Access Management System

AMS configuration and operation

ru Руководство по программному обеспечению

Содержание

1 Использование справки

Использование файла справки.

Кнопки панели инструментов

Кнопка	Функция	Описание
	Скрыть	Нажмите эту кнопку, чтобы скрыть панель навигации (вкладки "Содержание", "Указатель", "Поиск"), оставив отображаться только область справки.
	Показать	После нажатия кнопки "Скрыть" будет отображаться кнопка "Показать". При нажатии этой кнопки снова отображается панель навигации.
	Назад	Нажмите эту кнопку для перемещения к последнему просмотренному разделу.
	Вперед	Нажмите эту кнопку для перехода вперед по этой же цепочке разделов.
	Печать	Нажмите эту кнопку, чтобы начать печать. Выберите "Напечатать выбранный раздел" или "Напечатать выбранный заголовок и все подразделы".

Вкладки

Содержание На этой вкладке представлено иерархическое отображение содержания. Нажмите на значок с изображением книги  , чтобы развернуть ее  , и нажмите на значок раздела  , чтобы открыть его.

Указатель На данной вкладке отображается указатель терминов в алфавитном порядке. Выберите раздел из списка или введите слово, чтобы найти содержащие его разделы.

Поиск Используйте эту вкладку для поиска любого текста. Введите текст в поле, затем нажмите кнопку **Разделы** для поиска разделов, содержащих все введенные слова.

Изменение размера окна справки

Перетащите угол или край окна до необходимого размера.

Дальнейшие условные обозначения, используемые в этой документации

– Текст (метки) интерфейса пользователя отображается **полужирным шрифтом**.

Например: **Сервис, Файл, Сохранить как...**

- Последовательность нажатия связана с помощью символа **>** (знаком "больше чем").
  Например: **Файл > Создать > Папка**
- Изменения типа управления (например, меню, кнопка, флажок, вкладка) в последовательности указаны перед меткой элемента управления.
  Например: Нажмите меню: **Дополнительно > Параметры >** вкладка: **Просмотр**
- Комбинации клавиш описаны двумя следующими способами.
  - Ctrl+Z: нажать первую клавишу и, удерживая ее нажатой, нажать вторую.
  - Alt, C: нажать и отпустить первую клавишу, затем нажать вторую.
- Функции кнопок-значков добавлены в квадратные скобки после самого значка.
  Например: [Сохранить]

2 Об этом документе

Это основное руководство по программному обеспечению Access Management System.
В нем рассматривается использование основной программы диспетчера диалоговых окон, которая далее называется AMS

– Конфигурация системы управления доступом в AMS,
– Работа системных операторов с настроенной системой.

Связанная документация

Следующая информация представлена в отдельных документах:

– Установка AMS и дополнительных программ.
– Функционирование AMS - Map View.

3 Обзор системы AMS

Access Management System — это мощная система, предназначенная исключительно для контроля доступа, которая может использоваться самостоятельно или в сочетании с флагманской системой видеонаблюдения Bosch BVMS.
Своими преимуществами эта система во многом обязана уникальному сочетанию передовых и проверенных временем технологий:

- Удобство использования: практичный пользовательский интерфейс и представление Map View с возможностью перетаскивания, а также оптимизированные диалоговые окна биометрической регистрации.
- Безопасность данных: система поддерживает новейшие стандарты (EU-GDPR 2018), операционные системы, базы данных и зашифрованные системные интерфейсы.
- Устойчивость: главные контроллеры доступа среднего уровня обеспечивают автоматическую отработку отказа и компенсируют работу локальных контроллеров доступа в случае сетевого сбоя.
- Ориентация на будущее: регулярные обновления и многочисленные инновационные усовершенствования.
- Масштабируемость: доступны различные уровни ввода от низкого до высокого.
- Совместимость: API-интерфейсы RESTful, интерфейсы для подключения к системам обработки событий и видеонаблюдения Bosch, а также к специализированным партнерским решениям.
- Защита инвестиций: возможность повышения эффективности установленного оборудования для контроля доступа и создания на его основе новой системы.

4 Лицензирование системы

Требования

– Система успешно установлена.
– Вы выполнили вход на компьютер с сервером AMS (желательно с правами администратора)

Процедура для приобретенных лицензий

Требования. Вы приобрели лицензии, используя подпись компьютера этого устройства. Для получения инструкций обратитесь к торговому представителю.
Путь к диалоговому окну: **Конфигурация** > **Лицензии**

1. Выполните вход в AMS, систему управления доступом.
   Примечание. Если система AMS установлена в папке Windows Program Files? выполните вход с правами администратора Windows.
2. Перейдите в раздел **Конфигурация** > **Лицензии**
3. Нажмите **Запустить License Manager**
4. В окне **License Manager** установите флажок напротив приобретенного вами базового пакета.
5. Во всплывающем окне **Активация лицензии**:
   – Вставьте **подпись компьютера** сервера Access Manager.
   – Вставьте **ключ активации лицензии**, полученный для базового пакета,
   – Нажмите **Активировать...**
6. В окне **License Manager** убедитесь, что базовый пакет, лицензию для которого вы только что активировали, теперь имеет статус **Активация действительна**.
7. В окне **License Manager**:
   – Нажмите **Импорт сведений о пакете**, чтобы найти и активировать пакеты лицензий, которые вы приобрели и получили в качестве файлов.
   – Нажмите **Импорт лицензий**, чтобы найти и активировать отдельные лицензии, которые вы приобрели и получили в качестве файлов.
8. Нажмите **Закрыть**, чтобы закрыть **License Manager**.
9. Вернитесь в главное диалоговое окно **Лицензии**, убедитесь, что приобретенные компоненты перечислены в списке с правильно указанным числом единиц.

Процедура для демонстрационного режима

Демонстрационный режим предоставляет лицензии на все системные компоненты на ограниченное время. Используйте демонстрационный режим только в непроизводственных средах, чтобы опробовать компоненты перед покупкой.

1. Вход в Access Manager
2. Перейдите в раздел **Конфигурация** > **Лицензии**
3. Нажмите кнопку **Активировать демонстрационный режим**
4. Убедитесь, что соответствующие компоненты перечислены в диалоговом окне **Лицензии**.

Демонстрационный режим активируется на 5 часов. Обратите внимание, что время до окончания срока действия режима отображается вверху диалогового окна **Лицензии** и в строке заголовка большинства диалоговых окон.

5 Настройка календаря

Планирование мероприятий по контролю доступа осуществляется с помощью **временных моделей**.

Временная модель — это абстрактная последовательность продолжительностью один или более дней, каждый из которых характеризуется **дневной моделью**.

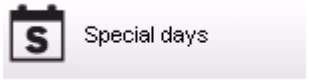
Временные модели контролируют действия, когда они применяются к базовому **календарю** системы контроля доступа.

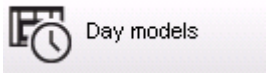
Календарь системы контроля доступа основан на календаре операционной системы хост-компьютера, однако в системном календаре также предусмотрены **особые дни**, которые свободно определяются администратором системы контроля доступа.

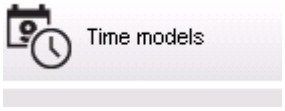
Особыми днями можно назначить определенную дату в календаре или определить их относительно какого-либо культурного события, например Пасхи. Они могут повторяться, но это необязательно.

Чтобы эффективно настроить календарь для своей системы контроля доступа, выполните следующие действия.

1. Определите **особые дни** календаря, актуальные для вашего расположения.
2. Определите **дневные модели**, описывающие активные и неактивные периоды для каждого типа дней. Так, дневная модель государственного праздника будет отличаться от модели обычного рабочего дня. Работа по сменам также влияет на тип и необходимое количество дневных моделей.
3. Определите **временные модели**, состоящие из одной или более дневных моделей.
4. Назначьте временные модели владельцам карт, разрешениям и входам.



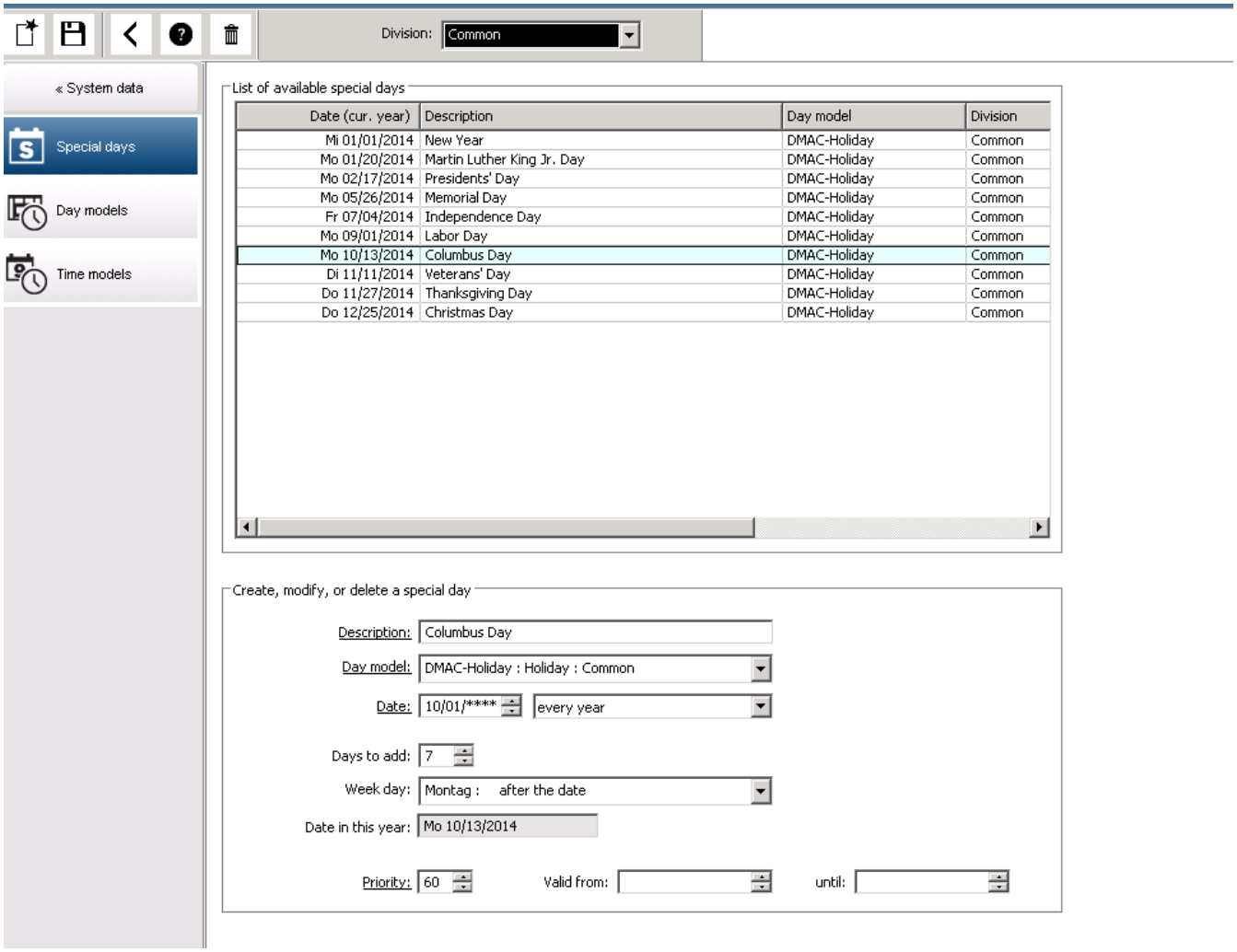




5.1 Определение особых дней

При открытии данного диалогового окна в верхнем поле списка появляется список всех указанных праздничных дней. Обратите внимание, что даты всех праздничных дней указаны только для текущего года. Однако календарь обновляется из года в год в соответствии с введенными данными.

Под данным списком находятся различные поля для создания новых особых дней, а также для изменения или удаления существующих особых дней. Чтобы добавить новый особый день, хотя бы три из этих полей ввода должны содержать данные. Во-первых, в соответствующих полях необходимо ввести **описание** и **дату**. В-третьих, в соответствующем списке выбора необходимо выбрать **класс**, к которому относится данный особый день.



Такая дата указывается за несколько шагов. Сначала в поле **Дата** вводится основная дата. В данный момент такая дата описывает некоторое событие текущего года. Если теперь пользователь указывает частоту периодического повторения в списке выбора рядом с полем даты, элементы даты, определяющие периодичность, замещаются подстановочными символами (*).

однократно	__.__.____
раз в год	__.__.****
раз в месяц в течение года	__.**.____
раз в месяц каждый год	__.**.****
в зависимости от даты Пасхи	**.**.****

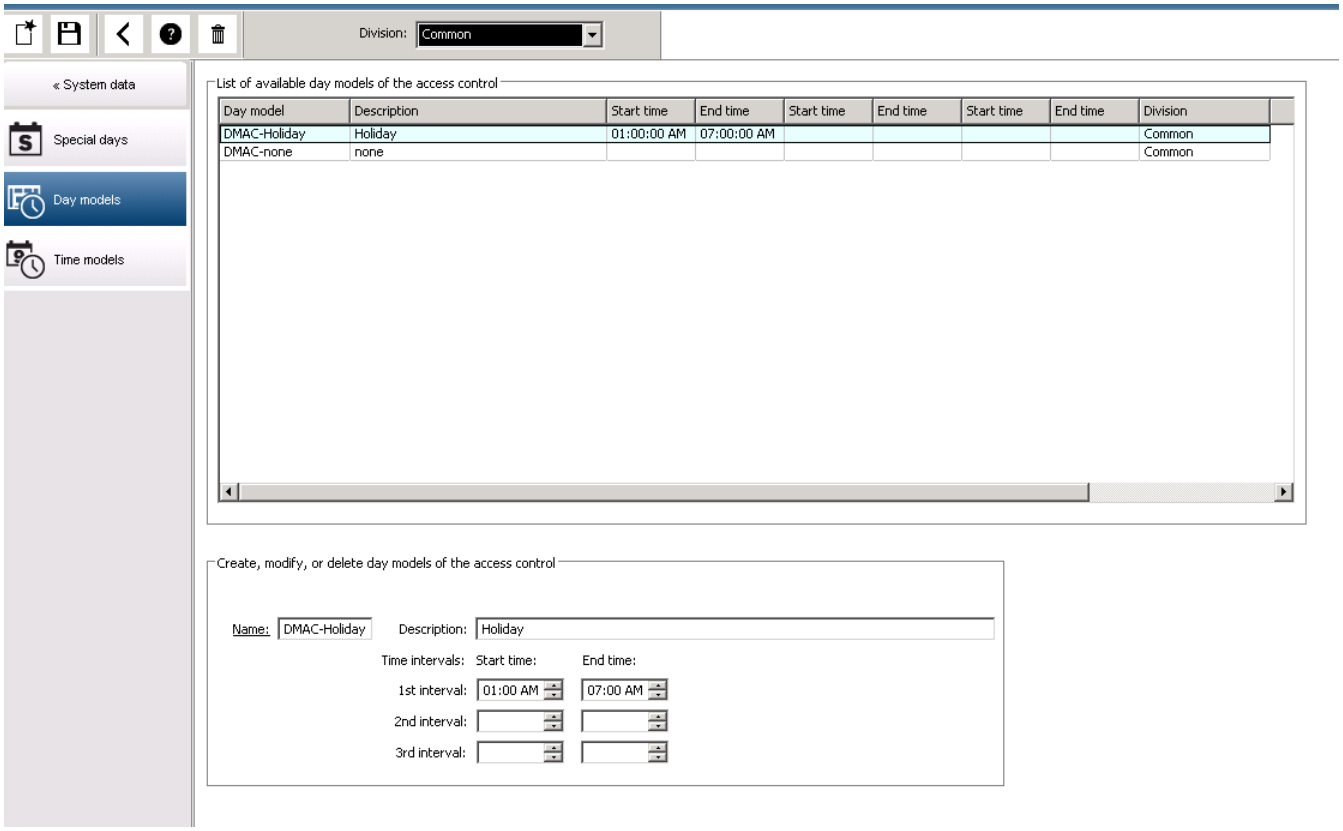
Праздничные дни, которые зависят от даты Пасхи, указываются не по дате, а по разности дней с Пасхальным воскресением. Дата Пасхального воскресения в текущем году указывается в поле **Дата в данном году**, а отклонение от этой даты вводится или выбирается в поле **Добавить дни**. Максимальное число дней — 188, поэтому добавляя или вычитая, можно определить любой день данного года.

Другие данные, например **день недели** для праздничного дня, не обязательны. Обратите внимание, что список дней недели определяется региональными настройками операционной системы (ОС). Это неизбежно ведет к отображению данных на разных языках, когда язык системы контроля доступа отличается от языка ОС.
Назначение **срока действия** также не обязательно. Если длительность не указана, по умолчанию устанавливается неограниченный срок действия начиная с даты ввода.
Также можно задать **приоритет**. Приоритет от 1 до 100 определяет, какой праздник должен быть использован. Если на один день приходятся два праздничных дня, сначала идет праздник с более высоким приоритетом. Если приоритеты равны, выбор праздника не осуществляется.
Праздник с приоритетом 0 деактивируется и не используется.
В диалоговом окне **Временные модели** отображаются только активные праздники, т.е. с приоритетом выше 0.

Замечание!
Временная модель подразделения "Общее" может использовать только те праздники, которые назначены для этого подразделения.
Временная модель особого подразделения "A" может использовать только те праздники, которые назначены для этого подразделения.
Невозможно смешивать праздники для разных подразделений, т. е. каждое подразделение может использовать только конкретные праздники, которые назначены для этого подразделения в его временной модели.

5.2 Определение дневных моделей

Модели дня определяют шаблон для любого дня. В них может быть до трех временных интервалов.
После открытия данного диалогового окна отображаются все существующие модели дня.



Это диалоговое окно используется для определения и изменения имени моделей, описаний и интервалов. Значок  запускает новую модель.

Время начала и конца интервала указывается в часах и минутах. Как только наступает соответствующее время, интервал активируется и деактивируется соответственно. Чтобы более четко представить эти значения времени как ограничители, на панели списка они отображаются с секундами (всегда 00). Например, авторизация в модели времени с интервалом 8:00 – 15:30 разрешает доступ с 08:00 утра до 15:30, но запрещает доступ после 15:30:01.

При вводе значений времени начала и конца выполняется их логическая проверка, например время начала должно предшествовать соответствующему времени конца. Одно из следствий — ни один интервал не переходит за полночь, а должен быть разделен в этой точке:

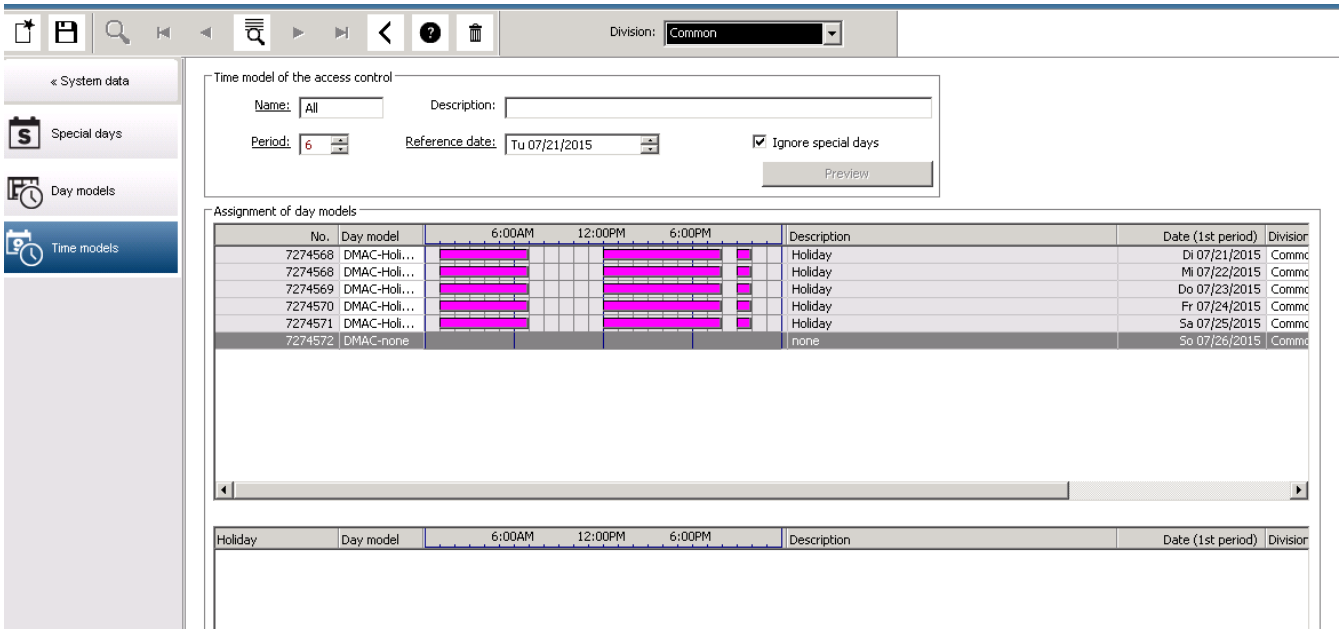
1-й интервал	от:	...	до:	00:00
Следующий интервал	от:	00:00	до:	...

За исключением полуночи (00:00), не допускаются пересечения между разделителями интервалов в модели одного дня. Обратите внимание, это правило препятствует вводу одного и того же времени в качестве конца одного интервала и начала следующего. Исключение: у 24-часового интервала в качестве времени начала и конца задано 00:00.

Замечание!
Совет. Интервалы можно проверять, просматривая их в диалоговом окне "Модели времени". Сначала создайте модель времени с заданными интервалами (Системные данные > Календарь > Модели дня). Затем назначьте данную модель дня фиктивной модели времени с периодом в один день ("Системные данные" > "Календарь" > "Модели времени"). Затем интервалы иллюстрируются на гистограмме.
Выйдите из диалогового окна "Модели времени" без сохранения изменений.

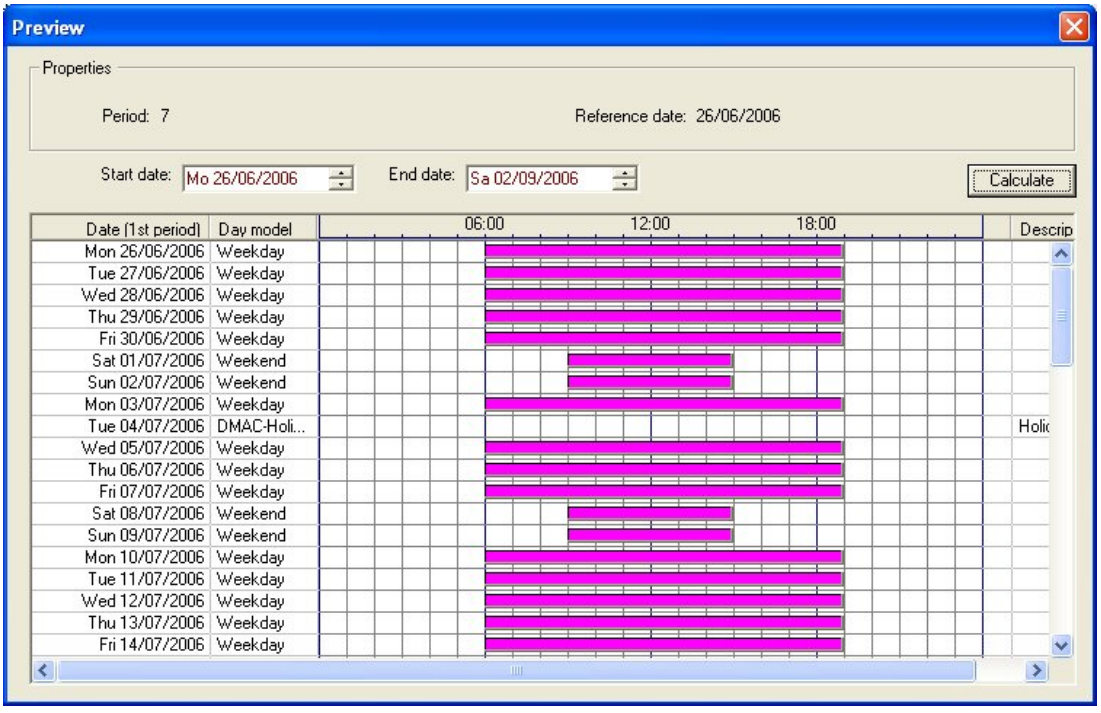
Модель дня можно удалить только в том случае, если она не назначена ни одному специальному дню и не используется во временных моделях.

5.3 Определение временных моделей

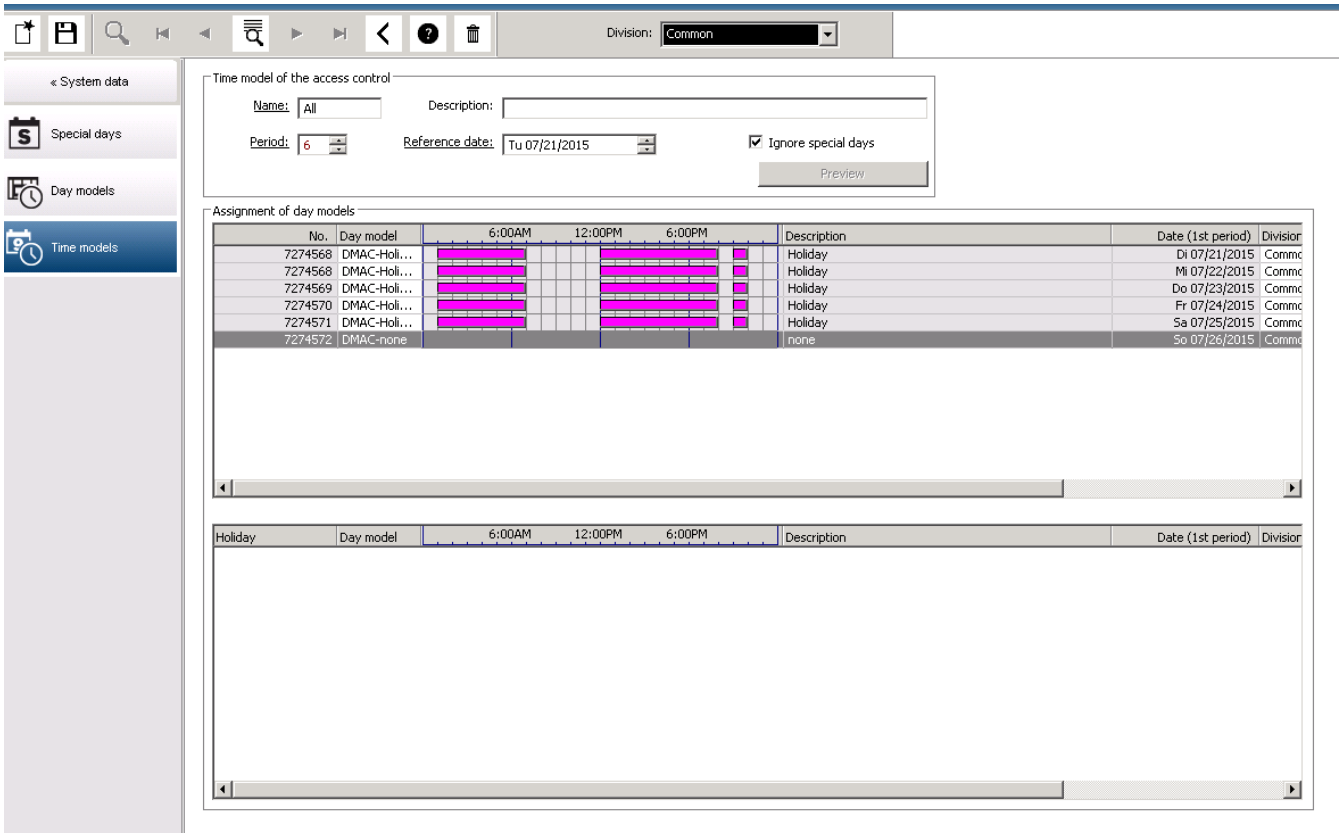


Существующие модели времени можно выбрать из списка поиска, а сведения о них отображаются в полях диалогового окна. Любая обработка осуществляется в соответствии с процедурой создания новых моделей времени.
Если маска пуста, модели времени можно создавать с нуля. Для этого необходимо ввести **имя** и число дней в **периоде**, а затем выбрать дату начала или **исходную дату**. После подтверждения этой даты (нажатие клавиши **ВВОД**) в расположенном ниже поле диалогового окна **Назначение моделей дня** появляется список. Число строк в данном списке соответствует заданному выше числу дней. В данных столбцах уже содержится порядковый номер и даты для этого периода, начиная с выбранной даты начала.
В этом списке пользователь может изменять или вставлять только записи в столбце **Имя**. Как уже упоминалось, записи в столбцах **№** и **Дата** берутся из описаний заголовка диалогового окна. Столбец **Описание** заполняется системой на основе выбора модели дня и объяснений, введенных в данном диалоговом окне.
Поле списка выбора активируется двойным щелчком в соответствующей строке столбца **Модель дня**. В этом списке можно выбрать одну из существующих моделей дня. Таким способом конкретную модель времени можно назначить каждому дню данного периода. Когда пользователь переходит к другой строке, система вносит в столбец **Описание** существующее описание выбранной модели дня.

В целях навигации и проверки в нижнем поле списка отображаются предварительно определенные **праздничные дни** с соответствующими моделями дня. Для выбранной или недавно созданной модели времени можно изменить назначение моделей дня определенным праздничным дням. Однако такие изменения применяются только к данной конкретной модели времени. Общие изменения, которые распространяются на все существующие и будущие модели, выполняются только в диалоговом окне «Праздничные дни». В соответствии с такими настройками дни недели задаются назначенными моделями дня с учетом праздничных дней.
Когда это допускается данными настройками, дни недели сопоставляются с назначенными моделями дня при рассмотрении особых дней. Для быстрой проверки правильного назначения и использования моделей дня (особенно в праздничные дни) в этом диалоговом окне предусмотрена область **предварительного просмотра**, в которой отображается распределением дней определенных периодов.
Наконец, если нажать кнопку **Предварительный просмотр**, открывается отдельное диалоговое окно, в котором можно указать временной период до 90 дней, включая праздничные дни. Если нажать кнопку **Рассчитать**, создается и отображается отчет (см. ниже). Этот процесс может занять несколько секунд в зависимости от величины интервала.



По умолчанию особые дни применяются к моделям времени в соответствии с их определениями. Если требуется найти особые дни, но результатов нет, это может быть обусловлено выбором настройки **Игнорировать особые дни**. Записи из двух нижних списков удаляются одновременно, поэтому очевидно, что пользователь немедленно обнаружит, что данные особые дни и классы дней не используются в этой модели.


Division: Common
« System data
Special days
Day models
Time models
Time model of the access control
Name: All
Description:
Period: 6
Reference date: Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No. Day model 6:00AM 12:00PM 6:00PM Description Date (1st period) Division
7274568 DMAC-Holi... Holiday Di 07/21/2015 Commc
7274568 DMAC-Holi... Holiday Mi 07/22/2015 Commc
7274569 DMAC-Holi... Holiday Do 07/23/2015 Commc
7274570 DMAC-Holi... Holiday Fr 07/24/2015 Commc
7274571 DMAC-Holi... Holiday Sa 07/25/2015 Commc
7274572 DMAC-none none So 07/26/2015 Commc
Holiday Day model 6:00AM 12:00PM 6:00PM Description Date (1st period) Division

6 Настройка подразделений

Введение

Система может быть дополнительно лицензирована для обеспечения совместного контроля доступа для объекта, который совместно используется любым количеством независимых сторон, которые называют **Подразделения**.

Операторам системы может быть назначено одно или несколько подразделений.

Операторам видны лица, устройства и проходы только этих подразделений.

Если функция **Подразделения** не лицензирована, все объекты, управляемые системой, принадлежат одному подразделению под названием **Общие**.

Предварительные требования

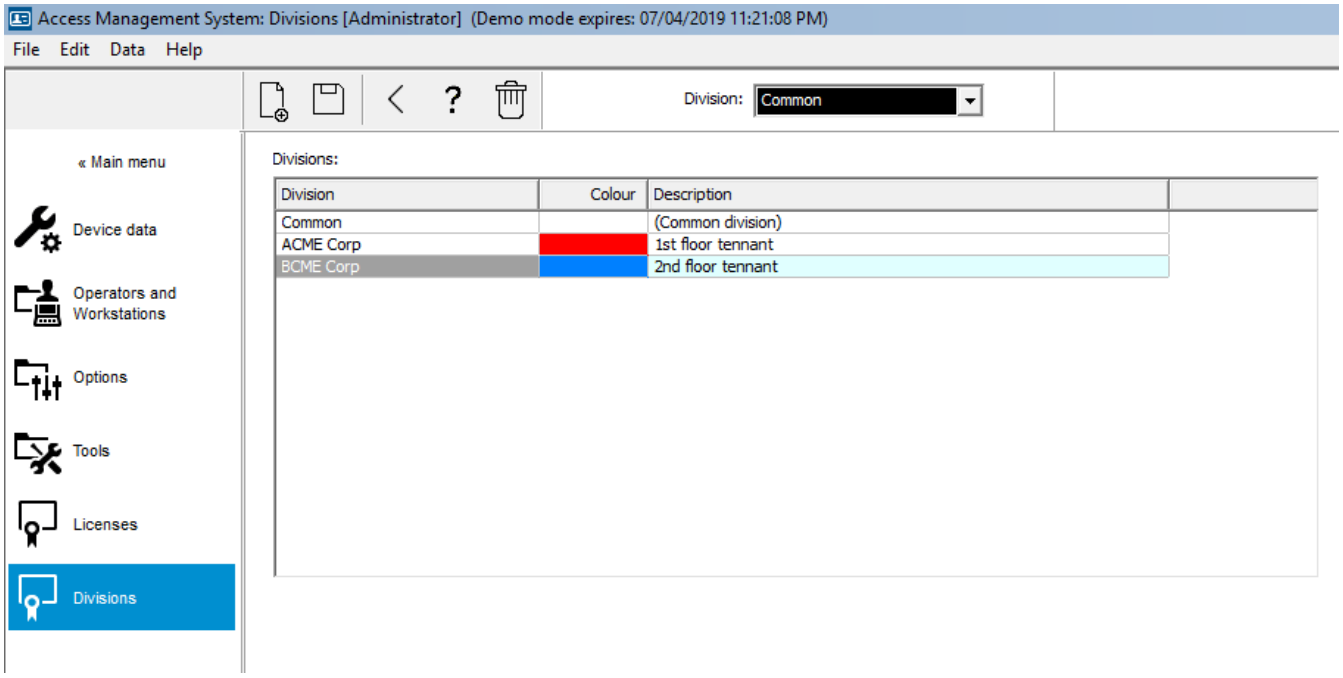
– Функция «Подразделения» лицензирована для вашей установки.

Путь к диалоговому окну

– Главное меню > **Конфигурация** > **Подразделения**

Процедура

1. Нажмите  на панели инструментов.
   – Создается новое подразделение с именем по умолчанию.
2. Замените имя по умолчанию и (при необходимости) введите описание для других операторов.
3. Щелкните столбец **Цвет**, чтобы назначить цвет и различить активы подразделения в пользовательском интерфейсе.
4. Нажмите  для сохранения.



6.1 Назначение подразделений устройствам

Назначение подразделений устройствам в редакторе устройств

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Данные устройства**

Предварительные требования

– Подразделения лицензированы и используются
– Создано по крайней мере одно подразделение.

Процедура

1. В дереве устройств выберите устройство для назначения.
   – Редактор устройства появится в главном панели диалогового окна.
2. В списке подразделений выберите новое подразделение для устройства
   – В списке появится новое подразделение.
3. Нажмите (Сохранить) для сохранения

Замечание!

Все компоненты прохода должны принадлежать одному подразделению
Система не позволит сохранить проход, пока все его компоненты не будут принадлежать одному подразделению.

6.2 Назначение подразделений операторам

Назначайте подразделения операторам в диалоговом окне **Права пользователей**

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Операторы и рабочие станции > Права пользователей**

Предварительные требования

– Подразделения лицензированы и используются
– Создано по крайней мере одно подразделение.
– В системе создан по крайней мере один оператор

Процедура

1. В диалоговом окне **Права пользователей** выберите запись о персонале для назначаемого оператора.
2. На вкладке **Подразделения** используйте клавиши со стрелками для перемещения подразделений из списка **Доступные подразделения** в список **Назначенные подразделения** для этого оператора.
3. Нажмите (Сохранить) для сохранения

7 Настройка IP-адресов

Локальные контроллеры доступа в сети требуют согласованной схемы IP-адресов для участия в системе контроля доступа. Инструмент **AccessIPConfig** находит контроллеры в сети и предоставляет удобный интерфейс для централизованного администрирования адресов и других сетевых параметров.

Требования

- Локальные контроллеры доступа подключены к электропитанию и сети.
- При необходимости можно воспользоваться схемой IP-адресов контроллеров и их паролями.

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Инструменты**

Процедура

1. Пройдите по пути к диалоговому окну (см. выше) и нажмите кнопку **Конфигурация AMC и устройства для считывания отпечатков пальцев.**
   Откроется инструмент **AccessIPConfig**.
2. Нажмите **Сканировать AMC**
   Отобразится список локальных контроллеров доступа, доступных в сети. Для каждого контроллера отображаются следующие параметры:
   - **MAC-адрес**: аппаратный адрес контроллера. Обратите внимание, что это **не** адрес главного контроллера доступа, который также называется MAC исключительно из-за совпадения.
   - **Сохраненный IP-адрес**:
   - **Номер порта**: по умолчанию — `10001`
   - **DHCP**: используется значение **Да**, только если контроллер настроен получать IP-адрес от DHCP
   - **Текущий IP-адрес**
   - **Серийный номер**
   - Заметки, добавленные командой специалистов по настройке сети
3. Дважды щелкните AMC в списке, чтобы изменить его параметры во всплывающем окне. Кроме того, можно выбрать строку нужного AMC и нажать кнопку **Задать IP-адрес...** Обратите внимание, что может потребоваться ввести пароль, если он установлен для устройства.
   Измененные параметры будут сохранены, как только вы нажмете кнопку OK во всплывающем окне.
4. Завершив настройку IP-параметров контроллеров, нажмите **Файл** > **Выйти**, чтобы закрыть инструмент.
   Вы вернетесь в основное приложение.

Для получения более подробной информации нажмите **Справка** в инструменте **AccessIPConfig**, чтобы просмотреть его собственный файл справки.

8 Использование редактора устройств

Введение

Редактор Device Editor (**DevEdit**) предназначен для добавления и удаления небольшого количества проходов и устройств или для добавления, изменения или удаления отдельных параметров.

Для импорта крупных существующих конфигураций используйте функцию **Импорт/ экспорт конфигурации** в разделе **Главное меню** > **Конфигурация** > **Инструменты**

В редакторе устройств доступны представления, соответствующие следующим редактируемым иерархиям:

- **Конфигурация устройств**: электронные устройства в системе контроля доступа.
- **Рабочие станции**: компьютеры, взаимодействующие в системе контроля доступа.
- **Области**: физические зоны, на которые разделена система контроля доступа.

Требования

Система правильно установлена, лицензирована и подключена к сети.

Путь к диалоговому окну

- **Главное меню** > **Конфигурация** > **Данные устройства**

Использование панели инструментов DevEdit

Кнопки панели инструментов DevEdit обладают следующими функциями независимо от того, какое представление активно, например **Устройства**, **Рабочие станции** или **Области**.

Кнопка	Ярлык	Описание
	Ctrl + N	Создание нового элемента в выбранном узле. Кроме того, можно щелкнуть по узлу правой кнопкой, чтобы открыть его контекстное меню.
	Del	Удаление выбранного элемента и всех элементов под ним.
	Ctrl-Page up	Первый элемент в дереве
	Ctrl -	Предыдущий элемент
	Ctrl +	Следующий элемент
	Ctrl-Page down	Последний элемент в дереве
	Ctrl-A	Разворачивание и сворачивание дерева.
	Ctrl-K	Обновление данных путем их повторной загрузки из базы данных. **Все несохраненные изменения удаляются.**
	Ctrl-S	Сохранение текущей конфигурации

	Ctrl-F	Открытие окна поиска
		Открытие дерева **Конфигурация устройства**
		Открытие дерева **Рабочие станции**
		Открытие дерева **Области**

Во всех представлениях DevEdit начинайте с корня дерева и добавляйте элементы, используя кнопки панели инструментов, меню или контекстное меню каждого элемента (щелкните правой кнопкой мыши, чтобы вызвать его). Чтобы добавить вложенные элементы в дерево, сначала выберите элемент, под которым должен отображаться этот вложенный элемент.

Завершив добавление элементов в дерево, нажмите кнопку **Сохранить**  , чтобы сохранить конфигурацию.
Чтобы закрыть DevEdit, нажмите **Файл** > **Выход**.

9 Настройка областей контроля доступа

Вводные сведения об областях

Охраняемые объекты можно разделить на области. Области могут быть любого размера: одно или несколько зданий, один этаж или даже отдельные комнаты.

Некоторые варианты использования областей:

– Локализация отдельных лиц на охраняемом объекте.
– Оценка числа лиц в заданной области в случае эвакуации или аварийной ситуации.
– Ограничение числа лиц или автомобилей в некоторой области:
  по достижении предварительно заданного предела заполнения дальнейшие попытки входа могут отклоняться, пока лица или автомобили не покинут область.
– Реализация контроля последовательности доступа и запрет двойного прохода

Система различает два типа областей с контролем доступа:

– Области для людей
– Области для автомобилей (автостоянки)

Каждая область может иметь подобласти для более точного и детального контроля.

Области для людей могут иметь до 3 уровней вложения, области для автомобилей — только 2 уровня, а именно парковка в целом и парковочные зоны: от 1 до 24.

Область по умолчанию, которая существует во всех установках, называется **Снаружи**. Она является родительской для всех определяемых пользователем областей обоих типов: для людей и для автомобилей.

Использовать область можно только в том случае, если к ней ведет по меньшей мере один вход.

Редактор устройств **DevEdit** можно использовать для назначения любому входу области местоположения и области назначения. Когда кто-либо сканирует карту в считывателе, принадлежащем определенному проходу, это новое местоположение лица становится областью назначения данного прохода.

Замечание!

Для управления последовательностью доступа и запрета двойного прохода требуется, чтобы на проходах соответствующих областей были установлены считыватели входа и выхода.

Для предотвращения случайного или намеренного прохода «впритык» настоятельно рекомендуется использовать входы типа «Турникет».

Порядок создания областей

Требования

Оператору системы требуется разрешение системного администратора на создание областей.

Путь к диалоговому окну (AMS)

1. В диспетчере диалоговых окон AMS выберите **Главное меню** > **Конфигурация** > **Данные устройства**

2. Нажмите «Области» 

3. Выберите узел **Снаружи** или один из его дочерних узлов и нажмите  на панели инструментов. Кроме того, можно щелкнуть правой кнопкой мыши **Снаружи**, чтобы добавить область через контекстное меню.
   Все области, созданные изначально, получают уникальное имя **Область** и числовой суффикс.
4. Во всплывающем окне выберите тип (**Область** для людей или **Автостоянка** для автомобилей.
   Обратите внимание, что дочерние элементы обоих типов может иметь только область **Снаружи**. Любая вложенная зона этих дочерних элементов всегда наследует тип родительского элемента.
   - **Области** для людей могут иметь вложенные уровни (до трех). Для каждой области или подобласти можно определить максимальную вместимость.
   - **Автостоянки** — это виртуальные объекты, состоящие по меньшей мере из одной **зоны стоянки**. Если вместимость автостоянки не требуется ограничивать системным образом, отображается 0. В противном случае максимальное количество парковочных мест на зону составляет 9999, а на главной панели автостоянки отображается сумма всех свободных мест в ее зонах.

Порядок редактирования областей

1. Щелкните область в иерархии, чтобы выбрать ее.
2. Перезапишите один или несколько следующих атрибутов на главной панели диалогового окна.

Имя	Имя по умолчанию, которое можно перезаписать.
Описание	Свободное текстовое описание области.
Макс. кол-во людей/ автомобилей	Значение по умолчанию 0 (ноль), если ограничивать вместимость не требуется. В противном случае необходимо ввести целое число, ограничивающее вместимость.

Примечания.

- Невозможно переместить область, перетащив ее в другую ветвь иерархии. При необходимости ее необходимо удалить и снова создать в другой ветви.

Порядок удаления областей.

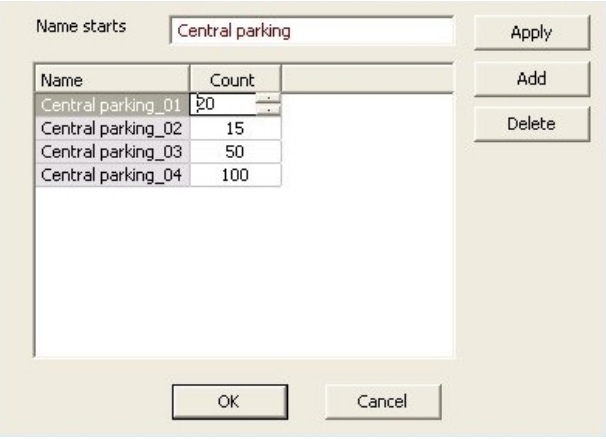
1. Щелкните область в иерархии, чтобы выбрать ее.
2. Нажмите **Удалить**  или щелкните правой кнопкой мыши, чтобы выполнить удаление через контекстное меню.

Примечание. Невозможно удалить область, пока не будут удалены все ее дочерние элементы.

9.1 Настройка областей для автомобилей

Создание областей для автомобилей (автостоянка, парковочная зона)

Если выбран тип области **Автостоянка**, отобразится всплывающее окно.



1. Введите имя в поле **Имя начинается с**, чтобы создать главное имя для всех подобластей автостоянки или **парковочных зон**.
   С помощью кнопки **Добавить** можно создать до 24 **парковочных зон**, и имя каждой будет состоять из главного имени и двузначного суффикса.
2. Если необходимо системным образом ограничить вместимость этих областей, введите число парковочных мест в столбце **Количество**. Если ограничивать вместимость не требуется, введите 0.

Примечание. Максимальная вместимость всей автостоянки должна быть равна сумме этих чисел. Только парковочные зоны могут содержать парковочные места; **автостоянка** представляет собой виртуальный объект, состоящий из по меньшей мере одной **парковочной зоны**. Максимальное число парковочных мест на одну зону — 9999.

Создание входов для автостоянок

Как и с обычными областями, парковкам требуется вход. Подходящая модель двери — **Автостоянка 05c**.

Для мониторинга заполнения автостоянки в одном AMC требуется использовать 2 входа с этой моделью двери. Один — для въезда, другой — для выезда.

Требование

Создайте автостоянку с по меньшей мере одной парковочной зоной, как описано выше.

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Данные устройства**

Выберите **LACs/Проходы/Устройства** 

Процедура

1. В иерархии устройств создайте AMC или выберите AMC, у которого нет зависимых входов.
2. Щелкните правой кнопкой мыши панель AMC и выберите **Создать вход**.
3. Во всплывающем окне **Создание входа** выберите модель входа **Автостоянка 05c** и добавьте входной считыватель, тип которого соответствует типу установленного на въезде на автостоянку.
4. Нажмите кнопку **ОК**, чтобы закрыть всплывающее окно.
5. Выберите только что созданный вход в иерархии устройств.
   – Обратите внимание, что система автоматически назначила считыватель в качестве считывателя входа.

6. В основной панели редактирования на вкладке **Автостоянка 05c** выберите в выпадающем меню **Место назначения** ранее созданную автостоянку.
7. Щелкните правой кнопкой мыши AMC и создайте еще один вход типа **Автостоянка 05c**, как указано выше.
   – Обратите внимание, что в этот раз можно выбрать только выходной считыватель.
   – Нажмите кнопку **OK**, чтобы закрыть всплывающее окно.
8. Выберите второй только что созданный вход в иерархии устройств
   – Обратите внимание, что система автоматически назначила второй считыватель в качестве выходного считывателя.

10 Настройка операторов и рабочих станций

Вводные сведения об административных правах контроля доступа

Административные права для системы контроля доступа определяют, какие диалоговые окна системы можно открыть и какими функциями можно воспользоваться в этих окнах. Права можно назначать как операторам, так и рабочим станциям.

Права рабочей станции могут временно ограничить права ее оператора, поскольку критически важные для безопасности операции должны выполняться только с особо безопасных рабочих станций.

Права назначаются операторам и рабочим станциям в связках, называемых **Профили**. Каждый профиль адаптирован к обязанностям одного из определенных типов операторов или рабочих станций.

Каждый оператор или рабочая станция могут иметь несколько профилей авторизации.

Общая процедура и пути к диалоговым окнам

1. Создайте рабочие станции в редакторе устройств:

   Конфигурация > **Данные устройства** > **Рабочие станции** 
2. Создайте профили рабочих станций в диалоговом окне:
   Операторы и рабочие станции > **Профили рабочих станций**.
3. Назначьте профили рабочим станциям в следующем диалоговом окне:
   Операторы и рабочие станции > **Права рабочих станций**
4. Создайте профили оператора в следующем диалоговом окне:
   Операторы и рабочие станции > **Профили пользователей**.
5. Назначьте профили операторам в следующем диалоговом окне:
   Операторы и рабочие станции > **Права пользователя**

10.1 Создание рабочих станций

Рабочие станции — это компьютеры, с которых операторы работают с системой контроля доступа.

Сначала рабочую станцию необходимо создать, то есть зарегистрировать компьютер в системе контроля доступа.

Путь к диалоговому окну

Конфигурация > **Данные устройства** > **Рабочие станции**

Процедура

1. Щелкните **DMS** правой кнопкой мыши и выберите **Новый объект** в контекстном меню или щелкните ✚ на панели инструментов.
2. Введите следующие значения для параметров:
   - **Имя** рабочей станции должно в точности совпадать с именем компьютера.
   - **Описание** — это необязательное поле. Его можно использовать, например, чтобы описать функцию и расположение рабочей станции
   - **Вход через считыватель**: установите этот флажок только в том случае, если операторы должны входить в систему на этой рабочей станции, предъявляя свои карточки регистрационному считывателю, подключенному к этой рабочей станции. Подробные сведения см. в разделе Двухфакторная проверка подлинности

– **Автоматический выход после:** время в секундах после входа с использованием регистрационного считывателя, после которого сеанс автоматически завершается. Установите значение 0, чтобы это время было неограниченным.

10.2 Создание профилей рабочих станций

Вводные сведения о профилях рабочих станций

В зависимости от физического расположения рабочая станция контроля доступа должна быть тщательно настроена независимо от применения, например:

– какие операторы могут ее использовать;
– какие учетные данные нужны для ее использования;
– Какие задачи контроля доступа можно выполнять с нее.

Профиль рабочей станции представляет собой набор прав, который определяет следующее:

– Меню диспетчера диалоговых окон и диалоговые окна, которые можно использовать на рабочей станции
– Какой(ие) профиль(и) пользователя должен иметь оператор, чтобы выполнить вход на этой рабочей станции.

Замечание!

Профили рабочих станций переопределяют профили пользователей

Оператор может получить только те из прав своего профиля, которые также входят в профиль рабочей станции компьютера, с которого он вошел в систему. Если у профилей рабочих станций и профилей операторов нет общих прав, у пользователя не будет никаких прав на этой рабочей станции.

Путь к диалоговому окну

Конфигурация > **Операторы и рабочие станции** > **Профили рабочих станций**

Создание профиля рабочей станции

1. Щелкните  , чтобы создать новый профиль
2. Введите имя профиля в поле **Имя профиля** (обязательно)
3. Введите описание профиля в поле **Описание** (необязательно, но рекомендуется)
4. Нажмите  или **Применить**, чтобы сохранить изменения

Назначение прав выполнения для функций системы

1. В списке **Функции** выберите функции, которые должны быть доступны этой рабочей станции, и дважды щелкните их, чтобы задать значение `Yes` в столбце **Выполнение**.
   – Кроме того, необходимо убедиться, что для всех функций, которые должны быть недоступны, задано значение `No`.
2. Нажмите  или **Применить**, чтобы сохранить изменения

Назначение профилей пользователей профилям рабочих станций

В области **Профиль пользователя**.

