Access Management System V5.2

Конфигурация и эксплуатация

ru Software manual

Содержание

1 Безопасность

Используйте самую актуальную версию ПО

Перед первым использованием устройства установите самую актуальную версию ПО. Для обеспечения оптимальных функциональных возможностей, совместимости, производительности и безопасности регулярно обновляйте ПО в течение всего срока эксплуатации устройства. Следуйте инструкциям в документации к продукту в отношении обновлений ПО.

Более подробную информацию можно получить по следующим ссылкам:

– общие сведения: https://www.boschsecurity.com/xc/en/support/product-security/
– рекомендации по безопасности, а именно список обнаруженных уязвимых мест и предлагаемых решений: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Компания Bosch не берет на себя никакой ответственности за какой-либо ущерб, вызванный эксплуатацией ее продуктов при использовании устаревшего ПО.

2 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]

3 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.

4 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.

5 Лицензирование системы

Предварительные 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 этого компьютера. Для получения инструкций обратитесь к торговому представителю.

Активация лицензии

Путь

– Диспетчер диалоговых окон системы AMS > **Главное меню** > **Конфигурация** > **Лицензия**

1. Нажмите **Диспетчер лицензий**
   Откроется мастер **Менеджер лицензий**.
2. Нажмите кнопку **Сохранить** для сохранения информации о системе в файл.
3. Нажмите кнопку **Продолжить**.
4. Войдите на удаленный портал remote.boschsecurity.com с учетными данными компании.
5. Выберите продукт, для которого нужно активировать лицензию, и следуйте инструкциям на портале, чтобы создать и скачать лицензионный файл.
6. Вернитесь в **менеджер лицензий**.
7. Нажмите кнопку **Продолжить**.
8. Нажмите кнопку **Импорт**, чтобы найти загруженный лицензионный файл и добавить его в систему.
9. Нажмите кнопку **Готово**.

Замечание!
Если в процессе появляются сообщения об ошибках, обратитесь в службу поддержки Bosch.

Замечание!
Результаты аппаратных и программных изменений
Изменение аппаратного обеспечения сервера может привести к аннулированию лицензии и прекращению функционирования программного обеспечения. Перед внесением изменений в сервер проконсультируйтесь со специалистом службы поддержки.

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.

6 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**.

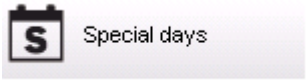
Временные модели контролируют действия, когда они применяются к базовому **календарю** системы контроля доступа.

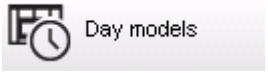
Календарь системы контроля доступа основан на календаре операционной системы хост-компьютера, однако в системном календаре также предусмотрены **особые дни**, которые свободно определяются администратором системы контроля доступа.

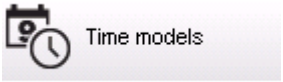
Особыми днями можно назначить определенную дату в календаре или определить их относительно какого-либо культурного события, например Пасхи. Они могут повторяться, но это необязательно.

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.



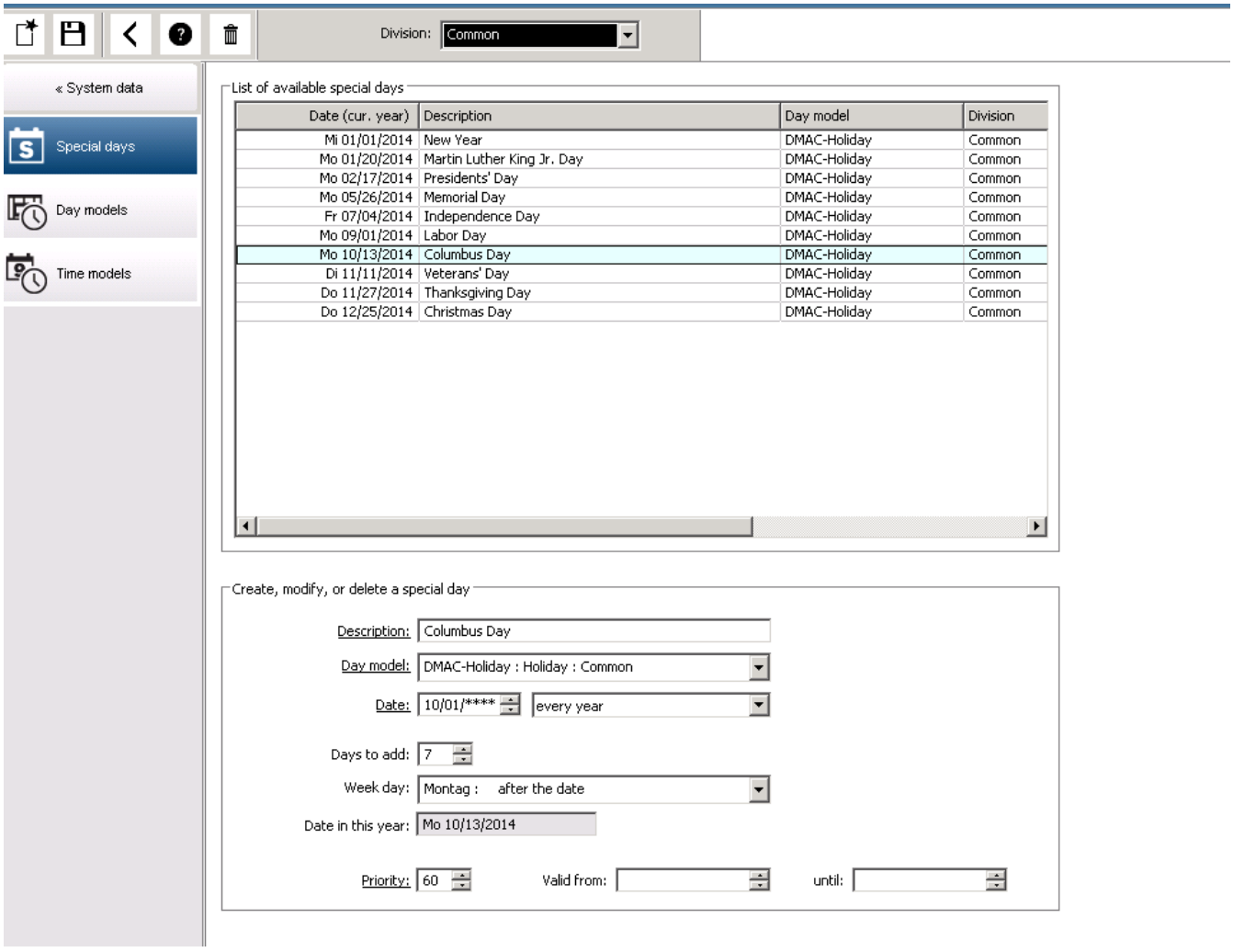




6.1 Определение особых дней

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	**.**.****

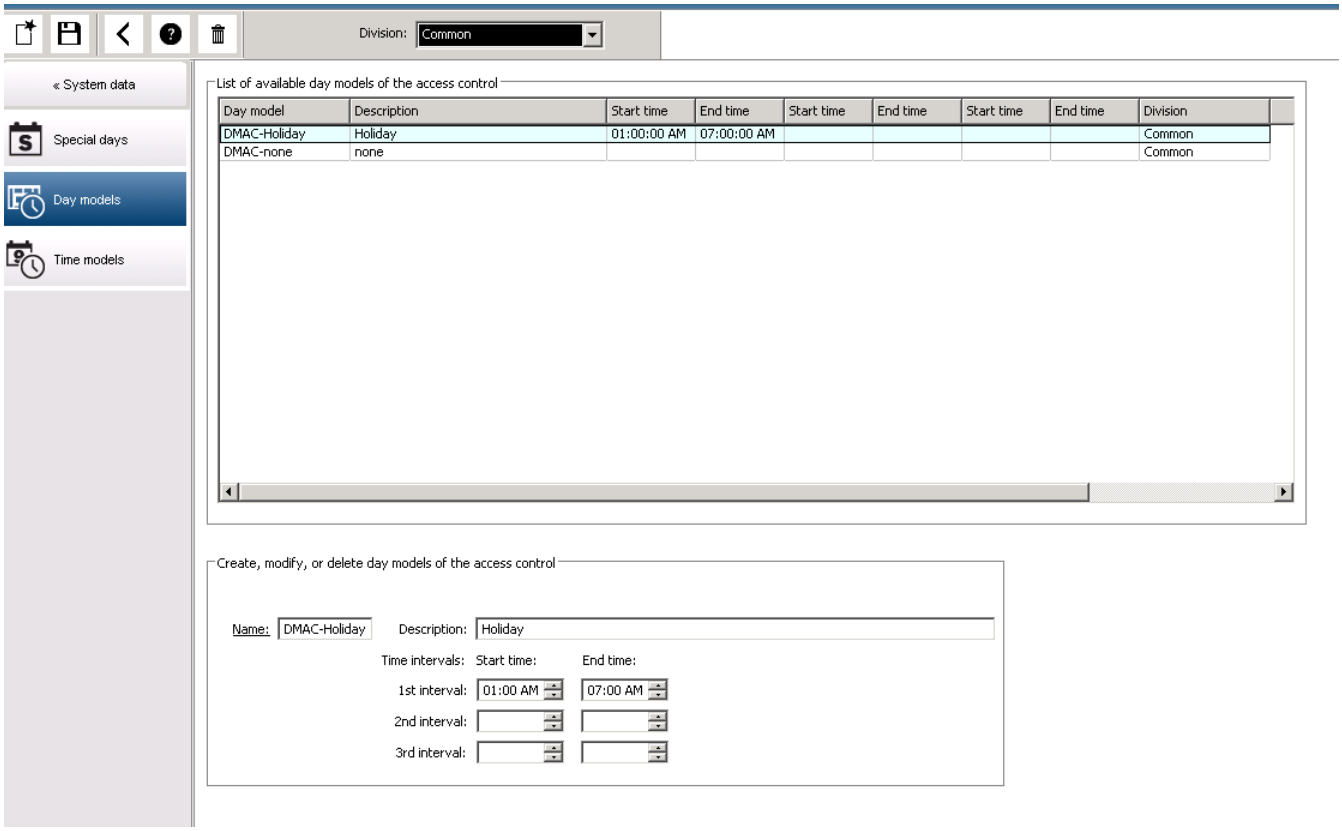
Праздничные дни, которые зависят от даты Пасхи, указываются не по дате, а по разности дней с Пасхальным воскресением. Дата Пасхального воскресения в текущем году указывается в поле **Дата в данном году**, а отклонение от этой даты вводится или выбирается в поле **Добавить дни**. Максимальное число дней — 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.

6.2 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:

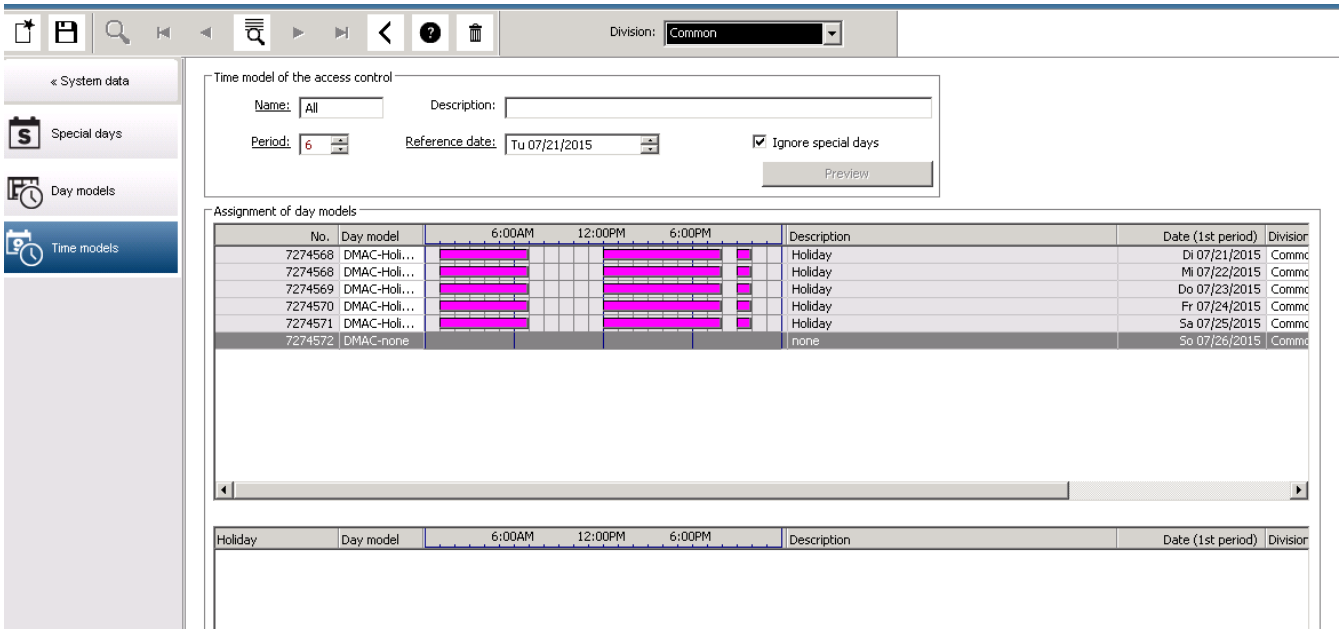
1-й интервал	от:	...	до:	00:00
Следующий интервал	от:	00:00	до:	...

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.

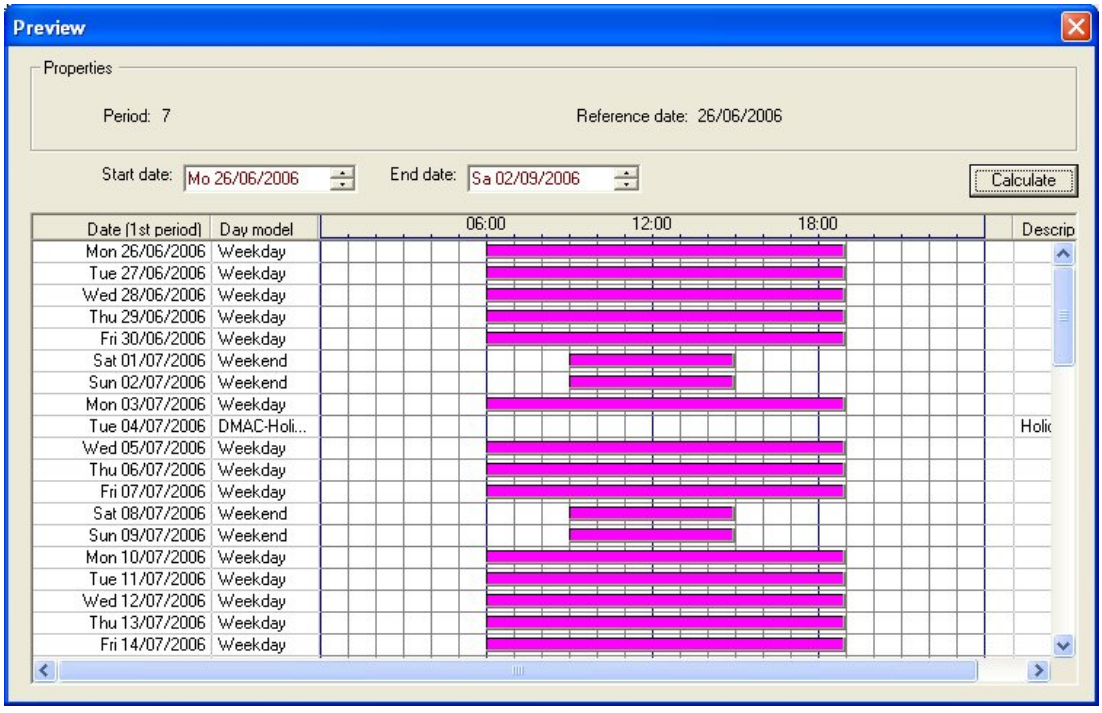
Модель дня можно удалить только в том случае, если она не назначена ни одному специальному дню и не используется во временных моделях.

6.3 Определение временных моделей

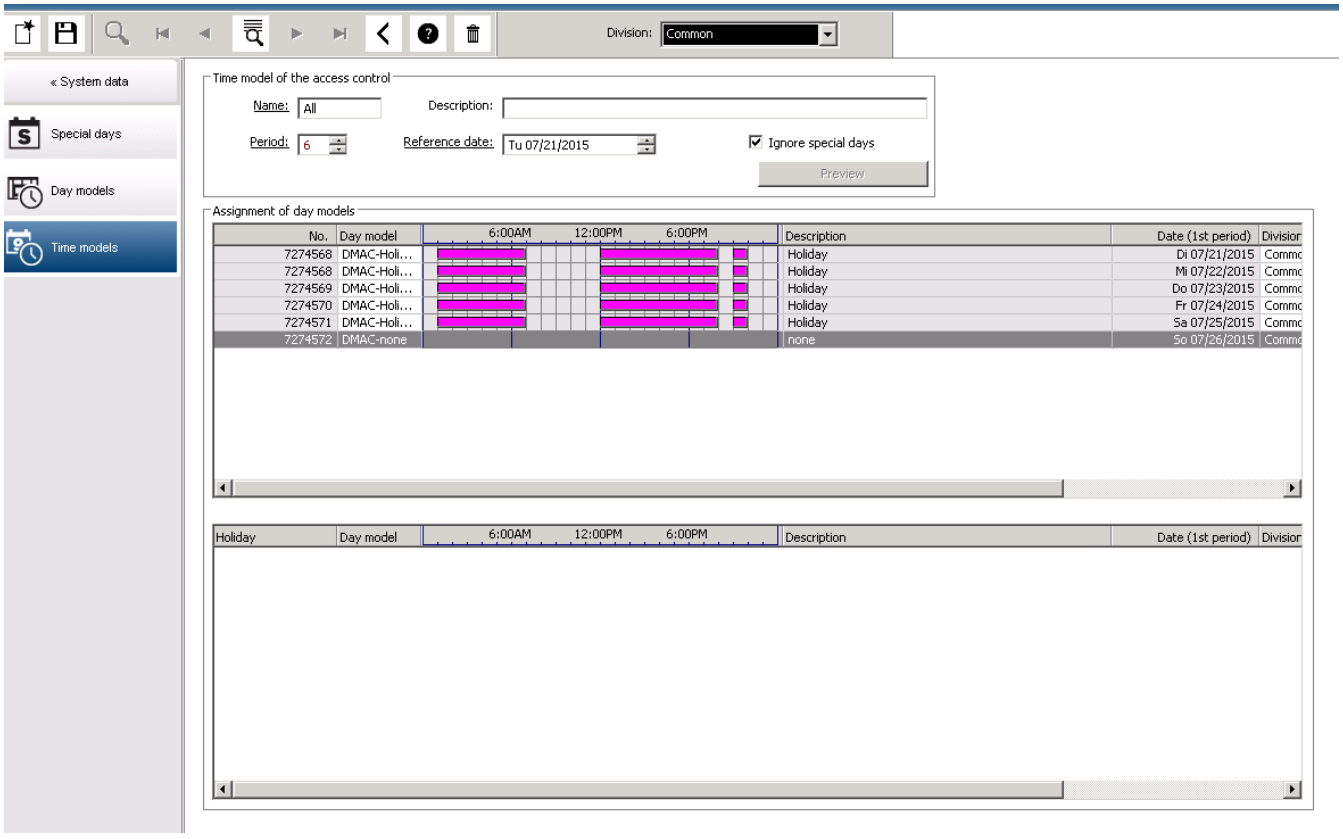


Существующие модели времени можно выбрать из списка поиска, а сведения о них отображаются в полях диалогового окна. Любая обработка осуществляется в соответствии с процедурой создания новых моделей времени.
Если маска пуста, модели времени можно создавать с нуля. Для этого необходимо ввести **имя** и 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)
7274568 DMAC-Holi... Holiday Di 07/21/2015
7274568 DMAC-Holi... Holiday Mi 07/22/2015
7274569 DMAC-Holi... Holiday Do 07/23/2015
7274570 DMAC-Holi... Holiday Fr 07/24/2015
7274571 DMAC-Holi... Holiday Sa 07/25/2015
7274572 DMAC-none none So 07/26/2015
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)

7 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

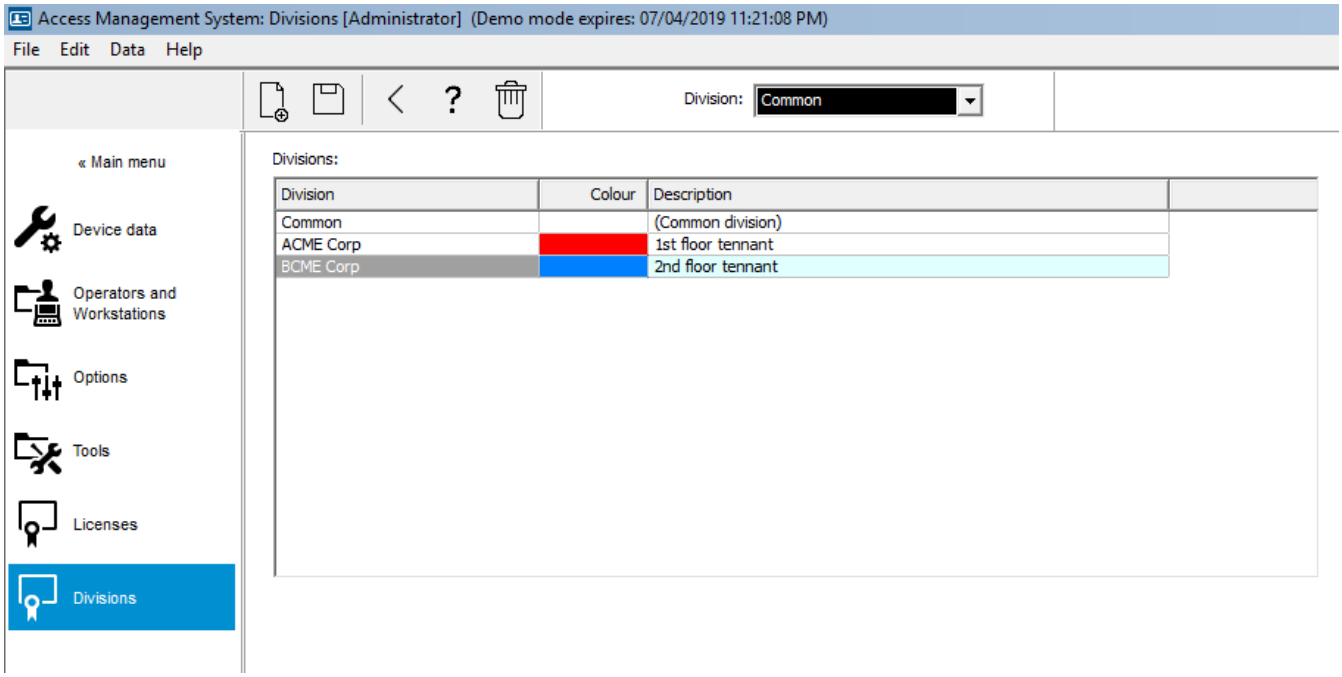
– Функция «Подразделения» лицензирована для вашей установки.

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.



7.1 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.

7.2 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

8 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.

9 Использование редактора устройств

Введение

Редактор устройств — это инструмент для добавления, удаления и изменения точек доступа и устройств.

В нем доступны представления для следующих редактируемых иерархий:

- **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.

Предварительные требования

Система правильно установлена, лицензирована и подключена к сети.

Путь к диалоговому окну

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

Использование панели инструментов редактора устройств

Независимо от того, какое представление активно (**Устройства**, **Рабочие станции** или **Области**), на панели инструментов редактора устройств доступны приведенные ниже функции.

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 редактора устройств 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 к устройству, сначала выберите родительское устройство, под которым должен отображаться этот вложенный элемент.

Копирование и вставка устройств AMC

Чтобы копировать устройства AMC из одной части дерева в другую:

1. Щелкните устройство AMC правой кнопкой мыши и в контекстном меню выберите **Копировать**.
2. Щелкните правой кнопкой мыши подходящее родительское устройство в другой части дерева и в контекстном меню выберите **Вставить**.
   - Устройство копируется в новое расположение вместе со вложенными устройствами и параметрами.
   - Значения параметров устройства, такие как **IP-адрес** и **имя**, которые должны быть уникальными, **не копируются**.
3. При необходимости введите уникальные значения для таких параметров устройств. Это обязательно для сохранения дерева устройств.

Сохранение работы

Завершив добавление элементов в дерево и их изменение, нажмите **Сохранить**  , чтобы сохранить конфигурацию.

Чтобы закрыть редактор устройств, нажмите **Файл** > **Выход**.

9.1 Режимы конфигурирования и переопределения

Режим конфигурирования — это состояние устройств управления доступом по умолчанию в редакторе устройств. В режиме конфигурирования авторизованный пользователь AMS или BIS ACE может вносить в редакторе устройств изменения, которые ACS немедленно передает в подчиненные устройства.

Оператор может **переопределить** режим конфигурирования, посылая команды непосредственно в устройство управления доступом вне редактора устройств. Обычно это происходит, когда оператор обрабатывает входящие сообщения и тревоги. Пока оператор не отправит команду **Восстановить конфигурирование**, для устройства сохраняется Режим работы.

Если в редакторе устройств пользователь выбирает устройство, находящееся в режиме работы, на странице основных свойств устройства отображается уведомление:

Это устройство не находится в режиме конфигурирования.

Пользователь может выполнять конфигурирование и сохранение, но изменения помещаются в буфер и вступают в силу только после завершения режима работы для тревоги и восстановления режима конфигурирования.

10 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.

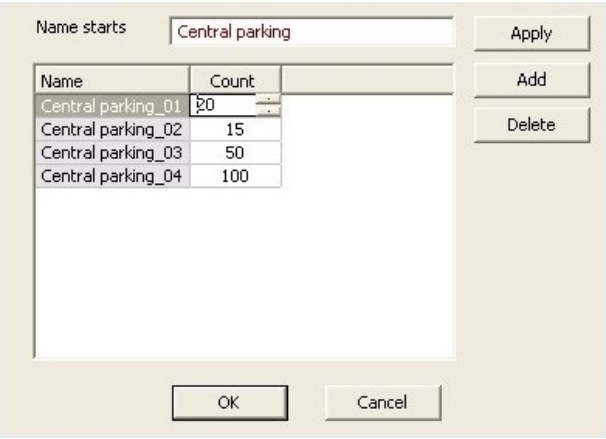
1. Щелкните область в иерархии, чтобы выбрать ее.
2. Нажмите **Удалить**  или щелкните правой кнопкой мыши, чтобы выполнить удаление через контекстное меню.

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

10.1 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.

11 Настройка охраняемых областей и панелей

Введение

Система управления доступом задействуется в управлении охранными панелями Bosch и их администрировании. Сведения о поддерживаемых моделях см. в кратком описании системы управления доступом. Система управления доступом привносит свою специфику в администрирование **пользователей** охранной панели. Эти пользователи являются подмножеством всех держателей карт общей системы управления доступом. Администраторы системы управления доступом предоставляют этим держателям карт специальные разрешения на работу с охранными панелями с помощью диспетчера диалоговых окон ACE.

Что касается самих охранных панелей, для их настройки и обновления, как и прежде, используется их собственное программное обеспечение для удаленного программирования Remote Programming Software (RPS). ACE непрерывно считывает данные из RPS и отображает доступные для нее панели.

ACE содержит диалоговые окна для создания и назначения профилей авторизации, а также для управления пользователями панелей в RPS.

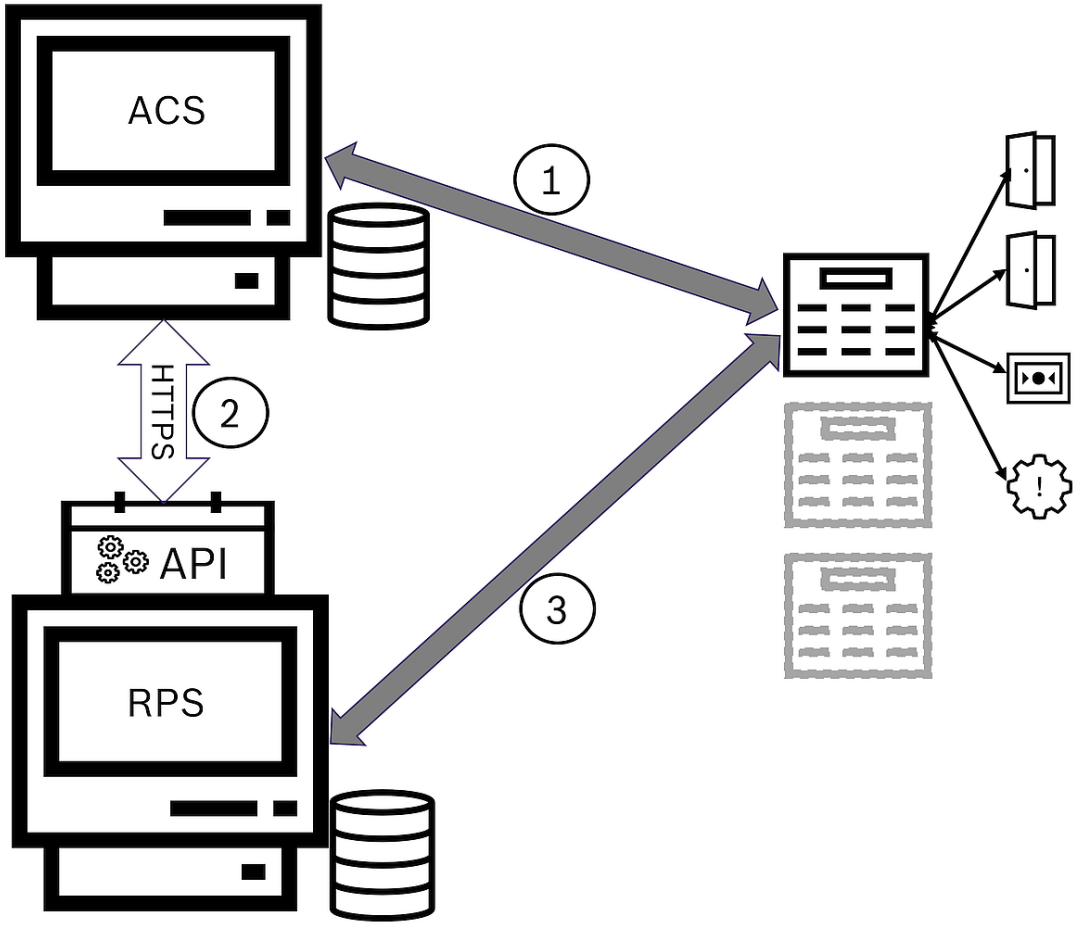


Рис. 11.1: Упрощенная топология системы охранной сигнализации ACS

ACS	Основная система управления доступом: AMS или BIS-ACE
API	Интерфейс прикладного программирования

RPS (Remote Programming Software)	Система удаленного программирования: приложение для управления охранными панелями
1	От ACS до панели: команды панели. От панели до ACS: события на огранных точках.
2	От ACS до RPS: данные держателей карт
3	От RPS до панели: параметры конфигурации

Предварительные требования

- Программное обеспечение RPS поддерживаемых охранных панелей Bosch установлено на отдельном компьютере с сетевым подключением к серверу ACE, а **не** на самом сервере ACE. Инструкции по установке RPS см. в соответствующем руководстве.
- ПО RPS настроено для работы с охранными панелями, которые будут принадлежать системе управления доступом ACE. См. инструкции в руководстве пользователя RPS или в онлайн-справке.
- Часы на панелях находятся в пределах 100 дней относительно часов на сервере ACE для обеспечения автоматической синхронизации.
- Протокол режима 2 задан на всех участвующих панелях.
- Карты с одним из следующих стандартных определений:
  - HID 37 BIT -> Вторжение 37 БИТ с кодом объекта 32767 или ниже.
  - HID 26 BIT- > Вторжение 26 БИТ
  - EM 26 BIT- > Вторжение 26 БИТ

Обзор

Процесс настройки состоит из перечисленных ниже этапов, которые будут описаны в следующих разделах этой главы:

1. Установка охранного интерфейса RPS API на компьютер с RPS
2. Подключение системы управления доступом к охранным панелям.
   - Определение подключения к интерфейсу RPS API.
   - Настройка подключений панели.
3. Создание профилей прав доступа к панелям, определяющих, какие функциональные возможности подключенных панелей могут использоваться.
4. Назначение профилей прав доступа к панелям держателям карт.
   - Таким образом, эти держатели карт становятся операторами охранных панелей.

11.1 Установка охранного интерфейса RPS API на компьютер с RPS

Охранный интерфейс RPS API — это канал связи между программами AMS и RPS на соответствующих компьютерах. Сначала необходимо установить интерфейс API на компьютере с RPS, а затем установить сертификаты, создаваемые программой установки на компьютере с AMS.

Процедура

1. Запустите файл установки интерфейса RPS API в соответствии с прилагаемой к нему документацией.

– Файл установки и его документация находятся на установочном носителе AMS:
  `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
  `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
– Программа установки создаст два сертификата и сохранит их на компьютере с RPS:
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (необходимо установить пароль)

2. Скопируйте файлы сертификатов компьютер с AMS.
3. Установите сертификаты на компьютере с AMS в **расположение хранилища**: `Local Machine`, **хранилище сертификатов**: `Trusted Root Certification Authority`.

11.2 Подключение системы управления доступом к охранным панелям

Введение

В этом разделе описывается, как отобразить охранные панели и сделать их доступными для управления с помощью ACE client. Система управления доступом подключается через интерфейс API к ПО RPS в своей сети. Через этот интерфейс API система постоянно обновляет внутренний список доступных совместимых охранных панелей. Для подключения этой системы к охранным панелям в AMS нужно выполнить два шага:

– Шаг 1. Определение подключения к RPS API
– Шаг 2. Настройка подключений панели

Путь к диалоговому окну

– Главное меню > **Конфигурация** > **Панели** и вложенные диалоговые окна

11.2.1 Шаг 1. Определение подключения к RPS API

На шаге 1 в систему управления доступом передается информация об адресе компьютера с RPS и учетные данные администратора.

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Панели > Конфигурация RPS API**

Процедура

1. Введите следующую информацию:

Информация	Описание
Имя хоста/IP-адрес	HTTPS-адрес компьютера, на котором выполняется RPS, и номер порта, через который обменивается данными RPS. Использование `localhost` не разрешено. Номер порта по умолчанию — `9000`.
Имя пользователя	Имя администратора RPS для API.
Пароль	Пароль администратора RPS.

2. Нажмите кнопку **Проверить подключение**, чтобы проверить работу RPS и допустимость имени пользователя и пароля.
3. Нажмите  (Сохранить) для сохранения изменений.

11.2.2 Шаг 2. Настройка подключений панели

На шаге 2 настраивается уровень управления системы управления доступом для отдельных панелей в сети.

Путь к диалоговому окну

Главное меню > **Конфигурация** > **Панели > Администрирование панели**

В этом диалоговом окне приведен список совместимых охранных панелей, которые интерфейс RPS API предоставил для ACE.

Этот список периодически обновляется в фоновом режиме. После открытия диалогового окна можно время от времени нажимать кнопку  , чтобы немедленно выполнить обновление вручную.

Данный список доступен только для чтения, за исключением элементов управления, описанных в следующем разделе.

Процедура

1. Выберите панель из списка
2. Используйте указанные ниже элементы управления, чтобы определить, какие возможности система управления доступом будет иметь на выбранной охранной панели.

Столбец списка **Администрирование пользователей**	Установите флажок, чтобы пользователи охранной панели, указанные в этой строке, были сохранены в системе управления доступом, а **не** в самой панели. **ВАЖНО!** При выборе этой настройки все пользователи панели, созданные локально в RPS, будут перезаписаны.
Столбец панели **Map View**	Чтобы панель была доступна для выполнения команд и управления посредством ACE client, установите этот флажок.
Значок настройки  (шестеренка) в столбце **Данные доступа**.	Если в столбце **Map View** установлен флажок, нажмите значок, чтобы указать – IP-адрес; – номер порта (по умолчанию — 7700); – пароль для отдельной панели. Этот пароль устанавливается в RPS.
Кнопка: **Удалить выбранную панель**	Если панель была удалена в RPS, она отображается в списке с состоянием **Удалено**. Выберите панель и нажмите эту кнопку, чтобы полностью удалить ее из базы данных.

11.3 Создание профилей прав доступа к панелям

Введение

В этом разделе описывается порядок создания профилей авторизации панели.

Профиль прав доступа к панелям — это настраиваемый набор разрешений на работу с настраиваемым набором охранных панелей. Администратор ACE может создать несколько профилей авторизации панели в зависимости от обязанностей разных групп держателей карт.

Путь к диалоговому окну

– Главное меню > **Системные данные Профили авторизации для охранных панелей**

Процедура

1. Чтобы создать новый профиль, щелкните  .
2. (Обязательно) Введите имя профиля.
3. (Необязательно) Введите произвольное текстовое описание панели.
4. Под списком **Назначенные панели** нажмите **Добавить...**, чтобы добавить в список одну или несколько панелей из всплывающего списка панелей, доступных в сети. Чтобы, напротив, удалить панели из списка, выберите одну или несколько панелей и нажмите **Удалить**.
5. Выберите панель в списке **Назначенные панели**, щелкнув по ней.
   - В области **Полномочия** отобразится список, содержащий все охраняемые области, принадлежащие выбранной панели.
6. В столбце **Уровень полномочий** списка **Полномочия** выберите уровень полномочий для каждой охраняемой области панели, которую нужно включить в этот профиль.
   - Уровни полномочий определяются и хранятся в RPS. Там же их можно настраивать. Прежде чем назначать уровень полномочий профилю, перепроверьте его определение в RPS.
   - По умолчанию самый широкий круг полномочий дает уровень **L1**, а с увеличением номера уровня (**L2**, **L3**, ...) полномочия все более ограничиваются.
   - Если оставить эту ячейку пустой, то получатель данного профиля **не** будет иметь прав доступа к данной охраняемой области выбранной панели.
7. Повторите эту процедуру для всех охраняемых областей всех панелей, которые нужно включить в данный профиль.
8. (Необязательно) В списке **Группа пользователей** выберите группу пользователей панели, если нужно, чтобы предоставленные полномочия действовали лишь в определенные периоды времени.
   - Группы пользователей определяются и хранятся в RPS. Там же их можно настраивать. Прежде чем назначать группу пользователей профилю, перепроверьте ее определение в RPS.
9. Нажмите  (Сохранить) для сохранения изменений.

11.4 Назначение профилей авторизации панелей держателям карт

Введение

В этом разделе описано, как назначать разные профили авторизации панели держателям карт различных типов или групп.

Предварительное требование

Вы определили один или несколько профилей авторизации панели в системе управления доступом.

Путь к диалоговому окну

Главное меню > **Лица** > **Карты**

Процедура

1. Обычным способом найдите и выберите требуемого держателя карты в базе данных.
2. Откройте вкладку **Охрана**.
3. На вкладке **Охрана** установите флажок **Пользователь панели**.

4. (Обязательно) В поле **Код допуска** введите код допуска, который данный держатель карты будет использовать для работы с охранными панелями.
   – При необходимости используйте кнопку, чтобы сгенерировать новый неиспользуемый код допуска.
5. В списке **Идентификационная карта** выберите одни из учетных данных управления доступом, присвоенных данному держателю карты.
6. (Дополнительно) В поле **Номер удаленного устройства** введите номер, который напечатан на устройстве удаленного управления держателя карты для охранных панелей.
7. В списке **Язык** выберите язык диалоговых окон панели, предпочтительный для держателя карты.
8. Если держатель карты использует мобильное приложение Bosch для охранных панелей, установите флажок **Удаленный доступ**.
9. В списке **Профиль авторизации** выберите профиль авторизации панели, подходящий для держателя карты.
10. Нажмите  (Сохранить) для сохранения изменений.
    – Держателю карты будет назначен этот профиль авторизации панели со всеми включенными в него панелями и полномочиями. Таким образом, держатель карты становится оператором охранных панелей.

Обратите внимание, что в этом диалоговом окне также можно использовать поля данных с кнопкой  для поиска держателей карт в базе данных.

11.5 Управление дверями с помощью модулей B901 на охранных панелях

Начиная с версии AMS 4.0.1, модулями интерфейса управления доступом B901 можно управлять с помощью AMS Map View.
Модуль B901 — это простой контроллер двери, подключаемый к охранным панелям Bosch системным администратором. Соответствующая охранная панель подключается к AMS, как описано в предыдущих разделах.
Модуль B901 не настраивается в редакторе устройств.
Модули B901 могут отпирать/запирать, переводить в режим защиты/выводить из него и выполнять цикл двери, но передают в систему управления доступом только ограниченную информацию о состоянии. Например, они сообщают, что дверь разблокирована, но не могут сообщить, открыта ли она физически.
Как и в случае с другими охранными устройствами, для отправки команд модулю B901 из AMS Map View нужно включить представление Map View для соответствующей панели в диалоговом окне AMS:
Главное меню > **Конфигурация** > **Панели > Администрирование панелей**

Приложение Swipe ticker в Map View и двери с модулями B901
Для предоставления правильной информации приложению **Swipe ticker** в представлении AMS Map View идентификаторы дверей с модулями B901 должны совпадать с идентификаторами их дверных точек. Например, дверь 1 должна быть назначена дверной точке 1, дверь 2 дверной точке 2 и т. д.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Эти назначения для контроллера дверей B901 выполняются в инструменте RPS для настройки охранных панелей и контроллеров.

12 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**

12.1 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 времени неактивности:** время в секундах после сеанса входа с использованием регистрационного считывателя, после которого сеанс автоматически завершается. Установите значение `0`, чтобы это время было неограниченным.

12.2 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.

12.3 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.

12.4 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

12.5 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

12.6 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.
Предварительные 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.
При первом входе в систему после установки потребуется изменить пароль администратора.

Процедура изменения паролей других операторов.
Предварительные 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/

13 Настройка карт

13.1 Описание карты

Это диалоговое окно используется для активации, деактивации, изменения или добавления описаний карт, используемых системой управления доступом.

Путь к диалоговому окну

– Главное меню AMS > **Конфигурация** > **Параметры** > **Описание карты**

Система поставляется с набором предварительно определенных типов карт. Предварительно определенные типы карт отображаются на сером фоне в таблице **Доступные типы карт** и не подлежат редактированию. Однако их можно перемещать между таблицами **Активные типы карт** и **Доступные типы карт**.

13.1.1 Создание и изменение

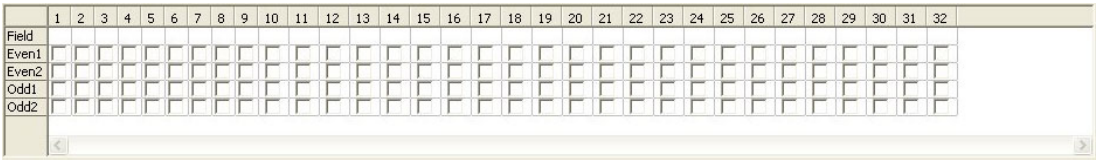
Нажмите кнопку со знаком плюс зеленого цвета (✚) над правым полем списка, чтобы создать новый элемент списка. В отличие от предварительно определенных типов карт данные вновь созданных типов можно свободно редактировать. Чтобы изменить **имя**, **описание** и **количество битов**, дважды щелкните соответствующие поля. Максимальная длина имени — 80 символов, максимальная длина описания — 255 символов. Число битов ограничено 64 (если введено большее значение, оно сбрасывается до указанного максимума, как только данное текстовое поле перестает быть в фокусе ввода).

Замечание!
Длины битов используются, чтобы различать определения Wiegand. Поэтому у каждого нового определения должна быть уникальная длина битов, еще не использованная в существующих определениях.

- Чтобы изменить бит данных, дважды щелкните соответствующее поле. Чтобы его удалить, сначала выберите бит данных, а затем щелкните красную кнопку x (✕).

Замечание!
Можно изменить или удалить только те типы карт, которые были созданы пользователем.

При выборе одного типа карты (в левом или правом списке) в нижней части диалогового окна отображается его кодировка. В данном окне отображаются биты данных в 5 строках, а число столбцов равно количеству битов в описании.



Каждому столбцу строки **Поле** может быть присвоена метка, которая определяет интерпретацию этой части кода. Доступны следующие метки:

F	Помещение: помечает принадлежность данной части кода к помещению	
C	Номер кода: часть кода, содержащая индивидуальный номер карты	
E1	Четность 1: бит для балансировки первой маски проверки на четность	При объявлении этих значений устанавливаются флажки для соответствующих строк.
E2	Четность 2: бит для балансировки второй маски проверки на четность	
O1	Нечетность 1: бит для балансировки первой маски проверки на нечетность	
O2	Нечетность 2: бит для балансировки второй маски проверки на нечетность	
1	В коде содержатся фиксированные битовые значения	
0		

В случае меток E1, E2, O1 и O2 достаточно установить флажок в соответствующей строке. Флажки в строке **Поле** устанавливаются автоматически.

Описание:

Сигнал, отправляемый считывателем при предъявлении карты, состоит из последовательности нулей и единиц. Для каждого типа карт точно определяется длина такого сигнала (т. е. число битов).

Кроме актуальных данных пользователя, которые сохраняются как данные кода, сигнал также содержит управляющие данные, чтобы а) идентифицировать сигнал как сигнал карты и б) проверить правильность передачи.

В общем, фиксированные нули и единицы полезны для идентификации типа сигнала. Для проверки правильности передачи используются биты проверки четности, которые должны давать ноль (проверка на четность) или единицу (проверка на нечетность) в качестве контрольной суммы выбранных битов сигнала. Контроллеры можно настроить так, чтобы они вычисляли одну или две контрольные суммы и при проверке на четность, и при проверке на нечетность.

В соответствующих строках контрольных сумм четности (Четность 1, Четность 2, Нечетность 1 и Нечетность 2) можно отменить биты, которые должны быть включены в контрольную сумму. В верхней строке (Поле) для каждой используемой контрольной суммы определяется бит, чтобы сбалансировать контрольную сумму в соответствии с типом четности. Если какой-то из вариантов четности не используется, соответствующая строка просто остается пустой.

13.1.2 Активация / деактивация определений карт

Одновременно может быть активно до 8 описаний карт. Активируемые определения необходимо перенести в левый список **Активные типы карт**. Для этого следует выбрать одно или несколько определений на правой стороне и нажать кнопку со стрелкой влево (**<**).

