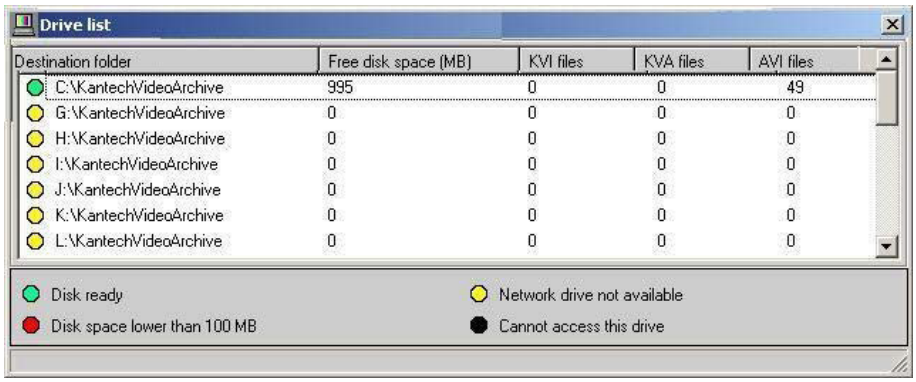
3 Для просмотра списка видеосерверов, связанных с видеохранилищем EntraPass Video Vault, и проверки статусов операций архивирования следует зайти в меню **View Video server** (Посмотреть видеосерверы).



- **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.

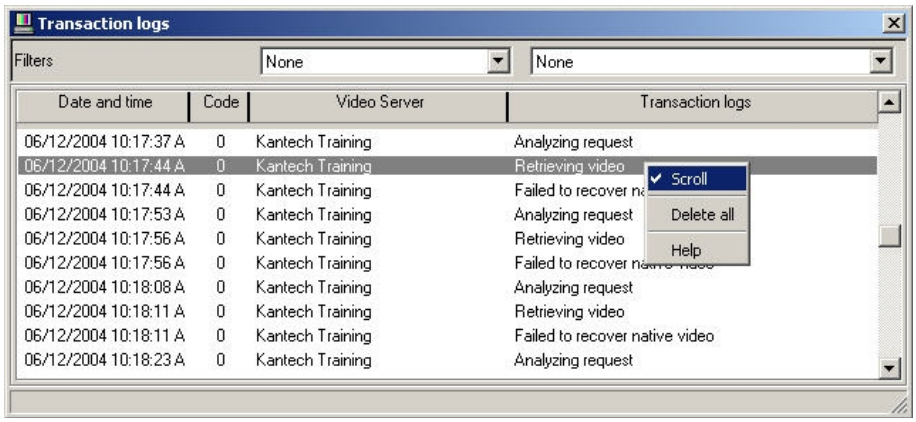
- **Video server online, archive period not valid** (Видеосервер подключён, период архивирования не достоверен).
- **Video server offline, archive period not valid** (Видеосервер отключён, период архивирования не достоверен).

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 видеосервера (Video server).



- 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 транзакций, 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 EntraPass.

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)

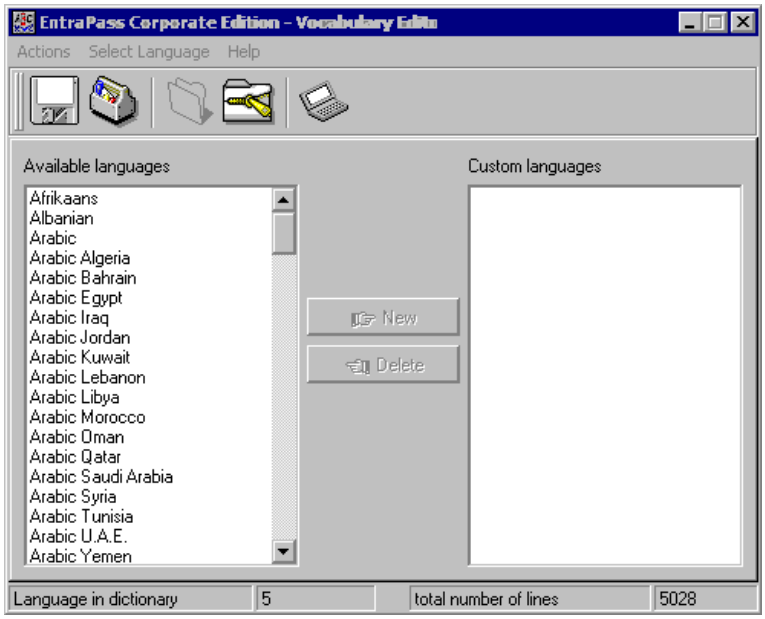
EntraPass Vocabulary Editor является автономной программой. Её можно установить и использовать независимо от других программ EntraPass. Чтобы перевести интерфейс системы на другой язык, необходимо установить программу Vocabulary Editor и перевести при помощи этой программы все слова из базы данных словаря.

ПРИМЕЧАНИЕ. *Для установки редактора языков Vocabulary Editor не требуется приобретение дополнительной лицензии. Её можно запустить из окна настройки Setup. Более подробная информация приведена в разделе "Установка системы" на стр. 13.*

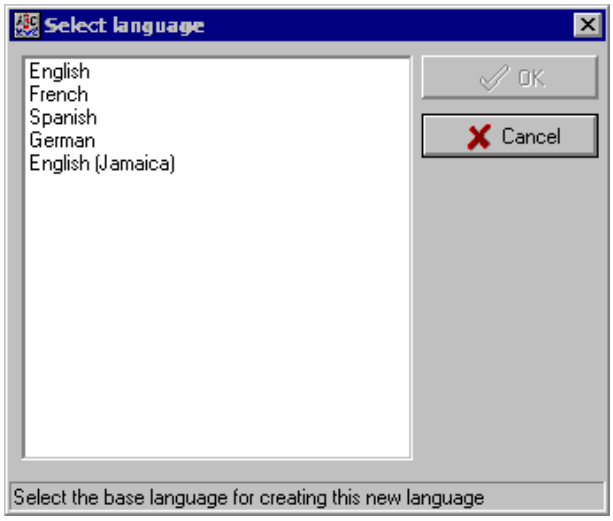
Перевод словаря системы на другой язык

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).

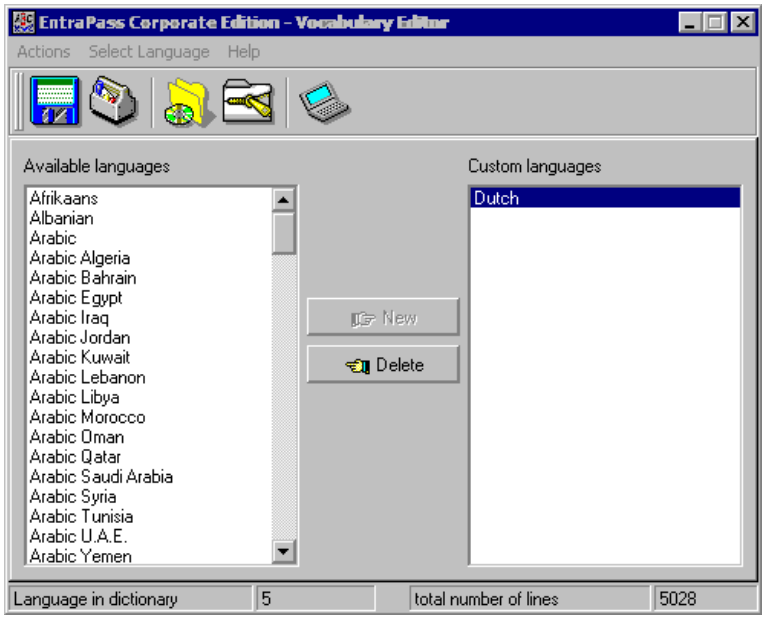
1 Для запуска программы Vocabulary editor перейти в меню **Start** (Пуск) в операционной среде Windows® : нажать **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Corporate Edition** (Система EntraPass) > **Vocabulary Editor** (Редактор языков) > **Vocabulary Editor** (Редактор языков).



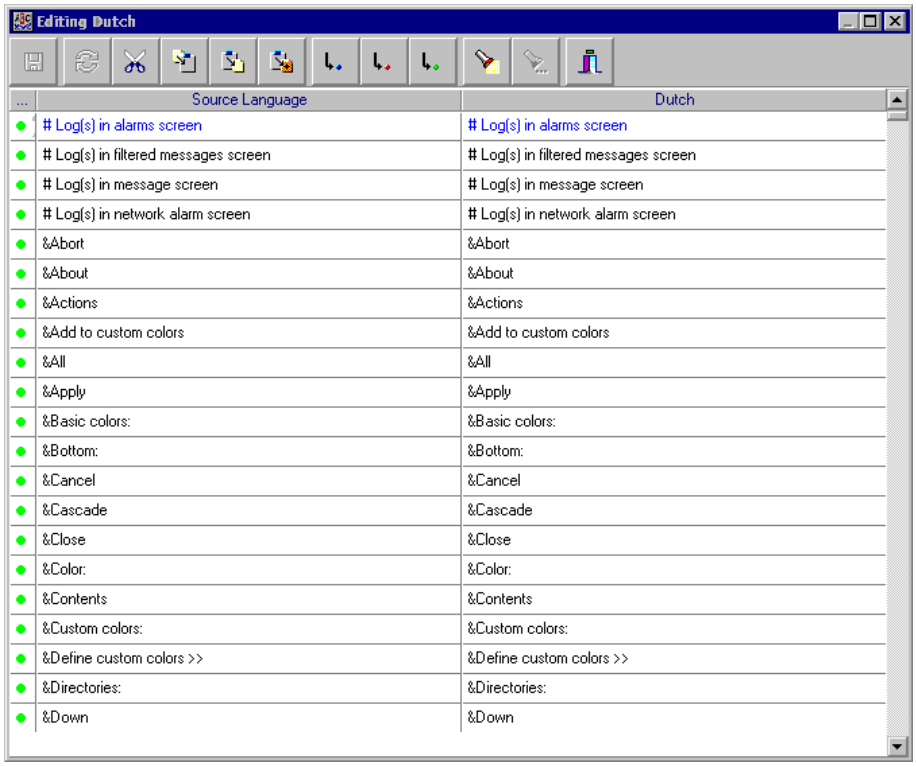
2 В списке доступных языков **Language list** найти название создаваемого языка и нажать кнопку **New** (Создать). Система снова откроет окно **Select language** (Выбор языка).



3 В списке языков найти язык оригинала, с которого будет выполняться перевод, и нажать **OK**. Новый выбранный язык будет отображаться справа в колонке **Custom Languages** (Пользовательские языки). Кнопки **Edit** (Редактировать) и **Delete** (Удалить) станут активными.



4 Чтобы начать перевод словаря программы, нажать кнопку **Edit** (Редактировать). Система выведет на экран 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.