Список **Назначенные профили** содержит все профили, которым разрешено входить на рабочую станцию с помощью текущего профиля рабочей станции.

Поле **Доступные профили** содержит все остальные профили. Они еще не авторизованы для входа на рабочую станцию с использованием текущего профиля рабочей станции.

1. с помощью кнопок со стрелками переместите профили из одного списка в другой.
2. Нажмите  или **Применить**, чтобы сохранить изменения

Замечание!
Профили администратора по умолчанию для пользователя (**UP-Administrator**) и для рабочей станции (**WP-Administrator**) невозможно изменить или удалить.
Профиль **WP-Administrator** привязан к серверной рабочей станции, и изменить это невозможно. Это гарантирует, что существует как минимум один пользователь, который может войти в систему на рабочей станции сервера.

10.3 Назначение профилей рабочих станций

Используйте это диалоговое окно для управления назначениями профилей рабочих станций рабочим станциям. Каждая рабочая станция должна иметь по меньшей мере один профиль рабочей станции. При наличии нескольких профилей все права в этих профилях применяются одновременно.

Путь к диалоговому окну
Конфигурация > **Операторы и рабочие станции** > **Права рабочей станции**

Процедура
Список **Назначенные профили** содержит все профили рабочих станций, которые относятся к этой рабочей станции.
Список **Доступные профили** содержит все профили рабочих станций, которые еще не были назначены этой рабочей станции.

1. В списке рабочих станций выберите рабочую станцию, которую требуется настроить
2. С помощью кнопок со стрелками перемещайте выбранные профили между списками **Назначенные** и **Доступные**.
3. Нажмите  или **Применить**, чтобы сохранить изменения

Замечание!
Профили администратора по умолчанию для пользователя (**UP-Administrator**) и для рабочей станции (**WP-Administrator**) невозможно изменить или удалить.
Профиль **WP-Administrator** привязан к серверной рабочей станции, и изменить это невозможно. Это гарантирует, что существует как минимум один пользователь, который может войти в систему на рабочей станции сервера.

10.4 Создание профилей пользователя (оператора)

Вводные сведения о профилях пользователей
Примечание. Термин **Пользователь** в контексте прав пользователя синонимичен термину **Оператор**.
Профиль пользователя представляет собой набор прав, который определяет следующее:
– Меню диспетчера диалоговых окон и диалоговые окна, которые видны оператору.
– Возможности оператора в этих диалоговых окнах, в основном права на выполнение, изменение, добавление и удаление элементов этих диалоговых окон.

Следует тщательно настраивать профили пользователей в зависимости от опыта, благонадежности с точки зрения безопасности и обязанностей человека:

Путь к диалоговому окну

Конфигурация > **Операторы и рабочие станции** > **Профили пользователей**

Процедура

1. Щелкните  , чтобы создать новый профиль
2. Введите имя профиля в поле **Имя профиля** (обязательно)
3. Введите описание профиля в поле **Описание** (необязательно, но рекомендуется)
4. Нажмите  или **Применить**, чтобы сохранить изменения

Замечание!

Присваивайте профилям имена, которые понятно и точно описывают возможности и ограничения профиля.

Добавление прав на редактирование и выполнение для системных функций

1. В области списка выберите функции (первый столбец) и возможности в составе этой функции (**Выполнить**, **Изменить**, **Добавить**, **Удалить**), которые должны быть доступны этому профилю. Дважды щелкните их, чтобы изменить значение параметра на `Yes`.
   - Кроме того, необходимо убедиться, что для всех функций, которые должны быть недоступны, задано значение `No`.
2. Нажмите  или **Применить**, чтобы сохранить изменения

10.5 Назначение профилей пользователей (операторов)

Примечание. Термин **Пользователь** в контексте прав пользователя синонимичен термину **Оператор**.

Требования

- Оператор, который должен получить этот профиль пользователя, определен в системе контроля доступа как **Лицо**.
- Соответствующий профиль пользователя определен в системе контроля доступа.
  - Обратите внимание, что всегда можно назначить профиль пользователя с неограниченными правами **UP-Administrator**, но эта практика устарела по соображениям безопасности.

Путь к диалоговому окну

Конфигурация > **Операторы и рабочие станции** > **Права пользователей**

Процедура

1. Загрузите запись личного дела предполагаемого пользователя в диалоговое окно.
2. При необходимости ограничьте действительность профиля пользователя, указав даты в полях **Действительно с** до **Действительно до**.

Назначение профилей пользователя операторам

В области **Профили пользователей**:

Список **Назначенные профили** содержит все профили пользователя, которые назначены этому пользователю.
В поле **Доступные профили** перечислены все профили, доступные для назначения.

1. с помощью кнопок со стрелками переместите профили из одного списка в другой.
2. Установите флажок **Глобальный администратор**, чтобы предоставить этому оператору доступ к записям из личного дела с правами чтения и записи, для которых активирован атрибут **Глобальное администрирование**. По умолчанию оператор получает доступ к таким записям из личного дела только с правом чтения.
3. Нажмите  для сохранения изменений.

Назначение операторам прав на использование API
При наличии необходимых настроек и лицензий внешний программный код может вызывать функции системы контроля доступа через интерфейс прикладного программирования (или API). Внешняя программа функционирует в системе через прокси-оператора. Раскрывающийся список **Использование API** контролирует возможности текущего оператора, если он используется внешним кодом в качестве прокси-оператора.
Конфигурация > **Операторы и рабочие станции** > **Права пользователей**
– Выберите настройку из списка **Использование API**.
Доступные на выбор варианты:

Доступ запрещен	Оператор не может использоваться API для выполнения системных функций.
Только считывание	Оператор может использоваться API для чтения системных данных, но не для добавления, изменения или удаления этих данных.
Без ограничений	Оператор может использоваться API для чтения, добавления, изменения и удаления системных данных.

– Нажмите  для сохранения изменений

10.6 Настройка паролей для операторов

Как задать безопасные пароли для себя и для других.

Введение
Системе требуется хотя бы один оператор. Оператор по умолчанию в новой установке имеет имя пользователя **Administrator** и пароль **Administrator**. Первым шагом в настройке системы всегда должен быть вход в систему с этими учетными данными и изменение пароля пользователя **Administrator** в соответствии с парольными политиками вашей организации.
После этого можно добавлять других операторов: с привилегиями и без них.

Процедура изменения собственного пароля.
Требования
Вы вошли в диспетчер диалоговых окон.

Процедура
1. В диспетчере диалоговых окон выберите меню: **Файл** > **Изменить пароль**

2. Во всплывающем окне введите текущий пароль, новый пароль, а затем новый пароль еще раз, чтобы подтвердить его.
3. Нажмите **Изменить**.

Обратите внимание, что эта процедура — единственный способ изменить пароль для Administrator.

Процедура изменения паролей других операторов.

Требования

Чтобы изменить пароли других пользователей, необходимо войти в диспетчер диалоговых окон с помощью учетной записи с привилегиями администратора (Administrator).

Процедура

1. В главном меню диспетчера диалоговых окон перейдите в раздел **Конфигурация** > **Операторы и рабочие станции** > **Права пользователя**
2. В главном диалоговом окне с помощью панели инструментов загрузите оператора, пароль которого требуется изменить.
3. Нажмите **Изменить пароль...**
4. Во всплывающем окне введите новый пароль, а затем введите его еще раз, чтобы подтвердить.
5. Во всплывающем окне введите срок действия нового пароля: **Неограниченный** или укажите число дней.
   - Для производственных сред настоятельно рекомендуется установить срок действия.
6. Нажмите кнопку **ОК**, чтобы закрыть всплывающее окно.

В главном диалоговом окне нажмите значок  , чтобы сохранить запись пользователя.

Обратите внимание, что инструменты выбора даты **Действует с** и **Действует до** под кнопкой **Изменить пароль...** относятся к сроку действия прав пользователя в этом диалоговом окне, а не к паролю.

Подробные сведения

Всегда устанавливайте пароли в соответствии с политикой паролей вашей организации. Инструкции по составлению такой политики можно получить, например, в руководстве Microsoft по следующему адресу.
https://www.microsoft.com/en-us/research/publication/password-guidance/

XREF для создания новых пользователей

11 Настройка кодов карт

Кодирование карт контроля доступа гарантирует уникальность всех данных карт.

Путь к диалоговому окну
Главное меню > **Конфигурация** > **Параметры** > **Конфигурация кодирования карты**
Ввод чисел в диалоговом окне
Чтобы избежать ошибок в кодировании карт все номера можно вводить в десятичных или шестнадцатеричных форматах. Выберите переключатели **Шестнадцатеричный** или **Десятичный** в соответствии с инструкциями производителя карт. Любые введенные ранее значения автоматически конвертируются внутри системы.
Основное диалоговое окно разделено на две группы, которые более подробно описаны ниже:

- **Кодировочные данные карты по умолчанию**
- **Проверять только значения членства**

Кодировочные данные карты по умолчанию
Используйте эти поля для определения значений параметров **Версия**, **Код страны** и **Код объекта**, которые присваиваются номеру карты, когда карта регистрируется в системе. Если карта регистрируется вручную на рабочей станции оператора, отображается диалоговое окно со значениями по умолчанию, которые можно настроить для каждой карты.

Полный номер карты (по умолчанию)	Вводится только код сооружения (шестнадцатеричный или десятичный).  **Ввод данных кодирования** Код сооружения предоставляется производителем как десятичное значение: 56720 Установите переключатель **Десятичное** и введите код сооружения. Нажмите кнопку «Применить», чтобы сохранить данные.
Разделенный номер карты	Версию, код страны и код сооружения необходимо ввести как **десятичные значения**.  **Ввод данных кода:** Эти данные предоставляются производителем в виде следующих десятичных значений:

	Версия: 2 Код страны: 99 Код помещения: 56720 Введите данные в соответствующие текстовые поля. Нажмите кнопку «Применить», чтобы сохранить данные.

Примечания по вводу данных кодов по умолчанию

Данные по умолчанию хранятся в реестре операционной системы, а номер каждого бэйджа добавляется во время кодирования. Регистрация принимает вид **8-значного шестнадцатеричного** значения с начальными нулями, если необходимо.

Если номера кодов переданы полностью, система может преобразовывать десятичные значения в шестнадцатеричные, дополняя до 8 разрядов начальными нулями, и сохранить соответствующий системный параметр.

- Пример:
  - Ввод: 56720
  - Преобразование: DD90
  - Сохранено как: 0000DD90

Если номера кодов переданы отдельно (раздельная форма), тогда используется только **десятичный формат**. Они преобразуются в 10-значное десятичное число, которое строится следующим образом:

- Версия: 2 цифры
- Код страны: 2 цифры
- Код помещения: 6 цифр
- Если какие-либо из этих 10 цифр пусты, они заполняются начальными нулями.
  - Пример: 0299056720

Такое 10-значное десятичное значение преобразуется для хранения в 8-значное шестнадцатеричное значение.

- Пример:
  - Десятичное: 0299056720
  - Шестнадцатеричное: 11D33E50

Замечание!

Система проверяет шестнадцатеричные значения в случае разделенных номеров кодов, чтобы предотвратить ввод недопустимых кодов стран (превышающих шестнадцатеричное 63 или десятичное 99) и недопустимых кодов объекта (превышающих шестнадцатеричное F423F или десятичное 999 999)

Замечание!

Если запись карты осуществляется посредством подключенного диалогового считывателя, тогда значения по умолчанию назначаются автоматически. В случае записи из считывателя невозможно перезаписать значения по умолчанию.

Для этого тип записи следует переключить на **Диалоговое окно**.

При ручном вводе номера карты используется десятичный формат.

При сохранении данных создается 10-значное десятичное значение (с начальными нулями), которое затем преобразуется в 8-значное шестнадцатеричное значение. Это значение сохраняется вместе с данными кода по умолчанию как 16-значный номер кода карты.

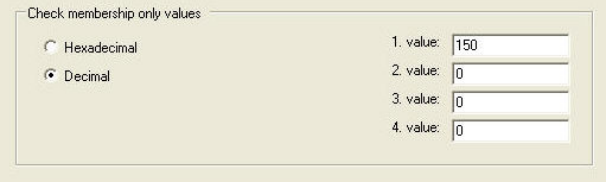
- Пример:
  - Ввод номера корты: 415
  - 10-значный: 0000000415

– Преобразовано в шестнадцатеричное значение: 0000019F
– Комбинируется с данными кодов по умолчанию (см. выше) и сохраняется как номер кода бэйджа: 11D33E500000019F

Проверять только значения членства

Проверка только значений членства означает, что учетные данные проверяются только на членство в компании или организации, а не с целью идентификации индивида. Следовательно, не используйте значение **Проверять только значения членства** для считывателей, предоставляющих доступ к зонам повышенной безопасности.

Эта группа параметров используется для ввода четырех кодов компании или клиента. Данные можно вводить в десятичном или шестнадцатеричном, однако в реестре операционной системы они сохраняются в виде десятичных значений.



Выберите считыватель в редакторе устройств, DevEdit, и активируйте параметр считывателя **Проверка членства**.
Из данных карты только коды компании или клиента считываются и сравниваются с сохраненными значениями.

Замечание!
Проверка членства работает только с описаниями карт, которые предопределены в системе (серый фон), а не с пользовательскими определениями.

12 Настройка контроллеров

Введение

Контроллеры в системе контроля доступом представляют собой виртуальные и физические устройства, которые отправляют команды на периферийное оборудование на входах (считывателях и дверях) и отправляют запросы со считывателей и дверей на централизованное программное обеспечение по принятию решений.

Хранилище контроллеров копирует определенную информацию об устройстве и владельце карты из централизованного ПО и, если эта функция настроена, может принимать решения в области контроля доступа даже в случае временной изоляции от централизованного ПО.

Программное обеспечение для принятия решений — это Система управления данными.

Существуют контроллеры двух типов:

– Главный контроллер доступа, известный как MAC, и его резервный дубликат RMAC.
– Локальные контроллеры доступа, известные как LAC или AMC.

Контроллеры настроены в редакторе устройств, DevEdit

Путь к диалоговому окну редактора устройств

Главное меню > **Конфигурация** > **Данные устройств** > **Дерево устройств** 

Использование редактора устройств, DevEdit

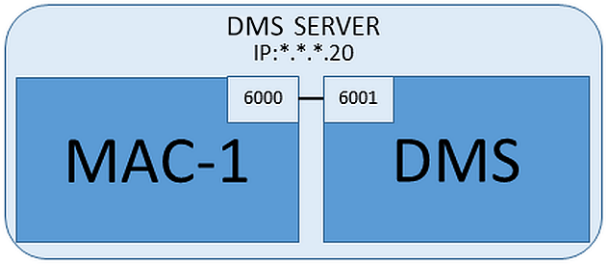
Базовое использование DevEdit описано в разделе **Использование редактора устройств** по ссылке ниже.

См.

– *Использование редактора устройств, Страница 21*

12.1 Настройка контроллеров MAC и RMAC

12.1.1 Настройка контроллера MAC на сервере DMS



Минимальная конфигурация системы требует наличия всего одного контроллера MAC. В этом случае контроллер MAC может находиться на сервере DMS.

Процедура

Откройте редактор устройств на сервере DMS и создайте контроллер MAC в дереве устройств, как описано в разделе **Использование редактора устройств**.

Выберите контроллер MAC в редакторе устройств. На вкладке **MAC** укажите значения следующих параметров:

Параметр	Описание
Имя	Имя, которое должно отображаться в дереве устройств, например MAC-1.

Параметр	Описание
Описание	Необязательное описание для системных операторов
С контроллером RMAC (флажок)	**<Оставить пустым>**
RMAC-порт	**<Оставить пустым>**
Активен (флажок)	**Снимите** этот флажок, чтобы временно приостановить синхронизацию в реальном времени между этим контроллером MAC и системой DMS. Это может быть полезным после обновлений системы DMS в крупных системах, поскольку позволяет избежать одновременного перезапуска всех контроллеров MAC.
Загружать устройства (флажок)	**Снимите** этот флажок, чтобы временно приостановить синхронизацию в реальном времени между этим контроллером MAC и подчиненными устройствами. Это позволяет быстрее открывать контроллер MAC в редакторе устройств.
IP-адрес	`Localhost 127.0.0.1`
Часовой пояс	**ВАЖНО!** Часовой пояс контроллера MAC и всех подчиненных контроллеров AMC.
Подразделение	Подразделение, к которому относится контроллер MAC (если применимо).

Поскольку у этого локального контроллера MAC нет избыточных контроллеров MAC, обеспечивающих отказоустойчивость, то запускать для него средство MACInstaller не требуется. Просто оставьте поля для двух параметров RMAC на вкладке **MAC** пустыми.

12.1.2 Подготовка компьютеров сервера MAC к работе контроллеров MAC и RMAC

В этом разделе описана подготовка компьютеров к использованию в качестве серверов MAC.

По умолчанию первый контроллер MAC в системе Access Engine выполняется на том же компьютере, что и сервер DMS, однако в целях обеспечения дополнительной устойчивости рекомендуется, чтобы контроллер MAC выполнялся на отдельном компьютере, который сможет принять на себя задачи по контролю доступа в случае сбоя компьютера DMS.

Отдельные компьютеры, где расположены контроллеры MAC или RMAC, называются серверами MAC независимо от того, какой контроллер на них расположен: MAC или RMAC.

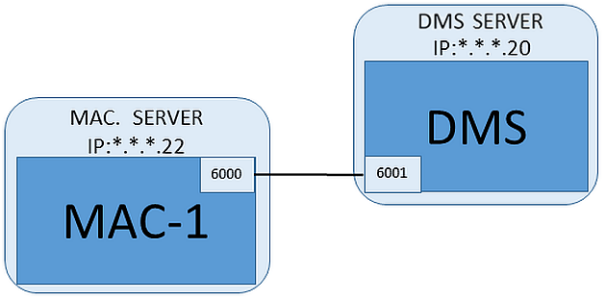
В целях обеспечения отказоустойчивости контроллеры MAC и RMAC **должны** выполняться на отдельных серверах MAC.

Убедитесь, что на всех соответствующих серверах MAC соблюдаются следующие условия:

1. На всех серверах установлена операционная система той же версии, что и на сервере DMS, с актуальными обновлениями Windows.
2. Администратор на всех серверах имеет один и тот же пароль

3. Вы выполнили вход в систему как администратор (при работе с MSTC используйте только сессии /Admin /Console)
4. Отключите IPv6. Запомните IPv4-адрес каждого сервера.
5. Включите .NET 3.5 на всех соответствующих компьютерах.
   Примечание. В Windows 7 компонент устанавливается. В операционных системах Windows 10 и Windows Server компонент активируется в качестве дополнительного
6. Перезагрузите компьютер

12.1.3 Настройка контроллера MAC на собственном сервере MAC



– Сервер MAC подготовлен в соответствии с описанием в разделе Подготовка компьютеров сервера MAC к работе контроллеров MAC и RMAC

1. На сервере DMS деактивируйте контроллер MAC, сняв флажки **Активировать** и **Загрузить устройства** для данного контроллера MAC в редакторе устройств.
2. На сервере MAC остановите работу контроллера MAC с помощью программы Windows `services.msc`.
3. Запустите `MACInstaller.exe`
   – Для ACE этот файл находится на установочном носителе BIS `\AddOns\ACE\MultiMAC\MACInstaller` (см. раздел Использование инструмента MACInstaller ниже).
   –
4. Выполните инструкции, которые отображаются в инструменте, указав значения для следующих параметров.

Номер экрана	Параметр	Описание
1	**Папка назначения**	Локальный каталог для установки контроллера MAC. По возможности используйте значения по умолчанию.
2	**Сервер**	Имя или IP-адрес сервера, на котором запущен DMS.
2	**Порт (порт для DMS)**	Порт на сервере DMS, который будет использоваться для получения данных от контроллера MAC**.** Используйте порт 6001 для первого

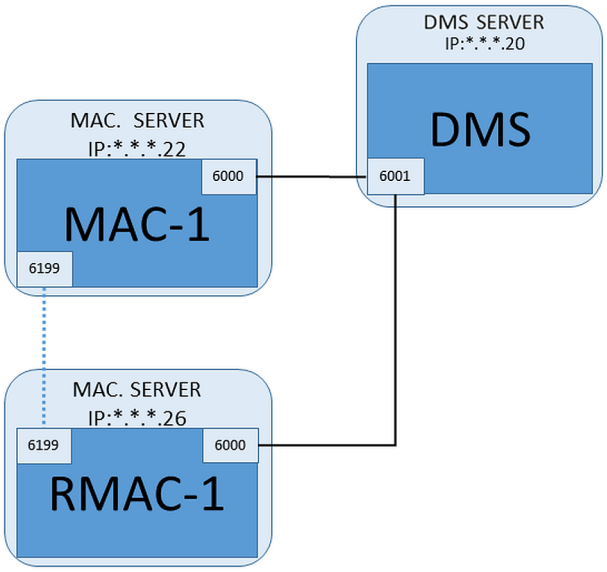
Номер экрана	Параметр	Описание
		контроллера MAC на сервере DMS, а для каждого последующего контроллера MAC — порт с номером на 1 больше.
2	**Номер (системный номер MAC)**	Задайте 1 для этого и всех остальных контроллеров MAC (в отличие от RMAC)**.**
2	**Пара (имя или IP-адрес контроллера-партнера MAC)**	Оставьте это поле пустым, если контроллеру MAC не должен соответствовать контроллер RMAC.
2	**Только настройка** (переключатель)	Не устанавливайте этот переключатель, потому что вы не настраиваете контроллер MAC на главном сервере входа DMS.
2	**Обновление программного обеспечения** (переключатель)	Установите этот переключатель, потому что вы настраиваете MAC на соответствующем компьютере (сервере MAC), а не на главном логин-сервере DMS.

5. Завершив работу инструмента, перезагрузите сервер MAC или запустите контроллер MAC на сервере MAC с помощью программы Windows `services.msc`.
6. На сервере DMS в редакторе устройств выберите MAC.
7. На вкладке **MAC** укажите значения следующих параметров:

Параметр	Описание
Имя	Имя, которое должно отображаться в дереве устройств, например MAC-1.
Описание	Необязательное описание для операторов ACE
С контроллером RMAC (флажок)	**<Оставить пустым>**
RMAC-порт	**<Оставить пустым>**
Активен (флажок)	Сейчас следует установить этот флажок
Загружать устройства (флажок)	Сейчас следует установить этот флажок
IP-адрес	IP-адрес сервера MAC (компьютера).
Часовой пояс	**ВАЖНО!** Часовой пояс контроллера MAC и всех подчиненных контроллеров AMC.
Подразделение	Подразделение ACE, к которому относится контроллер MAC (если применимо).

12.1.4 Добавление контроллеров RMAC к MAC

Замечание!
Не добавляйте контроллеры RMAC к стандартным контроллерам MAC, пока не убедитесь, что последние установлены и функционируют правильно.
В противном случае это может помешать репликации данных или повредить данные.



– Контроллер MAC для данного контроллера RMAC установлен, как описано в предыдущих разделах, и функционирует правильно.
– Компьютер сервера MAC для контроллера RMAC подготовлен, как описано в разделе Подготовка компьютеров сервера MAC к работе контроллеров MAC и RMAC

Контроллеры MAC могут быть задублированы избыточными контроллерами MAC (RMAC), обеспечивая отказоустойчивость и, следовательно, более надежную работу контроля доступа. В этом случае данные контроля доступа автоматически реплицируются между двумя контроллерами. Если в одном из контроллеров пары возникает сбой, другой контроллер принимает на себя управление локальными контроллерами доступа в его ведении.

На сервере DMS в BIS конфигураторе

1. В редакторе устройств выберите контроллер MAC, для которого необходимо добавить контроллер RMAC.
2. На вкладке **MAC** измените значения следующих параметров:

Параметр	Описание
С контроллером RMAC (флажок)	**Снимите** этот флажок и не устанавливайте его до тех пор, пока на сервере резервного подключения не будет установлен соответствующий контроллер RMAC
Активен (флажок)	**Снимите** этот флажок, чтобы временно приостановить синхронизацию в реальном времени между этим контроллером MAC и системой DMS. Это может быть полезным после обновлений системы DMS в крупных системах, поскольку позволяет избежать одновременного перезапуска всех контроллеров MAC.

Параметр	Описание
Загружать устройства (флажок)	**Снимите** этот флажок, чтобы временно приостановить синхронизацию в реальном времени между этим контроллером MAC и подчиненными устройствами. Это позволяет быстрее открывать контроллер MAC в редакторе устройств.

3. Нажмите кнопку **Применить**
4. Не закрывайте редактор устройств, так как мы к нему скоро вернемся.

На сервере MAC для MAC

Чтобы перенастроить контроллер MAC для взаимодействия с RMAC выполните следующие действия.

– На ранее подготовленном компьютере сервера MAC запустите инструмент MACInstaller (см. раздел Использование инструмента MACInstaller) и задайте следующие параметры:
  – **Сервер**: имя или IP-адрес компьютера сервера DMS
  – **Порт**: `6001`
  – **Номер**: `1` (все контроллеры MAC имеют номер 1)
  – **Пара**: IP-адрес компьютера, на котором будет выполняться контроллер RMAC.
  – **Обновление программного обеспечения**: установите этот флажок, так как вы настраиваете сервер MAC, а не DMS.

На сервере MAC для RMAC

Для настройки сервера RMAC выполните следующие действия.

– На отдельном и ранее подготовленном компьютере сервера MAC запустите инструмент MACInstaller (см. раздел Использование инструмента MACInstaller) и задайте следующие параметры:
  – **Сервер**: имя или IP-адрес компьютера сервера DMS
  – **Порт**: `6001` (такой же, как для контроллера MAC)
  – **Номер**: `2` (все контроллеры RMAC имеют номер 2)
  – **Пара**: IP-адрес компьютера, где работает парный контроллер MAC.
  – **Обновление программного обеспечения**: установите этот флажок, так как вы настраиваете сервер MAC, а не DMS.

Вернитесь в редактор устройств на сервере DMS

1. **ВАЖНО!** Убедитесь, что контроллеры MAC и RMAC на соответствующих компьютерах функционируют и видны друг другу в сети.
2. На вкладке **MAC** измените параметры следующим образом:

Параметр	Описание
С контроллером RMAC (флажок)	**Выбранные** Новая вкладка с меткой **RMAC** отображается рядом с вкладкой **MAC**.
RMAC-порт	`6199` (статический по умолчанию) Все контроллеры MAC и RMAC используют этот порт, чтобы проверить, что их партнеры функционируют и доступны**.**

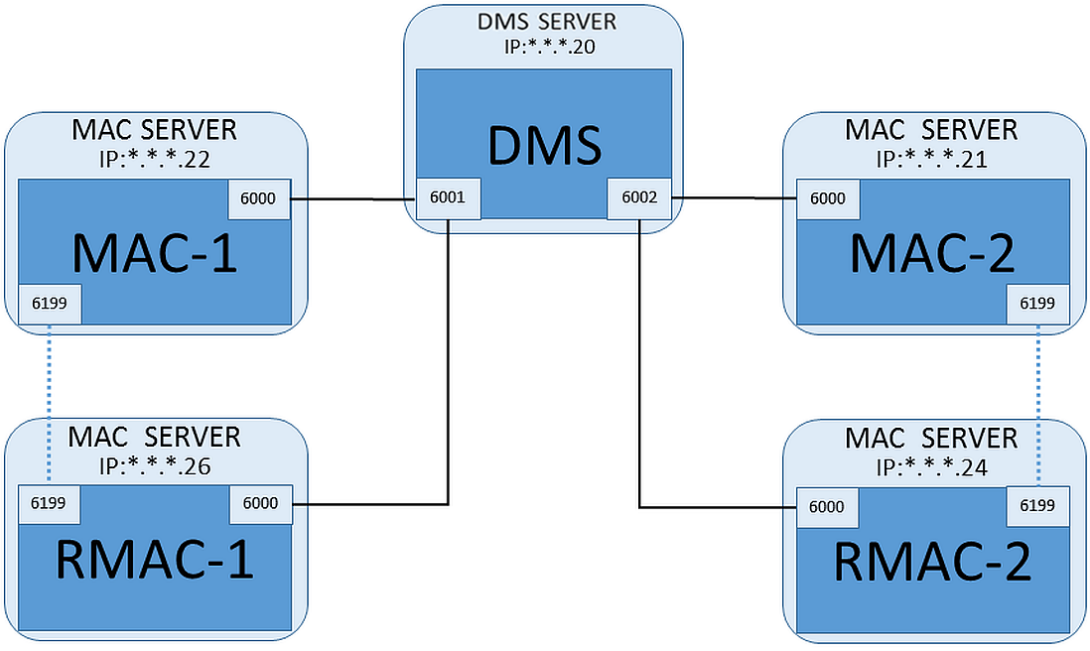
Параметр	Описание
Активен (флажок)	**Выбранные** Позволяет осуществлять синхронизацию между этим контроллером MAC и подчиненными устройствами.
Загружать устройства (флажок)	**Выбранные** Сокращает время, необходимое для открытия контроллера MAC в редакторе устройств.

3. На вкладке **RMAC** укажите значения следующих параметров:

Параметр	Описание
Имя	Имя, которое должно отображаться в дереве устройств. Например, если соответствующий контроллер MAC имеет имя MAC-01, контроллеру RMAC можно присвоить имя RMAC-01
Описание	Дополнительная документация для операторов ACE
IP-адрес	IP-адрес контроллера RMAC
MAC-порт	`6199` (статический по умолчанию) Все контроллеры MAC и RMAC используют этот порт, чтобы проверить, что их партнеры функционируют и доступны**.**

12.1.5 Добавление других пар контроллеров MAC/RMAC

В зависимости от числа контролируемых входов и необходимого уровня отказоустойчивости в системную конфигурацию можно добавить большое количество пар MAC/RMAC. Чтобы узнать точное количество пар, поддерживаемых в вашей версии, обратитесь к соответствующему краткому описанию.



Для каждой дополнительной пары MAC/RMAC...

1. Подготовьте отдельные компьютеры для контроллеров MAC и RMAC, как описано в разделе Подготовка компьютеров сервера MAC к работе контроллеров MAC и RMAC

2. Настройте контроллер MAC, как описано в разделе Настройка контроллера MAC на собственном сервере MAC
3. Настройте RMAC для этого контроллера MAC, как описано в разделе Добавление контроллеров RMAC к MAC

Обратите внимание, что каждая пара MAC/RMAC передает данные на отдельный порт на сервере DMS. Следовательно, для параметра **Порт (порт для DMS)** в `MACInstaller.exe` используйте следующее:

– `6001` для обоих компьютеров в первой паре MAC/RMAC
– `6002` для обоих компьютеров во второй паре MAC/RMAC
– и т. д.

В редакторе устройств порт `6199` можно всегда использовать для параметров **MAC-порт** и **RMAC-порт**. Номер порта зарезервирован для подтверждения в каждой паре MAC/RMAC, с помощью которого каждый контроллер будет знать, доступен ли его партнер.

Замечание!
Повторная активация контроллеров MAC после обновления системы
После обновления системы контроллеры MAC и зависимые от них AMC по умолчанию деактивированы. Не забудьте повторно активировать их в конфигураторе, установив соответствующие флажки в редакторе устройств.

12.1.6 Использование средства установки MAC

`MACInstaller.exe` — это стандартный инструмент для настройки и повторной настройки контроллеров MAC и RMAC на соответствующих компьютерах (MAC-серверах). Инструмент собирает значения параметров для контроллера MAC или RMAC и вносит необходимые изменения в реестр Windows.

Замечание!
Поскольку инструмент вносит изменения в реестр Windows, перед перенастройкой контроллера MAC необходимо остановить все выполняемые с его участием процессы.

Инструмент MACInstaller доступен на установочном носителе BIS по следующему пути:
`\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe`
Инструмент собирает значения для параметров ниже с помощью нескольких экранов.

Номер экрана	Параметр	Описание
1	**Папка назначения**	Локальный каталог для установки контроллера MAC.
2	**Сервер**	Имя или IP-адрес сервера, на котором запущен DMS.
2	**Порт (порт для DMS)**	Номер порта на сервере DMS; этот порт будет использоваться для связи между контроллером MAC и DMS. **См. подробные сведения ниже.**

Номер экрана	Параметр	Описание
2	**Номер (системный номер MAC)**	Задайте значение 1 для всех исходных контроллеров MAC. Задайте 2 для всех резервных контроллеров MAC (RMAC).
2	**Пара (имя или IP-адрес контроллера-партнера MAC)**	IP-адрес компьютера, где будет работать резервный партнер для этого сервера MAC. Если неприменимо, оставьте это поле пустым.
2	**Только настройка** (переключатель)	Выберите этот параметр, если выполняется перенастройка контроллера MAC на главном сервере DMS. **См. подробные сведения ниже**
2	**Обновление программного обеспечения** (переключатель)	Выберите этот параметр, если выполняется установка или перенастройка контроллера MAC на собственном компьютере (сервере MAC), а не на главном сервере входа DMS. **См. подробные сведения ниже**

Номера портов присваиваются по следующей схеме нумерации:

– В неиерархической системе, где существует только один сервер DMS, каждый контроллер MAC и соответствующий ему RMAC передает данные с одного и того же номера порта (как правило, 6000). В один момент времени DMS может взаимодействовать только с одним из контроллеров в паре MAC/RMAC.
– DMS получает сигналы от первого контроллера MAC или пары MAC/RMAC в порту 6001, от второго контроллера MAC или пары MAC/RMAC в порту 6002 и т. д.

Замечание!
Порт приемника DMS в иерархических системах
Обратите внимание, что схема нумерации портов приемника DMS в иерархических системах отличается от описанной выше. См. подробные сведения в разделе Контроллеры MAC и RMAC в иерархических топологиях

Этот параметр позволяет различать исходные контроллеры MAC и резервные контроллеры RMAC:

– Все исходные контроллеры MAC имеют номер 1.
– Все резервные контроллеры MAC (RMAC) имеют номер 2

Выберите этот параметр, чтобы изменить конфигурацию существующего контроллера MAC на главном сервере DMS, в частности проинформировать контроллер о только что установленном на другом компьютере резервном контроллере RMAC.
В этом случае введите IP-адрес или имя хоста контроллера RMAC в поле параметра **Пара**.

Выберите этот параметр на компьютере, отличном от главного сервера DMS, чтобы установить контроллер RMAC или изменить его конфигурацию.
В этом случае введите IP-адрес или имя хоста парного контроллера MAC этого контроллера RMAC в поле параметра **Пара**.

12.2 Настройка LAC

Создание локального контроллера доступа AMC

Модульные контроллеры доступа (AMC) подчиняются главным контроллерам доступ (MAC) в редакторе устройств.

Чтобы создать контроллер AMC, выполните следующие действия:

1. В редакторе устройств щелкните контроллер MAC правой кнопкой мыши и в контекстном меню выберите **Новый объект**
   или
2. Нажмите кнопку ✚.
3. Выберите один из следующих типов AMC в отобразившемся диалоговом окне:

AMC 4W (по умолчанию)	с четырьмя интерфейсами считывателей Wiegand для подключения до четырех считывателей
AMC 4R4	с четырьмя интерфейсами считывателей RS485 для подключения до восьми считывателей

Результат: в иерархии DevEdit создается новая запись AMC выбранного типа

AMC2 4W	**Модульный контроллер доступа** с четырьмя считывателями Wiegand.	Можно настроить не более четырех считывателей Wiegand для подключения к 1–4 проходам. Данный контроллер поддерживает восемь входных и восемь выходных сигналов. При необходимости платы расширения могут обеспечить до 48 дополнительных входных и выходных сигналов.
AMC2 4R4	**Модульный контроллер доступа** с четырьмя интерфейсами считывателей RS485	Можно настроить не более восьми считывателей RS485 для подключения к 1–8 проходам. Данный контроллер поддерживает восемь входных и восемь выходных сигналов. При необходимости платы расширения могут обеспечить до 48 дополнительных входных и выходных сигналов.
AMC2 8I-8O-EXT	Плата расширения для AMC с восемью входными и выходными сигналами	Делает доступными дополнительные сигналы. К AMC можно подключить до трех плат расширения.
AMC2 16I-16O-EXT	Плата расширения для AMC с 16 входными и выходными сигналами	

AMC2 8I-8O-4W	Плата расширения для Wiegand AMC с восемью входными и выходными сигналами	

Активация/деактивация контроллеров

Изначально при создании нового контроллера для него выбран (флажок) следующий параметр: **Связь с хостом включена**.

Это открывает сетевое соединение между MAC и контроллерами, так что любые измененные или расширенные данные конфигурации автоматически распространяются на контроллеры.

Отключите этот параметр, чтобы сохранить пропускную способность сети, и таким образом повысить производительность, создавая несколько контроллеров и зависимых от них устройств (входы, двери, считыватели, платы расширения). В редакторе устройств эти устройства затем помечены затененными значками.

ВАЖНО! Не забудьте снова включить этот параметр по окончании конфигурации устройств. Это позволит непрерывно обновлять контроллеры с любыми изменениями конфигурации, выполненными на других уровнях.

Использование разных типов контроллеров в одной установке

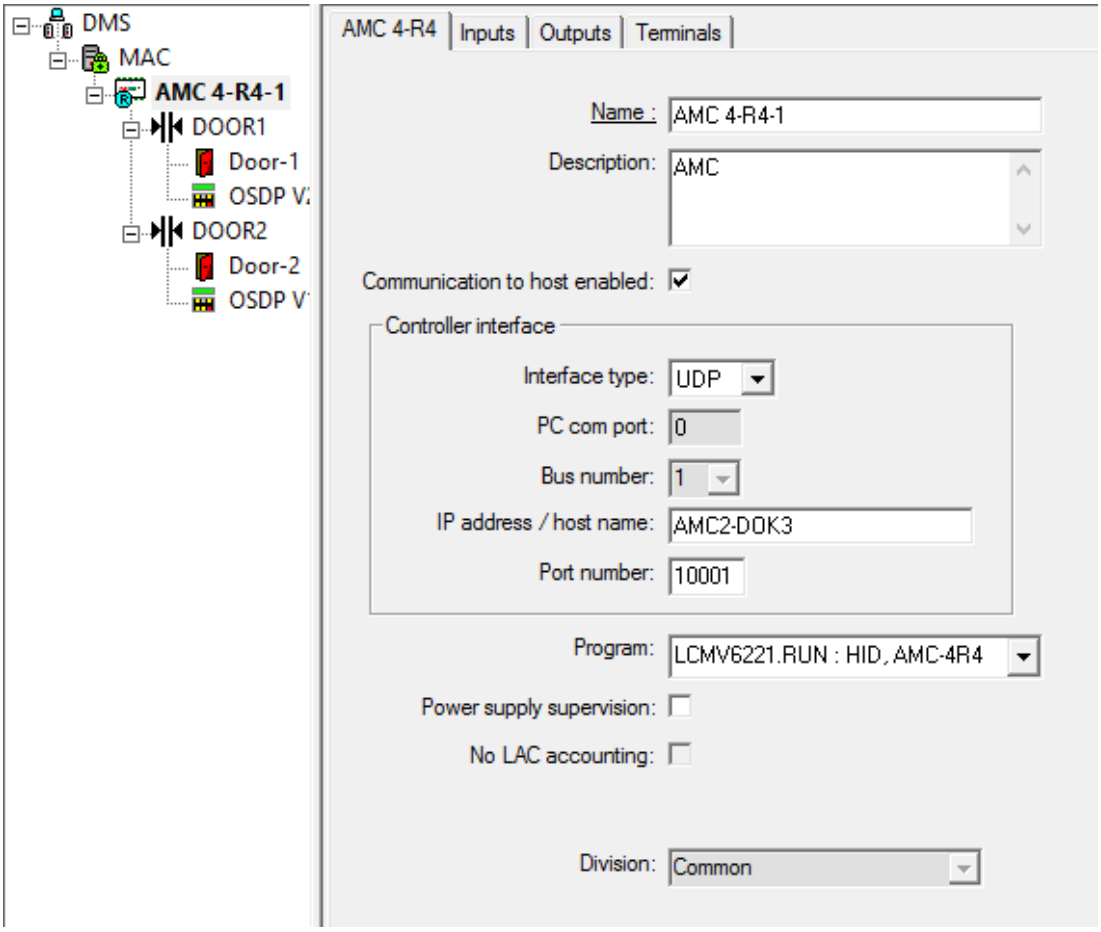
Системы управления доступом обычно оснащаются контроллером и считывателем лишь одного типа.

В результате обновления программного обеспечения и расширения установок может потребоваться дополнить существующие аппаратные компоненты новыми. Возможны даже конфигурации, объединяющие варианты RS485 (AMC 4R4) с вариантами Wiegand (AMC 4W), если учитываются следующие предостережения:

– считыватели RS485 передают "телеграмму", содержащую номер кода;
– считыватели Wiegand передают свои данные таким образом, что их необходимо декодировать с помощью определения бэйджа, чтобы сохранить правильную форму номера кода;
– смешанный режим работы контроллеров может функционировать только в том случае, если оба номера кодов построены одинаково.

12.2.1 Параметры и настройки AMC

Основные параметры AMC



Настройка параметров AMC

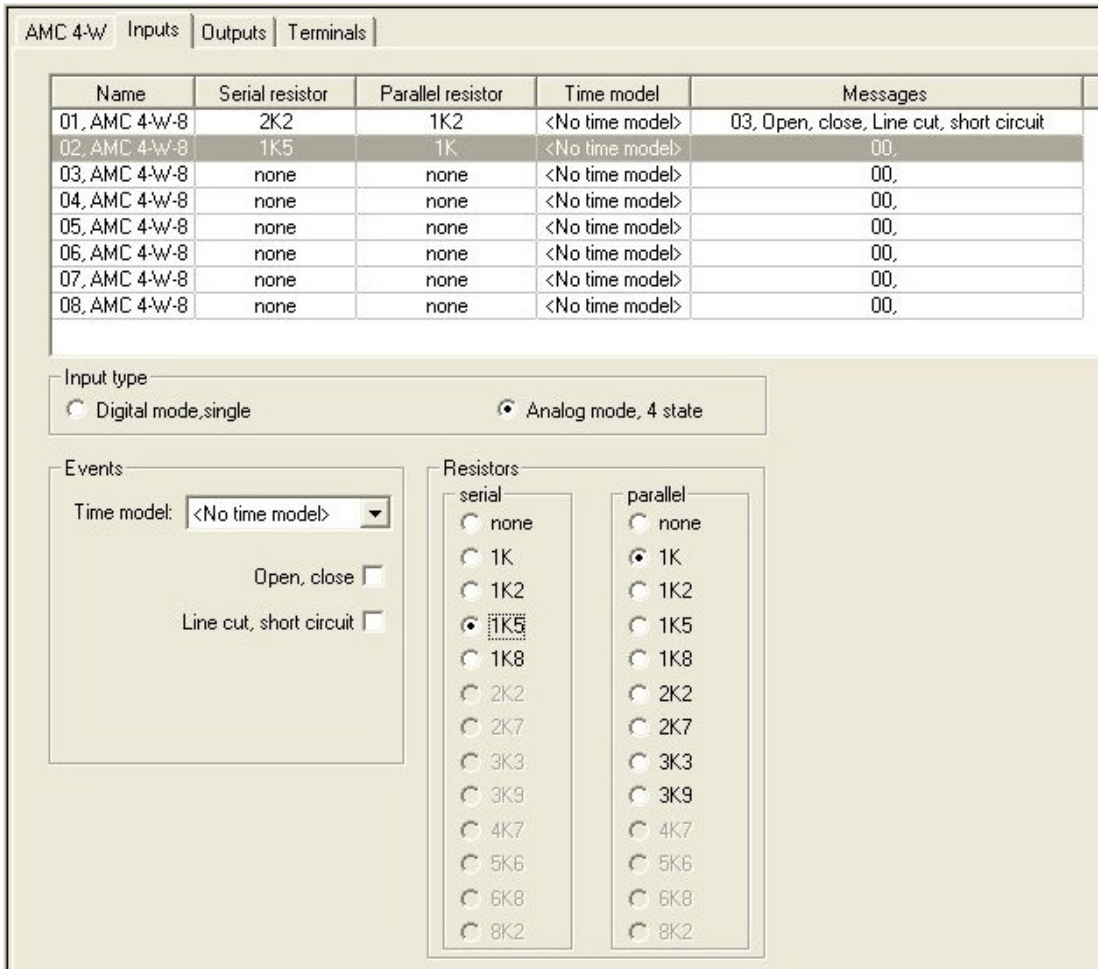
Параметр	Возможные значения	Описание
Имя контроллера	алфавитно-цифровое значение, ограничение: 1–16 знаков	Создание идентификаторов (по умолчанию) гарантирует уникальность имен, но их можно перезаписать по отдельности. В случае перезаписи имени за уникальность идентификаторов отвечает пользователь. Поэтому рекомендуется для сетевых подключений к DHCP-серверам использовать сетевое имя.
Описание контроллера	алфавитно-цифровое значение: 0–255 знаков	Этот текст отображается в данном ответвлении OPC.
Связь с хостом активирована	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Значение по умолчанию = активно Данный флажок отображает текущую настройку, а также позволяет ее изменить. На состояние подключения к хосту указывают следующие значки в Проводнике: Вариант контроллера:

		активно не активно AMC2 4W   AMC2 4R4   Деактивация позволяет создавать и параметризовать устройства, которые требуется включить в систему управления доступом позднее. Эти устройства не следует активировать и, следовательно, добавлять в базу данных хоста, пока они не будут введены в эксплуатацию. Это также сокращает бесполезные опросы устройств хостом.  В целях безопасности после обновления программного обеспечения все контроллеры переводятся в автономный режим (флажок снят). Это гарантирует, что установка может продолжать работать со старым программным обеспечением, а новое программное обеспечение можно вводить в действие постепенно. Новые контроллеры следует включать в установку постепенно, устанавливая соответствующие флажки.
Интерфейс контроллера		
Тип интерфейса	COM UDP	COM, где подключение к AMC осуществляется через один из COM-портов MAC. UDP (= User Datagram Protocol), где подключение осуществляется через сеть. Там, где выбран данный тип подключения, можно настроить параметры "имя хоста" (host name) и "дистанционно управляемый порт (remote-controlled port)".

		 Для типа интерфейса "UDP" на AMC **необходимо** задать DIP-переключатель "5". Также рекомендуется установить переключатель "1" в положение ВКЛ (ON).
COM-порт компьютера:	числовое значение: с COM-портами: 1–256 с UDP-портами: 1–65535	Число COM-портов, через которые данный AMC подключается к MAC. Для подключений Ethernet через преобразователи создаются виртуальные COM-порты и отображаются здесь. Для типа "UDP" введите порт, через который MAC будет принимать информацию от AMC. Если этот порт неизвестен, поле можно оставить пустым. Свободный порт будет выбран автоматически.
Номер шины	числовое значение: 1–8	С помощью интерфейсного адаптера AMC-MUX на одном COM-порте можно настроить до 8 контроллеров. В таких случаях введите уникальный адрес каждого AMC, как задано его DIP-переключателем. **Примечание.** Переключатель 5 здесь можно игнорировать, так как для адресации используются только первые четыре переключателя. Для соединений UDP используется настройка по умолчанию (=0)
IP-адрес/ имя хоста	Сетевое имя или IP-адрес AMC	Это поле ввода доступно только в случае, если выбран тип портов **UDP**. Если IP-адреса назначаются DHCP-сервером, то следует предоставить сетевое имя AMC, чтобы AMC можно было найти после перезапуска, даже если изменился IP-адрес. Для сетей без DHCP необходимо задавать IP-адрес.
UDP-порт	числовое значение: 1–10001 в конфигурации по умолчанию	Это поле ввода активно, только если выбран тип портов **UDP**. Это порт AMC, через который принимаются MAC-сообщения.

Другие параметры		
Программа	алфавитно-цифровое значение	Имя файла программы, который требуется загрузить в AMC. Доступные программы находятся в MAC в каталоге BIN. Их можно выбрать из списка. Для удобства также отображаются протокол и описание. Этот дополнительный параметр настраивается автоматически, так как программы загружаются автоматически в зависимости от подключенных считывателей. В случае несоответствия считывателя/программы значение параметра перезаписывается.
Контроль питания	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Контроль напряжения питания. В случае отказа источника питания генерируется информационное сообщение. Наличие ИБП (источника бесперебойного питания) — обязательное условие использования функции контроля, чтобы можно было выдать сообщение. 0 = без контроля 1 = контроль активирован
Без учета LAC	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Установите этот флажок для устройств AMC, работающих совместно для обеспечения доступа к парковкам, где учет входящих и исходящих элементов осуществляется только родительским контроллером MAC. **Примечание**: если эта опция выбрана, и контроллер AMC находится в автономном режиме, AMC не сможет предотвращать доступ к переполненным областям, так как у него нет доступа к полным данным о количестве элементов.
Подразделение	Значение по умолчанию = общее	Это информационное поле доступно только для чтения. «Подразделения» означают разделение установок контроля доступа между несколькими автономными участками, создаваемыми и обслуживаемыми в BIS менеджере.

Настройка входов AMC



Это диалоговое окно разделено на четыре части:

- Список входов по имени
- Типы входа
- События, о которых сообщается входами
- Типы резисторов, используемых в аналоговом режиме

Параметры входов

Параметры входов AMC описаны в следующей таблице:

Имя столбца	Описание
Имя	Нумерация входа (от 01 до 08) и имя соответствующего AMC или AMC-EXT.
Последовательный резистор	Отображается заданное значение последовательного резистора. "нет" (none) или "---" = цифровой режим
Параллельный резистор	Отображается заданное значение параллельного резистора. "нет" (none) или "---" = цифровой режим
Временная модель	Имя выбранной временной модели

Сообщения	Номер контрольного документа и обозначение сообщений, которые будут генерироваться 00 = нет сообщений 01 = если были активированы события **Открыть**, **Закрыть** 02 = если были активированы события **Разрыв линии**, **Короткое замыкание** 03 = если были активированы оба варианта событий
Назначенный	При использовании модели прохода 15 отображается имя сигнала DIP.

Используйте клавиши Ctrl и Shift для одновременного выбора нескольких входов. Любые изменяемые вами значения будут применяться к выбранным входам.

События и временные модели

В зависимости от режима работы обнаруживаются и сообщаются следующие состояния дверей: **Открыто**, **Закрыто**, **Линия прервана** и **Короткое замыкание**.

Установите соответствующие флажки, чтобы сделать возможной передачу этих состояний в качестве событий контроллерами AMC в общую систему.

Выберите **Временную модель** из раскрывающегося списка с тем же именем, чтобы ограничить передачу событий периодами, которые определены моделью. Например, событие **Открыто** может иметь значение только в нерабочее время.

Тип входа

Резисторы могут работать в **Цифровом режиме** или **Аналоговом режиме (4 состояния)**.

Значение по умолчанию — **Цифровой режим**: обнаруживаются только состояния дверей **открыто** и **закрыто**.

В аналоговом режиме помимо этого обнаруживаются проводные состояния **Линия разорвана** и **Короткое замыкание**.

Дверь открыта	сумма значений последовательного (R_S) и параллельного (R_P) резисторов: $R_S + R_P$
Дверь закрыта	равно значениям последовательных резисторов: R_S
Разрыв цепи	сумма значений последовательного (R_S) и параллельного (R_P) резисторов стремится бесконечности.
Короткое замыкание	сумма значений последовательного (R_S) и параллельного (R_P) резисторов равна нулю.

Резисторы

По умолчанию для резисторов задаются значения «нет» или «---» (**цифровой режим**).

В **аналоговом режиме** значения для последовательных и параллельных резисторов можно задать, выбрав соответствующие переключатели.

отсутствует, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2 (при 100 Ом)

В зависимости от выбранного значения резистора для соответствующего резистора доступны лишь ограниченные диапазоны.

В таблицах ниже в левых столбцах показаны выбранные значения, а в правых столбцах указаны диапазоны, доступные другому резистору.