За один раз можно переместить не более четырех определений. Если активны четыре определения, в переносе дополнительных определений будет отказано. Чтобы добавить дополнительные определения в список **Активные типы карт**, необходимо удалить одно или несколько определений из имеющихся: выбрать и переместить на правую сторону с помощью кнопки (**>**), тем самым их деактивируя.

Замечание!

При использовании считывателей с протоколами L-Bus или BG900 активируйте тип карты **Считыватель с последовательным интерфейсом**. При этом для диспетчера диалоговых окон системы управления доступом станет доступным диалоговое окно ручного ввода **Диалоговое окно Bosch**.

13.1.3 Создание данных карты в диспетчере диалоговых окон

Ввод данных вручную

Для карт Wiegand и Bosch используются разные методы ввода.

Для всех определений Wiegand (HID 26, HID 35, HID 37 и 32 Bit CSN) в окне **Диалоговое окно (Wiegand)** можно ввести **Код клиента** и **Номер карты**.

Для считывателей с последовательным интерфейсом в окне **Диалоговое окно (Bosch)** доступны также поля **Версия** и **Код страны**.

Ввод данных с помощью регистрационного считывателя

Кроме средств ручного ввода, любую рабочую станцию можно оснастить диалоговым считывателем для сбора данных карт. Используйте считыватель из списка в следующем диалоговом окне:

– Главное меню AMS > **Конфигурация** > **Параметры** > **Считыватель карт**

Если указанный считыватель выбран в качестве считывателя ввода для карт Wiegand, все активные типы карт Wiegand будут указаны вместе со считывателем.

– Главное меню AMS > **Данные персонала** > **Карты** > кнопка «Считыватель» > ▶ (стрелка вправо)

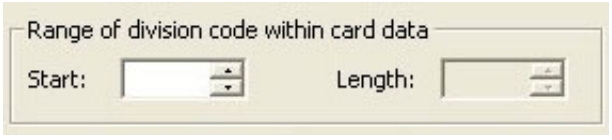
Необходимо выбрать один из данных типов карт, чтобы обеспечить правильное сохранение кодирования карт. То есть сам считыватель нельзя выбрать напрямую, а только опосредованно, путем выбора определения Wiegand.

Если требуемый тип карты не отображается в раскрывающемся списке, его необходимо активировать в диалоговом окне описания карты.

– Главное меню AMS > **Конфигурация** > **Параметры** > **Описание карты**

Регистрационные считыватели HITAG, LEGIC и MIFARE можно выбрать прямо в списке.

Определение карты для подразделений
Если лицензирована функция подразделений для управления несколькими отделами (или «подразделениями») для помещений с контролем доступа, на карте можно настроить код области, позволяющий оператору различать карты разных подразделений. Дополнительные поля (доступны для выбора, только если лицензирована функция подразделений) используются для определения на картах позиции **стартового** бита и **длины** кодирования подразделения.



13.2 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
Ввод чисел в диалоговом окне
Для удобства можно вводить числа в десятичном или шестнадцатеричном формате. Выберите переключатели **Шестнадцатеричный** или **Десятичный** в соответствии с форматом производителя карт.
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 текстовые поля для определения значений параметров **Версия**, **Код страны** и **Код объекта**, которые присваиваются номеру карты, когда карта регистрируется в системе. Если поля недоступны для записи, они не относятся ни к одному активному определению карт. Для кода Bosch все поля доступны для записи. Если карта регистрируется вручную на рабочей станции оператора, отображается диалоговое окно со значениями по умолчанию, которые можно настроить для каждой карты.

Ввод данных кода:
Если данные предоставляются производителем в виде десятичных значений, выберите переключатель «Десятичное» и введите предоставленные значения, например:
Версия: 2
Код страны: 99
Код предприятия: 56720
Нажмите **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**.

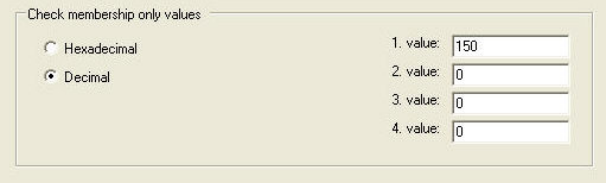
При ручном вводе номера карты используется десятичный формат.
При сохранении данных создается 10-значное десятичное значение (с начальными нулями), которое затем преобразуется в 8-значное шестнадцатеричное значение. Это значение сохраняется вместе с данными кода по умолчанию как 16-значный номер кода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

14 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

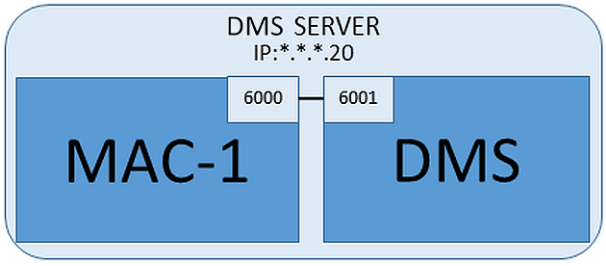
Базовое использование DevEdit описано в разделе **Использование редактора устройств** по ссылке ниже.

См.

– *Использование редактора устройств, Страница 24*

14.1 Настройка контроллеров MAC и RMAC

14.1.1 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.

14.1.2 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 управления доступом 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.

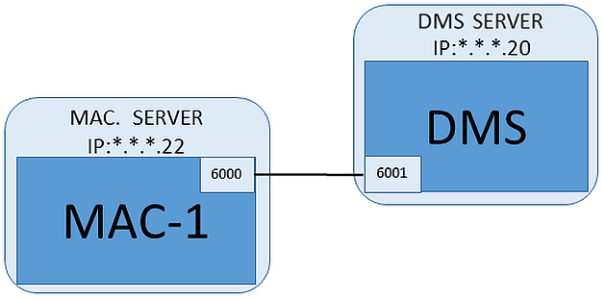
В целях обеспечения отказоустойчивости контроллеры MAC и RMAC **должны** выполняться на отдельных серверах MAC.

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

1. В данный момент операционные системы всех серверов MAC поддерживаются корпорацией Майкрософт и имеют самые последние обновления.
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 операционных системах Windows 10 и Windows Server она включена как функция.
6. Перезагрузите компьютер.

14.1.3 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 компьютере с DMS сервером в редакторе устройств
   – щелкните правой кнопкой на контроллере MAC и выберите **Disable all LACs** (Отключить все контроллеры LAC).
   – Деактивируйте контроллер MAC, сняв для него следующие флажки: **Activate** (Активация) и **Load devices** (Загрузка устройств).
2. На компьютере с MAC сервером в Windows `services.msc`
   – Остановите службу **AUTO_MAC2** контроллера MAC
   – Настройте параметр **Startup type** (Тип запуска) этой службы MAC, указав значение **Manual** (Вручную).
3. Запустите `MACInstaller.exe`
   – Для AMS этот файл находится в папке `\AddOns\MultiMAC\MACInstaller` на установочном носителе AMS (см. раздел Использование инструмента MACInstaller ниже).
4. Выполните инструкции, которые отображаются в инструменте, указав значения для следующих параметров.

Номер экрана	Параметр	Описание
3	**Папка назначения**	Локальный каталог для установки контроллера MAC. По возможности используйте значения по умолчанию.
4	**Сервер**	Имя или IP-адрес сервера, на котором запущен DMS.

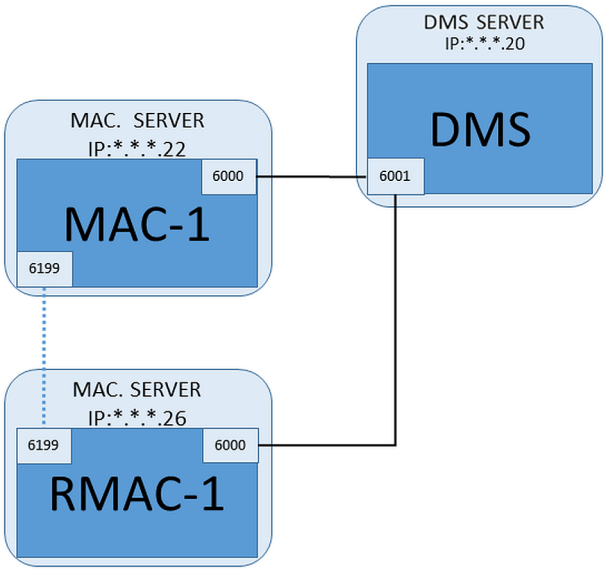
Номер экрана	Параметр	Описание
4	**Порт (порт для DMS)**	Порт на сервере DMS, который будет использоваться для получения данных от контроллера MAC**.** Используйте порт 6001 для первого контроллера MAC на сервере DMS, а для каждого последующего контроллера MAC — порт с номером на 1 больше.
4	**Номер (системный номер MAC)**	Задайте 1 для этого и всех остальных контроллеров MAC (в отличие от RMAC)**.**
4	**Пара (имя или IP-адрес контроллера-партнера MAC)**	Оставьте это поле пустым, если контроллеру MAC не должен соответствовать контроллер RMAC.

5. На сервере DMS в редакторе устройств выберите MAC.
6. На вкладке **MAC** укажите значения следующих параметров:

Параметр	Описание
Имя	Имя, которое должно отображаться в дереве устройств, например MAC-1.
Описание	Необязательное описание для системных операторов
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 MAC и всех подчиненных ему AMC.
Подразделение	(Если применимо) **Подразделение**, к которому принадлежит MAC.

14.1.4 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.

В конфигураторе на сервере DMS

1. В редакторе устройств выберите MAC, для которого необходимо добавить 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.
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 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.

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**.**
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:

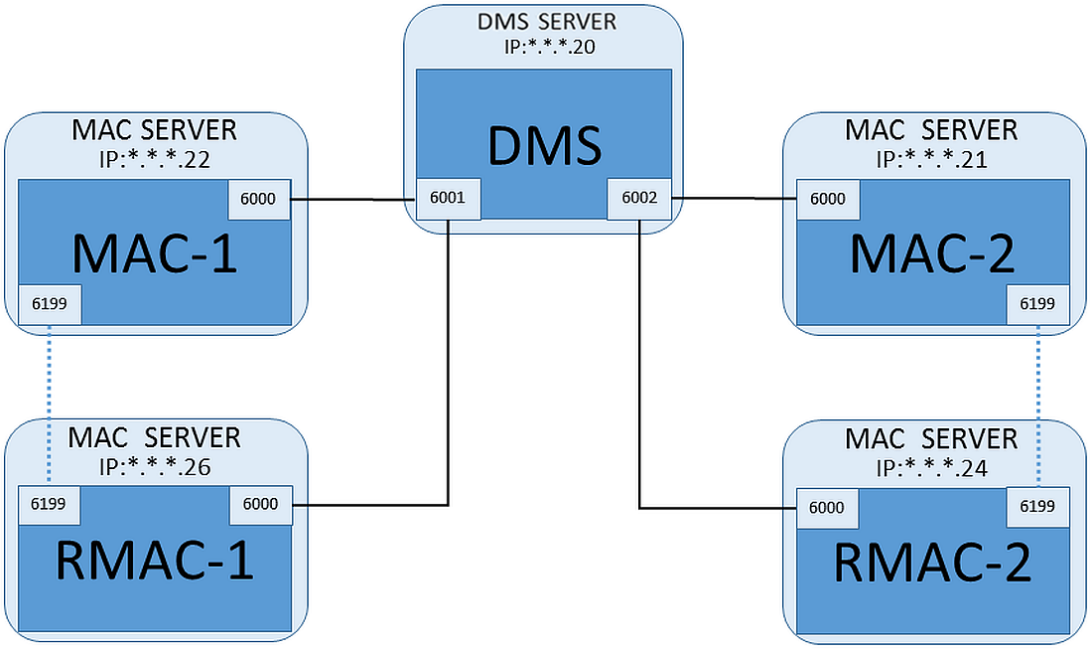
Параметр	Описание
Имя	Имя, которое должно отображаться в дереве устройств. Например, если соответствующий MAC имеет имя MAC-01, то RMAC можно присвоить имя RMAC-01.
Описание	Дополнительная документация для операторов управления доступом.
IP-адрес	IP-адрес RMAC.
Порт MAC	`6199` (Статический по умолчанию)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

См.

– *Использование средства установки MAC, Страница 57*

14.1.5 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.

14.1.6 Использование средства установки MAC

MACInstaller.exe — это стандартный инструмент для установки контроллеров MAC и RMAC на компьютерах (серверах MAC), на которых они находятся. Инструмент собирает значения параметров для контроллера MAC или RMAC и вносит необходимые изменения в реестр Windows.

Замечание!
Поскольку данный инструмент вносит изменения в реестр Windows, то перед его перенастройкой необходимо остановить выполнение всех связанных с MAC процессов.

Инструмент MACInstaller можно найти на установочном носителе по следующему пути:
– \AddOns\MultiMAC\MACInstaller.exe
Инструмент собирает значения для указанных ниже параметров, последовательно отображая ряд экранов.

Номер экрана	Параметр	Описание
3	**Папка назначения**	Локальный каталог для установки контроллера MAC.
4	**Сервер**	Имя или IP-адрес сервера, на котором запущен DMS.
4	**Порт (порт для DMS)**	Номер порта на сервере DMS; этот порт будет использоваться для связи между контроллером MAC и DMS. **См. подробные сведения ниже.**
4	**Номер (системный номер MAC)**	Задайте значение 1 для всех исходных контроллеров MAC. Задайте 2 для всех резервных контроллеров MAC (RMAC).
4	**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.

Параметр: порт (порт для DMS)
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.

Параметр: номер (системный номер MAC)
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

Параметр: Только настройка (переключатель)
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**.

Параметр: Обновление программного обеспечения (переключатель)
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**.

14.2 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

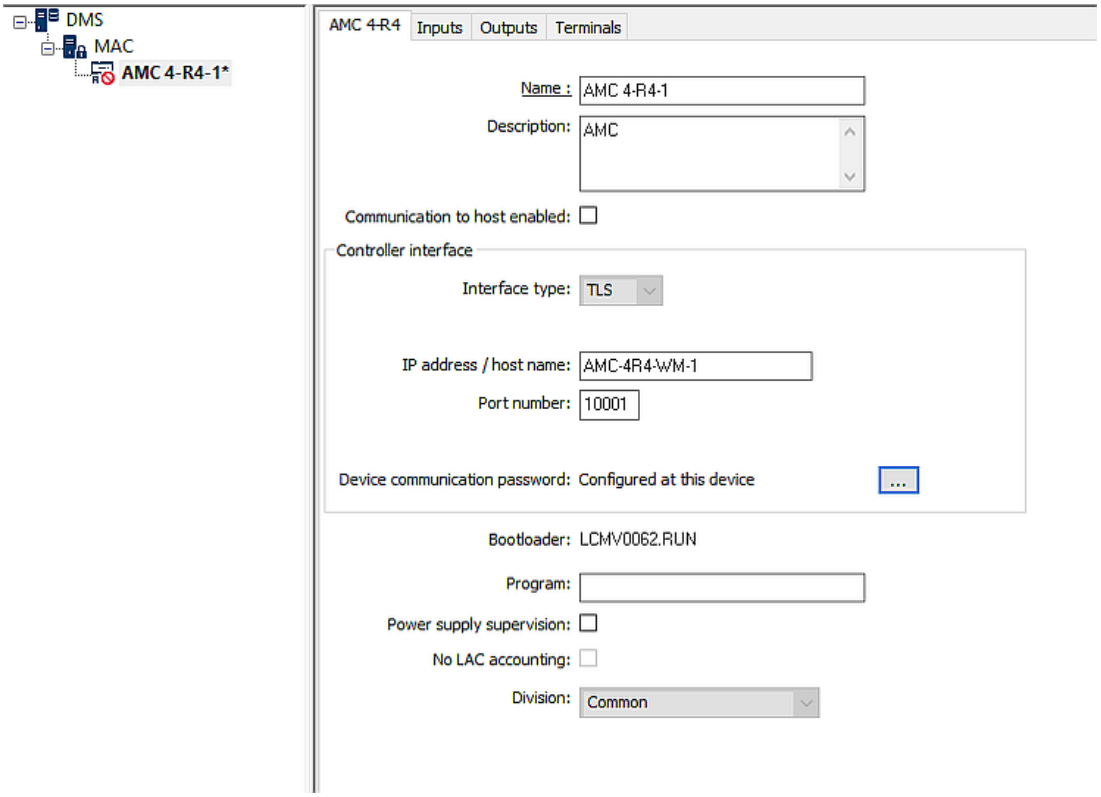
Системы управления доступом обычно оснащаются контроллером и считывателем лишь одного типа.

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.

14.2.1 Параметры и настройки AMC

Основные параметры AMC



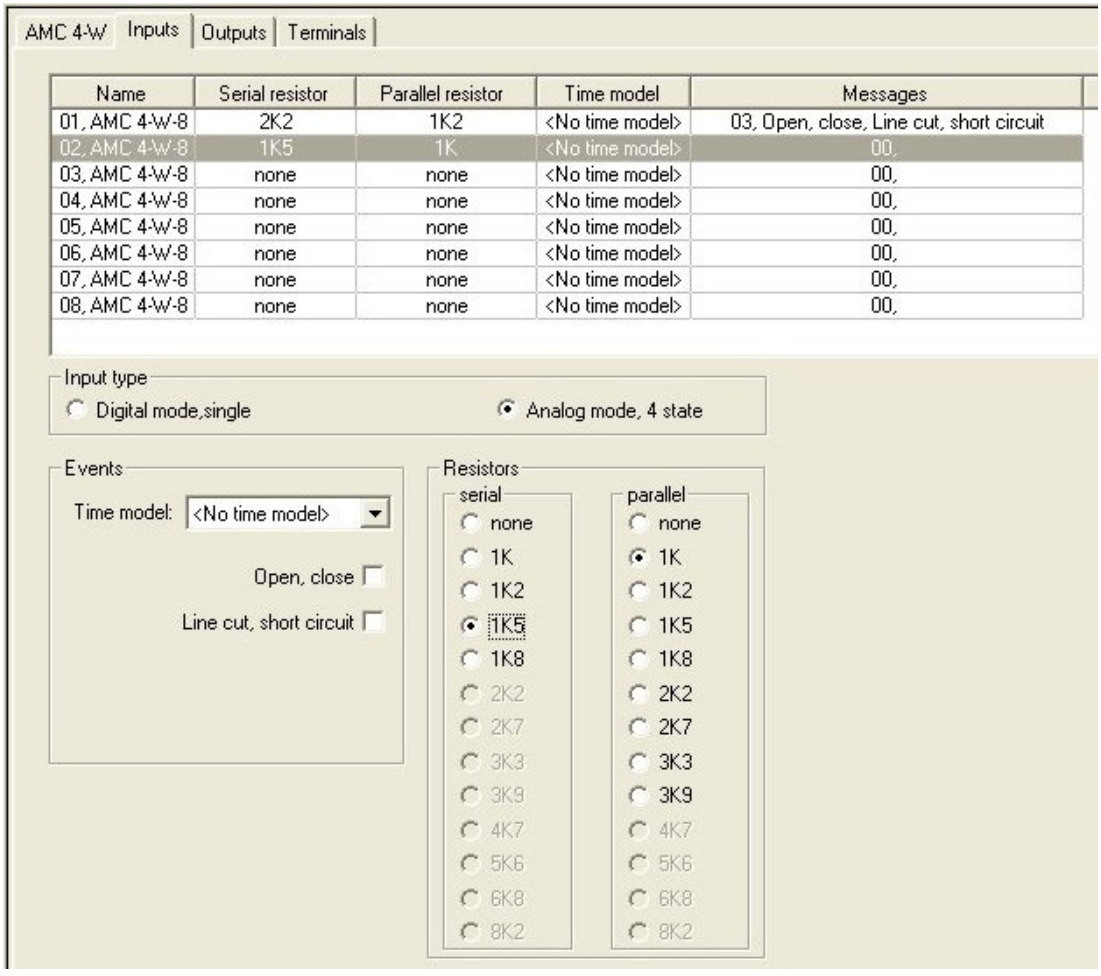
Настройка параметров AMC

Параметр	Возможные значения	Описание
Имя контроллера	Ограниченное алфавитно-цифровое значение: 1–16 знаков	Создание идентификаторов (по умолчанию) гарантирует уникальность имен, однако пользователи могут их перезаписать. При перезаписи имени необходимо убедиться, что идентификаторы уникальны.
Описание контроллера	алфавитно-цифровое значение: 0–255 знаков	Произвольный текст.
Связь с хостом активирована	0 = отключено (флажок снят) 1 = включено (флажок установлен)	По умолчанию = включено Наложенные значки на контроллерах в дереве устройств показывают состояние подключения к главной системе (подключено/отключено). Снятие флажка делает службу AMS временно недоступной. Это полезно для перенастройки и тестирования.

		При обновлении системы управления доступом до новой версии флажки всех контроллеров автоматически снимаются. Установите и снимите флажки AMC, чтобы проверить работу каждого в обновленном программном обеспечении.
		Установите флажок при использовании редактора устройств для установки DCP (пароля связи с устройством) на AMC при развертывании DTLS «сверху вниз». При этом появляется 15-минутный интервал для передачи DCP в AMC. Снимите и установите флажок для перезапуска временного интервала.
Интерфейс контроллера		
Тип интерфейса	UDP TLS	UDP (= User Datagram Protocol), где подключение осуществляется через сеть, а DCP (пароль связи с устройством) для AMC не задан. TLS (= Transport Layer Security): при установке DCP (пароль связи с устройством) для AMC связь с MAC осуществляется через DTLS с усиленной безопасностью. Для UDP и TLS установите DIP-переключатели 1 и 5 на AMC в положение «ВКЛ».
IP-адрес/ имя хоста	Сетевое имя или IP-адрес AMC	Это текстовое поле активно 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 введите IP-адрес.
Номер порта	числовое значение: 10001 (по умолчанию)	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 этот параметр выбран 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	Применяется только в том случае, если функция **Подразделения** лицензирована.

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.

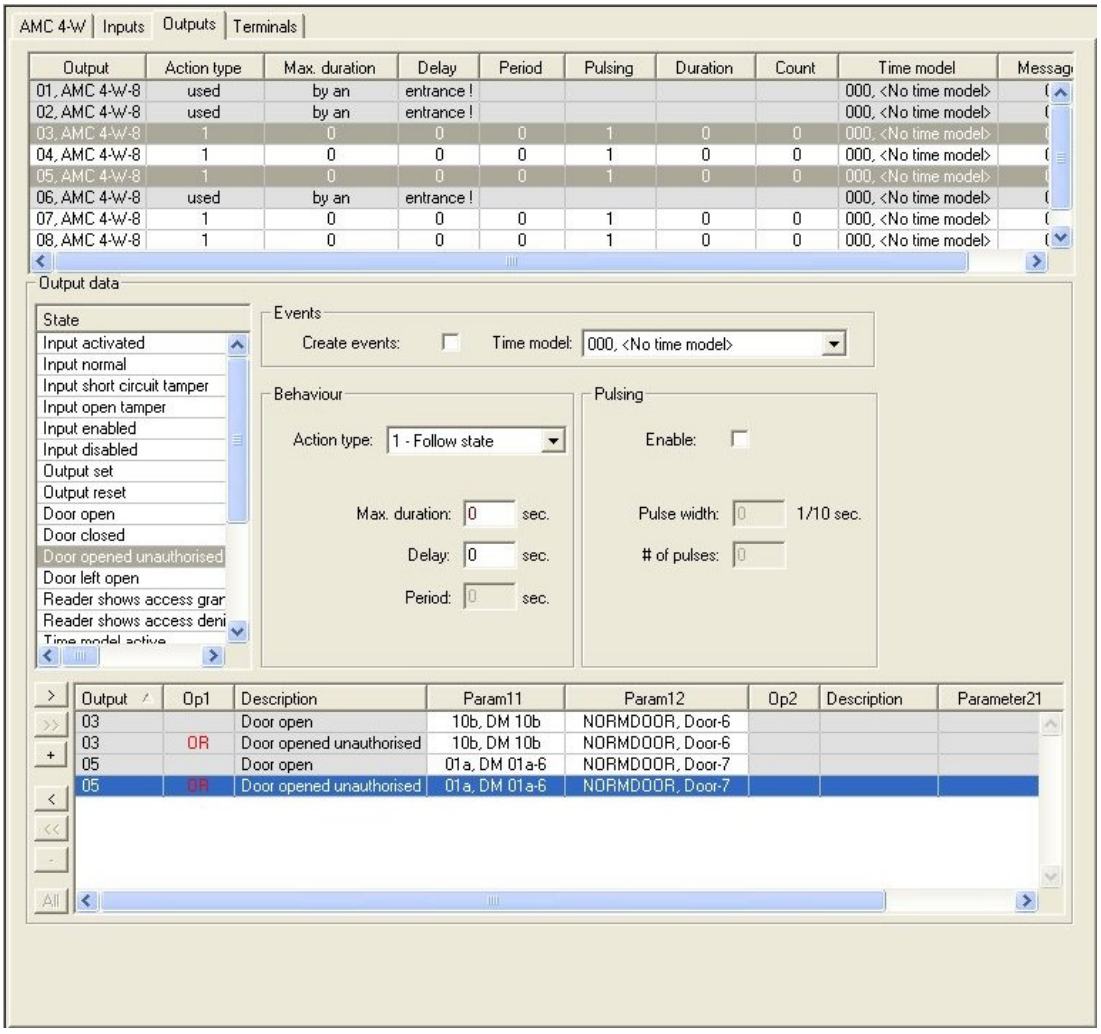
Последовательно	**Диапазон**		**Параллельно**	**Диапазон**

"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

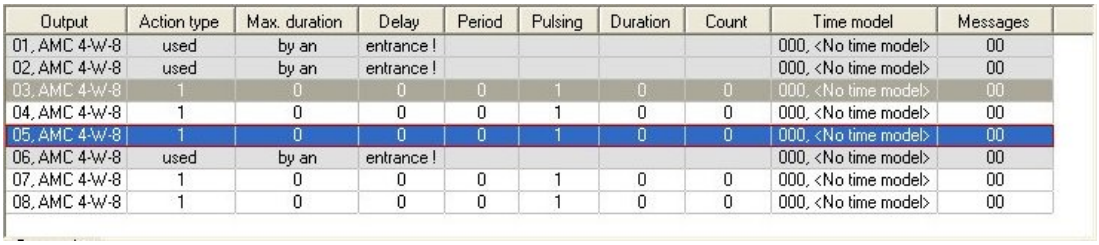
В этом диалоговом окне предоставляется конфигурация каждого выходного сигнала в AMC или AMC-EXT. Предусмотрены три основные области:

– 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.

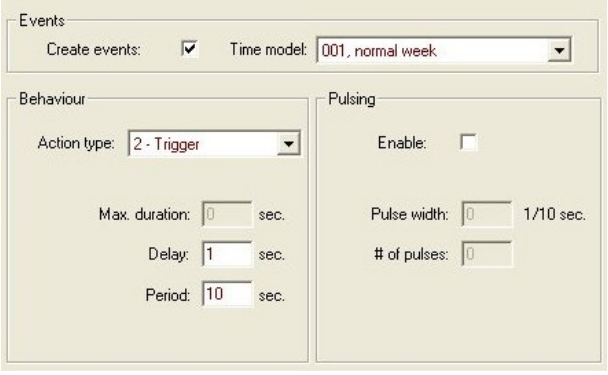
Параметры выходов AMC

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, Действие, 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:

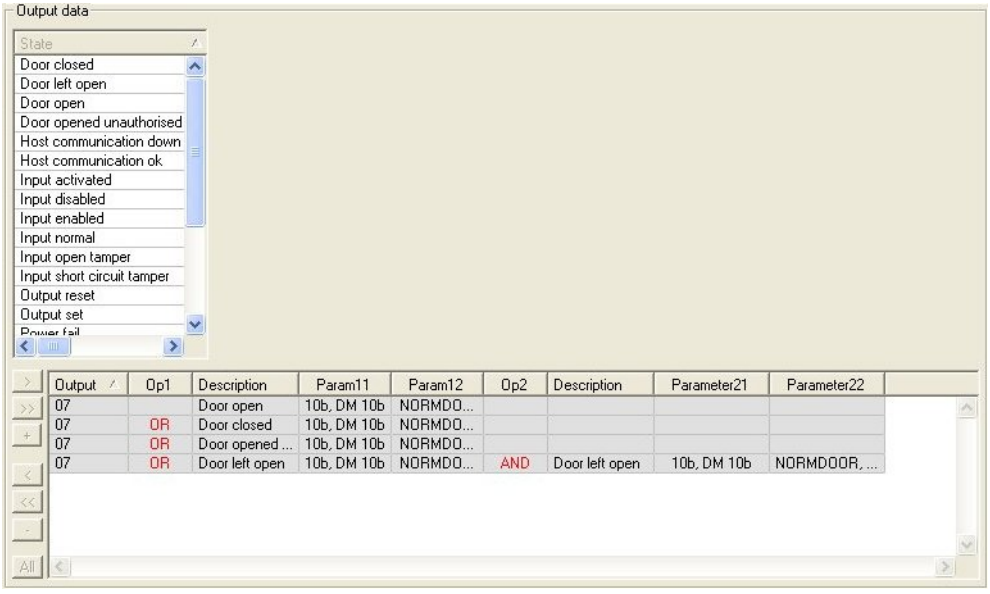
тип действия	макс. продолжительность	задержка	период	пульсация/ включено	длительность импульса	кол-во импульсов
Соответствие состоянию	0 = всегда 1 - 9999	0 - 9999	нет	да	1 - 9999	Нет
Триггер	нет	0 - 9999	0–9999 если пульсация **не** включена	Да отключает период	1 - 9999	1 - 9999
Переменный	нет	нет	нет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



Настройка выходов, которые должны инициироваться определенными состояниями

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

– Выберите один или более 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 состояние), чтобы для каждого выбранного выхода создать вход с этим состоянием для первого устройства (например, AMC, первый вход) и установки (например, первый сигнал, первая дверь).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2

При нажатии » выбранный статус перемещается в список и создается вместе с логическим оператором ИЛИ 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:

– Состояние уже может быть назначено, и к нему добавляется условие путем его выбора в любом столбце.
– Затем при нажатии · выбирается другое состояние 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 условий ИЛИ.
Каждое условие может содержать **одно** условие И.

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

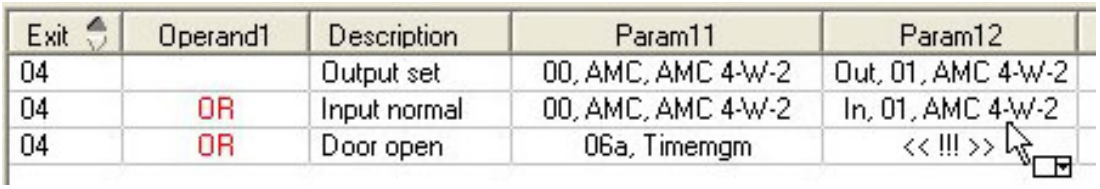
– Выберите назначенную запись в любом столбце.
– Этот статус создается для всех имеющихся устройств и установок при нажатии All.

Изменение параметров выходов

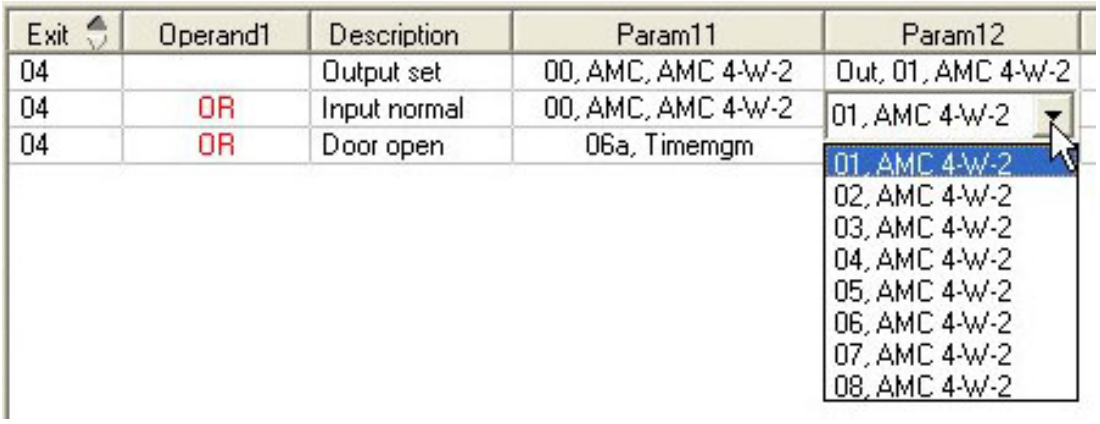
Строки в списке можно изменить

Для нескольких устройств и установок, которым может соответствовать назначенный статус, всегда заданы первые устройства и установки этого типа.

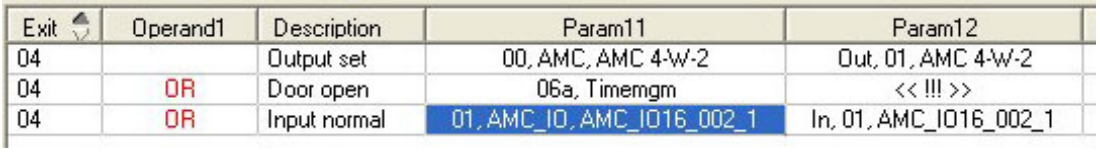
В столбцах **Парам11** и **Парам21** (с ярлыками И) отображаются устройства (например, AMC, проход). В столбцах **Парам12** и **Парам22** содержатся специальные установки (например, входной сигнал, дверь, считыватель).
При наличии нескольких устройств (например, платы ввода-вывода) или установок (например, дополнительные сигналы, считыватели) указатель мыши меняет форму при наведении на такой столбец.



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**:



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.

Состояние	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 отключен	5	Локальный вход деактивирован моделью времени
Вход включен	6	Локальный вход активирован временной моделью
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	---
Сообщение от считывателя	23	Адрес считывателя
Сообщение от LAC	24	Номер платы
Контроль карт	25	Адрес считывателя, функция управления через карту.

Настройка выходов

Кроме назначения сигналов с моделями дверей или с отдельным назначением можно определить условия для выходов, 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 внешнего устройства 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 внешнего устройства:

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

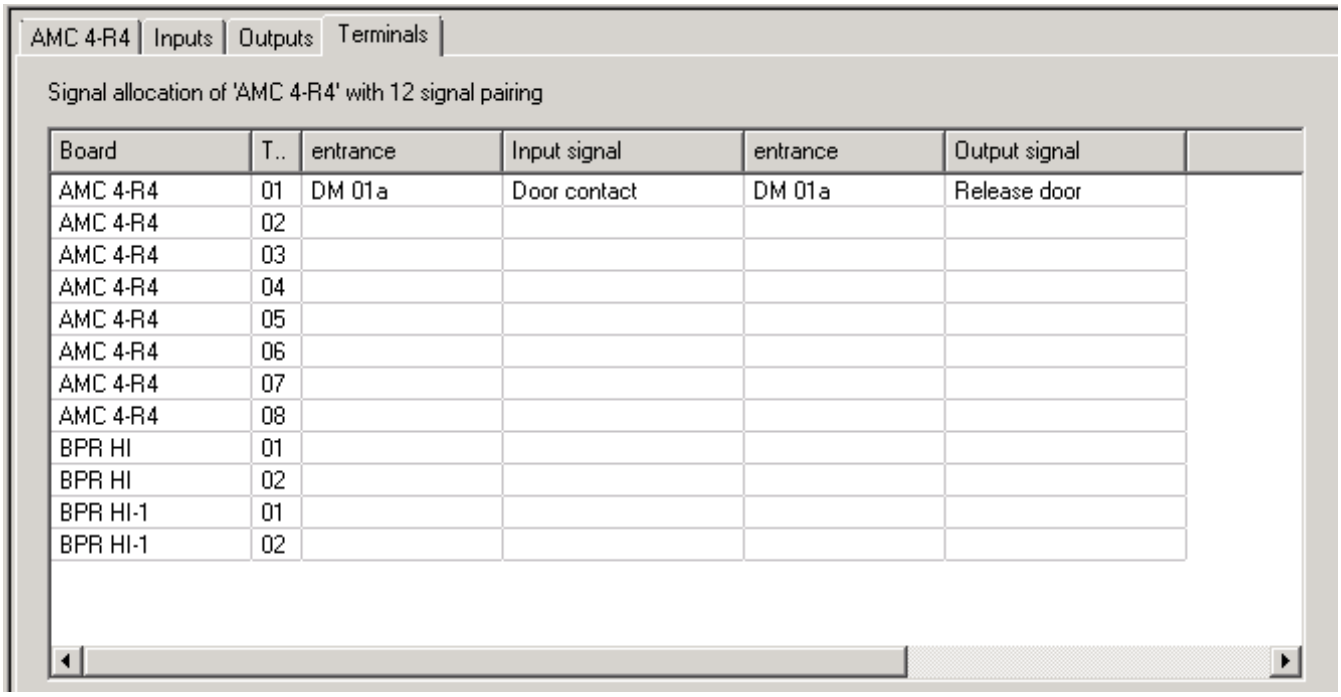
Список всех существующих состояний со значениями по умолчанию для параметров 11/21 и 12/22:

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.



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				

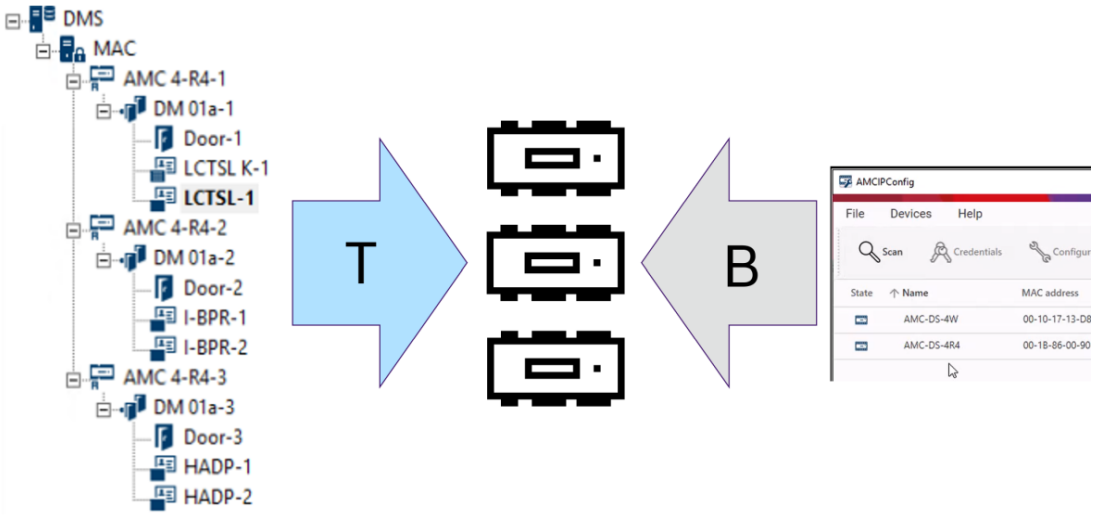
15 Настройка DTLS для безопасной связи

Введение

Система управления доступом (ACS) обеспечивает высокую безопасность связи между устройствами, защищенную DTLS. Существует два основных способа развертывания протокола связи DTLS между устройствами в системе управления доступом:

Развертывание «сверху-вниз» (T) выполняется в редакторе устройств в системе управления доступом.

Развертывание «снизу-вверх» (B) выполняется главным образом в средстве AMCIPConfig, однако для завершения процесса требуется редактор устройств.



- Развертывание «сверху-вниз» (T) можно выполнить двумя альтернативными способами в редакторе устройств:
  - используя один пароль связи с устройством (DCP) на уровне DMS для всех устройств AMC;
  - используя несколько паролей DCP для различных ветвей дерева устройств, начиная с соответствующих контроллеров MAC или AMC.
- Развертывание «снизу-вверх» (B) можно инициировать двумя альтернативными способами в средстве AMCIPConfig:
  - используя аппаратный ключ AMC;
  - используя случайный ключ ЖК-дисплея.

Замечание!

При развертывании «снизу-вверх» по-прежнему требуется настройка пароля DCP в редакторе устройств.

Развертывание «снизу-вверх» позволяет установить пароль DCP на устройстве AMC. Тем не менее, необходимо настроить один и тот же пароль DCP в том же AMC в редакторе устройств, чтобы обеспечить полноценную связь между контроллером MAC и AMC по протоколу DTLS.

Сводка вариантов развертывания DTLS

	Краткое название	Преимущества	Недостатки
Сверху-вниз	Системный администратор в **редакторе устройств** вводит надежный пароль. Из этого пароля система создает **главный ключ**, который она передает сверху вниз по дереву устройств управления доступом, от DMS через контроллеры MAC до контроллеров дверей AMC. Можно установить один пароль для всего дерева устройств или разные пароли для каждой ветви дерева устройств.	Быстрое, простое развертывание.	Во время передачи главного ключа на контроллеры дверей AMC связь устройств не защищается протоколом DTLS.
Снизу-вверх с помощью аппаратного ключа AMC	Системный администратор использует средство **AMCIPConfig**, чтобы выполнить развертывание DTLS на уровне контроллеров дверей AMC.	Улучшенное раздельное обслуживание и гибкость развертывания. Этот метод позволяет избежать основных недостатков развертывания «сверху-вниз», а именно разовое незащищенное подключение главного ключа. Тем не менее, при установке пароля DCP необходимо, чтобы подключение между средством AMCIPConfig и контроллером AMC было защищенным.	Во время установки пароля DCP на контроллере AMC с помощью средства IPConfig необходимо обеспечить защищенное подключение другими способами. Например, подключить AMC непосредственно к компьютеру, на котором запущено средство IPConfig. Заданные в средстве IPConfig пароли DCP также необходимо настроить на том же AMC с помощью редактора устройств.
Снизу-вверх с помощью случайного ключа ЖК-дисплея		Улучшенное раздельное обслуживание и гибкость развертывания.	Более сложное и продолжительное развертывание. Необходимо перенести 27-символьный ключ ЖК-дисплея в

	Краткое название	Преимущества	Недостатки
		Высочайший стандарт безопасности, так как ключ ЖК-дисплея не передается через сеть; а передача учетных данных защищается постоянно.	средство IPConfig с помощью не связанных с сетью средств.
Подробные сведения и инструкции приведены в следующих разделах данной главы.			

Терминология протокола DTLS

DCP (пароль связи с устройством)	Один надежный пароль, из которого система управления доступом (ACS) создает внутренний главный ключ. Пароль необходимо защитить, так как он не сохраняется в ACS.
Главный ключ	Код, созданный системой из пароля DCP и используемый для защиты устройств управления доступом. Главный ключ не отображается пользователям.
Случайный ключ ЖК-дисплея	Временный буквенно-цифровой код, который AMC создает заново при каждой загрузке. Ключ может быть отображен на жидкокристаллических дисплеях (ЖК-дисплеях) AMC и может запрашиваться программными средствами для аутентификации сетевых соединений.
Аппаратный ключ AMC.	Внутренний код проверки подлинности, который AMC создает на основе определенных параметров оборудования. Он не отображается пользователям.

15.1 Развертывание протокола DTLS сверху-вниз

Предварительные требования

- AMS 4.0 или BIS-ACE 4.9.1 (или более поздняя версия).
- Дерево устройств управления доступом от DMS до контроллеров AMC физически настроено и подключено к сети, но контроллеры AMC не включены. «Включено» означает, что флажки контроллеров AMC **Связь с хостом включена** установлены.
- DTLS еще не настроен на AMC одним из методов «снизу-вверх» с помощью средства IPConfig.

Процедура: один пароль DCP для всех

1. Запустите редактор устройств в системе управления доступом.

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

– Отобразится диалоговое окно с приглашением ввести надежный пароль связи с устройством (DCP).
2. Чтобы задать один пароль DCP для всех контроллеров AMC в дереве устройств, введите и подтвердите надежный пароль, соответствующий локальным политикам паролей.
– В зависимости от энтропии пароля в диалоговом окне появляется сообщение о надежности пароля.
3. Запомните пароль, так как он не сохраняется в системе управления доступом.
4. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно.

Альтернативная процедура: несколько паролей DCP для различных ветвей дерева устройств

1. Запустите редактор устройств в системе управления доступом.

– Главное меню AMS > **Конфигурация** > **Данные устройств** > **Дерево устройств** 
– Отобразится диалоговое окно с приглашением ввести надежный пароль связи с устройством (DCP).
2. Нажмите кнопку **Отмена**, чтобы настроить разные DCP в различных ветвях дерева устройств (контроллеров Mac и AMC).
– Во всплывающем диалоговом окне отображается количество контроллеров AMC, не имеющих паролей DCP, в системе.
– Дерево устройств можно открыть в редакторе устройств.
3. Разверните дерево устройств и выберите контроллер MAC или AMC, для которого требуется задать пароль DCP.
– При установке пароля DCP на уровне контроллера MAC он задается для всех подчиненных контроллеров AMC контроллера MAC.
– При установке пароля DCP на уровне контроллера AMC он задается только для указанного контроллера.
4. Нажмите кнопку с многоточием рядом с текстовым полем **Пароль связи с устройством:**
5. Введите и подтвердите надежный пароль, соответствующий локальным политикам паролей.
6. Запишите пароль и ветвь, к которым он применяется, поскольку он не сохраняется в ACS.
7. Повторите эту процедуру для каждого контроллера MAC или AMC, для которого необходимо установить отдельный пароль DCP.
8. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно.

Результат развертывания «сверху-вниз»

Система управления доступом использует один или несколько паролей DCP, чтобы создавать внутренние ключи для всех контроллеров AMC в выбранной DMS или MAC. Эту процедуру необходимо повторять, только если впоследствии меняется пароль DCP на одном или нескольких контроллерах AMC с помощью средства AMCIPConfig (см. развертывание «снизу-вверх»). В этом случае следует немедленно установить тот же самый пароль DCP сверху-вниз в том же в редакторе устройств AMC.
Если впоследствии устройства будут добавляться в дерево устройств, а именно в подчиненные DMS и MAC, для которых уже установлены пароли DCP, новые устройства будут автоматически наследовать установленный пароль DCP от вышестоящих устройств.

16 Настройка входов

16.1 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 **OK** 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.