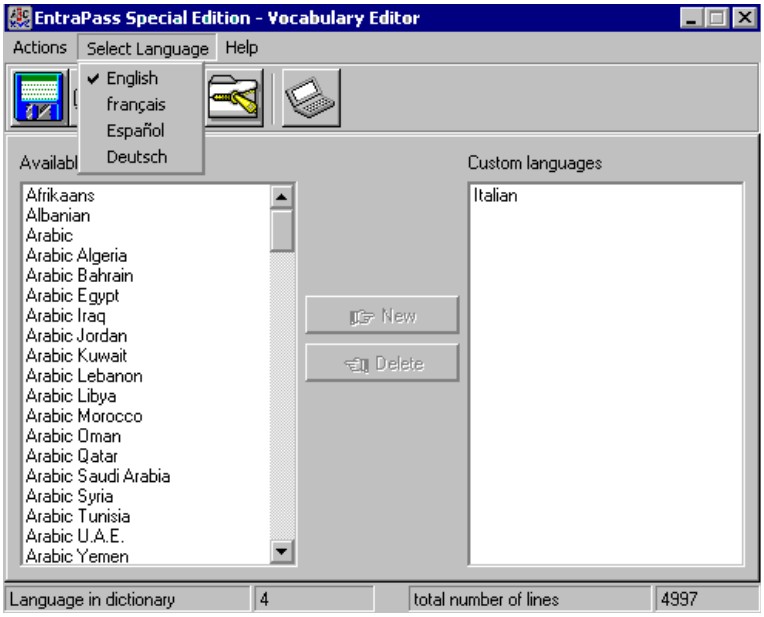
Цветовые коды программы VOCABULARY EDITOR	Описание
зелёный	достоверная текстовая строка
синий/зелёный	новая текстовая строка
красный	устаревшая текстовая строка

- 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

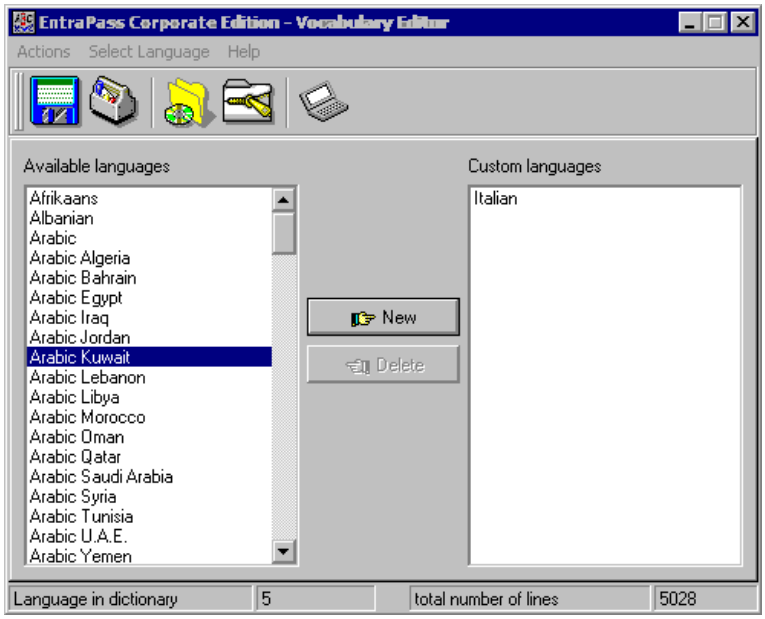
После завершения перевода необходимо интегрировать новый пользовательский словарь в словарь системы, чтобы системные операторы могли пользоваться им.

1 Запустить редактор языков (Vocabulary Editor). Панель инструментов в окне Vocabulary Editor содержит пять кнопок.



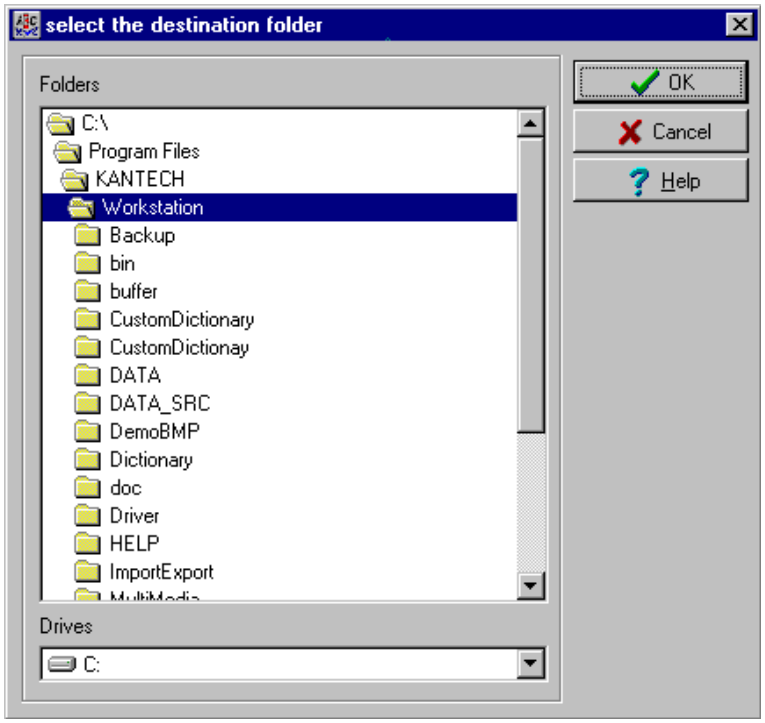
ПРИМЕЧАНИЕ. *Графический интерфейс пользователя (Graphic User Interface) будет отображаться только в одном из следующих пяти языков: английском (English), французском(French), немецком (German), итальянском (Italian) или испанском (Spanish).*

2 Выбрать созданный словарь.



- При необходимости выбрать опцию **Apply changes to the Operational dictionary** (Применить изменения к рабочему словарю) – эту опцию рекомендуется использовать, чтобы проверить внесённые изменения перед обновлением других рабочих станций.
- **Restore the operational vocabulary** (Восстановить рабочий словарь) – эта опция позволяет быстро восстановить использование языков по умолчанию. При помощи самораспаковывающегося файла восстанавливается исходный словарь.
- **Scan dictionary for new entries** (Искать новые записи в словаре) – эта опция полезна, например, в случае обновления программного обеспечения.

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

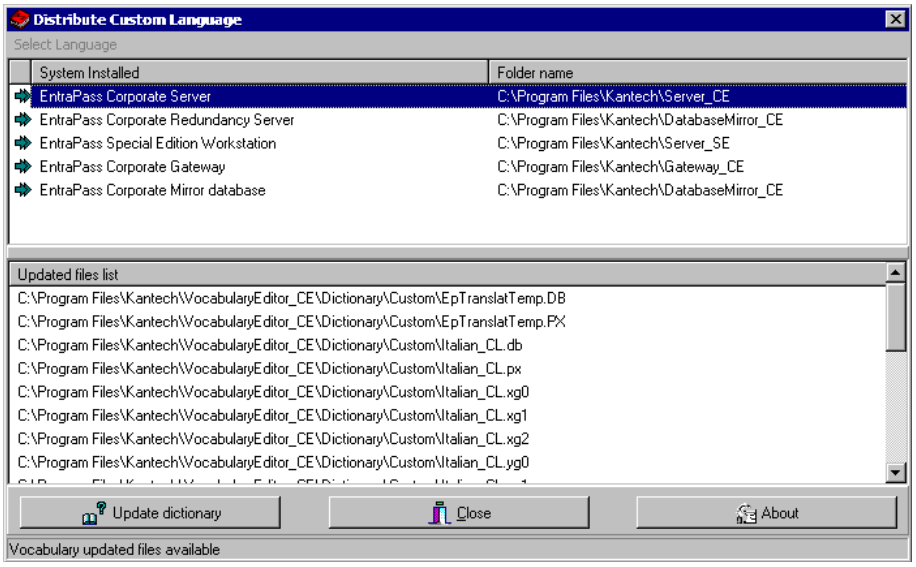
Запускать файл можно только после выхода из программы EntraPass; иначе это действие выполнено не будет. Чтобы обновить словарь системы, сначала необходимо обновить сервер EntraPass. В случае наличия зеркальной базы данных (Mirror database) её необходимо закрыть перед выключением сервера (чтобы она не 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).

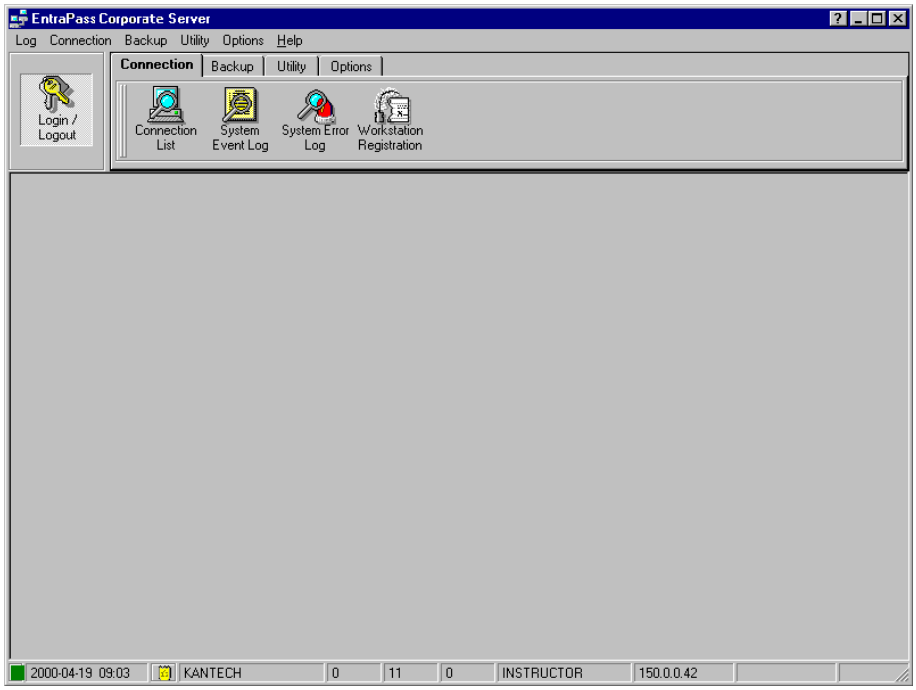
5 Файл **Updatedictionary.exe** необходимо скопировать на каждый компьютер, на котором установлено программное обеспечение EntraPass, и затем запустить его двойным щелчком мыши, чтобы выполнить обновление языков. Перед запуском самораспаковывающегося файла следует обязательно выйти из всех приложений 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.



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). Имя активного компьютера 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 автоматической установки Express Setup

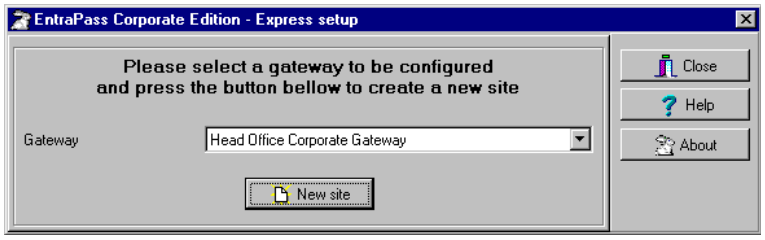
Программа Express Setup (Автоматическая установка) служит для быстрой и удобной настройки конфигурации всех компонентов, имеющих отношение к шлюзу системы, включая тип используемых считывателей карт, число сайтов, имена сайтов, число контроллеров на каждом сайте и др. Например, с помощью этой программы пользователи могут изменить имя двери путём автоматического назначения настроек по умолчанию ко всем реле и входам контроллеров, подсоединённых к указанной двери.