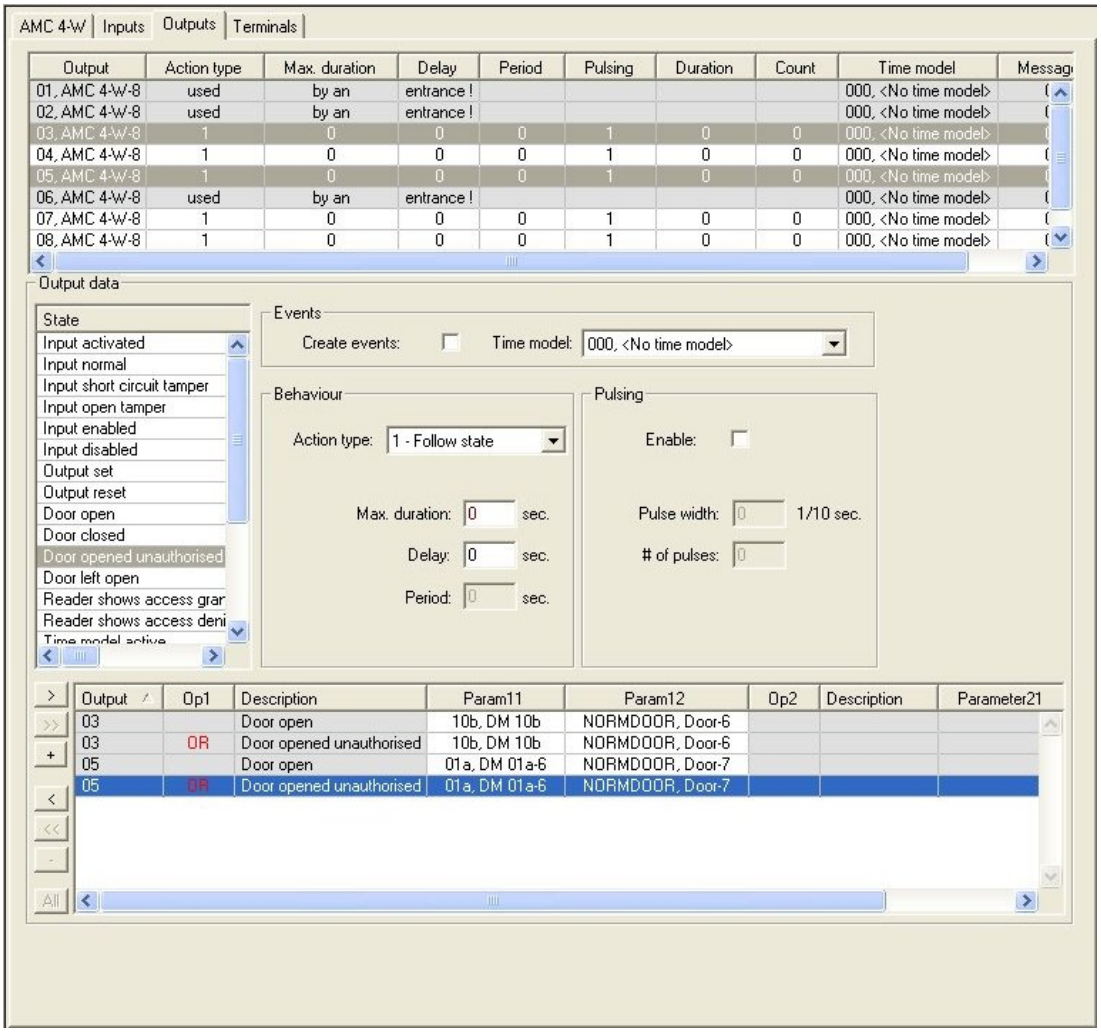
Последовательно	**Диапазон**		**Параллельно**	**Диапазон**

"нет" или "---"	1K – 8K2		"нет" или "---"	1K – 8K2
1K	1K – 2K2		1K	1K – 1K8
1K2	1K – 2K7		1K2	1K – 2K7
1K5	1K – 3K9		1K5	1K – 3K3
1K8	1K – 6K8		1K8	1K – 3K9
2K2	1K2 – 8K2		2K2	1K – 4K7
2K7	1K2 – 8K2		2K7	1K2 – 5K6
3K3	1K5 – 8K2		3K3	1K5 – 6K8
3K9	1K8 – 8K2		3K9	1K5 – 8K2
4K7	2K2 – 8K2		4K7	1K8 – 8K2
5K6	2K7 – 8K2		5K6	1K8 – 8K2
6K8	3K3 – 8K2		6K8	1K8 – 8K2
8K2	3K9 – 8K2		8K2	2K2 – 8K2

Настройка выходов AMC — Обзор

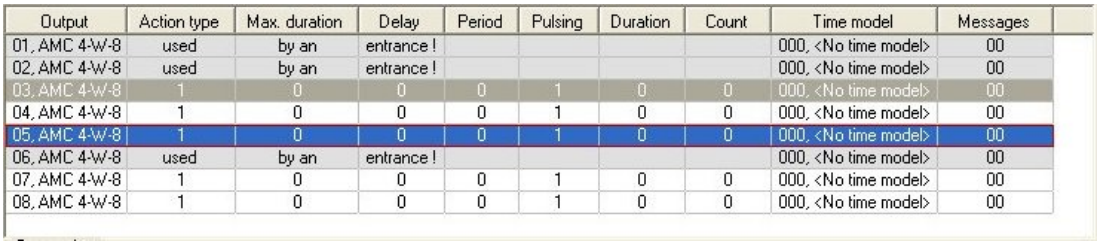
В этом диалоговом окне предоставляется конфигурация каждого выходного сигнала в AMC или AMC-EXT. Предусмотрены три основные области:

– поле списка с обзором заданного параметра для каждого выходного сигнала;
– параметры конфигурации для выходных сигналов, выбранных в списке;
– определение условий активации выходных сигналов.



Выбор выхода AMC в таблице

Для настройки контактов выхода необходимо сначала выбрать соответствующую строку в верхней таблице. Используйте клавиши Ctrl и Shift для одновременного выбора нескольких строк, если это необходимо. Изменения, вносимые вами в нижней части окна, отразятся только на выбранных вами выходах.



Строки, выходы которых уже были присвоены через модель двери, или другим способом, отображаются светло-серым цветом с сообщением «**используется проходом**». Такие выходы не подлежат дальнейшим изменениям.

Выбранные вами строки выделяются темно-серым цветом.

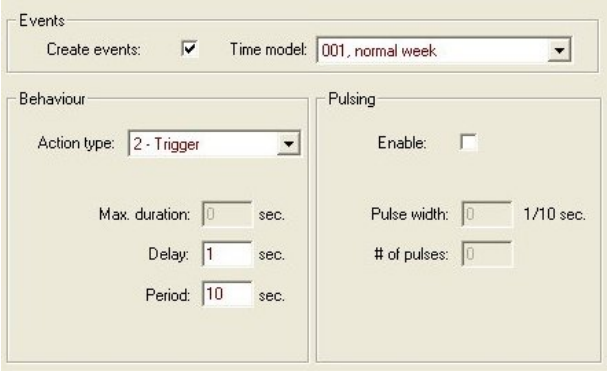
Параметры выходов AMC

Имя столбца	**Описание**
Выход	текущая нумерация выходов в соответствующих AMC или AMC-EXT

	01–08 с AMC и AMC_IO08 01–16 с AMC_IO16
Тип действия	указание выбранного типа действия 1 = По состоянию 2 = Триггер 3 = Переменный
Макс. продолжительность	длина сигнала в секундах [1–9999; 0 = всегда, если не появилось сообщение о преобразовании] — только с типом действия 1
задержка	задержка подачи сигнала в секундах [0–9999] — только с типами действия 1 и 2
период	период подачи сигнала в секундах — только с типом действия 2
Пульсация	активация импульса — в противном случае сигнал подается постоянно
Длит.	длина импульса
Кол-во	кол-во импульсов в секунду
Временная модель	имя выбранной временной модели
Сообщения	маркировка активности сообщений 00 = нет сообщений 03 = создаются сообщения о событиях
Назначенный	При использовании модели прохода 15 отображается имя сигнала DOP.

Выходы: события, поведение, пульсация

Все записи из приведенного выше списка создаются с помощью флажков и полей ввода в областях диалогового окна **События**, **Действие** и **Пульсация**. При выборе элемента списка в этих областях указываются соответствующие настройки. Это также верно для выбора нескольких элементов списка при условии, что все выбранные выходные сигналы имеют одинаковые параметры. Изменения настроек параметров применяются ко всем элементам, выбранным в данном списке.



Установите флажок **Создать события**, если необходимо отправлять сообщение для активированного выходного сигнала. Если такие сообщения должны отправляться только в особые промежутки времени, например только ночью или на выходных, можно назначить соответствующую **временную модель**.

Для отдельных типов действий можно задать следующие параметры:

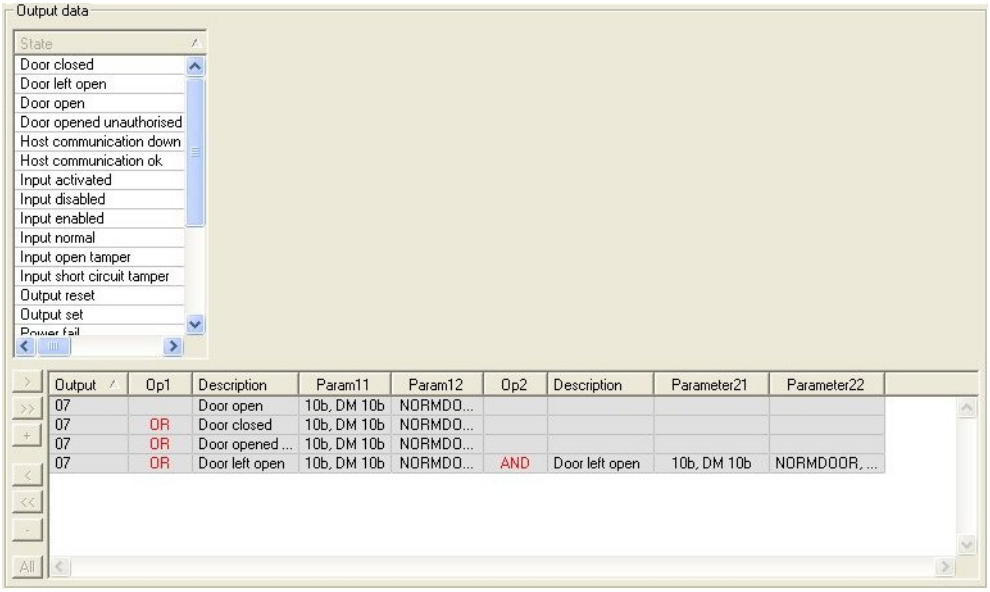
тип действия	макс. продолжительность	задержка	период	пульсация/ включено	длительность импульса	кол-во импульсов
Соответствие состоянию	0 = всегда 1 - 9999	0 - 9999	нет	да	1 - 9999	Нет
Триггер	нет	0 - 9999	0–9999 если пульсация **не** включена	Да отключает период	1 - 9999	1 - 9999
Переменный	нет	нет	нет	да	1 - 9999	нет

Выходные данные AMC

Нижняя часть диалогового окна **Выходы** содержит:

– список доступных **состояний** для выбранных выходов.

– таблицу с выходами и состояниями, настроенными для их инициирования.



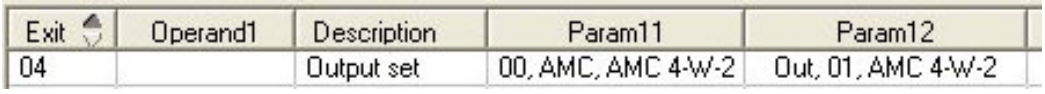
Настройка состояний для инициирования выходов

Вы можете изменить настройки выбранных выходов так, чтобы они инициировались отдельными состояниями или логическими комбинациями состояний.

– Выберите один или несколько выходов в верхнем поле списка.

– Выберите состояние из списка **состояний**.

– При наличии для выбранного статуса нескольких устройств или установок, которые могут передавать это состояние, рядом с кнопкой › активируется кнопка ». Щелкните › (или дважды щелкните статус), чтобы для каждого выбранного выхода создать вход соответствующего статуса для первого устройства (например, AMC, первый вход) и установки (например, первый сигнал, первая дверь).



При нажатии » выбранный статус перемещается в список и создается вместе с ярлыком OR для каждого установленного устройства (например, все входы AMC).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

– Для одного ярлыка ИЛИ можно назначить несколько состояний.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Также возможны ярлыки с И:

– Статус уже может быть назначен, и к нему добавляется условие путем его выбора в любом столбце.
– Затем при нажатии · выбирается другой статус и связывается с помеченным статусом.

Exit	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>

Замечание!
Каждому выходному сигналу можно назначить до 128 ярлыков ИЛИ.
Для каждого назначенного условия можно создать **один** ярлык И.

Когда устройству или установке назначен некоторый статус, его также можно назначить все остальным имеющимся устройствам и установкам.

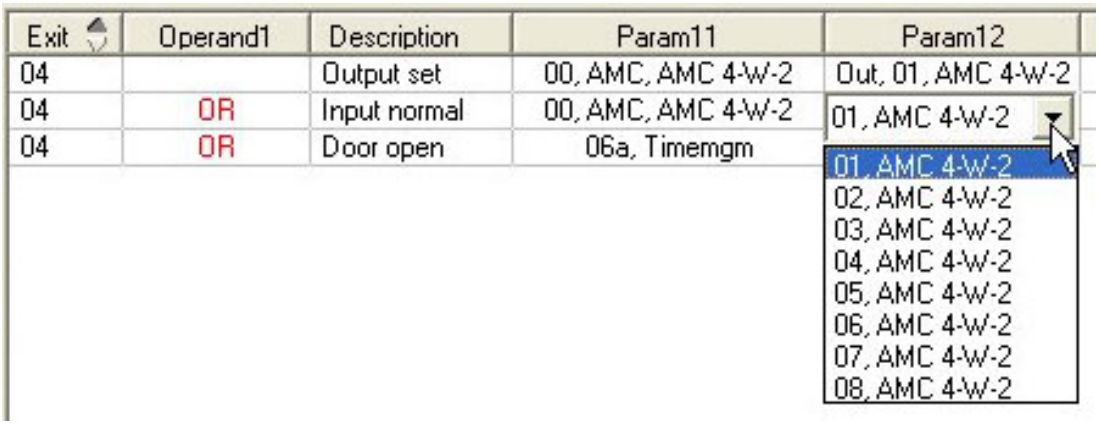
– Выберите назначенную запись в любом столбце.
– Этот статус создается для всех имеющихся устройств и установок при нажатии All.

Изменение параметров выходов

Элементы списка можно изменять.
Для нескольких устройств и установок, которым может соответствовать назначенный статус, всегда заданы первые устройства и установки этого типа.
В столбцах **Парам11** и **Парам21** (с ярлыками И) отображаются устройства (например, AMC, проход). В столбцах **Парам12** и **Парам22** содержатся специальные установки (например, входной сигнал, дверь, считыватель).
При наличии нескольких устройств (например, платы ввода-вывода) или установок (например, дополнительные сигналы, считыватели) указатель мыши меняет форму при наведении на такой столбец.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Если дважды щелкнуть запись столбца, появляется раскрывающийся список действительных записей для параметра.



При изменении записей в столбцах **Парам11** и **Парам21** обновляются записи в столбцах **Парам12** и **Парам22**:

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>
04	OR	Input normal	01, AMC_IO, AMC_IO16_002_1	In, 01, AMC_IO16_002_1

Замечание!
Это возможно только для столбцов **Парам11**, **Парам12**, **Парам21** и **Парам22**.
Если нет других вариантов (например, так как был настроен только один проход), то указатель мыши не изменяется, и все поля отображаются серым цветом. Если дважды щелкнуть такую запись, это интерпретируется как команда на удаление, и появляется сообщение для проверки удаления.

Удаление состояний для инициирования выходов

Выбранные назначения можно удалить, нажав '**<**' (или дважды щелкнув элемент списка). Всплывающее сообщение запросит подтверждение удаления.

Если с выходом связано несколько состояний, их можно удалить одновременно с помощью следующих действий:

- выберите первый элемент списка (тот, который не имеет записи в столбцу **Op1**), а затем нажмите кнопку «**<<**».
- Это также можно сделать, дважды щелкнув по первой записи.
  - Появится всплывающее окно. Подтвердите или отмените удаление.
  - В случае подтверждения удаления, второе всплывающее окно запросит, желаете ли вы удалить все связанные записи (нажмите **Да**) или только выбранную запись (нажмите **Нет**).

Для удаления дополнительных состояний, которые определяют первое состояние с помощью оператора AND в столбце **Op2**, щелкните строку, а затем нажмите кнопку «минус» , которая активна только тогда, когда в строке присутствует определяющее состояние AND.

Описание состояния

В таблице ниже приведен обзор всех доступных для выбора состояний, их номеров типов и описания.

В поле списка **Состояние** также содержатся указанные параметры — они отображаются при прокрутке списка вправо.

Статус	Тип	Описание
Вход активирован	1	Локальный вход
Обычный вход	2	Локальный вход
Короткое замыкание на входе тампера	3	Локальный вход с резистором настроен
Срабатывание тамперного входа	4	Локальный вход с резистором настроен
Вход включен	5	Локальный вход активирован временной моделью
Вход отключен	6	Локальный вход деактивирован моделью времени
Установка выхода	7	Локальный выход, не текущий выход
Сброс выхода	8	Локальный вход, не текущий вход
Дверь открыта	9	GID прохода, номер двери
Дверь закрыта	10	GID прохода, номер двери
Дверь открыта без авторизации	11	GID прохода, номер двери, заменяет состояние "Дверь открыта" (9)
Дверь оставлена открытой	12	GID прохода, номер двери
Считыватель показывает, что доступ разрешен	13	Адрес считывателя
Считыватель показывает, что доступ запрещен	14	Адрес считывателя
Временная модель активна	15	Настроенная временная модель
Тампер считывателя	16	Адрес считывателя
Тампер AMC	17	---
Тампер платы входа/выхода	18	---
Сбой питания	19	только для AMC, работающего от батареи
Питание включено	20	только для AMC, работающего от батареи
Связь с хостом в порядке	21	---
Связь с хостом разорвана	22	---

Сообщения считывателей	23	(Сведения зависят от текущей версии программного обеспечения)
Сообщения LAC	24	(Сведения зависят от текущей версии программного обеспечения)

Настройка выходов

Кроме назначения сигналов с моделями дверей или с отдельным назначением, можно определить условия для выходных сигналов, которые еще не назначены. При выполнении таких условий активируется выходной сигнал в соответствии с заданным параметром. Необходимо решить, какое событие будет переключать данный сигнал. В отличие от сигналов, которые можно назначить конкретной модели дверей, ее дверям и считывателям, в этом случае можно использовать сигналы всех устройств и установок, подключенных к AMC.

Если, например, оптический, акустический сигнал или сообщение для UGM необходимо инициировать сигналами входа **Короткое замыкание на входе тампера** и **Дверь открыта без авторизации**, то вход или входы, которые могут быть рассмотрены, назначаются соответствующему выходу.

Пример, в котором в каждом случае был выбран только один контакт:

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

Пример со всеми контактами:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Пример с выбранными контактами:

Если нажать » или удалить ненужные контакты после назначения всех контактов, для каждого контакта создается одна запись:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Для нескольких выходных сигналов можно задать одинаковые условия, если, например, кроме оптического сигнала также нужен акустический. Одновременно следует отправить сообщение для UGM:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

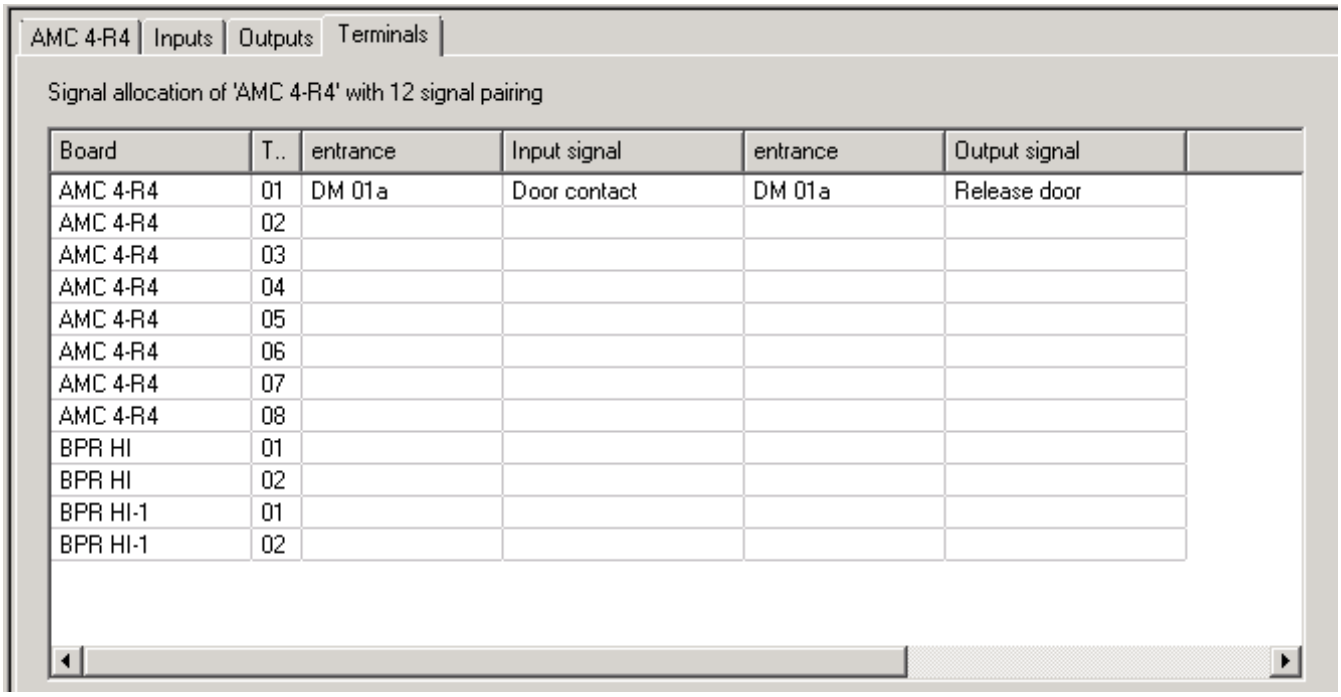
Список всех существующих состояний со значениями по умолчанию для параметров 11/21 и 12/22:

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

Определение сигналов на вкладке «Терминалы»

На вкладке **Терминалы** указано назначение контактов в AMC или AMC-EXT. После создания проходов указываются назначения сигналов в соответствии с выбранной моделью дверей.

На вкладке **Терминалы** контроллера или плат расширения нельзя внести изменения. Правки возможны только на вкладке терминалов страницы прохода. Поэтому настройки терминала отображаются на сером фоне. Проходы, которые отображаются красным цветом, указывают конфигурации соответствующих выходных сигналов.


AMC 4-R4
Inputs
Outputs
Terminals
Signal allocation of 'AMC 4-R4' with 12 signal pairing
Board
T..
entrance
Input signal
entrance
Output signal
AMC 4-R4 01 DM 01a Door contact DM 01a Release door
AMC 4-R4 02
AMC 4-R4 03
AMC 4-R4 04
AMC 4-R4 05
AMC 4-R4 06
AMC 4-R4 07
AMC 4-R4 08
BPR HI 01
BPR HI 02
BPR HI-1 01
BPR HI-1 02

13 Настройка входов

13.1 Входы — вводные сведения

Термин Проход означает весь механизм контроля доступа в точке входа.
Элементы системы контроля проходов включают следующее:

- Считыватели доступа: от 1 до 4
- Некий барьер, например дверь, турникет, ловушка или шлагбаум.
- Процедура доступа, определяемая предварительно заданными последовательностями электронных сигналов, которые передаются между элементами оборудования.

Модель двери — это шаблон для определенного типа прохода. Она описывает имеющиеся элементы двери (число и тип считывателей, тип двери или барьера и т. д.) и вызывает применение определенного процесса контроля доступа с использованием последовательностей предварительно определенных сигналов.
Модели дверей значительно упрощают настройку системы контроля доступа.

Модель двери 1	Простая или обычная дверь
Модель двери 3	Двусторонний турникет для входа и выхода
Модель двери 5	Въезд/выезд с автостоянки
Модель двери 6	Входные/выходные считыватели учета рабочего времени
Модель двери 7	Управление лифтом
Модель двери 9	Барьер типа шлагбаума для автомобилей и откатные шлюзные ворота
Модель двери 10	Простая дверь с постановкой на охрану/снятием с охраны IDS
Модель двери 14	Простая дверь с постановкой на охрану/снятием с охраны IDS и специальными правами доступа
Модель двери 15	Независимые входные и выходные сигналы

- Модели дверей 1, 3, 5, 9 и 10 включают возможность использования дополнительных считывателей карт на стороне входа или выхода.
- Локальный контроллер доступа, используемый в модели двери 05 (парковка) или 07 (лифт) невозможно одновременно использовать с другой моделью двери.
- Если проход настроен с использованием модели двери и сохранен, поменять модель двери на другую не удастся. Если требуется использовать другую модель двери, следует удалить проход и настроить его с другими параметрами с нуля.

Некоторые модели дверей имеют варианты (a, b, c, r) со следующими характеристиками:

a	входные **и** выходные считыватели
b	входной считыватель и кнопка запроса на выход
c	входной **ИЛИ** выходной считыватель (не оба — это был бы вариант **a**)
r	(Только для модели двери 1) Один считыватель исключительно для регистрации лиц в точке сбора, например в случае эвакуации. Эта модель дверей не предусматривает физического барьера.

Кнопка **ОК** для завершения конфигурации становится активной только после ввода всех необходимых значений. Например, для моделей дверей варианта (a) необходимо настроить входные **и** выходные считыватели. Данные записи можно сохранить не раньше, чем будет выбран тип «a» для обоих считывателей.

13.2 Создание проходов

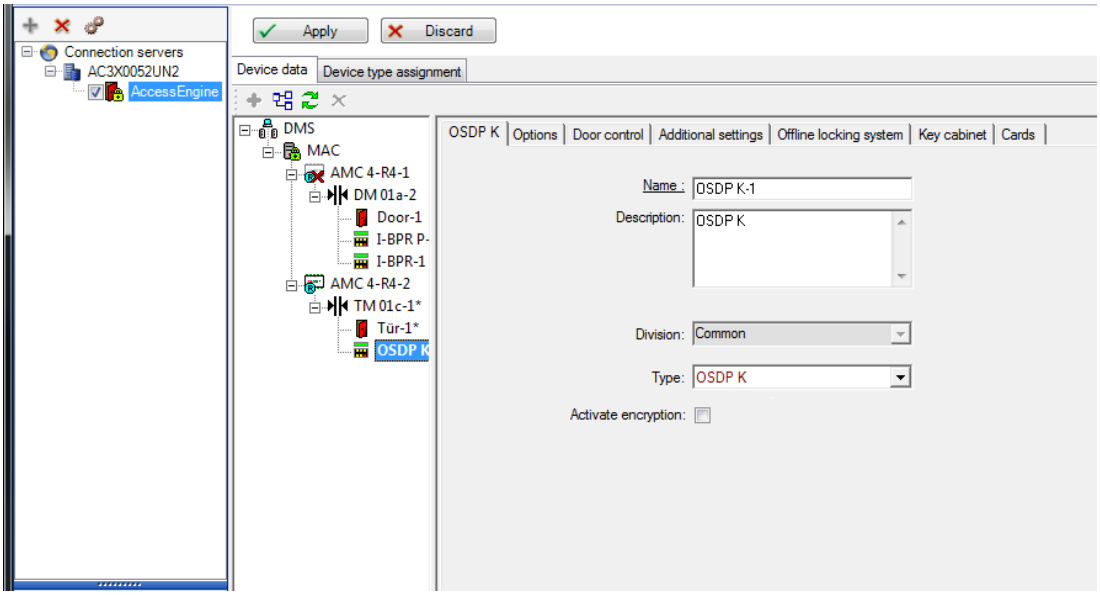
Список доступных для выбора считывателей будет адаптирован в зависимости от выбранного типа контроллера.

– Для типов **AMC 4W** доступны только считыватели Wiegand с клавиатурой и без.
– Для типа **AMC 4R4** доступны считыватели из следующей таблицы. Не используйте протоколы разных типов на одном контроллере.

Имя считывателя	Протокол Wiegand	Протокол BPR	Протокол I-BPR	Протокол HID
WIE1	X			
WIE1K (клавиатура)	X			
BPR MF		X		
BPR MF (клавиатура)		X		
BPR LE		X		
BPR LE (клавиатура)		X		
BPR HI		X		
BPR HI (клавиатура)		X		
TA40 LE		X		
TB30 LE		X		
TB15 HI1		X		
INTUS 1600			X	
I-BPR			X	
I-BPR K (клавиатура)			X	
DT 7020			X	
OSDP				X
OSDP K (клавиатура)				X
OSDP KD (с клавиатурой и дисплеем)				X
HADP				X
HADP K (клавиатура)				X
HADP KD (с клавиатурой и дисплеем)				X
RKL 55 (с клавиатурой и дисплеем)				X
RK40 (клавиатура)				X
R40				X
R30				X

R15				X

При использовании **считывателя OSDP** диалоговое окно будет выглядеть следующим образом:



Доступны следующие типы считывателей OSDP:

OSDP	Стандартный считыватель OSDP
OSDP Keyb	Считыватель OSDP с клавиатурой
OSDP Keyb+Disp	Считыватель OSDP с клавиатурой и дисплеем

Следующие считыватели OSDP были протестированы:

OSDPv1 — небезопасный режим	LECTUS duo 3000 C — MIFARE classic LECTUS duo 3000 CK — MIFARE classic LECTUS duo 3000 E — MIFARE Desfire EV1 LECTUS duo 3000 EK — MIFARE Desfire EV1
OSDPv2 — небезопасный и безопасный режимы	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

Замечание!

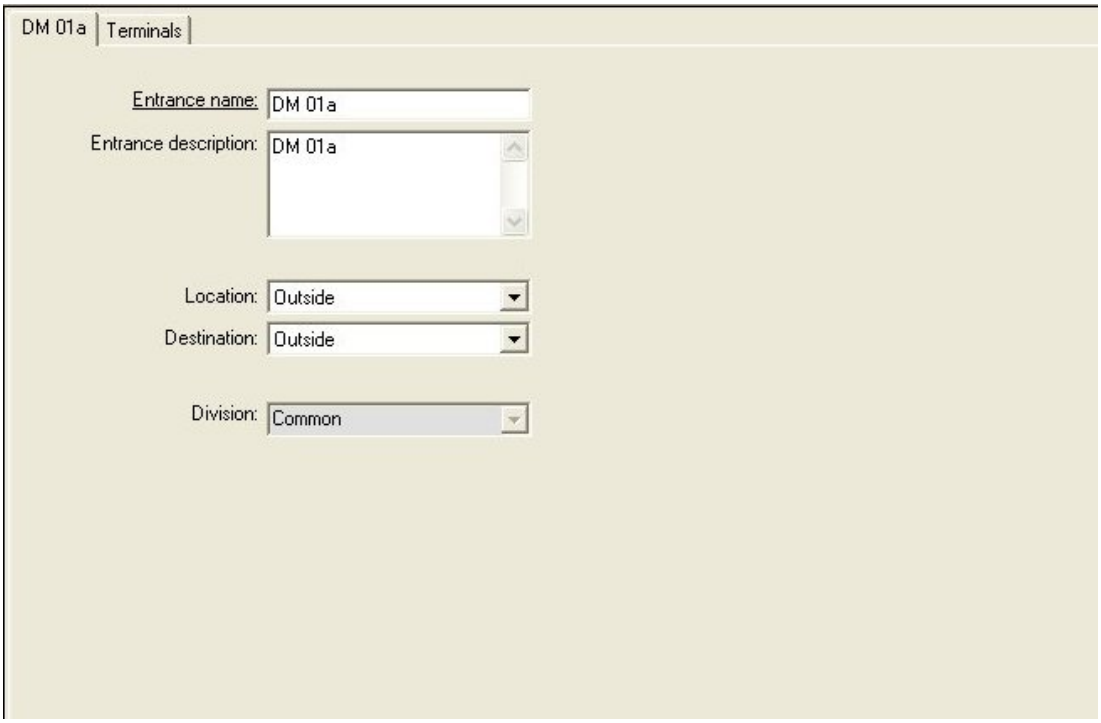
На что следует обратить внимание при работе с OSDP

Не используйте различные семейства продуктов одновременно (например, **LECTUS duo** и **LECTUS secure**) на одной шине OSDP.

Для зашифрованной передачи данных в считыватель OSDP создается и используется специальный ключ. Убедитесь, что существует сделанная должным образом резервная копия системы.

Храните ключи в безопасности Восстановить потерянные ключи невозможно; в случае утери ключей можно только сбросить настройки считывателя на заводские установки.

В целях безопасности не используйте одновременно зашифрованные и незашифрованные режимы на одной шине OSDP.



Параметр	Возможные значения	Описание
Имя прохода	алфавитно-цифровое значение, от 1 до 16 символов	В этом диалоговом окне генерируется уникальное имя прохода, однако при необходимости оператор, настраивающий проход, может его перезаписать.
Описание прохода	алфавитно-цифровое значение: 0–255 символов	Произвольное описание, которое будет отображаться в системе.
Местоположение	Любая определенная зона (не парковки)	Именованная зона (в соответствии с определением в системе), где расположен считыватель. Эта информация используется для управления последовательностью доступа: если кто-то пытается использовать этот считыватель, однако отслеживаемое системой расположение этого человека отличается от расположения считывателя, считыватель откажет в доступе такому пользователю.
Место назначения	Любая определенная зона (не парковки)	Именованная зона (в соответствии с определением в системе), к которой считыватель предоставляет доступ.

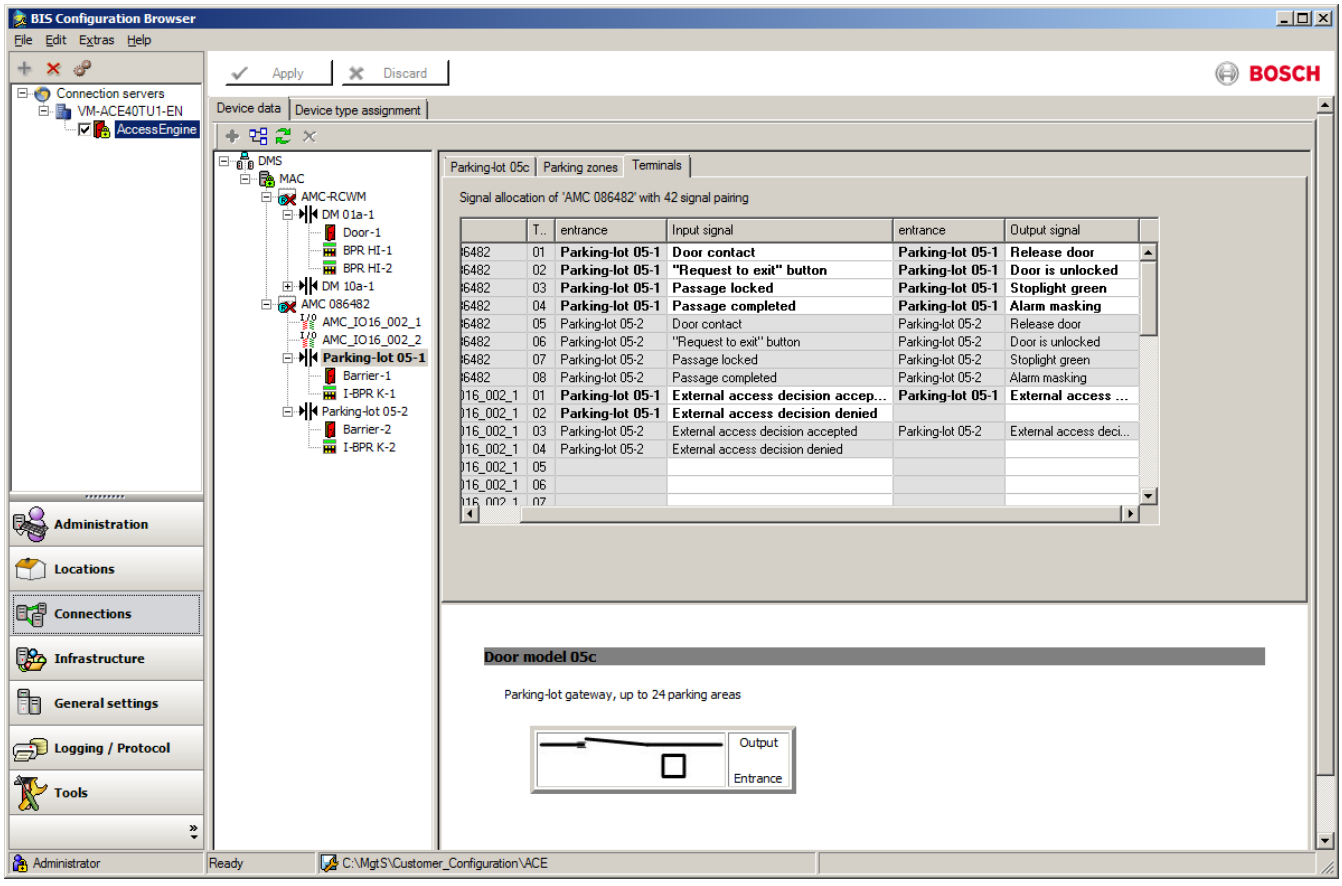
		Эта информация используется для управления последовательностью доступа: если лицо использует этот считыватель, местоположение этого лица будет изменено на значение **Место назначения**.
Время ожидания решения о доступе от внешней системы	Количество десятых секунд	Время ожидания решения от системы контроля доступа контроллером доступа перед принятием собственного решения.
Подразделение	Поле только для чтения	Определенное подразделение, к которому относится считыватель. Подразделение по умолчанию — **Общее**.
Время ожидания тревожного устройства (только для моделей прохода 10 и 14)	100 - 9999	Временной интервал, в течение которого устройство открытия двери может быть активировано без подачи сигнала тревоги. Это параметр считывателя, который задается, а затем передается считывателям. Единица этого параметра — десятая (1/10) секунды.
Область с постановкой на охрану (только для модели прохода 14)	Одна буква: от A до Z	Проходы группы IDS будут активироваться вместе с активацией считывателей области.

13.3 Дополнительная проверка входов/выходов

Дополнительные проверки входов/выходов могут, например, помочь идентифицировать посетителя с помощью системы считывания номерных знаков (ANPR).
AMC получает 1 вход через контакт AMC I/O:

– Посетитель авторизован для дополнительной проверки входов/выходов

AMC отказывает в доступе при получении сигнала «не авторизовано».

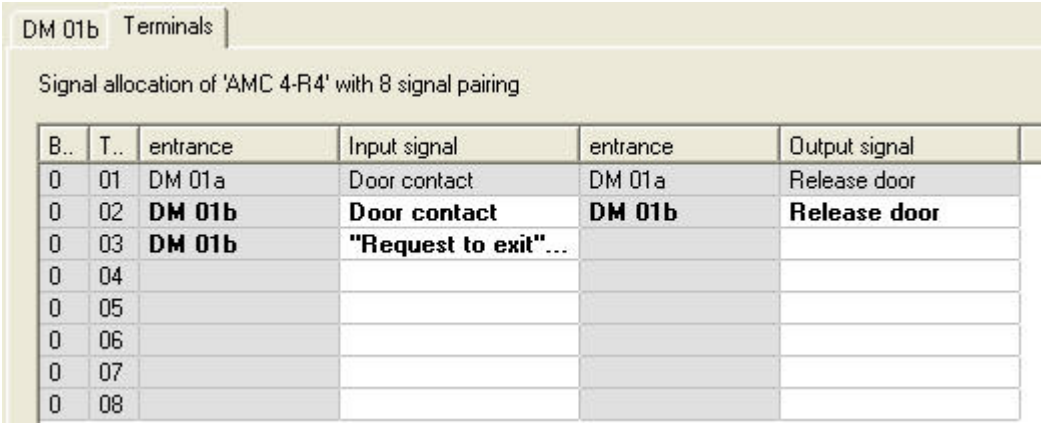


Статус карты	Сигнал = 1: авторизовано ANPR	Сигнал = 0: не авторизовано ANPR
Карта авторизована	Access (Доступ)	Событие "Недействительный номер автомобиля"
Карта в черном списке	Не авторизовано — черный список	Не авторизовано — черный список
Срок действия карты истек	Не авторизовано — истек срок действия	Не авторизовано — истек срок действия
Карта не авторизована для данного считывателя	Не авторизовано	Не авторизовано

Можно вручную открыть входной барьер, даже если посетитель не распознан.
Для этого к контактам входа/выхода AMC подключен переключатель.
AMC задает выходной сигнал **Активна дополнительная проверка** перед анализом входного сигнала.
При регистрации нового посетителя оператор должен ввести номер автомобиля в BIS (для отчетов) и в систему ANPR (для сканирования).
ANPR распознает зарегистрированный автомобиль из базы данных.

13.4 Настройка терминалов AMC

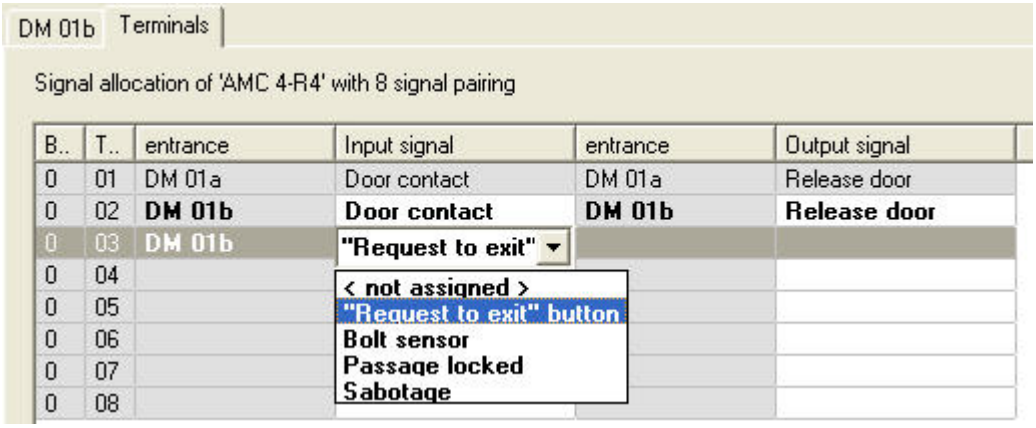
По своему содержимому и структуре эта вкладка идентична вкладке AMC **Терминалы**.


DM 01b Terminals

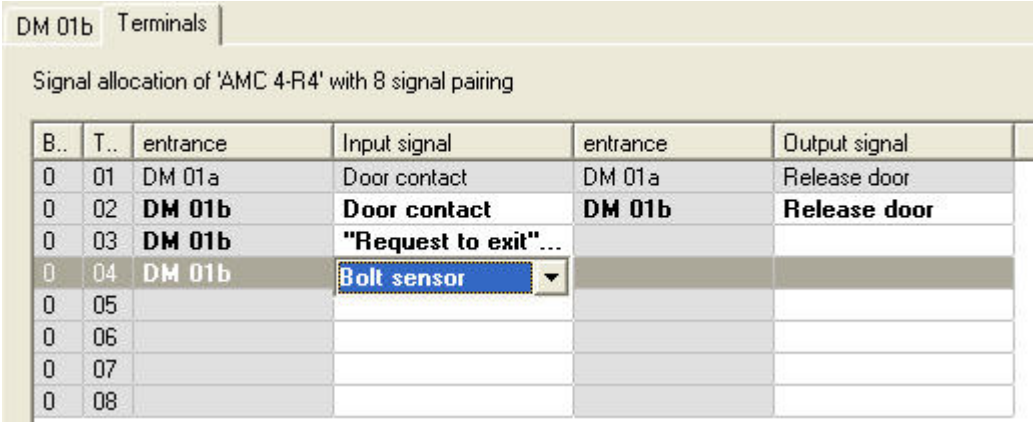
Signal allocation of 'AMC 4-R4' with 8 signal pairing

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	**DM 01b**	**Door contact**	**DM 01b**	**Release door**
0	03	**DM 01b**	**"Request to exit"...**		
0	04				
0	05				
0	06				
0	07				
0	08				

Однако здесь можно вносить изменения в назначения сигналов для выбранной модели проходов. Если дважды щелкнуть в столбцах **Выходной сигнал** или **Входной сигнал**, открываются поля со списками.



Кроме того, можно создать дополнительные сигналы для соответствующих проходов. Если дважды щелкнуть пустую строку, открывается подходящее поле со списком:



Назначения сигналов, которые не подходят для редактируемого прохода, доступны только для чтения и имеют серый фон. Их можно редактировать, только если выбран соответствующий проход.

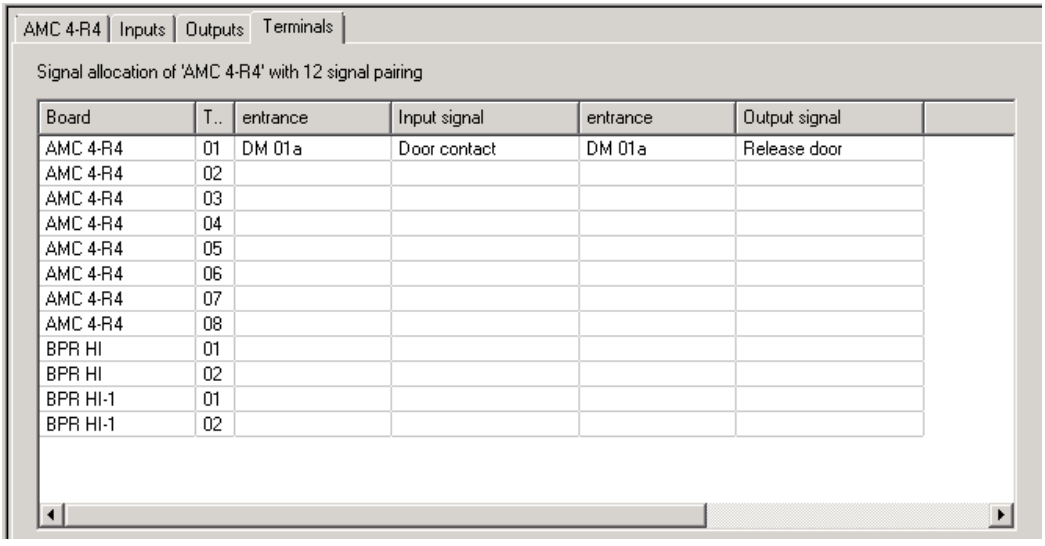
Подобный серый фон и передний план бледного цвета применяются к записям выходных сигналов, параметры которых задаются на вкладке **Выходы** контроллера AMC.

Замечание!
Поля со списками зависят от контекста не на 100 %, поэтому можно выбрать сигналы, которые в реальной жизни не сработают. При добавлении или удалении сигналов на вкладке **Терминалы** протестируйте их, чтобы убедиться в их логической и физической совместимости с проходом.

Назначение терминалов

Для каждого AMC и каждого прохода на вкладке **Терминалы** перечисляются все 8 сигналов для AMC на 8 отдельных строках. Неиспользованные сигналы помечены белым цветом, а использованные — синим.

Данный список имеет следующую структуру.

- **Плата**: порядок нумерации AMC Wiegand Extension (0) или платы расширения входа/выхода (1–3)
- **Терминал**: номер контакта на AMC (01–08) или на плате расширения Wiegand (09–16)
- **Проход**: название прохода
- **Выходной сигнал**: название выходного сигнала
- **Проход**: название прохода
- **Входной сигнал**: название входного сигнала
- 

Изменение назначения сигналов

На вкладках терминалов контроллеров назначения отдельных сигналов только отображаются (только для чтения). Однако на вкладках терминалов соответствующих проходов можно изменить или перегруппировать сигналы выбранных проходов.

Если дважды щелкнуть запись, которую требуется изменить, в столбце **Выходной сигнал** или **Входной сигнал** активируется раскрывающейся список, чтобы для сигнала данной модели прохода можно было выбрать другое значение. Если выбрать **Не назначено**, сигнал высвобождается и его можно использовать для других проходов.

Таким образом, сигналы можно не только изменять, но и назначать другим контактам, чтобы оптимизировать использование доступного питания. Все свободные или освобожденные сигналы можно использовать позднее как новые сигналы или в качестве новых позиций для существующих сигналов.

Замечание!
В принципе, все входные и выходные сигналы можно свободно выбирать, но не любой выбор имеет смысл для всех моделей дверей. Например, нет смысла назначать сигналы IDS модели дверей (например, 01 или 03), которая не поддерживает IDS. Дополнительные сведения см. в таблице в разделе "Назначение сигналов моделям дверей".

Назначение сигналов моделям дверей
Чтобы избежать неправильной параметризации раскрывающихся меню, предназначенных для назначения сигналов моделям дверей, в данных меню предлагаются только сигналы, совместимые с выбранной моделью дверей.

Таблица входных сигналов

Входные сигналы	Описание
Датчик двери	
Кнопка запроса на выход	Кнопка для открывания двери.
Ригельный датчик	Используется только для сообщений. Функции контроля нет.
Проход заблокирован	Используется для временной блокировки противоположной двери в шлюзовых воротах. Но также можно использовать для постоянной блокировки.
Саботаж	Сигнал о саботаже с внешнего контроллера.
Турникет в нормальном положении	Турникет закрыт.
Проход завершен	Проход был завершен успешно. Получен импульс внешнего контроллера.
IDS: готова к постановке на охрану	Задается системой IDS, если все детекторы находятся в покое и IDS можно поставить на охрану.
IDS: поставлена на охрану	IDS поставлена на охрану.
IDS: кнопка запроса постановки на охрану	Кнопка для запроса постановки IDS на охрану.
Локальное открытие разрешено	Используется, если в силу расположения дверного проема дверь открывается без привлечения AMC. AMC не отправляет сообщения о вторжении, но отправляет сообщение "локальная дверь открыта" (door local open).
Принято решение о доступе внешней системой	Сигнал задается, если внешняя система принимает доступ

Решение о доступе отклонено внешней системой	Сигнал задается, если внешняя система принимает доступ

Таблица выходных сигналов

Выходные сигналы	Описание
Устройство открывания дверей	
Шлюзовые ворота: запереть противоположное направление	Запирает другую сторону ловушки. Этот сигнал отправляется при открытии двери.
Подавление тревоги	... для IDS. Задается, когда дверь открыта, чтобы избежать создания системой IDS сообщения о вторжении.
Зеленый индикатор	Индикатор контролируется, пока дверь открыта.
Дверь открыта слишком долго	Трехсекундная пульсация. Если дверь открыта слишком долго.
Активация камеры	Камера активируется в начале перехода.
Открыть турникет внутрь	
Открыть турникет наружу	
Дверь постоянно открыта	Сигнал для разблокировки двери на длительный период.
IDS: постановка на охрану	Сигнал для постановки на охрану IDS.
IDS: снятие с охраны	Сигнал для снятия с охраны IDS.
Включено решение о доступе внешней системой	Для включения системы внешнего доступа необходимо задать сигнал

Таблица сопоставления моделей дверей входным и выходным сигналам

В следующей таблице перечислены значимые назначения сигналов и моделей дверей.