16.2 Создание проходов

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

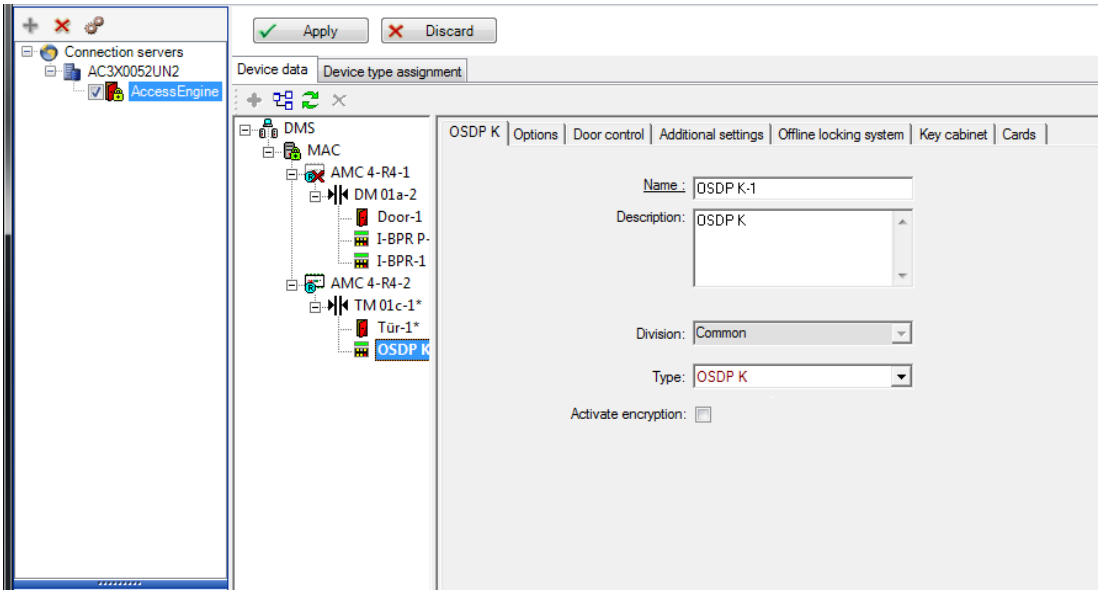
– Для типов **AMC 4W** доступны только считыватели Wiegand с клавиатурой и без.
– Для типа **AMC 4R4** доступны считыватели из следующей таблицы. Не используйте протоколы разных типов на одном контроллере.

Имя считывателя	Протокол Wiegand	Протокол BPR(*)	Протокол I-BPR	Протокол HADP	Протокол OSDP
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			
TB15 HI1		X			
TB30 LE		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	
R15				X	
R30				X	
R40				X	
RK40				X	
RKL55				X	

(*) Протокол BPR устарел и указан здесь только для совместимости.

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



Защищенное подключение через OSDP

По умолчанию флажок **Включить шифрование** снят. Установите его, если используете считыватели с поддержкой **OSDPv2 secure**.

Если впоследствии вы отключите шифрование, сняв флажок, выполните сброс считывателя в соответствии с инструкциями производителя.

В качестве дополнительной меры безопасности при любой попытке заменить настроенный считыватель OSDP другим считывателем OSDP в системе управления доступом генерируется тревога. Оператор может подтвердить тревогу в клиенте и одновременно предоставить разрешение на замену.

Сообщение тревоги: **Отказано в замене OSDP считывателя**

Команда: **Разрешить замену OSDP считывателя**

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

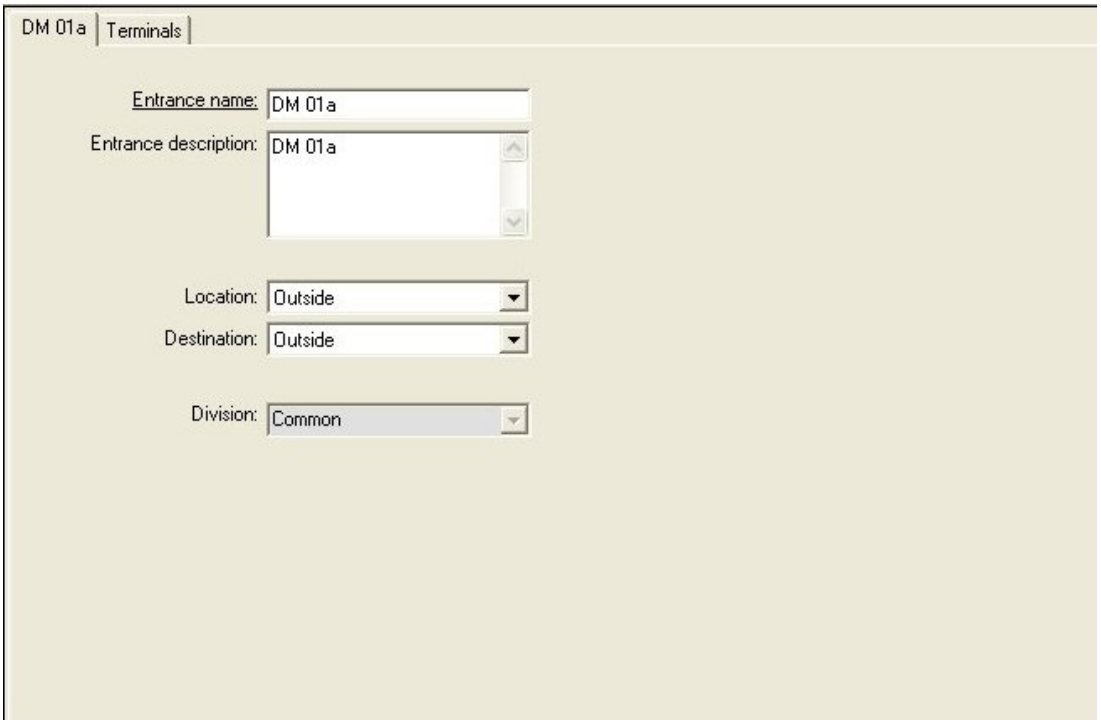
Не используйте различные линейки продуктов одновременно (например **LECTUS duo** и **LECTUS secure**) на одной шине OSDP.

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.

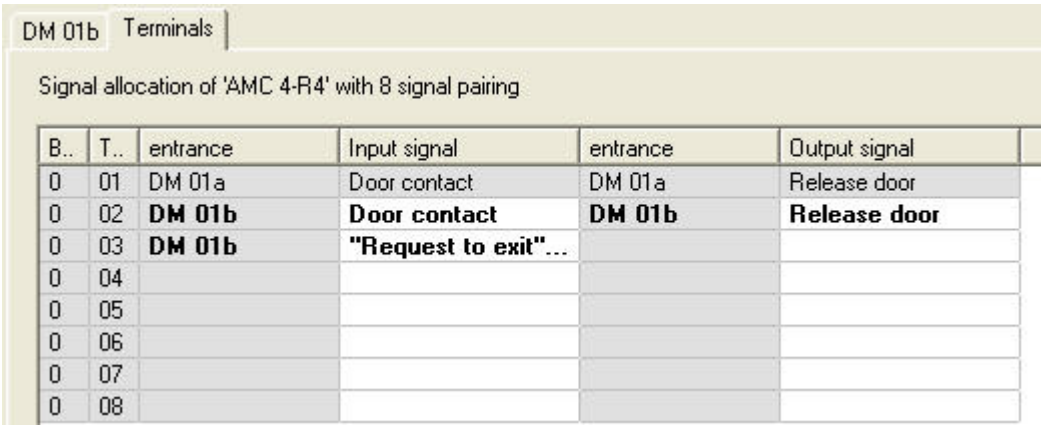
Если вы деактивировали шифрование, сняв флажок на вкладке OSDP считывателя в редакторе устройств, выполните сброс считывателя в соответствии с инструкциями производителя.



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, в течение которого контроллер доступа ожидает решения от внешней системы или устройства, подключенного к одному из входов.
Подразделение	Подразделение, к которому относится считыватель. Значение по умолчанию — **Общее**	Применяется только в том случае, если функция **Подразделения** лицензирована.
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.

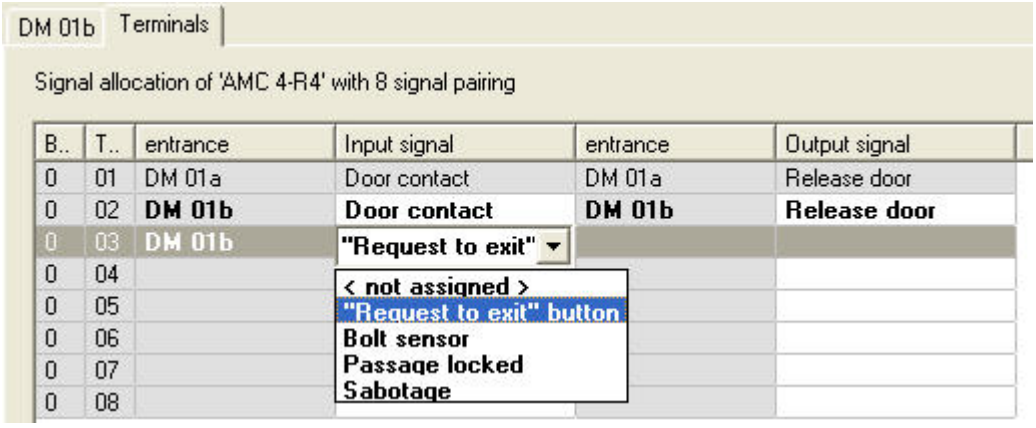
16.3 Настройка терминалов AMC

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



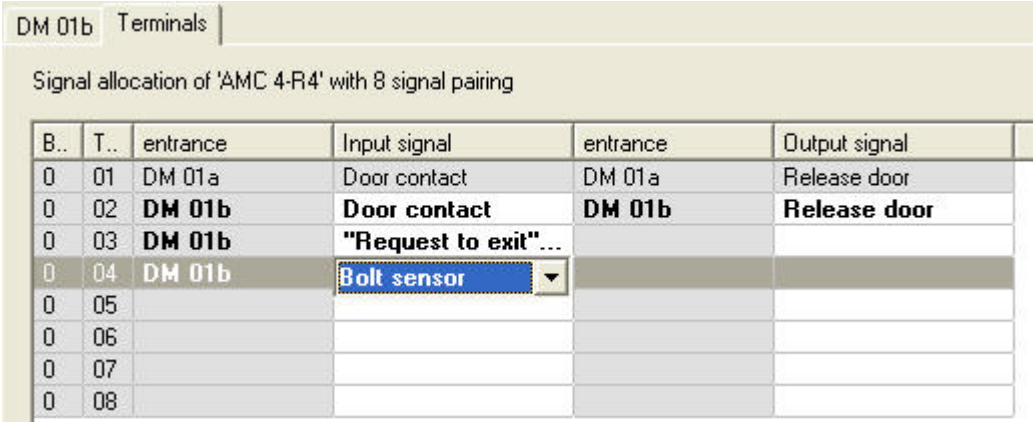
B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	**DM 01b**	**Door contact**	**DM 01b**	**Release door**
0	03	**DM 01b**	**"Request to exit"...**		
0	04				
0	05				
0	06				
0	07				
0	08				

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.



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				

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



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	**DM 01b**	**Bolt sensor**		
0	05				
0	06				
0	07				
0	08				

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.

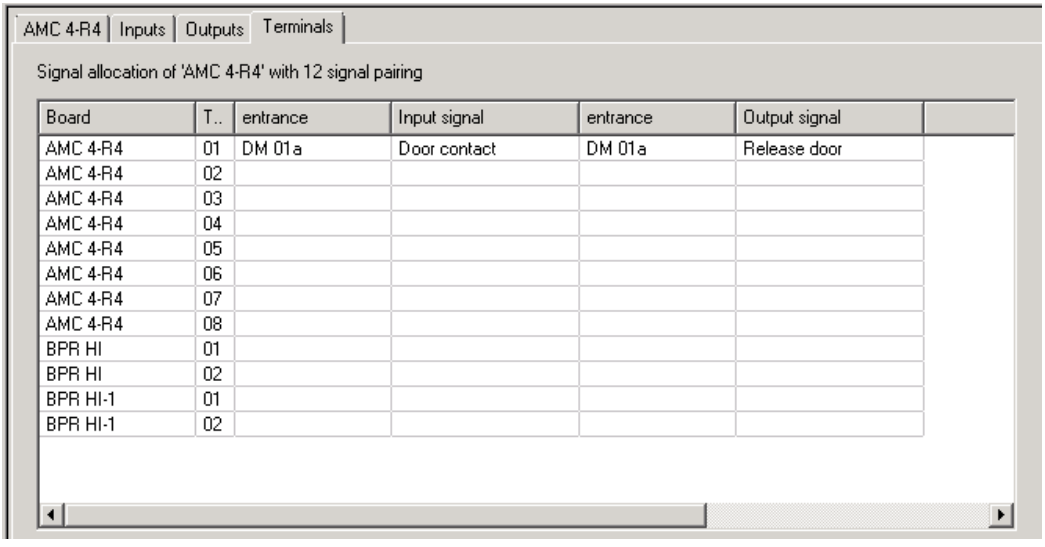
Замечание!
Поля со списками зависят от контекста не на 100 %, поэтому можно выбрать сигналы, которые в реальной жизни не сработают. При добавлении или удалении сигналов на вкладке **Терминалы** протестируйте их, чтобы убедиться в их логической и физической совместимости с проходом.

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
-



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				

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
Дверной контакт	
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 длительной блокировки.
Датчик вскрытия корпуса	Сигнал тампера 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.

Подавление тревоги при неавторизованном открытии	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 отклоняет доступ

Таблица выходных сигналов

Выходные сигналы	**Описание**
Разблокировать дверь	
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 сигнал	Индикатор контролируется, пока дверь открыта.
Максимальное время ожидания открытия двери истекло или нарушена безопасность двери	Если дверь удерживается открытом состоянии или остается открытой слишком долго
Подключение камеры	Камера активируется в начале перехода.
Разблокировать турникет на вход	
Разблокировать турникет на выход	
Дверь разблокирована	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 Доступно решение о доступе внешней системой	- Дверной контакт - Кнопка запроса на выход - Ригельный датчик - Проход заблокирован - Датчик вскрытия корпуса - Локальное открытие разрешено - Принято решение о доступе внешней системой - Решение о доступе отклонено внешней системой	- Разблокировать дверь - Шлюзовые ворота: запереть противоположное направление - Подавление тревоги - Зеленый сигнал - Подключение камеры - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери - 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 - Датчик вскрытия корпуса - Принято решение о доступе внешней системой - Решение о доступе отклонено внешней системой	- Шлюзовые ворота: запереть противоположное направление - Разблокировать турникет на вход - Разблокировать турникет на выход - Подавление тревоги - Подключение камеры - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери - 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	- Дверной контакт - Кнопка запроса на выход - Проход заблокирован - Проход завершен - Принято решение о доступе внешней системой - Решение о доступе отклонено внешней системой	- Разблокировать дверь - Подавление тревоги - Зеленый сигнал - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери - Дверь разблокирована - 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	- Дверной контакт - Кнопка запроса на выход - Проход заблокирован - Проход завершен - Принято решение о доступе внешней системой - Решение о доступе отклонено внешней системой	- Разблокировать дверь - Подавление тревоги - Зеленый сигнал - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери - Дверь разблокирована - 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	- Дверной контакт - Кнопка запроса на выход - IDS: готова к постановке на охрану - IDS: поставлена на охрану - Датчик вскрытия корпуса - IDS: запрос постановки на охрану - Принято решение о доступе внешней системой - Решение о доступе отклонено внешней системой	- Разблокировать дверь - Подключение камеры - IDS: постановка на охрану - IDS: снятие с охраны - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери - 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	- Дверной контакт - Кнопка запроса на выход - IDS: готова к постановке на охрану - IDS: поставлена на охрану - Датчик вскрытия корпуса - IDS: запрос постановки на охрану	- Разблокировать дверь - Подключение камеры - IDS: постановка на охрану - Максимальное время ожидания открытия двери истекло или нарушена безопасность двери
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.

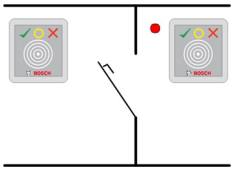
Такие локальные для считывателей сигналы не могут быть назначены функциям и параметризованы как сигналы контроллеров и плат. Они также не появляются на вкладках **Входной сигнал** и **Выходной сигнал**. Их также нельзя использовать для лифтов (например, чтобы преодолеть ограничение в 56 этажей). Поэтому 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.

16.4 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

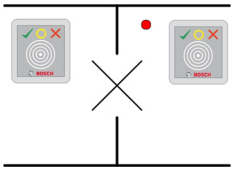
Возможные сигналы:

Входные сигналы	Выходные сигналы
Дверной контакт	Разблокировать дверь
Кнопка запроса на выход	Шлюзовые ворота: запереть противоположное направление
Датчик вскрытия корпуса	Зеленый сигнал
Подавление тревоги при неавторизованном открытии	Подключение камеры
	Максимальное время ожидания открытия двери истекло или нарушена безопасность двери

Замечание!
Для функций 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

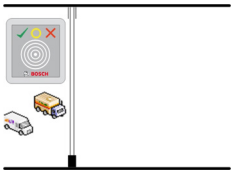
Возможные сигналы:

Входной сигнал	Выходные сигналы
Турникет в нормальном положении	Разблокировать турникет на вход
Кнопка запроса на выход	Разблокировать турникет на выход
Датчик вскрытия корпуса	Проход заблокирован

Подавление тревоги при неавторизованном открытии	Подключение камеры
	Максимальное время ожидания открытия двери истекло или нарушена безопасность двери
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**
Дверной контакт	Разблокировать дверь
Кнопка запроса на выход	Дверь разблокирована
Проход заблокирован	Зеленый сигнал
Проход завершен	Подавление тревоги
	Максимальное время ожидания открытия двери истекло или нарушена безопасность двери

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 или барьерами, а лишь пересылают данные карты в систему учета рабочего времени. Такие считыватели обычно установлены в местах с уже контролируемым доступом.
Поэтому сигналы не определены.

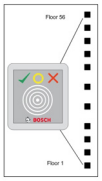
Замечание!
Чтобы в системе учета времени и присутствия можно было создать допустимую пару регистрации (время входа плюс время выхода), необходимо задать параметры для двух отдельных считывателей с моделью дверей 06: один для регистрации времени входа, другой для регистрации времени выхода.

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. На вкладке **Учет времени** в диалоговых окнах **Авторизации доступа** и **Авторизации области/времени** перечисляются все считыватели учета рабочего времени, 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 <SW_installation_folder>\AccessEngine\AC\TAExchange\ под именем TAccExc_EXP.txt в ожидании экспорта в систему учета рабочего времени. 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 содержит все проходы в хронологическом порядке. В этом файле в качестве разделителя полей используется точка с запятой.

Варианты входной модели 07



Варианты моделей:

07a	Лифт макс. на 56 этажей
07c	Лифт до 56 этажей с временной моделью

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.

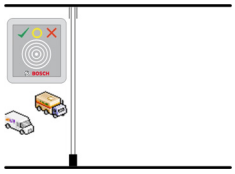
Модель прохода 07c
Сигналы:

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

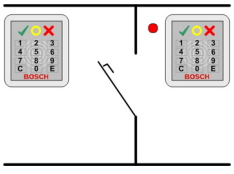


Возможные сигналы:

Входные сигналы	**Выходные сигналы**
Дверной контакт	Разблокировать дверь
Кнопка запроса на выход	Дверь открыта долгосрочно
Проход заблокирован	Горит зеленый светофор
Проход завершен	Подавление тревоги
	Максимальное время ожидания открытия двери истекло или нарушена безопасность двери

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**
Дверной контакт	Разблокировать дверь
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	Подключение камеры
Ригельный датчик	Максимальное время ожидания открытия двери истекло или нарушена безопасность двери
Датчик вскрытия корпуса	
Подавление тревоги при неавторизованном открытии	
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 с последовательным интерфейсом (включая I-BPR, HADP и OSDP)
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 (#).

Считыватели Wiegand (включая последовательный протокол BPR)
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.]

Специальные проходы

Для моделей прохода с особыми функциями, такими как:

- Лифты
- Обнаружение вторжения
- Универсальные цифровые или бинарные переключатели
- Шлюзы

дополнительную информацию см. в разделе «Специальные проходы».

См.

- *Специальные проходы, Страница 99*

16.5 Специальные проходы

16.5.1 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

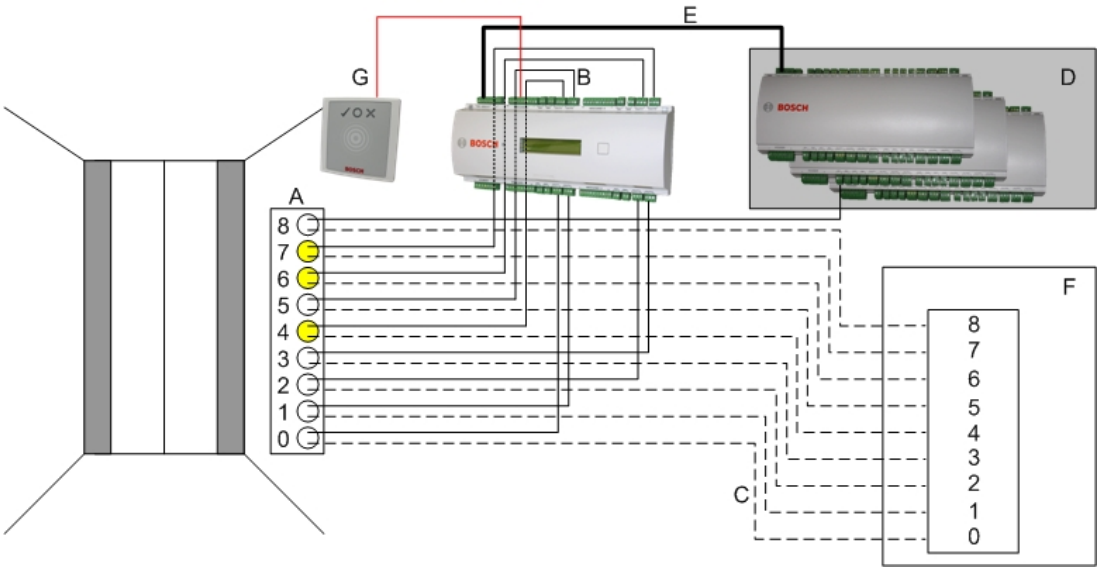
Диалоговые окна авторизации доступа системы позволяют назначать конкретные этажи определенному лицу.

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.

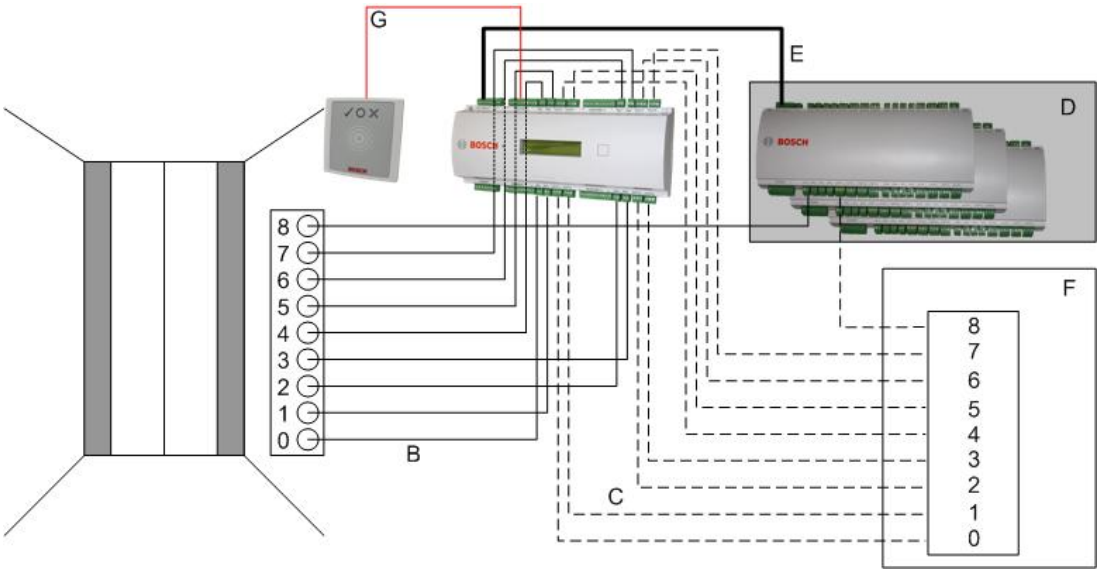
На рисунке ниже показана схема соединения лифта в рамках модели дверей 07a.



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.

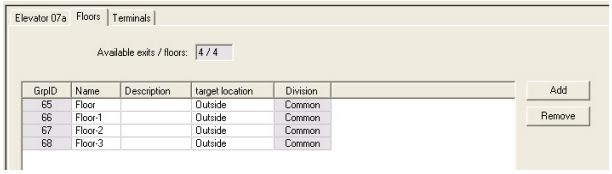


Условные обозначения:

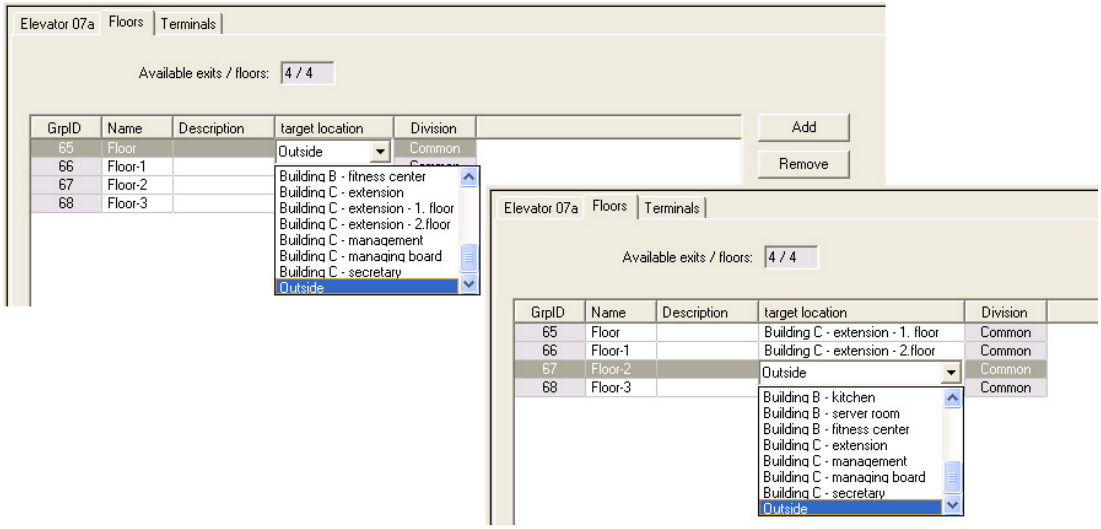
- B = (сплошная линия) выходные сигналы AMC
- C = (прерывистая линия) Подключение к элементам управления лифтом
- D = к AMC можно подключить до трех плат входа/выхода, если его собственных восьми входов и выходов недостаточно.
- E = передача данных и питания от AMC к платам входа/выхода
- A = выбор этажа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

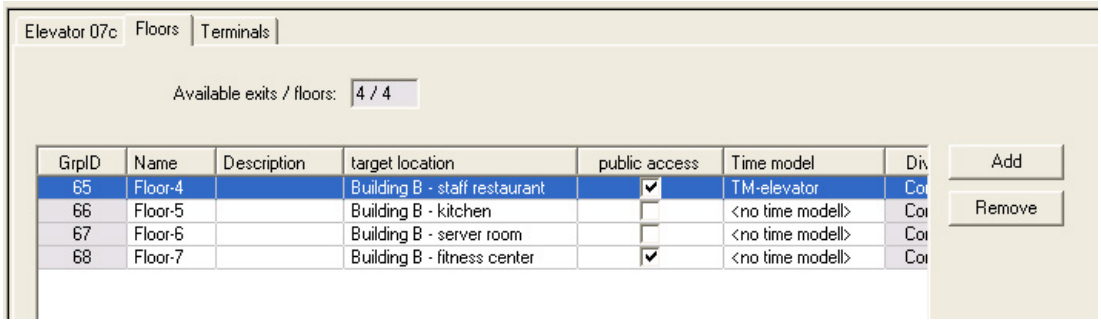
Этажи для модели прохода 07
Используйте вкладку **Этажи** для добавления и удаления этажей для лифта (с помощью кнопок **Добавить** и **Удалить**).



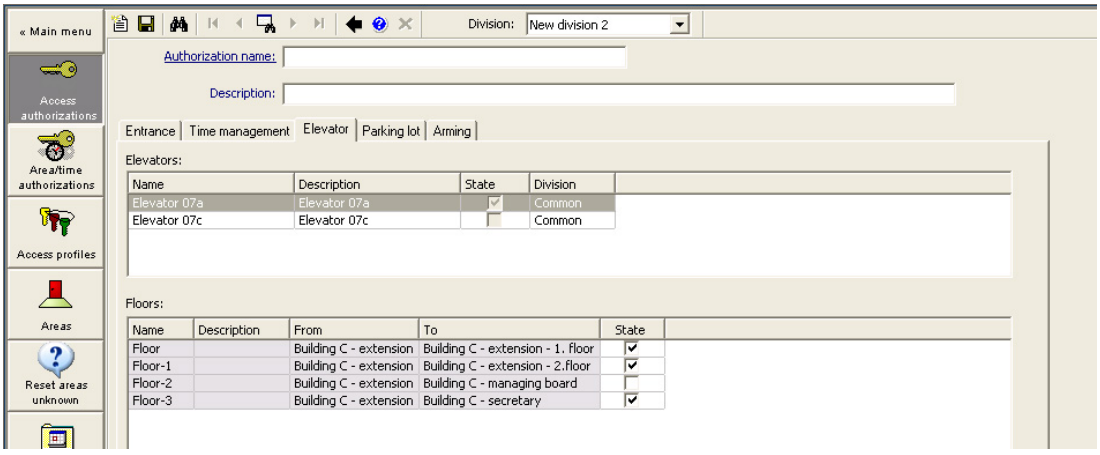
Целевыми местоположениями для этажа могут быть любые **Области**, кроме автостоянок и зон парковки.
Определенному этажу можно назначить только одну область. Поэтому выбор областей, предлагаемых в полях со списками, сокращается после каждого назначения, предотвращая непреднамеренные двойные назначения.



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 **Авторизации доступа** и **Авторизации области/времени** сначала выберите требуемый лифт, а затем (ниже) этажи, к которым держателю карты разрешен доступ.



16.5.2 Модели дверей с тревожными сигнализациями (DM14)

Введение

В отличие от модели прохода 10 (DM10), модель **DM14** допускает постановку системы охранной сигнализации (или системы IDS) на охрану и снятие ее с охраны для определенной области постановки на охрану. Проход DM14 также можно настроить так, чтобы держателю карты, снимающему систему с охраны на этом проходе, предоставлялся доступ при условии, что у держателя карты есть все остальные требуемые разрешения на доступ.

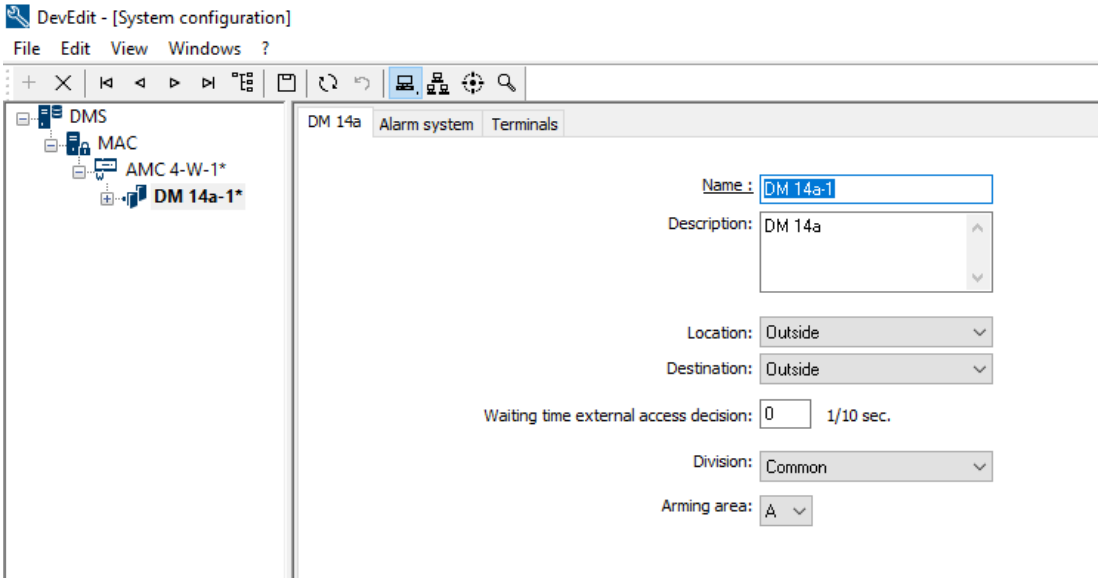
Процедура настройки для DM14 в редакторе устройств и диспетчере диалоговых окон включает следующие задачи:

1. Настройте общие параметры для идентификации прохода и его области постановки на охрану.
2. Настройте конкретные параметры, чтобы точно настроить процедуру снятия области с охраны.
3. Определите входные и выходные сигналы системы IDS в терминалах прохода дверного контроллера.
4. Включите разрешения на постановку на охрану/снятие с охраны в полномочия доступа тех владельцев карт, которые будут управлять проходами DM 14.

Выполнение этих задач описывается в следующих разделах.

Общие параметры

На первой вкладке, **DM14a** или **DM14b**, задайте следующие параметры.

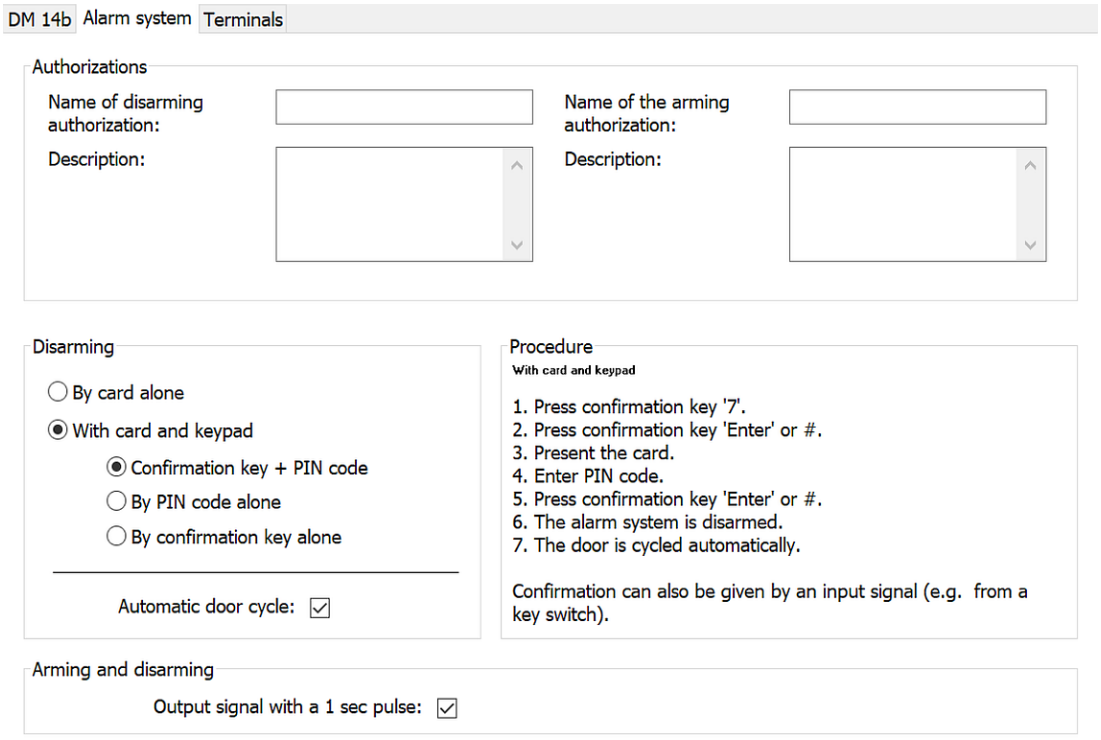


Параметр	Тип значения	Описание
Имя	Произвольный текст	Имя прохода.
Описание	Произвольный необязательный текст	Описание прохода.
Местоположение	Список определенных областей, если они используются	Область доступа, в которой расположен проход.
Место назначения	Список определенных областей, если они используются	Область доступа, в которую ведет проход.

Параметр	Тип значения	Описание
Подразделение	Список определенных подразделений, если они используются	Подразделение или арендатор в системе управления доступом, к которому относится данный проход.
Время ожидания решения о доступе от внешней системы	Десятые доли секунды	Если вы подключили внешнюю систему к клеммам AMC, чтобы решения о доступе принимались этой системой, этот параметр ограничивает время ожидания ответа от внешней системы. Примечание. Решение о доступе требует выполнения **всех** условий, определенных в системе управления доступом, например полномочий доступа, временных моделей и подразделений (если они используются). По умолчанию установлено значение 0, т. е. этот параметр игнорируется.
Область постановки на охрану	Список прописных букв от A до Z	Буква, по которой проходы DM14 группируются в области постановки на охрану.

Параметры системы сигнализации

На второй вкладке **Система сигнализации** установите перечисленные ниже параметры. Эти параметры определяют учетные данные и процедуру для снятия IDS с охраны, а снятие с охраны влияет на все проходы в пределах одной области постановки на охрану, как определено на первой вкладке.



Параметр	Тип значения	Описание
Область «Полномочия»		
Имя полномочий на снятие с охраны	Произвольный текст	Имя, которое отображается в протоколах и отчетах, когда держатель карты снимает IDS с охраны на этом проходе.
Имя полномочий на постановку на охрану	Произвольный текст	Имя, которое отображается в протоколах и отчетах, когда держатель карты ставит IDS на охрану на этом проходе.
Описание (одно для каждых полномочий)	Произвольный необязательный текст	Описание полномочий на постановку на охрану.
Область «Снятие с охраны»		
Только карта	Переключатель	Выберите этот вариант, если нужно разрешить снятие IDS с охраны с помощью лишь карты и считывателя без дополнительной аутентификации.
Карта и клавиатура	Переключатель	Выберите этот вариант, если нужно, чтобы для снятия IDS с охраны нужно было предъявить карту считывателю и пройти дополнительную аутентификацию с помощью клавиатуры считывателя.

Параметр	Тип значения	Описание
		Процедура аутентификации и снятия с охраны уточняется следующими дополнительными параметрами:
Ключ подтверждения + PIN-код	Переключатель	Держатели карт должны использовать для аутентификации свою карту, ключ подтверждения и PIN-код.
Только PIN-код	Переключатель	Держатели карт должны использовать для аутентификации свою карту и PIN-код.
Только ключ подтверждения	Переключатель	Держатели карт должны использовать для аутентификации свою карту и ключ подтверждения.
Автоматический цикл двери	Флажок	Установите этот флажок, если после снятия с охраны должен быть выполнен цикл управления замком двери, чтобы держатель карты мог войти одновременно со снятием с охраны. **Примечание.** Цикл управления замком будет выполнен, только если у держателя карты также есть разрешение на доступ через эту дверь.
Область «Процедура»		
В зависимости от параметров, заданных в области **Снятие с охраны**, в этой области отображается стандартная процедура для снятия IDS с охраны. Сообщите эту процедуру владельцам карт, которые будут использовать проходы DM14 в этой области постановки на охрану.		
Область «Постановка на охрану и снятие с охраны»		
Выходной сигнал с импульсом 1 с	Флажок	Установите этот флажок, если вы используете охранную панель **B-Series или G-Series** компании Bosch. В этом случае на выход будет подаваться не постоянный уровень «1» (поставить на охрану) или «0» (снять с охраны), а одиночный импульс для переключения состояния постановки на охрану охраняемой области, относящейся к проходу.

Клеммы дверного контроллера

Чтобы для прохода DM14 можно было выполнять постановку на охрану и снятие с охраны, необходимо определить используемые входные и выходные сигналы IDS для соответствующих клемм дверного контроллера прохода.

Это действие требуется выполнить один раз для каждого контроллера с проходами DM14. Все остальные проходы DM14, которые вы после этого определите на этом же контроллере и его платах расширения, будут наследовать сигналы этого общего контроллера.

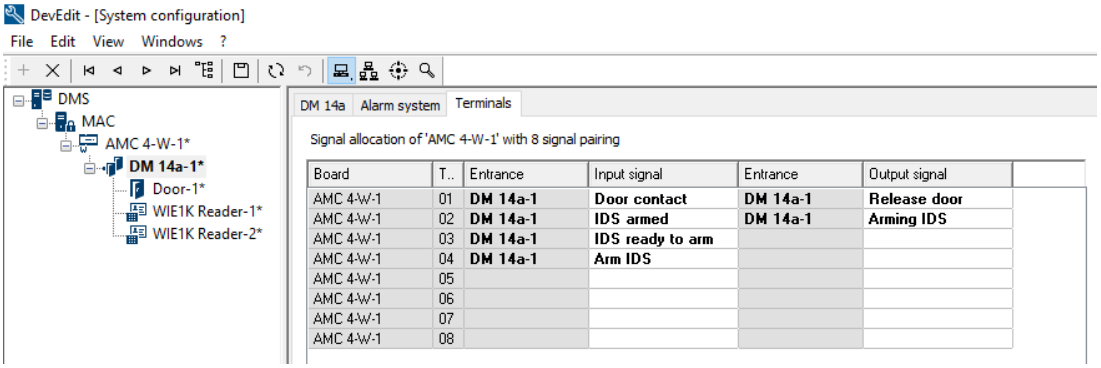
Сигналы по умолчанию описаны в следующей таблице.

Сигнал	Вход / выход	Описание
IDS поставлена на охрану	Вход	IDS поставлена на охрану для данной охраняемой области.
IDS готова к постановке на охрану	Вход	Ни одна точка IDS не находится в состоянии неисправности (разомкнута или не готова).
Поставить IDS на охрану	Вход	Запрос постановки IDS на охрану.
Кнопка запроса на выход (REX)	Вход	
Ригельный датчик	Вход	Датчик, контролирующий засов двери.
Датчик вскрытия корпуса	Вход	Обнаружено вскрытие корпуса.
Подавление тревоги при неавторизованном открытии	Вход	Подавление тревоги на указанное дополнительное количество секунд, если сигнал REX подан детектором движения. Подробнее см. в разделе о функции шунтирования REX.
Разблокировать дверь	Выход	Разблокировать и снова заблокировать механизм двери, чтобы разрешить доступ.
Постановка IDS на охрану	Выход	Поставить на охрану или снять с охраны IDS в зависимости от ее текущего состояния (переключение).
Подключение камеры	Выход	Активирование камеры, соединенной с проходом.
Истекло макс. время открытия двери или **Нарушена безопасность двери**	Выход	Дверь удерживается открытой или система предполагает, что произошло нарушение безопасности двери.

Процедура назначения сигналов клеммам

1. Откройте 3-ю вкладку **Терминалы**.

– В таблице отображаются терминалы дверного контроллера данного прохода, а также любых плат расширения этого контролера.



2. Выберите строку, соответствующую терминалу, которую вы хотите использовать для входного сигнала.
3. В соответствующей ячейке столбца **Входной сигнал** выберите требуемый сигнал из раскрывающегося списка. Обратите внимание, что в списке отображаются только еще не назначенные сигналы.
4. Повторите предыдущие шаги, чтобы добавить любые другие входные сигналы, необходимые для данного прохода.
5. Повторите эту процедуру столько раз, сколько нужно, чтобы добавить любые требуемые выходные сигналы в столбец **Выходной сигнал**.

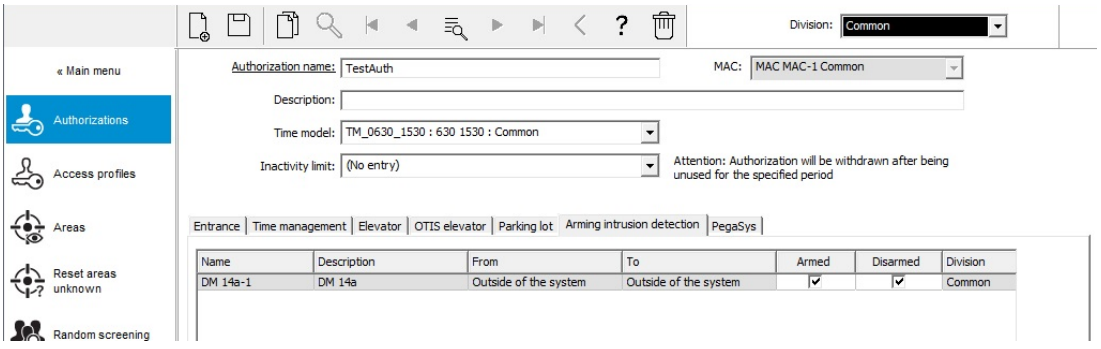
Определение полномочий для постановки на охрану и снятия с охраны проходов DM14

После создания прохода DM14 в редакторе устройств этот проход становится доступен для включения в полномочия доступа.

1. В диспетчере диалоговых окон перейдите к:

– Главное меню > **Системные данные** > **Полномочия** > вкладка: **Постановка на охрану извещателей вторжения**

2. Загрузите существующие полномочия доступа в диалоговое окно или нажмите значок (Создать), чтобы создать новые.
3. Найдите требуемый проход DM14 в списке и установите флажки **Поставлен на охрану** и (или) **Снят с охраны**.

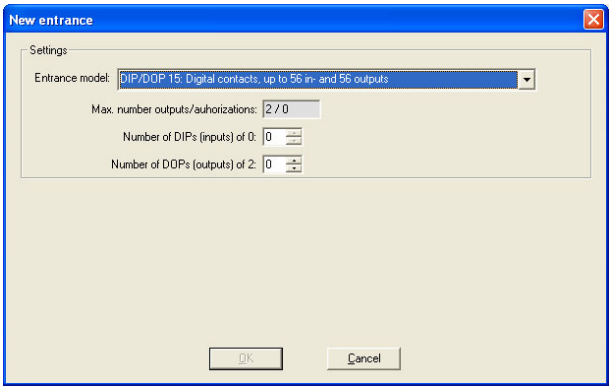


4. Нажмите значок (Сохранить), чтобы сохранить полномочия доступа с выбранными разрешениями.
5. Назначьте эти полномочия доступа держателям карт, которые должны управлять проходами DM 14.

16.5.3 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 в редакторе устройств.