Настройка конфигурации сайта на шлюзе Corporate Gateway при помощи программы Express Setup

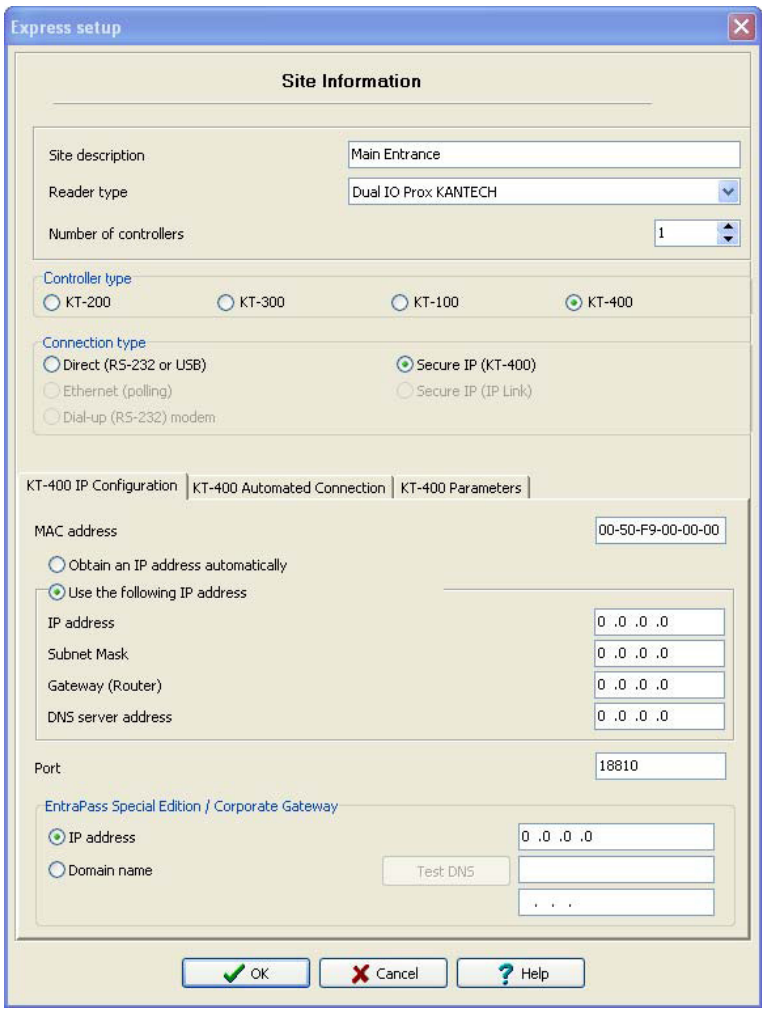
1 В меню Start (Пуск) в операционной среде Windows® войти в меню **All Programs** (Все программы) > **EntraPass Corporate Edition** > **Workstation/Server** (Рабочая станция/Сервер) > **Express Setup** (Автоматическая установка). Для запуска Express Setup из меню можно воспользоваться иконкой Express Setup в окне регистрации или в окне описания 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 сайт).



4 Указать имя сайта в поле **Site description** (Описание сайта), затем указать тип считывателя.

5 Ввести данные в поле **Reader type** (Тип считывателя).

6 Указать число контроллеров в поле **Number of controllers**.

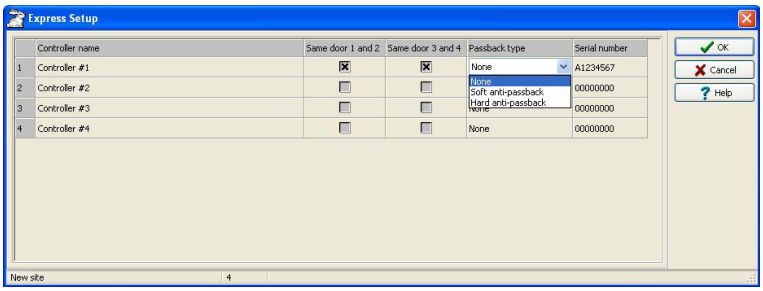
7 Указать тип контроллера для этого сайта в поле **Controller type**.

8 Указать тип соединения в поле **Connection type**. Этот параметр указывает, как осуществляется связь между сайтом и компьютером шлюза. Доступные типы соединений соответствуют выбранному типу контроллера.

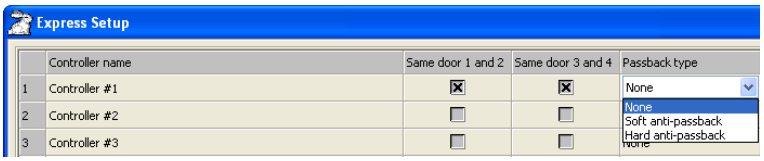
- Отметить флажком поле **Direct (RS-232 or USB),** если сайт объединён с компьютером шлюза и подсоединяется к нему через последовательный порт RS-232. Если используется прямое соединение через последовательный порт, то следует указать его номер (com:), а также скорость обмена данными (как правило, 9600 или 19200). По умолчанию установлено значение 19200.

- Выделить тип соединения **Ethernet (polling)**, если сайт 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 (IP Link)**, если используется этот тип безопасного соединения. Заполнить поля в соответствующих закладках.

9 Нажать **OK**.



ПРИМЕЧАНИЕ. *Необходимо указать минимальные параметры конфигурации контроллеров, связанных с сайтом. Для этого следует назначить имя контроллера в колонке Controller name, указать опции для режима запрета повторного прохода в колонке Passback type и ввести серийный номер контроллера в колонке Serial number (эта колонка появляется только при использовании контроллеров типа KT-100, KT-300 или KT-400).*



ПРИМЕЧАНИЕ. *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.*

10 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.

11 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 (Служебная дверь), 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).

12 Указать серийный номер в колонке **Serial number**, если эта колонка отображается в таблице. Как правило, серийный номер указан на шильдике контроллера (эта информация не указывается для контроллеров типа KT-200).

13 Нажать **OK**. Компоненты, связанные с контроллером и с сайтом, будут созданы и внесены в базу данных сервера. По умолчанию, контроллеры типа KT-200 и KT-300 назначаются для двух дверей, а контроллеры типа KT-400 используются для четырёх дверей, если опции **Same door** не отмечены флажками. Далее в таблице указаны значения параметров по умолчанию, назначаемые для контроллеров различного типа.

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
KT-400	4	4	16	16

Различные варианты использования входных зон в системе проиллюстрированы в таблице:

Входные зоны	Использование	Контроллеры
1	Дверь 1, контакт	все
2	Дверь 1, запрос на выход (REX)	все
3	Дверь 2, контакт	KT-100 и KT-300
4	Дверь 2, запрос на выход (REX)	KT-100 и KT-300
5	Дверь 2, контакт	KT-400
6	Дверь 2, запрос на выход (REX)	KT-400
9	Дверь 2, контакт	KT-200
10	Дверь 2, запрос на выход (REX)	KT-200
9	Дверь 3, контакт	KT-400
10	Дверь 3, запрос на выход (REX)	KT-400
13	Дверь 4, контакт	KT-400
14	Дверь 4, запрос на выход (REX)	KT-400

Варианты использования выходных зон приведены в следующей таблице:

Доп. выходы	Использование	Контроллеры
1	Светодиод (Дверь 1)	KT-100, KT-200 и KT-300
2	Зуммер (Дверь 1)	KT-100, KT-200 и KT-300
3	Светодиод (Дверь 2)	KT-200 и KT-300
4	Зуммер (Дверь 2)	KT-200 и KT-300
1	Выход OUT1 (Дверь 1)	KT-400
2	Выход OUT2 (Дверь 1)	KT-400
3	Светодиод (Дверь 1)	KT-400
4	Зуммер (Дверь 1)	KT-400
5	Выход OUT1 (Дверь 2)	KT-400
6	Выход OUT2 (Дверь 2)	KT-400
7	Светодиод (Дверь 2)	KT-400
8	Зуммер (Дверь 2)	KT-400
9	Выход OUT1 (Дверь 3)	KT-400
10	Выход OUT2 (Дверь 3)	KT-400
11	Светодиод (Дверь 3)	KT-400
12	Зуммер (Дверь 3)	KT-400
13	Выход OUT1 (Дверь 4)	KT-400
14	Выход OUT2 (Дверь 4)	KT-400
15	Светодиод (Дверь 4)	KT-400
16	Зуммер (Дверь 4)	KT-400

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 (Resistor type) - одиночный (KT-100 и KT-300),
- Ожидание второй карты (Waiting for second card) составляет 30 секунд.

Настройка конфигурации контроллера при помощи программы Express Setup

Если после добавления к компонентам системы контроллера сразу выполнить сохранение данных, 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.

1 В окне описания контроллера **Controller** открыть закладку **General** (Общие параметры) и указать тип контроллера в поле **Controller type**.

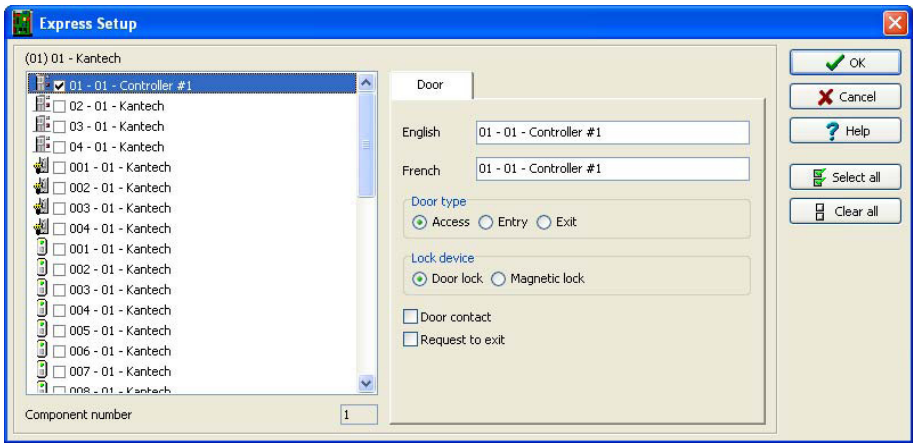
2 Нажать **Save** (Сохранить). На экране появится окно с вопросом: "Do you want to use the Express Setup program to configure the associated devices?" (Хотите ли Вы использовать программу **Express Setup** для настройки соответствующих устройств?). Нажать **Yes** (Да) для продолжения работы с программой **Express Setup.**

- Или нажать **No** (Нет), чтобы вернуться к программе **Express Setup** позже. Программу всегда можно вызвать нажатием иконки.

ПРИМЕЧАНИЕ. *Необходимо помнить, что контроллер KT-300 рассчитан на две двери, а KT-400 на четыре двери.*

3 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.

4 Нажать кнопку **Advanced** (Дополнительно), чтобы описать другие устройства, например, двери, входы, реле и выходы.

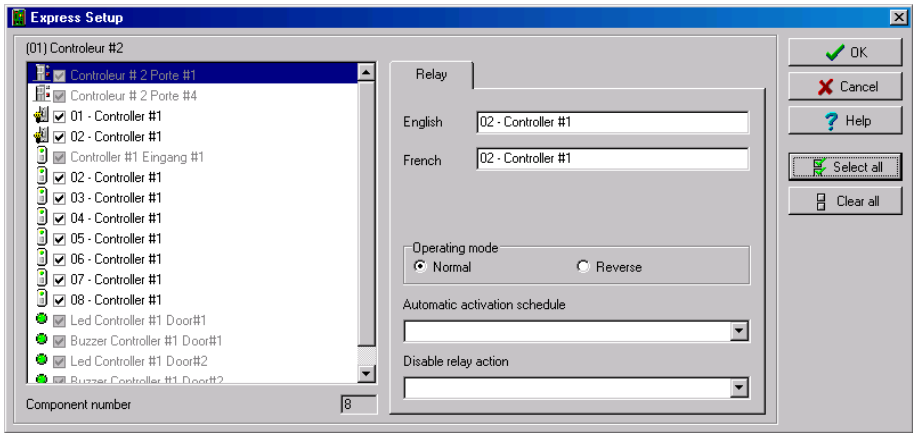


ПРИМЕЧАНИЕ. *Компоненты перечислены в списке на панели слева. Соответствующие закладки отображаются в середине окна. Если выделить компонент, то в справа отображается его имя по умолчанию (на используемых языках), номер и настройки по умолчанию. Чтобы получить доступ к закладке с настройками компонента, 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).*

Порядок описания реле

В настройках реле можно описать 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.