Модель дверей	Описание	Входные сигналы	Выходные сигналы
01	Простая дверь со считывателем на входе и выходе Считыватели учета времени и присутствия	- Датчик двери - Кнопка запроса на выход - Ригельный датчик - Проход заблокирован - Саботаж - Локальное открытие разрешено	- Устройство открывания дверей - Шлюзовые ворота: запереть противоположное направление - Подавление тревоги - Зеленый индикатор

	Доступно решение о доступе внешней системой	- Принято решение о доступе внешней системой - Отклонено решение о доступе внешней системой	- Активация камеры - Дверь открыта слишком долго - Включено решение о доступе внешней системой
03	Вращающаяся дверь со считывателем на входе и выходе Считыватели учета времени и присутствия Доступно решение о доступе внешней системой	- Турникет в исходном состоянии - Кнопка запроса на выход - Проход заблокирован - Саботаж - Принято решение о доступе внешней системой - Отклонено решение о доступе внешней системой	- Шлюзовые ворота: запереть противоположное направление - Открыть турникет внутрь - Открыть турникет наружу - Подавление тревоги - Активация камеры - Дверь открыта слишком долго - Включено решение о доступе внешней системой
05	Вход на автостоянку и выход с нее — до 24 зон парковки Считыватели учета времени и присутствия Доступно решение о доступе внешней системой	- Датчик двери - Кнопка запроса на выход - Проход заблокирован - Проход завершен - Принято решение о доступе внешней системой - Отклонено решение о доступе внешней системой	- Устройство открывания дверей - Подавление тревоги - Зеленый индикатор - Дверь открыта слишком долго - Дверь постоянно открыта - Включено решение о доступе внешней системой
06	Считыватели учета времени и присутствия		
07	Лифт — до 56 этажей		
09	Автомобильный въезд или входной считыватель и кнопка Считыватели учета времени и присутствия Доступно решение о доступе внешней системой	- Датчик двери - Кнопка запроса на выход - Проход заблокирован - Проход завершен - Принято решение о доступе внешней системой - Отклонено решение о доступе внешней системой	- Устройство открывания дверей - Подавление тревоги - Зеленый индикатор - Дверь открыта слишком долго - Дверь постоянно открыта - Включено решение о доступе внешней системой

10	Простая дверь со считывателем на входе и выходе и постановкой на охрану / снятием с охраны IDS Считыватели учета времени и присутствия Доступно решение о доступе внешней системой	- Датчик двери - Кнопка запроса на выход - IDS: готова к постановке на охрану - IDS: поставлена на охрану - Саботаж - IDS: запрос постановки на охрану - Принято решение о доступе внешней системой - Отклонено решение о доступе внешней системой	- Устройство открывания дверей - Активация камеры - IDS: постановка на охрану - IDS: снятие с охраны - Дверь открыта слишком долго - Включено решение о доступе внешней системой
14	Простая дверь со считывателем на входе и выходе и постановкой на охрану / снятием с охраны IDS Считыватели учета времени и присутствия	- Датчик двери - Кнопка запроса на выход - IDS: готова к постановке на охрану - IDS: поставлена на охрану - Саботаж - IDS: запрос постановки на охрану	- Устройство открывания дверей - Активация камеры - IDS: постановка на охрану - Дверь открыта слишком долго
15	Цифровые контакты		

Назначение сигналов считывателям

Возможности считывателей с последовательным интерфейсом (т. е. считывателей на AMC2 4R4) и считывателей с интерфейсом OSDP можно расширить с помощью локальных сигналов ввода/вывода. Таким способом можно сделать доступными дополнительные сигналы и сократить электрические пути к контактам дверей.

При создании считывателя с последовательным интерфейсом на вкладке **Терминалы** соответствующего прохода отображаются два входных и два выходных сигнала для каждого считывателя, подчиненного данному контроллеру, и сигналы платы расширения.

Замечание!

Данные элементы списка создаются для каждого считывателя с последовательным интерфейсом, независимо от наличия у него локальных операций ввода-вывода.

Такие локальные для считывателей сигналы не могут быть назначены функциям и параметризованы как сигналы контроллеров и плат. Они также не появляются на вкладках **Входной сигнал** и **Выходной сигнал**. Их также нельзя использовать для лифтов (например, чтобы преодолеть ограничение в 56 этажей). Поэтому они лучше всего подходят для прямого управления дверями (например, защелкивание или освобождение дверей). Тем не менее, это освобождает сигналы контроллера для более сложных параметризованных функций.

Редактирование сигналов

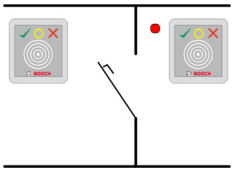
При создании прохода на вкладке **Терминалы** соответствующего прохода отображаются два входных и два выходных сигнала для каждого считывателя, подчиняющегося данному контроллеру. В столбце "Плата" указывается имя считывателя. Стандартные сигналы для

данного прохода по умолчанию назначаются первым свободным сигналам на контроллере. Чтобы перейти на собственные сигналы считывателя, их сначала необходимо удалить из своего исходного положения. Чтобы это сделать, выберите элемент списка **<Не назначено>**
Дважды щелкните в столбце **Входной сигнал** или **Выходной сигнал** считывателя, чтобы просмотреть список доступных сигналов для выбранной модели дверей и изменить положение сигнала. Как и все сигналы, их можно просматривать на вкладке **Терминалы** контроллера, но не редактировать.

Замечание!
Статус сигналов считывателя невозможно отслеживать.
Их можно использовать только для той двери, к которой относится данный считыватель.

13.5 Предопределенные сигналы для моделей дверей

Модель прохода 01



Варианты моделей:

01a	Обычная дверь со считывателем на входе **и** выходе
01b	Обычная дверь со считывателем на входе и кнопкой
01c	Обычная дверь со считывателем на входе **или** выходе

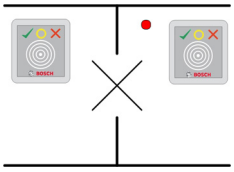
Возможные сигналы:

Входные сигналы	**Выходные сигналы**
Датчик двери	Устройство открывания дверей
Кнопка запроса на выход	Шлюзовые ворота: запереть противоположное направление
Саботаж	Зеленый индикатор
Локальное открытие разрешено	Активация камеры
	Дверь открыта слишком долго

Замечание!
Для функции разделения (в частности, для блокировки противоположенного направления) значения можно задавать только с помощью модели дверей 03.

Подавление тревоги активируется только в том случае, если время подавления тревоги перед открыванием двери больше 0.
Эту модель прохода также можно применить для въезда транспортных средств; в этом случае также рекомендуется использование вторичного считывателя для автомобилей.

Модель прохода 03



Варианты моделей:

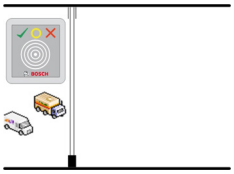
03a	Двусторонний турникет со считывателем на входе **и** выходе
03b	Двусторонний турникет со считывателем на входе и кнопкой
03c	Турникет со считывателем на входе **или** выходе

Возможные сигналы:

Входной сигнал	**Выходные сигналы**
Турникет в нормальном положении	Открыть турникет внутрь
Кнопка запроса на выход	Открыть турникет наружу
Саботаж	Проход заблокирован
	Активация камеры
	Дверь открыта слишком долго
Дополнительные сигналы, использующие параметры **ловушки**:	
Проход заблокирован	Шлюзовые ворота: запереть противоположное направление
	Подавление тревоги

Замечания по настройке для ловушек:
Когда турникет находятся в нормальном положении, включается первый входной сигнал всех подключенных считывателей. При наличии у владельца карты и прав доступа для данного прохода:
– если в считывателе на входе задан первый выходной сигнал на время активации;
– если в считывателе на выходе задан второй входной сигнал на время активации.
При нажатии кнопки "Запрос на выход" (REX) задаются второй входной и второй выходной сигналы. В течение этого времени можно использовать вращающуюся дверь в разрешенном направлении.

Модель прохода 05c



Вариант модели:

05c	Считыватель на въезде **или** выезде с автостоянки

Возможные сигналы для этой модели прохода:

Входные сигналы	**Выходные сигналы**
Датчик двери	Устройство открывания дверей
Кнопка запроса на выход	Дверь постоянно открыта
Проход заблокирован	Зеленый индикатор
Проход завершен	Подавление тревоги
	Дверь открыта слишком долго

Въезд на автостоянку и выезд с нее должны быть настроены на одном контроллере. Если доступ к автостоянке не назначен контроллеру, контроллер не может управлять никакими другими моделями дверей. Для въезда на автостоянку можно назначить только считыватель на входе (но не считыватель на выходе). Если вход назначен, то при выборе модели дверей можно определить только считыватель на выходе. Для каждой автостоянки можно определить до 24 подобластей, из которых одна должна содержаться в авторизациях карты, чтобы карта работала.

Модель прохода 06

Варианты моделей

06a	Считыватель на входе **и** выходе для учета времени и присутствия
06c	Считыватель на входе **или** выходе для учета времени и присутствия

Считыватели, созданные с этой моделью дверей, не управляют доступом, а используются исключительно для учета времени и посещения. Они не управляют дверями, а лишь пересылают данные карты в систему учета времени и присутствия.
Соответственно, сигналы не определены. Такие считыватели обычно устанавливаются в областях, которые уже контролируются.

Замечание!
Чтобы в системе учета времени и присутствия можно было создать допустимую пару регистрации (время входа плюс время выхода), необходимо задать параметры для двух отдельных считывателей с моделью дверей 06: один для регистрации времени входа, другой для регистрации времени выхода.

Если вход и выход не разделены, следует использовать вариант **a**. Если вход и выход разделены пространственно или если считыватели невозможно подключить к одному контроллеру, следует использовать вариант **c**. Убедитесь, что один из считывателей определен как входной считыватель, а второй - как выходной.
Как и для любого входа, необходимо создать и назначить авторизации. В Access Engine на вкладке **Учет времени** в диалоговых окнах **Авторизации доступа** и **Авторизации области/времени** перечисляются все считыватели учета времени и присутствия, которые были определены. Активируйте хотя бы один считыватель в направлении входа и один считыватель в направлении выхода. Авторизации для считывателей учета времени и присутствия можно назначать вместе с другими авторизациями доступа или как отдельные авторизации.
Если для заданного направления есть несколько считывателей учета времени и присутствия, то определенным считывателям можно назначить определенных владельцев карт. Такие считыватели будут регистрировать и сохранять только значения времени присутствия назначенных и авторизованных пользователей.

Замечание!
Поведение считывателей учета времени и присутствия также зависит от других функций управления доступом. Поэтому черные списки, временные модели и даты истечения срока действия также могут препятствовать регистрации значений времени доступа считывателями учета и присутствия.

Зарегистрированные значения времени входа и выхода сохраняются в текстовом файле в каталоге `C:\MgtS\AccessEngine\AC\TAExchange` под именем `TAccExc_EXP.tx` в ожидании экспорта в систему учета времени и присутствия.
Данные регистрации передаются в следующем формате:
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`
d=день, M=месяц, y=год, h=час, m=минут, s=летнее время (переход дна летнее время), 0=выход, 1=вход
Файл экспорта не отсортирован по лицам, все зарегистрированные данные содержатся в хронологическом порядке, в котором они были получены административным модулем. В этом файле в качестве разделителя полей используется точка с запятой.

Варианты входной модели 07

Варианты моделей:

07a	Лифт макс. на 56 этажей
07b	Лифт макс. на 56 этажей

Модель прохода 07a
Сигналы:

Входной сигнал	Выходные сигналы
	Высвободить <название этажа>
	По одному выходному сигналу на каждый определенный этаж, не более 56.

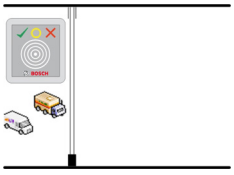
При вызове лифта владелец карты может выбрать только те этажи, для которых авторизована его карта.
Модели дверей лифта нельзя смешивать с другими моделями дверей на одном контроллере. С помощью плат расширения для каждого лифта в AMC можно определить до 56 этажей. Авторизации карты должны содержать сам лифт и хотя бы один этаж.

Модель прохода 07c
Сигналы:

Входной сигнал	Выходной сигнал
Входной код <название этажа>	Высвободить <название этажа>
Для каждого определенного этажа существует входная и выходная запись (до 56).	

При вызове лифта и нажатии кнопки выбора этажа (соответственно, требуются входные сигналы) проверяются авторизации карты, чтобы узнать, включают ли они выбранный этаж.
Более того, с данной моделью дверей можно определить любые этажи с **общим доступом**, т. е. для такого этажа авторизации не проверяются и любое лицо может подняться на лифте до этого этажа. Тем не менее, самим общим доступом можно управлять с помощью **временной модели**, ограничивающей его определенными часами определенных дней. В другое время проверки авторизации будет осуществляться в обычном режиме.
Модели дверей лифта нельзя смешивать с другими моделями дверей на одном контроллере. С помощью плат расширения для каждого лифта в AMC можно определить до 56 этажей. Авторизации карты должны содержать сам лифт и хотя бы один этаж.

Модель прохода 09

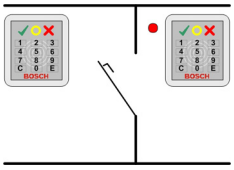


Возможные сигналы:

Входные сигналы	Выходные сигналы
Датчик двери	Устройство открывания дверей
Кнопка запроса на выход	Дверь открыта долгосрочно
Проход заблокирован	Горит зеленый светофор
Проход завершен	Подавление тревоги
	Дверь открыта слишком долго

Для управления шлагбаумом предполагается использование выделенного элемента управления (SPS). В отличие от **модели дверей 5c**, такие вход и выход можно настроить на других AMC. Более того, отсутствуют подобласти, имеется только общая авторизация для области парковки.

Модель прохода 10



Варианты моделей:

10a	Обычная дверь со считывателем на входе **и** выходе **и** постановкой на охрану / снятием с охраны IDS (системы обнаружения вторжений)
10b	Обычная дверь со входом, кнопкой REX (запрос на выход) и постановкой на охрану/снятием с охраны IDS
10e	Обычная дверь с входом, кнопкой REX и децентрализованной постановкой на охрану/снятием с охраны IDS

Возможные сигналы:

Входные сигналы	**Выходные сигналы**
Датчик двери	Устройство открывания дверей
IDS: поставлена на охрану	IDS: постановка на охрану
IDS: готова к постановке на охрану	IDS: снятие с охраны [только DM 10e]
Кнопка запроса на выход	Активация камеры
Ригельный датчик	Дверь открыта слишком долго
Саботаж	
IDS: кнопка запроса постановки на охрану	

Замечание!
Для этой модели дверей нужны клавиатурные считыватели. Владельцам карты требуются **PIN-коды** для постановки на охрану/снятия с охраны IDS.

Необходимые процедуры зависят от установленных считывателей.
Считыватели I-BPR: (например, DELTA 1010, INTUS 1600)
Чтобы поставить на охрану, следует нажать клавишу **7** и подтвердить, нажав Enter (#). При предъявлении карты вводится PIN-код, для подтверждения снова нажимается клавиша Enter (#).
Чтобы снять с охраны по предъявлению карты, следует ввести PIN-код и подтвердить, нажав Enter (#).

Считыватель BPR: (включая Wiegand)

Чтобы поставить на охрану, следует нажать клавишу 7, предъявить карту и ввести PIN-код. Подтверждение клавишей Enter не требуется.
Чтобы снять с охраны, следует предъявить карту и ввести PIN-код. Снятие с охраны и разблокировка дверей происходят одновременно.

Специальные функции DM 10e
Если в случае моделей дверей 10a и 10b каждый вход находится в собственной зоне безопасности, в случае модели 10e несколько входов можно сгруппировать в блоки. Любой считыватель из такой группы способен поставить на охрану или снять с охраны весь блок. Чтобы сбросить статус, заданный любым считывателем из данной группы, требуется выходной сигнал **Снять с охраны IDS**.
Сигналы:
- Модели дверей 10a и 10b:
  - - постановка на охрану инициируется постоянным сигналом,
  - - снятие с охраны запускается прерыванием постоянного сигнала.
- Модель дверей 10e:
  - - Постановка на охрану и снятие с охраны инициируются сигнальным импульсом длительностью 1 секунда.

[Двухпозиционное реле позволяет управлять IDS от нескольких дверей. Для этого сигналы всех дверей требуют операции ИЛИ на реле. Сигналы **IDS поставлена на охрану** и **IDS готова к постановке на охрану** должны дублироваться на всех задействованных дверях.]

13.6 Специальные проходы

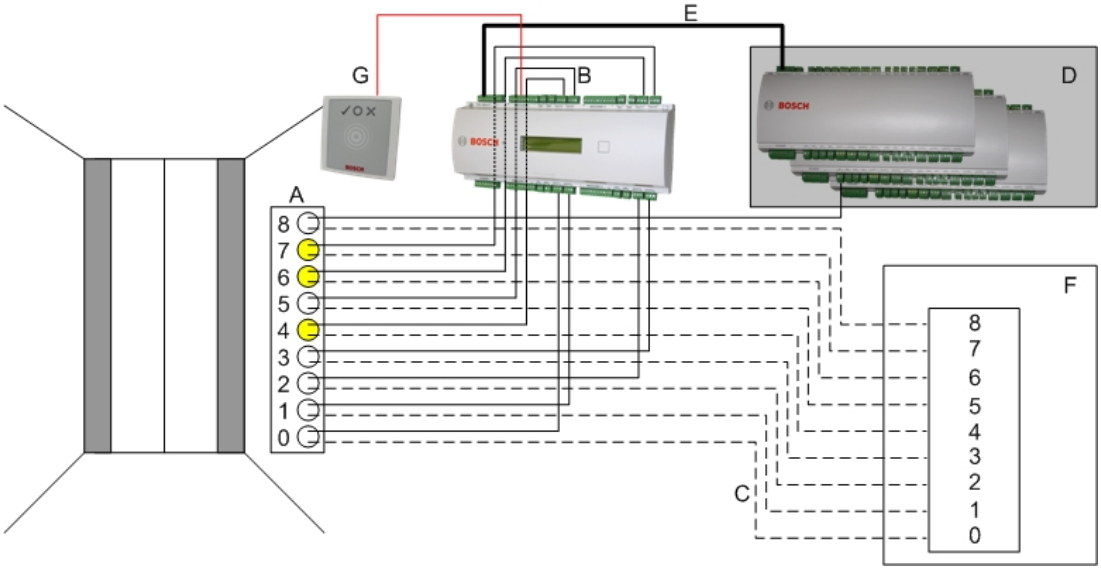
13.6.1 Лифты (DM07)

Общие замечания по лифтам (входная модель 07)
В одном контроллере AMC лифты невозможно комбинировать с другими моделями дверей.
Лифты нельзя использовать с функциями считывателя **Групповой доступ** или **Требуется сопровождение**
На одном AMC можно определить до 8 этажей. Плата расширения AMC предлагает 8 или 16 дополнительных выходов каждая.
Таким образом, используя максимальное количество самых больших плат расширения, возможно настроить до 56 этажей со считывателями RS485 и 64 этажа со считывателями Wiegand при использовании дополнительной специальной платы расширения Wiegand.

Различия между моделями прохода 07a и 07c
Диалоговые окна авторизации доступа системы Access Engine позволяют назначать конкретные этажи определенному лицу.
Если лифт создан с помощью модели прохода **07a**, то пользователь предъявляет свою идентификационную карту и получает доступ к тем этажам, для которых у него есть разрешение.
В случае модели прохода **07c** система проверяет авторизацию для выбранного этажа после того, как пользователь его выберет. Этажи, помеченные как **общедоступные**, доступны всем лицам независимо от авторизации. С помощью временной модели данную общедоступную функцию можно ограничить заданным периодом. Вне этого периода авторизация для данного этажа будет проверяться.

Схема подключения лифтов.

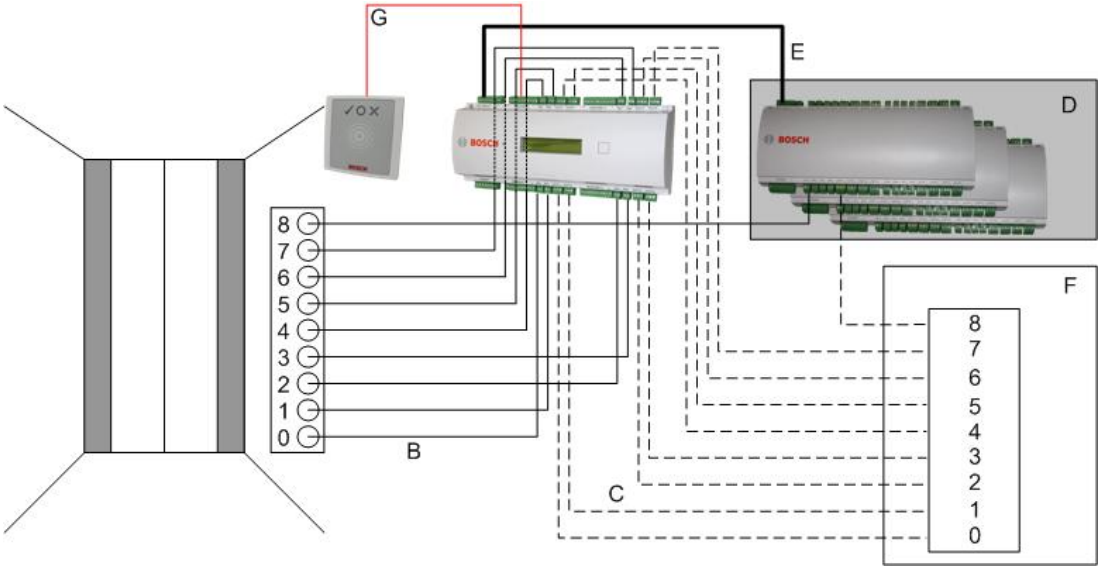
На рисунке ниже показана схема соединения лифта в рамках модели дверей 07a.



Условные обозначения:

- A = клавиатура лифта
- B = (сплошная линия) выходные сигналы AMC
- C = (прерывистая линия) Подключение к элементам управления лифтом
- D = к AMC можно подключить до трех плат входа/выхода, если его собственных восьми входов и выходов недостаточно.
- E = передача данных и питания от AMC к платам входа/выхода
- A = выбор этажа
- G = считыватель. Для каждого лифта можно настроить два считывателя.

На рисунке ниже показана схема соединения лифта в рамках модели дверей 07c.



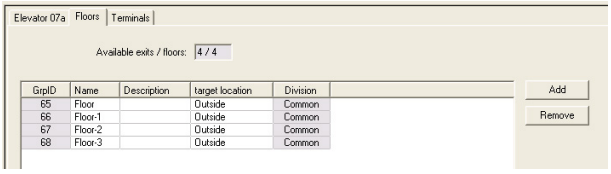
Условные обозначения:

- B = (сплошная линия) выходные сигналы AMC
- C = (прерывистая линия) Подключение к элементам управления лифтом

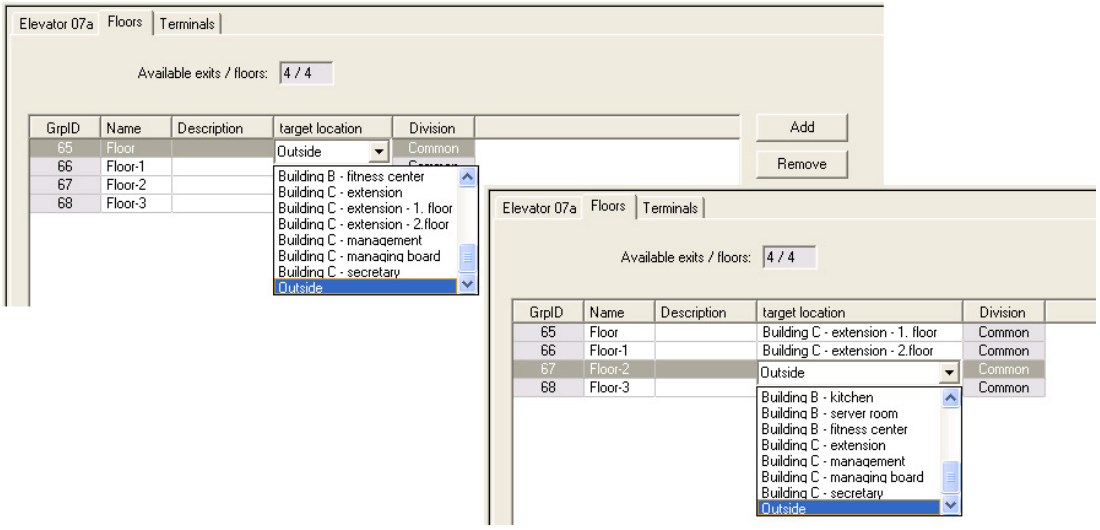
– D = к AMC можно подключить до трех плат входа/выхода, если его собственных восьми входов и выходов недостаточно.
– E = передача данных и питания от AMC к платам входа/выхода
– A = выбор этажа
– G = считыватель. Для каждого лифта можно настроить два считывателя.

Как и автостоянки, лифты имеют параметр **Общедоступно.** Этот параметр можно задать отдельно для каждого этажа по отдельности. Если параметр **Общедоступно** активирован, авторизации на доступ не проверяются, то есть любой владелец карты в лифте может выбрать этаж.
При необходимости можно настроить временную модуль для модели входа: вне указанного периода авторизации будут проверяться.

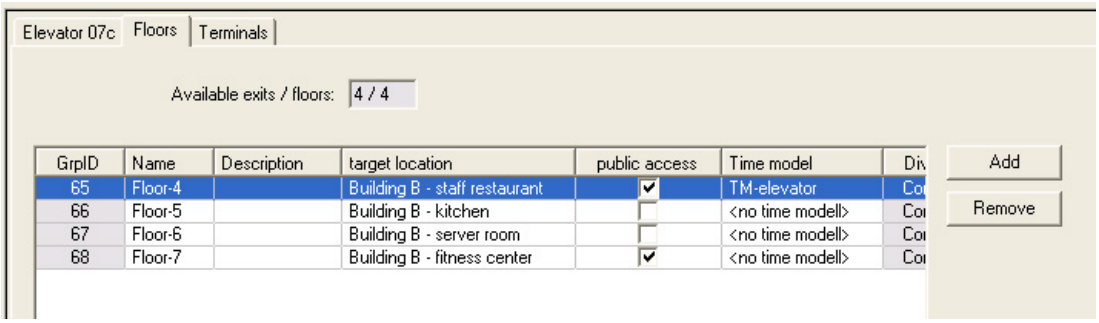
Этажи для модели прохода 07
Используйте вкладку **Этажи** для добавления и удаления этажей для лифта (с помощью кнопок **Добавить** и **Удалить**).



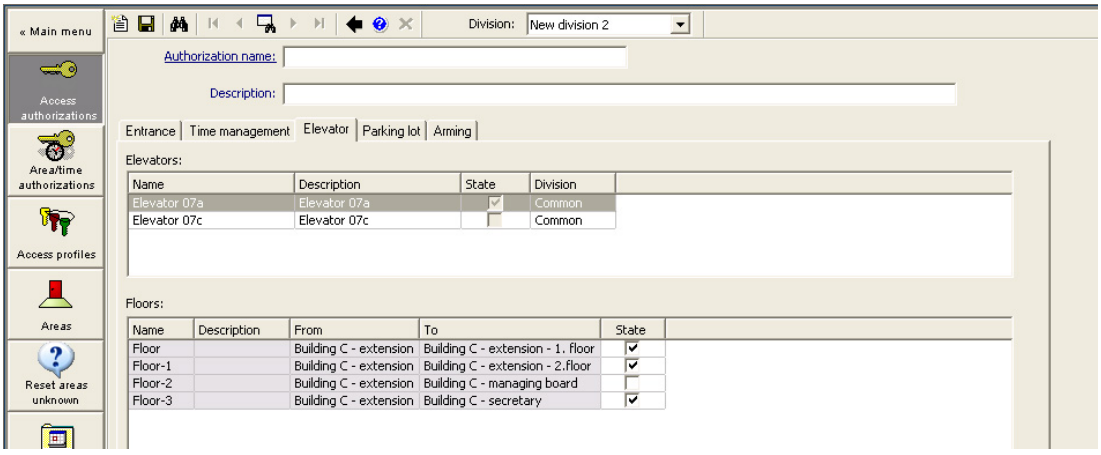
Целевыми местоположениями для этажа могут быть любые **Области**, кроме автостоянок и зон парковки.
Определенному этажу можно назначить только одну область. Поэтому выбор областей, предлагаемых в полях со списками, сокращается после каждого назначения, предотвращая непреднамеренные двойные назначения.



При использовании модели прохода 07a отдельные этажи можно делать общедоступными, устанавливая флажок **Общий доступ**. В этом случае авторизации не проверяются. Тем не менее, дополнительное назначение **временной модели** позволяет ограничить доступ предварительно определенными периодами.



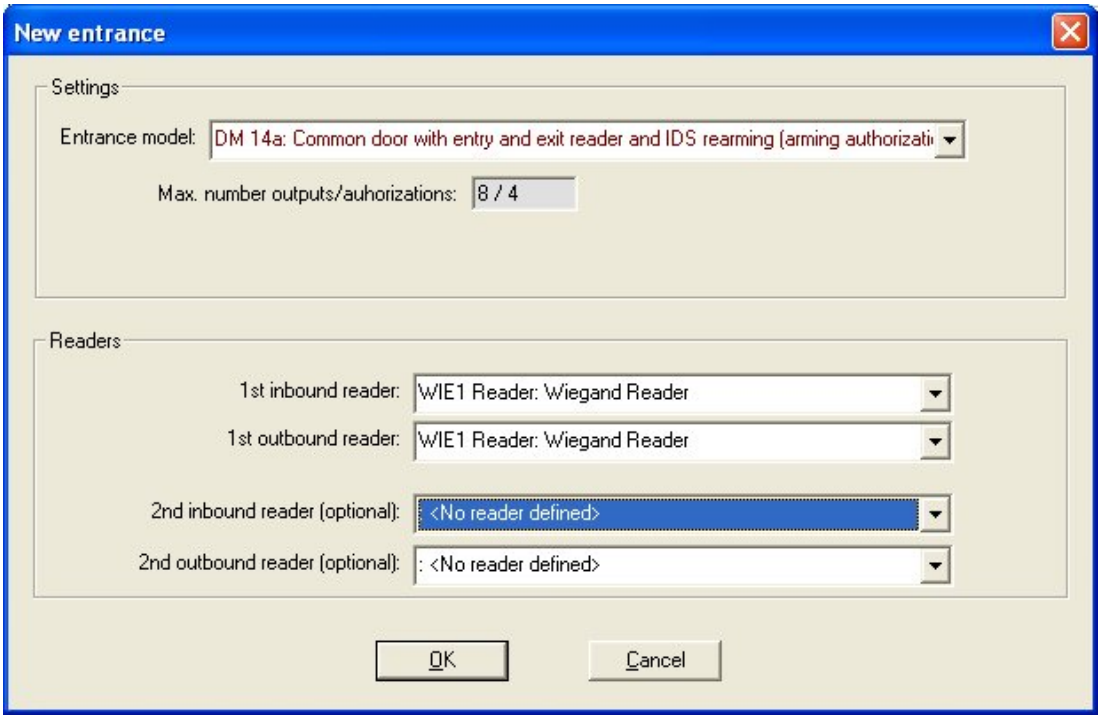
На вкладке **Лифт** над верхним полем списка в диалоговых окнах Access Engine **Авторизации доступа** и **Авторизации области/времени** выберите первый требуемый лифт, а затем (ниже) этажи, к которым владельцу карты разрешен доступ.



13.6.2 Модели дверей с тревожными сигнализациями (DM14)

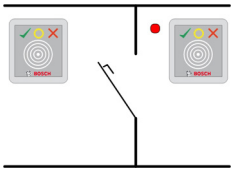
Постановка на охрану и снятие с охраны систем охранной сигнализации – DM 14

В отличие от модели прохода 10, DM 14 можно поставить на охрану/снять с охраны.



Охранная область обозначается заглавной буквой на первой странице прохода. Если назначить проход охранной области, то постановка на охрану на одном считывателе будет применена ко всем проходам данной области.

Модель прохода 14



Варианты моделей:

14a	Обычная дверь со считывателем на входе и выходе и постановкой на охрану / снятием с охраны охранной сигнализации (IDS)
14b	Обычная дверь с входом, кнопкой и постановкой на охрану /снятием с охраны охранной сигнализации (IDS)

Возможные сигналы:

Входные сигналы	**Выходные сигналы**
Датчик двери	Устройство открывания дверей
IDS: поставлена на охрану	IDS: постановка на охрану
IDS: готова к постановке на охрану	Активация камеры
Кнопка запроса на выход	Дверь открыта слишком долго
Ригельный датчик	
Саботаж	
IDS: кнопка запроса постановки на охрану	

Модель дверей 14 позволяет сформировать охраняемые зоны, в которых IDS (система обнаружения вторжений) может быть поставлена на охрану из любого считывателя данной зоны. В каждом случае сигналы **IDS поставлена на охрану** и **IDS готова к постановке на охрану** должны дублироваться на каждом проходе.

В отличие от модели 10 модель дверей 14 может использовать считыватели с клавиатурой или без нее. Еще одно отличие — назначение авторизаций постановки на охрану/снятия с охраны. Только владельцы карт с соответствующими авторизациями могут ставить на охрану/снимать с охраны.

В случае клавиатурных считывателей постановка на охрану и снятие с охраны выполняется как в модели дверей 10.

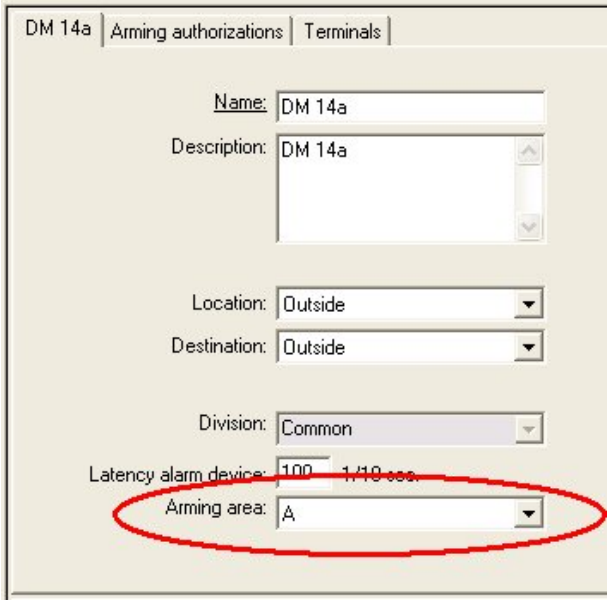
В случае бесклавиатурных считывателей постановка осуществляется не путем ввода PIN-кода, а с помощью переключателя рядом со считывателем, функция которого аналогична клавише 7 клавиатурных считывателей. После использования этого переключателя состояние тревожного устройства отображается цветными светодиодными индикаторами считывателя:

– Снято с охраны = индикатор попеременно мигает зеленым/красным цветом
– Поставлено на охрану = индикатор непрерывно горит красным цветом

Постановка на охрану выполняется по предъявлении должным образом авторизованной карты.

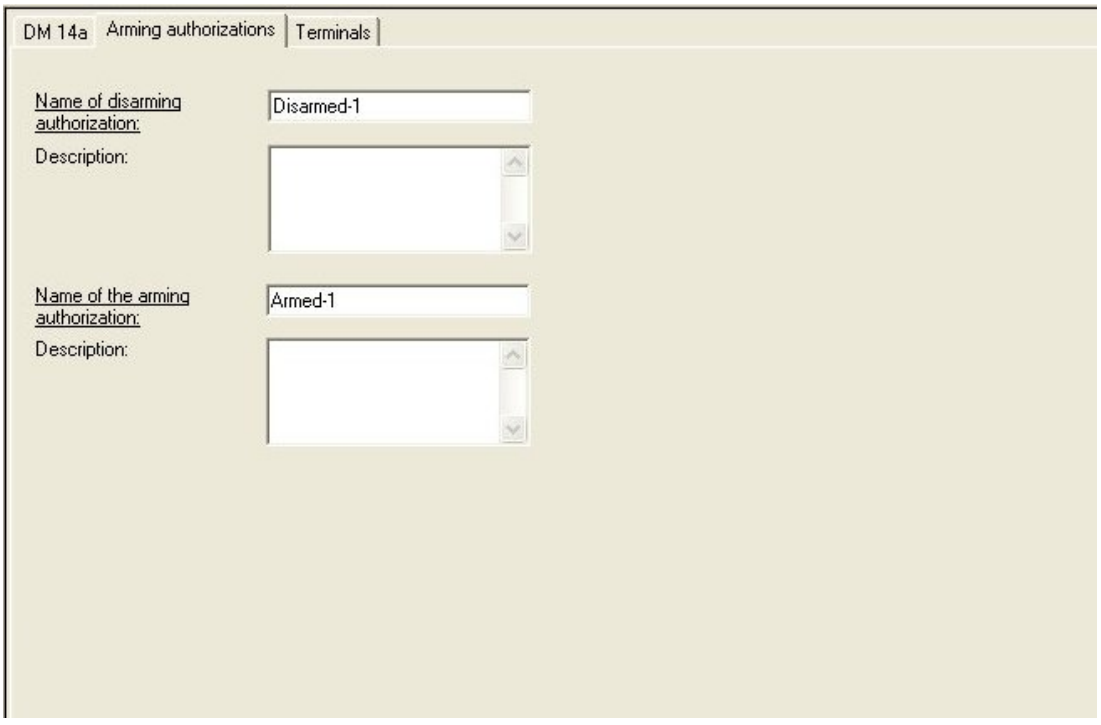
Снятие с охраны осуществляется с помощью переключателя и предъявления должным образом авторизованной карты.
При снятии с охраны двери не разблокируются автоматически; требуется повторно предъявить карту.

Авторизации для постановки области на охрану для модели прохода 14
На первой вкладке диалогового окна прохода 14 содержится дополнительный параметр для создания "охранных областей". Несколько проходов модели 14 могут ссылаться на одну и ту же охранную область, поэтому любой считыватель в этой области может поставить IDS (систему обнаружения вторжений) на охрану и снять ее с охраны.

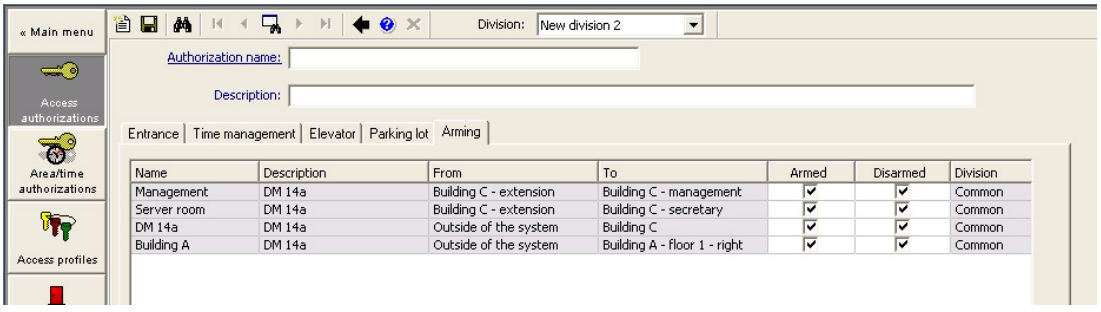


В этом случае сигналы **IDS поставлена на охрану** и **IDS готова к постановке на охрану** необходимо дублировать на входах других проходов. При создании второй модели прохода для той же охранной области редактор устройств выполняет репликацию самостоятельно. Описание сигнала второй двери будет дополнено номером соответствующего сигнала первой модели прохода: например, 1:04 [= четвертый сигнал на плате 1].

После создания экземпляра модели прохода 14 на дополнительной вкладке **Авторизации для постановки области на охрану** перечисляются авторизации, сгенерированные при его создании. Пользователи могут свободно выбирать имена для авторизаций постановки на охрану/снятия с охраны.



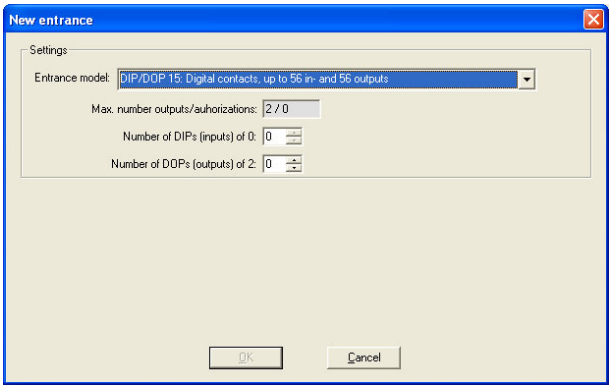
При сопоставлении авторизаций все созданные экземпляры модели прохода 14 перечисляются на вкладке **Постановка на охрану** диалоговых окон **Авторизации доступа** и **Авторизации области/времени.** Авторизации для постановки и снятия с охраны можно назначать отдельно.



13.6.3 Модули DIP и DOP (DM15)

Создание модели прохода 15.

Эта модель прохода предлагает независимые входные и выходные сигналы.



Если принимаются все интерфейсы считывателей, данная модель прохода становится доступной. Эту модель прохода можно определить, если свободны хотя бы два сигнала.

Данную модель прохода невозможно назначить AMC с лифтами (модель 07) или автостоянками (модель 05c).

Модель прохода 15

Возможные сигналы: эти имена по умолчанию можно перезаписать.

Входной сигнал	Выходной сигнал
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

В отличие от других моделей дверей, модель прохода 15 управляет все еще свободными входными и выходными сигналами контроллера и передает их как входные сигналы общего назначения и выходные сигналы без напряжения в распоряжение всей системы. В отличие от выходных контактов других моделей дверей, выходные контакты модели прохода 15 можно просматривать по отдельности с помощью графического пользовательского интерфейса BIS.

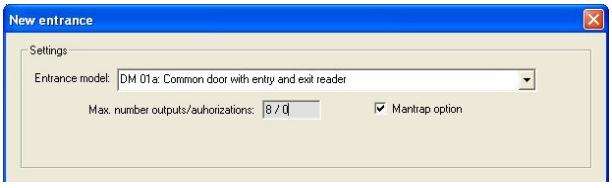
Восстановление модулей DOP после перезапуска

При перезапуске контроллера MAC или AMC значения состояний подчиненных модулей DOP, как правило, сбрасываются до значения по умолчанию 0 (нуль).
Чтобы гарантировать, что при перезапуске значение DOP всегда сбрасывается до последнего назначенного ему вручную состояния, выберите DOP в дереве устройств и установите **Сохранять состояние** в главном окне.

13.6.4 Модели дверей-ловушек

Создание ловушки

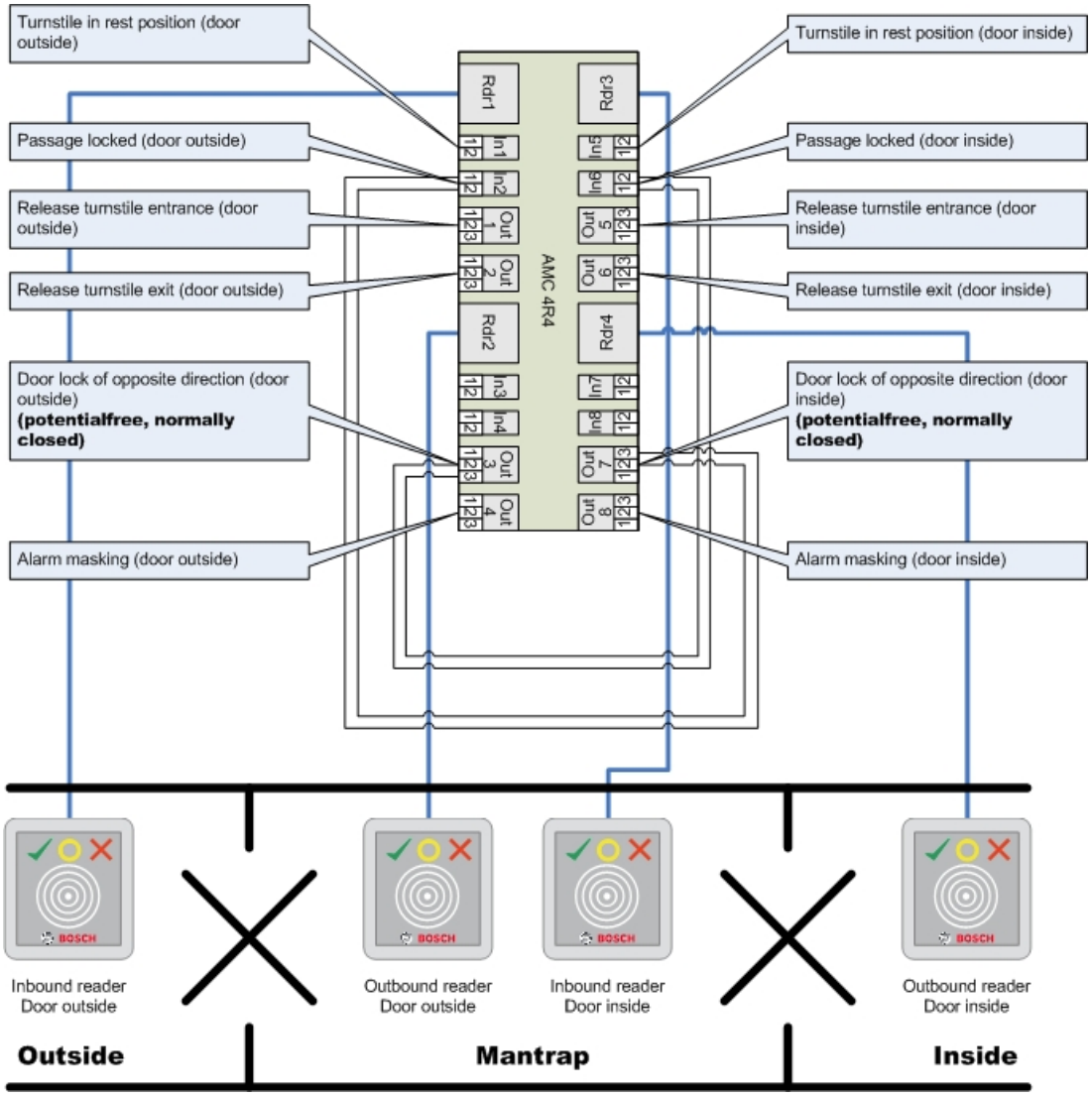
Модели прохода 01 и 03 можно использовать как «ловушки», чтобы разделить доступ владельцев карт. С помощью флажка **Параметры ловушки** можно сделать доступными необходимые дополнительные сигналы.



Можно комбинировать все типы моделей 01 и 03, но этот параметр следует задать на обоих проходах, принадлежащих к данной ловушке.
Наряду с обычными назначениями сигналов для данной модели дверей, для параметров ловушки требуются дополнительные собственные назначения сигналов.

Пример: ловушка на одном контроллере

Турникеты — наиболее распространенные средства разделить доступ владельцев карт. В следующих примерах используется модель дверей 3a (турникет со считывателем на входе и выходе).
Конфигурация ловушки с двумя турникетами (DM 03a):



Подключение к дверным замкам для обратного направления гарантирует, что только один из турникетов может быть открыт в каждый момент времени.

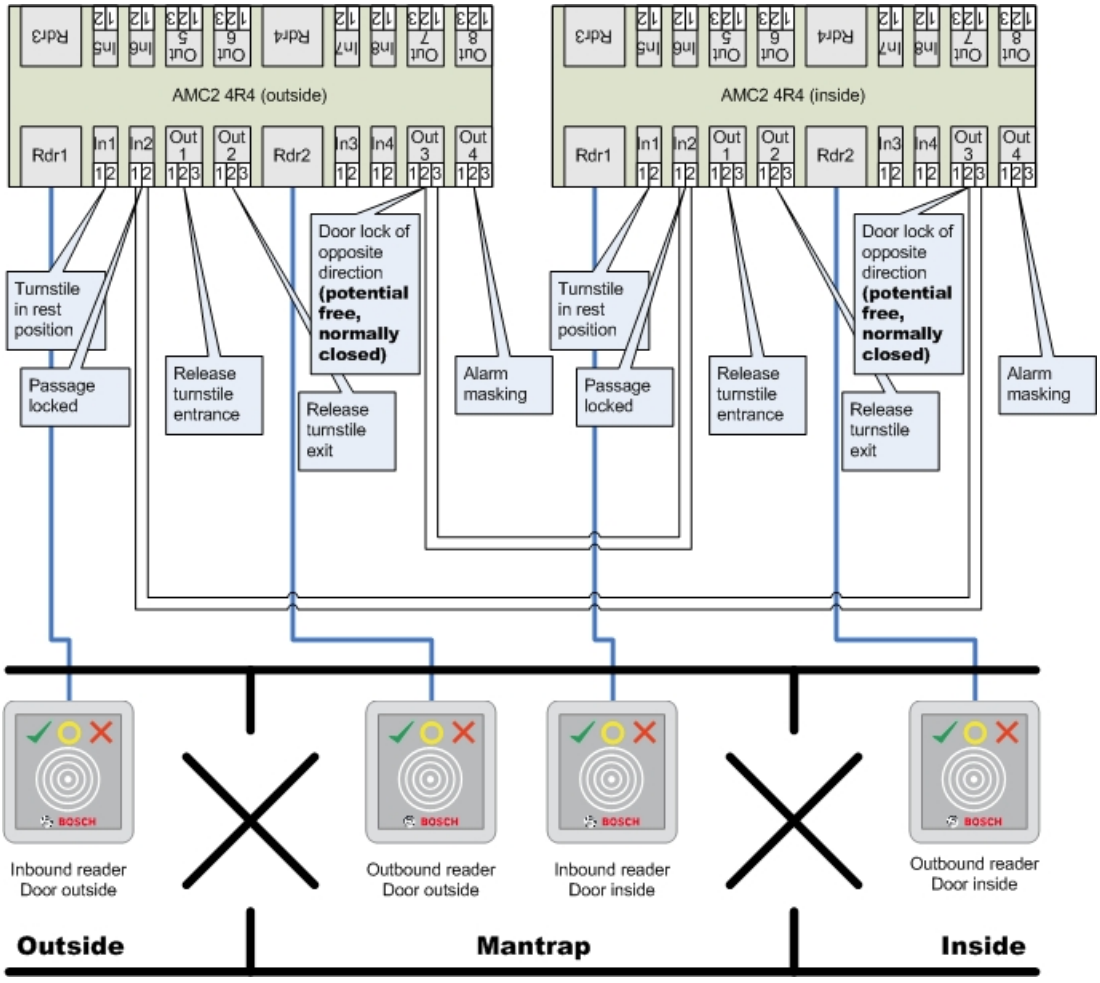
Замечание!

Выходные сигналы 3 и 7 должны быть заданы как потенциально свободные (режим с "сухим" контактом)

Сигнал «Запирание двери в противоположном направлении» активируется при значении 0. Он используется для «нормально закрытых» выходов 3 и 7.

Пример: ловушка на двух контроллерах

Конфигурация ловушки с двумя турникетами (DM 03a), распределенными между двумя контроллерами.



Подключение к дверным замкам для обратного направления гарантирует, что только один из турникетов может быть открыт в каждый момент времени.

Замечание!
Выходной сигнал 3 должен быть настроен как беспотенциальный (режим с «сухим» контактом).
Сигнал «Запирание двери в противоположном направлении» активируется при значении 0. Он используется для «нормально закрытого» выхода 3.

13.7 Двери:

Настройка двери: Основные параметры

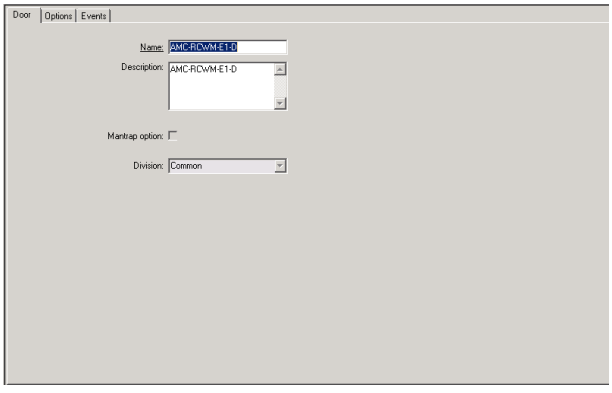
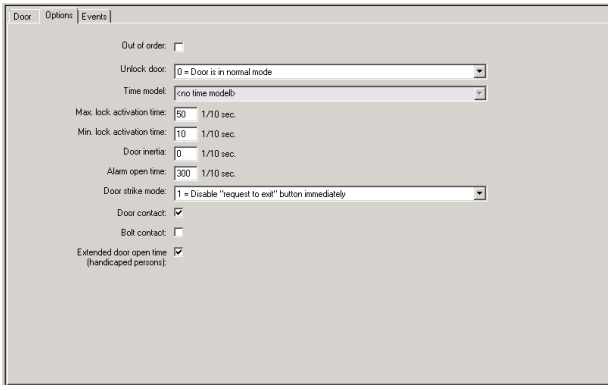


Рис. 13.1:

Параметр	Возможные значения	Описание
Имя	Алфавитно-цифровое значение, до 16 символов	Сгенерированное значение по умолчанию может быть заменено уникальным именем.
Описание	Алфавитно-цифровое значение, до 255 символов	
Подразделение	Подразделение по умолчанию — «Общее»	Это поле доступно только для чтения. Назначения подразделениям осуществляются в редакторе устройств DevEdit для каждой двери в иерархии устройств
Только для моделей дверей 01 и 03, если настроена ловушка:		
Функция ловушки	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Ловушка существует, если две объединенные двери используют модель дверей 01 или 03. Активируйте параметры ловушки для **обеих** дверей. Для данных дверей также потребуется специальная физическая проводка.