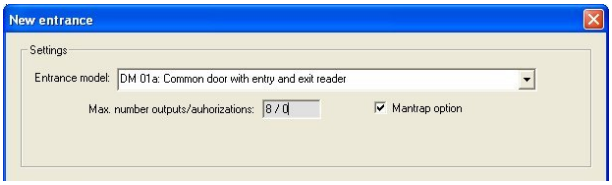
Восстановление модулей DOP после перезапуска

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.

16.5.4 Модели дверей-ловушек

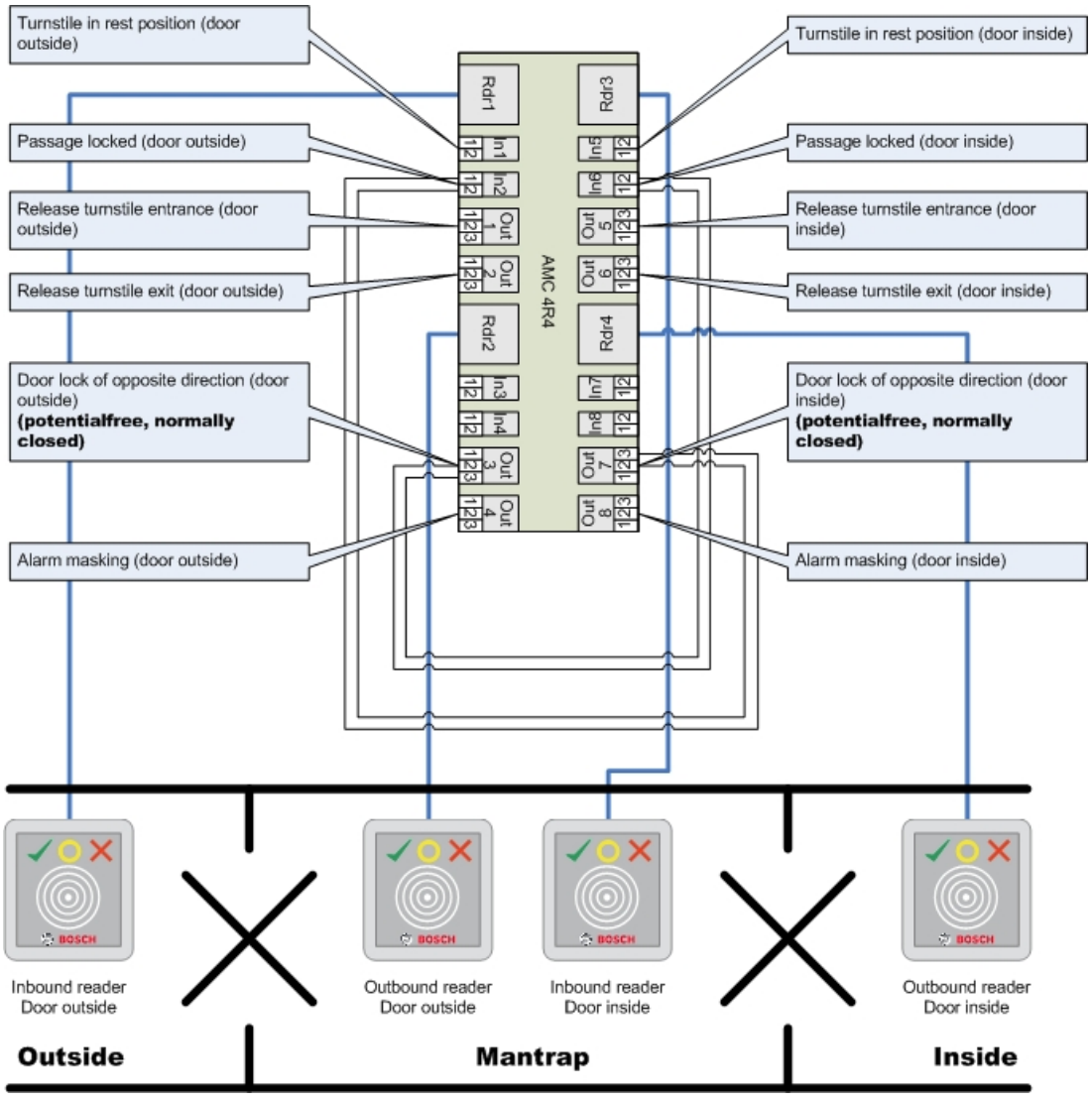
Создание ловушки

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.

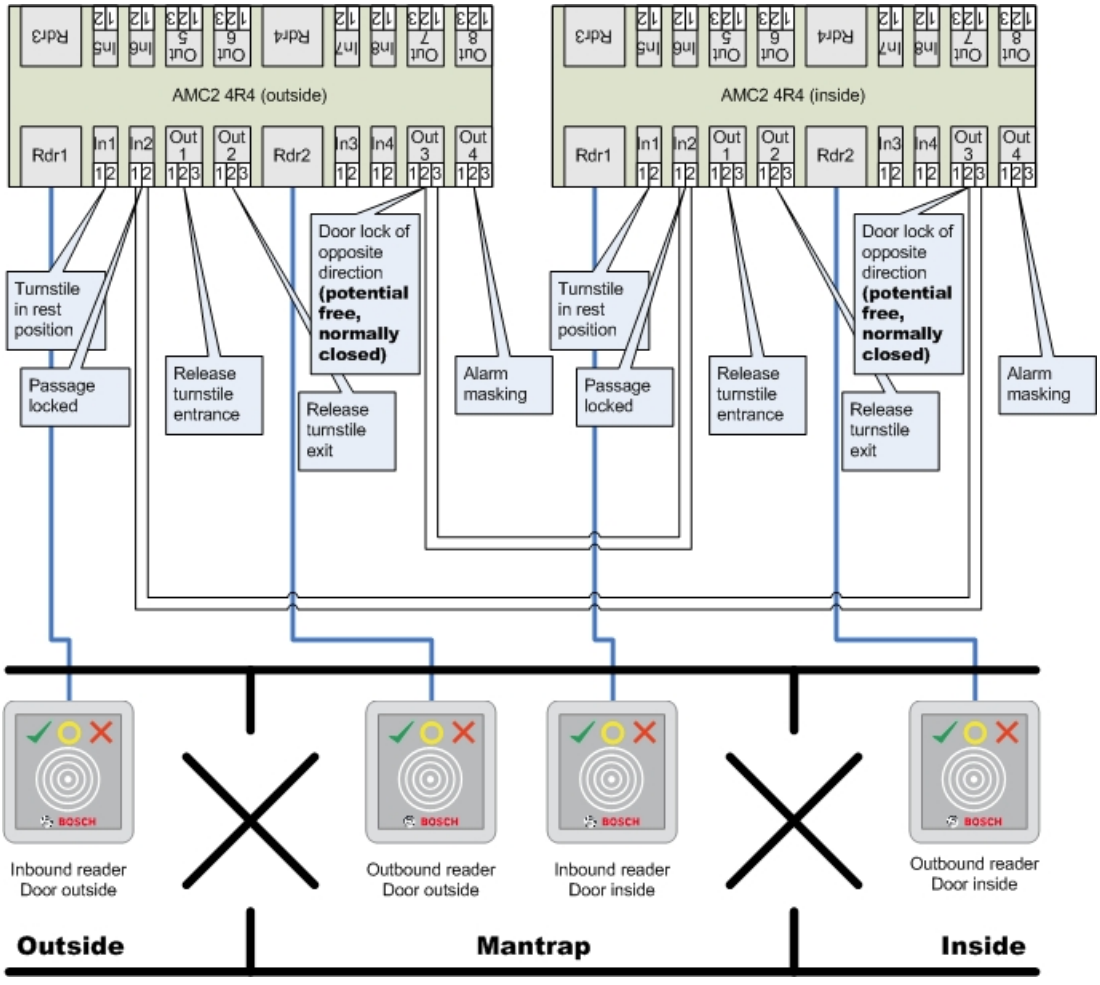
Пример: ловушка на одном контроллере
Турникеты — наиболее распространенные средства разделить доступ владельцев карт. В следующих примерах используется модель дверей 3a (турникет со считывателем на входе и выходе).
Конфигурация ловушки с двумя турникетами (DM 03a):



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.

16.6 Двери:

Вкладка: дверь

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»	Применяется только в том случае, если функция **Подразделения** лицензирована.
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.

Вкладка: параметры

Параметр	**Возможные значения**	**Замечания**
Создать сообщение для открытия/закрытия	0 = флажок снят 1 = флажок установлен.	0 = когда дверь открывается (отворяется от дверной рамы на определенный угол) или закрывается (полностью фиксируется в дверной раме), сообщения не создаются. 1 = в журнале событий создаются соответствующие сообщения.
Дверь установлена в ручной режим	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 управления доступом. 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.
Режим двери	0 = Дверь в нормальном режиме 1 = Дверь открыта 2 = Дверь разблокирована 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.

	3 = Дверь открывается в зависимости от модели времени после первого прохода 5 = Дверь постоянно заблокирована 6 = Дверь заблокирована в зависимости от модели времени	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 = заблокирована (исключена из системы управления доступом) до тех пор, пока не будет разблокирована вручную. 6 = заблокирована (исключена из системы управления доступом) пока действует 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.
Максимальная длительность импульса для дверной защелки:	0 - 9999	Максимальная длительность сигнала разблокировки. Единица измерения — 1/10 с. Значения по умолчанию: 50 для дверей, 10 для вращающихся дверей (модель двери 03) и 200 для шлагбаумов (модели дверей 05c или 09c).
Минимальная длительность импульса для дверной защелки:	0 - 9999	Минимальная длительность сигнала разблокировки в 1/10 сек. Значение по умолчанию — 10.
Предварительное подавление тревоги	0 - 9999	Дополнительное подавление тревоги **перед** импульсом для дверной защелки. (`$PARAMETER_WAITEMA`) В редких случаях, когда дверная защелка реагирует медленнее, чем сигнал охранной тревоги, можно временно подавить сигнал тревоги, прежде чем отправить на дверь сигнал разблокировки. Единица измерения — 1/10 сек. Значение по умолчанию — 0. Значение 20, равное 2 секундам, обычно является достаточным даже для очень медленной двери.
Последующее подавление тревоги	0 - 9999	Дополнительное подавление тревоги **после** импульса для дверной защелки. (`$PARAMETER_OPENINRT`)

		После прохождения импульса для дверной защелки (сигнала разблокировки) в течение определенного времени дверь можно открыть без срабатывания тревоги. Единица измерения — 1/10 с. Значение по умолчанию — 0.
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 датчик присутствует	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 датчик присутствует	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 (по умолчанию) = у двери нет ригельного датчика 1 = у двери есть ригельный датчик. Сообщение создается, когда дверь заперта или отперта.
Расширенное время открытия двери (для инвалидов)	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = сигнал разблокировки имеет стандартную продолжительность, которая задается параметром **двери** «Макс. время активации блокировки», т. е. продолжительность импульса для дверной защелки. 1 (по умолчанию) = продолжительность сигнала разблокировки умножается на коэффициент, заданный параметром **MAC** «**Временной фактор для лиц с ограниченными физическими возможностями**» (вкладка **Общие настройки доступа**). Значение 0 для этого параметра MAC отключает продление времени открытия двери.

Вкладка: безопасность дверей

Параметр	**Возможные значения**	**Замечания**
Создавать сообщение для состояния «Дверь открыта принудительно»	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = нет сообщений о вторжении. Это полезно, если дверь может свободно открываться изнутри. 1 = (по умолчанию) при неавторизованном открытии, а затем после закрытия отправляются сообщения.

Создавать сообщение для состояния «Дверь держится открытой» через:	0 - 9999	Если дверь остается открытой по истечении этого времени, отправляется сообщение, предупреждающее, что дверь остается открытой слишком долго. Единица измерения — 1/10 с. Значение по умолчанию — 300. 0 = без тайм-аута, без сообщений.
Продление подавления тревоги при состоянии «Дверь открыта принудительно»	0 - 9999	Используется в функции «шунт REX»: Единица измерения — 1/10 с. Значение по умолчанию — 0. Если после получения сигнала REX от детектора движения дверь закрывается в течение этого промежутка времени, то обычное сообщение `Unauthorized opening of door N` заменяется сообщением `Door N opened (in alarm suppression mode)`, где N — это номер двери.
Создавать локальный сигнал тревоги для состояния «Дверь открыта принудительно»	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Предварительные условия: флажок **«Создавать сообщение для состояния «Дверь открыта принудительно»** в этом диалоговом окне установлен (см. выше). 0 = (по умолчанию) считыватели, подключенные к этой двери, не подают локальный сигнал тревоги. 1 = считыватели, подключенные к этой двери, подают локальный сигнал тревоги, если дверь открывается принудительно.
Создавать локальный сигнал тревоги для состояния «Дверь держится открытой» после:	0 - 9999	Если дверь остается открытой по истечении этого времени, считыватели, подключенные к этой двери, подают локальный сигнал тревоги. Единица измерения — 1/10 с. 0 = (по умолчанию) локальный сигнал тревоги не подается.

16.6.1 Шунт REX

Введение

На проходах, где нет угрозы безопасности при открывании дверей вручную изнутри, детектор движения часто заменяет собой кнопку REX для разблокирования двери. Для таких сценариев в ACS предусмотрен простой способ увеличить продолжительность сигнала REX от детектора движения с одновременным шунтированием (подавлением) `Door forced open` тревоги.

Эта функция называется «шунт REX».

Когда эта функция активна, держатели карт, выходящие через двери в течение действия шунтирования, создают событие доступа
`Door N opened (in alarm suppression mode)`, а не
`Unauthorized opening of door N`.

Замечание!
Шунт REX в сочетании с поставленными на охрану системами детекторов вторжения
Функция шунтирования REX подавляет тревоги в течение времени, заданного в параметре
Редактор устройств > ... > **Дверь** > вкладка **Безопасность двери** > **Продление подавления тревоги при состоянии «Дверь открыта принудительно»**,
независимо от того, поставлена ли в данный момент эта дверь на охрану в составе системы обнаружения вторжения.

Предварительные требования

- Настраиваются двери следующих типов: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- Физическая дверь оснащается датчиком движения, а не кнопкой REX для разблокировки двери. Установите продолжительность сигнала от детектора движения по крайней мере на 1 секунду.

Путь к диалоговому окну

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

Процедура

1. В редакторе устройств перейдите к нужному проходу (непосредственному дочернему узлу контроллера двери).
2. На вкладке **Терминалы** прохода создайте новый входящий сигнал типа
   `Suppress alarm from unauthorized opening`
3. Нажмите (Сохранить) для сохранения изменений.
4. Выберите дверь, находящуюся в нужном проходе
5. На вкладке **Безопасность двери** этой двери задайте значение параметра **Продление подавления тревоги при состоянии «Дверь открыта принудительно»**
   - Значение задается в десятых долях секунды.
   - Значение по умолчанию — `0`. То есть по умолчанию продление подавления тревоги после выхода держателя карты из зоны действия детектора движения отсутствует.
6. Нажмите (Сохранить) для сохранения изменений.

16.6.2 Настройка дверей для локальных звуковых сигналов тревоги

Введение

При следующих состояниях дверей ACS подает звуковые сигналы на всех считывателях, подключенных к двери.

Состояние	Действие локального сигнала тревоги
Дверь открыта принудительно	Тревога звучит в течение 17 секунд или до закрытия двери.

Состояние	Действие локального сигнала тревоги
Дверь держится открытой	Сигнал тревоги звучит до закрытия двери.

Предварительные требования

– Считыватели используют протокол OSDP или Wiegand.
– Считыватели оснащены устройствами звуковой сигнализации, подключенными к электропроводке контроллера двери.
– Микропрограмм AMC обновлена до версии 02.38 иди более новой.

Следующие типы считывателей **не** поддерживаются:

– Считыватели IDEMIA
– Считыватели Suprema с протоколом Wiegand
– Считыватели LBUS
– Считыватели BG900

Путь к диалоговому окну

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

Процедура для состояния «Дверь открыта принудительно»

1. В дереве устройств выберите дверь, которую нужно настроить.
2. На вкладке **Безопасность двери** этой двери установите флажок **Создавать сообщение для состояния «Дверь открыта принудительно»**
3. Установите флажок **Создавать локальный сигнал тревоги для состояния «Дверь открыта принудительно»**
   Значение по умолчанию — `0` (флажок не установлен). Это означает, что по умолчанию локальный сигнал тревоги отключен.
4. Нажмите (Сохранить) для сохранения изменений.

Процедура для состояния «Дверь держится открытой»

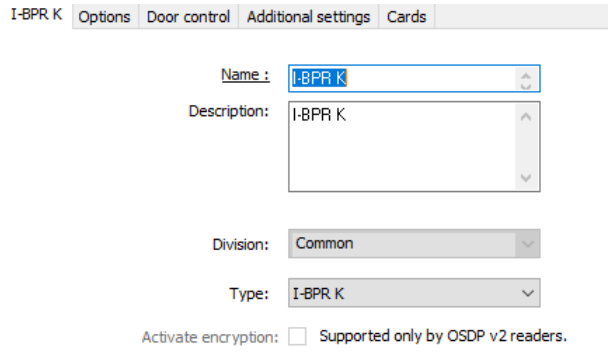
1. В дереве устройств выберите дверь, которую нужно настроить.
2. На вкладке **Безопасность двери** для этой двери задайте любое ненулевое значение параметру
   «Дверь держится открытой» после:

– Значение задается в десятых долях секунды.
– Значение по умолчанию — `0`. Это означает, что по умолчанию локальный сигнал тревоги отключен.

3. Нажмите (Сохранить) для сохранения изменений.

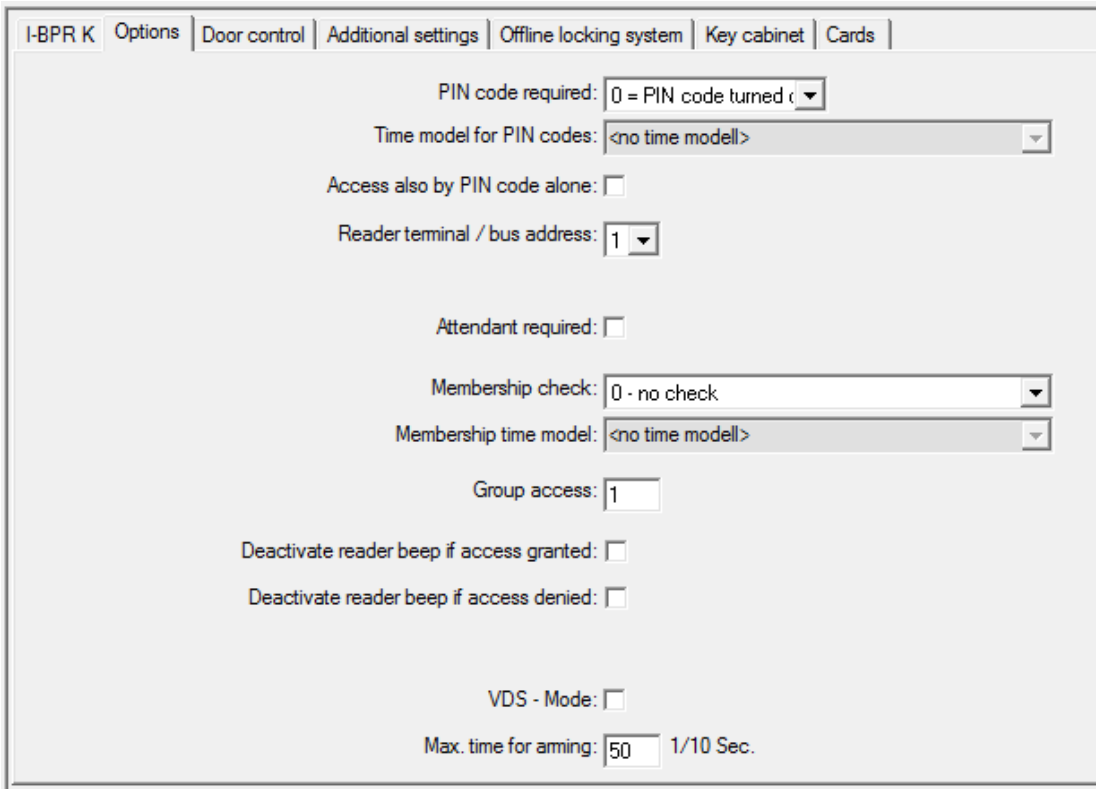
16.7 Устройства чтения

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)	Если система контроля доступа настроена соответствующим образом, определяет, может ли этот считыватель разрешать

	1 = включено (флажок установлен)	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

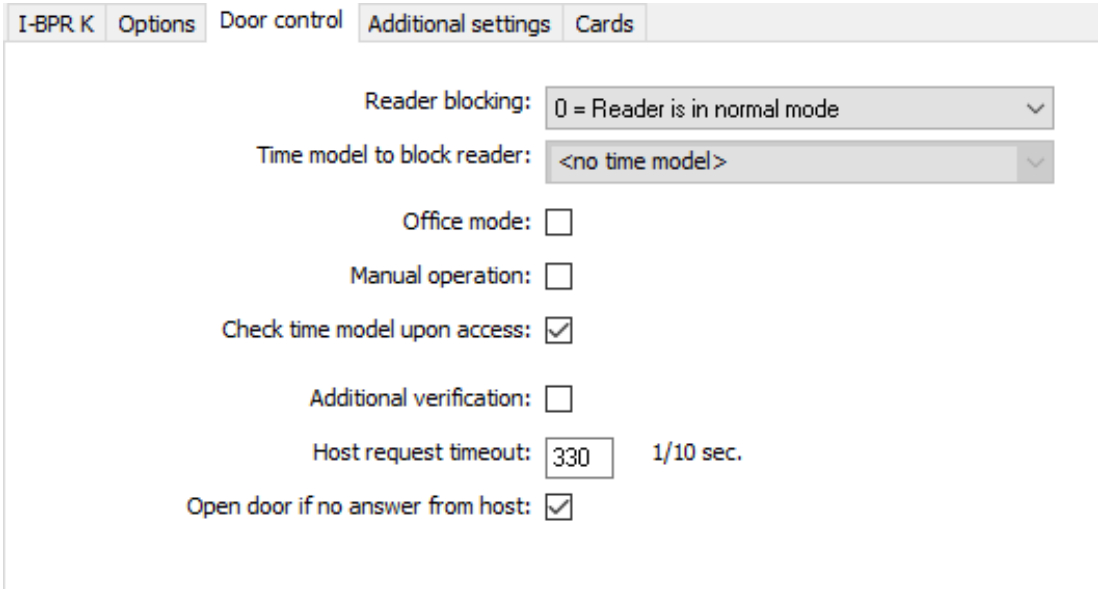
Эта вкладка отображается только для сетевых биометрических считывателей.

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

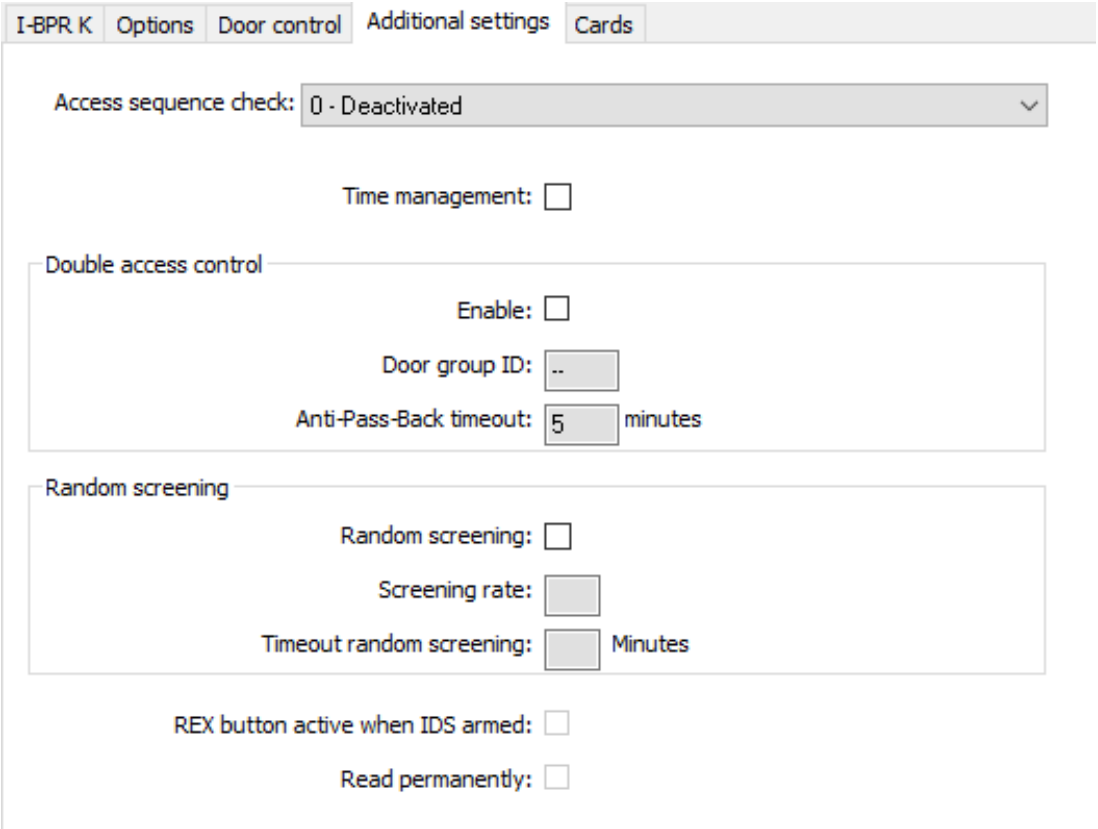


Параметр	Возможные значения	Замечания
Блокировка считывателя	Запись в поле списка	0 = считыватель в обычном режиме — без блокировки (= по умолчанию) 1 = считыватель постоянно заблокирован — постоянная блокировка 2 = считыватель блокируется в зависимости от модели времени — блокировка осуществляется в 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 данному считывателю перевести проход в офисный режим. Считыватель должен иметь клавиатуру. Если этот параметр активировать, то авторизованный должным образом держатель карты может включать и выключать режим офиса нажатием клавиши 3 перед предоставлением своей карты. См. раздел *Авторизация лиц для настройки офисного режима, Страница 212*.

Ручная операция	0 = отключено (флажок снят) 1 = включено (флажок установлен)	0 = считыватель в нормальном режиме (=по умолчанию) 1 = считыватель эффективно удаляется из системы управления 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 этого параметра необходима для дополнительного видеоподтверждения оператором системы Bosch BVMS или системы управления доступом).
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). от 1 до 9999 x 1/10 секунды. (По умолчанию = 330 = 33 секунды). Считыватель запрашивает подтверждение от системы управления доступом. Если в течение этого периода подтверждение не получено, AMC проверяет параметр **Открыть дверь по исходу времени**

		ожидания и соответствующим образом предоставляет доступ или отказывает в нем.
Открыть дверь по исходу времени ожидания	0 = отключено (флажок снят) 1 = включено (по умолчанию) (флажок установлен)	Этот элемент управления активен только в том случае, если задан параметр **Проверка оператором**. 0 = дверь не открывается, если главная система не выдает подтверждение до истечения времени ожидания. 1 (по умолчанию) = дверь открывается по истечении времени ожидания, если главная система не выдала подтверждение до истечения времени ожидания.

Настройка считывателя. Дополнительные параметры

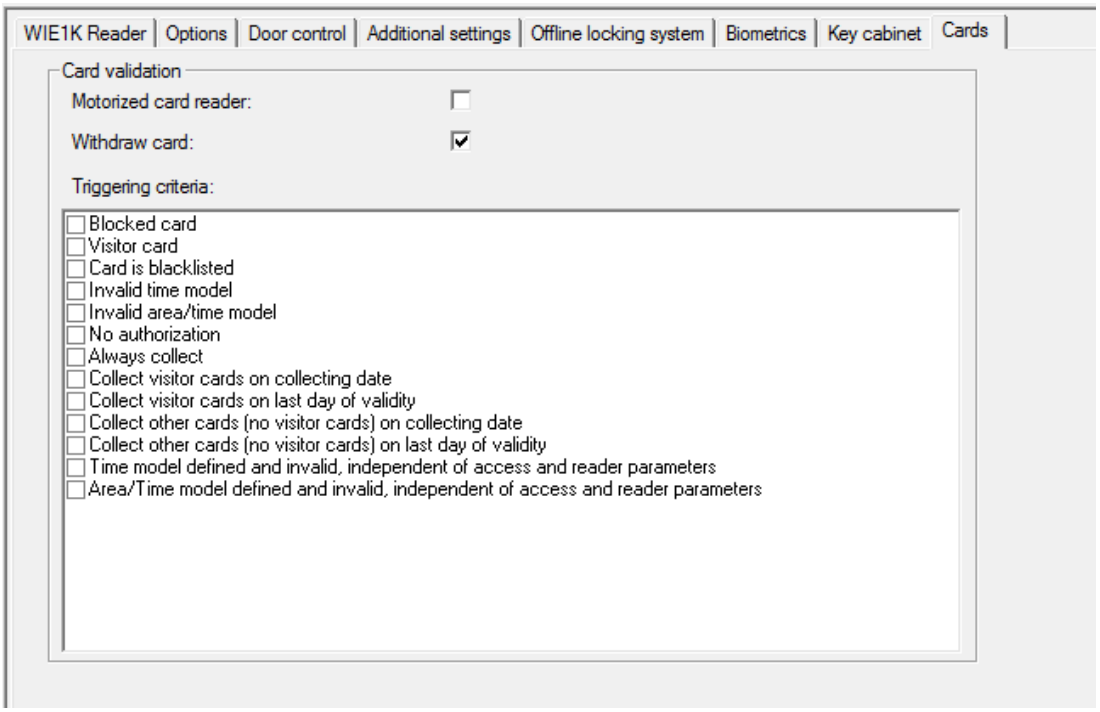


Параметр	**Возможные значения**	**Замечания**
Проверка последовательности доступа	0 — Деактивировано 1 — Активировано; деактивировать по неисправности LAC	0 = считыватель не участвует в проверке последовательности доступа (= по умолчанию) Активированная проверка последовательности может обрабатывать лиц с заданным статусом НЕИЗВЕСТНЫЕ указанным ниже образом.

	2 — Активировано; оставить активным по неисправности LAC 3 - Активировано; используйте четкую последовательность проверки даже при неисправности LAC (примечание: обновите местоположение лиц вручную)	1 = первое чтение карты будет завершено без проверки местоположения. Все контроллеры должны находиться в оперативном режиме. 2 = первое чтение карты будет завершено без проверки местоположения. 3 = если LAC неисправна, проверка местоположения будет завершена для каждого считывания карты.
 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 этот параметр выбран, система управления доступом собирает данные для учета рабочего времени.
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.
Постоянное считывание	0 = отключено (флажок снят) 1 = включено (флажок установлен)	Считыватель постоянно выполняет 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.

См.

– *Авторизация лиц для настройки офисного режима, Страница 212*

16.7.1 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.

16.8 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 системы управления доступом 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

16.9 Платы расширения AMC

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

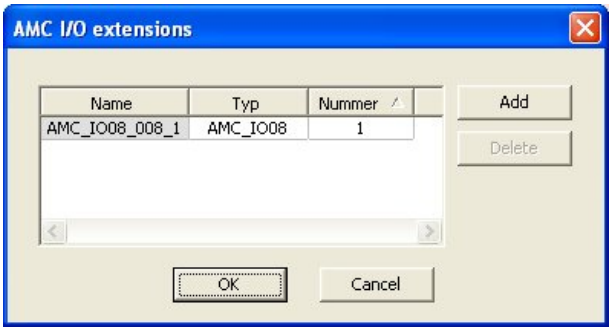
Платы расширения обеспечивают дополнительные входные и выходные сигналы, если восьми контактов, расположенных на AMC, не достаточно для подключения необходимых контактов (например, в случае лифтов).

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.

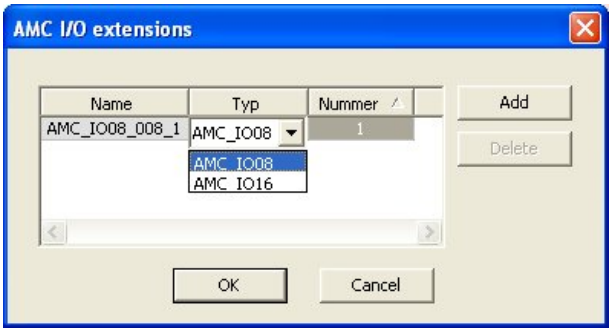
Появляется диалоговое окно для выбора критериев расширений.



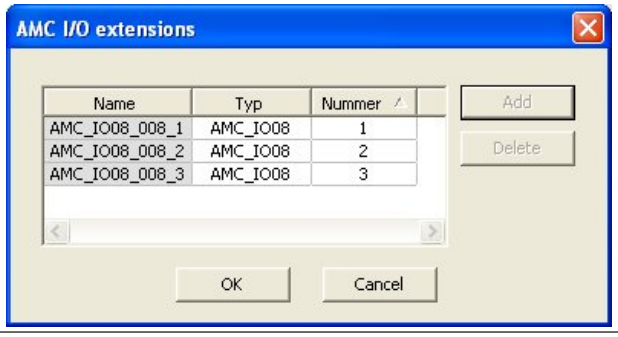
Плата AMC-EXT доступна в двух вариантах:

- 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

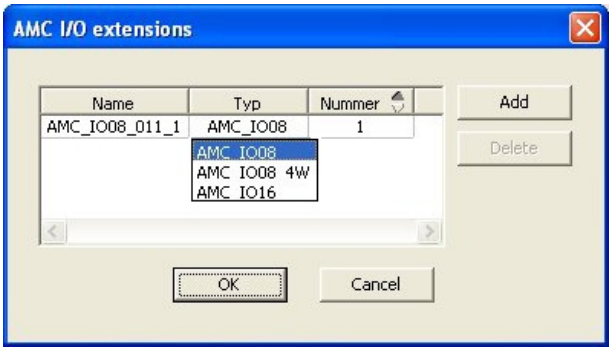
Для контроллеров с интерфейсами считывателей Wiegand (AMC2 4W) можно настроить специальные платы расширения (AMC2 4W-EXT). Каждый из этих модулей обеспечивает подключение четырех дополнительных считывателей Wiegand, а также 8 входных и 8 выходных контактов. Поэтому максимальное число считывателей и дверей, 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	Ограниченное алфавитно-цифровое значение: 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**	Применяется только в том случае, если функция **Подразделения** лицензирована.

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.

17 Специальные конфигурации считывателя

17.1 Введение

В системах BIS 4.9 и AMS 4.0 системы управления доступом Bosch позволяют использовать настраиваемые параметры MIFARE DESFire. Можно создавать зашифрованные файлы параметров с помощью дополнительного инструмента `Bosch.ReaderConfigTool.exe`. Он входит в комплекты установки для BIS ACE 4.9, AMS 4.0 и более поздних версий и имеет собственную документацию. Текущий список совместимых считывателей см. в документации
В следующих разделах рассматривается использование редактора устройств для импорта зашифрованного файла параметров и применения его к любому или всем совместимым считывателям в иерархии устройств управления доступом.

17.2 Свойство считывателя: Дополнительные параметры считывателя

Доступные наборы дополнительных параметров для совместимых считывателей отображаются на соответствующих страницах свойств в редакторе устройств в разделе **Дополнительные параметры считывателя**.

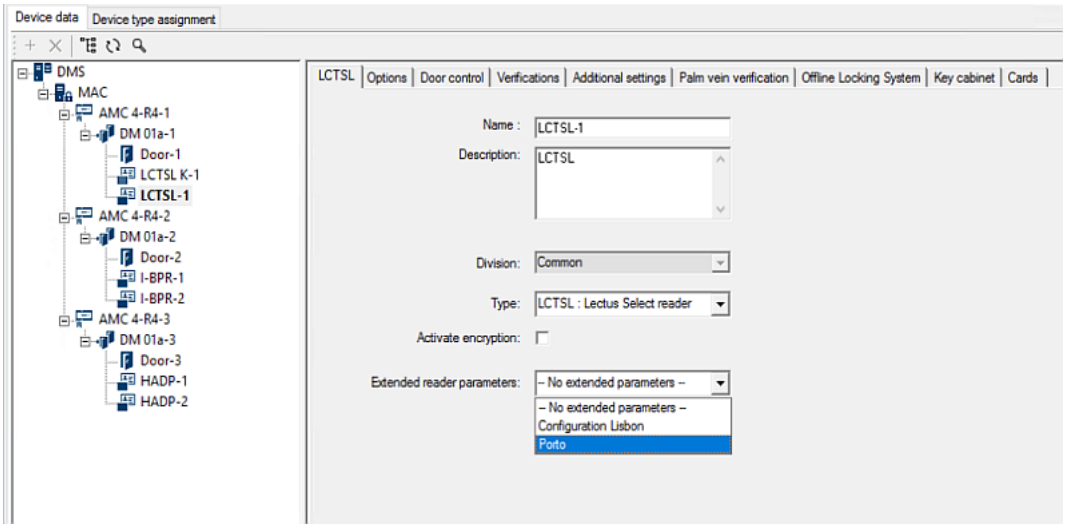


Рис. 17.1: Дополнительные параметры считывателя

Значением по умолчанию в раскрывающемся списке является `No extended parameters`. Это единственное значение, если наборы дополнительных параметров не импортированы.

Процедура

Чтобы применить импортированный набор параметров к отдельному совместимому считывателю, выполните следующие действия.

1. В редакторе устройств выберите нужный считыватель в дереве устройств
2. Выберите первую вкладку свойств
3. Выберите требуемый набор параметров в списке **Дополнительные параметры считывателя**
4. Нажмите кнопку **Применить** или 

17.3 Импорт набора параметров считывателя

Файлы параметров импортируются и удаляются только на уровне DMS в иерархии устройств.

Предварительные требования

Доступ к файлу параметров, утвержденному для вашей системы управления доступом.
Тип файла по умолчанию: `.ReaderConfigSave`

Процедура

1. В редакторе устройств щелкните правой кнопкой мыши узел DMS и выберите **Импорт наборов параметров считывателя** в контекстном меню.
   Откроется всплывающее окно **Импорт наборов параметров считывателя**.
2. Нажмите **Файл** и найдите файл параметров в проводнике.
3. В ответ на запрос введите пароль для файла параметров.
   Если пароль правильный, в нижней половине всплывающего окна отобразится следующая информация:

– Список типов считывателей, к которым применяется набор параметров.
– Имя набора параметров. В этом диалоговом окне его можно изменить.
– Произвольное текстовое описание, если создатель набора параметров предоставил его. В этом диалоговом окне можно добавить или изменить описание.

4. Нажмите кнопку **Импорт**, чтобы импортировать набор параметров для дальнейшего использования системой управления доступом.

– Набор параметров импортируется и сохраняется в системе управления доступом.
– Он добавляется в список доступных наборов параметров вверх всплывающего окна.

5. Нажмите кнопку **Выход**, чтобы закрыть всплывающее окно **Импорт наборов параметров считывателя**.

17.4 Применение набора параметров к считывателям

Введение

Импорт набора параметров в систему управления доступом сохраняет его для дальнейшего использования, но не применяет к считывателям в системе. Применение набора параметров — это дополнительный шаг, который можно выполнять на различных уровнях иерархии устройств:

– DMS
– MAC
– AMC

На уровне DMS, MAC или AMC набор параметров может применяться только к подчиненным считывателям тех типов считывателей, для которых он был создан. Все остальные подчиненные считыватели не затрагиваются.

Предварительные требования

Должен быть импортирован набор параметров считывателя.

Процедура

1. В редакторе устройств щелкните правой кнопкой мыши считыватель или устройство (DMS, MAC или AMC), чьи считыватели требуется параметризировать.
2. Выберите **Управление наборами параметров считывателя** в контекстном меню.
3. В верхней панели списка **Наборы параметров для типов считывателей** выберите набор параметров, который требуется применить.
   Соответствующие считыватели отображаются в нижней левой панели **Считыватели, к которым применим этот набор параметров**.

4. В списке **Считыватели, к которым применим этот набор параметров** выберите считыватели, к которым требуется применить выбранный набор параметров.
– Если количество считывателей велико, используйте раскрывающиеся списки, чтобы ограничить отображение подчиненными считывателями конкретных контроллеров MAC или AMC.
5. Используя клавиши со стрелками, переместите выбранные считыватели в нижнюю правую панель **Все считыватели, к которым применен выбранный набор параметров**.

Замечание!
Отображение совместимых считывателей
В список будут включены считыватели, совместимые с данным набором параметров. Если установить флажок **Показать все считыватели**, также будут отображаться считыватели с другими наборами параметров. Их серый фон означает, что они доступны только для чтения для выбранного набора параметров.

6. Нажмите кнопку **ОК**, чтобы закрыть всплывающее окно.
7. В редакторе устройств нажмите кнопку **Применить** или
Набор параметров применяется ко всем считывателям в списке **Все считыватели, к которым применен выбранный набор параметров** в данном всплывающем окне.

17.5 Управление наборами параметров считывателя

Введение
Применение наборов параметров можно менять на различных уровнях иерархии устройств:
– DMS
– MAC
– AMC
Изменения на уровне DMS, MAC или AMC можно применять к подчиненным считывателям тех типов считывателей, для которых был создан данный набор. Все остальные подчиненные считыватели не затрагиваются.

Предварительное требование
Должен быть импортирован набор параметров считывателя.

Процедура
1. В редакторе устройств щелкните правой кнопкой мыши считыватель или устройство (DMS, MAC или AMC)
2. Выберите **Управление наборами параметров считывателя** в контекстном меню.
3. В верхней панели списка **Наборы параметров для типов считывателей**выберите набор параметров, который требуется применить.
– Применимые считыватели отображаются в нижней левой панели **Считыватели, к которым применим этот набор параметров**.
– Считыватели, к которым уже применен файл параметров, отображаются в нижней правой панели **Все считыватели, к которым применен выбранный набор параметров**.
4. Выберите считыватели в любом списке. Используя клавиши со стрелками, переместите выбранные считыватели в нижний правый список **Все считыватели, к которым применен выбранный набор параметров** или из него.
– ВАЖНО! Обязательно запомните считыватели, которые вы убираете из списка, для последнего шага в этой процедуре.

5. Завершив изменения, нажмите кнопку **ОК**, чтобы закрыть всплывающее окно.
6. В редакторе устройств нажмите кнопку **Применить** или
– Данный параметр применяется ко всем считывателям, которые оставлены в списке **Все считыватели, к которым применен выбранный набор параметров.**
– Он удаляется из считывателей, которые были убраны из данного списка.
7. Выполните одно из следующих действий для всех считывателей, убранных из списка:
– Выполните сброс к заводским настройкам по умолчанию, используя DIP-переключатели на считывателях.
– Примените к ним другой набор параметров.

Замечание!
Удаление набора параметров не приводит к перенастройке использующих его считывателей.
Удаленная конфигурация будет сохраняться в использующих ее считывателях до выполнения сброса считывателя или применения другого набора параметров.

17.6 Удаление наборов параметров считывателя

Файлы параметров импортируются и удаляются только на уровне DMS в иерархии устройств.

Предварительные требования
Как минимум один файл параметров уже должен быть импортирован в систему управления доступом.

Процедура
1. В редакторе устройств щелкните правой кнопкой мыши узел DMS и выберите **Удалить наборы параметров считывателя** в контекстном меню.
Откроется всплывающее окно **Удалить наборы параметров считывателя**.
2. В списке **Наборы параметров для типов считывателей** выберите набор параметров, который требуется удалить.
– В нижней правой части всплывающего окна отображаются все считыватели, к которым в данный момент применен (настроен) выбранный набор параметров.
– Обязательно запомните эти считыватели, поскольку после удаления набора параметров потребуется выполнить их сброс или повторную настройку. Подробные сведения см. в последнем шаге этой процедуры.
3. Нажмите кнопку **Удалить**
4. Нажмите кнопку **Выход**
5. В редакторе устройств нажмите кнопку **Применить** или
6. Выполните одно из следующих действий для всех считывателей, которые использовали удаленный набор параметров.
– Выполните сброс к заводским настройкам по умолчанию, используя DIP-переключатели на считывателях.
– Примените к ним другой набор параметров.

Замечание!
Удаление набора параметров не приводит к перенастройке использующих его считывателей.
Удаленная конфигурация будет сохраняться в использующих ее считывателях до выполнения сброса считывателя или применения другого набора параметров.

18 Пользовательские поля для данных персонала

Введение

Поля данных для персонала можно настраивать многочисленными способами:

- Являются ли поля **видимыми**, то есть отображаются ли они в 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) в клиенте они отображаются.
- Насколько большими они отображаются.
- Будут ли данные использоваться в стандартных отчетах и где.

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

18.1 Предварительный просмотр и редактирование настраиваемых полей

Путь к диалоговому окну

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

Главное окно разделено на две вкладки

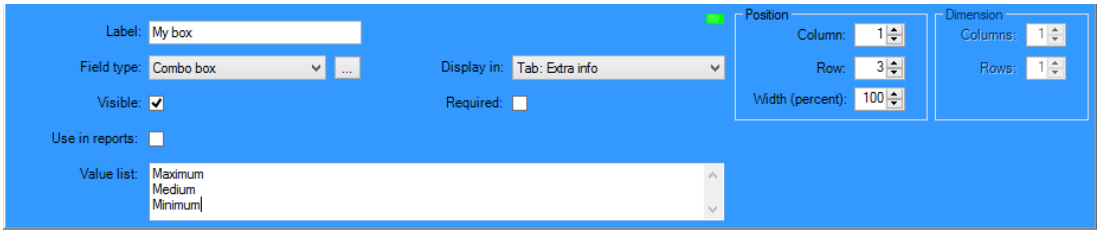
Обзор Эта вкладка и ее вложенные вкладки (**Адрес, Контакт, Дополнительные личные данные, Дополнительные данные о компании, Примечания, Контроль карт** и **Дополнительные сведения**) доступны только для чтения и содержат примерное представление вида WYSIWYG («что видишь, то и получишь») о том, какие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

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
Метка	**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	Чтобы поле данных не отображалось в клиенте, снимите этот флажок.
Уникальное	Чтобы гарантировать уникальность значений, вводимых в данном поле, установите этот флажок. После этого система будет отклонять ввод любого значения, которое уже было сохранено для этого поля в базе данных. Например, у каждого сотрудника должен быть уникальный учетный номер, а у транспортных средств — номерные знаки.
	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.

Текст метки	Описание
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. 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.

18.2 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.

19 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.

19.1 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).

19.2 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.

19.3 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.

19.3.1 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.

19.3.2 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.

19.3.3 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.

19.3.4 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.