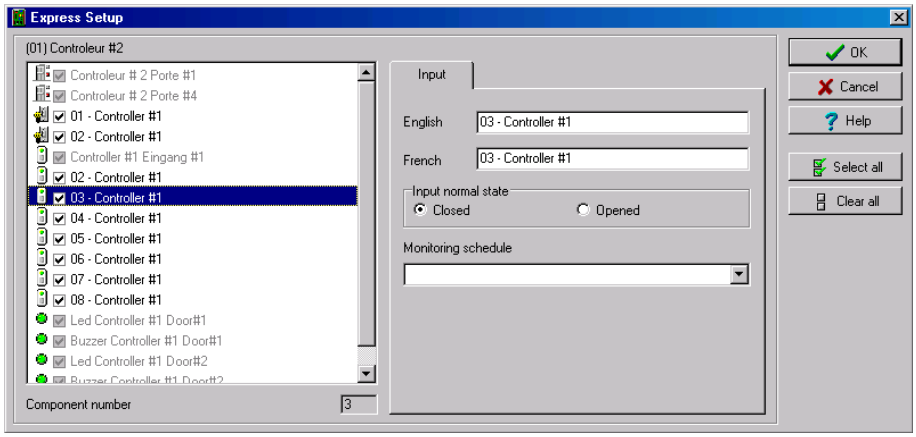
2 Установить нужные опции для режима работы в разделе **Operating mode** и режим активации (**Activation mode**).

3 В выпадающем списке **Automatic activation schedule** (Расписание автоматической активации) выбрать соответствующее расписание.

Порядок описания 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 для каждого входа нормальный статус (**Input Normal State**) и выбрать расписание мониторинга 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 В выпадающем списке **Monitoring schedule** (Расписание мониторинга) выбрать нужную опцию. Чтобы назначить специальное расписание для выделенного входа, следует описать его в меню: Definition (Описания) > Schedule (Расписания).

Порядок описания дополнительных выходов

По умолчанию все выходы настроены следующим образом:

- Дополнительный выход №1 используется как светодиодный индикатор для двери №1 (KT-100, KT-200 и KT-400).
- Дополнительный выход №2 используется как звуковой зуммер для двери №1 (KT-100, KT-200 и KT-400).
- Дополнительный выход №3 используется как светодиодный индикатор для двери №3 (KT-200 и KT-300).
- Дополнительный выход №4 используется как звуковой зуммер для двери №2 (KT-200 и KT-300).
- Дополнительный выход №3 используется как светодиодный индикатор для двери №1 (KT-400).
- Дополнительный выход №4 используется как звуковой зуммер для двери №1 (KT-400).
- Дополнительный выход №7 используется как светодиодный индикатор для двери №2 (KT-400).
- Дополнительный выход №8 используется как звуковой зуммер для двери №2 (KT-400).
- Дополнительный выход №11 используется как светодиодный индикатор для двери №3 (KT-400).
- Дополнительный выход №12 используется как звуковой зуммер для двери №3 (KT-400).
- Дополнительный выход №15 используется как светодиодный индикатор для двери №4 (KT-400).
- Дополнительный выход №16 используется как звуковой зуммер для двери №4 (KT-400).

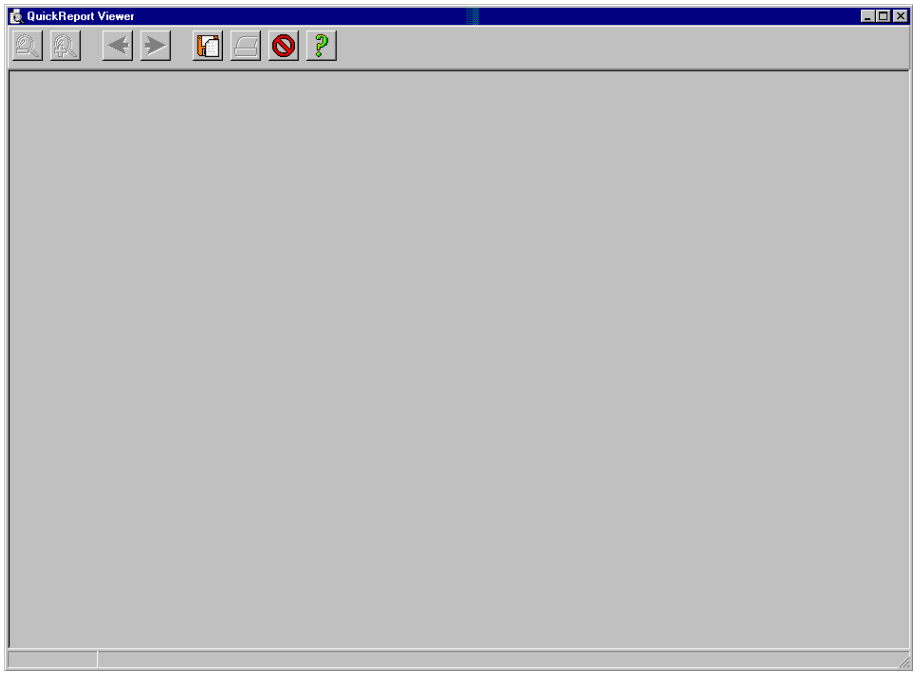
Изменить эти настройки можно при описании параметров контроллера или в соответствующем разделе меню: **Devices** (Устройства) > **Auxiliary Outputs** (Дополнительные выходы).

Программа просмотра быстрых отчётов (Quick Report Viewer)

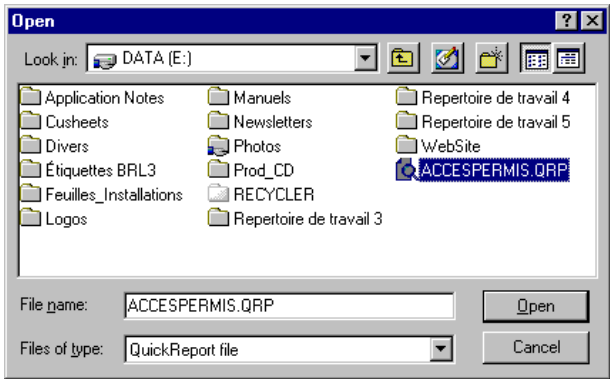
Quick Report Viewer позволяет оператору просматривать предварительно сохранённые отчёты, не запуская EntraPass. Эта программа предназначена для просмотра/отображения/загрузки отчётов, сохранённых во время предварительного просмотра перед выводом на принтер в формате .QRP (так называемых быстрых отчётов). Подробнее порядок обращения и создания отчётов описан *в разделе "Отчёты" на стр. 411.*

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 **Open** (Открыть) предназначена для открытия отчёта, находящегося в любой папке на этом 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.

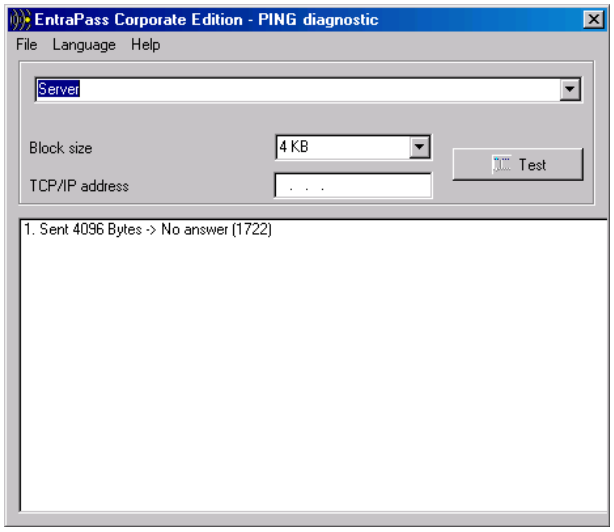
Диагностика по методу "запрос-ответ" (PING Diagnostic)

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). Более подробная информация приведена в разделе "Сервер EntraPass" на стр. 481.*

1 В меню **Start (**Пуск) в операционной среде Windows® войти в меню **All Programs** (Все программы) > **EntraPass Corporate 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 – программа конфигурации

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 Corporate Edition** > **Server** (Сервер) > **Workstation for Configuration** (Настройка конфигурации рабочей станции). Эту программу можно также запустить при помощи контекстного меню на рабочем столе.

Чтобы воспользоваться данной опцией, необходимо сначала создать описания операторов и уровней безопасности для операторов в меню **System** (Системные настройки), а затем описать настройки шлюзов, сайтов, контроллеров в меню **Devices** (Устройства).

ПРИМЕЧАНИЕ. *Более подробная информация изложена в разделе "Установка программного обеспечения" на стр. 9.*

Утилита переноса данных (Migration Utility)

Переход с версии Special Edition к версии Corporate Edition

Система EntraPass позволяет перенести базы данных, используемые в системе EntraPass версии Special Edition, в систему версии Corporate Edition. Перед началом переноса данных настоятельно рекомендуется создать резервную копию базы данных в системе EntraPass Special Edition. Подробнее о резервном копировании базы данных смотрите *в разделе "Резервное копирование" на стр. 487.* Затем следует установить версию EntraPass Corporate Edition. Более подробные сведения по установке изложены *в разделе "Установка системы" на стр. 13.*

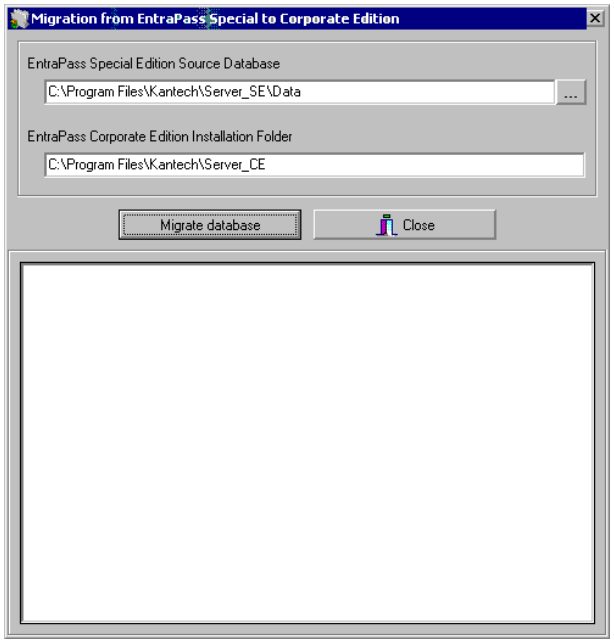
ПРИМЕЧАНИЕ. *Запрещается запуск и регистрация системы EntraPass Corporate Edition на этом этапе.*

Следующим шагом должен стать запуск утилиты переноса данных. После того как данные будут успешно перенесены, следует запустить программное обеспечение EntraPass Corporate Edition и зарегистрировать его при помощи службы технической поддержки Kantech Technical Support. Более подробная информация по обновлению системы EntraPass Special Edition до версии EntraPass Corporate Edition изложена в брошюре *Application Note DN1619 (Указания по применению).*

Порядок переноса базы данных из версии Special в версию Corporate

1 Установить программное обеспечение версии EntraPass Corporate Edition (не запускать его и не регистрировать на этом этапе). Подробные указания по установке программного обеспечения изложены в разделе "Установка программного обеспечения" на стр. 9.

2 Запустить программу Migration Utility из меню **Start** (Пуск) в среде Windows: All Programs (Все программы) > **EntraPass Corporate Edition** > **Server** (Сервер) > **Migration from EntraPass Special Edition**. При этом должно открыться главное окно программы.



3 В окне Migration указать папку, в которой находится база данных старой версии (EntraPass SE).