Настройка двери. Параметры

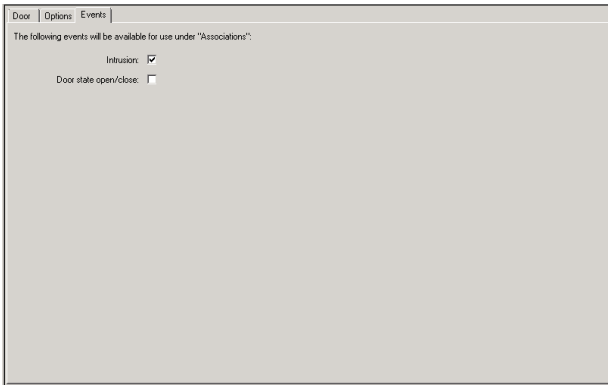


Параметр	Возможные значения	Замечания
Ручная операция	0 = флажок снят 1 = флажок установлен.	0 = дверь находится в нормальном режиме (по умолчанию), то есть контроль доступа осуществляет вся система. 1 = дверь исключена из системы контроля доступа. Данная дверь не контролируется, и сообщения создаваться не будут. Ее можно запереть или отпереть только вручную. Все остальные параметры для этой двери выключены.

		Этот параметр необходимо отдельно задать для двери и считывателя.
Разблокировать дверь	0 = Дверь в нормальном режиме 1 = Дверь открыта 2 = Дверь разблокирована в зависимости от модели времени 3 = Дверь открывается в зависимости от модели времени после первого прохода 5 = Дверь постоянно заблокирована 6 = Дверь заблокирована в зависимости от модели времени	0 = обычный режим (по умолчанию) — дверь блокируется и разблокируется в зависимости от прав доступа учетных данных. 1 = разблокировать на длительный период — контроль доступа на этот период будет приостановлен. 2 = разблокировать на период времени, определенный по временной модели. Контроль доступа на этот период приостанавливается. 3 = заблокировано, пока временная модель активна, до тех пор, пока первое лицо не получит доступ. После этого дверь открыта, пока активна временная модель. 5 = заблокировано, пока не будет разблокировано вручную. 6 = заблокировано, пока активна временная модель — управление дверью отсутствует, дверь нельзя использовать, пока действует временная модель.
Временная модель	одна из доступных временных моделей	Временная модель для времени открывания двери. Если выбраны модели дверей 2, 3, 4, 6 и 7, доступно поле списка для моделей времени. Требуется выбрать временную модель.
Макс. время активации блокировки	0 - 9999	Временной интервал активации устройства открывания дверей по умолчанию (кратно 1/10 с): 50 для дверей, 10 для вращающихся дверей (03) и 200 для барьеров (05с или 09с).
Мин. время активации блокировки	0 - 9999	Минимальный временной интервал для активации устройства открывания двери, кратный 1/10 с. Электромагнитным замкам требуется некоторое время на размагничивание — по умолчанию: 10.
Инерция двери	0 - 9999	По прошествии времени активации дверь может быть открыта в течение этого временного промежутка без подачи сигнала тревоги (кратно 1/10 с). Гидравлическим дверям требуется некоторое время для повышения давления — по умолчанию: 0.

Время в открытом состоянии до тревоги	0 - 9999	Если по истечении данного временного интервала дверь остается открытой, появляется сообщение «дверь открыта слишком долго», кратно 1/10 с — по умолчанию: 300. 0 = без тайм-аута, без сообщений
Режим дверной защелки	Запись в поле списка	0 = Кнопка REX (Запрос на выход) отключается после времени активации 1 = Кнопка REX (Запрос на выход) отключается мгновенно (= по умолчанию)
Дверной контакт	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = у двери нет дверного контакта 1 = у двери есть дверной контакт. Замкнутый контакт обычно означает, что дверь закрыта. (= по умолчанию)
Ригельный контакт	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = у двери нет ригельного контакта (= по умолчанию) 1 = у двери есть ригельный контакт. Сообщение создается, когда дверь открыта или закрыта.
Расширенное время открытия двери (для инвалидов)	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = нормальное время активации замка. 1 = время активации замка увеличивается на коэффициент, заданный параметром EXTIMFAC в масштабах системы. Это даст лицам с ограниченными физическими возможностями достаточно времени для прохода через дверь. (= по умолчанию)

Настройка двери: события

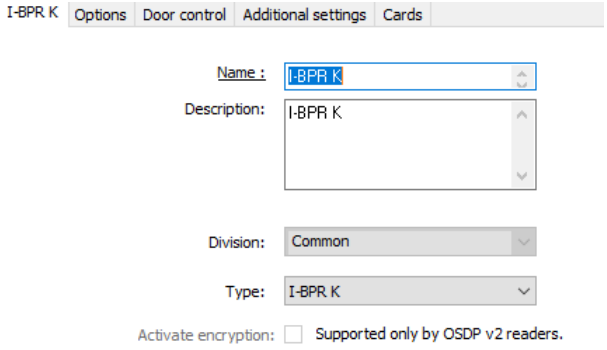


Параметр	**Возможные значения**	**Замечания**
Вторжение	0 = отключено (флажок снят)	0 = нет сообщений о вторжении. Это полезно, если дверь может свободно открываться изнутри.

	1 = включено (флажок установлен)	1 = при неавторизованном открытии отправляется сообщение. Еще одно сообщение укажет на последующее закрытие. (по умолчанию)
Дверь открыта/ закрыта	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = нет сообщения «дверь открыта» (по умолчанию) 1 = при открытии или закрытии отправляется сообщение.

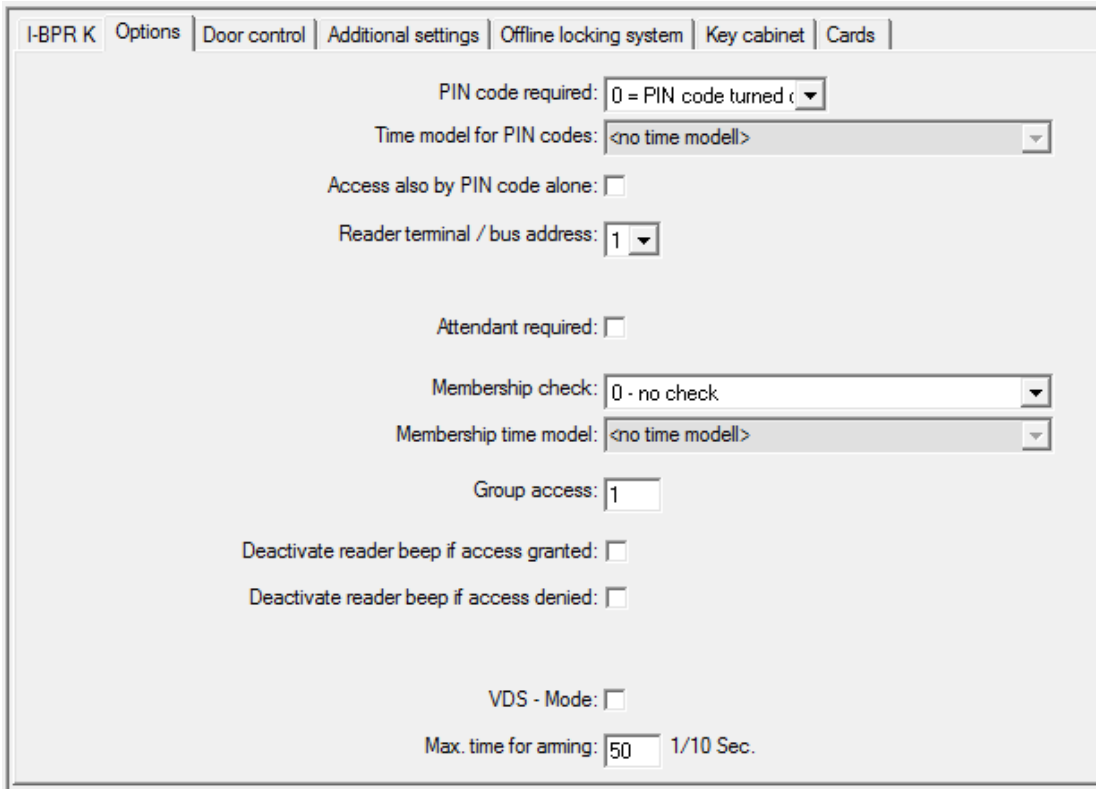
13.8 Устройства чтения

Настройка считывателя. Основные параметры



Параметр	Возможные значения	Описание
Имя считывателя	алфавитно-цифровое значение, 1–16 символов	Данное значение по умолчанию можно заменить уникальным именем.
Описание	алфавитно-цифровое значение: 0–255 символов	Произвольное текстовое описание.
Подразделение	Подразделение по умолчанию — «Общее».	Актуально, только если все подразделения лицензированы и используются.
Тип	алфавитно-цифровое значение, 1–16 символов	Тип считывателя или группы считывателей

Настройка считывателя. Параметры



Параметр	Возможные значения	Описание
Требуется PIN-код	0 = PIN-код отключен — ввод не требуется (по умолчанию) 1 = PIN-код включен — всегда требуется ввод 2 = PIN-код управляется временной моделью — ввод необходим, только когда временная модель не действует	Активируйте это поле только в случае, если у считывателя есть устройство ввода. Обратите внимание, что проверка на авторизацию и последовательность доступа (если она активирована) карты превалирует над правильностью PIN-кода.
Временная модель для PIN-кодов	одна из доступных временных моделей	Выбор временной модели обязателен, если параметру **Требуется PIN-код** задано значение 2.
Также доступ осуществляется исключительно по PIN-коду	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если система контроля доступа настроена соответствующим образом, определяет, может ли этот считыватель разрешать

		доступ исключительно по PIN-коду без карты. См. раздел Доступ исключительно по PIN-коду.
Адрес терминала/ шины считывателя	1 - 4	Для AMC 4W: пронумерованы в соответствии с интерфейсами Wiegand. Для AMC 4R4: пронумерованы как адрес считывателя, заданный перемычками.
Требуется сопровождение	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = посетителю не требуется сопровождающий (по умолчанию) 1 = сопровождающий также должен использовать данный считыватель
Проверка членства	Запись в поле списка	Проверка членства обычно используется на ранних стадиях, прежде чем система управления доступом становится активной. Здесь предоставляется доступ с учетом универсального идентификатора компании, а не уникального идентификатора в качестве учетных данных. **ВАЖНО!** Проверка членства работает только с физическими учетными данными, для которых определения карт предварительно заданы в системе (серый фон), а **не** с пользовательскими определениями или биометрическими учетными данными. **0 — без проверки** Проверка членства выключена, однако карта проверяется на наличие авторизаций в обычном режиме (по умолчанию) **1 — проверка** Карта проверяется только на ID компании, то есть только на членство в системе. **2 — в зависимости от временной модели** Карта проверяется на ID компании (членство), но только в течение периода, определенного во временной модели членства.
Временная модель членства	одна из доступных временных моделей	Эта временная модель позволяет включить/ отключить проверку принадлежности. Выбор временной модели обязателен для варианта 2 **проверки членства**.
Групповой доступ	1 - 10	**Для считывателей с клавиатурой** Минимальное число допустимых карт, которые должны быть предъявлены считывателю карт, чтобы дверь открылась. Данная группа может состоять из большего

		числа карт; в этом случае используется клавиша ENTER/#, чтобы сигнализировать о завершении группы. Затем дверь открывается. **Для считывателей без клавиатуры:** Точное число действительных карт, которые должны быть предъявлены считывателю карт, чтобы дверь открылась. Значение по умолчанию: 1.
Деактивировать звуковой сигнал считывателя, если доступ предоставлен	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активирован (1), то считыватель не подает звуковых сигналов, если авторизованный пользователь получает разрешение на доступ.
Деактивировать звуковой сигнал считывателя, если доступ не предоставлен	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активирован (1), то считыватель не подает звуковых сигналов, если неавторизованный пользователь получает отказ в доступе.
 Функция "Деактивировать звуковой сигнал считывателя" зависит от соответствующего аппаратного обеспечения считывателя. Аппаратное обеспечение некоторых считывателей может не поддерживать эту функцию.		
Режим VDS	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активировано (1), сигнализация считывателя выключена.
Макс. время пост. на охрану	1–100 [1/сек]	Максимальное время ожидания сигнала подтверждения завершения постановки на охрану от охранной панели.

Сеть и режимы работы

Эта вкладка отображается только для сетевых биометрических считывателей.

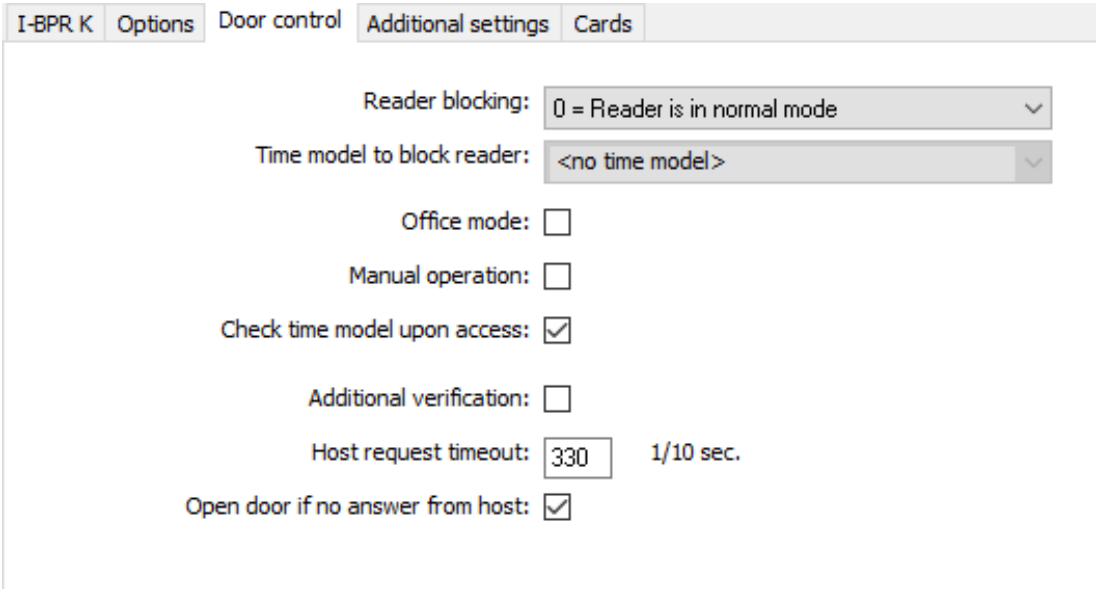
Шаблоны — это сохраненные образцы. Они могут представлять собой данные карт или биометрические данные.

Шаблоны можно хранить как на устройствах, которые в дереве устройств находятся выше считывателя, так и на самом считывателе. Данные о считывателе периодически обновляются устройствами, расположенными над ним.

Считыватель можно настроить для использования собственных шаблонов при принятии решений о доступе или для использования исключительно шаблонов с расположенных выше него устройств.

Параметр	Описание
IP-адрес.	IP-адрес этого подключенного к сети считывателя
Порт:	Порт по умолчанию — 51211
Шаблоны на сервере	
Только карта	Считыватель считывает только данные карт. Он выполняет их аутентификацию относительно данных, полученных от системы.
Карта и отпечаток пальца	Считыватель считывает и данные карт, и данные отпечатков пальцев. Он выполняет их аутентификацию относительно данных, полученных от системы.
Шаблоны на устройстве	
Проверка в зависимости от лица	Считыватель позволяет определять используемый **режим идентификации** по параметрам соответствующего владельца карт. Данные персонала предоставляют следующие возможности: – Только отпечаток пальца – Только карта – Карта и отпечаток пальца Они описаны ниже в этой таблице.
Только отпечаток пальца	Считыватель считывает только данные отпечатков пальцев. Он выполняет их аутентификацию относительно собственных сохраненных данных.
Только карта	Считыватель считывает только данные карт. Он выполняет их аутентификацию относительно собственных сохраненных данных.
Карта и отпечаток пальца	Считыватель считывает и данные карт, и данные отпечатков пальцев. Он выполняет их аутентификацию относительно собственных сохраненных данных.
Карта или отпечаток пальца	Считыватель считывает данные карты или данные отпечатка пальца в зависимости от того, что предлагает владелец карты. Он выполняет их аутентификацию относительно собственных сохраненных данных.

Настройка считывателя. Управление дверьми

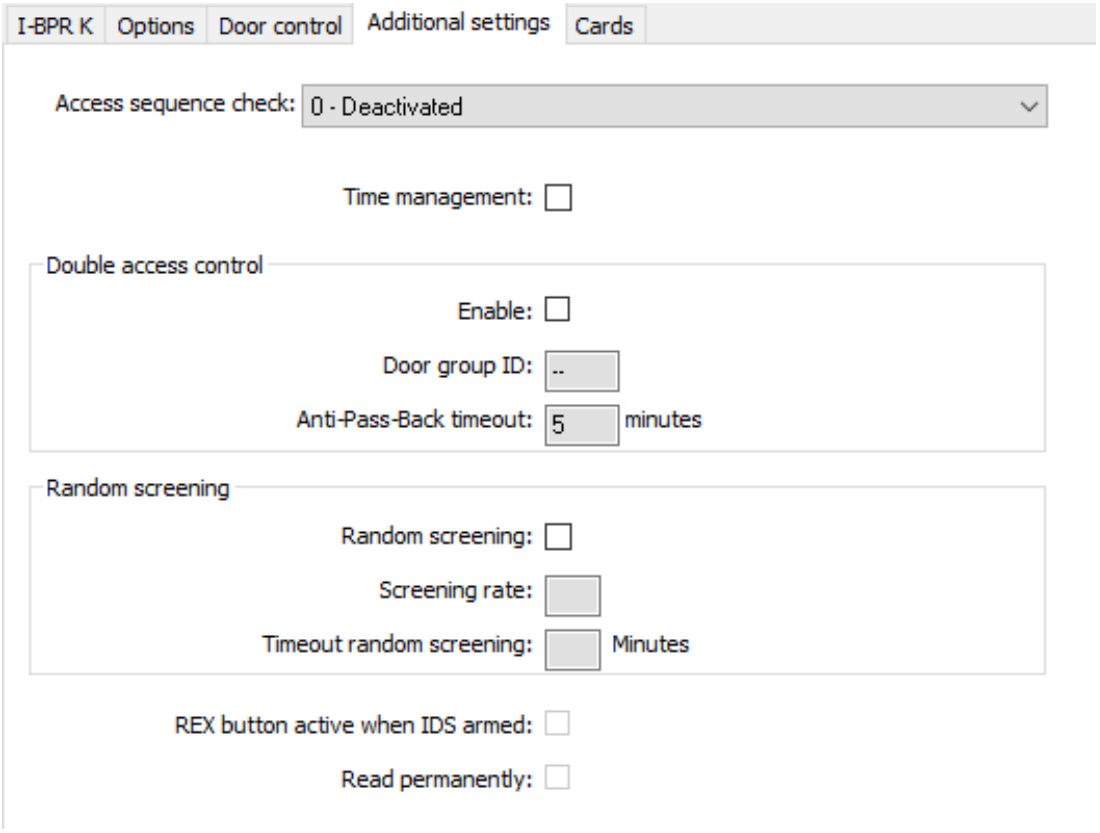


Параметр	**Возможные значения**	**Замечания**
Блокировка считывателя	Запись в поле списка	0 = считыватель в обычном режиме — без блокировки (= по умолчанию) 1 = считыватель постоянно заблокирован — постоянная блокировка 2 = считыватель блокируется в зависимости от модели времени — блокировка осуществляется в соответствии с моделью времени, заданной с помощью параметра *Модель времени для блокировки считывателя*
Модель времени для блокировки считывателя	одна из временных моделей, определенных в системе.	Считыватель блокируется в соответствии с выбранной временной моделью.
Офисный режим	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Позволяет использовать этот считыватель в офисном режиме ,
Ручная операция	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = считыватель в нормальном режиме (=по умолчанию) 1 = считыватель эффективно удаляется из системы контроля доступом, то есть «не работает». Система не получает никаких команд. Все остальные параметры для этого считывателя выключены.

		Этот параметр необходимо задавать независимо и для считывателя, и для двери.
Проверка моделей времени во время доступа	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = модели времени не будут проверяться. Нет ограничений по времени для доступа. 1 = если владельцу карты назначена временная модель (непосредственно или в качестве авторизации по времени и области), временная модель будет проверяться. (= по умолчанию)
Дополнительная проверка	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = проверка оператором не обязательна 1 = требуется проверка оператором (по умолчанию) (**ВАЖНО**! Активация этот параметра необходима для дополнительного видеоподтверждения оператором системы BVMS или BIS)
Ожидание ответа	0 = деактивировано	0 = AMC работает без проверки оператором (не работает с параметрами *Изменение области* или *Подсчет людей*). Этот элемент управления активен, только если параметр «Проверка оператором» = 0 (деактивирован), а параметр *Открыть дверь по исходу времени ожидания* = 1 (активирован). 1–9999 = используемому считывателю требуется запрос BIS. Ответ на запрос должен поступить в течение указанного временного интервала. По истечении данного временного интервала AMC проверяет параметр **Открыть дверь по исходу времени ожидания** и принимает для себя решение. Значения кратны 1/10 с. (По умолчанию = 30)
Открыть дверь по исходу времени ожидания	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Этот элемент управления активен только в том случае, если задан параметр **Проверка оператором**. 0 = не открывает дверь, если требуется решение оператора, но его не удается получить (работа в автономном режиме). 1 = открывает дверь по истечении времени ожидания, если это возможно выполнить с AMC. (= по умолчанию)

Проверка кредитов талонов на парковку	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активировано (1), проверяются кредиты талонов на парковку.
Проверка просроченной парковки	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активировано (1), проверяется просрочка срока парковки.

Настройка считывателя. Дополнительные параметры

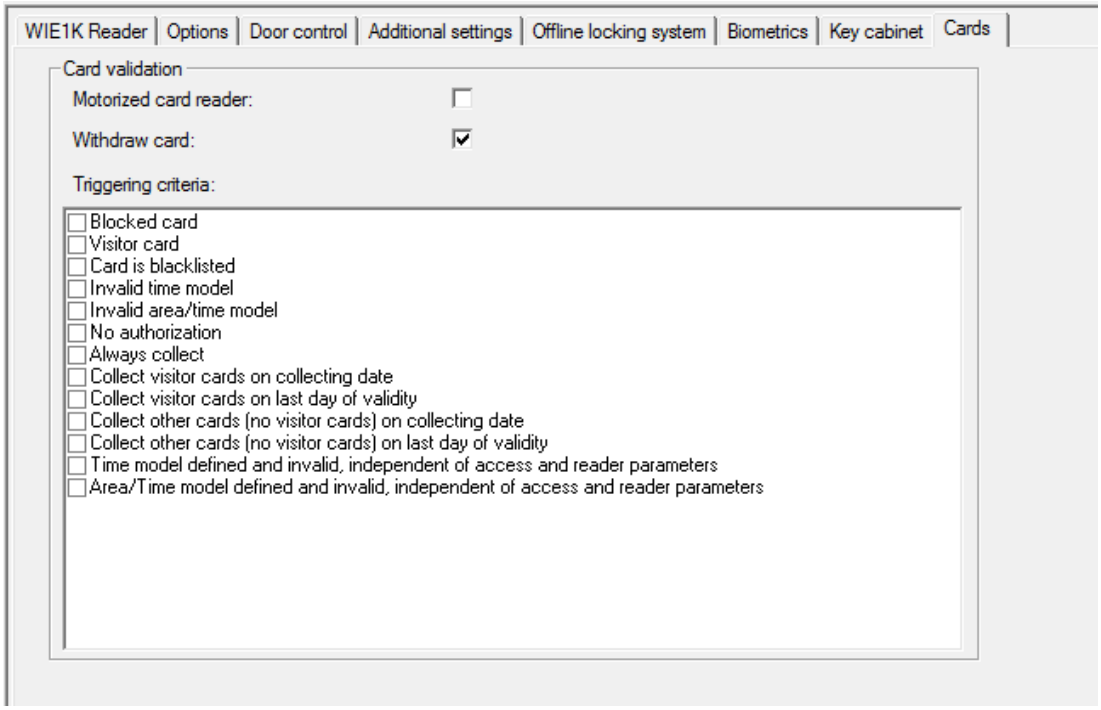


Параметр	**Возможные значения**	**Замечания**
Проверка последовательности доступа	0 — Деактивировано 1 — Активировано; деактивировать по неисправности LAC 2 — Активировано; оставить активным по неисправности LAC 3 - Активировано; используйте четкую последовательность проверки даже при	0 = считыватель не участвует в проверке последовательности доступа (= по умолчанию) Активированная проверка последовательности может обрабатывать лиц с заданным статусом НЕИЗВЕСТНЫЕ указанным ниже образом. 1 = первое чтение карты будет завершено без проверки местоположения. Все контроллеры должны находиться в оперативном режиме.

	неисправности LAC (примечание: обновите местоположение лиц вручную)	2 = первое чтение карты будет завершено без проверки местоположения. 3 = если LAC неисправна, проверка местоположения будет завершена для каждого считывания карты.
 Для платформы BIS есть общая MAC-команда для активации или деактивации всех проверок последовательности доступа. Чтобы деактивировать проверку последовательности доступа на некоторый период времени, задается значение в минутах не более 2880 (= 48 часов). Если задано значение "0", проверка последовательности доступа полностью деактивируется. **Примечание.** Эта команда может изменить проверку последовательности доступа только для тех считывателей, для которых задан параметр **Включить последовательность доступа**. Она не деактивирует/активирует проверку последовательности доступа для *всех* считывателей.		
Учет времени	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Если активировано (1), процесс Ace собирает данные для системы проверки времени присутствия.
Контроль двойного доступа (запрет двойного прохода)		
Включить	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = без контроля двойного доступа (= по умолчанию) 1 = с контролем двойного доступа В течение временного промежутка, задаваемого параметром **Длительность**, этот считыватель и другие считыватели в группе не могут использоваться с одной и той же картой. Если этот параметр активирован, необходимо использовать идентификатор группы дверей, даже если используется один считыватель.
Идентификатор группы дверей	Буквы A–Z и a–z, а также "-" 2 символа	Считыватели можно группировать с помощью идентификатора группы дверей. При предъявлении карты на одном считывателе последующие регистрации блокируются на всех считывателях из данной группы дверей (по умолчанию = **--**), пока не истечет тайм-аут.

Тайм-аут запрета двойного прохода	1 - 120	Данный считыватель можно использовать с одной и той же картой по истечении данного временного интервала. Как только данная карта используется на считывателе не из данной группы, немедленно включается блокировка. Значения задаются в минутах, по умолчанию = 5.
Случайный досмотр	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = без случайного досмотра 1 = случайный досмотр в соответствии с данным фактором не получит разрешения на вход, пока не будет снята блокировка в диалоговом окне **Блокировка**.
Частота досмотра	1 - 100	Процент случайных досмотров для расширенной проверки. Доступно, если включен случайный досмотр.
Время ожидания случайного досмотра	1 - 120	При заданном времени пользователь является объектом случайного досмотра. Значения задаются в минутах - по умолчанию = 5.
Кнопка REX активна, когда IDS под охраной	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Только для **DM10** и **DM14**: если IDS поставлена на охрану, кнопки REX по умолчанию отключены. Поэтому невозможно выйти из наблюдаемой области. Этот новый параметр считывателя активирует кнопку REX, даже если IDS поставлена на охрану. Этот параметр также необходимо задать, если вместо кнопки используется считыватель.
Постоянное считывание	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Считыватель выполняет постоянное считывание, если на нем установлено соответствующее микропрограммное обеспечение производителя.

Настройка считывателя. Карты



Параметр	**Возможные значения**	**Замечания**
Моторизированный считыватель	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Установите этот флажок, если используется моторизованный считыватель карт
Извлечение карты	0 = отключено (флажок снят) 1 = включено (флажок установлен)	«Извлечение» при использовании моторизованного считывателя карт означает физическое удержание карты. При использовании других считывателей карт «Извлечение» означает, что система делает карту недействительной.
Критерий срабатывания	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Выберите в этом списке критерии, которые должны инициировать действие **Извлечение карты**.

Замечание!
Моторизованные считыватели карт могут быть использованы только со считывателями IBPR.

13.8.1 Настройка случайного досмотра

Случайный досмотр — это распространенный метод повышения безопасности объекта путем случайного выбора персонала для дополнительных проверок безопасности.

Требования

- Проход должен быть оборудован ловушкой или турникетом, чтобы никто не смог пройти вплотную за другим человеком без предъявления собственного идентификатора.
- Устройство считывания карт должно присутствовать по меньшей мере в одном направлении прохода.
- Считыватели необходимо настроить на обычное управление доступом.
- Отдельно для каждого считывателя можно настроить генератор случайных чисел.
- При снятии любого блока, заданного системой, в непосредственной близости должна находиться рабочая станция.

Процедура

1. Найдите нужный считыватель в редакторе устройств DevEdit
2. На вкладке **Параметры** установите флажок **Случайный досмотр**.
3. В поле **Процентное соотношение досмотра** введите процент людей, которых требуется досматривать.
4. Сохраните свои настройки.

13.9 Доступ исключительно по PIN-коду

Предыстория

Считыватели с клавиатурой можно настроить таким образом, чтобы они разрешали доступ только по вводу PIN-кода.
Когда считыватели настроены таким образом, оператор BIS может присваивать индивидуальные PIN-коды отдельным сотрудникам. В действительности такие сотрудники получают «виртуальную карту», которая состоит только из PIN-кода. Это называется Идентификационный PIN-код. В отличие от него, Подтверждающий PIN-код — это PIN-код, используемый в сочетании с картой в целях усиления безопасности.

Оператор может вводить PIN-коды для сотрудников вручную или присваивать им PIN-коды, автоматически сгенерированные системой.
Обратите внимание, что те же сотрудники не утратят доступ с помощью физических карт, присвоенных им.

Предварительные условия авторизации для операторов

Право доступа в помещение только по PIN-коду может предоставляться держателю карты только операторами, имеющими специальное право выдачи виртуальных карт. Для предоставления оператору такого права выполните следующие действия:

1. Перейдите в Главное меню > **Конфигурация** > **Операторы и рабочие станции** > **Профили пользователей**
2. Выберите профиль пользователя, который должен получить авторизацию:
   Введите его в текстовом поле **Имя профиля** или воспользуйтесь механизмом поиска для нахождения нужного профиля.
3. В списке диалоговых окон щелкните ячейку, содержащую элемент **Карты**
   Всплывающее окно **Специальные возможности** появляется возле нижней части окна главного окна.
4. Установите флажок **Назначить виртуальные карты (PIN)** на панели «Специальные возможности».

5. Нажмите  или **Применить**, чтобы сохранить изменения

Настройка длины идентификационного PIN-кода для поддерживаемых типов считывателей

Длина введенных вручную или созданных системой PIN-кодов регулируется параметром, заданным в конфигурации системы.

– Главное меню > **Конфигурация** > **Параметры** > **ПИН-коды** > **Длина PIN-кода**

Настройка считывателя для доступа только по PIN-коду

1. Перейдите в Главное меню > **Конфигурация** > **Данные устройства** > **Рабочие станции**

2. В поле **Рабочая станция** выберите рабочую станцию, к которой физически подключен считыватель.
3. Правой кнопкой щелкните рабочую станцию, чтобы добавить считыватель, и выберите **Ввести PIN** или **Сгенерировать PIN**.
4. Выберите считыватель в поле **Рабочие станции**.
   Справа от поля **Рабочие станции** отобразится поле специальной настройки считывателя.
5. Убедитесь, что раскрывающийся список **Использование карты по умолчанию** содержит значение по умолчанию **Виртуальная карта. Использовать PIN-код как карту**.
6. Нажмите  или **Применить**, чтобы сохранить изменения
7. В редакторе устройств DevEdit перейдите к дереву **Конфигурация устройства** 
8. Выберите считыватель и проход, для которого требуется настроить доступ только по PIN-коду.
9. На вкладке **Параметры** установите флажок **Доступ только по PIN-коду.**
10. Нажмите  или **Применить**, чтобы сохранить изменения

13.10 Платы расширения AMC

Создание AMC-I/O-EXT (платы расширения ввода/вывода)

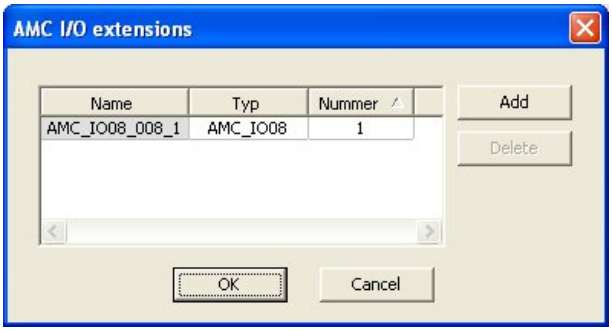
Платы расширения обеспечивают дополнительные входные и выходные сигналы, если восьми контактов, расположенных на AMC, не достаточно для подключения необходимых контактов (например, в случае лифтов).

Такие платы расширения физически подключаются к связанным AMC. В редакторе устройств их можно установить с подчинением соответствующим AMC. При создании AMC-EXT в проводнике выбирается соответствующая запись AMC, а в контекстном меню **Новый объект** — пункт **Новая плата расширения**.

Замечание!

Если нажать кнопку **+**  на панели инструментов редактора устройств, создаются только новые проходы. Платы расширения можно выбрать с помощью контекстного меню.

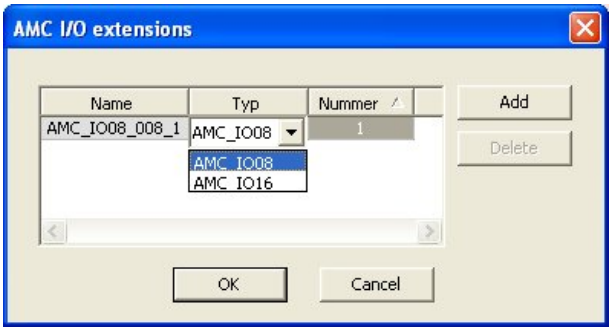
Появляется диалоговое окно для выбора критериев расширений.



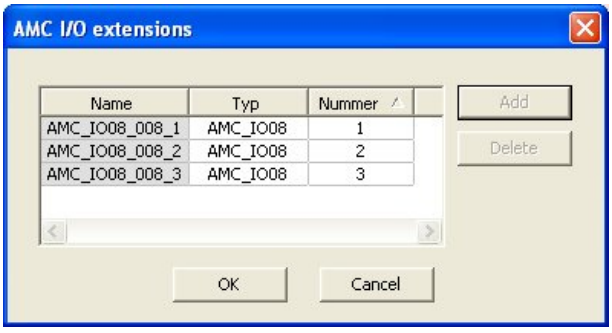
Плата AMC-EXT доступна в двух вариантах:

- AMC_IO08: 8 входов и 8 выходов;
- AMC_IO16: 16 входов и 16 выходов;
- расширение AMC 4W: 8 входов и 8 выходов.

В данном диалоговом окне выбора содержится запись AMC_IO08. Дважды щелкнув поле списка в столбце **Тип**, также можно разместить AMC_IO16.



К одному AMC можно подключить до трех плат расширений. Допускается смешанное использование данных двух вариантов. Нажмите кнопку **Добавить**, чтобы создать другие элементы списка. Все элементы столбцов можно настраивать.



При создании платы расширения нумеруются 1, 2 или 3. Для каждой платы нумерация сигналов начинается с 01. Номер сигнала вместе с номером платы обеспечивают уникальную идентификацию. Сигналы плат расширения также отображаются на вкладке AMC, к которому они относятся.
Таким образом, вместе с входными и выходными сигналами на AMC можно обеспечить до 56 пар сигналов.
Платы расширения можно добавлять по отдельности по мере необходимости или позднее, до максимального числа (по 3 на AMC).

Создание AMC2 4W-EXT

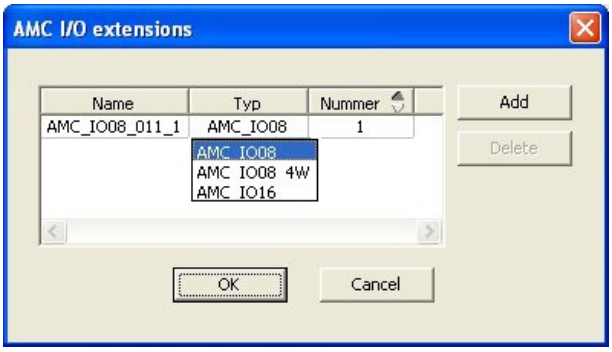
Для контроллеров с интерфейсами считывателей Wiegand (AMC2 4W) можно настроить специальные платы расширения (AMC2 4W-EXT). Каждый из этих модулей обеспечивает подключение четырех дополнительных считывателей Wiegand, а также 8 входных и 8 выходных контактов. Поэтому максимальное число считывателей и дверей, подключаемых через AMC2 4W, можно довести до 8.

Замечание!
AMC2 4W-EXT невозможно использовать в качестве автономного контроллера, только как расширение AMC2-4W. Управление дверями и принятие решений по управлению доступом осуществляет только контроллер AMC2 4W.

AMC2 4W-EXT можно использовать только вместе с AMC2 4W. Так как данная плата поддерживает только интерфейсы считывателей Wiegand, ее невозможно использовать с вариантом AMC2 4R4.
Подобно платам расширения ввода-вывода (AMC2 8I-8O-EXT и AMC2 16I-16O-EXT) AMC2 4W-EXT подключается через интерфейс расширений AMC2 4W. У данной платы расширения нет ни собственной памяти, ни дисплея. Она полностью управляется контроллером AMC2 4W.
К каждому контроллеру AMC2-4W можно подключить одну плату AMC2 4W-EXT и до трех плат расширения ввода-вывода.
Чтобы в системе создать AMC2 4W-EXT, правой кнопкой мыши щелкните в Проводнике нужный родительский контроллер AMC2 4W и в контекстном меню выберите **Новый объект** > **Новая плата расширения**.

Замечание!
Кнопка ✚ на панели инструментов редактора данных устройств используется только для добавления проходов. Платы расширения можно добавлять только через контекстное меню.

Появляется такое же диалоговое окно выбора, как для создания плат расширения ввода-вывода, только в списке для AMC2 4W содержится дополнительный элемент AMC_IO08_4W.



Элемент списка AMC2 4W добавляется только один раз, но можно добавить до трех плат расширения ввода-вывода.

При нажатии кнопки **Добавить** добавляются новые элементы списка. В случае AMC2 4W максимальное число — 4, поэтому можно создать четыре записи для платы AMC2 4W-EXT. Платы расширения нумеруются в порядке создания: 1, 2 или 3. AMC2 4W-EXT получает номер 0 (ноль). Нумерация сигналов AMC2 4W-EXT продолжается с номера этого контроллера (с 09 по 16), тогда как для каждой платы ввода/вывода нумерация начинается с 01. Сигналы для всех плат расширения также отображаются на вкладке соответствующего контроллера AMC2 4W.

Таким образом, вместе с входными и выходными сигналами AMC2 4W можно обеспечить до 64 пар сигналов.

Изменение и удаление плат расширения

На первой вкладке содержатся описанные ниже элементы управления для настройки плат расширения.

Параметр	**Возможные значения**	**Описание**
Имя платы	алфавитно-цифровое значение, ограничение: 1–16 знаков	Идентификация по умолчанию гарантирует уникальность имени, которое, однако, можно перезаписать вручную. Убедитесь в уникальности идентификатора. Для сетевых соединений с DHCP-серверами следует использовать данное сетевое имя.
Описание платы	алфавитно-цифровое значение: 0–255 знаков	Этот текст отображается в данном ответвлении OPC.
Номер платы	1 - 3	Номер платы, подключенной к AMC. Только отображаемое поле.
Источник питания	0 = выключено (флажок установлен) 1 = включено (флажок установлен)	Контроль напряжения питания. В случае электрических пробоев в конце задержки создается сообщение. Данная функция контроля предполагает использование USV, поэтому может быть создано сообщение. 0 = без контроля 1 = контроль активирован

Подразделение	Значение по умолчанию = общее	Это поле только для чтения применимо только в том случае, если функция «Подразделения» лицензирована и используется.

Вкладки «Входные сигналы», «Выходные сигналы» и «Настройки сигналов» имеют макет и функции, совпадающие с соответствующими вкладками контроллеров.

Удаление плат расширения

Плату расширения можно удалить, только если ни один из ее интерфейсов не занят. Сначала связанные с ней сигналы необходимо настроить на другой плате. Только затем становятся доступными кнопка удаления  и пункт контекстного меню **Удалить объект**.

AMC2 4W-EXT

Так как считыватели, занимающие платы расширения, нельзя по отдельности удалять и повторно настраивать, их необходимо удалить вместе с соответствующими проходами. Только после этого можно удалить AMC2 4W-EXT.

14 Пользовательские поля для данных персонала

Введение

Поля данных для персонала можно настраивать многочисленными способами:

- Являются ли поля **видимыми**, то есть отображаются ли они в ACE клиенте в принципе
- Являются ли они **обязательными**, то есть можно ли хранить запись данных, не введя допустимые данные в этом поле
- Должны ли значения, которые они содержат, быть **уникальными** в масштабе системы
- Какие типы данных они содержат (текстовые, дата и время, целочисленные и т. д.)
- Где (на какой вкладке, в каком столбце и какой строке) ACE клиента они отображаются
- Насколько большими они отображаются
- Будут ли данные использоваться в стандартных отчетах и где

Конечно, можно определить совершенно новые поля данных со всеми указанными здесь атрибутами.

14.1 Предварительный просмотр и редактирование настраиваемых полей

Путь к диалоговому окну

- Главное меню > **Конфигурация** > **Параметры** > **Настраиваемые поля**

Основное окно разделено на две вкладки

Обзор Эта вкладка и ее вложенные вкладки (**Адрес, Контакт, Дополнительные личные данные, Дополнительные данные о компании, Примечания, Контроль карт** и **Дополнительные сведения**) доступны только для чтения и содержат примерное представление вида WYSIWYG («что видишь, то и получишь») о том, какие данные будут отображаться и на каких вкладках ACE клиента.

Подробно Эта вкладка содержит список редакторов — по одному для каждого заранее определенного или определенного пользователем поля данных.

Редактирование существующих полей данных

На вкладке **Настраиваемые поля** > **Подробно** у каждого поля данных (предопределенного или определенного пользователем) имеется собственное окно редактора, где можно изменить атрибуты этого поля.

Щелкните в редакторе поля, которое требуется изменить. Активный редактор будет выделен.

Редактируемые атрибуты настраиваемых полей описаны в следующей таблице.

Текст метки	Описание
Маркировка	**Метка** — это метка поля данных в том виде, в котором она отображается в клиенте. Ее можно свободно перезаписывать в соответствии с принятой на объекте терминологией.
Тип поля	**Тип поля** — это тип данных, определяет диалоговый элемент управления, который оператор будет использовать для создания записей в клиенте. Каждый тип поля предоставляет инструменты для проведения проверки определенных вводимых значений на единообразие с целью проверки правильности дат, времени, соблюдения длины текста и числовых ограничений. – **Текстовое поле** – Нажмите кнопку с многоточием рядом, чтобы указать допустимое число символов. – **Флажок** – **Поле даты** – **Время** – **Поле даты и времени** – **Поле со списком** – Введите в открывшемся текстовом поле допустимые значения для вашего поля со списком. Разделите их запятыми или символами возврата каретки. – **Цифровой ввод** – Введите минимальное и максимальное значения числового ввода в соответствующих полях со счетчиком. – **Контроль здания 1** и **Контроль здания 2** – Это специальные элементы управления, которым здесь (в поле **Метка**) можно присвоить другую метку и которые можно связать с командами в пользовательском интерфейсе клиента. Таким образом можно предоставить определенным пользователям (через их карты) разрешение на выполнение определенных операций на объекте. В качестве примера таких операций можно назвать включение прожекторов или контроль специального оборудования.
Видимое	Снимите этот флажок, чтобы поле данных не отображалось в клиенте.
Уникальное	Установите этот флажок, чтобы система отклоняла неуникальное содержимое полей данных. Так, личные номера сотрудников должны быть уникальными.
	Зеленый свет означает, что поле данных в настоящее время **не** используется в базе данных. Красный свет означает, что поле данных в настоящее время используется в базе данных.
Отображать в	Используйте этот раскрывающийся список, чтобы выбрать вкладку клиента, на которой должно отображаться поле данных.
Требуется	Установите этот флажок, чтобы сделать ввод данных в этом поле обязательным. Например, записи всех сотрудников должны содержать их фамилии. Хранить запись данных без фамилии невозможно.

Текст метки	Описание
	Обратите внимание, что редактор не позволит сделать обязательное поле данных невидимым с помощью флажка **Видимое**. Для удобства работы настоятельно рекомендуется помещать все обязательные поля на первую вкладку клиента.
Расположение	Используйте счетчики **Столбец** и **Строка**, чтобы расположить поле данных на вкладке, указанной в раскрывающемся списке **Отображать в**. Обратите внимание, что редактор не позволяет выбрать положение, которое уже используется, или перекрыть существующие поля данных. Используйте счетчик **Ширина (в процентах)**, чтобы задать размер определенных элементов управления с возможностью изменения размера, таких как поля данных. Значение «100 %» означает, что элемент управления займет все пространство, которое еще не занято меткой поля данных.
Размеры	Используйте поля со счетчиком для параметров **Столбец** и **Строка**, чтобы указать число столбцов и строк, которые должны быть заняты на вкладке с именем в раскрывающемся списке **Отображать в**. Обратите внимание, что редактор не позволит перекрыть существующие поля данных.

Создание и редактирование новых полей данных

На вкладке **Настраиваемые поля** > **Подробно** у каждого поля данных (предопределенного или определенного пользователем) имеется собственная область редактора, где можно изменить атрибуты этого поля.

Нажмите кнопку **Новое поле**, чтобы создать новое настраиваемое поле с собственным редактором. Область активного редактора будет выделена.

В этом редакторе доступны те же диалоговые элементы управления, что и для редактирования существующих полей данных (см. таблицу выше), и еще два:

Использовать в отчетах (флажок)	Установите этот флажок, чтобы отображать новое поле данных в стандартных отчетах.
Порядковый номер	Порядковый номер определяет столбец, который будет занимать поле данных в стандартных отчетах.

Замечание!

В настоящее время в **Конструкторе бэйджей** и **Отчетах** поддерживаются только порядковые номера от 1 до 10.

14.2 Правила для полей данных

- Расположение полей данных
  - Каждое поле может отображаться только на одной вкладке.
  - Каждое настраиваемое поле может появиться на любой доступной для выбора вкладке.
  - Поля можно переместить на другие вкладки, изменив запись в раскрывающемся списке **Отображать в**.

- Метка может содержать любой текст длиной не более 20 символов.
- Настраиваемые текстовые поля могут содержать любой текст длиной не более 2000 символов.
- Любое поле можно сделать обязательным, однако необходимо установить его флажок **Видимое**.

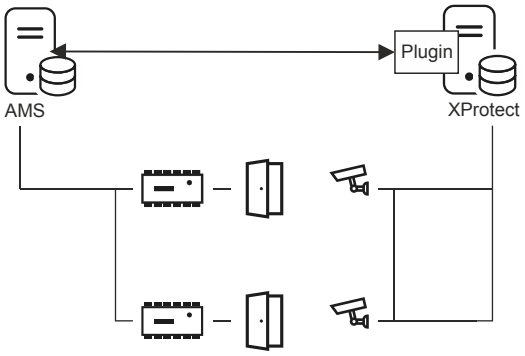
Замечание!
Настоятельные рекомендации перед продуктивным использованием
Согласуйте и определите типы полей и их назначение, прежде чем сохранять в них данные каких-либо лиц.
Каждое поле для ввода данных назначается конкретному полю базы данных, чтобы данные могли быть найдены как вручную, так и генераторами отчетов. После сохранения записей данных из настраиваемых полей в базе данных эти поля больше нельзя перемещать или изменять без риска потери данных.

15 Настройка Milestone XProtect для использования AMS

Введение

В этой главе описывается, как настроить Milestone XProtect для использования функций управления доступом AMS.

Подключаемый модуль, предоставляемый AMS, но установленный на сервере XProtect, передает события и команды в AMS и возвращает результаты XProtect.



Конфигурация состоит из трех этапов, которые описаны в следующих разделах:

- Установка общедоступного сертификата AMS на сервере XProtect.
- Установка подключаемого модуля AMS на сервере XProtect.
- Настройка AMS в приложении XProtect.

Предварительные требования

- AMS устанавливается и лицензируется.
- XProtect устанавливается и лицензируется на том же компьютере или на отдельном компьютере.
- Между обеими системами существует сетевое подключение.

Установка общедоступного сертификата AMS на сервере XProtect

Обратите внимание, что эта процедура требуется только в том случае, если AMS работает на другом компьютере.

1. Скопируйте файл сертификата с сервера AMS
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System \Certificates\Access Management System Internal CA.cer`
   на сервер XProtect.
2. На сервере XProtect дважды щелкните файл сертификата.
   Появляется мастер сертификатов.
3. Нажмите **Установить сертификат...**
   Откроется мастер импорта сертификатов.
4. Выберите **Локальный компьютер** в поле **Местоположение хранилища** и нажмите **Далее**
5. Выберите **Разместить все сертификаты...**
6. Нажмите **Обзор...**
7. Выберите **Доверенные корневые центры сертификации** и нажмите **OK**
8. Нажмите кнопку **Далее**
9. Просмотрите сводку настроек и нажмите **Готово**

Установка подключаемого модуля AMS на сервере XProtect

1. Скопируйте файл настройки
   `AMS XProtect Plugin Setup.exe`
   с установочного носителя AMS на сервер XProtect.
2. Выполните файл на сервере XProtect.
   Откроется мастер настройки.
3. В мастере настройки убедитесь, что подключаемый модуль AMS XProtect помечен для установки и нажмите **Далее**.
   Появится лицензионное соглашение конечного пользователя. Нажмите кнопку **Принять**, чтобы принять условия соглашения, если вы хотите продолжить.
4. Мастер отображает путь установки подключаемого модуля по умолчанию. Нажмите кнопку **Далее**, чтобы принять путь по умолчанию, или нажмите кнопку **Обзор**, чтобы изменить его, прежде чем нажать **Далее.**
   Мастер подтвердит, что он собирается установить подключаемый модуль AMS XProtect.
5. Нажмите **Установить**.
6. Дождитесь подтверждения завершения установки и нажмите **Готово**.
7. Перезапустите службу Windows с именем **Milestone XProtect Event Server**.

Настройка AMS в приложении XProtect

1. В приложении управления XProtect перейдите в раздел **Дополнительные параметры конфигурации** > **Управление доступом**.
2. Щелкните правой кнопкой **Управление доступом** и выберите **Создать новый...**
   Появится мастер подключаемых модулей.
3. Введите следующую информацию в мастере подключаемых модулей:
   - **Имя**: описание этой интеграции AMS-XProtect, позволяющее отличить ее от других интеграций в той же системе XProtect.
   - **Подключаемый модуль интеграции**: `AMS - XProtect Plugin` (это имя будет доступно в раскрывающемся списке после успешной установки подключаемого модуля).
   - **Конечная точка обнаружения AMS API**: `https://<hostname of the AMS system>:44347/`
     , где `44347` — это порт по умолчанию, выбранный при установке AMS API.
   - **Имя оператора**: имя пользователя оператора AMS с разрешениями по крайней мере для использования дверей, к которым будут привязаны камеры XProtect.
   - **Пароль оператора**: пароль AMS этого оператора.
4. Нажмите **Далее**
   Подключаемый модуль AMS подключается к серверу AMS, который вы указали, и выводит элементы управления доступом, которые он обнаруживает (двери, устройства, серверы, команды событий и состояния).
5. Когда индикатор выполнения будет заполнен, нажмите кнопку **Далее**
   Откроется страница мастера камер **Связанные камеры**.
6. Чтобы связать камеры с дверями, перетащите камеры из списка **Камеры** к точкам в списке **Двери**.
7. После завершения нажмите **Далее**.
   XProtect сохраняет конфигурацию и подтверждает, что она успешно сохранена.