19.3.5 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.

19.4 Этапы настройки в диалоговых окнах системных данных

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

19.4.1 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)

19.4.2 Назначение профиля безопасности лица типу персонала

Путь к диалоговому окну

- **Главное меню** > **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.

19.5 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.

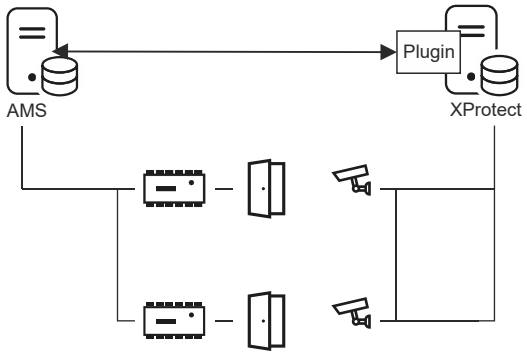
– *Назначение профиля безопасности лица типу персонала, Страница 150*
– *Создание данных персонала и управление ими, Страница 201*

20 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.

Замечание!

Потенциальная несовместимость подключаемых модулей из разных источников
Подключаемые модули Milestone XProtect работают не в изолированной среде, т. е. они не полностью изолированы друг от друга. Поэтому при запуске нескольких подключаемых модулей с различными версиями технологии .NET, а также ее пакетов и библиотек на одном сервере Xprotect могут возникать программные ошибки. Компания BOSCH может гарантировать правильность работы подключаемого модуля AMC только при отсутствии других установленных подключаемых модулей.

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.

21 Интеграция Otis Compass

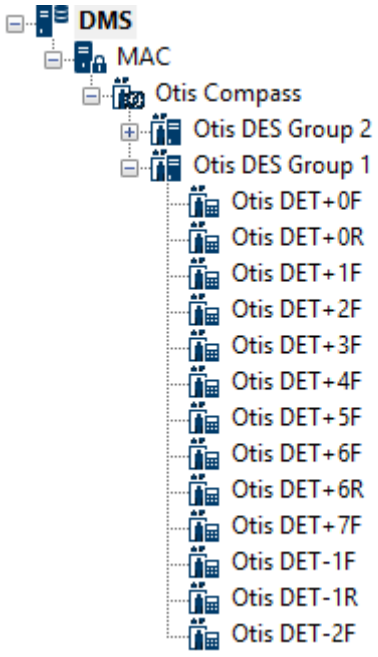
Введение

Compass – это система управления назначением компании Otis Elevator. Она используется для управления несколькими лифтовыми холлами и направляет лифты пассажирам, чтобы они могли как можно эффективнее достичь места назначения. Чтобы предоставить необходимые данные, пассажиры теперь не просто нажимают кнопки **Вверх** или **Вниз**, но запрашивают место назначения на считывателе карт, сенсорном экране или терминалах с клавиатурой.

Интеграция с системами управления доступом Bosch добавляет безопасность решению. В зависимости от учетных данных и используемых временных моделей пассажиры эффективно попадают на домашние этажи и другие авторизованные места назначения. Система не принимает запросы для этажей, которые не указаны в профилях авторизации пассажира, или времени суток, которое выходит за рамки текущей временной модели.

Топология оборудования системы Compass

Оборудование системы Compass настраивается сверху вниз в виде трехуровневой иерархии под одним контроллером MAC в редакторе устройств.



В иерархии выше показаны:
система **Otis Compass** на выделенном MAC;
одна группа лифтов, управляемая одним **DES**;
несколько терминалов (**DET**), каждый из которых имеет номер этажа от -2 до +7 и символ F (передняя дверь) или R (задняя дверь).

Первый уровень: (Otis Compass)
Система управления направлениями.
Каждая система **Compass** может управлять 8 группами лифтов (лифтовыми холлами).
Параметры: диапазон этажей,
сетевых адресов,
номеров портов и тайм-аутов.

Второй уровень: (Otis DES/DER)
До 8 групп лифтов, каждой из которых управляет сервер ввода направлений (Destination Entry Server - DES), состоящий из 1 или 2 физических устройств.
Кроме того, этот уровень может иметь до двух дополнительных устройств для оптимизации, которые называются перенаправителями ввода направлений (DER).
Параметры: 1 идентификатор на каждую группу лифтов.
1 IP-адрес для устройства.
Таблица этажей с дверями лифта с указанием, являются ли они общедоступными.

Третий уровень: Otis DET
Терминалы ввода направлений (Destination Entry Terminals - DET)

	Параметры: 1 IP-адрес на каждый терминал. Доступные этажи с дверями лифта для каждого терминала.

Обзор интеграции системы управления доступом

Администраторы системы управления доступом интегрируют Compass на следующих этапах, подробно описанных далее в главе:

1. Настройка оборудования Compass на одном контроллере MAC в редакторе устройств.
2. Настройка пользовательских полей для характеристик держателей карт, необходимых для функционирования системы Otis, таких как домашний этаж.
3. Создание профилей авторизации, которые управляют доступом к конкретным местам назначения лифта.
4. Назначение профилей авторизации соответствующим держателям карт

21.1 Настройка системы Compass в редакторе устройств

В этом разделе описывается настройка системы Otis Compass в редакторе устройств.

Путь к диалоговому окну

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

21.1.1 Уровень 1: настройка системы Compass

Процедура для уровня 1: настройка системы Compass

1. Выберите нужный MAC в представлении дерева редактора устройств
2. Щелкните правой кнопкой мыши и выберите **Новый Otis Compass**. На странице свойств есть 2 вкладки.
   – **Otis Compass**
   – **Этажи**
3. Самые важные параметры на вкладке **Otis Compass**:
   – **Имя** (имя, которое должно отображаться в дереве устройств);
   – **IP-адрес контроллера MAC** (обратный IP-адрес для системы Compass на выделенной сетевой плате, с помощью которой система Compass взаимодействует с контроллером MAC).
   ПРИМЕЧАНИЕ. Это **не** IP-адрес самого контроллера MAC.
   – **Подразделение** (только если подразделения лицензированы и используются в вашей системе).

Оставьте для остальных параметров значения по умолчанию, кроме случаев, когда их изменение предписано специалистами технической поддержки. Эти параметры кратко описаны в следующей таблице:

Параметр	Значение по умолчанию	Описание
Адрес группы MC	234.46.30.7	IP-адрес группы многоадресной рассылки

Параметр	Значение по умолчанию	Описание
Порт MC для DES/DER (удаленный) Порт MC для DES/DER (локальный)	48307 47307	Многоадресные порты
Порт UDP для DES/DER (удаленный) Порт UDP для DES/DER (локальный)	46303 45303	Порты UDP для устройств DES и DER
Порт UDP для DET (удаленный) Порт UDP для DET (локальный)	45308 46308	Порты UDP для устройств DET
Время жизни пакета при многоадресной передаче (TTL)	5 секунд	
Интервал сердцебиения	1 секунда	Промежуток времени между интервалами сердцебиения. Эти сигналы показывают другим устройствам, что данное устройство работает
Макс. количество пропущенных интервалов сердцебиения	3	Число интервалов сердцебиения, которые можно пропустить, прежде чем устройство будет считаться неработающим
Истекло время ожидания сообщения	1 секунда	
Число повторных попыток сообщения	3	

1. На вкладке **Этажи** нажмите **Изменить диапазоны этажей**
2. Введите номера самых нижних и самых высоких этажей, которые должны обслуживаться всеми лифтовыми холлами системы Otis Compass.
   – Максимальный диапазон: от -127 до +127
3. Нажмите  (Сохранить) для сохранения изменений.

21.1.2 Уровень 2: группы лифта, устройства DES и DER

Процедура для уровня 2: настройка групп лифтов (устройства DES и DER)
Введение
DES (сервер ввода направлений) — это компьютер, который управляет группой лифтов. При необходимости два физических устройства DES с отдельными IP-адресами можно объединить в логическое устройство с поддержкой отработки отказа.

Сервер DER (Перенаправитель ввода направлений) соединяет группы лифтов и позволяет серверам DET в общей точке входа в здание (например в вестибюле) принимать запросы места назначения для любого этажа в здании. Сервер DER не настроен на работу в отказоустойчивом режиме.

Создание устройств DES в дереве устройств:

1. Выберите нужную систему Otis Compass в представлении дерева редактора устройств.
2. Щелкните правой кнопкой мыши и выберите **Новый Otis DES**. На странице свойств есть 2 вкладки.
   - **Otis DES**
   - **Этажи**
3. На вкладке **Otis DES** настройте следующие параметры.
   - **Имя**: (имя, которое должно отображаться в дереве устройств). Используйте систематическую схему именования, которая упростит ориентацию по конфигурациям устройств DES и DET позднее в процессе настройки.
   - **Описание:** (необязательно) описание устройства в виде произвольного текста.
   - **Группа:** целое число от 1 до 10**.** Укажите уникальное целое число среди всех групп лифтов (обозначенных устройствами DES или DER) в этой системе Otis Compass. Вы не сможете сохранить изменения устройств, если использовать один и тот же номер **группы** несколько раз.
   - **1-й IP-адрес:** IP-адрес этого устройства DES.
   - **2-й IP-адрес:** если у этого устройства DES есть резервная пара, введите здесь ее IP-адрес.
   - **Подразделение** (только если подразделения лицензированы и используются в вашей системе).

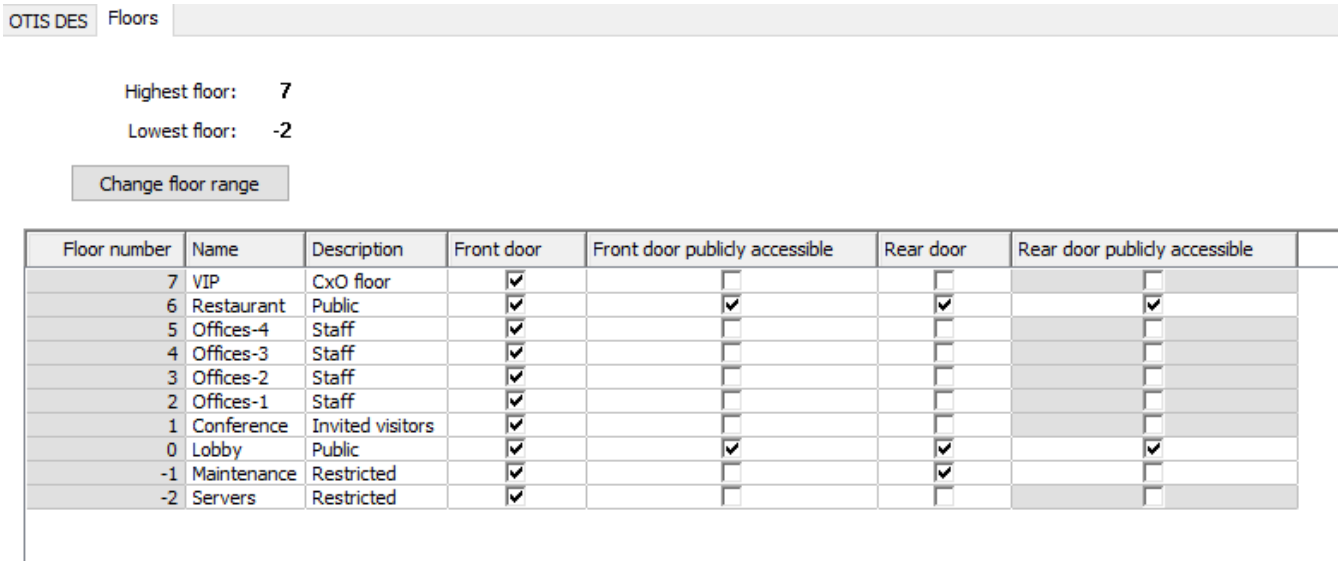
На вкладке **Этажи** представлены этажи, определенные для уровня 1 (система Compass), в виде таблицы редактируемых ячеек.

Создание устройств DER в дереве устройств:

Создание устройств DER аналогично созданию устройств DES. Единственная разница заключается в том, что DER не требуется устройство для переключения на резервные мощности при отказе, поэтому для него не предусмотрена возможность ввода **второго IP-адреса**.

Пример группы лифта.

В приведенном ниже примере показаны этажи для группы лифтов на 10 этажей с передними и задними дверьми и общедоступными первым и шестым этажами.



Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	☑	☐	☐	☐
6	Restaurant	Public	☑	☑	☑	☑
5	Offices-4	Staff	☑	☐	☐	☐
4	Offices-3	Staff	☑	☐	☐	☐
3	Offices-2	Staff	☑	☐	☐	☐
2	Offices-1	Staff	☑	☐	☐	☐
1	Conference	Invited visitors	☑	☐	☐	☐
0	Lobby	Public	☑	☑	☑	☑
-1	Maintenance	Restricted	☑	☐	☑	☐
-2	Servers	Restricted	☑	☐	☐	☐

1. В столбце **Передняя дверь** установите флажки всех этажей, на которых лифт использует переднюю дверь.
2. Аналогичным образом установите флажки напротив столбца **Задняя дверь**, если применимо.
3. Для столбца **Передняя дверь общедоступна** установите флажки напротив тех этажей, которые доступны всем пассажирам лифта без ограничений.
4. Установите флажки таким же образом в столбце **Задняя дверь общедоступна**, если применимо.
5. (Необязательно) Нажмите **Изменить диапазоны этажей** на этой вкладке, чтобы ограничить диапазон этажей, который был установлен на уровне **Otis Compass**.
6. Замените имена по умолчанию в столбцах **Имя** и **Описание** на требуемые.
7. Нажмите (Сохранить) для сохранения изменений.

21.1.3 Уровень 3: устройства DET

Процедура для уровня 3: настройка терминалов (устройства DET)
Введение
DET (или DEC — компьютер ввода направлений) считывает физические учетные данные или PIN-коды. DET может находиться на определенном этаже за передней или задней дверью лифта или внутри кабины лифта.

Создание устройств DET в дереве устройств:
1. Выберите нужное устройство Otis DES или DER в представлении дерева редактора устройств.
2. Щелкните правой кнопкой мыши и выберите **Новый терминал Otis**.
   – Появится всплывающее окно **Создать терминалы Otis**.
3. Введите количество терминалов, которое требуется настроить для этого DES или DER.
4. Примите значения по умолчанию или введите новые начальные значения для четырех октетов IP-адреса.

- Для любого октета (обычно для 4-го) установите флажок **Автоматическое приращение**, если требуется, чтобы система настроила уникальный IP-адрес для каждого терминала, увеличивая октет на единицу.

5. Нажмите кнопку **ОК**.
   - Нужное количество устройств DET будет создано в дереве устройств.
   - Их IP-адреса увеличиваются на единицу в соответствии с определением на предыдущем шаге.

Настройка устройств DET

На странице свойств каждого устройства DET есть 2 вкладки.

- **Терминал Otis**
- **Этажи**

1. На вкладке **Терминал Otis** настройте следующие параметры.
   - **Имя:** имя, которое должно отображаться в дереве устройств.
   - **Описание:** (необязательно) описание устройства в виде произвольного текста.
   - **IP-адрес:** IP-адрес этого устройства DET.
   - **Рабочий режим:** `1..4`
     определяет, как терминал запрашивает направления у пассажира лифта и передает запросы устройству DES или DER для проверки. В следующей таблице приведены подробные сведения.

Рабочий режим	**Описание**	**Поведение**
1	Этаж по умолчанию	(Рабочий режим по умолчанию) Пассажир предоставляет свои учетные данные или вводит PIN-код. Если учетные данные или PIN-код допустимы и пассажир больше ничего не вводит, DET запрашивает у DES этаж пассажира по умолчанию («домашний этаж»). Если пассажир вводит другой целевой этаж, DET запрашивает место назначения у DES.
2	Доступ к авторизованным этажам	Пассажир предоставляет учетные данные или вводит PIN-код, а затем вводит целевой этаж. DET запрашивает место назначения у DES. Система управления доступом предоставляет доступ к запрошенному месту назначения или отказывает в нем.
3	Ввод целевого этажа пользователем	Пассажир вводит целевой этаж. Если место назначение общедоступно, DET запрашивает место назначение у DES. В противном случае DET запрашивает у пассажира учетные данные для проверки.
4	Этаж по умолчанию или ввод целевого	Пассажир предоставляет свои учетные данные или вводит PIN-код. Если учетные данные или PIN-код действительны, DET запрашиваются у DES этаж пассажира по умолчанию («домашний» этаж).

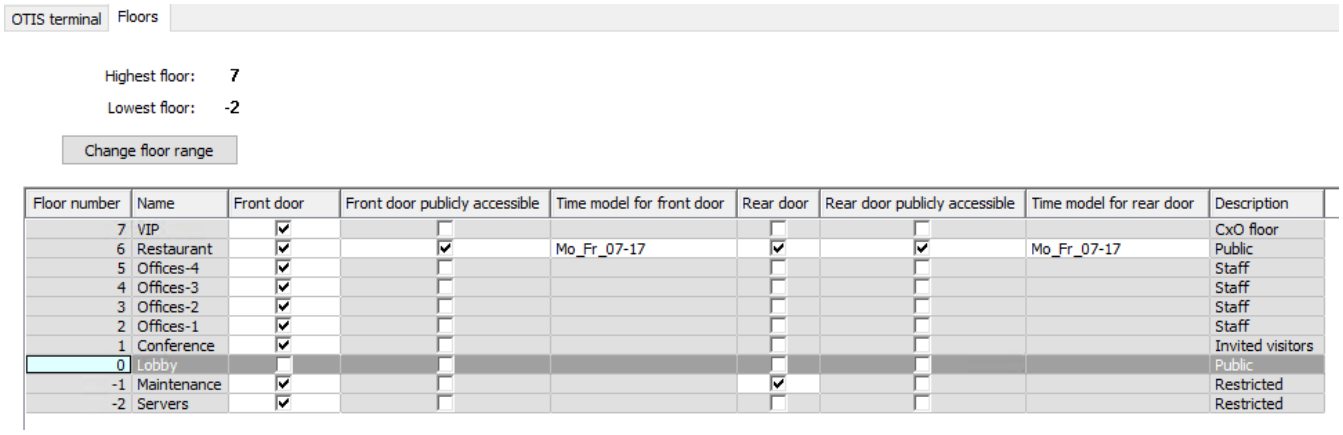
Рабочий режим	Описание	Поведение
	этажа пользователем.	В течение установленного периода времени ожидания пассажир может переопределить выбор этажа по умолчанию и выбрать другое место назначения.

- **Записи для аудита:** установите этот флажок для записи вводимых пассажиром данных на этом терминале в журнал событий.
- **PIN-код:** установите этот флажок, чтобы разрешить использование идентификационного PIN-кода на данном терминале в качестве альтернативы физическим учетным данным.
  Примечание. Воспользуйтесь регистрационными считывателями типа **Диалоговое окно PIN-карты (ввод)**, чтобы зарегистрировать PIN-коды, которые будут использоваться в терминалах Otis.
- **Временные модели:** установите этот флажок, чтобы разрешить временным моделям ограничивать время, в течение которого можно использовать этот терминал.
- **Подразделение** (только если подразделения лицензированы и используются в вашей системе)

На вкладке **Этажи** на странице свойств **Терминал Otis** этажи, которые вы определили для уровня 2 (DES или DER) представляются как таблица редактируемых ячеек.
Примечание. Схема именования, определенная для уровня 2 выше, должна упростить ориентацию. В противном случае рекомендуется сохранить работу и вернуться к уровню 2, чтобы завершить схему именования.

1. Выберите каждое устройство DET, которое вы создали в дереве устройств, и откройте вкладку **Этажи**.
   - Отобразится таблица **Этажи**.
2. В столбце **Передняя дверь** установите флажок для каждого этажа, который должен быть доступен из текущего DET.
3. В столбце **Передняя дверь общедоступна** установите флажок напротив каждой передней двери, которая должна быть общедоступна (то есть доступ через нее осуществляется без явной авторизации).
4. (Необязательно) В столбце **Временная модель для передней двери** выберите временную модель, чтобы ограничить общественный доступ к передней двери на этом этаже, если это необходимо. Например, этаж ресторана может быть доступен только в определенное время дня.
5. При необходимости повторите предыдущие действия для столбцов **Задняя дверь**, **Задняя дверь общедоступна** и **Временная модель для задней двери**.
6. Нажмите  (Сохранить) для сохранения изменений.

Пример:
В примере ниже показаны этажи для группы лифтов на 10 этажей. Эти этажи и двери доступны из передней двери лифта в зале ожидания. Доступ к этажу ресторана через переднюю и заднюю дверь лифта ограничен временной моделью.



Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	☑	☐		☐	☐		CxO floor
6	Restaurant	☑	☑	Mo_Fr_07-17	☑	☑	Mo_Fr_07-17	Public
5	Offices-4	☑	☐		☐	☐		Staff
4	Offices-3	☑	☐		☐	☐		Staff
3	Offices-2	☑	☐		☐	☐		Staff
2	Offices-1	☑	☐		☐	☐		Staff
1	Conference	☑	☐		☐	☐		Invited visitors
0	Lobby	☐	☐		☐	☐		Public
-1	Maintenance	☑	☐		☑	☐		Restricted
-2	Servers	☑	☐		☐	☐		Restricted

21.2 Конфигурация настраиваемых полей с характеристиками владельцев карт, необходимыми для функционирования системы Otis

Введение

В этом разделе описано создание таких настраиваемых полей, в которых оператор может вводить необходимые для функционирования системы Otis характеристики владельцев карт, в частности «дом» или любое другое место назначения по умолчанию. Такой «дом» должен определяться **тремя координатами**:

1. группа лифтов,
2. этаж,
3. дверь.

Обратите внимание, что, задавая домашний этаж держателя карты в клиенте системы контроля доступа, оператор должен вводить данные в том же порядке: группа лифтов, этаж, дверь. Поэтому три настраиваемых поля следует разместить в удобном для чтения порядке, предпочтительно — снизу вверх.

Нажмите кнопку **ОК**, чтобы подтвердить и скрыть всплывающие напоминания о том, что необходимо создать все три координаты.

Определите 3 обязательных настраиваемых поля и любые другие параметры, необходимые для работы системы Otis, которые будут отображаться на вкладке **Лифты** в клиентском интерфейсе контроля доступа.

Общие сведения о конфигурировании настраиваемых полей доступны в разделе **Настраиваемые поля с данными о персонале** справки по конфигурации ACE/AMS.

Путь к диалоговому окну

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

Процедура

На странице свойств **Настраиваемые поля** перейдите на вкладку **Лифты**.

Первая координата: группа лифтов

1. Дважды щелкните в ячейке на вкладке и нажмите кнопку **Да**, чтобы создать новое поле ввода.
2. В списке **Тип поля** выберите **Выбор сервера Otis DES**.
3. В поле **Метка** введите `Elevator Group`
4. В списке **Отображать в** выберите `Tab:Elevators`

5. В группе **Положение** выберите уникальное расположение на вкладке **Лифты**, где должно отображаться это настраиваемое поле.

Вторая координата: домашний этаж

1. Нажмите **Новое поле**, чтобы создать новое настраиваемое поле
2. В списке **Тип поля** выберите **Домашний этаж**.
3. В поле **Метка** введите `Home floor`
4. В списке **Отображать в** выберите `Tab:Elevators`
5. В группе **Положение** выберите уникальное расположение на вкладке **Лифты**, где должно отображаться это настраиваемое поле. Для удобства системных операторов это поле следует расположить под предыдущей координатой.

Третья координата: выходная дверь

1. Нажмите **Новое поле**, чтобы создать новое настраиваемое поле
2. В списке **Тип поля** выберите **Выходная дверь**.
3. В поле **Метка** введите `Exit door`
4. В списке **Отображать в** выберите `Tab:Elevators`
5. В группе **Положение** выберите уникальное расположение на вкладке **Лифты**, где должно отображаться это настраиваемое поле. Для удобства системных операторов это поле следует расположить под предыдущей координатой.

Характеристики владельцев карт, необходимые для функционирования оборудования Otis

Введение

Восемь специальных двоичных параметров Otis предоставляется для функционирования стандартной системы Otis. Если эти параметры определены в качестве настраиваемых полей на вкладке **Лифты**, они отображаются в качестве полей с флажками на вкладке **Данные лифта** для владельцев карт в диалоговом окне **Лица** (Главное меню > **Данные о персонале** > **Лица**). Эти флажки могут устанавливать и снимать операторы системы контроля доступа.

Настройте эти параметры в строгом соответствии с инструкциями, полученными от своего представителя Otis.

Процедура

1. Нажмите **Новое поле**, чтобы создать новое настраиваемое поле
2. В списке **Тип поля** выберите **Параметры Otis**.
3. В поле **Метка** введите собственную метку, например `Otis flag 1` или в соответствии с документацией Otis.
4. В списке **Отображать в** выберите `Tab:Elevators`
5. В списке **Тип функции** выберите один из параметров в диапазоне от `OTIS option 1` до `OTIS option 8`
6. В группе **Положение** выберите уникальное расположение на вкладке **Лифты**, где должно отображаться это поле с флажком.
7. Нажмите  (Сохранить) для сохранения изменений.

21.3 Создание и настройка авторизаций для лифтов Otis

Введение

В этом разделе описано, как включить права доступа для групп лифтов, этажей и дверей лифтов Otis в **авторизацию**.

Авторизации назначаются напрямую держателям карт или, как правило, вместе с другими авторизациями включаются в **профили доступа**, которые затем назначаются владельцам карт.

Предварительные требования

Система Otis Compass определена в контроллере MAC с помощью редактора устройств. В нее включена группа лифтов (представленная соответствующим сервером DES) и пары «этаж+дверь» (представленные соответствующими серверами DET).

Путь к диалоговому окну

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

Процедура

1. В поле **Имя авторизации** введите имя существующей авторизации или нажмите  (Создать), чтобы создать новую авторизацию.
2. В списке контроллеров **MAC** выберите название контроллера MAC, на котором была создана система Otis Compass.
3. Перейдите на вкладку **Лифт Otis**
4. В списке **Лифты Otis** выберите сервер DES или DER для группы лифтов, которую требуется добавить в авторизацию (обратите внимание, что авторизация может содержать только один сервер DES или DER).
   - Этажи выбранной группы лифтов отображаются на вкладке **Этажи**.
5. В столбцах **Передняя дверь** и **Задняя дверь** на вкладке **Этажи** выберите двери на этажах, которые требуется включить в эту авторизацию.
   - Обратите внимание, что этажи и двери, которые **не** были выбраны для этой группы лифтов, когда она определялась в редакторе устройств, будут неактивны и недоступны для выбора в этом диалоговом окне.
6. Кроме того, можно нажать на кнопки **Назначить все этажи** и **Удалить все этажи**, чтобы выбрать все этажи и двери одновременно или снять с них выделение.
7. Нажмите  (**Сохранить**), чтобы сохранить авторизацию.

22 Настройка универсальной программы BioBridge от IDEMIA

В этом разделе описано, как настроить биометрические устройства IDEMIA для работы с системой управления доступом Bosch с помощью **MorphoManager** и **BioBridge**.
В подразделах рассматриваются задачи конфигурации для приведенных ниже областей:

- системы управления доступом Bosch;
- MorphoManager;
- клиент регистрации BioBridge в системе MorphoManager;
- адаптация под различные технологии и форматы карт.

22.1 Настройка клиента BioBridge в системе управления доступом Bosch

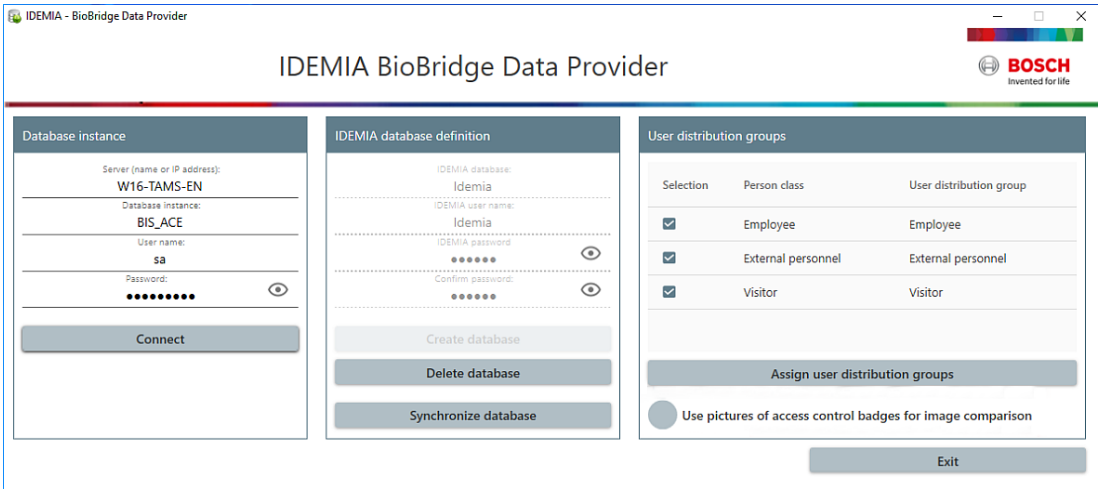
Для Чтобы создать базу данных, связывающую биометрические устройства IDEMIA с системой управления доступом Bosch, в ACS выполняются приведенные ниже действия.
Сопоставляемые базой данных сущности:

- **класс лиц** (Bosch); и
- **группа распределения пользователей** (IDEMIA).

Путь к диалоговому окну

- Главное меню AMS > **Конфигурация (Configuration)** > **Инструменты (Tools)** > **Конфигурация базы данных IDEMIA (IDEMIA database configuration)**

1. Нажмите **Конфигурация базы данных IDEMIA**
   .Откроется диалоговое окно **Поставщик данных BioBridge IDEMIA**.



2. На панели **Экземпляр базы данных**, введите приведенные ниже сведения:

- **Сервер**: имя хоста или IP-адрес компьютера, на котором запущен экземпляр базы данных ACS в SQL Server. Это может быть локальное имя хоста, если SQL Server работает локально.
- **Экземпляр базы данных**: экземпляр ACS (по умолчанию: `ACE`).
- **Имя пользователя**: имя учетной записи администратора экземпляра базы данных ACS (по умолчанию: `sa`).
- **Пароль**: пароль учетной записи администратора, настроенный во время установки ACS.

3. Нажмите **Подключить (Connect)**, чтобы проверить подключение. Пока это не будет сделано, все остальные элементы управления будут недоступны.

На панели «Определение базы данных IDEMIA»

Первые два поля доступны только для чтения:

– **База данных IDEMIA**: имя базы данных, которая объединяет данные Bosch и IDEMIA.
– **Имя пользователя IDEMIA**: имя пользователя базы данных, под учетной записью которого программное обеспечение выполняет команды в базе данных.

1. Введите и подтвердите надежный пароль для учетной записи **Имя пользователя IDEMIA**.
2. Запомните пароль. Он потребуется в последующих задачах конфигурации, его невозможно восстановить в случае потери.
3. Нажмите **Создать базу данных**.
   Если база данных была создана успешно, появится соответствующее сообщение. Нажмите кнопку **OK**
4. После успешного завершения проверки нажмите кнопку **Выход**, чтобы закрыть диалоговое окно.

На панели «Группы распределения пользователей»

Группы распределения пользователей — это объекты MorphoManager, которые сопоставляют пользователей (владельцев учетных данных) с группами биометрических считывателей или клиентами MorphoManager. Они сопоставляются с **классами лиц** системы управления доступом Bosch.

1. В столбце «Выбрать» установите флажок для каждого **класса лиц** ACE, используемого при установке.
2. Для каждой выбранной строки скопируйте имя класса лиц в соответствующую ячейку в столбце **Группы распределения пользователей**.

– Обратите внимание, что названия **класса лиц** и **группы распределения пользователей** должны полностью совпадать.

3. После завершения сопоставления нажмите **Назначить группы распределения пользователей**.

Предоставление идентификационных фотографий для терминала распознавания лиц VisionPass

Чтобы позволить считывателям IDEMIA выполнять распознавание лица по технологии VisionPass с помощью идентификационных фотографий держателей карт из базы данных ACE:

- Нажмите **Использовать для сравнения изображений изображения на бейджах для управления доступом** и подтвердите выбор во всплывающем окне.
  Окно **Поставщик данных BioBridge IDEMIA** подтвердит, что выполняется синхронизация.
  Обратите внимание, что в зависимости от количества используемых изображений передача может занять значительное время.

22.2 Выбор технологий и форматов карт

Введение

Если вы планируете использовать идентификацию с помощью карт, а также биометрическую идентификацию, вы должны создать профиль (или «Профиль Wiegand») в MorphoManager, включающий формат (или форматы) этих карт.

В следующей таблице представлен обзор поддерживаемых форматов. Обратите внимание, что для технологии MIFARE поддерживается только идентификация с использованием CSN.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

Рис. 22.1: Поддерживаемые карты IDEMIA

Общая процедура

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Профиль Wiegand**.
2. Нажмите кнопку **Добавить**, чтобы создать пользовательский профиль Wiegand.
3. В соответствующих диалоговых окнах введите информацию о форматировании и технологии карт, используемых системой.
4. Чтобы использовать в системе недавно заданный профиль Wiegand, введите его имя в поле **Профиль Wiegand** в приведенных ниже диалоговых окнах MorphoManager:

– **Администрирование > Профиль биометрического устройства**.
– **Администрирование > Политика пользователя**.

Mifare Classic CSN

1. Добавьте элемент Wiegand `User CSN Element` и введите приведенные ниже сведения:

– **Имя**: `CSN` (например).
– **Длина:** `32`.
– **Режим трансформации:** `Reversed`.

2. В разделе **Администрирование > Профиль биометрического устройства**на странице **Настройки многофакторного режима** установите флажок **MIFARE Classic**.

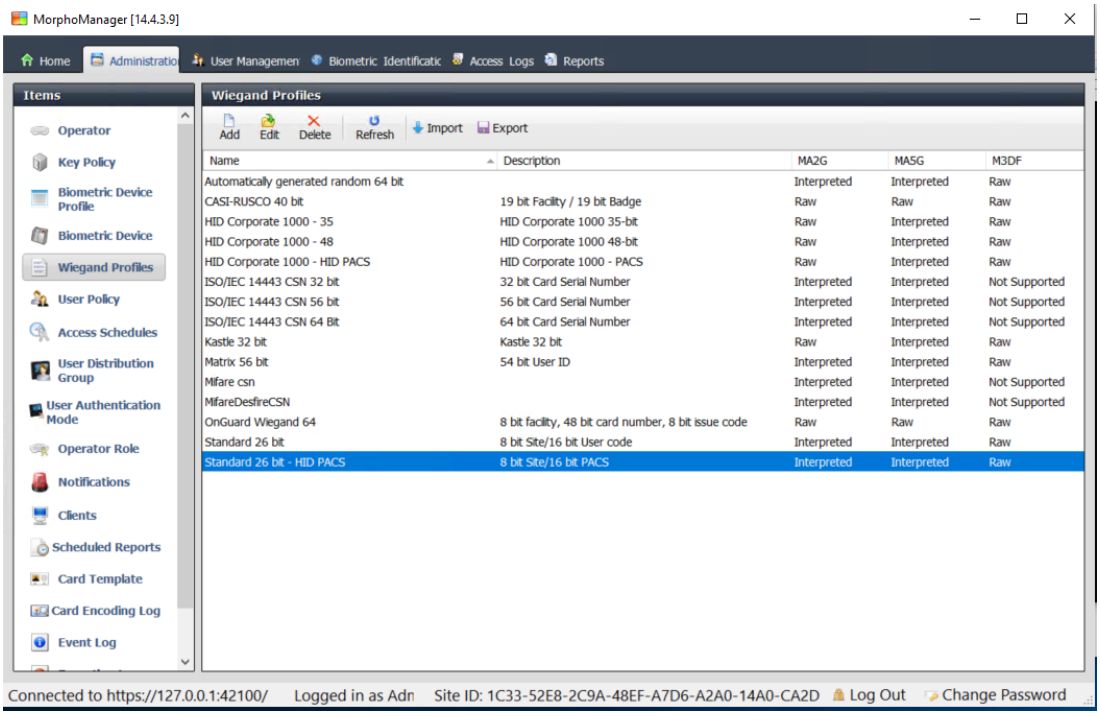
Mifare DESFire CSN

Конфигурация идентична Mifare Classic, за исключением приведенных ниже сведений:

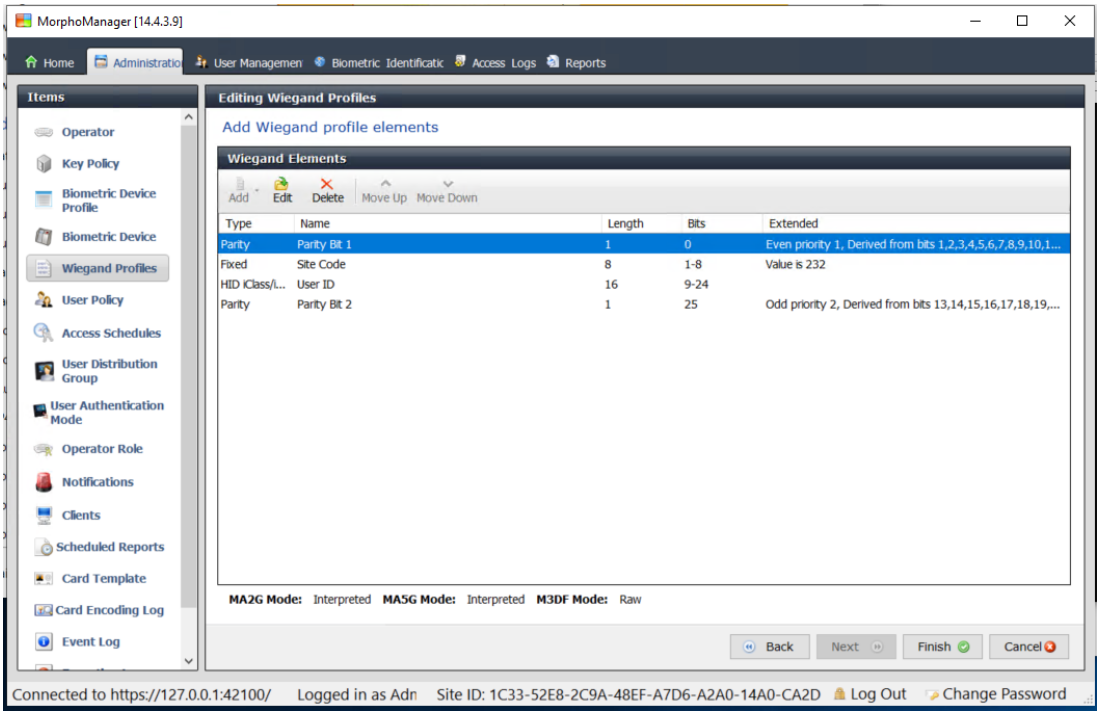
– **Длина:** `56`.
– добавление элемента Wiegand **User CSN Element**:
  – Введите имя в поле **Имя:**.
  – В поле **Длина** введите значение «56».
  – В поле **Режим трансформации:** введите значение `Reversed`.
– В разделе **Администрирование > Профиль биометрического устройства**на странице **Настройки многофакторного режима** установите флажок **Mifare DESFire 3DES**.

iCLASS 26 БИТ

1. Выберите предопределенный профиль `Standard 26 bit-HID PACS`.



2. Нажмите кнопку **Изменить**.
3. Нажмите кнопку **Далее**



4. Нажмите кнопку **Изменить**.
5. Удалите строку `Fixed Facility Code`.
6. Выберите строку `HID iClass SEP User ID`.
7. Нажмите кнопку **Изменить**.
8. Измените длину идентификатора пользователя с `1..16` на `1..24`.
9. В разделе **Администрирование > Профиль биометрического устройства**на странице «Настройки биометрического устройства» в поле «Профиль Wiegand» выберите значение `Standard 26 BIT-HID-PACS`.

10. В разделе **Администрирование > Профиль биометрического устройства** на странице **Настройки многофакторного режима** установите флажок `HID iClass`.
11. Нажимайте кнопку «Далее», пока не перейдете на страницу **Пользовательские параметры**.
12. Нажмите кнопку **Добавить**.
13. Добавьте пользовательский параметр (с учетом регистра) `wiegand.site_code_propagation`.
14. Задайте ему значение `1`.
15. Нажмите кнопку **Готово**.
16. Введите этот заполненный профиль Wiegand в разделе **Администрирование > Политика пользователя**.

iCLASS 35 БИТ

1. Выберите предопределенный профиль `HID Corporate 1000 35 BIT`.
2. Нажмите кнопку **Изменить**.
3. Нажмите кнопку **Далее**
4. Выберите и удалите строку элемента `Fixed Company ID`.
5. Выберите и удалите строку элемента `User Card ID Number`.
6. Добавьте строку элемента `HID iClass/iClass SE PACS Data` и в сведениях об элементе задайте параметры:

– Имя: `Card ID Number`.
– Длина: `32`.
– В разделе **Администрирование > Профиль биометрического устройства** на странице **Настройки многофакторного режима** установите флажок `HID iClass`.
– Нажимайте кнопку **Далее**, пока не перейдете на страницу **Пользовательские параметры**.
– Нажмите кнопку **Добавить**.
– Добавьте пользовательский параметр (с учетом регистра) `wiegand.site_code_propagation`.
– Задайте ему значение `1`.
– Нажмите кнопку **Готово**.
– Введите этот заполненный профиль Wiegand в разделе **Администрирование > Политика пользователя**.

iCLASS 37 БИТ

– **Администрирование > Wiegand**
– Щелкните **Добавить новый профиль**
– **Длина:** `37`.

1. Добавьте четность элемента:

– **Имя**: (например) `EvenParityBit 1`.
– **Приоритет**: `1`.
– **Длина**: `18`.
– **Режим**: `Even`.
– **Базовые биты**: `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18 .`
– Нажмите кнопку **Далее**

2. Добавьте элемент `User HID iClass/iClass SE PACS Data` и в сведениях об элементе задайте параметры:

– **Имя:** `UserID`
– **Длина**: `35`.

– Нажмите кнопку **Далее**
3. Добавьте четность элемента:
– **Имя**: например: `Parity Bits 2`.
– **Приоритет**: `2`.
– **Длина**: `19`.
– **Режим**: `Odd`.
– **Базовые биты**: `19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`.
– Нажмите кнопку **Далее**
– В разделе **Администрирование > Профиль биометрического устройства** на странице **Настройки многофакторного режима** установите флажок `HID iClass`.
– Нажимайте кнопку **Далее**, пока не перейдете на страницу **Пользовательские параметры**.
– Нажмите кнопку **Добавить**.
– Добавьте пользовательский параметр (с учетом регистра) `wiegand.site_code_propagation`.
– Задайте ему значение `1`.
– Нажмите кнопку **Готово**.
– Введите этот заполненный профиль Wiegand в разделе **Администрирование > Политика пользователя**.

iClass 48 БИТ

1. Выберите предопределенный профиль `HID Corporate 1000 48 BIT`.
2. Нажмите кнопку **Изменить**.
3. Нажмите кнопку **Далее**
4. Выберите и удалите строку элемента `Fixed Company ID`.
5. Выберите и удалите строку элемента `User Card ID Number`.
6. Добавьте строку элемента `HID iClass/iClass SE PACS Data` и в сведениях об элементе задайте параметры:
– Имя: `User`.
– Длина: `45`.
7. В разделе **Администрирование > Профиль биометрического устройства** на странице **Настройки многофакторного режима** установите флажок `HID iClass`.
8. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Пользовательские параметры**.
9. Нажмите кнопку **Добавить**.
10. Добавьте пользовательский параметр (с учетом регистра) `wiegand.site_code_propagation`.
– Задайте ему значение `1`.
11. Нажмите кнопку **Готово**.
12. Введите этот заполненный профиль Wiegand в разделе **Администрирование** > **Политика пользователя**.

HID Prox

1. Выберите предопределенный профиль `Standard 26 BIT`.
2. Нажмите кнопку **Изменить**.
3. Нажмите кнопку **Далее**
4. Удалите строку `Fixed Facility Code`.
5. Нажмите кнопку **Изменить**.
6. Измените длину идентификатора пользователя с `1..16` на `1..24`.

7. В разделе **Администрирование > Профиль биометрического устройства**на странице «Настройки биометрического устройства» в поле «Профиль Wiegand» выберите значение `Standard 26 BIT`.
8. В разделе **Администрирование > Профиль биометрического устройства** на странице **Настройки многофакторного режима** установите флажки:

– **Биометрические данные**.
– **Бесконтактная карта**.

9. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Пользовательские параметры**.
10. Нажмите кнопку **Добавить**.
11. Добавьте пользовательский параметр (с учетом регистра) `wiegand.site_code_propagation`.

– Задайте ему значение `1`.

12. Нажмите кнопку **Готово**.
13. Введите этот заполненный профиль Wiegand в разделе **Администрирование** > **Политика пользователя**.

22.3 Выбор режима идентификации

Введение

Биометрические считыватели могут идентифицировать владельца учетных данных различными способами. Эти способы называются режимами идентификации или режимами проверки подлинности.

– По **карте или биометрическим данным** в зависимости от того, что владелец учетных данных представляет считывателю.
– По **карте И биометрическим данным**, т. е. проверка биометрических учетных данных пользователя выполняется, чтобы подтвердить, что данный пользователь является истинным владельцем карты.
– **Только** по **биометрическим данным**.

В этом разделе описана настройка этих режимов в системе MorphoManager.
Обратите внимание, что во всех случаях, когда используются учетные данные на карте, разумеется, необходимо создавать профиль для соответствующих технологии и формата карты.