4 Запустить систему EntraPass Corporate Edition. Зарегистрировать EntraPass Corporate Edition. Для получения регистрации следует обратиться в службу технической поддержки Kantech. Более подробная информация изложена *в разделе "Установка программного обеспечения" на стр. 9.*

Интерфейс шлюза

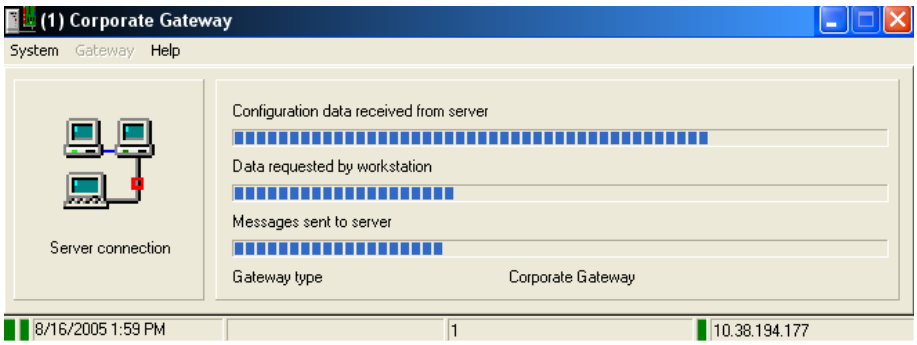
Шлюз представляет собой программный интерфейс, используемый для преобразования данных, полученных с сайтов/шлюзов (которые получают данные с ветвей контроллеров) и передачи их на сервер. Сервер и шлюз используют один протокол для связи, контроллеры и сайт/шлюз также используют один и тот же протокол. 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 ветви), которыми управляют через шлюз. Меню System позволяет операторам входить/выходить из системы, а также повторно загружать шлюз.

Запуск шлюза Gateway

Система предусматривает запуск интерфейса рабочей станции (Workstation) и шлюза (Gateway) вместе 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.



Повторная загрузка данных шлюза Gateway

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). 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 информация, полученные с рабочих станций EntraPass Workstations (любая). Это разные запрашиваемые данные, в частности, запросы статуса (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 Server и передаваемые 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 и использующая интерфейс MS/SQL Interface, будет автоматически обновляться при появлении новых доступных данных в базе данных по картам в системе EntraPass.

ПРИМЕЧАНИЕ. *После запуска и загрузки основного сервера можно запустить зеркальную базу данных и резервный сервер (**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 обеих базах 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.

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 раздел "Системные требования к компьютеру" на стр. 10).*

1. Установить компонент Oracle/MS-SQL Interface (CardGateway), следуя указаниям по установке, *смотрите раздел "Установка системы" на стр. 13* (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 обеспечение 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

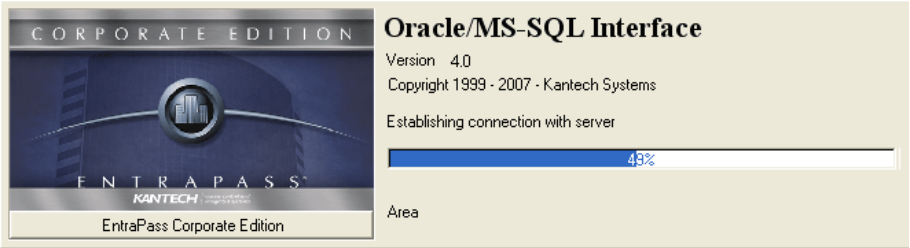
Более подробная информация о том, как настроить конфигурацию программы MS/SQL Interface, чтобы автоматически или вручную создавать базы данных, а также указывать имена пользователей и пароли на сервере MS/SQL / ORACLE Server, изложена *в разделе "Создание баз данных сервера вручную" на стр. 73.*

Запуск программы CardGateway

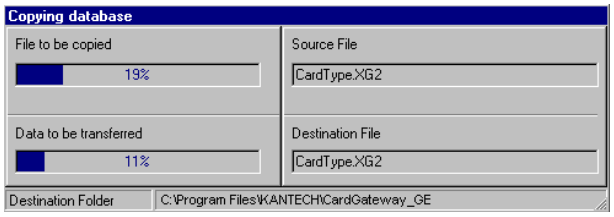
1 Для запуска программы CardGateway следует перейти в меню **Start** (Пуск) в операционной среде Windows® : нажать **Start** (Пуск) > **All Programs** (Все программы) > **EntraPass Corporate Edition** (Система EntraPass) > **MS-SQL and Oracle Interface** (Интерфейс MS-SQL и Oracle) > **MS-SQL and Oracle 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.

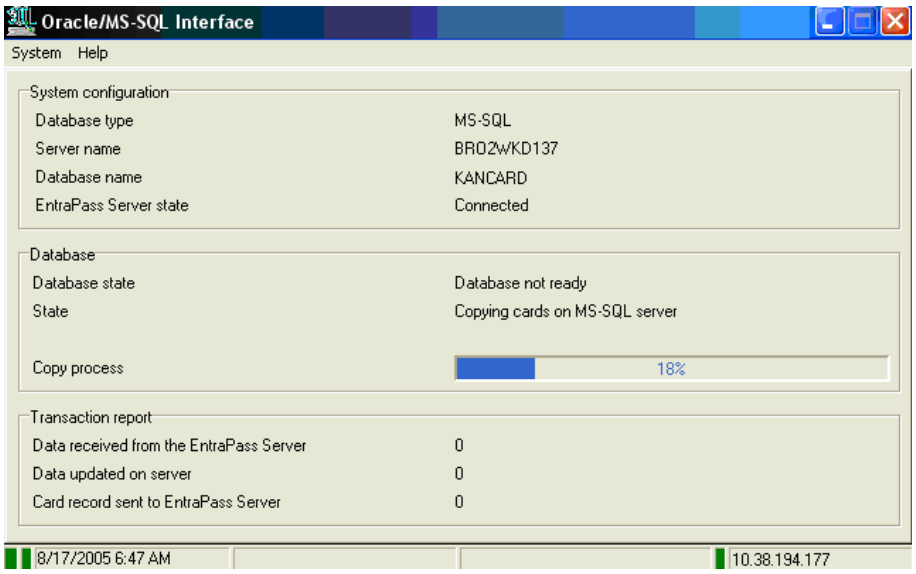


ПРИМЕЧАНИЕ. *Информация и данные, передаваемые с основного сервера EntraPass в базу данных MS/SQL Interface, будут сжаты для более быстрой передачи.*

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)

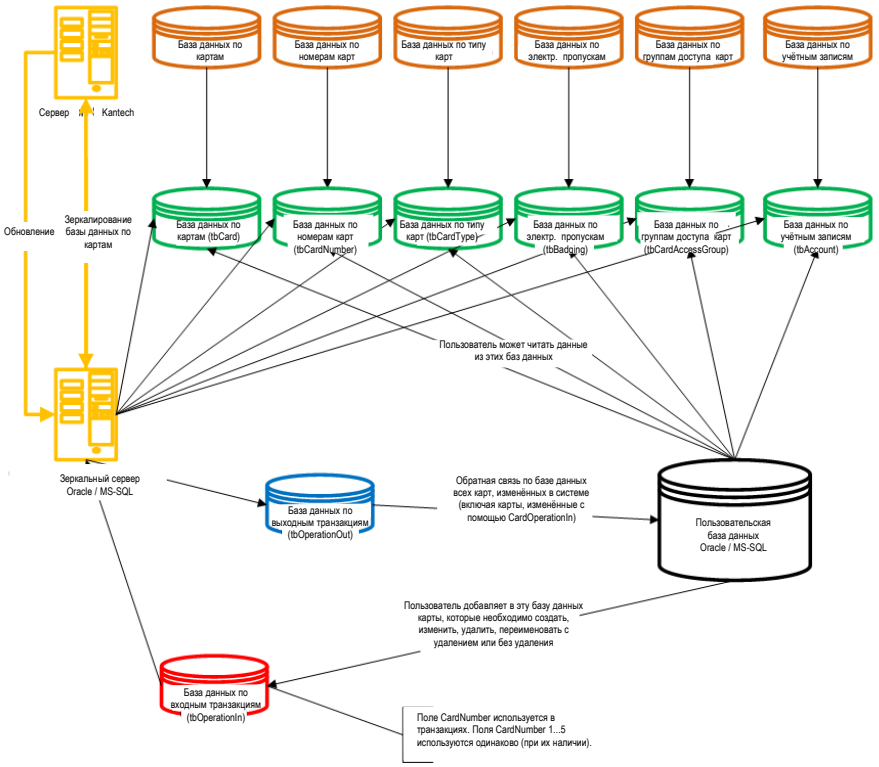
- **Data received from the EntraPass Server** (Данные, полученные с сервера EntraPass). Если данные по картам изменяются на сервере EntraPass (в базе данных), то эта информация также передается в базу данных MS/SQL Interface, где её будет собирать сервер SQL или Oracle. В этом поле отображается число 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.

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 раздел "Системные требования к компьютеру" на стр. 10),
- установочный компакт-диск для приложения SmartLink с серийным номером.

Установка

1. Создать новое приложение в меню Workstation Registration (Регистрация рабочей станции), используя подробные указания *в разделе "Системные требования к компьютеру" на стр. 10.*
2. Установить приложение SmartLink на компьютер *(смотрите раздел "Установка системы" на стр. 13)*.
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. Более подробная информация о создании инструкций приведена *в разделе "Описание команд" на стр. 357.*

Настройка конфигурации приложения типа 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 техническим характеристикам приложения SmartLink (**SmartLink Specifications Manual**).

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.

Повторные загрузки:

Поскольку повторные загрузки шлюза выполняются время от времени и оказывают незначительное влияние на сеть, их влияние на общий трафик сети можно не учитывать.

Функции	Объём, байт	Примечания
Система	256	-
Контроллеры	# * 32	где # = от 0 до 128
Двери	# * 32	где # = от 0 до 256
Реле	# * 16	где # = от 0 до 2048
Входы	# * 16	где # = от 0 до 2048
Дополнительные выходы	# * 16	где # = от 0 до 512
Зоны	# * 32	где # = от 0 до 100
Тревожные разделы	# * 64	где # = от 0 до 100
Группы контроллеров	# * 32	где # = от 0 до 100
Группы дверей	# * 80	где # = от 0 до 100
Группы реле	# * 320	где # = от 0 до 100
Группы входов	# * 320	где # = от 0 до 100
Группы уровней доступа	# * 80	где # = от 0 до 100
Уровни доступа	# * 640	где # = от 0 до 248
Расписания	# * 64	где # = от 0 до 99
Карты	# * 16	где # = от 0 до 32 000
Праздничные дни	# * 64	-
Параметры событий	# * 16	где # = от 0 до 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.

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.

Контроллеры

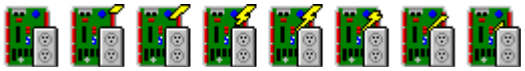
Анимированные иконки контроллеров указывают статус контроллера двери в окне графики (Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)) или в окне “Operation” (Операции).