16 Настройка управление уровнем угрозы

Введение

Цель управления уровнем угрозы заключается в том, чтобы эффективно реагировать на чрезвычайные ситуации, внося мгновенные изменения в работу проходов во всей затронутой области.

16.1 Концепции управления уровнем угрозы

- **Угроза** — это критическая ситуация, требующая немедленного и одновременного отклика всех или некоторых проходов в системе управления доступом.
- **Уровень угрозы** — это реакция системы на ожидаемую ситуацию. Каждый уровень угрозы должен быть тщательно настроен таким образом, чтобы каждый из проходов MAC знал, как реагировать.

  Уровни угроз полностью настраиваются, например стандартные высокие уровни угрозы можно настроить следующим образом.
  - **Блокировка**: входить могут только службы быстрого реагирования с высоким уровнем безопасности.
  - **Закрытие**: все двери заперты. Как вход, так и выход запрещены для всех учетных данных с уровнем безопасности ниже указанного.
  - **Эвакуация**: все выходные двери открыты.
- Стандартные низкие уровни угрозы можно настроить следующим образом.
  - **Спортивное мероприятие** : двери в спортивные зоны открыты, все другие области защищены.
  - **Вечер родителей**: доступны только выбранные аудитории и главный проход.
- **Предупреждение об угрозе** — это сигнал тревоги, который активирует уровень угрозы. Уполномоченные лица могут активировать предупреждение об угрозе с помощью кратковременного действия, например в пользовательском интерфейсе оператора, с помощью аппаратного сигнала (например, кнопки) или предъявив специальную тревожную карту на любом считывателе.
- **Уровень безопасности** — это атрибут **профилей безопасности** владельцев карт и считывателей в виде целого числа в диапазоне 0–100. Каждый уровень угрозы устанавливает для считывателей главного контроллера доступа (MAC) назначенные уровни безопасности. Затем эти считыватели предоставляют доступ только лицам с учетными данными такого же или более высокого уровня безопасности, заданного в их профилях безопасности.
- **Профиль безопасности** — это набор атрибутов, которые можно назначить **типу персонала** (**Профиль безопасности лица**), двери (**Профиль безопасности двери**) или считывателю (**Профиль безопасности считывателя**). Профили безопасности регулируют следующие типы поведения управления доступом.
  - **Уровень безопасности**, как определено выше, для типа лица, двери или считывателя
  - **Частота досмотра**. Вероятность случайного досмотра этим типом лица или считывателя (в процентах).

16.2 Обзор процесса конфигурации

Для управления уровнями угроз требуются следующие шаги конфигурации, подробно описанные после этого обзора.

1. В редакторе устройств
   - Определение уровней опасности
   - Определение профилей безопасности дверей

- Определение профилей безопасности считывателей
- Назначение профилей безопасности дверей проходам

2. В диалоговом окне «Системные данные»
   - Определение профилей безопасности лиц
   - Назначение профилей безопасности лиц типам лиц
3. В диалоговых окнах данных о персонале
   - Назначение типов лиц соответствующим лицам
   - Назначение типов лиц группам лиц

После успешной настройки управления уровнем угрозы можно отслеживать и контролировать тревоги и состояния устройств контроллера MAC из приложения Map View. Подробные сведения см. в интерактивной справке по Map View.

16.3 Шаги конфигурации в редакторе устройств

В этом разделе описываются необходимые шаги конфигурации, используемые в редакторе устройств.

Замечание!
Данные устройства не могут быть изменены в редакторе устройств, пока действует уровень угрозы.

16.3.1 Создание уровня угрозы

В этом разделе описывается, как создавать уровни угроз для вашего объекта. Можно создать до 15 уровней.

Путь к диалоговому окну

- **Главное меню** > **Конфигурация** > **Данные устройства**

Процедура

1. Выберите вложенную вкладку **Уровни угроз**.
   - Отобразится таблица «Уровни угроз». Она может содержать до 15 уровней угроз, у каждой из которых есть имя, описание и флажок для активации уровня угрозы после настройки.
2. Щелкните строку **Введите название уровня угрозы**.
3. Введите имя, которое будет понятно операторам системы.
4. (Необязательно) В столбце **Описание** введите более полное описание поведения проходов на этом уровне угрозы.
5. **Не** устанавливайте флажок **Активен** сейчас. Сначала выполните все остальные шаги конфигурации для этого уровня угроз, как описано в следующих разделах.
6. Нажмите (Сохранить), чтобы сохранить новый уровень угрозы.

16.3.2 Создание профиля безопасности двери

В этом разделе описывается создание профилей безопасности для различных типов дверей и определение состояния, в которое будут переходить все двери данного профиля при активации определенного уровня угрозы.

Путь к диалоговому окну

- **Главное меню** > **Конфигурация** > **Данные устройства**

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.

Процедура

1. Выберите вложенную вкладку **Профили безопасности дверей**.
   – Главное диалоговое окно разделено на две области: **Выбор** и **Профиль безопасности двери** (имя по умолчанию).
2. Нажмите кнопку **Создать**.
   – Будет создан новый профиль безопасности двери с именем по умолчанию.
   – Таблица **Уровень угрозы** на панели **Профиль безопасности двери** заполняется уже созданными уровнями угроз вместе со значением **не определено** для каждого столбца **Состояние**.
3. В области **Профиль безопасности двери** введите имя типа двери, которому будет назначен этот профиль.
   – Имя нового профиля отобразится на панели **Выбор**. При необходимости его можно удалить из конфигурации, нажав **Удалить** в этой области.
4. (Необязательно) Введите описание профиля, чтобы помочь операторам правильно назначить профиль.
5. Если этот профиль должен быть назначен турникетам, установите флажок **Турникет**.
   – Это предоставит дополнительные параметры для целевого состояния двери на различных уровнях угроз, например параметры, позволяющие входить или выходить только по одному или только вместе.
6. В столбце **Состояние** таблицы **Уровень угрозы** для каждого уровня угроз выберите подходящее целевое состояние для всех дверей данного профиля при срабатывании данного уровня угроз.
7. Нажмите  (Сохранить) для сохранения изменений.

Повторите процедуру, чтобы создать столько профилей безопасности двери, сколько существует типов дверей в вашей конфигурации. Ниже представлены распространенные типы дверей:

– Главная общедоступная дверь.
– Эвакуационный доступ извне.
– Доступ в аудитории.
– Общий доступ к спортивной арене.

16.3.3 Создание профиля безопасности считывателя

В этом разделе описана процедура создания профилей безопасности для различных типов считывателей. Профили безопасности считывателей определяют следующие атрибуты считывателей **для каждого уровня угрозы**.

– Минимальный уровень безопасности, необходимый учетным данным для получения доступа на считывателе.
– Коэффициент досмотра, т. е. процент владельцев карт, которые будут выбраны случайным образом для дополнительной проверки безопасности.
   – **Примечание**. Частота досмотра, заданная в профиле безопасности считывателя, переопределяет частоту, заданную на самом считывателе.

Путь к диалоговому окну

– **Главное меню** > **Конфигурация** > **Данные устройства**

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.

Процедура

1. Выберите вложенную вкладку **Профили безопасности считывателей**.
   – Главное диалоговое окно разделено на две области: **Выбор** и **Профиль безопасности считывателя** (имя по умолчанию).
2. Нажмите кнопку **Создать**.
   – Будет создан новый профиль безопасности считывателя с именем по умолчанию.
   – Таблица **Уровни угроз** в области **Профиль безопасности считывателя** заполняется уже созданными уровнями угроз, а также значением по умолчанию **0** для каждого из них в столбцах **Уровень безопасности** и **Частота досмотра**.
3. В области **Профиль безопасности считывателя** введите имя типа считывателя, которому будет назначен этот профиль.
   – Имя нового профиля отобразится на панели **Выбор**. При необходимости его можно удалить из конфигурации, нажав **Удалить** в этой области.
4. (Необязательно) Введите описание профиля, чтобы помочь операторам правильно назначить профиль.
5. В столбце **Уровень безопасности** таблицы **Уровень угрозы** для каждого уровня угрозы выберите минимальный уровень безопасности (целое число в диапазоне 0–100), который необходим оператору, чтобы работать со считывателем данного профиля при активации этого уровня угрозы.
6. В столбце **Частота досмотра** таблицы **Уровень угрозы** для каждого уровня угрозы выберите процент владельцев карт, которые будут выбираться считывателем случайным образом для дополнительной проверки безопасности при активации этого уровня угроз.
7. Нажмите  (Сохранить) для сохранения изменений.

16.3.4 Назначение профилей безопасности дверей и считывателей проходам

В этом разделе описывается, как назначить профили безопасности дверей и считывателей дверям и считывателям на конкретных проходах.
Первая подпроцедура заключается в том, чтобы идентифицировать и отфильтровать наборы проходов, которые требуется назначить, а вторая процедура — в том, чтобы сделать назначения.
Кроме того, вы можете просмотреть состояния, уровни безопасности и частоты досмотра выбранных проходов, которые будут задаваться различными определенными уровнями угроз, настроенных вами.

Путь к диалоговому окну

– **Главное меню** > **Конфигурация** > **Данные устройства**

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.

Процедура

1. В дереве устройств выберите **DMS** (корень дерева устройств).

2. В главном диалоговом окне выберите вкладку **Управление уровнем угроз**.
   – В главном диалоговом окне появятся несколько вложенных вкладок.

Подпроцедура 1: выбор проходов для назначения

1. Выберите вложенные вкладки **Проходы**.
   – Главное диалоговое окна разделится на две области: **Условия фильтра** и таблицу со всеми проходами, которые были созданы в системе.
2. (Необязательно) В области **Условия фильтра** введите критерии, чтобы ограничить набор проходов, отображаемых в таблице, в нижней части диалогового окна, например:
   – Установите или снимите флажки, определяющие, отображаются ли в таблице **входные считыватели**, **выходные считыватели** и (или) **двери**.
   – Введите символьные строки, которые должны присутствовать в именах проходов, областей, профилей или считывателей всех входов, перечисленных в таблице.
   – Установите или снимите флажок, определяющий, отображаются ли в таблице двери и считыватели, которые еще не настроены.
3. Нажмите **Применить фильтр**, чтобы отфильтровать список проходов, или нажмите **Сбросить фильтр**, чтобы присвоить элементам управления фильтрам значения по умолчанию.

Процедура 2: назначение профилей безопасности выбранным проходам

Предварительное требование. Назначаемые проходы были идентифицированы и отображаются в таблице в нижней части диалогового окна.

Обратите внимание, что каждый проход обычно состоит из двери или барьера и одного или нескольких считывателей карт. Однако у некоторых специализированных типов проходов, таких как **точки сбора**, они могут отсутствовать.

1. В столбце **Профиль безопасности двери или считывателя** щелкните ячейку, соответствующую двери или считывателю, который требуется назначить.
2. Выберите профиль безопасности двери или считывателя из раскрывающегося списка ячейки.

(Необязательно) Предварительный просмотр поведения дверей и считывателей на различных уровнях угроз

Столбцы в правой части таблицы доступны только для чтения. В них отображаются состояние блокировки (**Режим**), **уровень безопасности** и **частота досмотра** дверей и считывателей в таблице, которые были бы актуальными, если бы этот уровень угрозы был выбран в списке **Выберите уровень угрозы для сведений**.

Предварительное требование. Проходы, которые вы хотите просмотреть, определены и отображаются в таблице в нижней части диалогового окна.

- ▸ В списке **Выберите уровень угрозы для сведений** выберите уровень угрозы, который требуется просмотреть.
- ✓ В таблице отображается состояние блокировки дверей (**Режим**), а также **уровень безопасности** и **частота досмотра** считывателей, которые были бы актуальны, когда выбран этот уровень угрозы.

16.3.5 Назначение уровня угрозы аппаратному сигналу

В этом разделе описывается, как назначить аппаратный входной сигнал для активации или отмены предупреждения об угрозе.

Путь к диалоговому окну

– **Главное меню** > **Конфигурация** > **Данные устройства**

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.

Процедура

1. В дереве устройств выберите **проход** под контроллером AMC, входные сигналы которого требуется назначить.
2. В главном диалоговом окне выберите вкладку **Терминалы**.
   – Появится таблица проходов и сигналов.
3. В строке сигнала, который требуется назначить, щелкните ячейку **входного сигнала**.
   – В раскрывающемся списке содержится команда **Уровень угрозы: отключить** и **Уровень угрозы:** <name> для каждого уровня угрозы, который был определен ранее.
   – Команда **Уровень угрозы: отключить** отменяет все текущие уровни угроз.
4. Назначьте команды требуемым входным сигналам.
5. Нажмите (Сохранить) для сохранения изменений.

Замечание!
Ограничение для DM 15
Модель двери 15 (DIP/DOP) в настоящее время не может использоваться для активации уровня угрозы.

16.4 Этапы настройки в диалоговых окнах системных данных

В этом разделе описывается, как создать **профили безопасности лиц** и назначить их **типам лиц**.

16.4.1 Создание профиля безопасности лица

Путь к диалоговому окну

– **Главное меню** > **Системные данные** > **Профиль безопасности лица**

Предварительные требования

Профили безопасности лиц требуют тщательного планирования и предварительной настройки, поскольку они оказывают важное влияние на работу системы в критических ситуациях.

Процедура

1. Если диалоговое окно уже содержит данные, нажмите (Создать), чтобы очистить его.
2. Введите имя нового профиля в текстовом поле «Имя профиля безопасности»:
3. (Необязательно) Введите описание профиля, чтобы помочь операторам правильно назначить профиль.
4. Введите целое число от 0 до 100 в поле **Уровень безопасности**.
   – С учетом того, что владельцу карты разрешено использовать проход, значения 100 достаточно, чтобы получить доступ к любому считывателю, даже если в настоящее время установлен уровень безопасности 100.
   – В противном случае уровень безопасности в профиле безопасности лица владельца карты должен быть равен или больше текущему уровню безопасности считывателя.

5. Введите целое число от 0 до 100 в поле **Частота досмотра**.
   – **Примечание**. Частота досмотра профиля лица является вторичной для профиля считывателя. В таблице ниже описывается взаимодействие двух частот досмотра профиля.
6. Нажмите (Сохранить) для сохранения изменений.

Взаимодействие частот досмотра для профилей безопасности лиц и считывателей

Частота досмотра (%) в профиле безопасности считывателя R	Частота досмотра (%) в профиле безопасности лица P	Лицо выбрано для дополнительных проверок безопасности?
0	Любой	**Нет**
100	Любой	**Да**
1..99	0	**Нет**
1..99	100	**Да**
1..99	1..99	**Возможная** вероятность = MAX(R,P)

16.4.2 Назначение профиля безопасности лица типу персонала

Путь к диалоговому окну

– **Главное меню** > **Системные данные** > **Тип персонала**
– **Клиент ACE** > **Системные данные** > **Тип персонала**

Процедура

Примечание. По историческим причинам **идентификатор сотрудника** здесь является синонимом **типа персонала**.

1. В таблице **Стандартные ID сотрудников** или в таблице **Пользовательские ID сотрудников** выберите ячейку в столбце **Имя профиля безопасности**, соответствующую требуемого типу персонала.
2. Выберите профиль безопасности лица из раскрывающегося списка.
   – Повторите эту процедуру для всех типов сотрудников, которым требуется профиль безопасности лица.
3. Нажмите (Сохранить), чтобы сохранить назначения.

16.5 Шаги конфигурации в диалоговых окнах данных о персонале

В этом разделе описывается, записи о **лицах**, создаваемые в системе, получают **профиль безопасности лица** в соответствии с **типом персонала**.

Пути к диалоговым окнам

– **Главное меню** > **Данные о персонале** > **Лица**
– **Главное меню** > **Данные о персонале** > **Группа лиц**

Примечание. По историческим причинам **идентификатор сотрудника** здесь является синонимом **типа персонала**.

Процедура

Все записи **сотрудников**, созданные в системе, должны иметь **тип персонала**.

1. Убедитесь, что системные операторы назначают только **типы персонала**, которые были связаны с **профилем безопасности лица** в диалоговом окне **Главное меню** > **Системные данные** > **Тип персонала**.
2. Дополнительные сведения о связывании **профилей безопасности лиц** и создании записей **сотрудников** щелкните следующие ссылки.

См.

– *Назначение профиля безопасности лица типу персонала, Страница 124*
– *Создание данных персонала и управление ими, Страница 126*

17 Создание данных персонала и управление ими

Путь к диалоговому окну

Главное меню > **Данные о персонале** > <вложенные диалоговые окна>

Общая процедура

1. Во вложенном диалоговом окне **Лица** введите идентификационные данные этого лица.
2. Во вложенном диалоговом окне **Карты**:
   - назначьте профили доступа или отдельные авторизации на доступ;
   - при необходимости назначьте временную модель;
   - назначьте карту.
3. Во вложенном диалоговом окне **PIN-код**: при необходимости назначьте PIN-код.
4. Во вложенном диалоговом окне **Печать бэйджей** напечатайте карту.

Для **посетителей** выполните следующие действия:

- Введите персональные данные в диалоговом окне **Посетители** меню **Посетители** и назначьте сопровождающего, если необходимо.

Замечание!

Идентификационные карты и авторизации доступа не обязательно назначать одновременно. Поэтому идентификационные карты можно назначить лицам, не назначая им прав доступа, и наоборот. Однако в обоих случаях таким лицам будет отказано в доступе.

Процесс сканирования карт.

При сканировании карт считывателями считыватель выполняет ряд проверок:

- Данная карта действительна и зарегистрирована в системе?
- Владелец карты в настоящее время заблокирован (отключен в системе)?
- Есть ли у владельца карты авторизация доступа для прохода в данном направлении?
- Данная авторизация доступа является авторизацией области/времени? Если да, то время сканирования приходится на периоды, установленные временной моделью?
- Активна ли авторизация доступа, т. е. ее срок действия не **истек** и она не является в данный момент **заблокированной** (отключенной)?
- Владелец карты подчиняется временной модели? Если да, укладывается ли время сканирования в заданные интервалы?
  Предварительное требование. Необходимо включить на соответствующем считыватели проверки временной модели.
- Находится ли владелец карты в правильном местоположении согласно системе мониторинга последовательности доступа?
  Предварительное требование. Мониторинг последовательности доступа включается на соответствующем считывателе.
- Для целевой области этого считывателя определено максимальное число лиц и это число уже достигнуто?
- Если осуществляется мониторинг последовательности доступа, включая запрет двойного прохода: карта сканируется считывателем до истечения времени блокировки, заданного системой запрета двойного прохода?
- Требуется дополнительный PIN-код? **Предварительное требование**. Считыватель оснащен клавиатурой.
- Если используется уровень угрозы, есть ли у **профиля безопасности** владельца карты **уровень безопасности**, который равен по крайней мере равен уровню безопасности считывателя на этом уровне угроз?

17.1 Лица

Данные лиц, для которых установлен флажок **Управляется глобально**, могут изменить только операторы с дополнительным правом **Общий администратор**. Это право задается в диалоговом окне оператора в BIS конфигураторе.
Защищенные данные:

- Все данные диалогового окна **Лица** за исключением вкладки **Замечания** и специально определенных полей дополнительных сведений на вкладке **Дополнительные сведения**.
- Все данные диалогового окна **Карты**.
- Все данные диалогового окна **PIN-код**.

Все остальные данные этих лиц могут редактироваться любым оператором.

В следующей таблице перечислены основные типы данных, которые можно зарегистрировать. Почти все поля необязательны. Обязательные поля четко помечены подчеркнутыми метками в пользовательском интерфейсе.

Вкладка	**Имя поля**
Заголовок диалогового окна	Имя
	Имя
	Фамилия (в некоторых странах называется девичьей фамилией)
	Персональный номер
	Дата рождения
	Идентификатор сотрудника (или тип персонала)
	Пол
	Компания
	Должность
	№ идентификационной карты
	Номер а/м
Адрес	Почтовый индекс
	Улица, дом
	Страна, регион
	Гражданство
Контактная информация	Телефон: проч.
	Телефон компании
	Факс компании
	Мобильный телефон
	Телефон
	Электронная почта

	Адрес веб-страницы
Дополнительные личные данные	Отчество (дополнительное имя, используемое во множестве стран)
	Место рождения
	Семейное положение
	Служебное удостоверение
	№ удостоверения личности
	Действует до
	Рост
Дополнительные данные о компании	Отдел
	Место
	Центр затрат
	Должность
	Сопровождающий (эскорт)
	Причина посещения
	Замечания
Замечания	(Предоставляется текстовое поле для ввода примечаний и замечаний о лице в произвольной форме.)
Дополнительные сведения	10 определяемых пользователем полей
Подпись	Захват, повторная регистрация и удаление подписей
Отпечатки пальцев	Захват, повторная регистрация, удаление и проверка отпечатков пальцев как биометрического удостоверения личности. Назначение определенных отпечатков пальцев для сообщения о действии по принуждению.

17.1.1 Параметры контроля карт/контроля здания

17.1.2 Дополнительная информация: регистрация определенных пользователем сведений

Используйте вкладку **Дополнительная информация** для определения дополнительных полей, которые не предоставлены на других вкладках. Если дополнительные поля не определены, вкладка остается пустой.

17.1.3 Регистрация подписей

В системе необходимо подключить и настроить панель захвата подписей от компании Signotec для захвата подписей. В случае сомнений обратитесь к системному администратору.

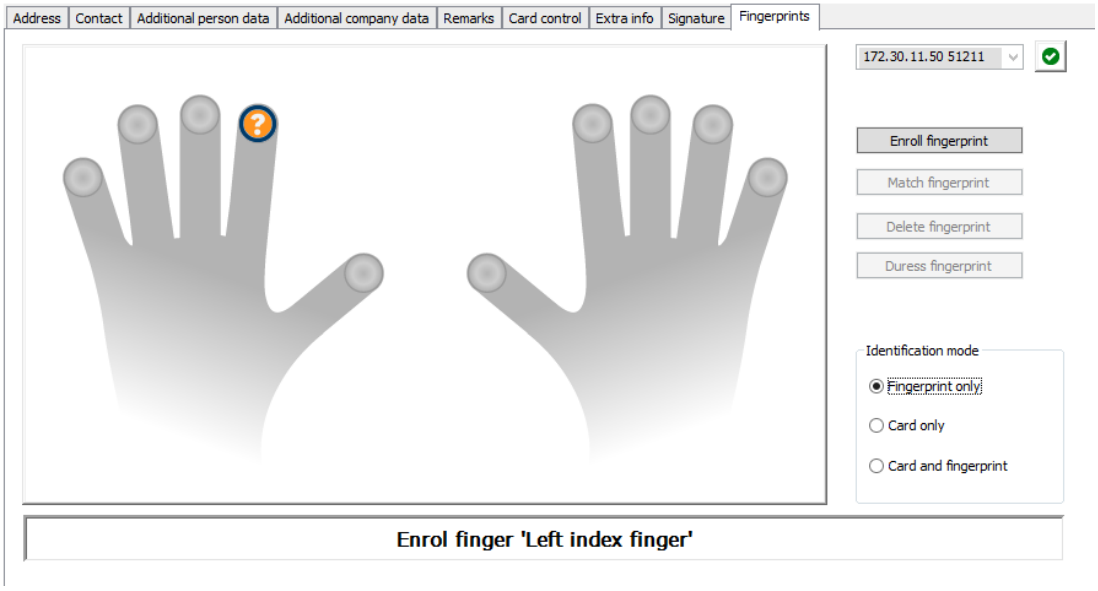
1. Откройте вкладку **Подпись**.
2. Для регистрации новой подписи нажмите кнопку **Захватить подпись**.
3. Оставьте подпись непосредственно на панели захвата с помощью специального пера.

4. Нажмите кнопку с флажком на панели захвата, чтобы подтвердить.
   Теперь на экране отображается новая подпись (щелкните подпись, чтобы увеличить масштаб).

Связанные процедуры:

– Нажмите кнопку **Захватить подпись**, чтобы перезаписать существующую подпись.
– Нажмите кнопку **Удалить подпись**, чтобы удалить существующую подпись.

17.1.4 Регистрация данных отпечатка пальца



Требования

– Для осуществления биометрического управления доступом необходимо настроить один или несколько считывателей отпечатков пальцев.
– ВАЖНО! Эти считыватели периодически получают и хранят данные карт и отпечатков пальцев с серверов. В конечном счете решение о том, какие учетные данные будут приняты, определяется параметрами конкретного считывателя. Они переопределяют любые параметры, заданные для конкретного лица.
– Чтобы использовать отпечатки пальцев в качестве подтверждения (или альтернативы) аутентификации на основе карт, все владельцы карт должны просканировать свои отпечатки пальцев.
– Регистрируемый пользователь должен стоять перед считывателем отпечатков пальцев, подключенным к вашей рабочей станции и настроенным для нее.
– Оператор общается непосредственно с регистрируемым пользователем, то есть с лицом, чьи отпечатки пальцев должны быть зарегистрированы как биометрическое удостоверение личности для доступа.
– Вы неоднократно ознакомились с тем, как следует поместить палец на определенный считыватель, чтобы эффективно захватить отпечатки пальцев.

Процедура регистрации отпечатка пальца для доступа

1. Перейдите в диалоговое окно управления отпечатками пальцев: **Данные о персонале** > **Лица** > вкладка:**Отпечатки пальцев** и создайте или найдите регистрируемого пользователя в базе данных.

2. Спросите регистрируемого пользователя, какой палец он желает использовать для обычного доступа на считывателе отпечатков пальцев.
3. Выберите соответствующий палец на схеме рук.
   Результат: отпечаток пальца будет помечен вопросительным знаком.
4. Нажмите кнопку **Зарегистрировать отпечаток пальца**.
5. Предоставьте регистрируемому пользователю инструкции относительно того, как поместить палец на считыватель.
   Пример инструкций можно просмотреть в диалоговом окне под схемой рук, но для различных типов считывателей процедуры могут немного отличаться.
6. Если отпечаток пальца успешно зарегистрирован, откроется окно подтверждения.
7. Выберите **Идентификационный режим**; эта настройка определяет учетные данные, которые будут проверяться считывателем отпечатков пальцев при запросе доступа. Обратите внимание, что указанный режим действует, только если выбран параметр считывателя **Проверка в зависимости от лица**.
   Параметры:
   - **Только отпечаток пальца** — используется только сканер отпечатков пальцев в считывателе
   - **Только карта** — используется только сканер карт в считывателе
   - **Карта и отпечаток пальца** — используются оба сканера в считывателе. Регистрируемый пользователь должен будет представлять и карту, и выбранный палец, чтобы получить доступ.
8. Нажмите кнопку  (Сохранить), чтобы сохранить отпечаток пальца и идентификационный режим для регистрируемого пользователя.

Замечание!
Параметры считывателя перезаписывают настройки пользователя
Обратите внимание, что идентификационный режим, выбранный в диалоговом окне отпечатков пальцев, будет работать только в том случае, если сам считыватель отпечатков пальцев имеет параметр **Проверка в зависимости от лица** в редакторе устройств. В случае сомнений обратитесь к системному администратору.

Процедура регистрации отпечатка пальца для сообщения о действии по принуждению
Предварительные требования

- По крайней мере один отпечаток пальца регистрируемого пользователя уже успешно зарегистрирован и сохранен.
- Считыватель отпечатков пальцев работает в онлайн-режиме. В автономном режиме считыватель, конечно, не сможет отправить в систему сигнал действия по принуждению.

1. Попросите регистрируемого пользователя выбрать палец, который он желает использовать для сообщения о действии по принуждению, то есть в случае, когда он вынужден использовать считыватель отпечатков пальцев под давлением постороннего лица.
2. Повторите процедуру регистрации отпечатка пальца, описанную выше, для этого пальца.

3. После успешной регистрации второго отпечатка пальца выберите его на схеме рук и нажмите кнопку **Палец по принуждению**.
   Указанный палец по принуждению будет помечен восклицательным знаком на схеме рук.

Если впоследствии регистрируемый пользователь приложит к считывателю палец, зарегистрированный для сигнала о действии по принуждению, и считыватель не будет находиться в автономном режиме, система отправит сигнал о действии по принуждению оператору с помощью всплывающего окна.

Процедура тестирования сохраненных отпечатков пальцев

1. На схеме рук выберите отпечаток пальца, который требуется протестировать.
2. Попросите регистрируемого пользователя поместить палец на считыватель.
3. Нажмите кнопку **Сопоставить отпечаток пальца**.
   Результат: откроется всплывающее окно с подтверждением того, соответствует ли сохраненный отпечаток пальца пальцу на считывателе. Обратите внимание, что эту процедуру может потребоваться повторить для снижения вероятности ложной тревоги.

Процедура удаления сохраненных отпечатков пальцев

1. На схеме рук выберите отпечаток пальца, который требуется удалить.
2. Нажмите кнопку **Удалить отпечаток пальца**.
3. Подождите подтверждения удаления.

17.2 Компании

- Данное диалоговое окно позволяет создавать новые записи о компаниях, а также изменять или удалять существующие данные о компаниях.
- Необходимо ввести название и краткое наименование компании. Краткое наименование должно быть уникальным.
- Если указать компанию в диалоговом окне **Лица** строго обязательно, то прежде чем пытаться создать записи персонала для этой компании, создайте в диалоговом окне эту компанию.
- Компании невозможно удалить из системы, если им назначены какие-либо записи персонала.

17.3 Карты: создание и назначение учетных данных и авторизаций

Цель этого диалогового окна — назначать **карты**, **авторизации доступа** или пакеты авторизаций на доступ, называемые **профили доступа**, записям о персонале.
Авторизации на доступ и профили назначаются лицам, а не картам.
Новые карты, назначенные человеку, получают авторизации на доступ, которые уже назначены этому лицу.

Примечание. Использование профилей доступа для объединения авторизаций

Для единообразия и удобства авторизации на доступ не назначаются по отдельности, а, как правило, объединяются в **профили доступа** и назначаются таким образом.

- Главное меню: **> Системные данные** > **Профили доступа**

Список карт

В диалоговом окне «Карты» отображается список карт, принадлежащих выбранному лицу. В списке указаны, среди прочих, следующие атрибуты.

- Тип использования карты.
- Флаг, указывающий можно ли использовать карту для настроенной автономной системы.
- Сведения о том, заблокирована ли карта в результате многократного использования неверных PIN-кодов. Это состояние выделено особым образом.
- Дата создания карты.
- Дата окончания срока действия (дата сбора) карты.
  Примечание. Если используется моторизованный считыватель кар, он может физически удержать карту с истекшим сроком действия. В противном случае карта просто становится недействительной.
- Дата последней печати карты и количество напечатанных карт.
- Сведения о данных кода.

Параметр **Управляется глобально**

Данные лиц, для которых установлен флажок **Управляется глобально** (флажок рядом с рамкой для фотографии), могут изменить только операторы с дополнительным правом **Общий администратор**.

Операторам без этого права следующие данные доступны только для чтения:

- Все данные в диалоговом окне **Лица** за исключением вкладок **Замечания, Дополнительные сведения** и настраиваемых полей.
- Все данные в диалоговом окне **Карты**.
- Все данные в диалоговом окне **PIN-код**.

Право **Глобальный администратор** можно назначить с помощью следующего флажка:

- Главное меню: **Конфигурация** > **Операторы и рабочие станции** > **Права пользователя** > **Глобальный администратор**.

17.3.1 Назначение карт лицам

Введение

У каждого лица, доступ которого контролируется, должна быть карта или другое электронное удостоверение личности, назначенное держателю карты в диалоговом окне «Карты».

Номера карт могут назначаться вручную или автоматически с помощью считывателя регистрации.

Путь к диалоговому окну

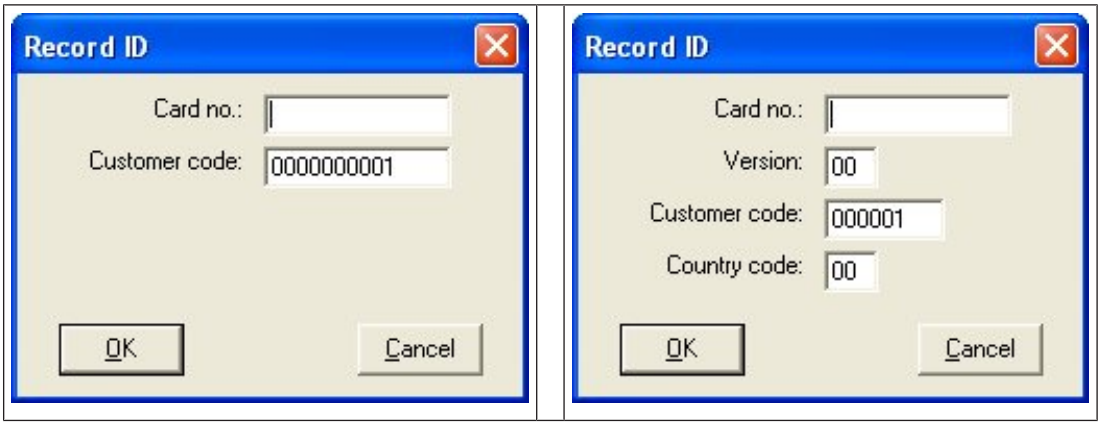
Главное меню > **Данные о персонале** > **Карты**

Требование

Вы загрузили запись персонала, которая должна получить карту в заголовке диалогового окна **Карты**.

Ручной ввод данных карты

Нажмите кнопку **Зарегистрировать карту**, чтобы назначить идентификационную карту лицу. Отобразится маска диалогового окна **Идентификатор записи**. Отобразится одно из двух диалоговых окон ввода в зависимости от типа карты, а также используемых контроллеров и считывателей.



Вручную введите номер, указанный на идентификационной карте. Недостающие знаки номеров карт автоматически заменяются нулями, чтобы длина номера всегда составляла 12 цифр. В некоторых системах в случае потери идентификационной карты новые номера карты идентификации не выдаются. Вместо этого выдается тот же номер идентификационной карты, но с более высоким номером версии. Код страны и код клиента предоставляются производителем. Их необходимо ввести в файле регистрации системы.
Если номер карты еще не используется в системе, он назначается этому лицу. Отобразится всплывающее окно с подтверждением успешного назначения.

Использование считывателя регистрации

Требование

Считыватель регистрации подключен к рабочей станции, с которой вы работаете.

Порядок регистрации

1. Нажмите кнопку справа от кнопки **Зарегистрировать карту**, чтобы выбрать настроенный считыватель регистрации.
2. Нажмите кнопку **Записать карту** и следуйте инструкциям на экране.
3. В зависимости от типа считывателя теперь можно ввести сведения о карте в диалоговом окне или считать данные с карты с помощью считывателя.

Порядок смены карт

1. Выберите карту из списка.
2. Нажмите кнопку **Изменить карту**
3. Измените данные карты во всплывающем окне и нажмите кнопку «OK», чтобы сохранить.

Удаление карт

1. Выберите карту из списка.
2. Нажмите кнопку **Удалить карту**, чтобы удалить назначение лица карте.

Примечание. При удалении последней карты держателя карт состояние держателя карты меняется на **не зарегистрировано** (красная метка рядом с записью **Зарегистрировано** в строке состояния). На это лицо более не распространяется контроль доступа.

17.3.2 Вкладка «Авторизации»

Назначение авторизаций, объединенных в виде профилей доступа

Самый удобный и гибкий способ назначать авторизации владельцам карт — объединять их сначала в профили доступа, а затем назначать им профиль.

– Инструкции по созданию профилей доступа см. в разделе *Создание профилей доступа, Страница 148*
– Чтобы назначить профиль доступа этому владельцу карты, выберите определенный профиль из списка **Профиль доступа**.

Непосредственное назначение авторизаций на доступ

На вкладке **Авторизации**:

Все авторизации на доступ, которые уже назначены лицу, отображаются в списке слева.

Все авторизации на доступ, которые доступны для назначения, отображаются в списке справа.

Выберите элементы, а затем нажмите кнопки между списками, чтобы переместить элементы из одного списка в другой.

 назначает выделенный элемент.

 отменяет назначение выделенного элемента.

 назначает все доступные элементы.

 отменяет назначение всех назначенных элементов.

Параметр: **Сохранение назначенных авторизаций**

Результат назначения профиля доступа лицу зависит от флажка **Сохранение назначенных авторизаций**:

– Если флажок не установлен, то при назначении профиля доступа любой сделанный до этого выбор и любые уже назначенные авторизации доступа **замещаются**.
– Если флажок установлен, авторизации выбранного профиля **добавляются** к ранее назначенным авторизациям.

Ограничение сроков авторизаций

Используйте поля дат **Действительно с:** и **Действительно до:**, чтобы ограничить время начала и окончания действия авторизацией и профилей. Если никакие значения не заданы, авторизации вступают в силу немедленно и действуют бессрочно.

Нажмите  , чтобы открыть диалоговое окно и задать продолжительной отдельных авторизаций.

Отображение входов авторизации

Щелкните правой кнопкой мыши авторизацию в любом списке, чтобы отобразить список относящихся к ней входов.

17.3.3 Вкладка других данных: исключения и специальные разрешения

Назначение временной модели

В поле выбора **Временная модель** укажите ежедневные часы допуска держателя карты, то есть периоды времени, когда держатель карты будет иметь доступ по своему удостоверению личности.

Исключение лиц из случайного досмотра
Установите флажок **Исключено из случайного досмотра**, чтобы исключить лиц из случайного досмотра на входе и выходе.

Исключение лиц из проверок PIN-кода
Установите флажок **Отключить проверку PIN-кода**, чтобы держателям карт не приходилось вводить PIN-коды в считыватели PIN-кодов в нерабочее время.

Замечание!
Исключение из проверок PIN-кода влияет на всю систему.
Например, поскольку PIN-коды этих лиц не проверяются, они также не могут включить или отключить сигнализацию на проходах для модели дверей 10.

Увеличение времени открытия дверей
Установите флажок **Расширенное время открытия двери**, чтобы в три раза увеличить время, необходимое лицам с ограниченными возможностями для прохода, прежде чем активируется состояние **Дверь открыта слишком долго**.
Мониторинг маршрута
Маршрут патрулирования или **Маршрут** — это четкая последовательность считывателей, определенная в меню **Мониторинг маршрута** > диалоговое окно **Определить маршруты** в клиенте.
Чтобы назначить маршрут держателю карты, установите флажок **Мониторинг маршрута** и выберите определенный маршрут в раскрывающемся списке. Если маршруты не определены, флажок будет неактивен.
Если **Маршрут** назначен держателю карты, он активируется, как только держатель карты сканирует карту в первом считывателе в последовательности. После этого все считыватели в последовательности должны использоваться в определенном порядке, пока не будет завершен маршрут. Обычно это применяется, когда необходимо реализовать строгую последовательность доступа в чистых промышленных средах, зонах с контролем гигиены или зонах повышенной безопасности.
Разрешение на разблокировку дверей
Установите этот флажок, чтобы позволить держателю карты разблокировать двери на длительный период времени (см. раздел **Офисный режим**).

17.3.4 Авторизация лиц для настройки офисного режима

Введение
Термин «Офисный режим» описывает приостановку управления доступом на входе в рабочее время. Вход не блокируется в течение этого периода времени, обеспечивая беспрепятственный общественный доступ. В другое время применяется обычный режим, то есть доступ предоставляется только лицам, которые подносят действительные идентификаторы к считывателю.
Офисный режим является стандартным для компаний розничной торговли, образовательных и медицинских учреждений.

Требования
Чтобы офисный режим работал, должны быть соблюдены следующие требования:
В конфигурации (дерево устройств)

– Необходимо разрешить продолжительные периоды разблокировки для одного или нескольких входов.
– Необходимо использовать хотя бы один считыватель с клавиатурой на входе.

В клиенте (диалоговые окна «Люди»)
– Необходимо предоставить возможность включать и отключать офисный режим на входе одному или нескольким владельцам карт.
– Их карты должны быть действительными и разрешать доступ на вход в нерабочее время.

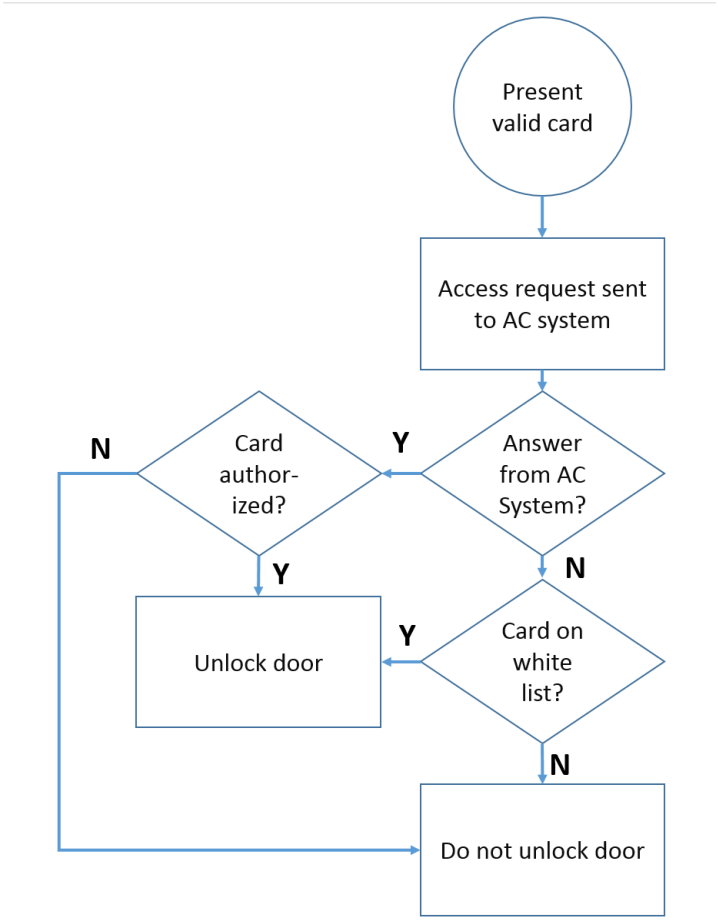
Процедуры для авторизации лиц, способных задать офисный режим
Процедуры для отдельных держателей карт
1. Перейдите в раздел: **Данные о персонале** > **Карты** > вкладка:**Другие данные** и создайте или найдите выбранного держателя карты в базе данных.
2. Установите флажок **Разрешение на разблокировку дверей**.
3. Нажмите кнопку с изображением дискеты  , чтобы сохранить данные о владельце карты.

Процедура для групп держателей карт
1. Перейдите в раздел: **Данные о персонале** > **Группы лиц** и используйте критерии фильтрации для создания списка держателей карт в окне списка.
2. В раскрывающемся списке **Поле для изменения** выберите **Разблокировать двери**
3. Установите флажок **Разблокировать двери**.
4. Нажмите кнопку **Применить изменения**, чтобы сохранить данные о держателе карт.

Инструкции держателю карты о том, как запустить и остановить офисный режим
Для запуска или остановки офисного режима на входе держатель карты должен нажать цифру 3на клавиатуре и затем поднести к считывателю карту с особой авторизацией. Вход остается открытым, пока авторизованный держатель карты не нажмет 3 и снова предъявит карту.
Обратите внимание, что с помощью карты охранника можно таким же образом остановить офисный режим без специального разрешения.

17.3.5 Вкладка Smartintego

Системы блокировки SmartIntego
Введение
Считыватель карт SmartIntego сначала пытается разрешить доступ через основную систему контроля доступа. В случае сбоя подключения система ищет номер карты в сохраненном белом списке.



Авторизации доступа к системе блокировки SmartIntego назначаются в целом так же, как любые другие авторизации доступа.

Требования

- Система блокировки SimonsVoss SmartIntego настраивается в рамках вашей системы управления доступом. См. инструкции в руководстве по конфигурации.
- Держатели карт должны использовать карты MIFARE Classic или MIFARE Desfire. SmartIntego использует серийный номер карты (CSN).

Процедура назначения

Ниже описано, как добавить номер карты в белый список SmartIntego в дополнение к любым другим авторизациям, уже назначенным через основную систему управления доступом.

Белые списки хранятся локально на дверях SmartIntego, поэтому считыватель может предоставить доступ для находящихся в белом списке номеров карт даже в том случае, если подключение к MAC нарушено.

Добавления и удаления карт из белых списков передаются на считыватели SmartIntego сразу после сохранения данных держателя карты при наличии подключения.

1. В главном меню клиента AMS нажмите **Данные о персонале** > **Карты**.
2. Выберите лицо, которое получит авторизации SmartIntego
3. Перейдите на вкладку **SmartIntego.**
4. Выполните назначения:
   - Все авторизации на доступ, которые уже назначены лицу, отображаются в списке слева.

– Все авторизации на доступ, которые доступны для назначения, отображаются в списке справа.

Выберите элементы, а затем нажмите кнопки между списками, чтобы переместить элементы из одного списка в другой.

 назначает выделенный элемент.

 отменяет назначение выделенного элемента.

 назначает все доступные элементы.

 отменяет назначение всех назначенных элементов.

17.3.6 Создание карты для предупреждения об угрозе

В этом разделе описана процедура создания карты для предупреждения об угрозе, которую можно использовать для активации уровня угрозы.

Введение

Карта для предупреждения об угрозе — это карта, которая активирует определенный уровень угрозы при предъявлении на считывателе. Уровень угрозы нельзя отменить с помощью карты для предупреждения об угрозе, это можно сделать только в программном обеспечении для управления доступом.

Предварительные требования

– В системе установлен считыватель для записи данных на карту.
– В системе определен как минимум один уровень угрозы.

Путь к диалоговому окну

Главное меню > **Данные о персонале** > **Карты** > **Карта для предупреждения об угрозе**

Процедура

1. Загрузите запись о сотруднике лица, которому будет назначена карта для предупреждения об угрозе.
2. На вкладке «для предупреждения об угрозе» щелкните «Зарегистрировать карту».
   – Отобразится всплывающее окно: **Выберите уровень угрозы**.
3. Во всплывающем окне выберите требуемый уровень угрозы и нажмите кнопку **ОК**.
   – Отобразится всплывающее окно: **Запись ID бэйджа**.
4. Введите стандартные данные карты, соответствующие установке, и нажмите кнопку **ОК**.
   – Записанная вами карта для предупреждения об угрозе отобразится в списке на вкладке **Карта для предупреждения об угрозе**.

17.4 Временные карты

Временная карта — это временная замена карты, которая была утеряна владельцем карты. Это дубликат, который содержит все авторизации и ограничения оригинала, включая права на автономные двери.

Во избежание злоупотреблений система может произвольно заблокировать одну или все остальные карты владельца карты в течение ограниченного периода времени или до разблокировки вручную.

Следовательно, временные карты **не подходят** для использования в качестве карт для посетителей.

Требования

– Оператор имеет доступ к считывателю регистрации, настроенному на рабочей станции.
– Подходящая физическая карта доступна для регистрации в системе в качестве временной карты.
– У получателя временной карты уже есть хотя бы одна другая карта.

Главное меню > **Данные о персонале** > **Карты**

Порядок действий: назначение временных карт

1. Загрузите требуемый отчет о персонале в диалоговом окне **Карты**
2. В списке карт выберите карту или карты, для которых требуется временная замена
3. Нажмите **Изменить карту**
4. Во всплывающем окне **Изменить карту** выберите **Временная карта**
5. В списке **Период** выберите один из следующих вариантов:
   – **Сегодня**
   – **Сегодня и завтра**
   – **Введите число дней**
6. Если выбран последний вариант, введите в поле целое число дней.
   Обратите внимание, что во всех этих трех случаях срок действия **периода** истекает в полночь соответствующего дня.
7. При необходимости установите флажок **Деактивировать все карты прямо сейчас**.
   – В этом случае все карты, принадлежащие этому владельцу, будут заблокированы.
   – Если флажок снят, будет заблокирована только карта, выбранная выше.
8. При необходимости установите флажок **Активировать карты автоматически после периода**.
   – Заблокированные карты будут разблокированы автоматически, когда определенный выше **Период** истечет.
9. Размещение временной карты в считывателе регистрации
10. Нажмите кнопку **ОК**
    ИД бэйджа запишется считывателем регистрации.
    – Временная карта отображается как активная ✔ в списке карт; кроме того, отображаются данные о сроке ее действия и данные кода.
    – Другая карта или карты отображаются как заблокированные ✘ в зависимости от настройки, сделанной выше: **Деактивировать все карты прямо сейчас**.
11. (Необязательно) В списке карт щелкните столбец **Дата сбора данных** для временной карты и установите дату ее возврата владельцем.
    Значение по умолчанию — **Никогда**.

Процедура: удаление временных карт

Когда исходная утерянная карта будет найдена, удалите временную карту следующим образом.

1. Загрузите требуемый отчет о персонале в диалоговом окне **Карты**.
2. В списке карт выберите временную карту.
3. Нажмите **Удалить карту**
   Временная карта удаляется из списка, а карта или карты, которые она заменяет, немедленно разблокируются

Порядок действий. Удаление временных блокировок карт

Если блокировать исходную карту больше не требуется, удалите блокировку следующим образом:

1. Перейдите в диалоговое окно **Блокировка**: **Данные о персонале** > **Блокировка**.
2. В списке карт выберите персональную карту, помеченную как заблокированная в столбце **Блокировки**.
3. Щелкните **Отменить временную блокировку**
   Обратите внимание, что запись в списке **Блокировка** сохраняется. Список содержит только историю всех блокировок для текущей записи о персонале (прошлых и действующих).

Примечания по временным картам

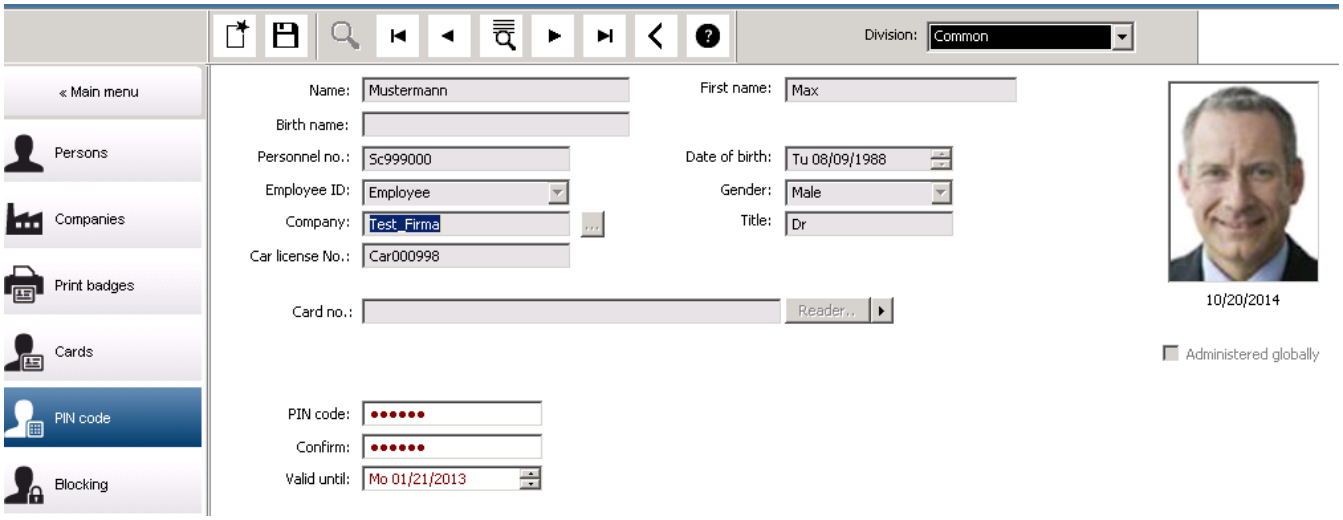
- Система не позволяет заменять временные карты временными картами.
- Система не позволяет создавать несколько временных карт для одной персональной карты.
- Для просмотра краткой сводки по всем картам, принадлежащим владельцу, наведите указатель мыши на небольшую панель с левого края, помеченную как **Зарегистрированные**, в строке состояния основного диалогового окна.

17.5 PIN-коды для персонала

Диалоговое окно: PIN-код

Для доступа к зонам с более высокими требованиями к безопасности авторизации доступа может быть недостаточно. Здесь также необходимо ввести PIN-код. У каждого лица или идентификационной карты может быть PIN-код, действительный для всех областей. Система предотвращает использование очень простых кодов (например, 123456 или палиндромы, такие как 127721). В данном диалоговом окне можно ограничить срок действия и указать его для каждого лица.
Если PIN-код блокирован или срок его действия истек, в доступе к области, требующей этот код, будет отказано даже в том случае, если идентификационная карта по-прежнему действительна для всех остальных областей.