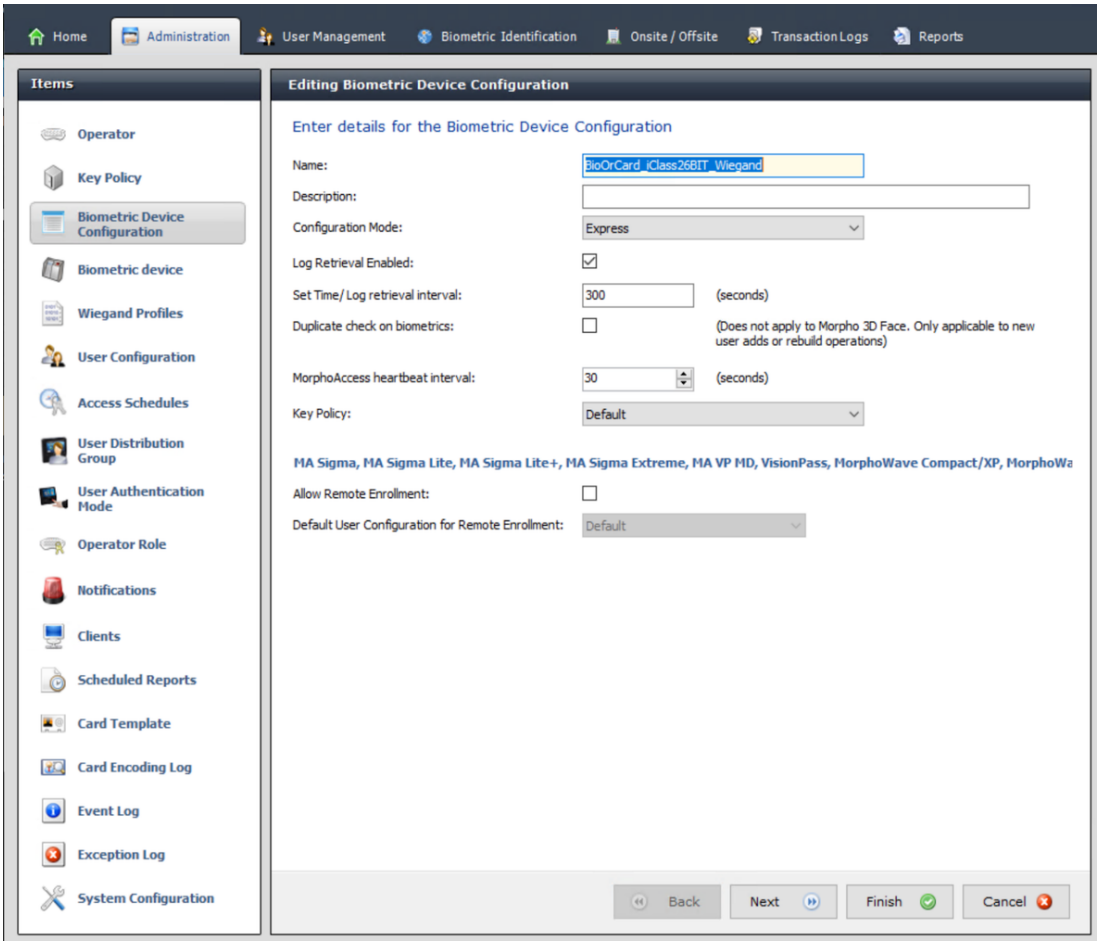
Путь к диалоговому окну

В системе MorphoManager на вкладке **Администрирование**

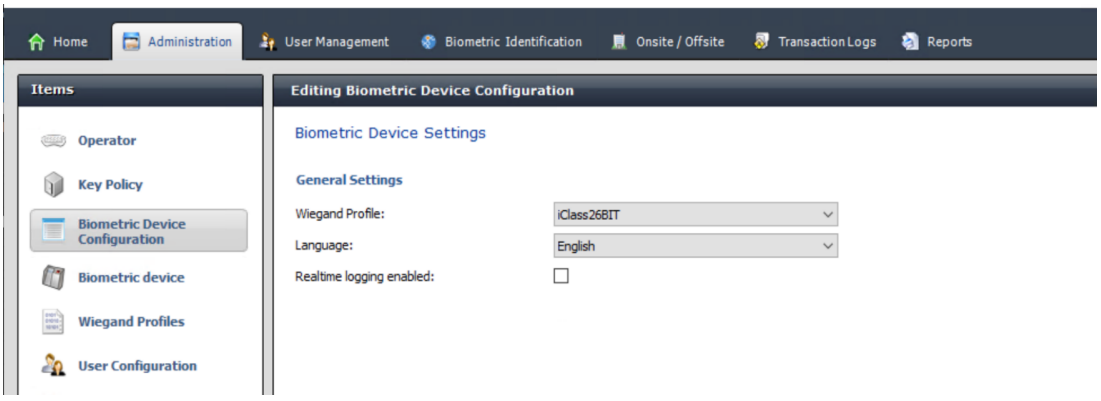
22.3.1 Карта ИЛИ биометрические данные

создайте пользовательский режим проверки подлинности, если пользователи должны идентифицировать себя по карте ИЛИ по биометрическим учетным данным.

1. В системе MorphoManager перейдите к разделу **Администрирование** > **Конфигурация биометрического устройства**.
2. Введите имя конфигурации биометрического устройства, например `CardORBiometric`.

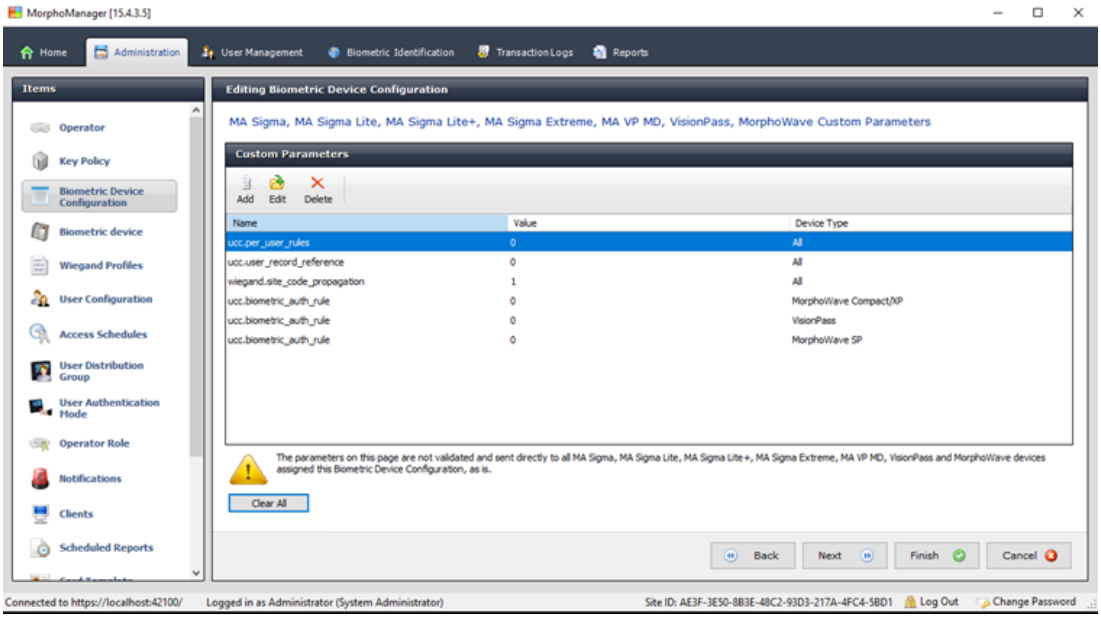


3. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Настройки биометрического устройства**.



4. В поле **Профиль Wiegand** выберите тот же профиль, который вы определили для своих биометрических устройств при настройке BioBridge.
5. Нажимайте **Далее** до тех пор, пока не откроется диалоговое окно **Настройки пороговых значений биометрических учетных данных**.
6. Установите значения параметра **Пороговые значения биометрических учетных данных** в соответствии с локальными условиями и документацией MorphoManager. Значение по умолчанию — `Recommended`.
7. Нажимайте кнопку **Далее**, пока не перейдете на экран **Настройки многофакторного режима**.
8. Установите флажок **Биометрические данные** и флажок для технологию карты, используемую в процессе установки.

9. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Пользовательские параметры**.



10. Для каждого используемого устройства нажмите кнопку **Добавить**, чтобы добавить два пользовательских параметра. (Если заданы эти два параметра, считыватель отправляет данные карты непосредственно в AMC. Пользователей не нужно регистрировать в считывателе IDEMIA).

– `ucc.per_user_rules`
– `ucc.user_record_reference`

11. Для считывателей WAVE и VisionPass добавьте еще один параметр:

– `ucc.biometric_auth_rule=0`
– Выберите значение параметра **Тип устройства** `MorphoWave Compact/XP`, `MorphoWave SP` или `VisionPass`.

12. Нажмите кнопку **Готово**.

Назначьте пользователям этот режим проверки подлинности пользователей.

В ACS необходимо назначить карту с допустимым описанием каждом держателю карты.

1. В системе MorphoManager перейдите к разделу **Администрирование** > **Режим проверки подлинности пользователя**.
2. Задайте следующие атрибуты**:**

– Установите переключатель **Режим** в положение `Enabled`.
– Установите в списке **Расположение шаблона** параметр `Download to Device`.
– Установите флажок **Разрешить запуск по биометрическим данным**.
– Установите флажок **Разрешить запуск по бесконтактной карте**.
– Выключите функцию **Требовать соответствие шаблона**.

3. Перейдите в радел **Администрирование** > **Конфигурация пользователей**.
4. Нажмите кнопку **Добавить**.
5. Выберите имя **режима проверки подлинности пользователя**, созданного вами ранее для карты или биометрических учетных данных.
6. Нажмите кнопку **Готово**.

См.

– *Выбор технологий и форматов карт, Страница 166*

22.3.2 Карта И биометрические данные

Выполните приведенные ниже настройки, пользователи должны идентифицировать себя по карте И биометрическим учетным данным, чтобы убедиться, что они являются владельцами карты.

1. В системе MorphoManager перейдите к разделу **Администрирование** > **Конфигурация биометрического устройства**.
2. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Настройки биометрического устройства**.
3. В поле **Профиль Wiegand** выберите тот же профиль, который вы определили для своих биометрических устройств при настройке BioBridge.
4. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Настройки многофакторного режима**.
5. Установите флажок для технологии карт, используемой при установке.
6. Нажмите кнопку **Готово**.

Назначьте пользователям этот режим проверки подлинности пользователей.

В ACS необходимо назначить карту с допустимым описанием каждом держателю карты.

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Конфигурация пользователей**.
2. В поле **Режим проверки подлинности пользователя** выберите значение `Contactless Card ID + Biometric` из списка.
3. Нажмите кнопку **Готово**.

См.

– *Выбор технологий и форматов карт, Страница 166*

22.3.3 Только биометрические данные

Выполните приведенные ниже настройки, если пользователи должны идентифицировать себя только с помощью биометрических учетных данных.

1. В системе MorphoManager перейдите к разделу **Администрирование** > **Конфигурация биометрического устройства**.
2. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Редактирование конфигурации биометрического устройства**.
3. В поле **Профиль Wiegand** выберите тот же профиль, который вы определили для своих биометрических устройств при настройке BioBridge.
4. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Настройки многофакторного режима**.
5. В поле **Многофакторный режим** выберите значение `Biometric only` из списка.
6. Нажмите кнопку **Готово**.

Назначьте пользователям этот режим проверки подлинности пользователей.

В ACS необходимо назначить карту с допустимым описанием каждом держателю карты.

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Конфигурация пользователей**.
2. В поле **Режим проверки подлинности пользователя** выберите значение `Biometric(1:many)` из списка.

3. Нажмите кнопку **Готово**.

22.4 Настройка интерфейса BioBridge в системе MorphoManager

Предварительные требования

Система управления доступом MorphoManager установлена на сервере MorphoManager в вашей сети. См. Руководство по установке MorphoManager и интерактивную справку.

Обзор

Чтобы использовать интерфейс BioBridge между системами управления доступом Bosch и MorphoManager необходимо настроить приведенные ниже параметры в системе MorphoManager:

- **Конфигурация биометрического устройства**
- **Биометрическое устройство**
- **Профили Wiegand**
- **Конфигурация пользователей**
- **Группа распределения пользователей**
- **Режим проверки подлинности пользователя**
- **Конфигурация системы**

Кроме того, необходимо настроить протокол ODBC (Open Database Connectivity) для связи между интерфейсом BioBridge системы Morphomanager и базой данных, которую она использует совместно с ACS.

Все эти задачи конфигурации описаны в следующих разделах.

22.4.1 Конфигурация биометрического устройства

Конфигурация биометрического устройства определяет общие настройки и параметры для одного или нескольких биометрических устройств. Конфигурация биометрического устройства применяется к биометрическим устройствам в системе при их добавлении на вкладке **Администрирование** в разделе **Биометрическое устройство**.

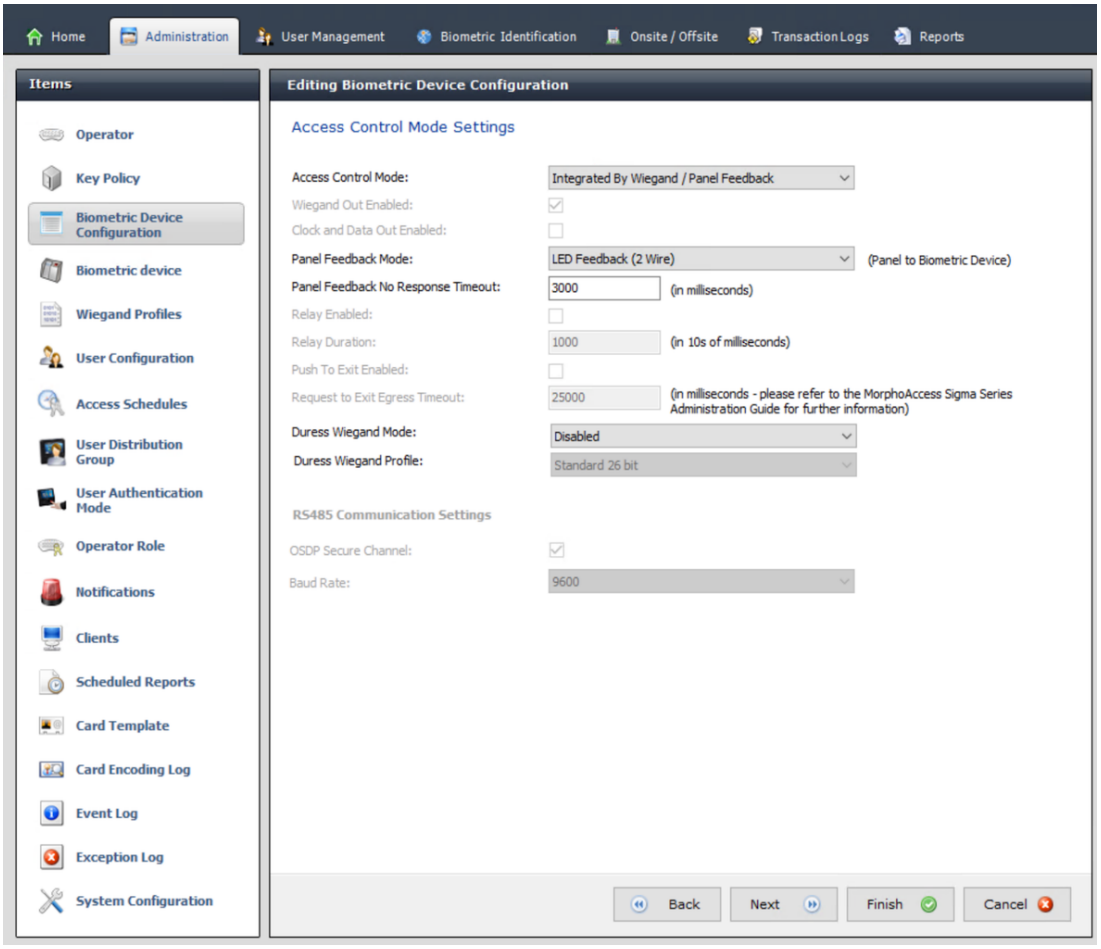
В следующей процедуре предполагается, что развертывание биометрических считывателей от IDEMIA выполняется с дополнительной технологией считывания карт.

Процедура

1. В MorphoManager перейдите в раздел **Администрирование** > **Конфигурация биометрического устройства**.
2. Нажмите **Добавить**, чтобы создать новую конфигурацию биометрического устройства.
3. На следующем экране введите имя и описание (необязательно) профиля. Если вы не используете поле описания, рекомендуем использовать имя, описывающее тип и режимы идентификации (биометрия и (или) карта) группы считывателей.
4. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Настройки биометрического устройства**.

– Выберите профиль Wiegand, который был создан ранее для установки.

5. Нажимайте кнопку **Далее**, пока не перейдете на страницу **Параметры режима управления доступом**.



Далее настройка Wiegand и контроллеров AMC по протоколу OSDP выполняется по отдельности. Выполните описанную ниже процедуру, соответствующую типу контроллера AMC:

Для контроллеров AMC Wiegand

1. В поле **Режим управления доступом** установите значение `Integrated by Wiegand`.
2. В поле **Режим обратной связи с панелью** установите значение `LED Feedback (2 wire)`.
3. Нажмите кнопку **Готово**.

Для контроллеров AMC OSDP

1. В поле **Режим управления доступом** установите значение `Integrated by OSDP`.
2. В поле **Режим обратной связи с панелью** установите значение `LED Feedback (2 wire)`.
3. Установите флажок **Безопасный канал OSDP**
4. Установите скорость передачи данных `9600`
5. Дополнительные сведения см. в разделе **Биометрическое устройство**
6. Нажмите кнопку **Готово** , чтобы выйти из MorphoManager.

Устранение неисправностей ключей OSDP

Если невозможно установить защищенное соединение со считывателем OSDP, попробуйте переустановить базовый ключ следующим образом:

1. Запустите отдельную программу **MorphoBioToolBox (MBTB)**.
2. В программе MorphoBioToolBox перейдите в меню **Настройки устройства** > **Сбросить**
3. Выберите базовый ключ OSDP
4. Нажмите **Сбросить криптографические ключи**
5. Выйдите из MorphoBioToolBox

В более сложных случаях обратитесь в службу технической поддержки IDEMIA.

См.

– *Биометрическое устройство, Страница 177*

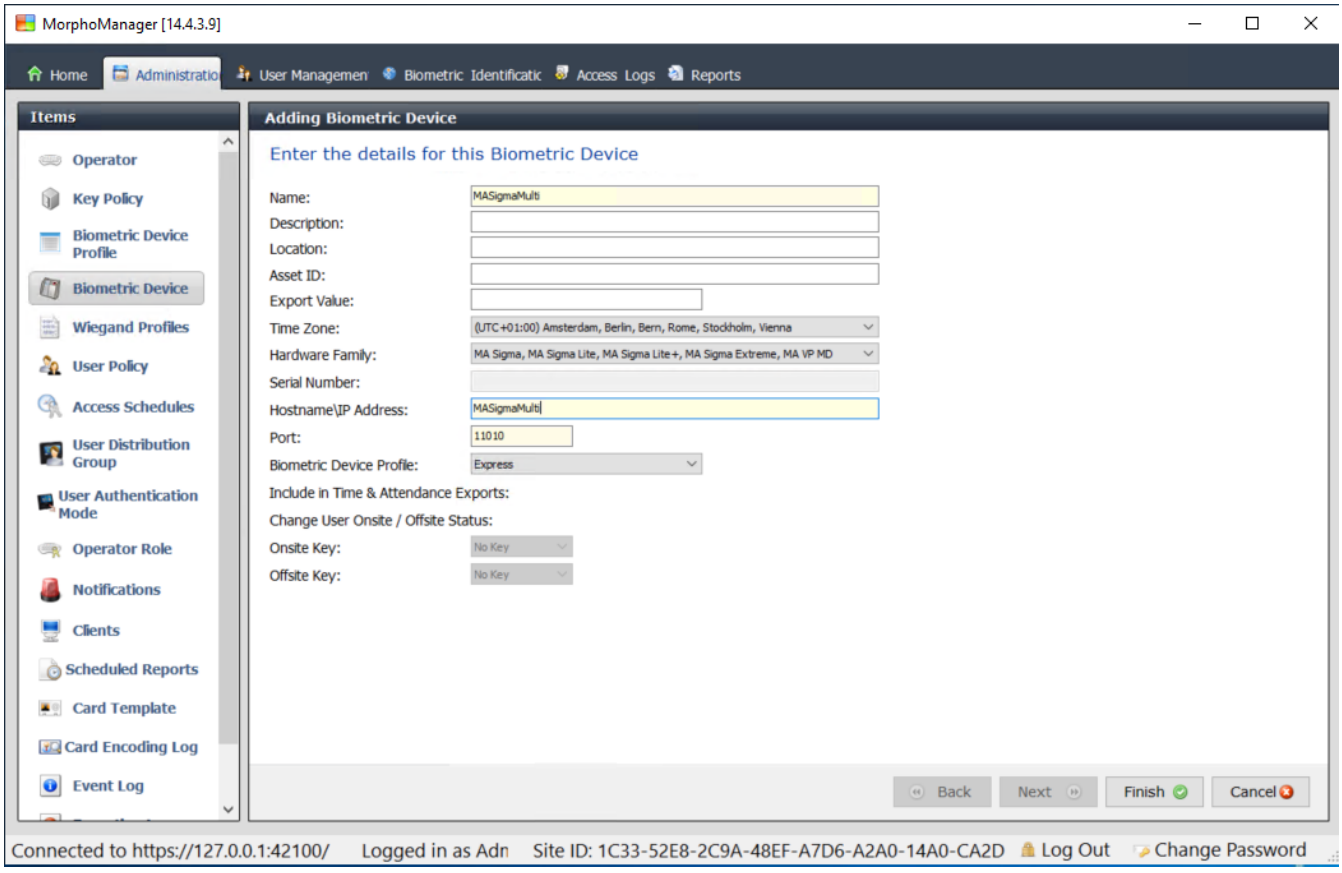
22.4.2 Биометрическое устройство

Биометрические устройства проверяют, совпадают ли считанные биометрические учетные данные с записями в базе данных. Они также ведут журнал всех событий использования.

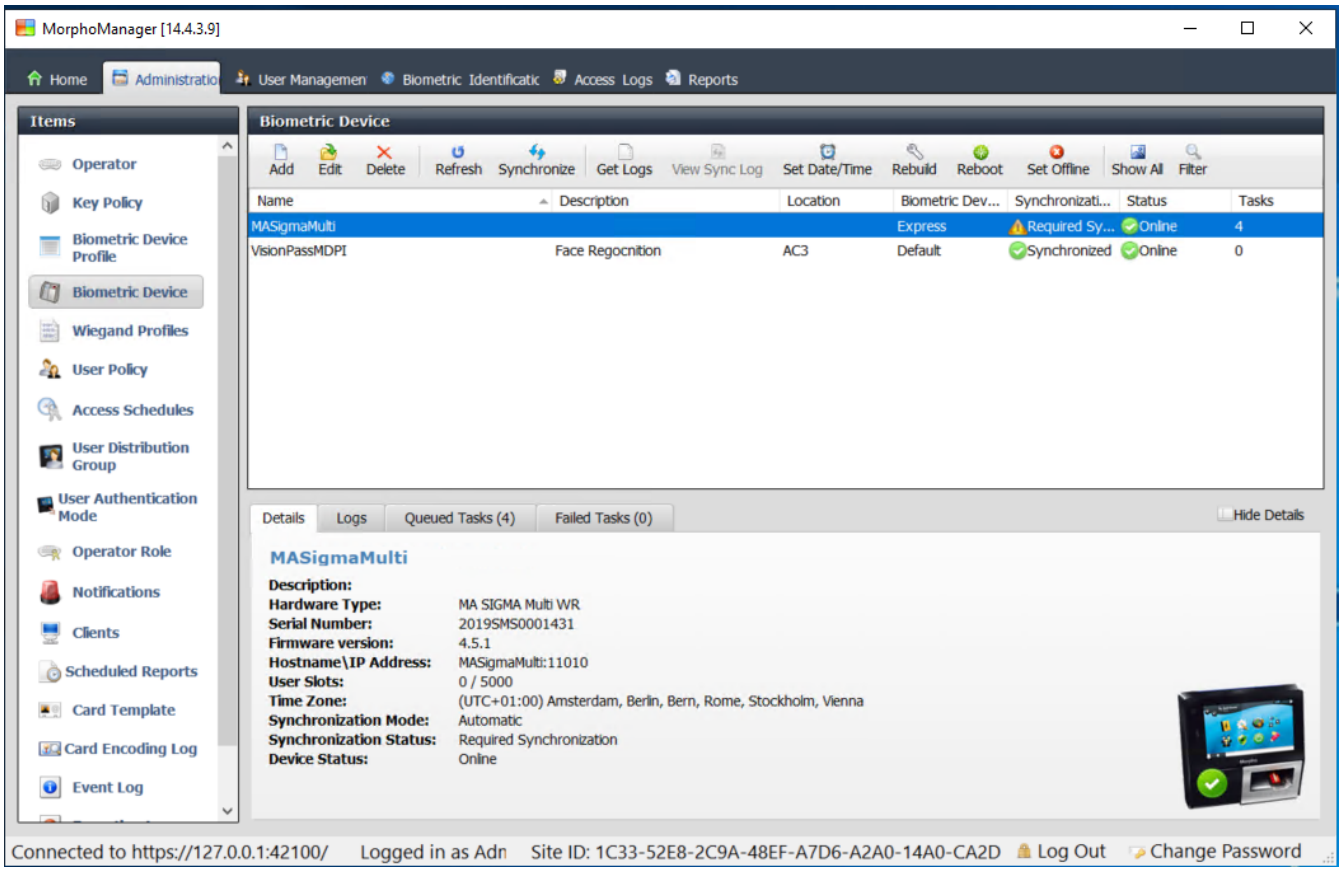
Процедура

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Биометрическое устройство**.
2. Нажмите **Добавить**, чтобы создать новое биометрическое устройство.
3. Введите как минимум основные сведения об устройстве:

– (из списка) **Семейство оборудования**;
– **имя хоста/IP-адрес**;
– (из списка) определенную ранее **конфигурацию биометрического устройства**.



4. Нажмите **Готово**
   В диалоговом окне «Биометрическое устройство» теперь указываются все настроенные устройства:

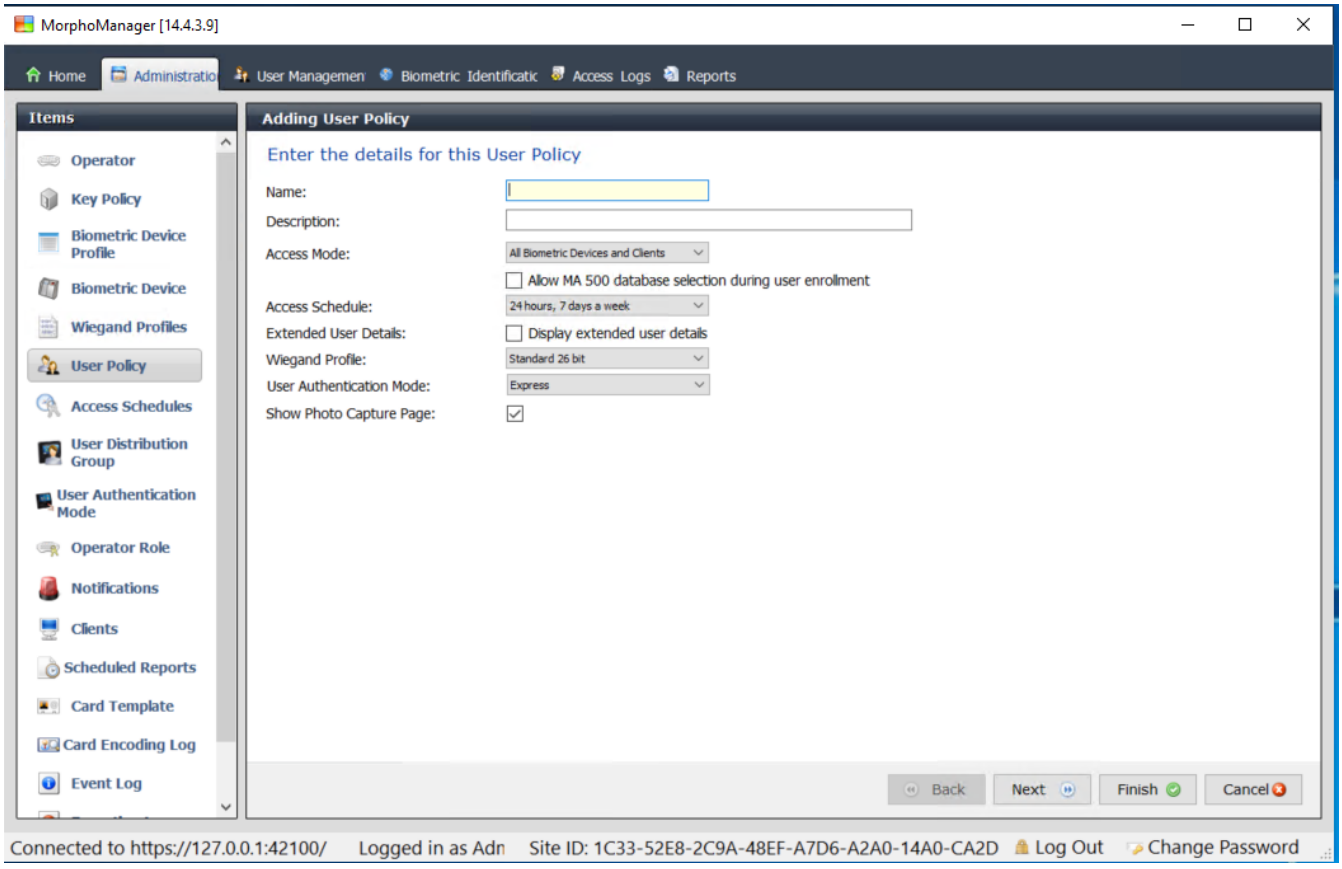


22.4.3 Конфигурация пользователей

Конфигурации пользователей — это наборы прав доступа, назначенные пользователям, которым предъявляются одинаковые требования для получения доступа, то есть в них описывается какие биометрические устройства разрешено использовать пользователям, в каких режимах и в какое время.

Процедура

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Конфигурация пользователей**.
2. Нажмите **Добавить**, чтобы создать новую конфигурацию пользователя.



3. В диалоговом окне **Добавление политики пользователя** введите:
- **Название** политики пользователя и описание (необязательно).
- **Режим доступа**: `Per User`.
- **Расписание доступа**, определяющее дни и время, в которые доступ разрешен.
- **Профиль Wiegand**, определенный и использованный для **Профиля биометрического устройства**.
- **Режим проверки подлинности пользователя**, в зависимости от того, как пользователи устройства будут использовать устройства (по отпечатку пальца, пальцу, лицу, картам и т. д.). Подробнее см. в разделе **Выбор режима идентификации**.

4. Нажмите кнопку **Готово**.

Режим проверки подлинности пользователя в политике пользователя по умолчанию: `(1: Many)`. Чтобы использовать другие режимы проверки подлинности, создайте дополнительные политики пользователя. Подробные сведения о различных свойствах, которые можно назначить политике пользователя, см. в «Руководстве пользователя MorphoManager».

См.
- *Выбор режима идентификации, Страница 171*

22.4.4 Группы распределения пользователей

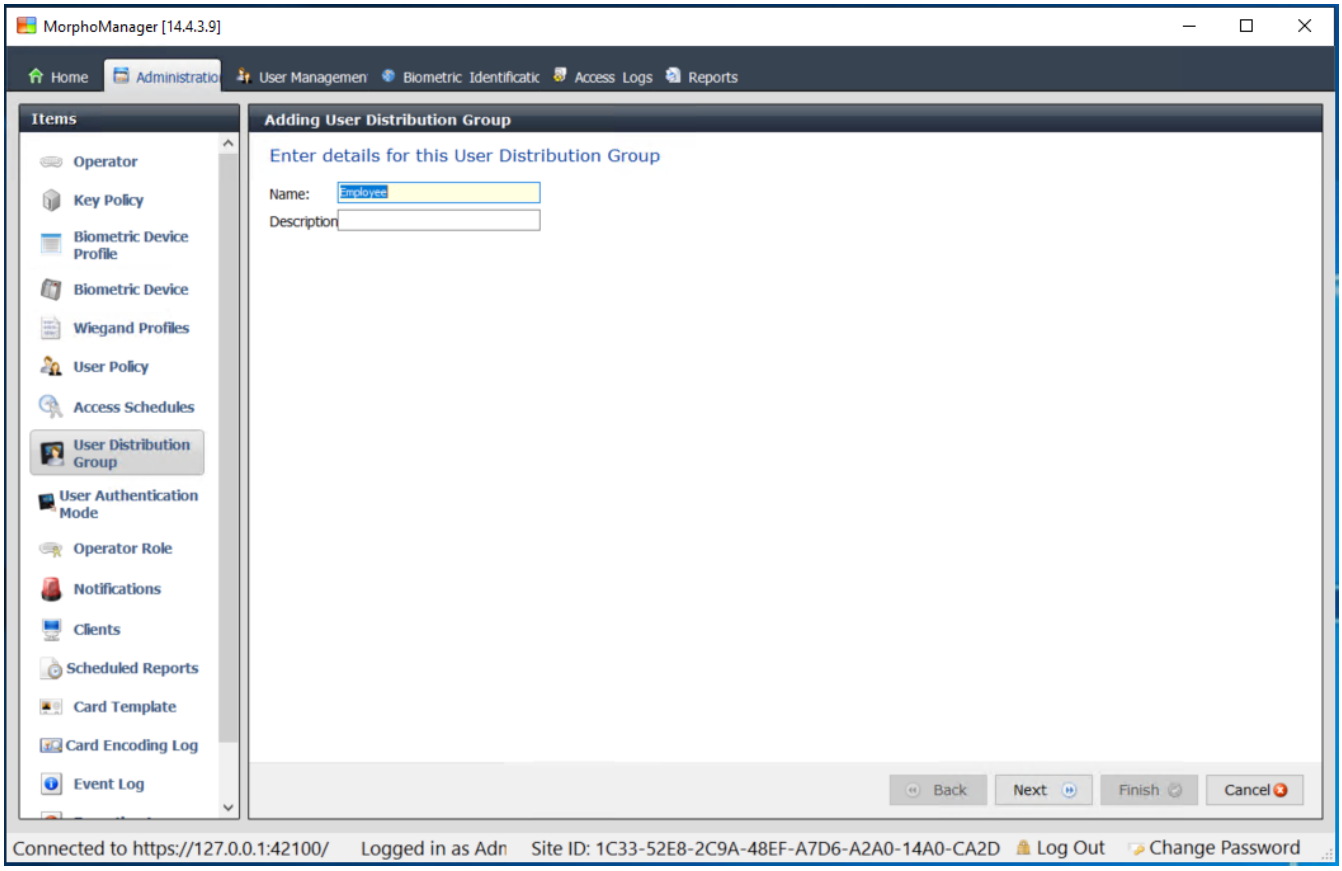
Группы распределения пользователей служат для сопоставления пользователей с группами биометрических считывателей или клиентов MorphoManager.

Требования

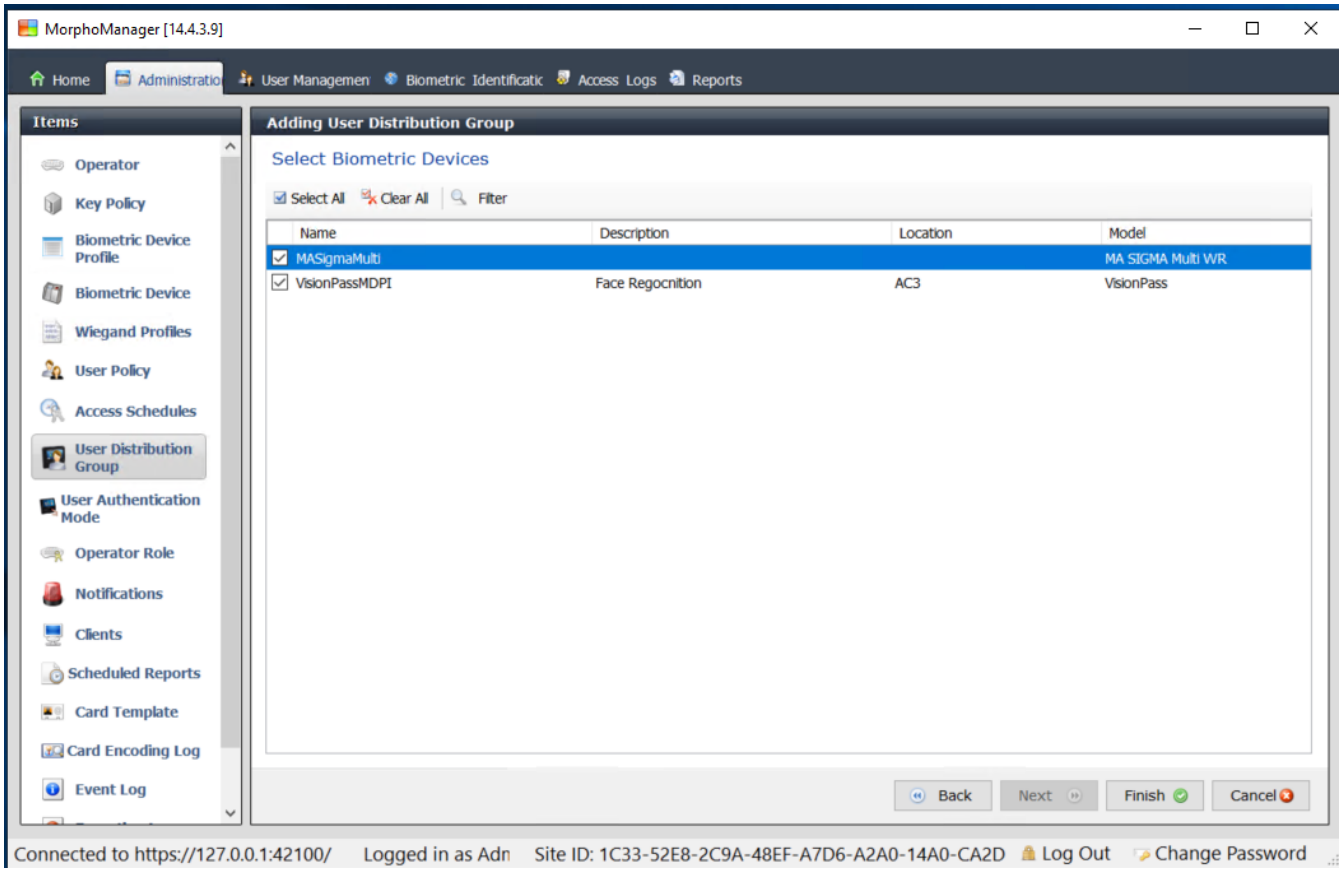
Каждая группа распределения пользователей должна быть сопоставлена хотя бы с одним классом лиц (Person Class) в ACS. Поэтому создайте хотя бы одну группу распределения пользователей для каждого используемого класса лиц.

Процедура

1. В системе MorphoManager перейдите в раздел **Администрирование (Administration)** > **Группа распределения пользователей (User Distribution Group)**.
2. Нажмите **Добавить (Add)**, чтобы создать новую группу распределения пользователей.



3. Нажимайте кнопку **Далее (Next)**, пока не перейдете на страницу **Выбор биометрических устройств (Select Biometric Devices)**.
4. Установите флажки для тех биометрических устройств, которые будут использоваться людьми в этой группе распределения пользователей.



5. Нажмите кнопку **Готово**.

22.4.5 Настройка интерфейса ODBC для клиента BioBridge

Введение

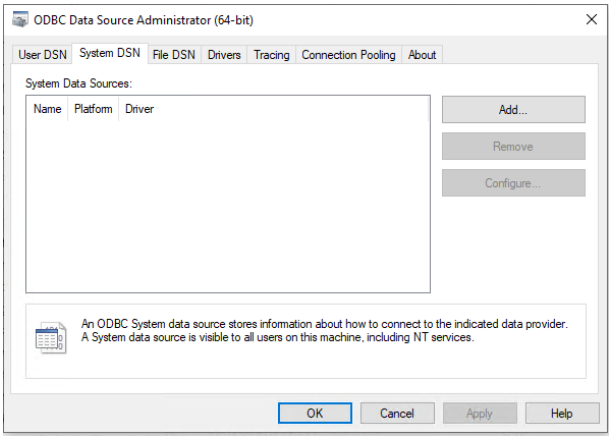
Интерфейс Open Database Connectivity (ODBC) — необходимое условие для использования клиента BioBridge системы MorphoManager. ODBC — это стандартизированный программный интерфейс для доступа к различным базам данных.
Рекомендуемый драйвер — `OdbCDriver17SQLServer`

- В случае с BIS драйвер находится на установочном носителе BIS в расположении `BIS\3rd_Party\OdbCDriver17SQLServer`
- В случае с AMS драйвер нужно скачать на сайте `www.microsoft.com`

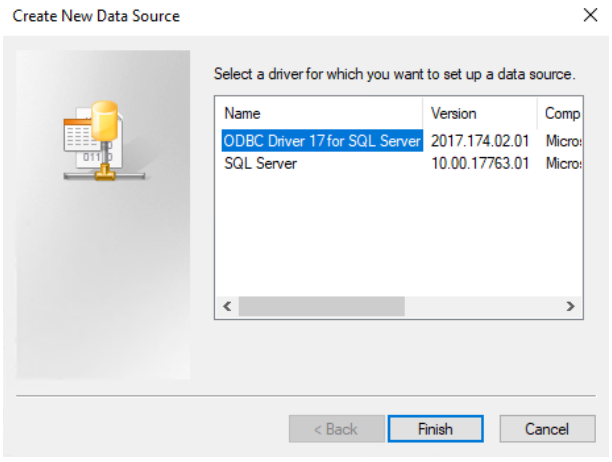
Создание источника данных

Создание имени источника данных (DSN) для ODBC

1. На панели управления Windows выберите **Администрирование**.
2. Выберите `ODBC Data Sources (64-bit)` из списка.
3. Выберите вкладку **Система DSN**.

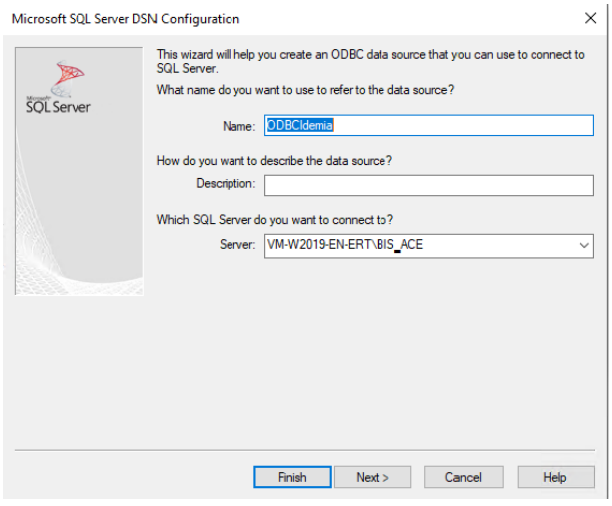


4. Нажмите **Добавить**, чтобы выбрать драйвер.
5. Выберите драйвер `ODBC Driver 17 for SQL Server` и нажмите кнопку **Готово**.

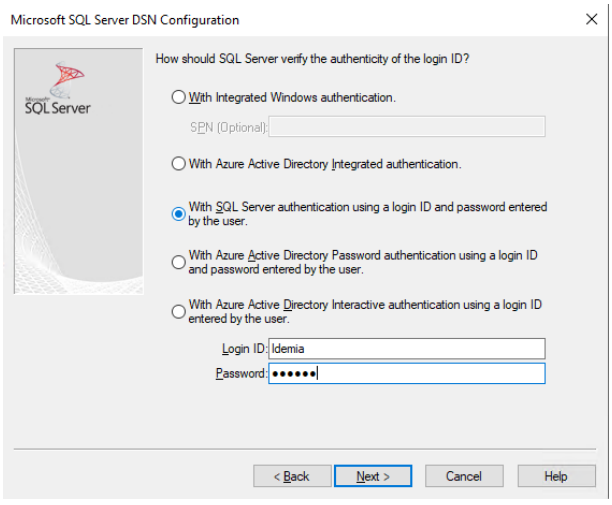


6. Введите приведенные ниже сведения для источника данных.

– **Имя**: имя источника данных.
– **Описание** (необязательно).
– **Сервер**: имя компьютера, на котором ACE установлена база данных, и имя базы данных (по умолчанию: <MyACS server>\`ACE`)



7. Нажмите кнопку **Далее >**
, откроется диалоговое окно сбора информации для входа.



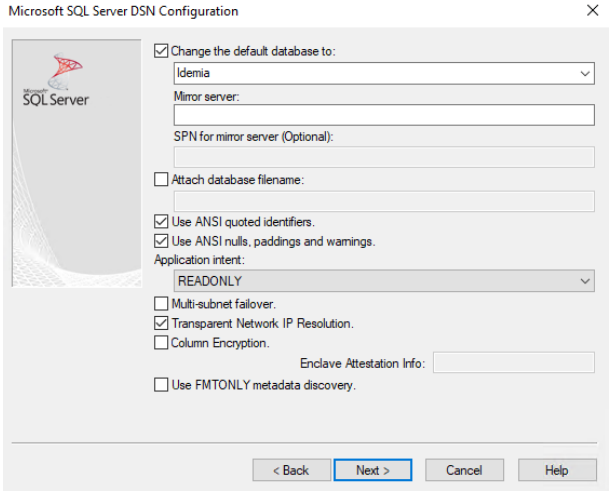
8. Выберите **С аутентификацией в SQL Server с использованием идентификатора входа...**.
9. Введите следующую информацию:

– **Идентификатор входа**: имя пользователя базы данных IDEMIA, настроенное в ACS. Оно всегда обозначается как `Idemia`.
– **Пароль**: пароль, установленный для пользователя базы данных IDEMIA, при настройке в ACS.

10. Нажмите кнопку **Далее >**.
11. В следующем диалоговом окне установите флажки:

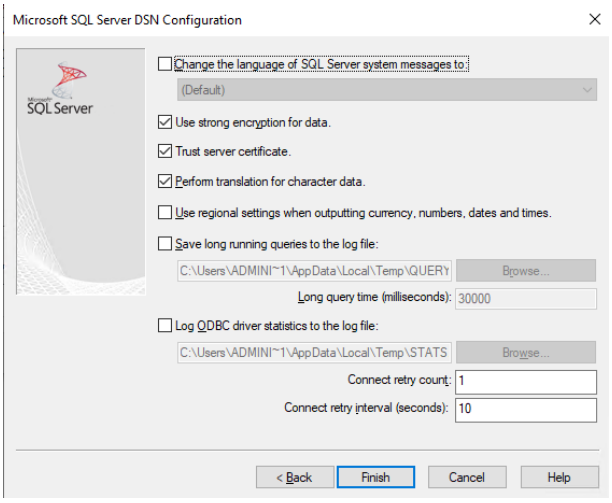
– **Изменить базу данных по умолчанию на:** и выберите `Idemia` .
– **Использовать идентификаторы в кавычках ANSI**.
– **Использовать значения NULL, поля и предупреждения в формате ANSI**.
– **Разрешение IP-адреса прозрачной сети**.