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:

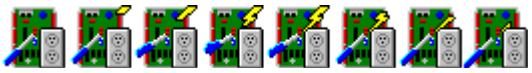
- окно "Operation" (Операции): тревоги, двери, двери лифтов, реле, входы, повторная загрузка данных
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Потеря напряжения в сети питания переменного тока контроллера



Иконка появляется в случае возникновения перебоя в питании контроллера. Отображается в следующих окнах программы:

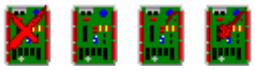
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- меню Operation (Операции) > Controller Reset (Перезагрузка контроллера), Controller AC failure (Сбой в питании контроллера) и Tamper Switch in “alarm” (Тревожный статус противовзломного реле)



Эта иконка отображается, когда возникает сбой в питании контроллера и противовзломное реле переключается в состояние тревоги. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset (Перезагрузка контроллера)

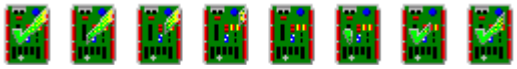
Отсутствует связь с контроллером



Иконка появляется, когда нет связи с контроллером. Отображается в следующих окнах программы:

- Operation (Операции) > Controller Reset (Перезагрузка 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:

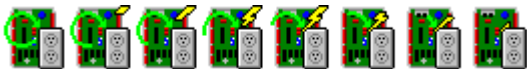
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset (Перезагрузка контроллера)

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, тревожный статус противовзломного реле

Иконка появляется в тех случаях, когда контроллер находится в состоянии перезагрузки и в сети питания отсутствует напряжение, а противовзломное реле перешло в тревожный статус. Отображается в следующих окнах программы:

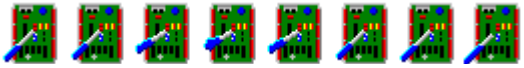
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset (Перезагрузка контроллера)

Контроллер перезагружается, противовзломное реле в статусе тревоги

Эта иконка показывает, что контроллер находится в состоянии перезагрузки, а противовзломное реле перешло в тревожный статус. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset (Перезагрузка контроллера)

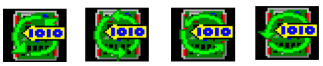
Противовзломное реле контроллера в состоянии тревоги



Иконка показывает, что противовзломное реле имеет статус тревоги. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Controller Reset when the controller tamper is in alarm (Перезагрузка контроллера при тревожном статусе противовзломного реле).

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 (Операции) > Controller Reset (Перезагрузка контроллера)

Двери

Анимированные иконки дверей указывают статус дверей в графическом окне (на рабочем столе) или в окне “Operation” (Операции).

Дверь взломана

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 (Операции) > Door (Двери), Elevator Door (Двери лифтов)

Дверь взломана (считыватель отключён)

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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 открытия двери (Open time). Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > 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 (Операции) > 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 не достоверно. Отображается в следующих окнах программы:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > 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 достоверно, а кроме того, 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 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 (Операции) > Door (Двери)/Elevator Door (Двери лифтов)

Дверь разблокирована по расписанию

Иконка показывает, что дверь разблокирована в соответствии с расписанием. Отображается в следующих окнах программы:

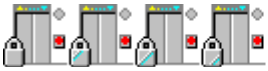
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Door (Двери)/Elevator Door (Двери лифтов)

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 (Операции) > 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 (Операции) > Door (Двери)/Elevator Door (Двери лифтов)

Реле

Анимированные иконки реле указывают статус реле в графическом окне (на рабочем столе) или в окне “Operation” (Операции).

Реле активировано событием

Эта иконка показывает, что срабатывание реле вызвано событием. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Relay (Реле)

Реле временно активировано событием

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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > 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 (Операции) > Relay (Реле)

Реле деактивировано

Иконка показывает, что реле деактивировано. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Relay (Реле)

Статус реле неизвестен

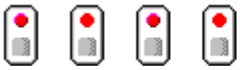
Иконка показывает, что статус реле ещё неизвестен. Отображается в следующих окнах:

- 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” (Операции).

Вход с тревожным статусом – 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 (Операции) > Input (Входы)

Вход с тревожным статусом – шунтирован (отключён от мониторинга) оператором

Иконка показывает, что вход находится в состоянии тревоги и отключён от мониторинга (шунтирован) оператором. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с тревожным статусом – контролируется

Иконка показывает, что вход находится в состоянии тревоги, и расписание мониторинга входа достоверно. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с тревожным статусом – контролируется оператором

Иконка показывает, что вход находится в состоянии тревоги и контролируется оператором (постоянный мониторинг). Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с нормальным статусом – не контролируется

Иконка показывает, что вход находится в нормальном состоянии, а расписание мониторинга входа не достоверно. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с нормальным статусом – шунтирован (отключён от мониторинга) оператором

Иконка показывает, что вход находится в нормальном состоянии и отключён от мониторинга (шунтирован) оператором. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с нормальным статусом – контролируется

Иконка показывает, что вход находится в нормальном состоянии, и расписание мониторинга входа достоверно. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Вход с нормальным статусом – контролируется оператором

Иконка показывает, что вход находится в нормальном состоянии и контролируется оператором (постоянный мониторинг). Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Input (Входы)

Статус входа неизвестен

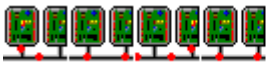
Эта анимированная иконка появляется на рабочем столе “Graphic” (Графические схемы), если статус входа ещё не определён.

Сайты и шлюзы

Анимированные иконки этого типа указывают статус сайта или шлюза в окне графических схем (на рабочем столе) или в окне “Operation” (Операции).

Сайт контроллера:

Статус сайта пока неизвестен



Иконка появляется в том случае, когда статус сайта контроллера ещё неизвестен. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Сайт контроллера подключён

Иконка показывает, что сайт подключён и связь в порядке. Отображается в следующих окнах:

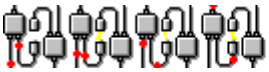
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Сайт контроллера подключён и находится в состоянии повторной загрузки данных (Reload Data)

Иконка показывает, что сайт подключён и имеет статус повторной загрузки данных. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Сайт контроллера – нет связи



Иконка показывает, что сайт не подключён, и с ним нет связи. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Шлюз:

Шлюз – нет связи

Иконка показывает, что со шлюзом нет связи. Отображается в следующих окнах:

- окно "Operation" (Операции): 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:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- окно "Operation" (Операции): двери, двери лифтов, реле, входы, повторная загрузка данных шлюза

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" (Операции): повторная загрузка данных шлюза
- 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:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Проблемы со шлюзом

Иконка появляется, когда нет связи со шлюзом. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Проблемы со шлюзом во время повторной загрузки данных

Иконка показывает, что во время повторной загрузки данных отсутствует связь со шлюзом. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Шлюз (программный интерфейс шлюза):

Шлюз в норме – есть связь

Иконка показывает, что связь со шлюзом в порядке. Отображается в следующих окнах:

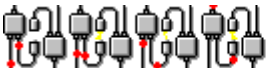
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Шлюз в состоянии повторной загрузки данных (Reload Data)

Иконка показывает, что на шлюзе выполняется повторная загрузка данных. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Шлюз – нет связи



Иконка показывает, что со шлюзом нет связи. Отображается в следующих окнах:

- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)
- Operation (Операции) > Reload data (Повторная загрузка данных)

Приложения EntraPass

Статус 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" (Операции): тревоги, двери, двери лифтов, реле, входы, повторная загрузка данных шлюза

Прочее

Инициализация базы данных

Иконка появляется, когда рабочая станция инициализирует 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.

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, 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, 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, двери, двери лифтов, реле, входы, повторная загрузка данных шлюза
- Desktop (Рабочие столы) > Graphic desktop (Рабочий стол графических схем)

Индекс

A

Access Levels
  Administrator 57
  Create groups 306
Access levels
  Arming 139
  Bad 137
Acknowledging Alarms
  Acknowledge schedule 352
  Alarm sound 452
  Automatic 323
  Set priority 352
Acknowledging alarms
  Definition and purpose 397
  Using the alarm message box 67
Additional system components 25
Advanced schedule capability 458
Alarm message box 67
Alarm Sound 452
Animated Icons
  Controllers 538
  Doors 540
  Inputs 546
  Others 551
  Site and gateway 548
  Relays 544
Assign picture from file 242
Authentication 62
Auto Acknowledge 323
Auto-connection 62
Automatic backup
  Backup scheduler 475

B

Background
  Live video 200
  Web page 200
Backup 487
Backup scheduler 472
  Service login information 460
Badging 3
  Get picture from file 242
  MCI 241
  Paste picture 242
  Video images 241
Bandwidth
  Video 455, 468
Buttons
  Cancel 48
  Enable Animation 49, 205
  Enable Graphic 49, 205
  OK 49
  Select All 205
  Unselect All 49, 205

C

Card
  Card number 232, 233
  Creation date 233
  Lost 233
  Modification date 233
  Modifications count 233
  Stolen 233
  trace 233
Card access group definition 283
Card format
  Hard reset 445
  Multiple card format 445
Card Information fields 231
Card last transaction files
  Rebuild 498
Card management
  WebStation 469
Card number
  Trace 233
Card type definition 286
Card use reports
  Schedule mode 421
  WebStation 420
CardGateway
  Mirror Database and Redundant Server 2, 74
  Oracle/MS-SQL Interface 70
Cards
  Assign a card access group 238
  Assign a picture 241
  Assign access levels to cardholders 238
  Card format 444
  Change card format 444
  Copy to visitor card 231
  Create a day pass 287
  Create access level groups 283
  Create card types 286
  Default card format 444
  Delete when expired 239
  Enhanced user management 469
  Information fields 231

Keep picture on desktop 379
Last transactions 281
Modification date 231
Modifications count 231
Number 230
Print a list of cards 277
Show cardholder information with picture 66
Start date 239
State 240
Trace 240
Use count options 241
User name 230, 232
Validate Card Access 275
Wait for keypad 239
Change card format
Decimal 444
Hexadecimal 445
Octal 444
Clean Database 498
Clear alarm messages 65, 67
Communication timing 92
Components physical address 329
Concurrent logins
Operator 323
Configure system devices 59
Configuring
Mirror Database and Redundant Server 74
Oracle/MS-SQL Interface 70
Controller
Definition 101
Express Setup 519
Controller local area
KT-400 123
Controller's Loop baud rate 515
Controller's loop baud rate 93
Controllers 59
Animated icons 538
Create groups 302
Reset 213
Status (graphic view) 315
Corporate 1000
Corporate Gateway
Configure 87
Corporate gateway
Express Setup 514
Creation date
Card 233
Credentials
Enhanced user management 469
CSV files 68
CSV Import/Export 291
Create patterns 292
Exporting procedure 293
Importing procedure 296

D

Database
Checking 479
Logical components (view) 367
Structure 367
Utility program
Rebuild card last transaction files 498
Swap descriptions 498
Verify Database hierarchy 497
Verify Database links 497
Verify Time and Attendance files 497
Verify video event files 498
Database integrity
Verify 494
Database Output Type 414
Database Status 318
Day Pass Definition 287
Define E-mail Parameters 428
Desktop
Alarms 391
Filtered messages 386
Desktops
Alarms desktop
Acknowledge 394
Delete log 395, 405
Display graphic screen 402
Display instruction screen 400
Flag 394
Print log 395, 404
Purge deleted log 395
Historical reports 387
Messages desktop
Auto-rescroll delay 380
Background color 380
Delete all 381
Display events in bold 379
Display last message on top 379
Display message (in full) 379
Display toolbar 379
Keep card picture 379
Manual properties 379
Message type 378
Multi-line 378
Play archived video recordings 390
Send to back 383
Show icons 378
View parent 382

Network alarms
Desktop 404
Diagnostic on Network (Server) 459
Dial-up modem 97
Directory 414
Disable Door Reader 219, 223
Disable video 63
Door
Return to schedule 217, 220, 224
Door contact 132
Door Group 303
Doors 59
Animated icons 540
Create groups 303
Door contact 132
Door unlock reading 132
Elevator cab 128
Lock mode 128
Open time 129
Pre-alarm on door opened too long 132
Re-lock on door closing 133
Re-lock on door opening 133
REX contact 133
Unlock on REX 133
Unlock time 129
Driver
Corporate 1000 444
Duress options 123