Если ввести неверный код три раза подряд (настройка по умолчанию, которую можно задать в пределах 1–99), данная карта блокируется, т. е. по карте будет отказано в доступе во все области. Заблокированную таким образом карту можно разблокировать только в диалоговом окне Блокировка.



Введите новый PIN-код в поле ввода **PIN-код**, затем введите его еще раз для подтверждения. Длина PIN-кода (от 4 до 9 знаков, значение по умолчанию — 6) настраивается системным администратором.

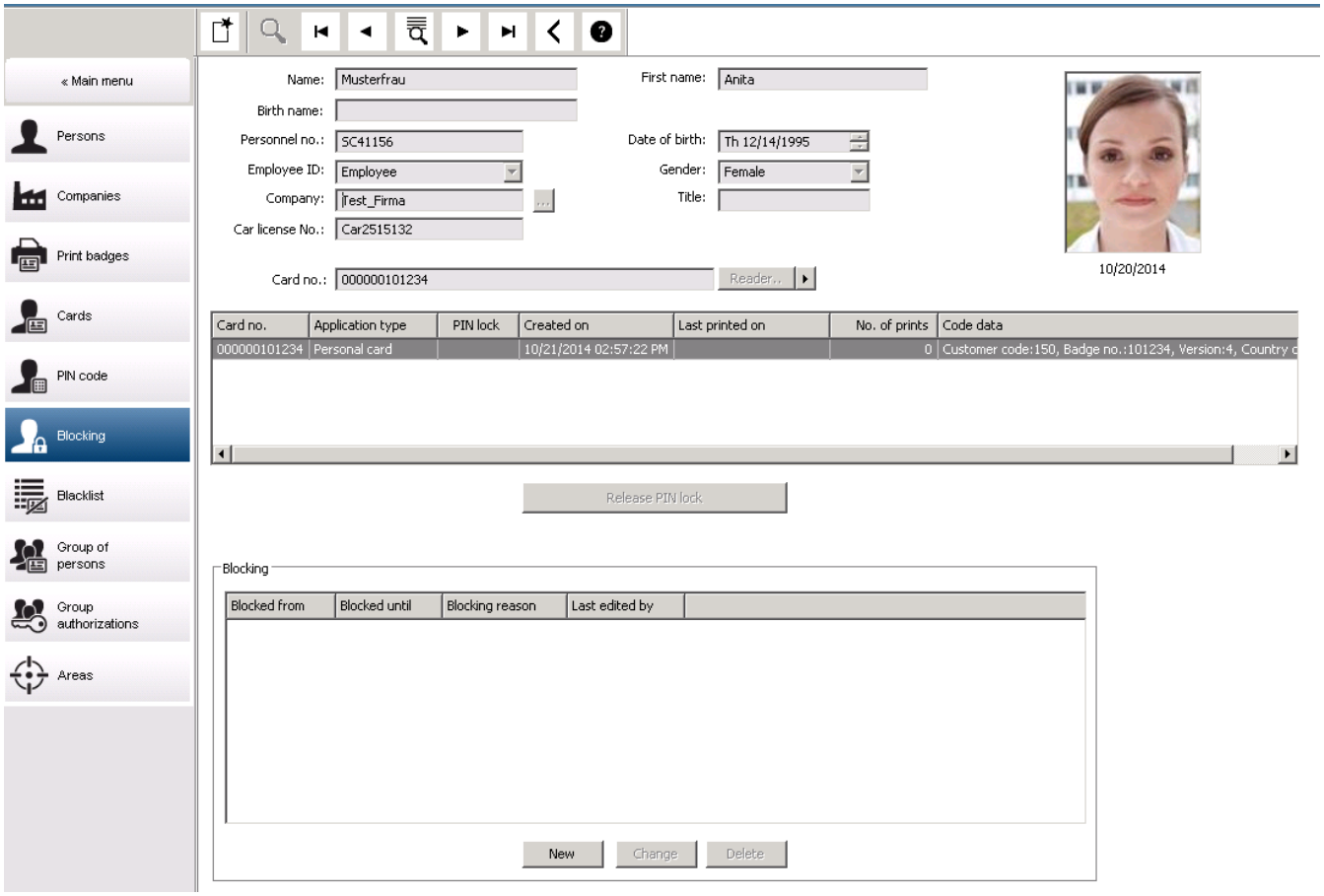
Замечание!
Способ ввода идентификационных PIN-кодов держателями карт зависит от типа считывателей, настроенных в системе. Например:
В считывателях карт RS485 держатель карты вводит: **4 #** `<the PIN>`
В считывателях карт Wiegand держатель карты вводит: `<the PIN>` **#**
Сообщите держателям карт, как вводить PIN-код. В случае сомнений обратитесь к системному администратору.

PIN-код для постановки на охрану систем охранной сигнализации (IDS)
Введите PIN-код из 4–8 цифр (по умолчанию длина = 6, как и у верификационного PIN-кода). Этот PIN-код будет использоваться для постановки на охрану IDS.
Отображение этих полей можно параметризовать. Элементы управления доступны, только если активирован элемент управления **Отдельный PIN-код IDS**.
– Главное меню > **конфигурация** > **Параметры** > **ПИН-коды**
При необходимости выберите дату окончания срока действия.
Если поля для ввода PIN-кода IDS недоступны, IDS также можно поставить на охрану и снять с охраны с помощью PIN-кода верификации. Однако если в данном диалоговом окне отображаются поля ввода, для IDS можно использовать только PIN-код постановки на охрану.
Настройка по умолчанию: поля для ввода PIN-кода постановки на охрану не видны.

PIN-коды тревоги (принуждения)
Лица под принуждением могут активировать бесшумный сигнал тревоги с помощью специального PIN-кода. Поскольку необходимо, чтобы бесшумный сигнал тревоги остался незамеченным со стороны агрессора, доступ предоставляется, но операторы системы получают оповещение о действии по принуждению.
Возможны два варианта, которые активируются одновременно, и подвергнувшееся угрозе лицо может выбирать между ними:
– Ввести PIN-код в обратном порядке (321321 вместо 123123).
– Увеличить значение PIN-кода на 1 (например, 123124 вместо 123123). Обратите внимание, что если последняя цифра — 9, то PIN-код по-прежнему увеличивается, например для PIN-кода 123129 PIN-кодом по принуждению будет 123130.

17.6 Блокирование доступа для персонала

Диалоговое окно: "Блокировка"
В определенных ситуациях необходимо временно блокировать некоторое лицо или снять блокировку, наложенную главным контроллером доступа MAC, например из-за трехкратного ввода неверного PIN-кода или для проведения случайного досмотра.
Блокировка означает, что этому человеку будет отказано в любом доступе независимо от используемых учетных данных.



1. Выберите человека как обычно.
2. На панели «Блокировка» нажмите **Создать** или «Создать блокировку для выбранного лица».
3. Во всплывающем диалоговом окне введите дополнительную информацию:
   - **Заблокировано с/до**: (если конечные дата и время не указаны, доступ для лица останется заблокированным до тех пор, пока не будет снят вручную).
   - **Тип блокировки:**
   - **Причина блокировки:** (Для записи человека, если тип блокировки — `Manual`)
4. Нажмите **Сохранить** во всплывающем окне, чтобы сохранить блокировку.

- При необходимости выберите блокировку из списка и нажмите **Изменить** или **Удалить**, чтобы изменить или удалить ее.

Если в качестве типа блокировки выбрано значение **Блокировка вручную**, введите для записи человека значение **Причина блокировки**.

Замечание!
Блокировка применяется к лицу, а не к определенным учетным данным. Поэтому невозможно отменить или избежать блокировки в результате назначения новой идентификационной карты.

17.7 Занесение карт в черный список

Диалоговое окно: "Черный список"

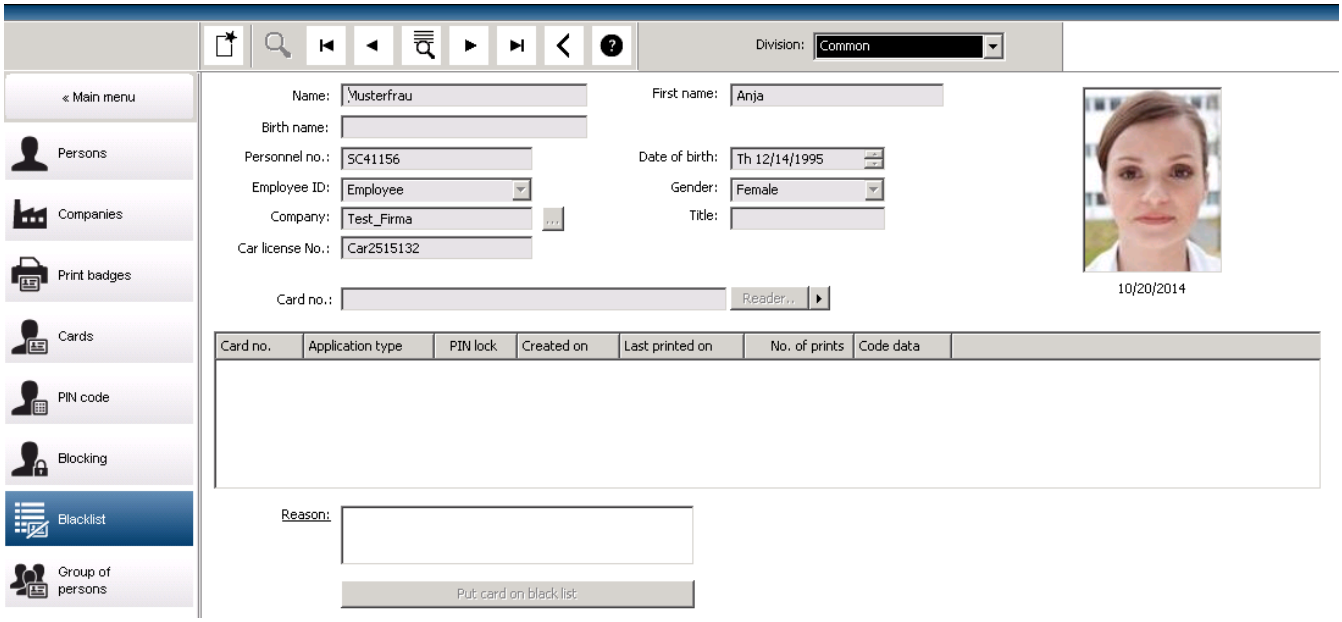
Любые карты, которые использовать впредь запрещено (например, украденные или потерянные), вносятся в таблицу черного списка.

Обратите внимание, что в черный список вносятся учетные данные, а не лицо.

Замечание!

Этот процесс необратим. Карты в черном списке невозможно разблокировать, но их можно заменить.

Внесенные в черный список карты не предоставляют доступ. Попытка использования этих карт фиксируется в файле журнала, при этом создается тревожный сигнал.



Главное меню > **Данные о персонале** > **Черный список**

1. Выберите лицо, идентификационная карта которого должна быть помещена в черный список.
2. Если владельцу карты назначено несколько карт, выберите нужную карту в списке **№ идентификационной карты**.
3. В поле ввода **Причина** укажите причину внесения этой карты в черный список.
4. Нажмите кнопку **Внести эту карту в черный список**.
5. Подтвердите внесение в черный список во всплывающем окне.

Карта немедленно внесена в черный список.

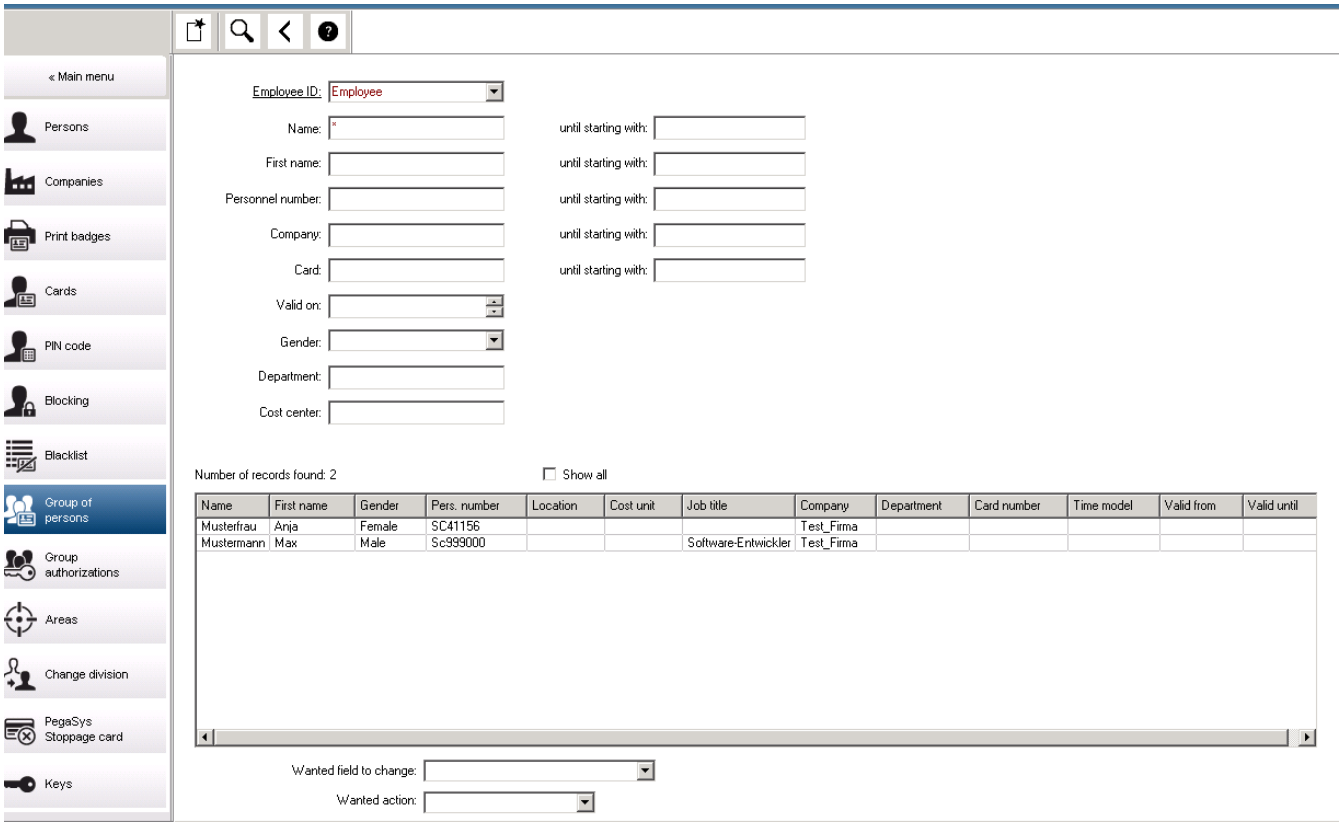
Замечание!

Внесение карты в черный список влияет на карты, а **не** на владельцев карт.

Карты того же владельца карт, не внесенные в черный список, не блокируются.

17.8 Одновременное редактирование нескольких лиц

Группа лиц



Другое диалоговое окно позволяет выбрать группу лиц, для которой можно определить групповые изменения. Чтобы сохранить контроль над выбранной группой лиц, перечисляются первые десять лиц вместе с именами и реальными данными из базы данных (реальные данные: если в качестве отдела выбрано "ST-AC", тогда, например, будет отображаться "ST-ACS" и "ST-ACX"). Кроме того, отображается несколько лиц выбранной группы.

После выбора группы лиц можно выбрать следующие записи:

- Идентификатор сотрудника
- Имя
- Имя
- Персональный номер
- Компания
- Карта
- Дата действия
- Пол
- Отдел
- Центр затрат
- Резервные поля, если определены

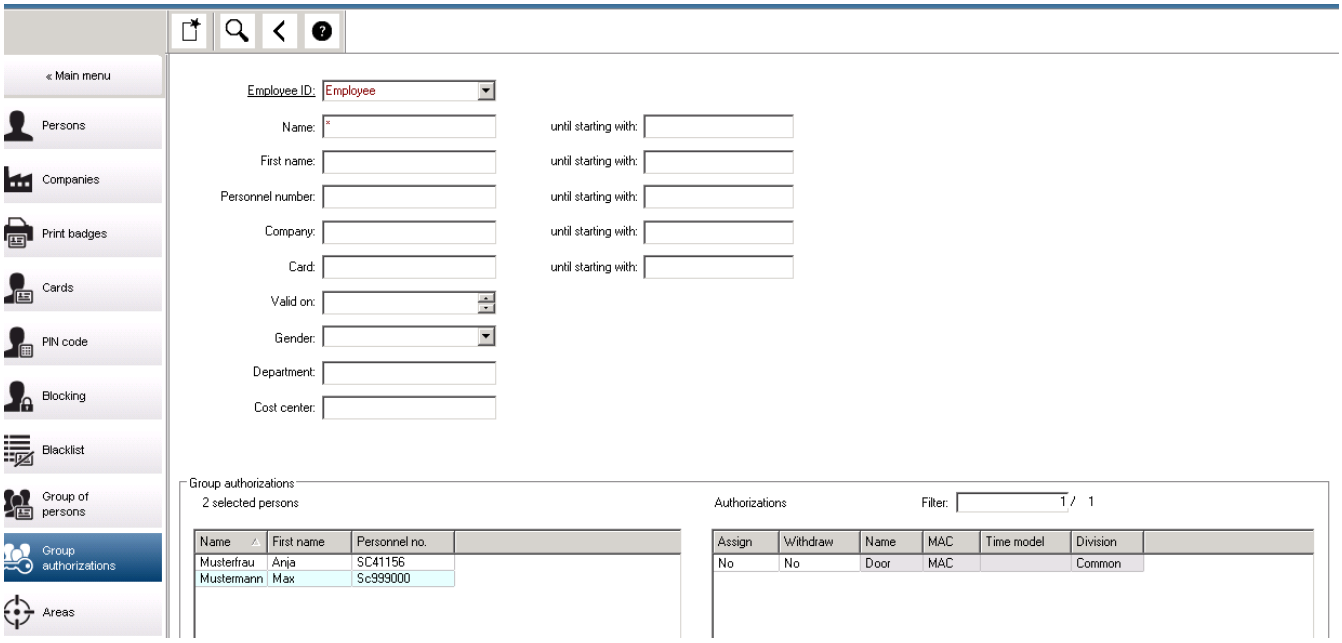
Затем можно выбрать вариант изменения:

- Изменяемое поле
- Требуемое действие
- Старое значение

– Новое значение

Таким образом, заданные значения вводятся в поля **Старое значение** или **Новое значение** соответственно. Если нажать кнопку **Применить изменения** и подтвердить запрос безопасности **применить изменения для всех выбранных лиц?**, то соответствующее действие будет завершено, т. е. данное диалоговое окно невозможно использовать, пока выполняется данное действие. Действия, инициируемые полями с *1 по *4, вероятно, займут больше времени, чем действия, инициируемые остальными полями (без звездочки). Кроме того, разрешены не все изменения. Например, **Требуемое действие** невозможно сравнить с **Новое значение**, так как введенные данные не преобразуются стандартным продуктом. Также могут меняться поля **Старое значение** и **Новое значение** соответственно.

Авторизация группы



В элементе меню **[Авторизация группы]** поддерживаются следующие критерии поиска:

– Идентификатор сотрудника
– Имя
– Имя
– Персональный номер
– Компания
– Карта
– Дата действия
– Пол
– Отдел
– Центр затрат
– Резервные поля, если определены

После этого в нижней части данного диалогового окна отображается список всех выбранных лиц (с фамилиями, именами и персональными номерами). Справа внизу перечисляются все авторизации с описанием авторизаций, модели времени и столбцами

[Назначить] и **[Аннулировать]**. При открытии списка авторизаций текущие авторизации не отображаются, а в столбцах **[Назначить]** и **[Аннулировать]** предварительно задано «Нет». Теперь можно назначать отдельные авторизации, дважды нажимая поле в любом из столбцов, чтобы преобразовать запись "Нет" в "Да" или наоборот. После нажатия кнопки "Применить изменения" все авторизации, назначенные с помощью выбора "Да", добавляются для всех выбранных лиц или аннулируются, соответственно. Все остальные авторизации данных лиц остаются без изменений, так как обычно у выбранных лиц не бывает полностью идентичных авторизаций.

18 Определение авторизаций и профилей доступа

18.1 Создание авторизаций доступа

Путь к диалоговому окну

Главное меню > **Системные данные** > **Авторизации**

Процедура

1. Очистите поля ввода, нажав кнопку **Создать**  на панели инструментов.

   Кроме того, можно нажать **Копировать**  , чтобы создать новую авторизацию на основе существующей.
2. Введите уникальное имя авторизации
3. (Необязательно) Введите описание
4. (Необязательно) Выберите временную модель, которая будет управлять этой авторизацией
5. (Необязательно) Выберите **Предел неактивности** из списка.
   Это период времени от 14 до 365 дней. Если лицо, которому назначена эта авторизация, не использует ее в течение определенного времени, он лишится ее. При каждом использовании авторизации таймер сбрасывается на ноль.
6. (Обязательно) Назначьте хотя бы один **Вход**.
   Существующие входы перечислены на разных вкладках в зависимости от соответствующих моделей дверей.
   (Общее) **Вход**, **Управление временем**, **Лифт**, **Автостоянка**, **Постановка на охрану системы охранной сигнализации**.
   Выберите отдельные входы из списков на разных вкладках, как описано ниже.
   Кроме того, можно использовать кнопки **Назначить все** и **Удалить все** на каждой из вкладок.
   - На вкладке **Вход** выберите вход, установив один или оба флажка (**Вход** или **Выход**)
   - На вкладке **Управление временем** (для считывателей времени и посещаемости) установите один или оба флажка (**Вход** или **Выход**)
   - На вкладке **Лифт** выберите разные этажи
   - На вкладке **Автостоянка** выберите автостоянку или область парковки
   - На вкладке **Постановка на охрану системы охранной сигнализации** выберите **Поставлено на охрану** или **Снято с охраны**.
7. Выберите соответствующий MAC из списка
8. Нажмите «Сохранить»  для сохранения авторизации.

Замечание!
Последующие изменения авторизаций повлияют на лиц, которым они в настоящее время назначены, если управляющий профиль не заблокирован.
Пример. Если предел неактивности 60 дней сокращается до 14 дней, то авторизация станет недействительной для всех лиц, которые не использовали ее последние 14 дней.
Исключение. Если авторизация является частью профиля доступа, который **привязан** к идентификатору сотрудника (тип лица), то на авторизации для таких лиц предел неактивности не влияет. Блокировки профилей можно задать с помощью следующего флажка.
Главное меню > **Системные данные** > **Типы лиц** > таблица: **Предопределенные идентификаторы сотрудников** > **Профиль заблокирован**

18.2 Создание профилей доступа

Примечание. Использование профилей доступа для объединения авторизаций
Для единообразия и удобства авторизации на доступ не назначаются по отдельности, а, как правило, объединяются в **профили доступа** и назначаются таким образом.

– Главное меню: **> Системные данные** > **Профили доступа**

Требования
Авторизации на доступ уже определены в системе.

Процедура

1. Очистите поля ввода, нажав кнопку **Создать** на панели инструментов.
   Кроме того, можно нажать **Копировать** , чтобы создать новый профиль на основе существующего.
2. Введите уникальное имя профиля
3. (Необязательно) Введите описание
4. (Необязательно) Установите флажок **Профиль посетителя**, чтобы ограничить этот профиль посетителями
5. (Необязательно) Задайте значение для параметра **Стандартная продолжительность действия**.
   – Если значение не задано, профиль останется назначенным в течение неопределенного времени.
   – Если значение назначено, оно будет использовано для вычисления даты истечения срока любых последующих назначений профиля.
6. (Обязательно) Назначьте хотя бы одну **авторизацию**:
   авторизации, доступные для назначения, перечислены справа.
   Авторизации, которые уже назначены, перечислены слева.
   Выберите элементы и с помощью кнопок перемещайте их из одного списка в другой.
   – ≤ назначает выделенный элемент.
   – ≥ отменяет назначение выделенного элемента.
7. Нажмите «Сохранить» для сохранения профиля.

19 Управление посетителями

Посетители имеют особый статус в системе управления доступом. Данные о них хранятся отдельно от персональных данных. Поэтому данные о посетителях также создаются и обрабатываются в отдельных диалоговых окнах.

19.1 Данные о посетителях

Введение

Система поддерживает быстрое и простое администрирование данных о посетителях. Для уже известных посетителей можно ввести данные и назначить авторизации доступа до прибытия самих посетителей. После прибытия посетителя остается только назначить карту. В конце посещения, когда карта возвращается, связь идентификационной карты с данным лицом снова удаляется, а авторизации доступа автоматически аннулируются. Если данные о посетителе не удалены пользователем, это сделает система по истечении настроенного промежутка времени (значение по умолчанию = 6 месяцев) после последнего возвращения идентификационной карты.

Существует два диалоговых окна для управления внешними посетителями.

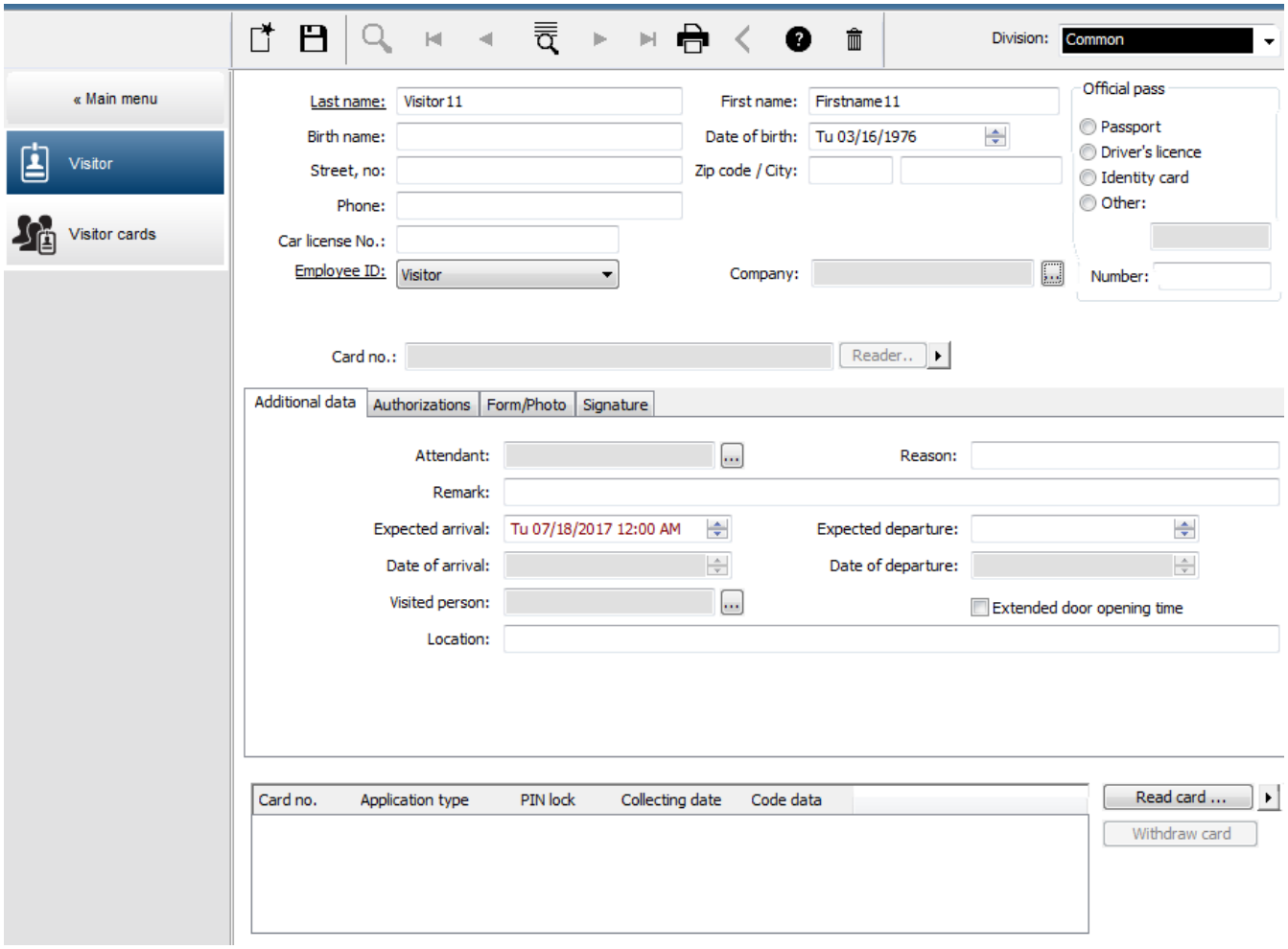
- Диалоговое окно **Посетители** используется для ввода данных о посетителях и назначении авторизаций доступа посетителей.
- Диалоговое окно **Карты посетителей** применяется для управления регистрацией и удалением карт посетителей.

Диалоговое окно: "Посетители"

Статус посетителей строго отличается от статуса других лиц. Поэтому их данные обрабатываются в отдельном диалоговом окне. Лица, которые идентифицируются как **посетитель**, нельзя создать в диалоговом окне **Лица**. Кроме того, с этой целью в данном диалоговом окне для них нельзя зарегистрировать идентификационные карты.

Кроме прочего, в диалоговом окне **Посетители** отсутствует поле ввода **Идентификатор сотрудника**. Так как для посетителей есть отдельная таблица базы данных, лица, созданные в описанном здесь диалоговом окне, автоматически идентифицируются как посетители. Это означает, что здесь можно создать только посетителей. Соответственно, в этом диалоговом окне предусмотрен выбор только из соответствующей таблицы базы данных. И наоборот, все зарегистрированные в системе лица можно выбирать в других диалоговых окнах с персональными данными, но их не всегда можно использовать для посетителей (диалоговое окно **Карты**).

До прибытия посетителя в систему можно полностью или частично ввести известные данные о посетителе. Это обеспечивает минимум времени ожидания для тех посетителей, для которых данные уже записаны.

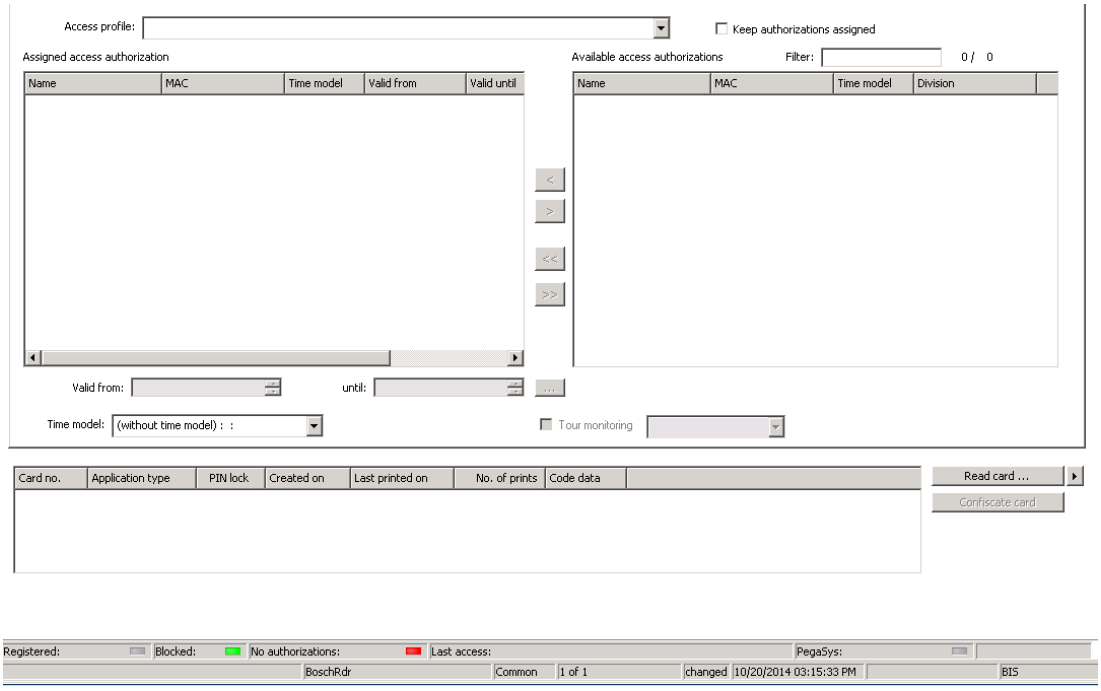


В полях ввода ниже можно указать **причину** посещения, **местоположение**, посещаемое посетителем, и **Примечание**.

Если решено вводить данные в полях **предполагаемое прибытие** и **предполагаемое убытие**, указанные даты также появятся в полях **действительно с** и **до**.

Соответствующие даты вводятся системой в полях **Дата прибытия** и **Дата убытия**, когда данные о посетителе соответствующим образом назначаются идентификационной карте посетителя и извлекаются из нее.

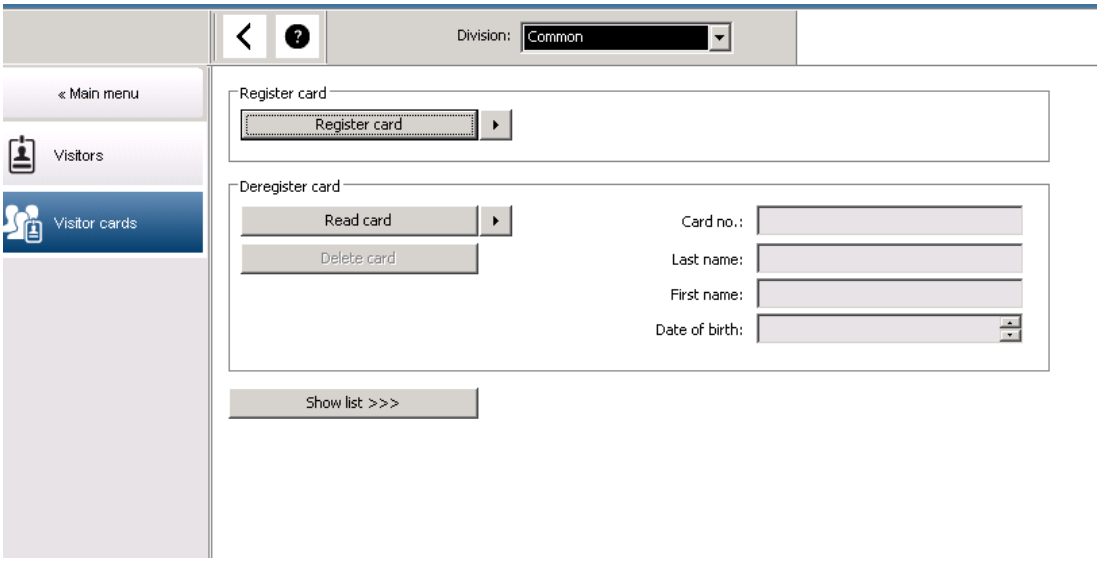
Как и в диалоговом окне **Карты**, можно назначить посетителям "расширенное время открытия дверей", чтобы облегчить доступ, например, для лиц с ограниченными физическими возможностями.



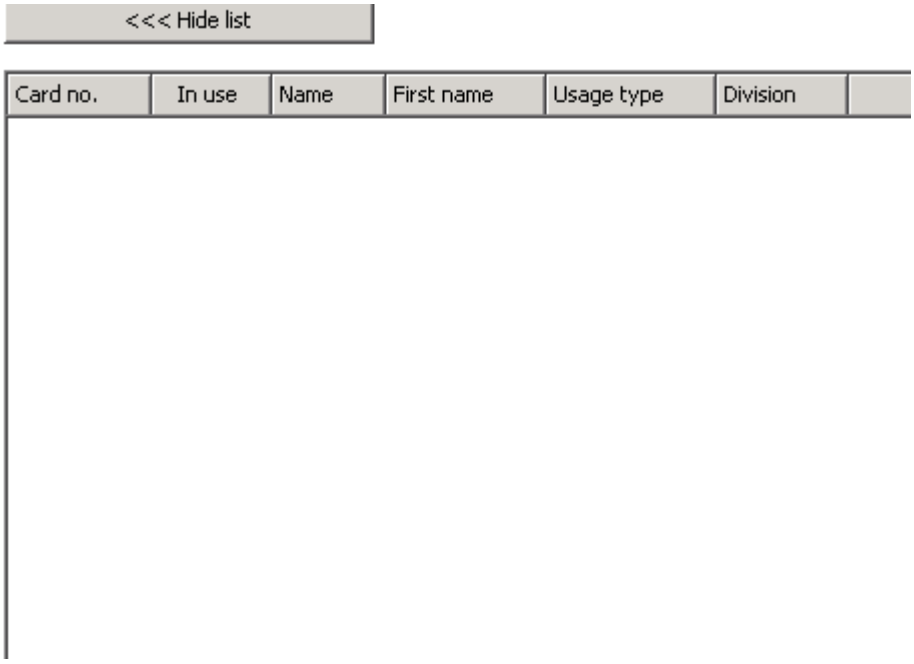
В поле диалогового окна **Назначить авторизацию** можно выбрать существующий профиль посетителя в списке выбора с тем же именем или выбрать отдельные авторизации доступа в правом списке **Доступные авторизации доступа** и перенести их в левый список **Назначенные авторизации доступа**.
В этом диалоговом окне можно выбирать только профили доступа, помеченные как "Профили посетителей". Так можно избежать того, что посетители получат доступ к специальным областям в результате назначения общих авторизаций.
Для каждой авторизации также можно назначить проверку авторизаций доступа.
Если при считывании карты возникла ошибка, номер идентификационной карты также можно ввести вручную. Текущая дата одновременно сохраняется как дата прибытия.
После завершения визита посетитель возвращает свою идентификационную карту. Пока осуществляется считывание идентификационной карты или ручной ввод ее номера, выбирается связанное лицо и на экране отображаются данные о нем.
Оператор подтверждает возврат карты. Сопоставление между идентификационной картой и посетителем удаляется при помощи кнопки **Изъять карту**. Дата и время этого действия сохраняются как дата убытия.

Диалоговое окно: "Карты посетителей"
Некоторые карты в системе зарезервированы как карты посетителей. Как правило, карта посетителя назначается приходящему посетителю и возвращается, когда он уходит. После этого карту можно использовать повторно. Чтобы такую карту можно было назначить посетителю, ее необходимо зарегистрировать как карту посетителя в этом диалоговом окне:

Замечание!
Как правило, идентификационные карты посетителей создаются без имен и фотографий, чтобы их можно было использовать повторно.



Нажмите кнопку **Регистрация идентификационной карты**, чтобы выполнить регистрацию. Затем используются описанные ранее данные процедуры ввода (см. разделы **Лица** и **Идентификационные карты** в главе **Персональные данные**) с номером идентификационной карты для обнаружения идентификационной карты. Это позволяет системе распознавать такую идентификационную карту как карту посетителя и применять ее в рамках области действия показанных ниже диалоговых окон.

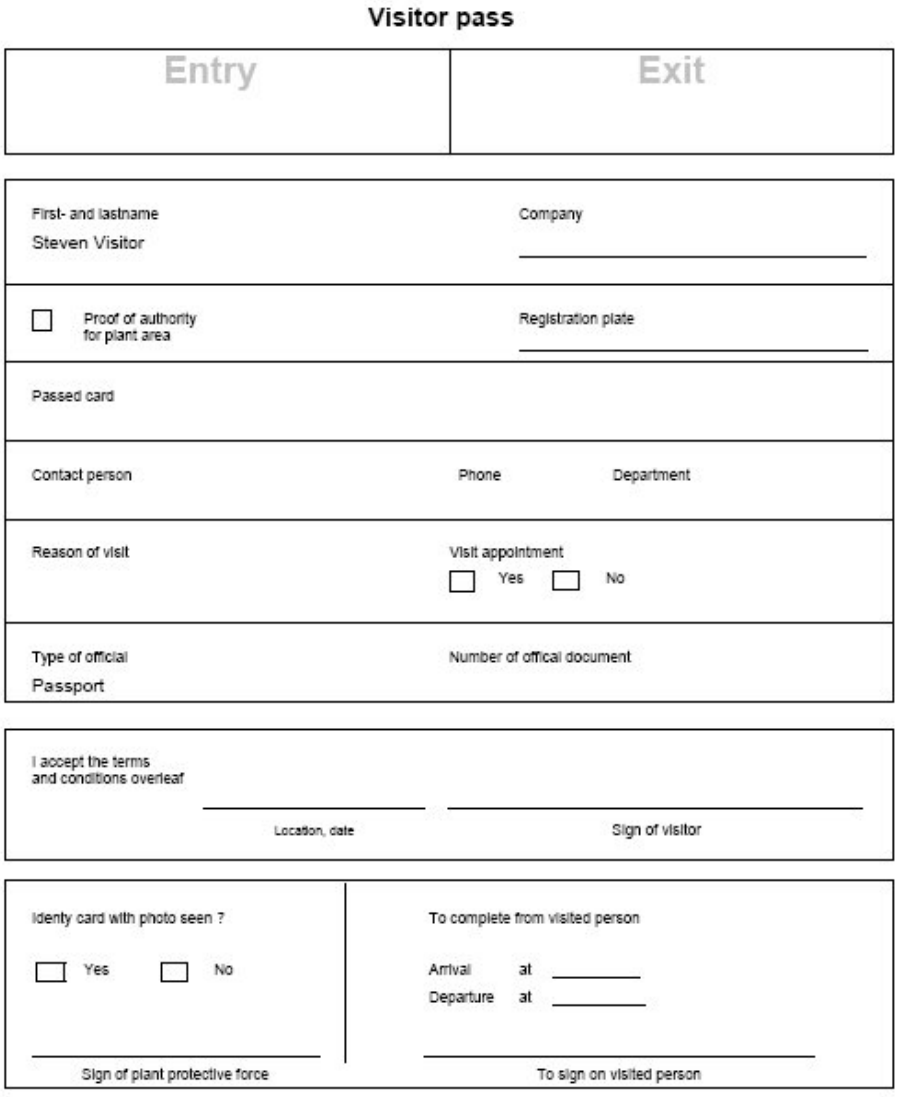


Чтобы ускорить назначение идентификационных карт посетителей, рекомендуется просканировать все существующие идентификационные карты, чтобы их можно было назначить соответствующим посетителям в следующем диалоговом окне.
В конце визита посетитель возвращает свою идентификационную карту. При сканировании его идентификационной карты в диалоговом считывателе или при вводе номера идентификационной карты выбирается лицо, которому назначена данная карта, и на экране отображаются его данные. [Сведения о вводе номеров идентификационных карт вручную и переходе на использование считывателей см. в разделах **Диалоговое окно: "Карты"** и **Диалоговое окно: "Посетители"**.] Пользователь подтверждает возврат

идентификационной карты. Связь между идентификационной картой и персональными данными посетителя удаляется при помощи кнопки. Текущая дата сохраняется как дата убытия.

Печать шаблона посетителя

На панели инструментов диалогового окна **Посетители** есть дополнительная кнопка для печати сертификата посетителя. Среди прочего, лицо, принимающее посетителя, может с помощью данного сертификата посетителя подтвердить факт и время прибытия и убытия посетителя.



Visitor pass

Entry | Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person Phone Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?
☐ Yes ☐ No

Sign of plant protective force

To complete from visited person
Arrival at
Departure at

To sign on visited person

19.2 Задержавшийся посетитель

Вид **Задержавшийся посетитель** клиент может проверить, где на объекте находятся посетители и не превышена ли ожидаемая продолжительность их пребывания на объекте. Для просмотра этого веб-сайта авторизованным пользователям BIS требуется настроить ссылку на своем начальном экране.

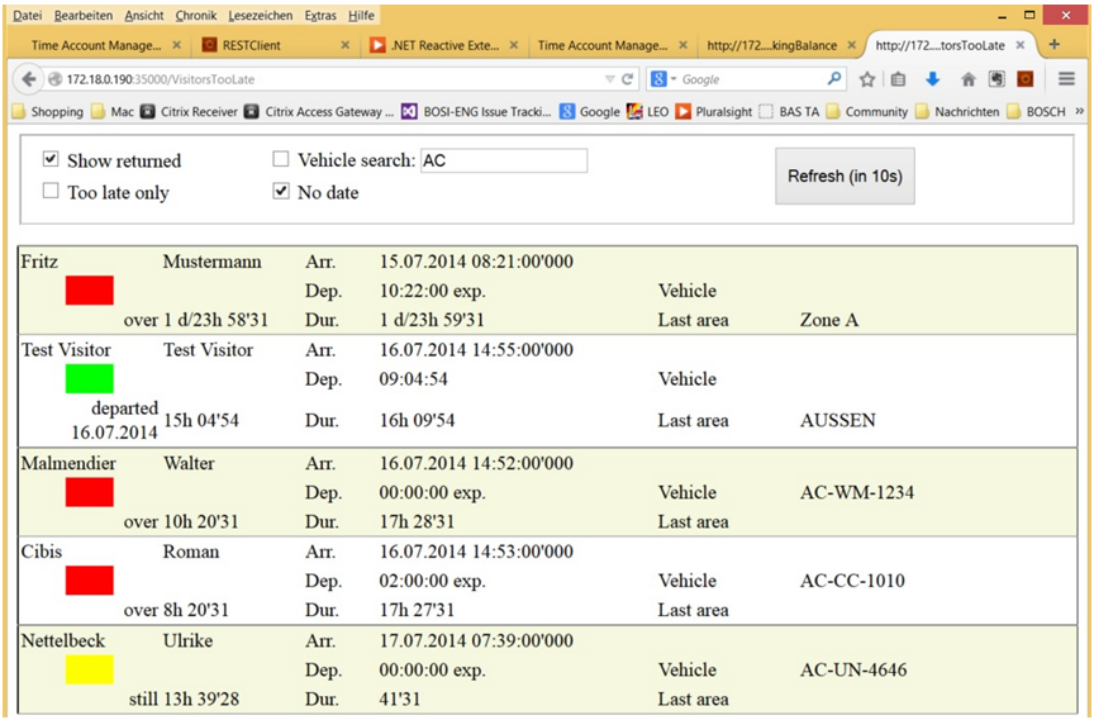
Кроме того, можно настроить триггер в системе BIS для устройства DMS, чтобы при получении сообщения "Задержавшийся посетитель" активировался сигнал тревоги, который, в свою очередь, открывал бы веб-сайт с отображением последних известных перемещений соответствующего лица.
[снимок экрана веб-сайта]

Ниже перечислены события, ведущие к появлению сообщения "Задержавшийся посетитель".
При назначении карты посетителю оператор указывает ожидаемое время убытия. Когда визит заканчивается, посетитель возвращает карту на стойку регистрации, где оператор отменяет ее.
Также на выходе для посетителей можно установить моторизированный считыватель карт и настроить его так, чтобы он задерживал карту посетителя, когда тот покидает территорию.
Если посетитель не возвращает карту до заранее оговоренного времени выхода, система создает сообщение **Задержавшийся посетитель** независимо от того, на территории ли еще посетитель.
Проверка карт, которые не вернули вовремя, выполняется с определенной частотой (например, каждую минуту). Сообщение **Задержавшийся посетитель** создается при каждой проверке, пока карта не будет возвращена. Интервал проверки можно настроить в реестре сервера в разделе `HKLM\Software\Micos\SPS\Default\VLDP\Interval`

Замечание!
Функцию создания такого сообщения можно отключить в реестре сервера в разделе `HKLM\Software\Micos\SPS\Default\VLDP\Active`

Эта функция позволяет клиенту обнаружить посетителей, которые не встретились с назначенным специалистом, не вернулись в приемную и не покинули объект после встречи со специалистом в отведенное время.
Проверяется следующее:
- в какой зоне объекта в последний раз использовалась метка доступа посетителя в здание;
- вернул ли посетитель метку доступа в здание;
- вернул ли посетитель метку доступа на территорию для автомобиля, если применимо.

Создаются отчеты **Задержавшийся посетитель** и **Задержавшийся автомобиль**.
Если метка не возвращена, в отчет "Задержавшийся посетитель" можно включить информацию о текущем расположении метки.
Статус посетителя отображается на веб-сайте с помощью цветных полос.
- **Зеленая**: посетитель вернул все карточки доступа.
- **Желтая:** визит еще не завершен, отведенное для посещения время не истекло.
- **Красная:** визит еще не завершен, а отведенное для посещения время истекло, то есть **Посетитель опаздывает**.



Страница автоматически обновляется каждые 30 секунд. Время обновления настраивается на веб-странице. Кроме того, представление оператора можно скорректировать с помощью фильтров **Показать возвращенные**, **Только задержавшиеся** и **Поиск автомобиля**.

20 Управление автостоянками

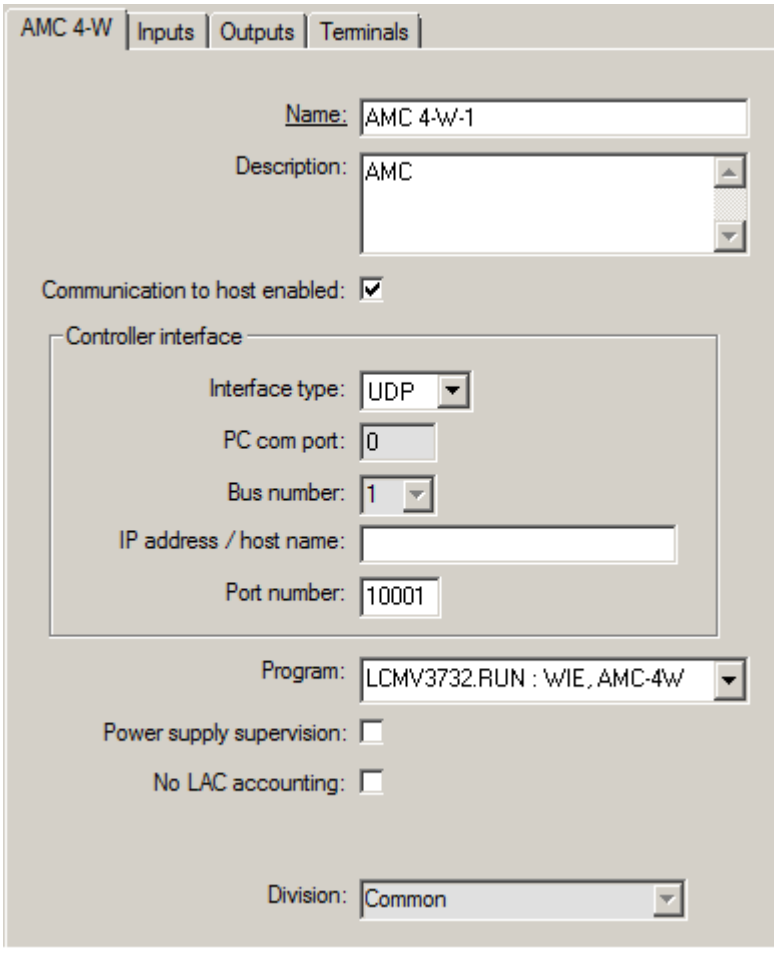
20.1 Авторизации для нескольких парковочных зон

На некоторых стоянках имеются специальные зоны для водителей с ограниченными физическими способностями. В данном случае действуют следующие правила.

– Владельцы сезонных талонов могут проехать на стоянку только при наличии свободных парковочных мест для водителей без ограниченных физических способностей.
– Водители с ограниченными физическими способностями могут проехать на стоянку только при наличии свободных парковочных мест для водителей с ограниченными физическими способностями и водителей без физических ограничений.

Замечание!
Предполагается, что владельцы талонов следуют правилам. В частности, это означает следующее.
Лица без физических ограничений не паркуются на парковочных местах для лиц с ограниченными физическими способностями.
Лица с ограниченными физическими способностями используют специальные парковочные места, если они доступны.

Лицо с несколькими авторизациями может парковаться на любых парковочных местах. AMC пытается выполнять бронирование для посетителей в соответствии с настроенным последовательным порядком парковочных зон. Если одна зона заполнена полностью, система выполняет поиск следующей свободной и доступной для парковки зоны.
Подсчёт в MAC и AMC:
1) Одна AMC контролирует все въезды и выезды стоянки:
=> система AMC выполняет подсчёт самостоятельно, при подключении к сети это значение может быть скорректировано MAC.
2) Въезды и выезды одной стоянки разделены на несколько зон AMC:
=> MAC выполняет подсчёт для AMC при наличии подключения к сети. При работе в автономном режиме устройства AMC предоставляют доступ (если настроены соответствующим образом), но не ведут подсчёт.
Если несколько устройств AMC контролируют одну стоянку, установите флажок **Без учета AMC** в конфигурации AMC.