12. Задайте в поле **Цель приложения** установите значение `READONLY`.

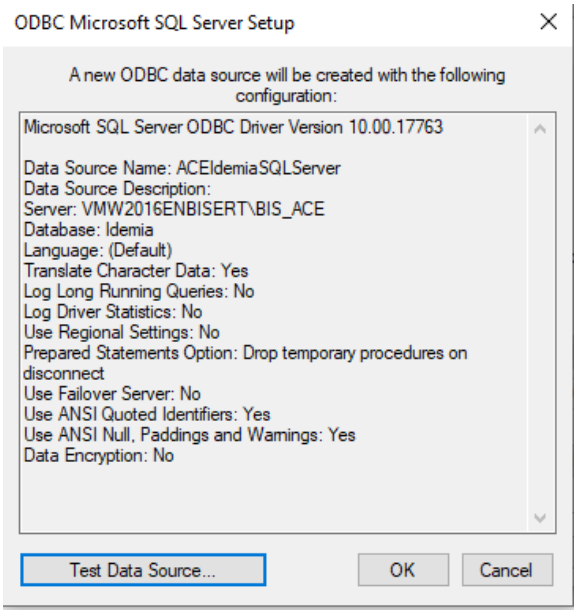


13. Нажмите кнопку **Далее >**.
14. В следующем диалоговом окне установите флажки:

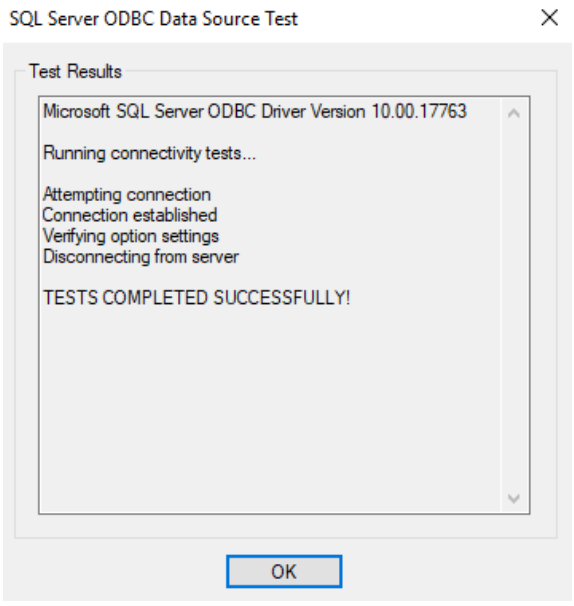
– **Использовать надежное шифрование данных**.
– **Выполнять перевод символьных данных**.
– **Доверенный сертификат сервера**.



15. Нажмите кнопку **Готово**.
16. В следующем диалоговом окне просмотрите сведенные данные.



17. Нажмите **Проверить источник данных...** и убедитесь, что проверка успешно завершена.



18. Сохраните все изменения и закройте мастер установки ODBC.

22.4.6 конфигурация системы BioBridge.

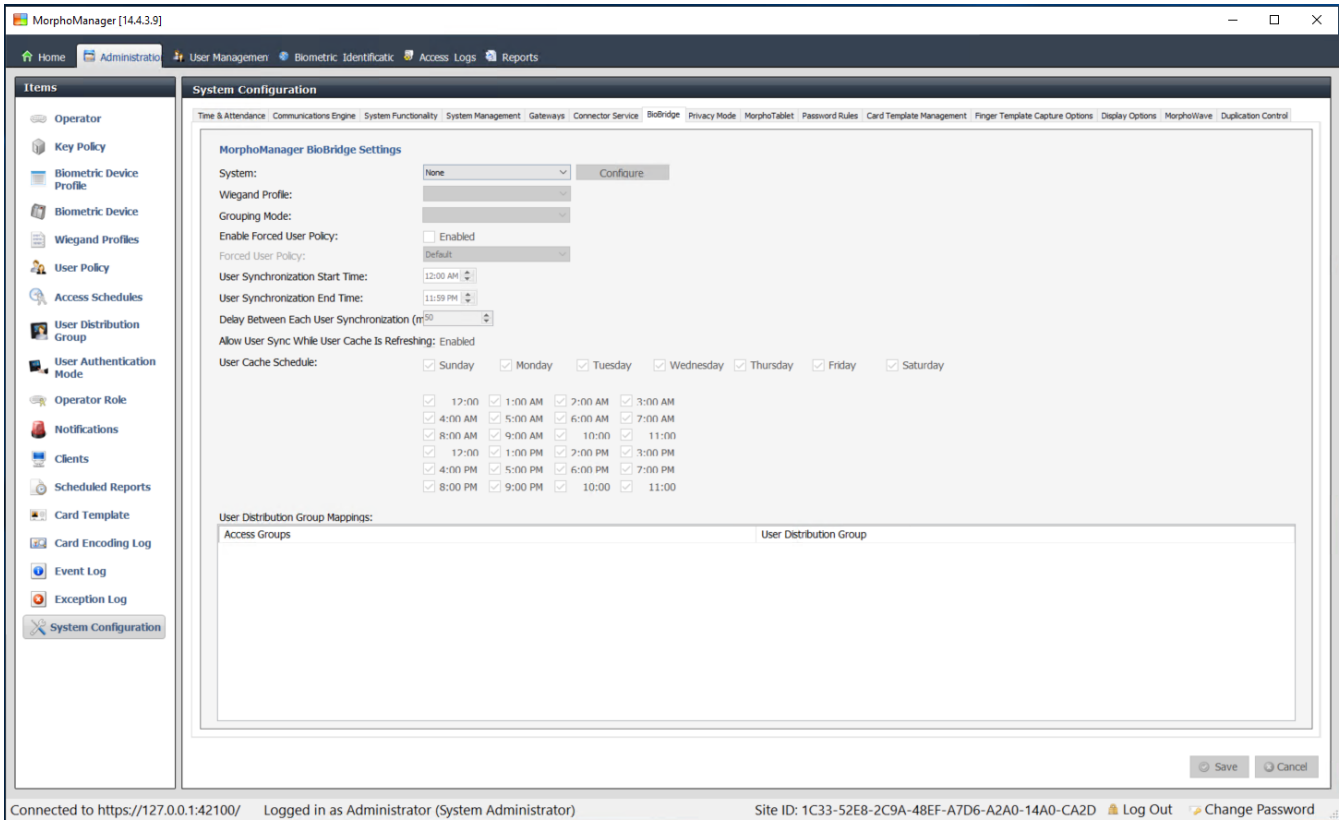
В этом разделе описываются остальные параметры, необходимые для использования интерфейса BioBridge систем управления доступом.

Предварительное требование

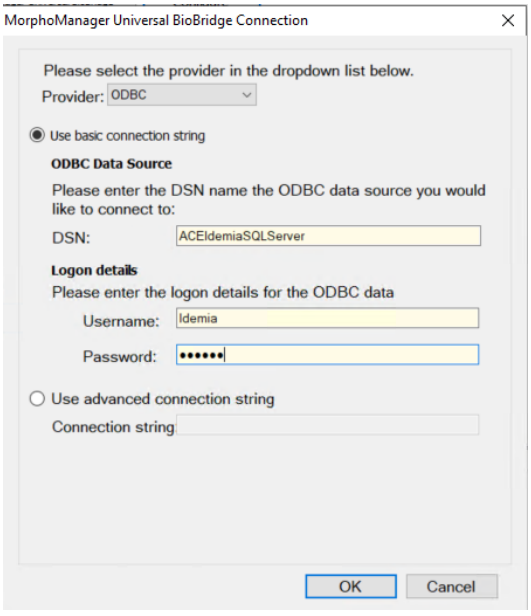
ODBC настроен для BioBridge. См. раздел *Настройка интерфейса ODBC для клиента BioBridge, Страница 181*.

Процедура:

1. В системе MorphoManager перейдите в раздел **Администрирование** > **Конфигурация системы**.
2. Перейдите на вкладку **BioBridge**.



3. В раскрывающемся списке **Система**, выберите `MorphoManager Universal BioBridge`.
4. Нажмите **Настроить** .Отобразится всплывающее окно.



Во всплывающем окне

1. В раскрывающемся списке **Поставщик**, выберите `ODBC`.
2. Введите имя источника данных (DSN) из программы установки ODBC.
3. В разделе **Данные для входа** введите имя пользователя (`Idemia`) и пароль, указанный в программе установки ODBC.
4. Нажмите кнопку **ОК**, чтобы вернуться в диалоговое окно **Конфигурация системы**.

В диалоговом окне **Конфигурация системы**

1. В поле **Профиль Wiegand**: выберите из списка определенный ранее профиль Wiegand.

Режим группирования:

Этот параметр определяет, как MorphoManager должен сопоставлять пользователей MM Universal BioBridge с группами распределения пользователей MorphoManager. Выберите один из параметров:

– **Автоматический**: этот режим автоматически сопоставляет **группы уровня доступа** из MM Universal BioBridge с **группами распределения пользователей** В системе MorphoManager, если у них одинаковое соглашение об именовании.
– **Ручной**: если **группы уровней доступа** в MM Universal BioBridge и **группы распределения пользователей** в MorphoManager не совпадают, можно выполнить сопоставление вручную в разделе **Сопоставление политик пользователя**.

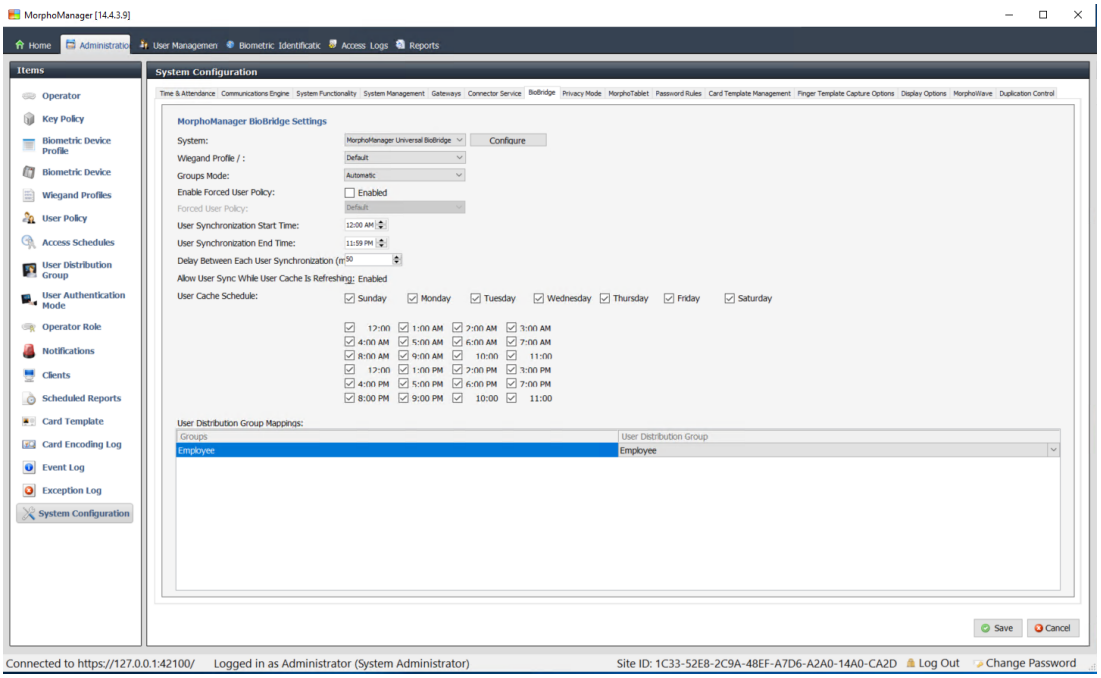
Другие параметры

В большинстве случаев для приведенных ниже параметров можно оставить значения по умолчанию:

Включить принудительную политику пользователя	Если этот параметр выбран, все пользователи, зарегистрированные в клиенте регистрации BioBridge, получат политику пользователя, выбранную из соседнего списка. Если этот флажок установлен, используйте политику пользователя с именем `Per User`.
Время начала и окончания синхронизации пользователей	Обработчику синхронизации пользователей может быть запущен только в этот период времени.
Задержка между синхронизацией каждого пользователя	Временной интервал между синхронизациями пользователей. Увеличение продолжительности задержки сэкономит системные ресурсы, но увеличит время обновления для всех пользователей.
Разрешить синхронизацию пользователей во время обновления кэша пользователя	Если этот параметр включен, обработчик синхронизации пользователей будет работать параллельно с обновлением кэша пользователя. Это очень затратно для системных ресурсов. Рекомендуется отключить этот параметр при использовании больших баз данных.
Расписание обновления кэша пользователя	Дни и время, когда можно обновлять кэш пользователя. Для максимальной точности следует обновлять его постоянно, но для увеличения производительности систем с большими базами данных требуется ввести ограничение.

Сопоставления групп распределения пользователей

– В таблице сопоставлений проверьте, чтобы все **группы** (**классы лиц**, определенные в ACS) были сопоставлены с **группами распределения пользователей** (определенными в MorphoManager).



22.5 Настройка клиента регистрации BioBridge

Введение

Клиент регистрации BioBridge — это компьютер, на котором можно создавать биометрические записи для пользователей системы управления доступом. Настройка клиента регистрации BioBridge состоит из трех частей:

- Добавление оператора регистрации в систему MorphoManager
- Настройка клиентских компьютеров MorphoManager для задач регистрации
- Проверка клиента регистрации

Предварительные требования

Клиент BioBridge системы MorphoManager установлен на каждой рабочей станции ACE, на которой вы проходите биометрическую регистрацию для входа в системы IDEMIA.

22.5.1 Добавление оператора регистрации в систему MorphoManager

Процедура

Следуйте инструкциям, приведенным в «Руководстве по установке клиента MorphoManager».

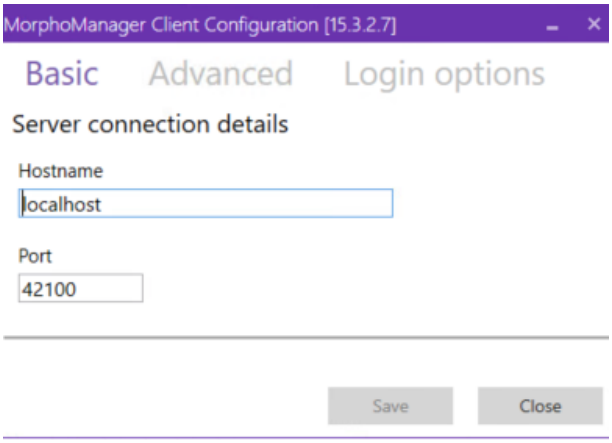
Примечание. В целях безопасности рекомендуется использовать учетные записи пользователей Active Directory.

22.5.2 Настройка клиентских компьютеров MorphoManager для задач регистрации

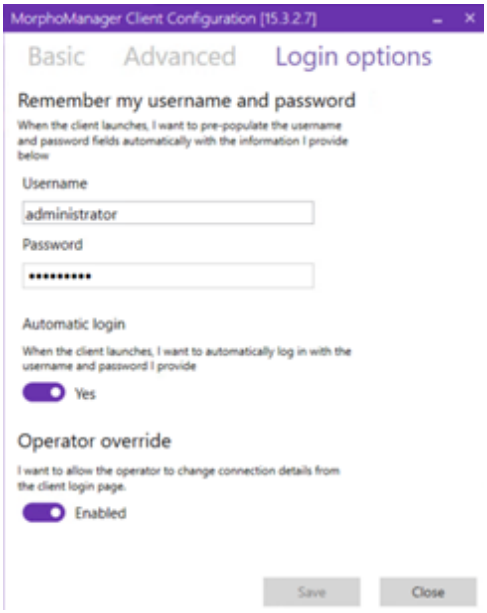
Выполните эту процедуру на каждом компьютере, который вы хотите использовать для регистрации биометрических данных.

Процедура

1. В каталоге установки MorphoManager (по умолчанию: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\ `) запустите файл `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` от имени администратора.



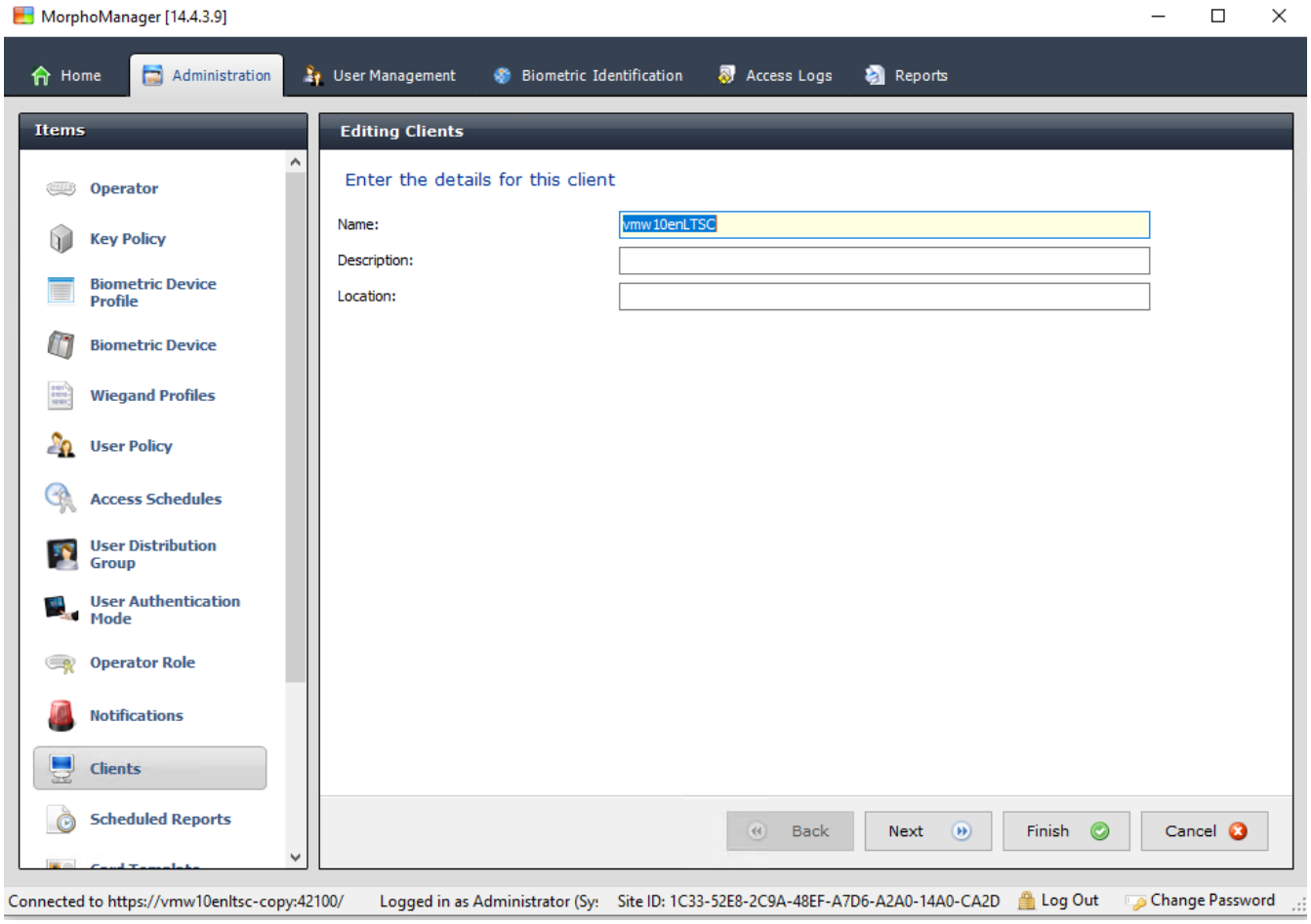
2. На вкладке **Общие** введите имя хоста сервера Morpho в поле **Имя узла**.
3. Для безопасных установок используйте Active Directory или собственное имя пользователя и пароль в соответствии с документацией по Morpho.
4. Или же (НЕ рекомендуется для установок с повышенной степенью безопасности) на вкладке **Параметры входа**



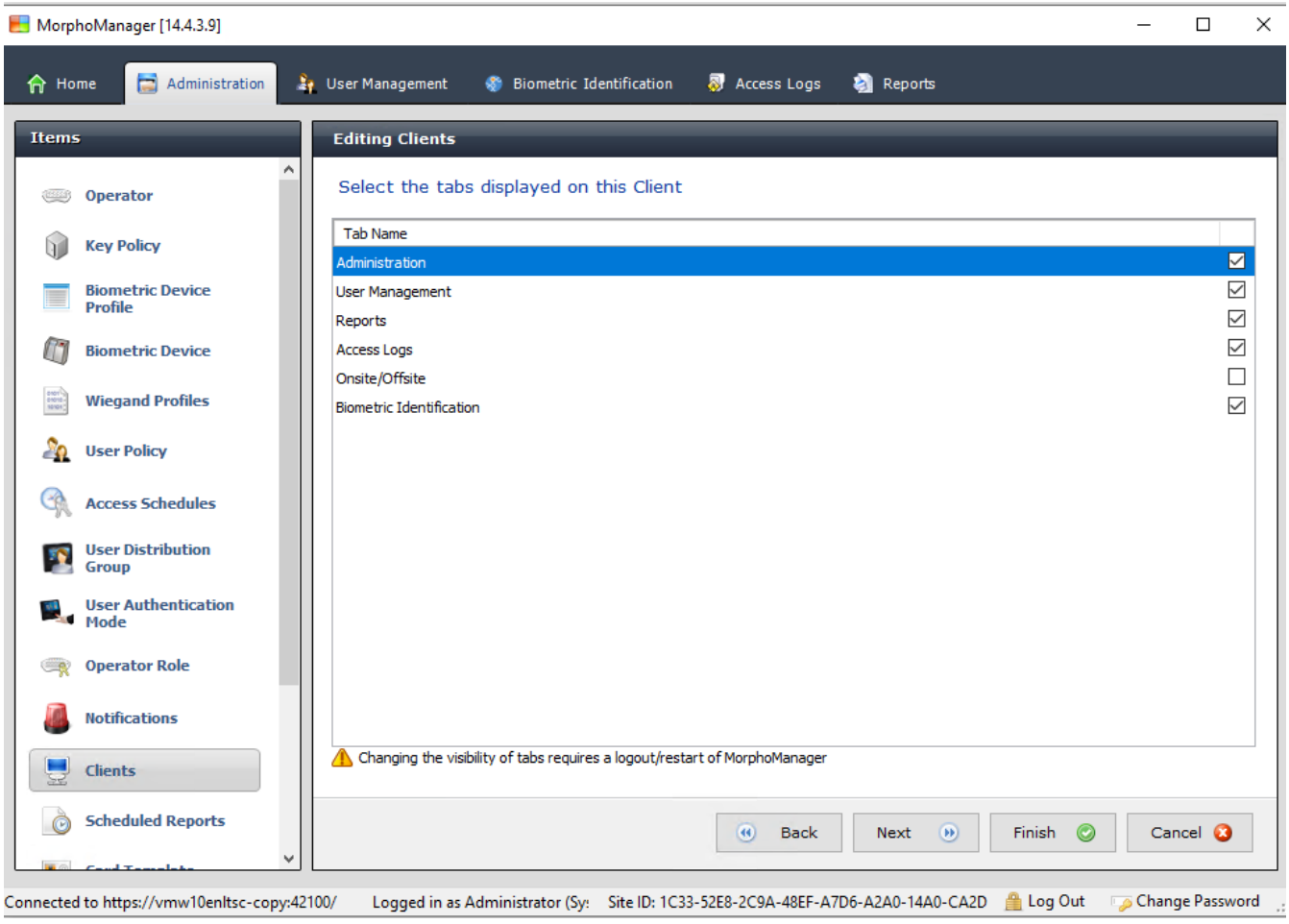
– введите имя пользователя и пароль, использованные для оператора регистрации в предыдущем разделе.
– Установите переключатель **Автоматический вход** в положение `Yes`

1. В каталоге установки MorphoManager (по умолчанию: `C:\Program Files(x86)\Morpho\MorphoManager\Client\ `) запустите файл `Start ID1.ECP4.MorphoManager.Client.exe` от имени администратора.
2. Перейдите в раздел **Администрирование** > **Клиенты**.

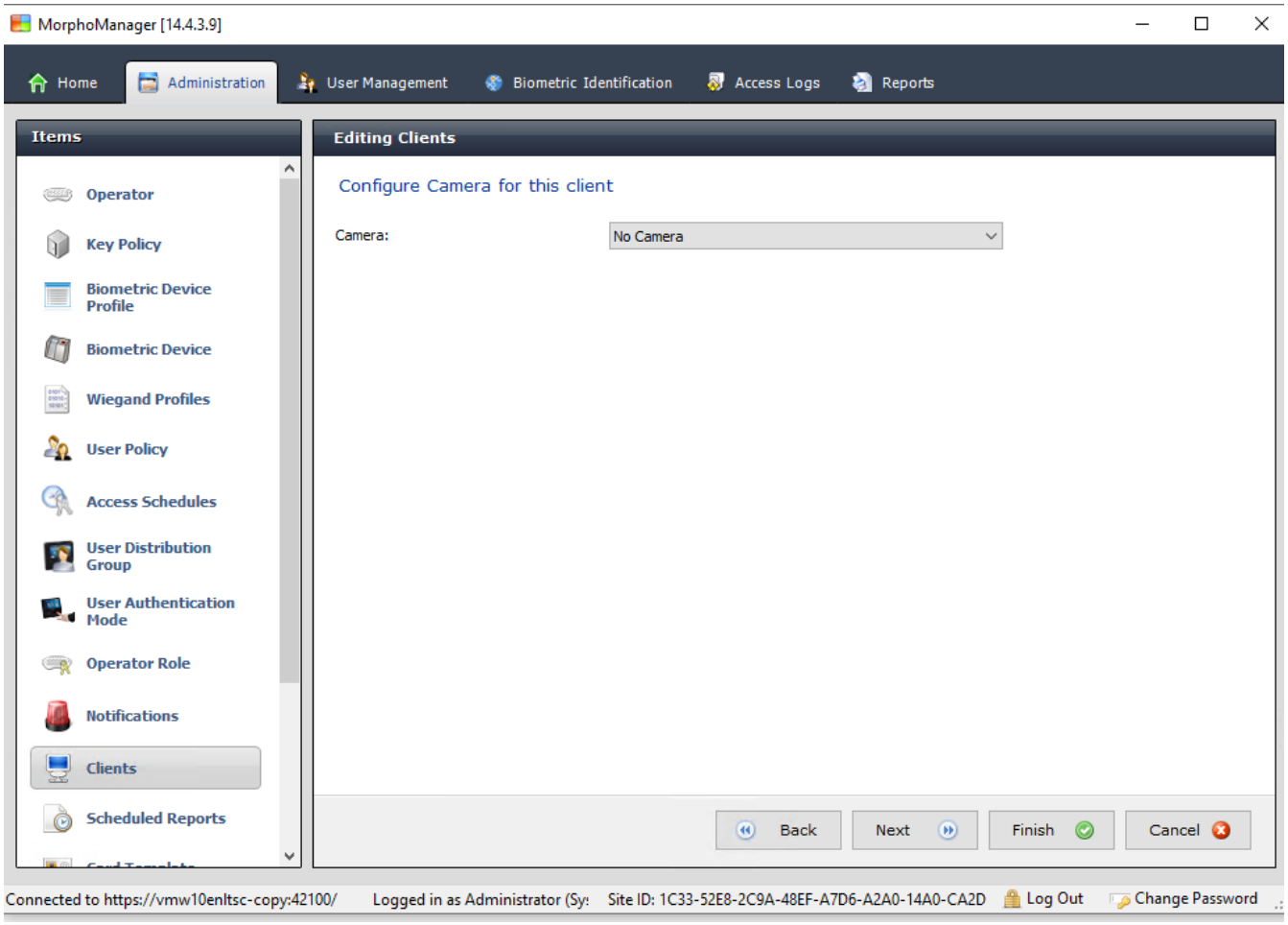
3. Выберите клиентский компьютер.
4. Нажмите кнопку **Изменить**.



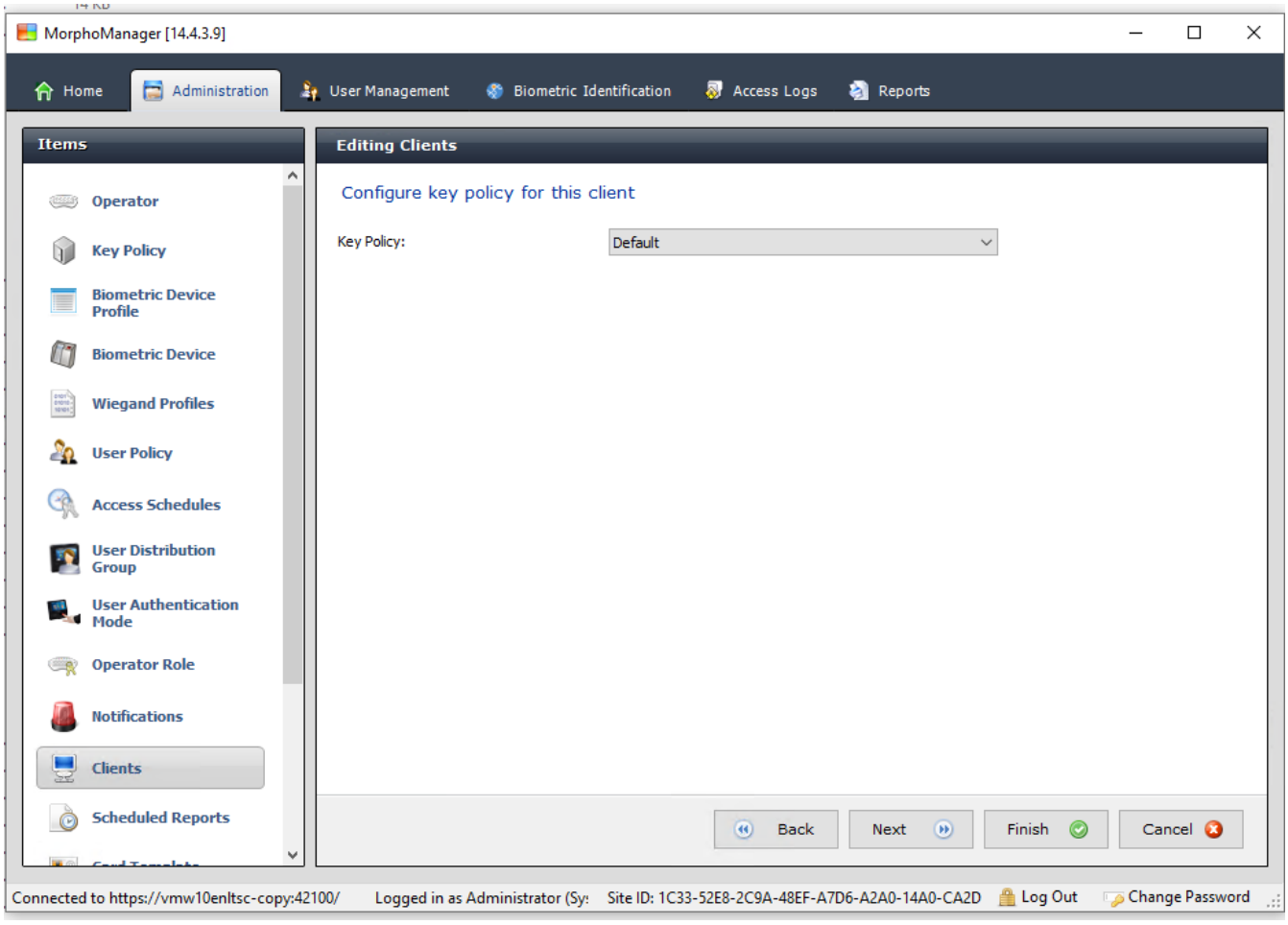
5. Введите имя предполагаемого клиента регистрации, а также местоположение и описание (необязательно).
6. Нажмите кнопку **Далее**



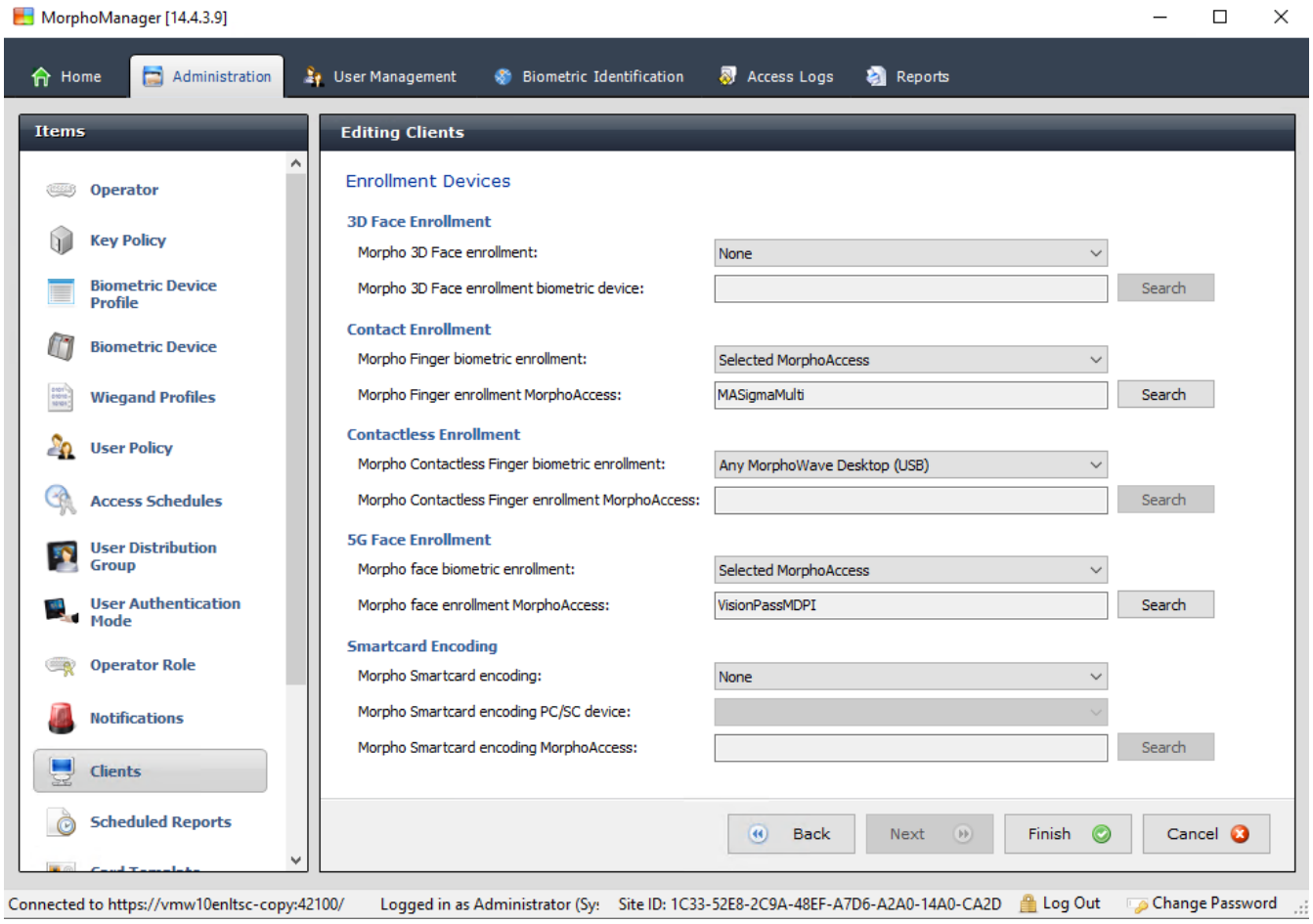
7. Установите флажки на вкладках, которые необходимо отображать в клиенте регистрации:
- **Администрирование;**
- **Управление пользователями;**
- **Отчеты;**
- **Журналы доступа;**
- **Биометрическая идентификация**.
8. Нажмите кнопку **Далее**



9. В поле **Камера:** выберите значение `No camera` из списка.
10. Нажмите кнопку **Далее**



11. В поле **Основная политика** выберите значение `Default` из списка.
12. Нажмите кнопку **Далее**



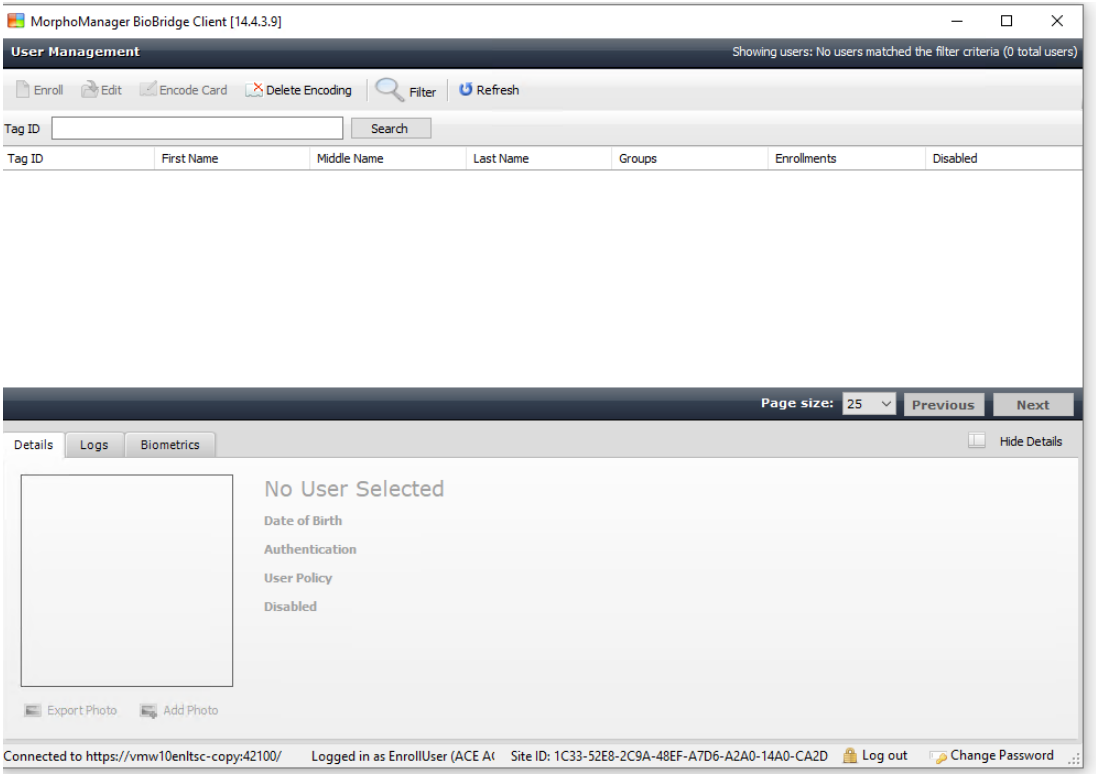
13. Выберите биометрический считыватель регистрации, который необходимо использовать на рабочей станции регистрации.
14. Нажмите кнопку **Готово**.
15. Закройте приложение MorphoManager.

См.

– *Настройка клиента регистрации BioBridge, Страница 188*

22.5.3 Проверка клиента регистрации

1. В каталоге установки системы MorphoManager (по умолчанию: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\ `)
   запустите файл `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`.



1. Убедитесь, что можно открыть окно регистрации, не вводя имя пользователя и пароль оператора регистрации.

22.6 Технические примечания и ограничения

Официально поддерживаемые операционные системы Windows
IDEMIA поддерживает те же версии Windows 10, что и Bosch ACS.

Официально поддерживаемая версия Microsoft SQL Server
Поддерживаемая версия — SQL Server 2017.

Одна система IDEMIA на одну систему доступа
Система управления доступом Bosch может поддерживать только одну систему IDEMIA.

Одна карта IDEMIA на одного владельца карты
Системы управления доступом Bosch поддерживают несколько карт на одного владельца карты, но IDEMIA поддерживает только одну. Поэтому при регистрации и синхронизации с BIS первая действительная карта (то есть со статусом status=1) типа «Доступ», «Временно» или «Парковка» назначается системе IDEMIA. Если позже карту блокируют, ее номер все равно передается и записывается в журнал событий.

Максимальное количество держателей карт IDEMIA
Клиент BioBridge системы MorphoManager может обрабатывать до 100 000 держателей карт.

Максимальное количество групп доступа
IDEMIA поддерживает до 5000 групп доступа (групп распределения пользователей). Они сопоставляются с **классами лиц** в системе управления доступом Bosch.

Производительность загрузки шаблонов
– 1000 шаблонов для 1 устройства: загрузка занимает менее 1 минуты.
– 1000 шаблонов для 100 устройств: загрузка занимает несколько минут.

IDEMIA не поддерживает подразделения
Если система IDEMIA интегрирована, система ACS не может достоверно проверять держателей карт одного подразделения из операторов управления доступом другого подразделения. Если между подразделениями обязательно абсолютное обеспечение конфиденциальности, не интегрируйте систему IDEMIA.

Виртуальные карты и доступ только по PIN-коду
IDEMIA не поддерживает доступ только по PIN-коду. Требуется физическая карта.

Функция IDEMIA «Отпечаток пальца для сообщения о действии по принуждению»
Функция IDEMIA «Отпечаток пальца для сообщения о действии по принуждению» в настоящее время не поддерживается контроллерами AMC.

Минимальный набор критериев идентификации
Для регистрации в системе IDEMIA требуются как минимум приведенные ниже критерии идентификации:
– имя;
– фамилия;
– класс лиц;
– одна физическая карта, назначенная держателю карты.

Отображаемые на считывателях состояния
Состояние считывателя (например, «Устройство заблокировано») не отображается на считывателях Wiegand и OSDP.

Резервное копирование и восстановление
Перед восстановлением резервной копии с IDEMIA удалите и заново создайте базу данных IDEMIA с помощью средства поставщика IDEMIA DataBridge.
В диалоговом окне **Биометрическое устройство** убедитесь, что все конфигурации успешно отправлены на считыватели IDEMIA. Если какая-либо из задач синхронизации завершилась сбоем, выполните перестройку конфигурацию считывателя:
1. В MorphoManager перейдите в режим **Биометрическое устройство**.
2. Выберите устройство, синхронизация которого завершилась сбоем.
3. Нажмите кнопку **Перестроить**.

Совместимость функций карт ACS с режимами проверки подлинности IDEMIA:

Функциональные возможности	Режим: карта И биометрические данные	Режим: карта ИЛИ биометрические данные

Карты доступа: вставить	OK	OK
Карты доступа: обновить	OK	OK
Карты доступа: удалить	OK	OK
Карты доступа: несколько карты	Только первая карта	Первая карта, используемая для биометрических учетных данных.
Запасная карта	OK	OK
Временная карта	OK	OK
Временная карта: только определенный период	OK	OK
Временная карта: деактивировать все карты немедленно	OK	OK
Временная карта: активировать карты автоматически после заданного периода	OK	OK
Временная карта: деактивировать карты и активировать автоматически	OK	OK
Карты для предупреждения об угрозе	Не поддерживается	OK
Офисный режим	Не поддерживается (*)	Не поддерживается (*)
Посетитель	Возможно, биометрические данные первого посетителя остаются назначенными карте.	Возможно, биометрические данные первого посетителя остаются назначенными карте.
Охранник	Не поддерживается	Биометрические данные не поддерживается. Карта работает.
Парковочная карта	OK	OK
PIN код	Не поддерживается (*)	Не поддерживается (*)
Проверка сторонней системой	Без PIN-кода (*)	Без PIN-кода (*)
(*) считыватель IDEMIA не подходит для использования в качестве считывателя с клавиатурой		

23 Обеспечение соответствия стандарту EN 60839

Введение

EN 60839 — это группа принятых в Европе международных стандартов в отношении оборудования и программного обеспечения для следующих систем:

- систем тревожной сигнализации и электронных систем безопасности
- электронных систем управления доступом

Чтобы обеспечить соответствие вашей системы управления доступом этому стандарту, может потребоваться адаптация определенных частей конфигурации. В списке ниже перечислены самые важные части. Полный список см. в стандарте, принятом в вашей стране.

Требования по использованию AMS 4.0 в качестве системы, сертифицированной по стандарту EN 60839 (класс 2)

- Система отвечает требованиям по глобальному запрету повторного прохода при условии использования одного пояса для каждого контроллера MAC.
- Возможность использования разных часовых поясов системы AMS зависит от количества контроллеров Mac. Для каждого контроллера MAC можно использовать отдельный часовой пояс.
- Проводка дверных контактов не должна препятствовать открыванию дверей для аварийной эвакуации в случае срабатывания противопожарной или охранной сигнализации.
- Только считыватели OSDP используют шифрование с интерфейсом RS485.
- Доступ в режим конфигурации должен строго контролироваться. Для этого, например, можно расположить компьютеры в защищенных зонах, настроить тайм-аут для сеансов входа в систему (в частности, тайм-ауты в случае неактивности на уровне приложения или операционной системы).
- Сетевые и электрические кабели необходимо прокладывать в безопасных зонах или в кабелепроводах.
- Размещать в незащищенных зонах можно только считыватели карт; все остальные устройства необходимо разместить в безопасных зонах.
- Минимальная длина проверочных PIN-кодов биометрических или физических учетных данных — не менее 4 знаков.
- Минимальная длина PIN-кодов идентификации — не менее 8 знаков.
- Необходимо синхронизировать компьютер основного сервера, серверы подключений, серверы MAC и клиенты с сетевым сервером времени.
- Необходимо включить мониторинг питания на локальных контроллерах доступа (например, AMC).
- Автономное функционирование локальных контроллеров доступа (например, AMC) допустимо только в случае сбоя сети. Так, запрещено задавать для параметра **Host timeout** (Тайм-аут хоста) AMC значение 0.

Правила надежности паролей

- Минимальное количество символов в пароле — 5.

24 Определение авторизаций и профилей доступа

24.1 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**

24.2 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.

25 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?

25.1 Лица

В следующей таблице перечислены данные, отображаемые *по умолчанию* в диалоговых окнах **Лица**. Для диалоговых окон предусмотрены гибкие настройки. См. раздел **Настраиваемые поля с данными о персонале**.
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.

См.

– *Пользовательские поля для данных персонала, Страница 140*

25.1.1 Параметры контроля карт или контроля здания

Обзор

На вкладке **Контроль карт** можно дать держателям карт возможность активировать 1 или 2 выхода общего назначения контроллера доступа для карты. Такую возможность можно назначить держателю карты, установив флажок **Управление зданием** в диалоговом окне **Лица**. Флажки **Управление зданием** (или **Контроль карт**) — это предварительно определенные настраиваемые поля, которые отображаются на вкладке **Контроль карт** лица по умолчанию, однако их можно разместить и в другом месте.