E

Editing system components 28
Elevator Control
Create floor groups 307
Create floors 197
Elevator cab (door) 128
Elevator control
REB-8s 106
Select cab for floor group activation 146
Unlock schedules (elevator floors) 135
Elevator controllers 105
e-mail
options 68
Enable Door Reader 219, 222
Enable/Disable Card Readers 217
Enable/Disable card readers 217, 220
Encryption 62
Enhanced user management
Credentials 469
Ethernet (polling) 516
Ethernet polling 96
Event buffer
Controller 100
Events
Acknowledge schedule 352
Color 352
Deleting and restoring associations 354
Display (schedule) 352
Instructions (assign to events) 352
Parameter definition 350
Print parameters 355
Print schedule 352
Set priority 352
Viewing associations 353
Expansion Modules
Configuring 115
Expired 240
Express Setup 514
Configuring a corporate gateway 514
Controller 519

F

Fail-Soft 366, 379
Floor
Confirmation 109
Definition 197
Group 307

G

Gateway
Animated icons 548
Hard reset 208
Gateway data reload 208
Graphic
Definition 198
Graphic Status (controller view) 315
Graphics
See also Animated Icons 537
Groups
Access levels 306
Controllers 302
Doors 303
Floors 307
Inputs 305
Relays 304

H

Hard anti-passback 123, 129

Hard reset
  Card format 445
Hardware
  Definition 91
Historical Reports
  Automatic filename 425
  Automatic report schedule screen 421
  Destination 425
  Filter mode 417
  Output process 423
  Output type 422
  Preview 440
  Report language 425
  Schedule mode 421
  Selected components 417

Historical reports 415
  Desktop 387
  State 388
  WebStation 416
Holiday definition 203
Host modem definition 87

I

Icons, see Animated Icons 537
Import/Export 291
Inputs
  Animated icons 546
  Continuous supervision 226
  Create groups 305
  Group 305
  Monitoring schedule 144
  Normal 226
  Normal condition 144
Installation 9
Installing the system 13
Instructions
  Assign to events 352
  Definition 357
Interlock options
  Mantrap 134

K

Kantech IP Link 93
Keypad escape key 104
KT Controllers 102
KT-100 103
KT-100 controller 104
KT-200
  Configuring 105
  Expansion devices 105
KT-2252 elevator controllers 105
  Program 106
KT-300 103
KT-400
  Configuring 113
  Controller local area 123
  Defining controller local areas 124
  Expansion modules 115
KT-400 Ethernet Four Door Controller 93
KT-MOD-INP16 115
KT-MOD-OUT16 115
KT-MOD-REL8 115

L

Language
  Modification 447
Language (operator) 323
Lock/Unlock
  Door 217
  Door temporarily 217
  Elevator door 220
  Elevator door temporarily 220
Login
  Name 323
  Schedule 324
Logout on idle 62
Lost
  Card 233

M

Mantrap 134
  Interlock options 134
Manual Operations
  Disable reader 217, 220
  Enable readers 217, 220
  Lock door 217
  Lock elevator door 220
  Temporarily lock door 217, 220
  Temporarily unlock door 217, 220
  Unlock doors 217, 220
Master Password 446
  New 446
  Verify 446
Messages
  Desktop 377
Messages Definition (Filters) 363
Mirror Database and Redundant Server

CardGateway 2, 74
Configuring 74
Modem dial-up 97
MS-SQL Interface
See Oracle/MS-SQL Interface 70
Multimedia Devices 443, 452
Alarm sound 452
Signature capture 454
Video options 453
Muster report
Service login information 460

N

Network alarms
Desktop 404

Normal condition 144

O

Online help 5
Operator
Concurrent logins 323
WebStation login 323
Operator definition 322
Operators
Allow login on server 328
Bypass workstation message filter 323
Language selection 323
Login name 323
Login Restrictions 328
Operator login schedule 324
Password 323
Oracle/MS-SQL Interface
CardGateway 70
Configuring 70
Output definition 148
Output filename 414
Outputs
Activation period 149
Associating door events to auxiliary outputs 149
Flash 150
Flash timed 150
Operating mode 149
Steady 150
Steady timed 149

P

Passback
Option 240
Password
Change master password 446
Operator 323
Pending 240
Picture 242
PIN
Duplicate PIN process 445
PIN number 104, 239
PING Diagnostic Program 524
Port number 516
Power supervision schedule 103
Print a log 395, 404
Print cards 277
Print Event Parameters 355
Printer, see Log printer 448

Q

Quick report viewer 522

R

REB-8 Elevator controllers
Program 108
REB-8 relay expansion board modules 105
Redundancy server address 76
Redundant Server
CardGateway Limitations 74
See Mirror Database and Redundant Server 74
Redundant server
CardGateway 457
System parameters 457
Register the system 22
Registration
see Workstation registration 478
Server 478
Relay
Activate 224
Deactivate 224
Temporarily activate 224
Relay Group 304
Relays 59
Activation schedule 142
Animated icons 544
Create groups 304
Operation mode 142
Temporary activation timer 142
Remote modem delay 100
Reports

WebStation 416, 420
Reset, see Controllers 213
REX 105
REX (Request to EXit) 133
REX contact 133
REX options 133
rpf files 68
RS-232 serial port 92, 515

S

Schedule definition 194
Schedules
Acknowledge schedule 352
Days 195
End time 195
Login schedule (operators) 324
Monitoring schedule (inputs) 144
Printing events 352
REX schedule 133
Start time 195
Unlock schedule # 1 (elevator doors) 135
Security level
Administrator 322
Assign to operator 324
Definition 326
Installer 322
Read only - (View components) 328
Restricted 322
Workspace 324
Security levels
Workspace 344
Security parameters 62
selecting accounts 331
selecting applications 332
Server
Database Utility Program, see Database 494
Getting Started 482
Login 482
Registration 478
Server's IP Address 516
Shunt delay 145
Signature capture 454
Site
Retrieving site events
SmartLink
Create instructions 358
WebStation 77
SmartLink application 77
Soft anti-passback 123, 129
Sound Notification 452
SPI Port
KT-400 115
SQL Interface
See Oracle/MS-SQL Interface 70
Start a session 38
State (cards), see Cards 240
Status icon
Refresh delay 66
Stolen
Card 233
Suspend messages 63
Swap descriptions 498
System components 28
System data 487
System Date & Time 451
System Log
View 485
System Parameters 456

T

TCP/IP 97
Technical Support 6
Terminal server 97
Time & Attendance Reports
Add transactions 436
Automatic Report output definition 434
Preview 441
Select doors 431
Use specific card range 432
Time and Attendance
Doors 128
Trace
Card 233
Card number 233
Option 240

U

UDP 97
Unlock schedules (elevator floors) 135
Upgrading the system 30
Usage restriction 241
User Datagram Protocol (UDP) 97
Users 229

V

Validate Card Access 275
Video

Background 200
Bandwidth 455, 468
Video server options 467
Video Vault
Configuring EntraPass Video Vault 80
File format 83
View Last Transactions 281
Visitor definition 285
Visual feedback
see Reader 101

W

Web page
Background 200
WebStation
Card number 233
Card use reports 420
Enhanced user management 469
Historical Reports 416
Operator login 323
SmartLink 77
WebViews
Add Web page as background 200
Graphic definition 198
What is access control? 1
Window
Description 63
Workspace 331, 332
Defining access levels 338
Defining applications 335
Defining card access group 340
Defining card types 339
Defining doors 336
Defining events 348
Defining gateways and sites 334
Defining graphics 343
Defining inputs 338
Defining relays 337
Defining reports 341
Defining video servers 345
Defining video views 348
Defining workspace 343
Filters 64
Security Levels 344
Security levels 324
Workstation
Automatic logout on idle 62
Suspend messages 63

А

Автоматическая установка (Express Setup) 514
контроллер 519
настройка конфигурации шлюза Corporate Gateway 514
Автоматическое подтверждение 323
Автоматическое соединение 62
Автоматическое создание резервных копий
планировщик заданий по созданию резервных копий 475
Адрес IP сервера 516
Адрес резервного сервера 76
Активировать/деактивировать использование считывателей карт 217, 220
Анимированные иконки
входов 546
дверей 540
контроллеров 538
прочие 551
реле 544
сайтов и шлюзов 548
Аппаратное обеспечение
описание 91
Архивные отчёты
автоматическое назначение имени файла 425
веб-станция 416
выбранные компоненты 417
выходной формат данных 422
окно расписания автоматических отчётов 421
описание 415
предварительный просмотр 440
путь для файла с результатами 425
рабочий стол 387
режим расписания 421
способы вывода 423
способы отбора 417
статус 388
язык отчёта 425

Аутенификация 62

Б

База данных
логические компоненты (просмотр) 367
проверка 479
служебная программа
восстановление файлов по последней транзакции с картой 498
замена описаний 498

проверка иерархической структуры 497
проверка ссылок базы данных 497
проверка файлов видеособытий 498
проверка файлов по учёту рабочего времени 497
структура 367
Безопасный режим 366, 379
Блокировка/разблокировка
двери 217
двери, временная 217
двери лифта 220
двери лифта, временная 220
Буфер событий
контроллера 100

В

Веб-представления
добавить веб-страницу как фон 200
описание графических схем 198
Веб-станция
SmartLink 77
архивные отчёты 416
вход в систему 323
номера карт 233
отчёты об использовании карт 420
режим усиленного администрирования пользователей 469
Веб-страницы
фон 200
Видео
пропускная способность 455, 468
фон 200
Видеосервер- опции 467
Видеохранилище
настройка конфигурации 80
формат файлов 83
Визуальная обратная связь
см. Считыватели 101
Восстановление файлов
по последней транзакции с картой 498
Время шунтирования (отключения от мониторинга) 145
Вход в систему (операторов) 38
Входы
анимированные иконки 546
группы 305
непрерывный мониторинг 226
нормальное состояние 144
нормальный статус 226
расписание мониторинга 144
создание групп 305
Выбор приложений 332
Выбор учётных записей 331
Выходной формат данных для баз данных 414
Выходы
мигание 150
мигание ограниченное время 150
период активации 149
привязка событий дверей к дополнительным выходам 149
режим работы 149
ровное свечение 150
ровное свечение ограниченное время 149

Г

Главный пароль 446
новый 446
подтверждение 446
Графические схемы
см. также Анимированные иконки 537
Графические схемы (Graphic)
описание 198
Графический статус (контроллера) 315
Группы
входы 305
двери 303
контроллеры 302
реле 304
уровни доступа 306
этажи 307
Группы дверей 303
Группы реле 304

Д

Данные регистрации для работы в режиме службы 460
Данные системы 487
Дата создания
карты 233
Двери 59
анимированные иконки 540
длительность открытия 129
длительность разблокировки 129
запирание при закрытии 133
запирание при открытии 133
кабины лифта 128
кнопка запроса на выход 133
контактный датчик 132
отпирание по сигналу запроса на выход 133
предтревожное состояние двери при слишком долгом открытии 132

режим блокировки 128
создание групп 303
считывание при незапертой двери 132
Дверь
вернуться к выполнению расписания 217, 220, 224
Диагностика по методу "запрос-ответ" 524
Диагностика сети (сервера) 459
Дополнительные компоненты системы 25
Драйвер
Corporate 1000 444

Ж

Жёсткая перезагрузка
формат карт 445
Жёсткий запрет повторного прохода 123, 129

З

Завершать сеанс при бездействии 62
Задержки удалённого модема 100
Замена описаний 498
Запретить использование считывателя карт на двери 219, 223
Запретить режим видео 63
Запрос на выход 105, 133
Звуковая сигнализация-подтверждение 452
Звуковая тревожная сигнализация 452
Зеркальная база данных и резервный сервер
CardGateway 2, 74
настройка конфигурации 74