20.2 Обзор парковки автомобиля

Parking lot list

Date 08.11.2013 , 14:51:23
Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

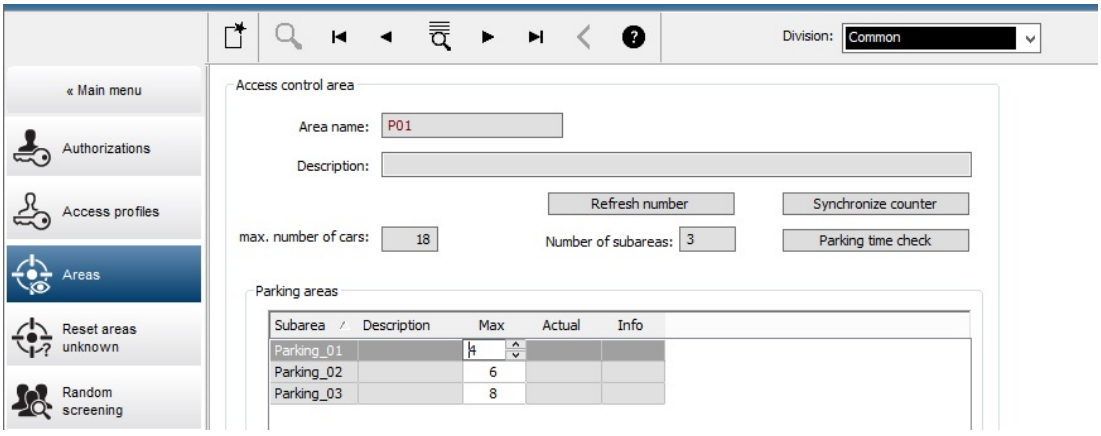
20.3 Дополнительное управление парковкой

Оператор может скорректировать количество парковочных мест в области парковки, чтобы компенсировать учитывать число транспортных средств нестандартного размера, например:

– грузовики;

– места для людей с ограниченными возможностями;
– мотоциклы.

1. Выбрать область парковки
2. На панели **Области парковки** измените значение в столбце **Макс.** на новое количество парковочных мест для этой области.



Главное меню > **Системные данные** > **Области**

21 Управление патрулированием и патрулями

Общие сведения о маршрутах патрулирования

Маршрут патрулирования — это маршрут по территории, разделенный считывателями карт, в которые сотрудники типа **Охранник** должны предоставлять специальную карту охранника при физическом прохождении через считыватель.

Карты охранника не открывают проходов, но используются исключительно для отслеживания. Чтобы открыть проходы, охранник к тому же должен предоставить карту доступа.

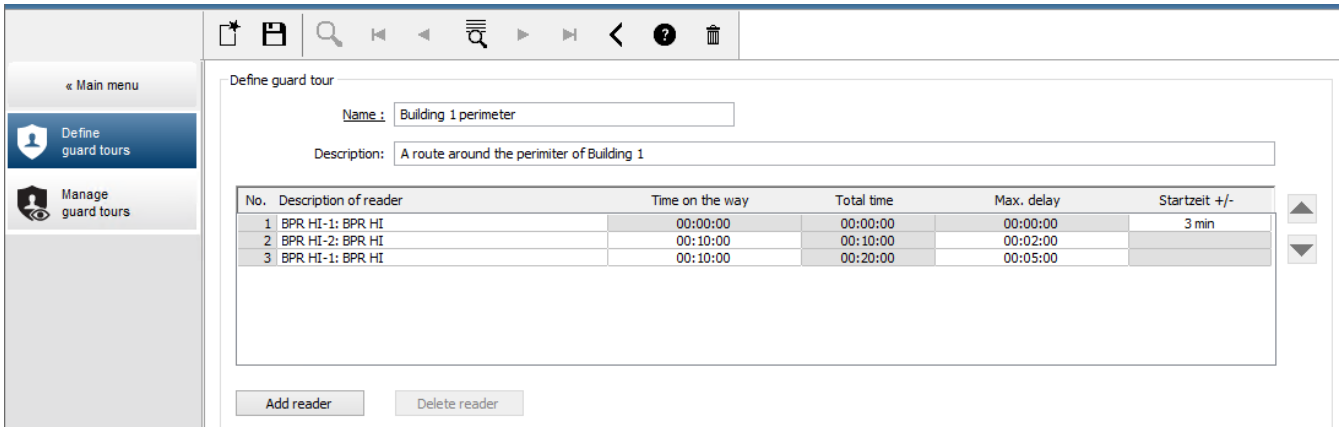
Маршрут патрулирования состоит из серии считывателей, для которых задано приблизительное временя, необходимое для того, чтобы дойти от одного считывателя к другому. Максимальное допустимое время задержки между считывателями и допустимое отклонение (+/-) от времени начала также являются параметрами маршрута патрулирования. Отклонения за пределами этих определенных допустимых значений могут потенциально активировать сигнал тревоги и регистрируются в журнале **Патрули**.

Общие сведения о патрулях

Патруль — это прохождение маршрута патрулирования в определенную дату и время. Каждый патруль создается и регистрируется как уникальный объект в системе в целях анализа.

21.1 Определение маршрутов патрулирования

Выберите **Маршруты патрулирования** > **Определить маршруты патрулирования**



– В текстовом поле **Имя** введите имя маршрута патрулирования.
– В текстовом поле **Описание** введите более подробное описание маршрута (дополнительно).

Добавление считывателей в маршрут патрулирования.

1. Нажмите кнопку **Добавить считыватель**.
   В таблице будет создана строка.
2. В столбце **Описание считывателя** выберите считыватель в раскрывающемся списке.
3. Введите значения допустимых отклонений:
   – Если это первый считыватель в последовательности в поле **Время начала +/-** введите число минут до или после времени начала, в течение которых время начала патруля все еще будет считаться допустимым в этом маршруте патрулирования.

– Если это **не** первый считыватель в последовательности, в поле **Время в пути** введите время (чч:мм:сс), необходимое охраннику на то, чтобы пройти расстояние между предыдущим считывателем и данным считывателем. Общее время маршрута за исключением задержек отображается в столбце **Общее время**.

4. В поле **Макс. задержка** введите максимальное количество дополнительного времени **Время в пути**, которое будет считаться допустимым до получения патрулем отметки **Задержка**.
5. Добавьте требуемое число считывателей. Обратите внимание, что один и тот же считыватель можно использовать несколько раз, если охранник проходит его несколько раз или возвращается к нему.

– Чтобы удалить считыватель из последовательности, выберите строку и нажмите кнопку **Удалить считыватель**.
– Чтобы изменить положение считывателя в последовательности, выберите строку и нажмите кнопки со стрелкой вверх/вниз

Кнопки  .

21.2 Управление патрулями

Выберите **Маршруты патрулирования** > **Управление маршрутами патрулирования**

Планирование нового патруля

Чтобы запланировать патруль по определенному маршруту патрулирования, выполните следующие действия.

1. Убедитесь, что имеется необходимая карта охранника для патруля и доступ к настроенному считывателю карт доступа или непосредственно подключенному регистрационному считывателю.
2. В столбце **Маршруты патрулирования** выберите один из определенных маршрутов патрулирования.
3. Нажмите кнопку **Создать патруль...**.
   Откроется всплывающее окно.
4. Во всплывающем окне при необходимости измените маршрут патрулирования в раскрывающемся списке.
5. Если необходимо задать предопределенное время начала патруля, установите флажок **Задать время начала:**
   – Введите дату и время начала.
   – При необходимости нажмите счетчик **Время начала +/-**, чтобы отрегулировать допуск для преждевременного или задержанного начала.
6. Щелкните стрелку вправо и выберите считыватель, который требуется использовать для регистрации карты охранника. Обратите внимание, что считыватель всегда должен быть настроен в системе, чтобы отображаться здесь для выбора.
7. Нажмите зеленую кнопку (+), чтобы начать считывание карты охранника, предъявите карту в считыватель и выполните инструкции во всплывающем окне.
   Карта охранника будет зарегистрирована для использования в патруле.
8. Повторите предыдущий шаг, чтобы зарегистрировать альтернативные карты охранников для этого патруля. Обратите внимание, что первая карта, предоставленная во время патруля, должна использоваться во всех считывателях во время этого патруля.

9. Нажмите кнопку **ОК**. Выбранный маршрут патрулирования будет помечен в списке как **запланированный**.

Отслеживание патруля

Все запланированные и активные патрули перемещаются наверх списка. Если запланировано или активировано несколько патрулей, выбранный патруль выделяется красной рамкой. Нажмите рамку, чтобы получить дополнительные сведения.

Патруль начинается, когда охранник предоставляет карту в первом считывателе маршрута патрулирования. Эту карту следует использовать до конца патруля, даже если для него были определены альтернативные карты.

Состояние патруля изменится на **Активно**.

Каждый считыватель, проходимый по расписанию, помечается зеленым флажком ✔. Запланированное и фактическое время между считывателями в текущем выбранном патруле отображается в нижней половине диалогового окна.

Каждый считыватель, который охранник проходит позже запланированного времени плюс **Макс. задержка**, помечается красным флажком ⊘. Патруль получает отметку **Задержка**. В этом случае охранник вызывает оператора, чтобы подтвердить отсутствие проблем. После этого оператор нажимает кнопку **Возобновить патрулирование**. Считыватель получает зеленый флажок с дополнительным символом "c": ✔c. Теперь охранник может продолжить патруль со следующего считывателя.

Если возникает непредвиденная, но неопасная задержка в активном патруле, охранник может вызвать оператора, чтобы скорректировать расписание. Введите количество минут задержки в счетчике **Задержка (мин)** и нажмите кнопку **Применить**.

Если патруль невозможно завершить по расписанию, оператор может отменить его, нажав кнопку **Прервать**. **Состояние** патруля изменится на **Прервано**, и он опустится ниже запланированных и активных маршрутов патрулирования в списке.

21.3 Мониторинг маршрута (ранее «Контроль пути»)

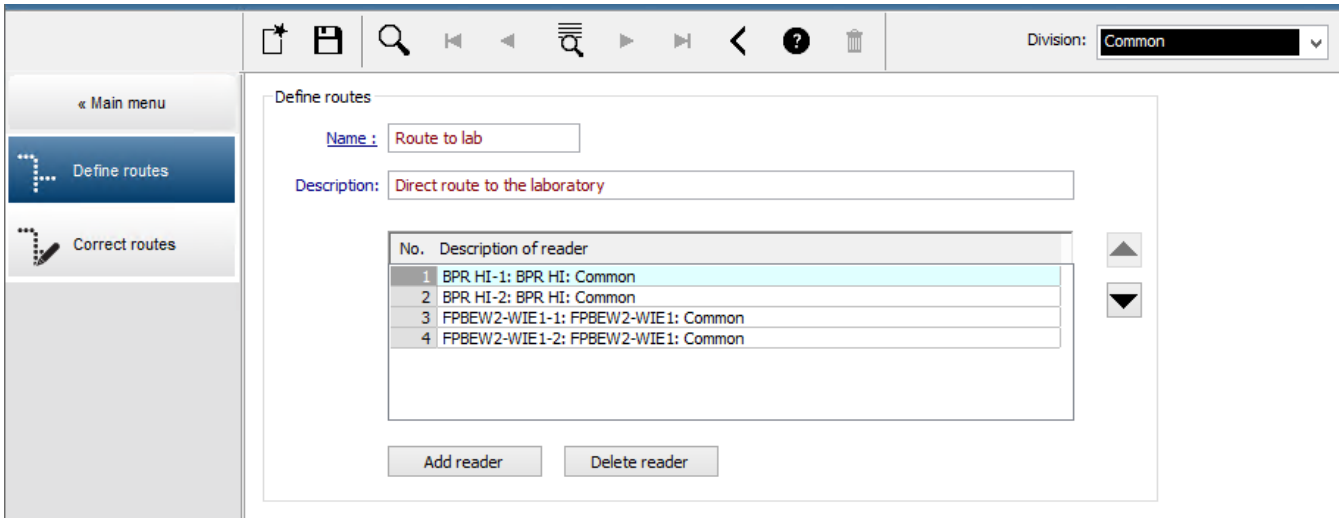
Введение

Маршрут — это предопределенная последовательность считывателей, которую можно применить к лицам, определенным в системе контроля доступа, чтобы управлять их перемещением по территории независимо от авторизаций лица.

Обычно это применяется, когда необходимо реализовать строгую последовательность доступа в чистых промышленных средах, зонах с контролем гигиены или зонах повышенной безопасности.

Определение маршрутов

1. В главном меню выберите **Мониторинг маршрута** > **Определить маршруты**.
2. Введите имя маршрута (до 16 символов).
3. Введите более подробное описание (дополнительно).
4. Как и в случае маршрутов патрулирования, нажмите кнопку **Добавить считыватель**, чтобы создать последовательность считывателей. Используйте кнопки со стрелками, чтобы изменить положение считывателя в последовательности, и кнопку **Удалить считыватель**, чтобы удалить считыватель.



Назначение маршрута лицу

Чтобы назначить маршрут лицу, выполните следующие действия.

1. В главном меню нажмите **Данные о персонале** > **Карты**
2. Загрузите запись о персонале для лица, которому требуется назначить маршрут
3. На вкладке **Другие данные** установите флажок **Мониторинг маршрута**.
4. В раскрывающемся списке рядом с ним выберите определенный маршрут (сведения по определению маршрута см. в предыдущем разделе).
5. Сохраните запись о персонале.

Маршрут активируется, когда назначенное лицо предоставит карту в первом считывателе на маршруте. После этого другие считыватели в маршруте должны использоваться в определенной последовательности, то есть только следующий считыватель в последовательности предоставит доступ. После успешного завершения маршрута лицо может использовать любой другой считыватель, на доступ к которому имеются соответствующие авторизации.

Корректировка и мониторинг маршрутов

1. В главном меню выберите **Мониторинг маршрута** > **Корректировать маршруты**.
2. Загрузите запись о персонале для лица, которое было назначено маршруту.
3. Чтобы найти лицо в маршруте, нажмите кнопку **Определить расположение**.
4. Успешно пройденные считыватели помечаются зеленым флажком ✔ в списке.
5. Чтобы сбросить или скорректировать расположение лица в маршруте, нажмите кнопку **Установить расположение**.

22 Случайный досмотр персонала

Процесс случайного досмотра

1. Владелец карты прикладывает свою карту к считывателю, настроенному на случайный досмотр.

   Примечание

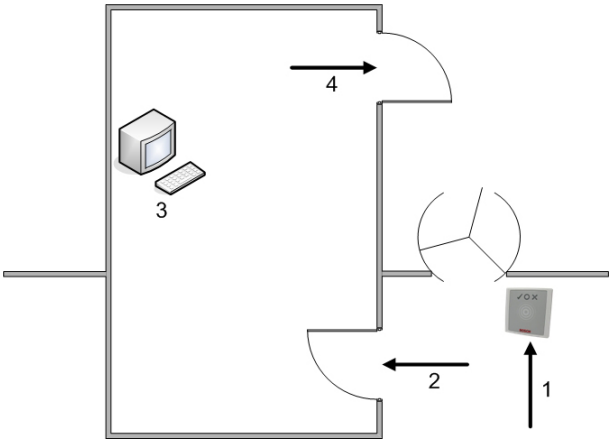
   Случайно могут быть выбраны только лица, которым разрешен проход через данный проход в заданном направлении. Поскольку авторизации проверяются перед случайным досмотром, любому неавторизованному лицу немедленно будет запрещен вход и это лицо не будет включено в процесс выбора.
2. Если генератор случайных чисел выбирает данное лицо для досмотра, карта лица блокируется в рамках всей системы.
   - Данное событие регистрируется в журнале системных событий.
   - Диалоговое окно **Блокировка** получает бессрочную запись с пометкой **Случайный досмотр**. [Рисунок ниже — номер 1]
   - В строке состояния диалоговых окон персональных данных Access Engine отображаются индикаторы блокировки (красные), при этом мигают индикаторы случайного досмотра (фиолетовые).

Замечание!
Лица, для которых задан параметр **Исключен из случайного досмотра** (в диалоговом окне **Карты**, вкладка **Другие данные**), не включаются в процесс досмотра.

3. Случайно выбранное лицо приглашается для дальнейшей проверки в отдельную кабину охраны.
4. После проведения проверок охрана сбрасывает данный блок в диалоговом окне **Блокировка** указанным ниже образом.
   - Выберите соответствующий блок в диалоговом окне со списком **Блокировка**.
   - Нажмите кнопку **Удалить**.
   - Подтвердите удаление, выбрав **Да**.

Теперь случайно выбранное лицо может использовать свою карту во всех считывателях, для которых оно авторизовано.

Пример планировки комнаты для случайного досмотра



1 = Прикладывается карта — досмотр — блокировка на системном уровне
2 = Владелец карты входит в кабину охраны

3 = Выполняется досмотр владельца карты, затем блокировка его карты снимается с помощью данного диалогового окна.
4 = Владелец карты покидает кабину охраны, не предъявляя карту считывателю еще раз.

Замечание!
Процент досмотра достигается совокупно с течением времени. Так, если для случайного досмотра выбрано значение 10 %, все равно существует вероятность (1 из 100 или 1/10 x 1/10), что для досмотра будут выбраны два человека подряд.

23 Использование средства просмотра событий

Введение

Средство просмотра событий позволяет операторам с соответствующими полномочиями изучать события, записанные в системе, и составлять отчеты (распечатывать их или выводить на экран).

Для извлечения и отображения нужных записей из базы данных журнала событий задайте критерии фильтрации и нажмите кнопку **Обновить** .

Критерии фильтрации можно задать разными способами:

Относительно	Выбор событий относительно текущего времени.
Интервал	Выбор событий относительно свободно определяемого интервала времени
Всего	Выбор событий независимо от времени их наступления

Требования

Вы вошли в диспетчер диалоговых окон.

Путь к диалоговому окну

Главное меню диспетчера диалоговых окон > **Отчеты** > **Средство просмотра событий**

23.1 Настройка критериев фильтрации для времени относительно настоящего

1. В разделе **Период времени** установите переключатель **Относительно**
2. В поле **Поиск за последние** укажите число временных единиц для поиска и выберите, какие из них следует использовать (недели, дни, часы, минуты, секунды).
3. В меню **Типы событий** выберите категорию событий для поиска, а затем типы событий, которые представляют для вас интерес.
4. В меню **Максимальное количество** ограничьте число событий, которые средство просмотра событий будет пытаться получить. По соображениям производительности **не** рекомендуется оставлять значение **(Не ограничено)**.
5. Укажите другие необходимые критерии фильтрации:
   - Фамилия
   - Имя
   - Персональный номер
   - Номер карты
   - Пользователь (то есть системный оператор)
   - Данные кода
   - Название устройства
   - Название области.

- Нажмите **Обновить** , чтобы начать сбор событий, и **Отмена**, чтобы остановить его.
- Нажмите , чтобы сохранить результаты, или , чтобы распечатать их.
- Нажмите , чтобы очистить результаты другого поиска.

23.2 Настройка критериев фильтрации для временного интервала

1. В разделе **Период времени** установите переключатель **Интервал**
2. С помощью инструментов выбора дат **Время с, Время до** укажите начало и окончание периода поиска событий.
3. В меню **Типы событий** выберите категорию событий для поиска, а затем типы событий, которые представляют для вас интерес.
4. В меню **Максимальное количество** ограничьте число событий, которые средство просмотра событий будет пытаться получить. По соображениям производительности **не** рекомендуется оставлять значение **(Не ограничено)**.
5. Укажите другие необходимые критерии фильтрации:
   - Фамилия
   - Имя
   - Персональный номер
   - Номер карты
   - Пользователь (то есть системный оператор)
   - Данные кода
   - Название устройства
   - Название области.

- Нажмите **Обновить**  , чтобы начать сбор событий, и **Отмена**, чтобы остановить его.
- Нажмите  , чтобы сохранить результаты, или  , чтобы распечатать их.
- Нажмите  , чтобы очистить результаты другого поиска.

23.3 Настройка критериев фильтрации независимо от времени

1. В разделе **Период времени** установите переключатель **Всего**
2. В меню **Типы событий** выберите категорию событий для поиска, а затем типы событий, которые представляют для вас интерес.
3. В меню **Максимальное количество** ограничьте число событий, которые средство просмотра событий будет пытаться получить. По соображениям производительности **не** рекомендуется оставлять значение **(Не ограничено)**.
4. Укажите другие необходимые критерии фильтрации:
   - Фамилия
   - Имя
   - Персональный номер
   - Номер карты
   - Пользователь (то есть системный оператор)
   - Данные кода
   - Название устройства
   - Название области.

- Нажмите **Обновить**  , чтобы начать сбор событий, и **Отмена**, чтобы остановить его.

– Нажмите  , чтобы сохранить результаты, или  , чтобы распечатать их.

– Нажмите  , чтобы очистить результаты другого поиска.

24 Использование отчетов

В этом разделе описывается набор функций для работы с отчетами, которые можно использовать для фильтрации системных данных и данных журнала событий, а также для представления этих данных в удобных форматах.

Путь к диалоговому окну

Главное меню > **Отчеты**.

Использование панели инструментов отчетов

Нажмите  , чтобы отобразить документ для предварительного просмотра перед печатью.

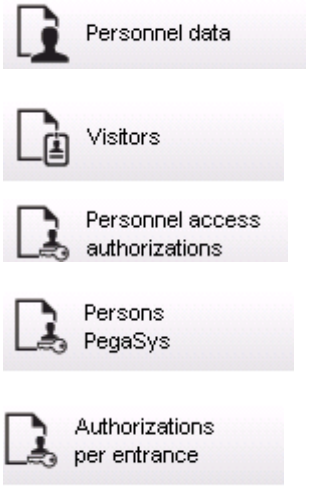
В окне предварительного просмотра есть собственная панель:

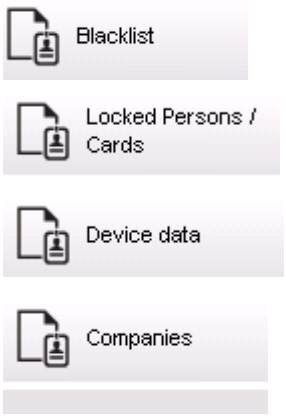
- Нажмите ✕, чтобы выйти из предварительного просмотра без печати.
- Используйте клавиши со стрелками |◀ ◀ 2 of 17 ▶ ▶| на панели инструментов предварительного просмотра для перемещения по документу или укажите номер нужной страницы.
- Нажмите  , чтобы распечатать документ немедленно, используя принтер по умолчанию
- Нажмите  , чтобы распечатать документ через диалоговое окно «Настройка печати», в котором можно указать дополнительные параметры печати.
- Нажмите  , чтобы экспортировать отчет в одном из поддерживаемых файловых форматов, включая PDF, RTF и Excel.
- Числа справа на панели инструментов обозначают следующее:
  - Совокупное количество существующих записей базы данных, соответствующих критериям фильтрации.
  - Процент записей базы данных, отображаемых для предварительного просмотра.

24.1 Отчеты: основные данные

Обзор отчета: основные данные

Отчеты с основными данными содержат все отчеты о лицах, посетителях, картах и авторизациях доступа. Кроме того, можно отобразить данные устройства и компании.





Отчет: персональные данные
При создании отчетов можно применять два фильтра.
Фильтр по лицам: оператор фильтрует отчет по стандартным полям данных о персонале.
Фильтр по картам доступа: оператор может выполнять фильтрацию по номерам карт, диапазонам номеров, статусу и статусу блокировки.

Отчет: Посетители
Как и для персональных данных, здесь можно создавать отчеты о посетителях. При этом сохраняется возможность доступа ко всем созданным данными о посетителях, т. е. можно даже выбирать посетителей, которые еще не прибыли, но уже зарегистрированы.

Отчет: "Авторизации доступа персонала"
В этом отчете дается обзор зарегистрированных в системе авторизаций доступа, а также перечисляются лица, которым они назначены.
В условиях фильтров можно использовать персональные данные и набор выбранных определенных авторизаций.
- Персональные данные: фамилия, имя, персональный номер
- Проверка всех авторизаций.
- Имя авторизации, которая распространяется на данный вход.
- Имя модели времени, если есть.
- Направление входа.
- Проверка специальной авторизации.

Отчет: "Черный список"
В этом диалоговом окне можно распечатать список с подробным описанием всех или нужных идентификационных карт, которые по разным причинам были внесены в черный список.

Отчет: Заблокированные лица/карты
Это диалоговое окно можно использовать для создания отчета с данными обо всех заблокированных лицах.
Используйте даты, чтобы найти блоки в определенные периоды времени.

Отчет: данные устройств

Это диалоговое окно можно использовать для создания отчетов на основе данных устройств, например имени или типа устройств.

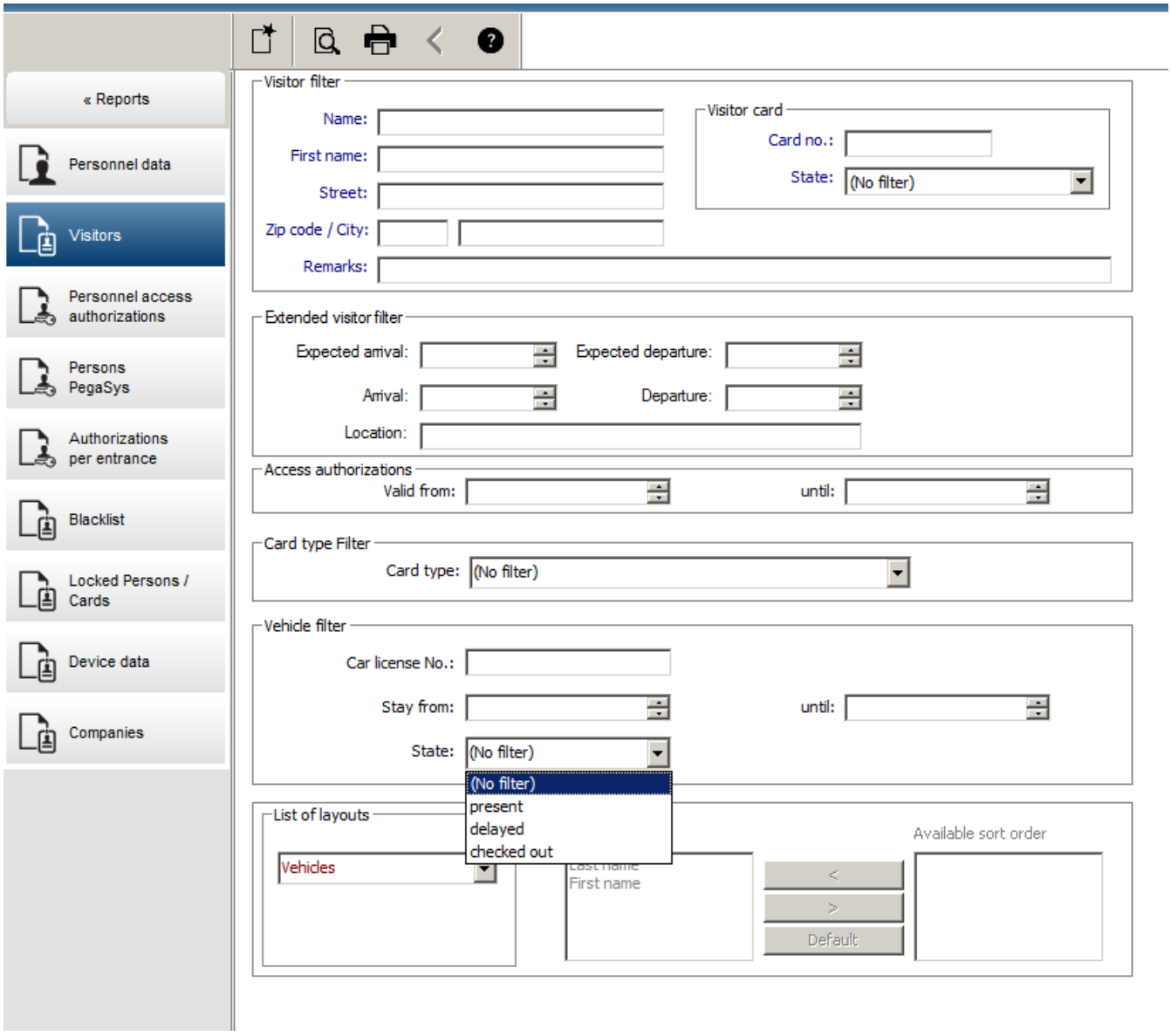
Отчет: компании

Диалоговое окно отчета «Компании» используется для сбора данных о компании. Используйте звездочки, чтобы найти компании с названием на определенную букву.

24.1.1 Отчетность по автомобилям

В диалоговом окне **Отчеты > Посетители** из списка макетов можно выбрать **Автомобили**. После выбора значения **Автомобили** в области диалогового окна активируется **Фильтр автомобилей**, с помощью которого оператор может фильтровать автомобили и их статус. Статус отображается следующим образом:

- Присутствует: визит еще не завершен, отведенное для посещения время не истекло.
- Задержка: визит еще не завершен, но отведенное для посещения время истекло.
- Зарегистрировано убытие: посетитель вернул все карточки доступа.



Отчет об автомобилях можно составить только для посетителей, потому что в таблице **Посетители** базы данных ожидаемая дата прибытия, ожидаемая дата убытия, дата прибытия и дата убытия доступны только для посетителей.
В отчете указаны только номера автомобилей, сохраненные в таблице **Лица** базы данных. В случае изменения номера автомобиля в отчете будут отображаться другие сведения.
Продолжительность пребывания вычисляется следующим образом.

- Если посетитель уже убыл, то отображается разница между прибытием и убытием в минутах.
- Если посетитель еще не убыл, отображается время с момента прибытия до текущего момента в минутах.

Access Engine

Vehicle

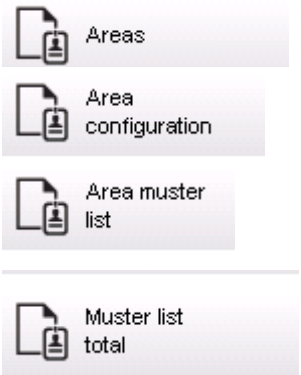
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

24.2 Отчеты: системные данные

Отчеты: системные данные

В отличие от основных данных, системные данные — это информация, которая назначена системе и не связана с лицами, идентификационными картами или компаниями. Данные отчеты подробнее описываются ниже.



Отчет: Области

Это диалоговое окно можно использовать для идентификации местоположений в отчете. В данном диалоговом окне содержится только один фильтр области, который предлагает на выбор различные здания и другие зоны.

Нужная область выбирается нажатием левой кнопки мыши. Прежде чем начать процесс печати с помощью кнопки **Печать**, пользователь может просмотреть отчет на экране, нажав кнопку **Предварительный просмотр**.
Доступно два макета.

	Стандарт	Находящиеся в данном местоположении лица — без автостоянок
	Занятость автостоянки	Находящиеся в данном местоположении лица — только автостоянки

Чтобы убедиться в актуальности отображаемых наборов данных, также указываются сведения о последних сканированиях карт для данных областей.
Поэтому для различных событий может быть предоставлена надежная информация о местоположении лиц.

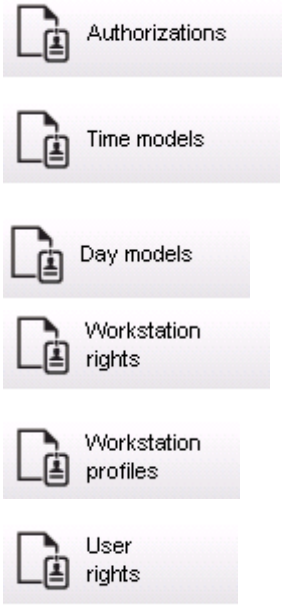
Отчет: "Конфигурация областей"
Определенные области и их подобласти с отмеченными флажками автостоянками и максимальным числом пользователей или автомобилей.

Отчет: "Список проверки области"
Лица в данной области можно перечислить не только по числовым данным, но и по именам.
Кроме времени сканирования для отдельных областей, в данных отчетах также содержатся значения времени для каждого лица.

Отчет: "Общий список опроса"
В принципе, списки опроса соответствуют диалоговому окну отчетов **Области**. Однако они предлагают списки для определенных зон, предоставляющих информацию о текущем числе лиц в области в соответствии с контролем доступа.

24.3 Отчеты: авторизации

Обзор
В этом пункте меню предоставляется сводка по различным авторизациям, заданным в соответствующих диалоговых окнах.



Отчет: Авторизации
Это диалоговое окно можно использовать для отображения авторизаций доступа, определенных в системе. Перечисляются проходы, принадлежащие к отдельным авторизациям доступа. Отображается имя выбранной временной модели. Кроме того, в этом отчете отображается число лиц, которым назначена данная авторизация.

Отчет: "Временные модели"
Этот отчет можно использовать для отображения выбранных временных моделей, определенных в системе. В этом отчете отображаются все данные, связанные с моделью, а также число лиц, которым она назначена.

Отчет: "Модели дня"
В этом отчете отображаются все заданные модели дня с их именами, описаниями и содержащимися в них интервалами.

Отчет: Права рабочей станции
Это диалоговое окно можно использовать для отображения прав рабочих станций, назначенных определенным в системе рабочим станциям.

Отчет: Профили рабочей станции
Это диалоговое окно можно использовать для отображения определенных в системе профилей рабочих станций. Это позволяет представить в удобном виде системные операции с отдельными рабочими станциями.

Отчет: "Права пользователя"
Это диалоговое окно можно использовать для отображения профилей пользователей, назначенных определенным в системе пользователям.

Отчет: "Профили пользователей"
Это диалоговое окно можно использовать для отображения диалоговых окон и прав диалоговых окон, назначенных определенным в системе профилям пользователей.

25 Использование функций управления уровнем угрозы

В этом разделе описываются различные способы активации уровня угрозы и его отмены. Дополнительные сведения см. в разделе *Настройка управление уровнем угрозы, Страница 118*.

Введение

Уровень угрозы активируется предупреждением об угрозе. Предупреждение об угрозе может быть инициировано одним из следующих способов:

- Командой в пользовательском интерфейсе программного обеспечения.
- По входному сигналу, определенным на локальном контроллере доступа, например сигналом кнопки.
- Считыванием тревожной карты на считывателе.

Обратите внимание, что предупреждения об угрозе могут быть отменены командой пользовательского интерфейса или аппаратным сигналом, но не картой для предупреждения об угрозе.

См.

- *Настройка управление уровнем угрозы, Страница 118*

25.1 Инициация и отмена предупреждения об угрозе с помощью команды пользовательского интерфейса

В этом разделе описывается, как активировать предупреждение об угрозе в AMS Map View.

Путь к диалоговому окну

- AMS Map View >  (дерево устройств)

Предварительные требования

- Определен хотя бы один уровень угрозы.
- Как минимум один уровень угрозы помечен в редакторе устройств как активный.
- Вы как оператор Map View и AMC обладаете необходимыми разрешениями:
  - Для работы с уровнями угроз.
  - Для просмотра MAC в подразделении, в котором необходимо активировать предупреждение об угрозе.

Процедура активации предупреждения об угрозе

1. В дереве устройств в AMS Map View щелкните правой кнопкой мыши устройство MAC, в котором необходимо активировать предупреждение об угрозе.
   - Отобразится контекстное меню с командами, которые вам разрешено выполнять на этом устройстве MAC.
   - Если ни один из уровней опасности еще не активирован, в меню будет один или несколько элементов с меткой **Активировать уровень угрозы**, где «<name>» — это имя уровня угроз, определенного в редакторе устройств.
2. Выберите уровень угрозы, который требуется активировать.
   - Уровень угрозы будет активирован.

Процедура отмены предупреждения об угрозе

Предварительное требование. Уровень угрозы уже используется.

1. В дереве устройств в AMS Map View щелкните правой кнопкой мыши устройство MAC, в котором необходимо отменить предупреждение об угрозе.
   – Отобразится контекстное меню с командами, которые вам разрешено выполнять на этом устройстве MAC.
2. Выберите **Отключить уровень угрозы** в контекстном меню.
   – Текущий уровень угрозы будет отключен.

25.2 Активация предупреждения об угрозе с помощью аппаратного сигнала

В этом разделе описано, как отправить аппаратный входной сигнал для активации предупреждения об угрозе.

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.
– Аппаратные сигналы определены в AMC, устройство подключено к соответствующему терминалу на этом контроллере AMC, который будет передавать сигнал. При необходимости щелкните ссылку в конце данного раздела, чтобы получить инструкции по настройке входного сигнала, или обратитесь к системному администратору.

Процедура

Активируйте устройство (как правило, с помощью кнопки или аппаратного переключателя, подключенного к AMC).

Чтобы отменить предупреждение об угрозе, активируйте устройство, которое отправляет входной сигнал, определенный как **Уровень угрозы: отключить**.

См.

– *Назначение уровня угрозы аппаратному сигналу, Страница 122*

25.3 Активация предупреждения об угрозе с помощью карты для предупреждения об угрозе

В этом разделе описывается, как активировать предупреждение об угрозе с помощью карты для предупреждения об угрозе.

Предварительные требования

– Определен хотя бы один уровень угрозы.
– В дереве устройств настроен хотя бы один проход.
– Для определенного владельца карты создана карта для предупреждения об угрозе. При необходимости щелкните ссылку в конце данного раздела, чтобы получить инструкции по созданию карты для предупреждения об угрозе, или обратитесь к системному администратору.

Процедура

1. Владелец карты подносит свою специальную карту для предупреждения об угрозе на любом считывателе, **не являющемся считывателем отпечатков пальцев**.
   – Активируется уровень угрозы, определенный для этой карты.

2. После устранения угрозы отмените уровень угрозы с помощью команды пользовательского интерфейса или аппаратного переключателя. Невозможно отменить уровень угрозы с помощью карты для предупреждения об угрозе.

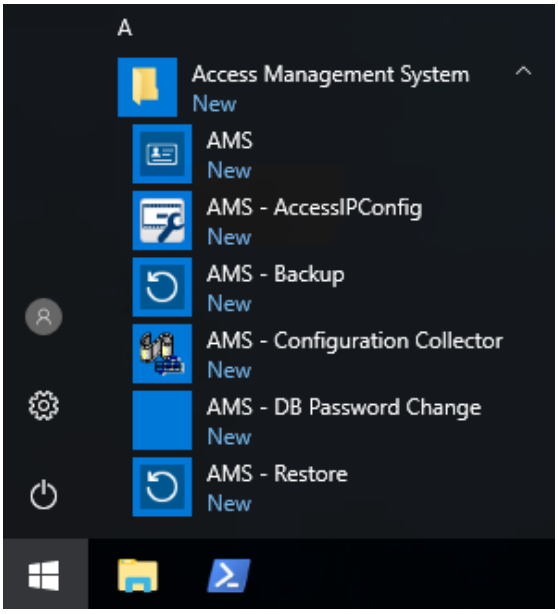
См.

– *Создание карты для предупреждения об угрозе, Страница 138*

26 Резервное копирование и восстановление

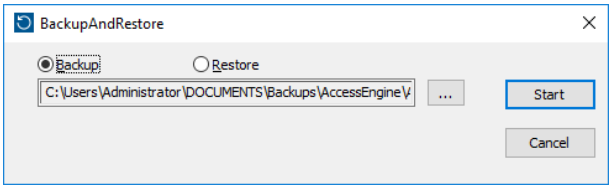
Функция **Резервное копирование и восстановление** позволяет восстановить установку на другом компьютере, если исходный компьютер вышел из строя.
Функцией **Резервное копирование и восстановление** можно воспользоваться только на компьютере с установленным сервером AMS. Для удобства создаются два ярлыка:

- **AMS — резервное копирование** для создания резервной копии
- **AMS — восстановление** для восстановления из резервной копии:

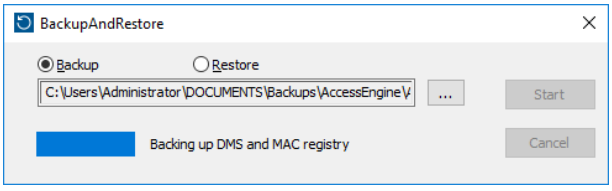


26.1 Процедура резервного копирования

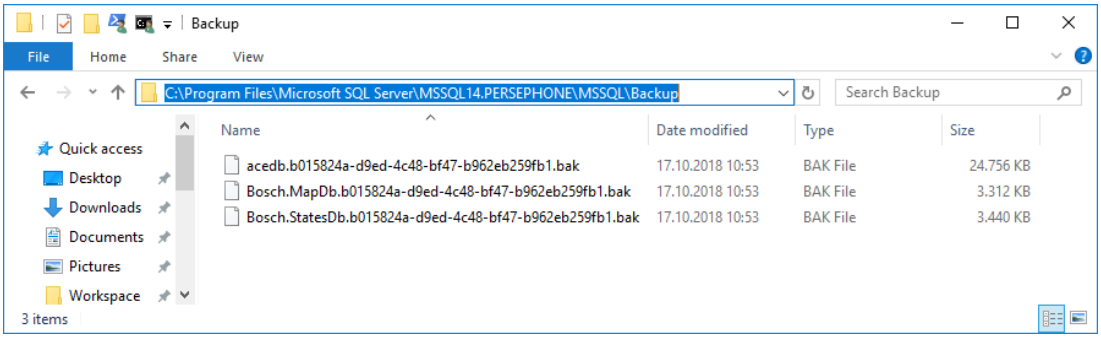
1. Щелкните ярлык **AMS — резервное копирование**.
   Это запустит инструмент **Резервное копирование и восстановление**:



2. Укажите путь сохранения файла GZIP.
3. Нажмите **Пуск**, чтобы сохранить резервную копию.
   Отобразится индикатор выполнения.
   По окончании операции будет создан файл GZIP.



Расположение резервной копии базы данных зависит от версии SQL Server и имени экземпляра базы данных.
Так, если экземпляр AMS SQL Server назван PERSEPHONE, резервная копия будет размещаться по следующему адресу:



ВАЖНО! В целях безопасности Bosch настоятельно рекомендует копировать эту папку и файл GZIP в безопасное удаленное расположение. Не оставляйте единственную резервную копию на компьютере сервера DMS.

Замечание!
Журнал событий сохраняется по следующему пути по умолчанию (установщик может выбрать другой путь):
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

26.2 Процедура восстановления

Требования

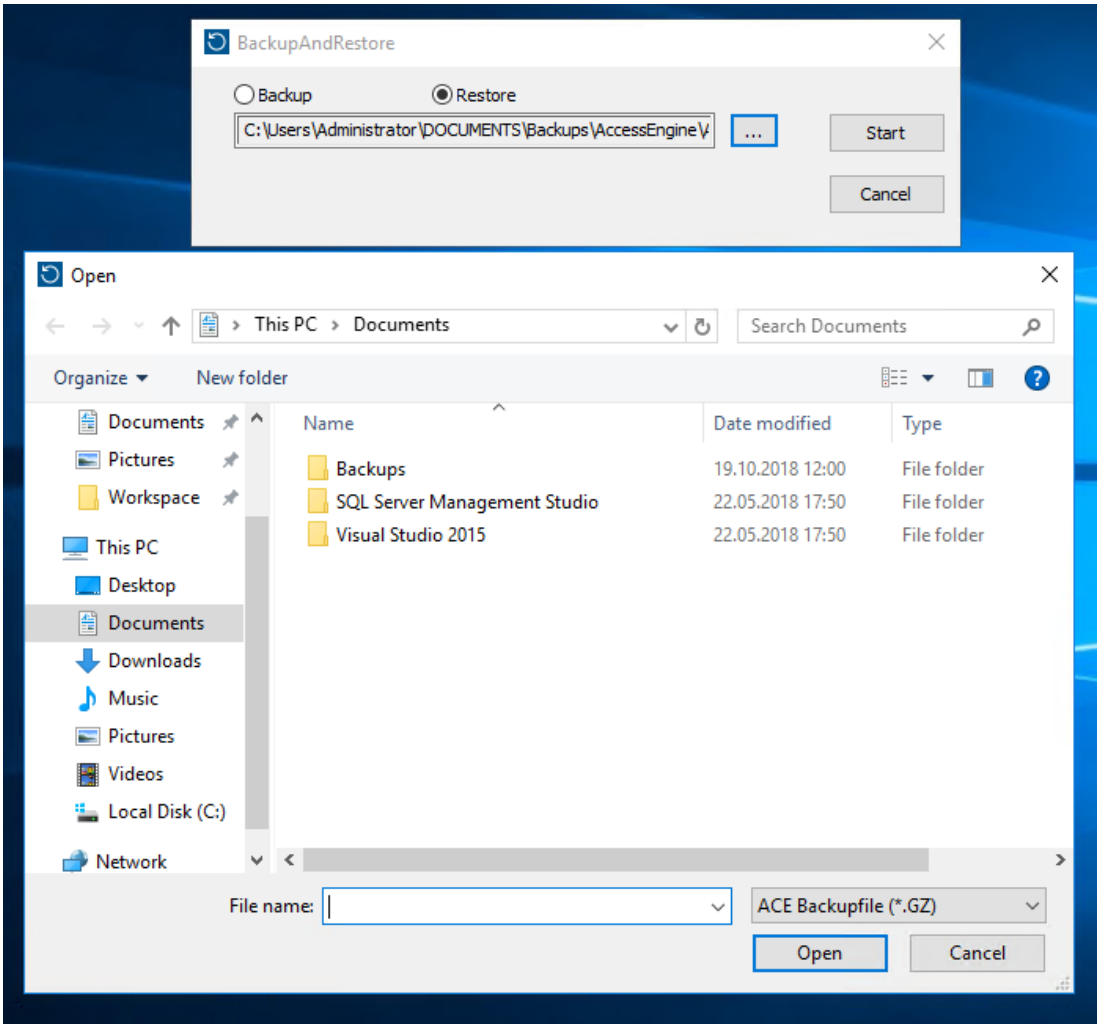
- Файл GZIP, созданный инструментов **Резервное копирование и восстановление**
- Данные резервного копирования, созданные SQL Server в резервной папке SQL Server.
- Учетная запись SQL с правами **sysadmin**, например `sa`.

Примечания о целевом компьютере

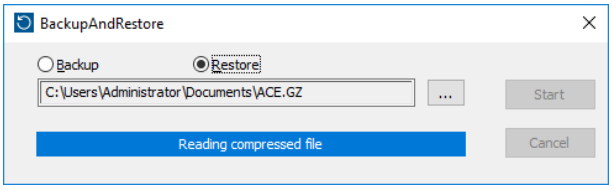
- Для запуска восстановленной конфигурации на целевом компьютере (где выполняется восстановление из резервной копии) необходимо установить лицензии, которые по меньшей мере эквивалентны лицензиям на компьютере, где создавалась резервная копия.
- Любые клиенты на целевом компьютере потребуют сертификаты, созданные в ходе установки на целевом компьютере, а не на исходном.
  См. инструкции по установке клиентских сертификатов в руководстве по установке.

Процедура

1. В программе AMS щелкните **Файл** > **Выход**, чтобы остановить все запущенные службы.
2. Когда работа программы будет завершена, запустите приложение **Службы Windows** и убедитесь, что службы `Access Engine` и `Access Management System` остановлены.
3. Нажмите «Пуск» в меню Windows> **AMS — восстановление**
4. Нажмите кнопку **[...]**, чтобы найти и выбрать файл резервного копирования GZIP.



5. Нажмите **Пуск**, чтобы начать процесс восстановления.
6. Введите учетные данные для входа **SQL sysadmin**.
   Процесс восстановления начинается



7. Когда процесс восстановления будет завершен, запустите приложение **Службы Windows** и убедитесь, что все службы `Access Engine` и `Access Management System` перезапущены.
   В противном случае перезапустите их вручную.
8. Запустите **AMS Map View** с рабочего стола.
9. Найдите и щелкните правой кнопкой мыши MAC в Map View.
10. Выберите **MAC холодного запуска**, чтобы повторно синхронизировать данные из резервной копии с текущими системными данными.

Глоссарий

1.MAC (первый контроллер MAC)

Главный контроллер доступа MAC в системе BIS Access Engine (ACE) или системе Access Manager (AMS). Он может находиться на том же компьютере, что и DMS, но может, как подчиненный контроллер MAC, находиться на отдельном компьютере — сервере MAC.

IDS

Система охранной сигнализации, которую также называют системой обнаружения вторжения.

MAC (главный контроллер доступа)

В системах контроля доступом серверная программа, которая координирует и контролирует локальные контроллеры доступа (как правило, AMC)

RMAC

Резервный главный контроллер доступа (MAC), который является синхронизированной парой существующего контроллера MAC и принимает на себя управление данными в случае сбоя или отключения основного контроллера.

SmartIntego

Цифровая система блокировки от Simons Voss Technologies. SmartIntego интегрируется с некоторыми системами контроля доступа Bosch.

Автоматическое считывание номерных знаков (ANPR)

)Использование видеотехнологии для считывания и обработки номерных знаков (как правило, на транспортных средствах).

Белый список (SmartIntego)

Белый список — это список номеров карт, который хранится локально на считывателях карт системы блокировки SmartIntego. Если MAC считывателя не в сети, считыватель предоставляет доступ картам, номера которых содержатся в локальном белом списке.

Верификационный PIN-код

Личный идентификационный номер (PIN) используется в сочетании с физическими учетными данными для обеспечения более высокой степени безопасности.

Запрет повторного прохода

Простая форма мониторинга последовательности доступа, не позволяющая владельцу карты дважды войти в определенную область в течение определенного периода времени (если за это время карта не была сканирована для выхода из области). Эта функция не позволяет передавать учетные данные для повторного использования на входе другим человеком, не имеющим соответствующих прав.

Идентификационный PIN-код

Личный идентификационный номер (PIN-код) представляет собой единственные учетные данные, необходимые для доступа.

Контроль последовательности доступа

Отслеживание человека или автомобиля, перемещающегося из одной определенной области в другую, путем записи каждого сканирования идентификационной карты и предоставления доступа только в областях, где карта уже была сканирована.

Локальный контроллер доступа (LAC)

Аппаратное устройство, которое отправляет команды доступа периферийным устройствам контроля доступа, таким как считыватели и блокировки, и обрабатывает запросы с этого оборудования для всей системы контроля доступа. Наиболее распространенным LAC является модульный контроллер доступа или AMC.

Модель дверей

Хранимый программный шаблон определенного типа входа. Модели дверей упрощают определение входов в системах контроля доступа.

Нормальный режим

В нормальном режиме, в отличие от офисного, доступ предоставляется только лицам, предъявившим считывателю действительные учетные данные.

Офисный режим

Приостановка контроля доступа на входе в рабочее время.

Предупреждение об угрозе

сигнал тревоги, который активирует уровень угрозы. Уполномоченные лица могут активировать предупреждение об угрозе с помощью кратковременного действия, например в пользовательском интерфейсе оператора, с помощью аппаратного сигнала (например, кнопки) или предъявив специальную карту для предупреждения об угрозе на любом считывателе.

Проход

Термин «Проход» означает весь механизм контроля доступа в точке входа. Он включает считыватели, запираемый барьер определенной формы и процедуру доступа, определяемую предварительно заданными последовательностями электронных сигналов, которые передаются между элементами оборудования.

Проход вплотную

Обход системы контроля доступа путем плотного следования на входе за владельцем карты с соответствующими разрешениями без предъявления собственных учетных данных.

Сервер MAC

Оборудование: компьютер A (кроме сервера DMS) в системе Access Engine (ACE) или системе управления доступом (AMC), где работает контроллер MAC или RMAC.

Система управления данными (DMS)

Процесс верхнего уровня для управления данными контроля доступа в Access Engine. DMS передает данные главным контроллерам доступа (MAC), которые, в свою очередь, предоставляют данные локальным контроллерам доступа (как правило, AMC).

Система управления данными (DMS)

Процесс верхнего уровня для управления данными контроля доступа в Access Engine. DMS предоставляет данные контроллерам MAC, которые, в свою очередь, отправляют эти данные контроллерам AMC.

Точка сбора

Место, где, согласно инструкции, должны собраться и ждать люди после эвакуации здания.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com