И

Идентификационные карты
дата изменения 233
дата создания 233
номер карты 232, 233
отслеживание 233
потеряна 233
счётчик изменений 233
украдена 233
Идентификационный код 104, 239
дублировать 445
Изменить формат карт
восьмеричная система счисления 444
десятичная система счисления 444
шестнадцатеричная система счисления 445
Иконки статуса
время обновления 66
Иконки, см. Анимированные иконки 537
Импорт и экспорт файлов CSV 291
процедура импорта 296
процедура экспорта 293
создание шаблонов 292
Импорт/Экспорт 291
Импортирование фотографии из файла 242
Имя выходного файла 414
Интерактивная поддержка 5
Интерфейс Kantech IP Link 93
Интерфейс MS-SQL
см. интерфейс Oracle/MS-SQL 70
Интерфейс SmartLink 77
Интерфейс SQL
см. Интерфейс Oracle/MS-SQL 70
Информационные поля идентификационных карт 231

К

Карты
вывод на печать списка идентификационных карт 277
групп доступа назначение 238
дата изменения 231
изменить формат карт 444
имя пользователя 230, 232
информационные поля карт 231
копировать на карту посетителя 231
начальная дата 239
номер 230
ожидание нажатия клавиши 239
опции счётчика использований 241
отслеживание 240
показывать информацию о владельце вместе с фотографией 66
последние транзакции 281
проверка уровня доступа карты 275
режим усиленного администрирования пользователей 469
создание групп уровней доступа 283
создание разового пропуска 287
создание типов карт 286
сохранить фотографию на рабочий стол 379
статус 240
счётчик изменений 231
удаление после окончания срока действия 239
уровни доступа владельцев карт, назначение 238
формат карт 444
формат карт по умолчанию 444
фотографии импортирование 241
Клавиша Escape 104
кнопка запроса на выход 133

Кнопки
OK 49
выделить все 205
отмена 48
разрешить анимацию 49, 205
разрешить графику 49, 205
снять выделение всех 49, 205
Кодирование 62
Команды
назначение для событий 352
описание 357
Контактный датчик двери 132
Контроллер
автоматическая установка 519
описание 101
Контроллеры 59
анимированные иконки 538
перезагрузка 213
создание групп302
статус (графические схемы) 315
Контроллеры KT 102
Контроллеры KT-100 103
Контроллеры KT-200
модули расширения 105
настройка конфигурации 105
Контроллеры KT-300 103
Контроллеры KT-400
локальные зоны контроля 123
модули расширения 115
настройка конфигурации 113
описание локальных зон контроля 124
Контроллеры лифтов 105
Контроллеры лифтов KT-2252 105
программа 106
Контроллеры лифтов REB-8
программа108
Контроллеры типа KT-100 104
Контроллеры типа KT-300 103

Л

Ловушка 134
функции взаимной блокировки 134
Локальные зоны контроля контроллера
KT-400 123

М

Модем для передачи данных по коммутируемой линии 97
Модули расширения
настройка 115
Модуль расширения входов KT-MOD-INP16 115
Модуль расширения выходов KT-MOD-OUT16 115
Мультимедийные устройства 443, 452
Звуковая тревожная сигнализация 452
оцифровка изображений 453
оцифровка подписей 454
Мягкий запрет повторного прохода 123, 129

Н

Настройка конфигурации
зеркальной базы данных и резервного сервера74
интерфейса Oracle/MS-SQL 70
Настройка конфигурации системных устройств 59
Номер карты
отслеживание 233
Номер порта 516
Нормальный статус 144

О

Обновление системы 30
Ограничение использования 241
Одновременный вход в систему
операторов 323
Окно
описание 63
окно тревожных сообщений 67
Окончание срока действия 240
Онлайн-справка 5
Операторы
выбор языков 323
игнорировать рабочее пространство на рабочей станции (фильтр сообщений) 323
ограничения на регистрацию 328
одновременный вход в систему 323
пароль 323
разрешение регистрации на сервере 328
расписание для входа в систему 324
регистрации на веб-станции 323
регистрационное имя 323
Описание выходов 148
Описание групп доступа для идентификационных карт 283
Описание карт посетителей 285
Описание операторов 322
Описание параметров электронной почты 428
Описание разовых пропусков 287
Описание типов карт 286
Описания расписаний 194

Опции видеосервера 467
опции запроса на выход 133
Отключить сообщения 63
Отложенная карта 240
Отслеживание
карт 233
карт по номерам 233
опции 240
Отчёты
с веб-станции 416, 420
Отчёты об использовании карт
режим расписания 421
с веб-станции 420
Отчёты по учёту рабочего времени
выбор дверей 431
добавить транзакции 436
описание выходных данных автоматического отчёта 434
предварительный просмотр 441
фильтры информационных полей карт 432
Оцифровка подписей 454
Очистить базу данных 498
Очистка рабочих столов тревог 65, 67

П

Параметры безопасности 62
Параметры доступа
режим усиленного администрирования пользователей 469
Пароль
операторов 323
смена главного пароля 446
Перезагрузка, см. Контроллеры 213
Печать журнала 395, 404
Печать карт 277
Печать параметров событий 355
Планировщик заданий по созданию резервных копий 472
данные регистрации для работы в режиме службы 460
Повторная загрузка данных шлюза 208
Повторный проход
опции 240
Подтверждение тревог
автоматическое 323
звуковая тревожная сигнализация 452
окно тревожных сообщений 67
Описание и назначение 397
расписание подтверждения 352
установить приоритет 352
Пользователи 229
Порт
номер 516
Порт SPI контроллера
KT-400 115
Последовательный порт связи RS-232 92, 515
Потерянная
карта 233
Праздничные дни - описание 203
Приложение SmartLink
веб-станция 77
создание инструкций 358
Принтер, см. принтер журналов 448
Проверка уровня доступа карты 275
Программа CardGateway
зеркальная база данных и резервный сервер 2, 74
интерфейс Oracle/MS-SQL 70
Программа просмотра быстрых отчётов 522
Пропускная способность
видео 455, 468
Просмотр последних транзакций 281
Протокол TCP/IP 97
Протокол пользовательских дейтаграмм UDP 97
Путь сохранения отчётов 414

Р

Работа с картами
с веб-станции 469
Рабочая станция
завершать сеанс при бездействии 62
отключить сообщения 63
Рабочее пространство 331, 332
задание уровней доступа 338
описание видеосерверов 345
описание входов 338
описание графических схем 343
описание групп доступа для идентификационных карт 340
описание дверей 336
описание окон видеонаблюдения 348
описание отчётов 341
описание приложений 335
описание рабочего пространства 343
описание реле 337
описание событий 348
описание типов идентификационных карт 339
описание шлюзов и сайтов 334
уровни безопасности 324, 344
фильтры 64
Рабочие столы
избранных сообщений 386
тревог 391

Рабочие столы
Архивные отчёты 387
Рабочий стол сообщений
задержка автоматического пролистывания 380
несколько строк 378
оставлять на экране фотографию карты 379
отправить на задний план 383
показывать панель инструментов 379
показывать пиктограммы 378
показывать последнее сообщение вверху 379
показывать родительский элемент 382
показывать события жирным шрифтом 379
показывать сообщение (полностью) 379
просмотр архивных видеозаписей 390
сохранять свойства только вручную 379
тип сообщения 378
удалить все 381
цвет заднего фона 380
Рабочие столы тревог
печатать записи 395, 404
подтверждение 394
показать графическое окно 402
показать окно команд 400
удалить запись 395, 405
уничтожить удалённые записи 395
флаги 394
Сетевые тревоги
рабочий стол 404
Разовые пропуска
описание 287
Разрешить использование считывателя карт 219, 222
Разрешить/запретить использование считывателя карт 217
Расписание контроля подачи питания 103
Расписания
время окончания 195
дни недели 195
начальное время 195
печать событий 352
расписание кнопки запроса на выход 133
расписание мониторинга (входов) 144
расписание подтверждения 352
расписание разблокировки №1 (двери лифтов) 135
расписание регистрации операторов 324
Расписания разблокировки (этажи лифта) 135
Расписания улучшенные характеристики 458
Регистрация
сервер 478
см. Регистрация рабочей станции 478
Регистрация в системе (операторов) 38
Регистрация операторов в системе
имён 323
расписания 324
Регистрация системы 22
Редактирование компонентов системы 28
Режим усиленного администрирования пользователей
параметры доступа 469
Резервное копирование 487
Резервный сервер
CardGateway 457
ограничения применения CardGateway 74
системные параметры 457
см. Зеркальная база данных и резервный сервер 74
Реле
активация 224
анимированные иконки 544
временная активация 224
деактивация 224
описание 59
расписание активации 142
режим работы 142
создание групп 304
таймер временной активации 142
Релейный модуль расширения KT-MOD-REL8 115
Релейный модуль расширения REB-8 105
Ручные операции
блокировка двери 217
блокировка двери лифта 220
временная блокировка двери 217, 220
временная разблокировка двери 217, 220
запретить использование считывателя 217, 220
разблокировка дверей 217, 220
разрешить использование считывателей 217, 220

С

Сайт
Отбор событий сайта 99
Связь через модем по коммутируемой линии 97
Сервер
первый запуск 482
программа Database Utility, см. Базы данных 494
регистрация операторов 482
регистрация программы 478
Сетевые тревоги
рабочий стол 404
Системные настройки даты и времени 451
Системные параметры 456
Системный журнал
просмотр 485

Скорость передачи данных в ветви контроллера 93, 515
События
инструкции (назначение событий) 352
описание параметров 350
отображение (расписание) 352
печать параметров 355
печать расписания 352
просмотр связей 353
расписание подтверждения 352
удаление и восстановление связей 354
установка приоритета 352
цвет 352
Соединение Ethernet (polling) 96, 516
Сообщения
рабочий стол 377
фильтры 363
Статус (карт), см. Карты 240
Статусы баз данных 318

Т

таймаут соединения 92
Терминальный сервер 97
Техническая поддержка 6

У

Украденная
карта 233
Улучшенные характеристики расписания 458
Управление лифтами
выбор кабины для активации групп этажей 146
двери лифтовой кабины 128
расписания разблокировки (этажи лифта) 135
реле REB-8 106
создание групп этажей 307
создание этажей 197
Уровни безопасности
администратора 322
запрещённые 322
назначение операторам 324
описание 326
рабочее пространство 324, 344
только для чтения (просмотр компонентов) 328
установщика 322
Уровни доступа
администратора 57
для постановки на охрану 139
неверный 137
создание групп 306
Уровни доступа операторов – см. уровни безопасности
Установка 9
Установка системы 13
Устройство запроса на выход 105, 133
Учёт рабочего времени
двери 128

Ф

Файлы формата rpf 68
физический адрес компонента 329
Фон
веб-страницы 200
живого видео 200
Формат карт
жёсткая перезагрузка 445
использование нескольких форматов карт 445
Формат файлов CSV 68
Фотография 242
Функции взаимной блокировки
ловушка 134
Функция "принуждение" 123

Х

Хост-модем - описание 87

Ц

Целостность базы данных
проверка 494

Ч

Четырёхдверный контроллер KT-400 93
Что такое система контроля доступа? 1

Ш

Шлюз Corporate Gateway
автоматическая установка 514
настройка конфигурации 87
Шлюзы
анимированные иконки 548
жёсткая перезагрузка 208

Э

Электронная почта

описание параметров 428
Электронная почта
опции 68
Электронные пропуска 3
видеоизображения 241
вставить фотографию 242
драйвера оцифровки MCI 241
импортирование фотографии из файла 242
Элементы устройства 28
Этажи
группы 307
описание 197
подтверждение 109

Я

Языки
изменение 447
Языки работы для операторов 323

© 2008 Холдинг Tyco International. Все права защищены.

тел.: +1 (450) 444-2030 • бесплатная телефонная линия: +1 888 222-1560 • факс: +1 (450) 444-2029

Internet: www.kantech.com • Эл. почта: kantechsupport@tycoint.com

DN1415-0810