Для параметра управления зданием существует две основных задачи. Их описание дано ниже:

– Настройте флажок: присвойте ему подходящую метку и (при необходимости) расположите на другой вкладке диалогового окна **Лица**.
– Назначьте функцию выходу контроллера доступа AMC и установите флажок.

Предварительные требования

– Выход контроллера доступа электрически соединен с устройством, которое должно быть активировано картой.

Путь к диалоговому окну

– Главное меню AMS > **Конфигурация** > **Параметры** > **Настраиваемые поля** > вкладка **Контроль карт**

Настройка флажков

1. На странице **Настраиваемые поля** выберите вкладку **Подробно** в верхней области.
2. Найдите функцию **Управление зданием**, 1 или 2, которую планируется использовать.
3. Перезапишите имя метки (рекомендуется). При необходимости установите флажок на вкладке, отличной от **Контроль карт**. Более подробные инструкции см. в разделе **Предварительный просмотр и редактирование настраиваемых полей** по ссылке ниже.

Назначение функции выходу контроллера доступа и флажку

См. раздел **Параметры и настройки AMC** по ссылке ниже.

1. В **редакторе устройств** в дереве устройств выберите контроллер доступа AMC, выходной сигнал которого требуется использовать.
2. На вкладке **Выходы** в верхней области выберите выход, который необходимо использовать.
3. В среднем окне **Выходные данные** выберите тип **25**, **Контроль карт**.
4. Нажмите кнопку **>**, чтобы добавить выход в нижнюю область.
5. В нижней области, столбец **Param11**, выберите метку функции управления зданием, выбранную на предыдущем шаге **Установка флажков**.
6. Сохраните дерево устройств.

См.

- *Параметры и настройки AMC, Страница 59*
- *Предварительный просмотр и редактирование настраиваемых полей, Страница 140*

25.1.2 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.

25.1.3 Регистрация подписей

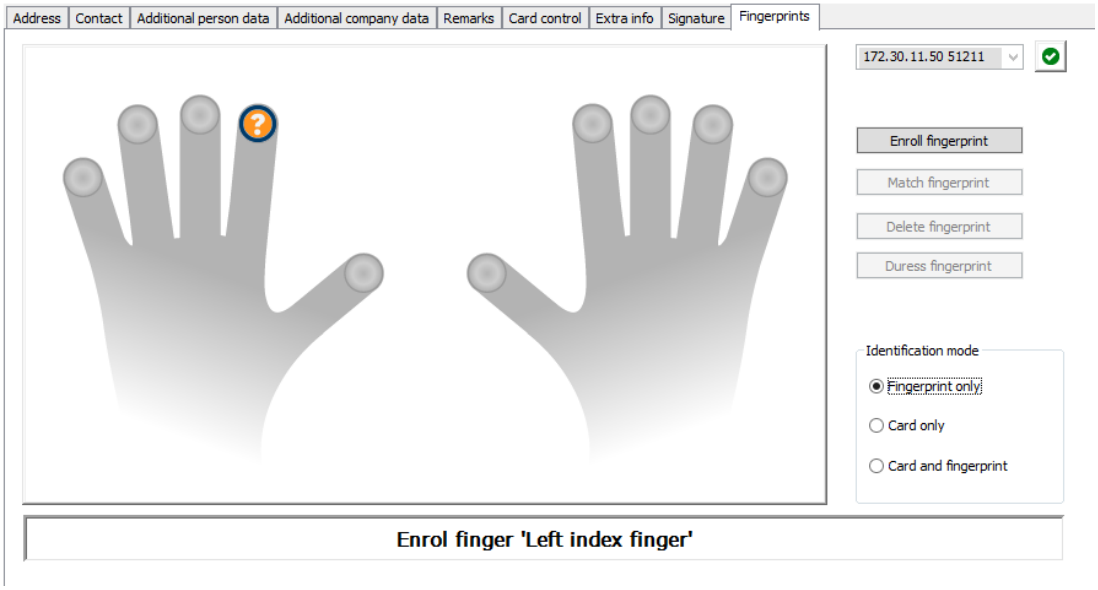
В системе необходимо подключить и настроить панель захвата подписей от компании Signotec для захвата подписей. В случае сомнений обратитесь к системному администратору.

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.

25.1.4 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. Этот регистрационный считыватель отпечатков пальцев **не должен** быть считывателем доступа.
- 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.

- Считыватели отпечатков пальцев могут отправлять сигналы для сообщения о действии по принуждению только в том случае, если они настроены в **редакторе устройств** на вкладке
  Сеть и режимы работы > **Шаблоны на сервере** > **Карта и отпечаток пальца**.
- 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.

25.2 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.

25.3 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**.

25.3.1 Назначение карт лицам

Введение

У всех лиц, доступ которых контролируется, должна быть карта или другой электронный идентификатор, назначенный держателю карты в диалоговом окне **Карты**.

Номера карт могут назначаться вручную или с помощью регистрационного считывателя.

Путь к диалоговому окну

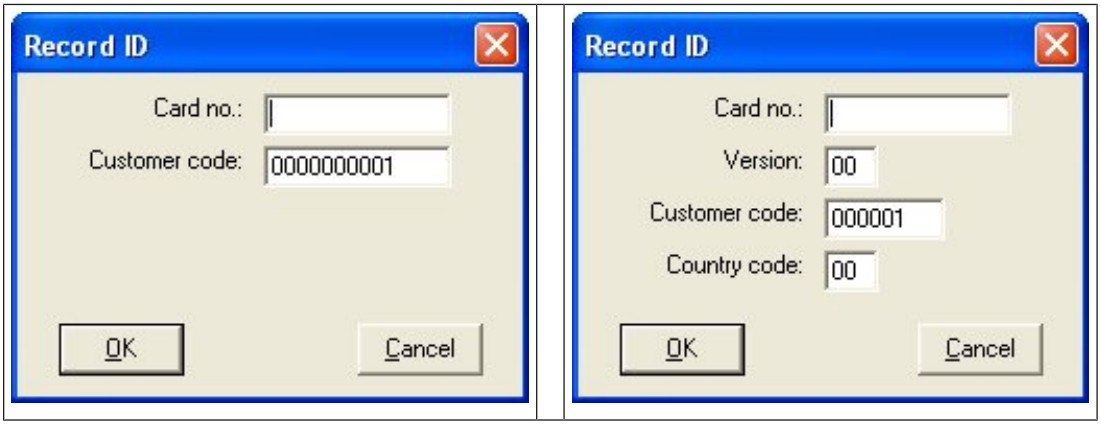
Главное меню > **Данные о персонале** > **Карты**

Предварительные требования

- 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 регистрационного считывателя

Предварительное требование

– На рабочей станции настроен регистрационный считыватель.

Порядок регистрации

1. Нажмите кнопку справа от кнопки **Зарегистрировать карту**, чтобы выбрать настроенный регистрационный считыватель.

– Обратите внимание, что для изменения выбора регистрационного считывателя необходимо войти в диспетчер диалоговых окон ACE с правами администратора.

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. Во всплывающем окне

– Выберите **Заменить карту**, если оригинал безвозвратно утерян или поврежден.
– Выберите **Временная карта**, если оригинал был забыт (оставлен дома) и требуется временная замена.
  – Введите срок действия временной карты.
  – Выберите, следует ли отключить все остальные карты.
  – Выберите, следует ли снова активировать оригинальные карты автоматически по истечении срока действия временной карты.

4. Нажмите **ОК** для сохранения.

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.

25.3.2 Печать бэйджей

Предварительные требования

- В системе уже должна существовать запись сотрудника для нового держателя карты.
- Рабочая станция со следующим подключенным оборудованием (как правило, по USB):
  - Принтер бэйджей
  - Камера для создания идентификационных фотографий

Процедура

Путь к диалоговому окну

Клиент AMS: **Данные о персонале** > **Печать бейджей**

1. Загрузите запись о персонале, для которой требуется напечатать карту.
2. В раскрывающемся меню **Макет** выберите требуемый макет карты из сохраненных макетов.
3. Сделайте идентификационную фотографию одним из следующих способов:
   - Нажмите кнопку **Захватить** и выберите требуемую камеру в списке подключенных камер.
   - Нажмите кнопку **Импорт изображения** и с помощью рамки обрезки выберите часть фотографии для печати на карте.
4. Нажмите **Предварительный просмотр**, чтобы убедиться, что на бейдже будут отображаться правильные данные с правильным макетом.
5. Нажмите **Печать** для печати бейджа.

Поддерживаемые камеры

Все устройства USB, которые распознаются операционной системой как камера.

25.3.3 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 200*
- 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.

25.3.4 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 увеличить время (по умолчанию в 3 раза), необходимое лицам с ограниченными возможностями для прохода, прежде чем активируется состояние **Дверь открыта слишком долго**.
Примечание. Коэффициент расширения по умолчанию можно сбросить в свойствах MAC в редакторе устройств.
Выберите **Общие настройки доступа** > **Временной фактор для лиц с ограниченными физическими возможностями**.

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**).

См.
– *Авторизация лиц для настройки офисного режима, Страница 212*

25.3.5 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

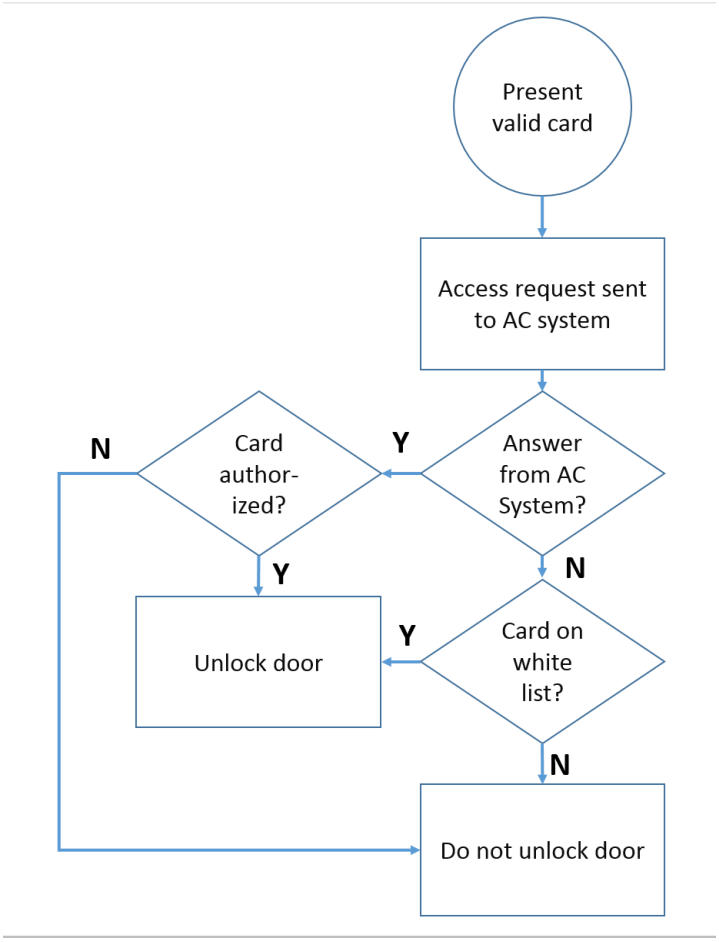
1. Перейдите в раздел: **Данные о персонале** > **Группы лиц** и используйте критерии фильтрации для создания списка держателей карт в окне списка.
2. В раскрывающемся списке **Поле для изменения** выберите **Разблокировать двери**
3. Установите флажок **Разблокировать двери**.
4. Нажмите кнопку **Применить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

Замечание!
Офисный режим и параметры устройств для двери
Офисный режим переопределяет параметр **Разблокировать дверь** на вкладке **Параметры** двери в редакторе устройств, разрешая только **0 = нормальный режим** и **1 = разблокировано**.

25.3.6 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.

25.3.7 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 настроен регистрационный считыватель.
– 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**.

25.4 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 регистрационному считывателю, настроенному на рабочей станции.
– Подходящая физическая карта доступна для регистрации в системе в качестве временной карты.

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. Нажмите **Снять временную блокировку**
   Обратите внимание, что при снятии **блокировки** временные карты не удаляются. Действие временных карт закончится по истечении срока их активности. При необходимости удалите их вручную.

Примечания по временным картам

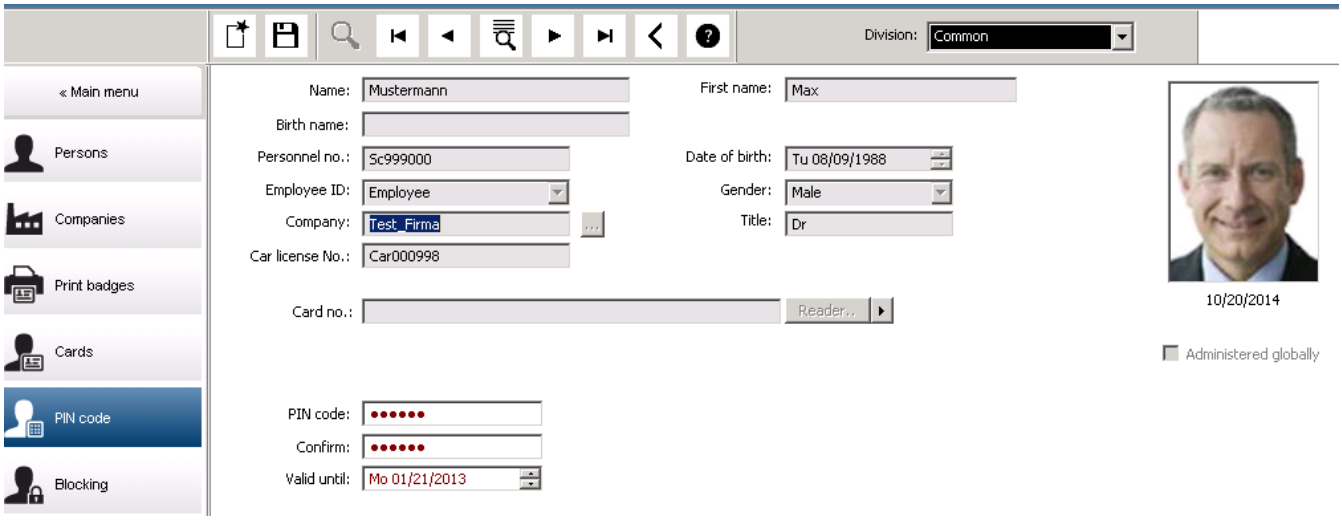
– Система не позволяет заменять временные карты временными картами.
– Система не позволяет создавать несколько временных карт для одной персональной карты.
– Для просмотра краткой сводки по всем картам, принадлежащим владельцу, наведите указатель мыши на небольшую панель с левого края, помеченную как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

25.5 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.

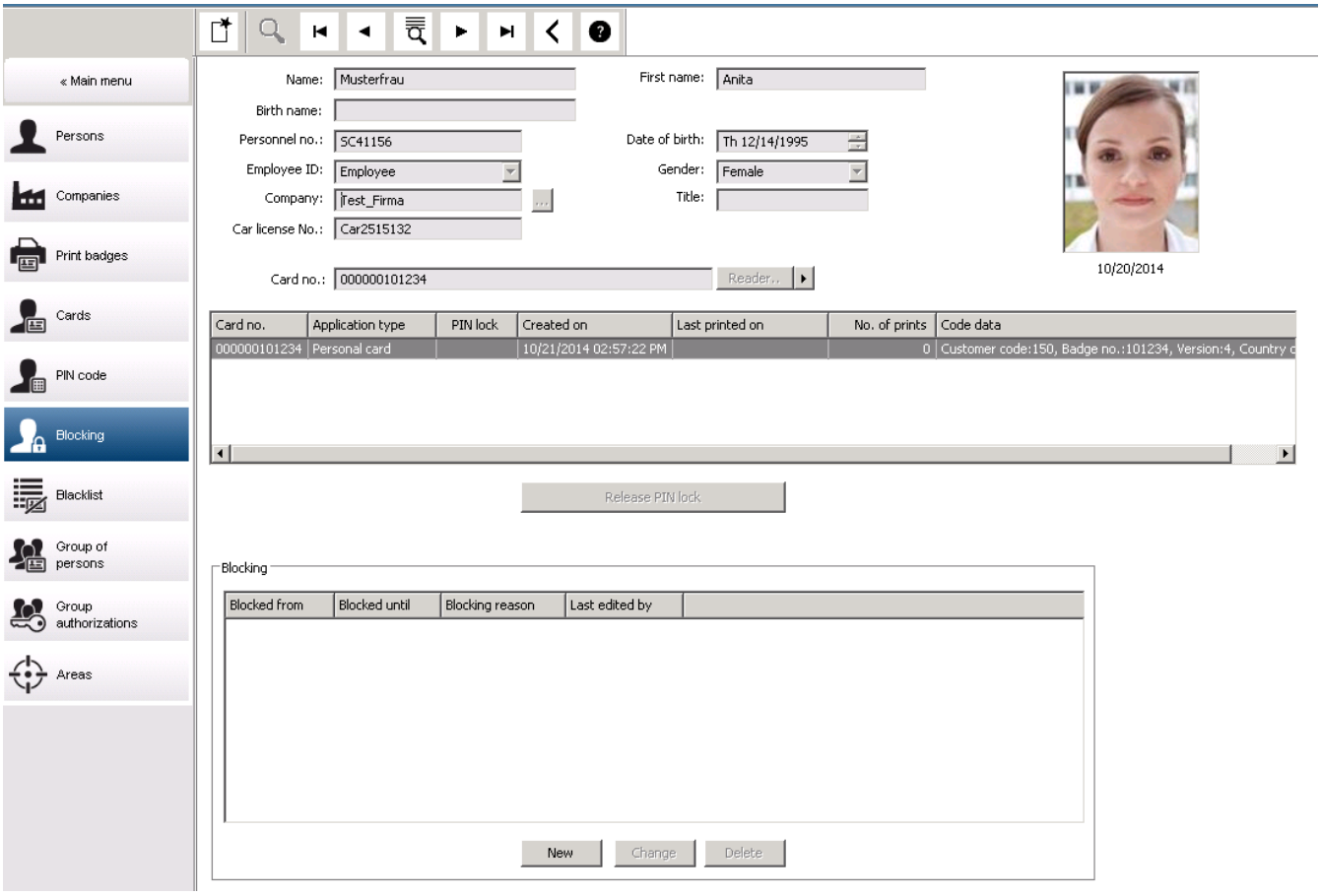
Замечание!
Способ ввода идентификационных PIN-кодов держателями карт зависит от типа считывателей, настроенных в системе. Например:
В считывателях карт RS485 держатель карты вводит: **4 #** `<the PIN>`
В считывателях карт Wiegand держатель карты вводит: `<the PIN>` **#**
Сообщите держателям карт, как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

25.6 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.

25.7 Занесение карт в черный список

Диалоговое окно: "Черный список"

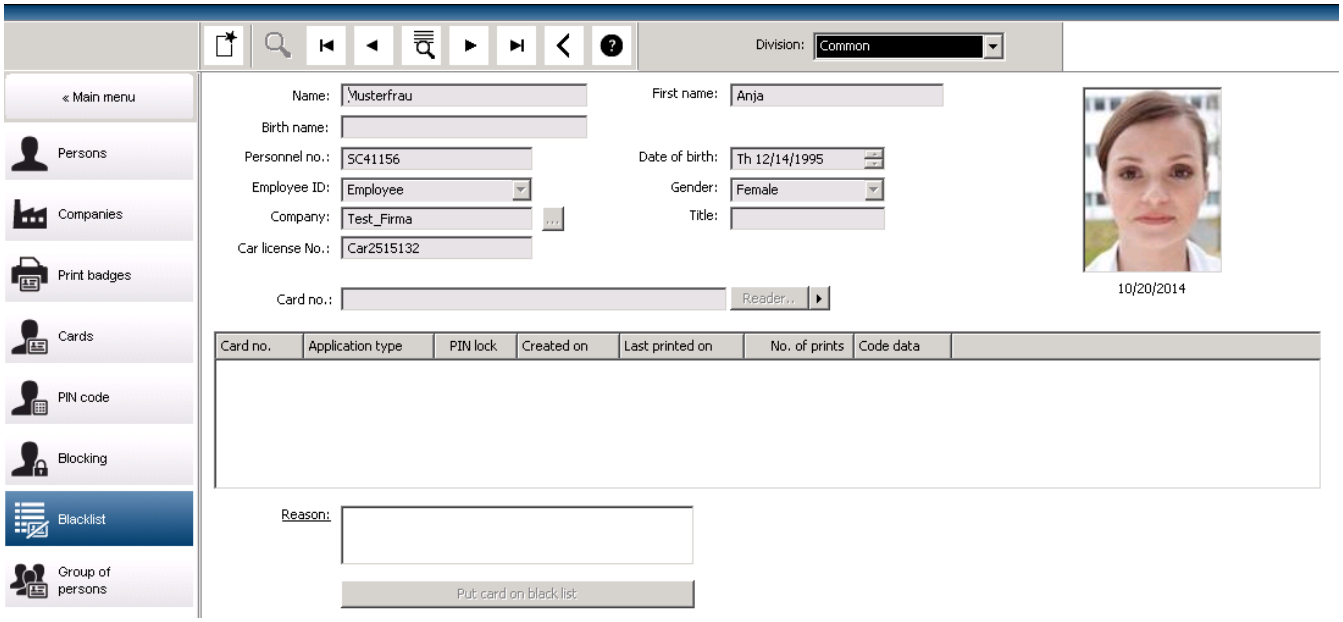
Любые карты, которые использовать впредь запрещено (например, украденные или потерянные), вносятся в таблицу черного списка.

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.

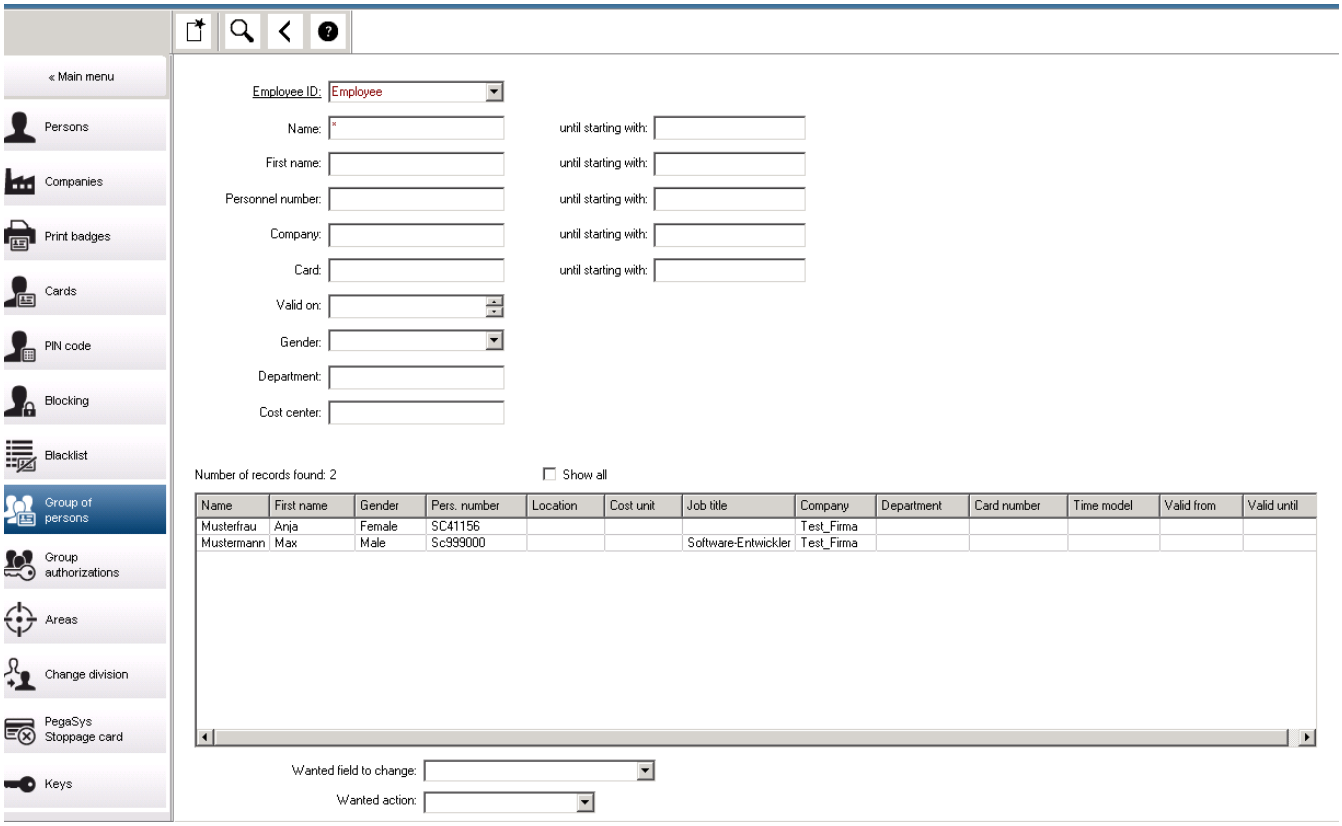
Замечание!

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.

25.8 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:

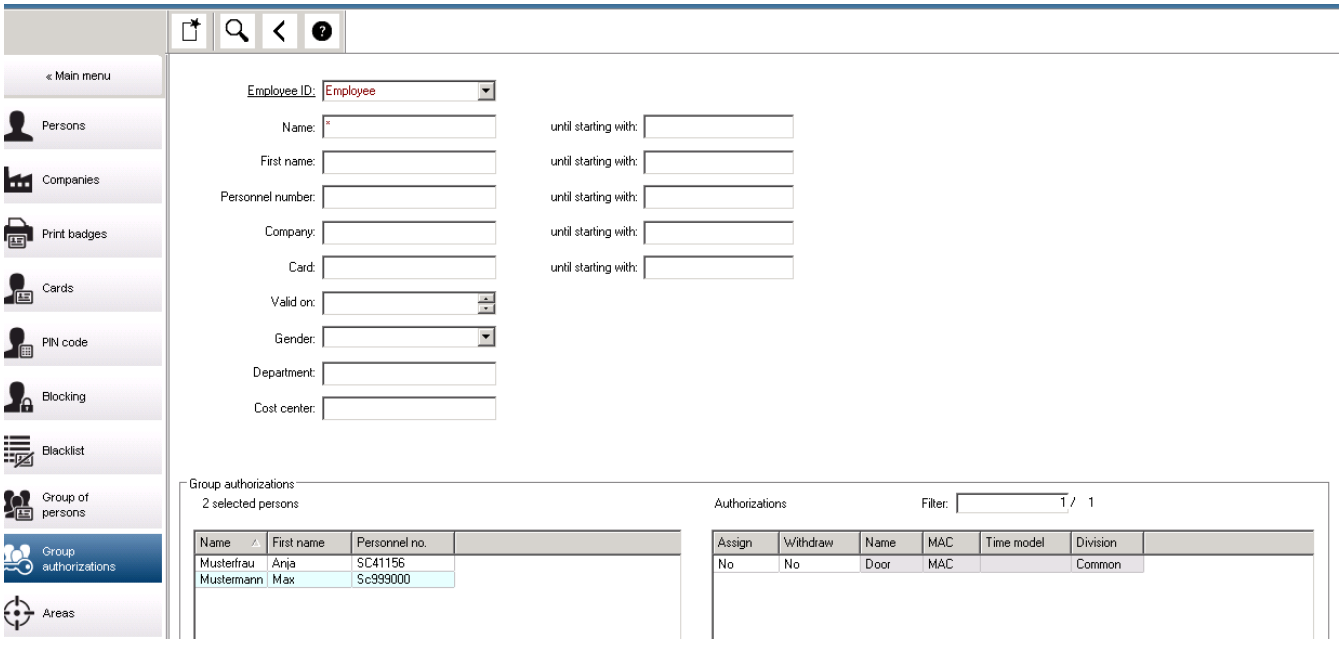
- Изменяемое поле
- Требуемое действие
- Старое значение

– 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.

25.8.1 Групповые полномочия

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.

25.9 Изменение подразделения для сотрудников

Введение

Изменение подразделения — это эффективное диалоговое окно, с помощью которого можно изменить подразделение для некоторого множества записей сотрудников в системе.

Замечание!
Используйте эту функцию с большой осторожностью!
Изменение подразделения для записей сотрудников имеет далеко идущие последствия.

Предварительные требования

Оператор, изменяющий подразделение для записей сотрудников, должен иметь полномочия на изменение данных этих сотрудников и соответствующих подразделений.

Путь к диалоговому окну

Главное меню > **Данные о персонале** > **Изменить подразделение**

Процедура

1. В области **Фильтр лиц** введите условия фильтрации в одном или нескольких следующих полях:

Фильтр	Примечания / описание
Фамилия	Введите одиночный символ звездочки (*), чтобы охватить всех сотрудников, или буквы **без** звездочек.
Номер сотрудника от/до	Для определения диапазона значений используйте оба поля.
Идентификатор сотрудника (тип сотрудника)	Выберите из списка.
Подразделение	После нажатия кнопки «Применить фильтр» будут отображены только сотрудники данного подразделения.
Компания	Выберите одну из доступных компаний.
Отдел	

Номер карты (от/до)	Для определения диапазона значений используйте оба поля.

2. Нажмите **Применить фильтр**.
   В списке **Выбранные лица** отобразятся все сотрудники, соответствующие фильтру**.**
3. Чтобы внести уточнения в набор выбранных сотрудников, щелкните одну или несколько строк в списке **Выбранные лица**, а затем нажмите кнопку **Удалить**. Для одновременного выбора нескольких записей используйте клавиши Ctrl и Shift.
   – **ВНИМАНИЕ!** Прежде чем продолжить, убедитесь, что список **Выбранные лица** содержит только сотрудников, для которых вы хотите изменить подразделение.
4. В списке **Новое подразделение** выберите целевое подразделение для выбранных сотрудников.
5. Нажмите **Изменить подразделение для лиц**.
   ВСЕ сотрудники, перечисленные в списке **Выбранные лица**, будут перемещены в **Новое подразделение**.

Последствия изменения подразделения

Сотрудники

– Права доступа и контроль пути.
– Связи с предыдущими подразделением удаляются.
– Связи с данными категории «Общее» сохраняются.

Компании

– Связи с компаниями предыдущего подразделения удаляются.

Последствия изменения подразделения «Общее» на другое подразделение

– Права доступа и контроль пути.
– Связи с подразделением «Общее» и новым подразделением сохраняются.
– Связи с другим подразделением удаляются.

Последствия изменения подразделения на подразделение «Общее»

Все связи сохраняются.

25.10 Настройка области для сотрудников или транспортных средств

Введение

В этом разделе описывается, как перенести зарегистрированное местоположение держателя карты или его автомобиля из одной определенной области в другую. Это может потребоваться, если держатель карты перейдет из одной области в другую без сканирования своей карты. В такой ситуации системы со строгим запретом повторного прохода далее будут отказывать держателю карты в доступе до тех пор, пока фактическое и зарегистрированное местоположения этого держателя карты снова не начнут совпадать.

Предварительные требования

– В системе определены и используются области контроля доступа. Документацию см. по ссылке ниже.
– Оператор уполномочен изменять данные держателя карты.

Процедура изменения местоположения отдельных держателей карт и автомобилей

Путь к диалоговому окну

Главное меню > **Данные о персонале** > **Области**

1. Выберите держателя карты из базы данных обычным образом.
2. Выберите новое местоположение в списке **Местоположение** или
3. выберите новое местоположение для автомобиля держателя карты в списке **Местоположение автомобиля**.
4. Нажмите  для сохранения.

См.

– *Настройка областей контроля доступа, Страница 27*

25.10.1 Процедура изменения местоположения всех держателей карт и автомобилей

Эта процедура может оказаться необходимой, например, после эвакуационных учений. Для всех местоположений устанавливается значение **НЕИЗВЕСТНО**, чтобы могли возобновиться мониторинг последовательности доступа и запрет повторного прохода.

Процедура

Путь к диалоговому окну

Главное меню > **Системные данные** > **Сброс областей в неизвестное местоположение**

– Нажмите **Установить значения областей для всех присутствующих лиц в «НЕИЗВЕСТНО»**.

или

– Нажмите **Установить значения областей для всех т/с в «НЕИЗВЕСТНО»**.

25.11 Настройка и печать форм для данных о персонале

Обзор

В окне **Формы** можно настроить формы для печати данных держателя карты из базы данных. Эта функция может потребоваться в соответствии с местным законодательством в области конфиденциальности данных.

Предусмотрены шаблоны форм. Эти шаблоны можно экспортировать как HTML-файлы, настроить в соответствии с требованиями, а затем обратно импортировать для использования в диспетчере диалоговых окон.

Создайте экземпляр и распечатайте форму из диалогового окна **Данные персонала** > **Печать бейджей**.

Путь к диалоговому окну

– Главное меню AMS > **Конфигурация** > **Параметры** > **Формы**

Настройка формы

1. В диалоговом окне **Формы**, список **Доступные формы**, выберите шаблон, который требуется настроить. Как правило, это шаблон `AllPersonalData_EN`, со всеми полями личных данных в базе данных.
2. Нажмите **Экспорт**, чтобы сохранить форму в системе как новый HTML-файл.
3. С помощью редактора HTML настройте HTML-файл в соответствии со своими требованиями.
4. В диалоговом окне **Формы** нажмите **Вставить**, чтобы импортировать настроенный HTML-файл в диспетчер диалоговых окон.

- (Дополнительно) Если форма допустима только для конкретного подразделения, выберите подразделение для нового элемента в столбце **Подразделение**.
- (Дополнительно) Нажмите **Предварительный просмотр**, чтобы просмотреть форму с несозданными экземплярами в средстве просмотра HTML.
- (Дополнительно) Нажмите **Удалить**, чтобы удалить форму из списка.

Создание экземпляра и печать формы

1. В диспетчере диалоговых окон перейдите
- Главное меню AMS > **Данные персонала** > **Печать бейджей**
2. Загрузите нужную запись о персонале в форму.
3. Выберите форму в списке **Форма**.
4. Нажмите **Печать формы**.
   - Создается экземпляр формы с данными выбранной записи о персонале и отправляется на выбранный принтер.

26 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.

26.1 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.

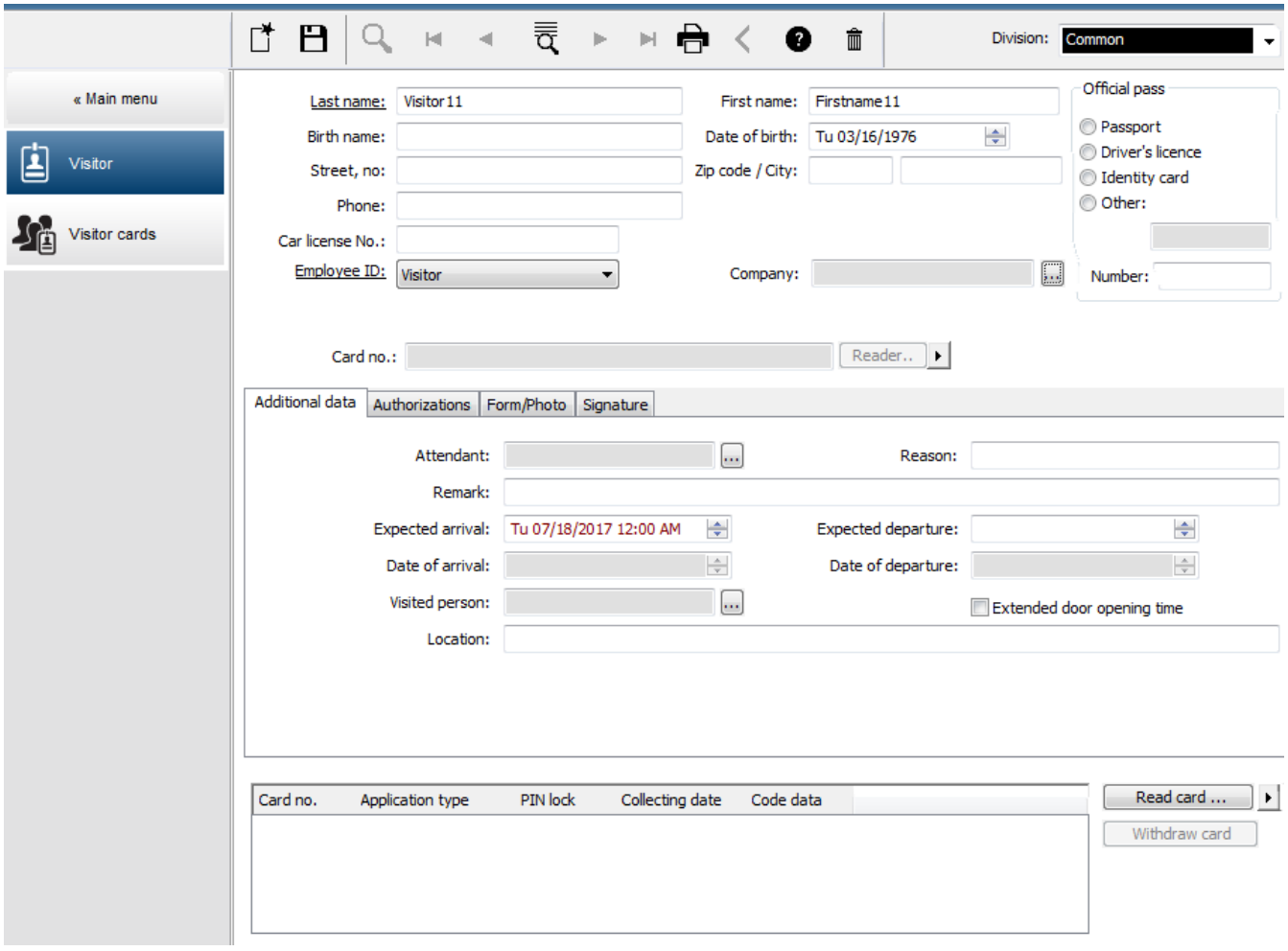
- Диалоговое окно **Посетители** используется для ввода данных о посетителях и назначении авторизаций доступа посетителей.
- Диалоговое окно **Карты посетителей** применяется для управления регистрацией и удалением карт посетителей.

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.

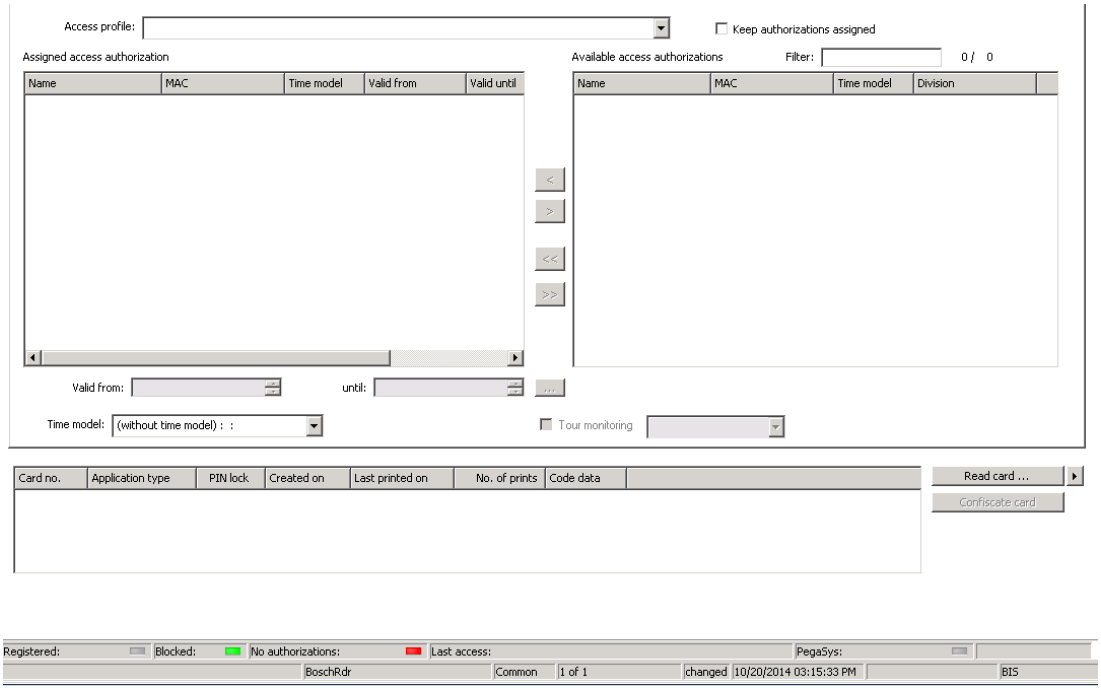


В полях ввода ниже можно указать **причину** посещения, **местоположение**, посещаемое посетителем, и **Примечание**.

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.

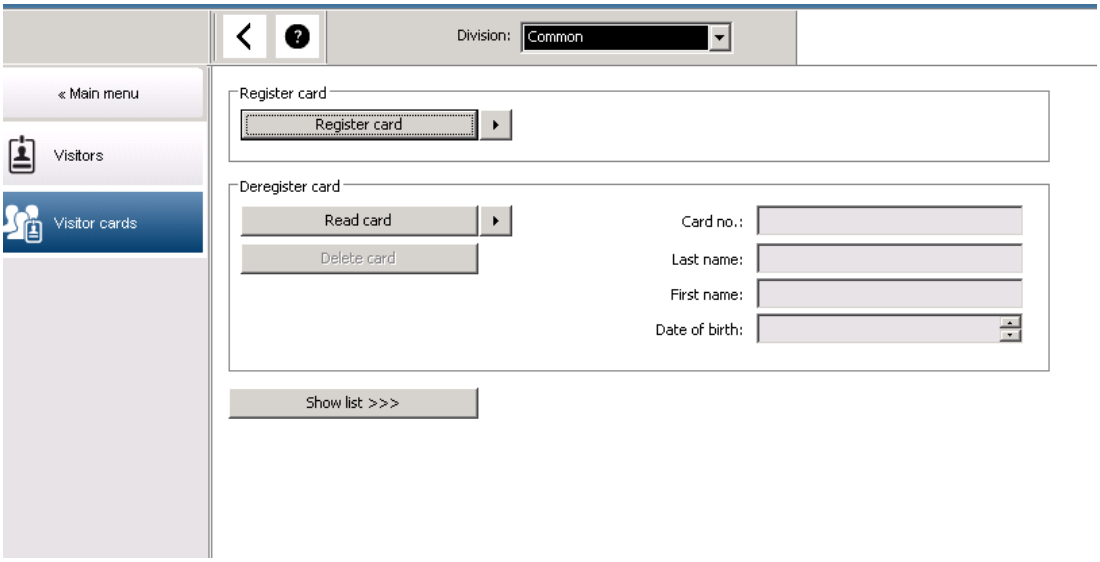
Как и в диалоговом окне **Карты**, можно назначить посетителям "расширенное время открытия дверей", чтобы облегчить доступ, например, для лиц с ограниченными физическими возможностями.



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.

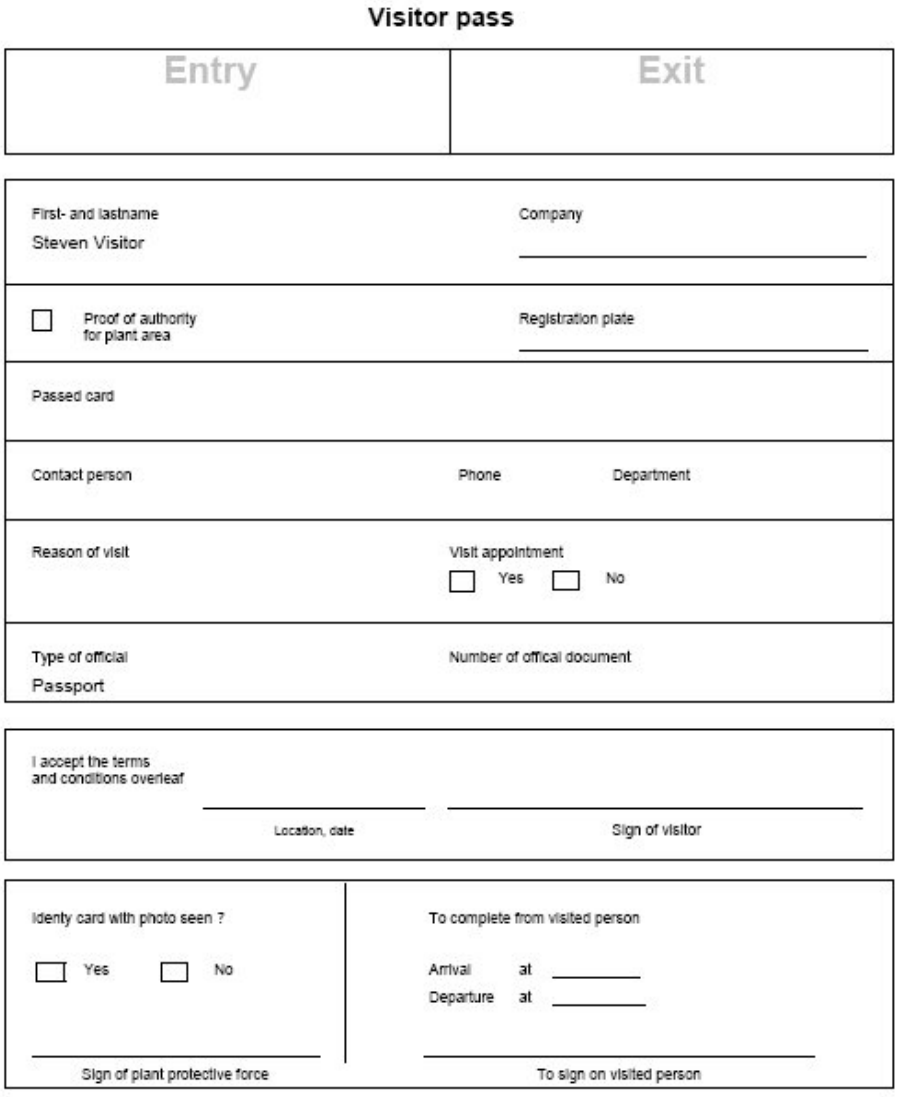
Чтобы ускорить назначение идентификационных карт посетителей, рекомендуется просканировать все существующие идентификационные карты, чтобы их можно было назначить соответствующим посетителям в следующем диалоговом окне.

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

27 Управление автостоянками

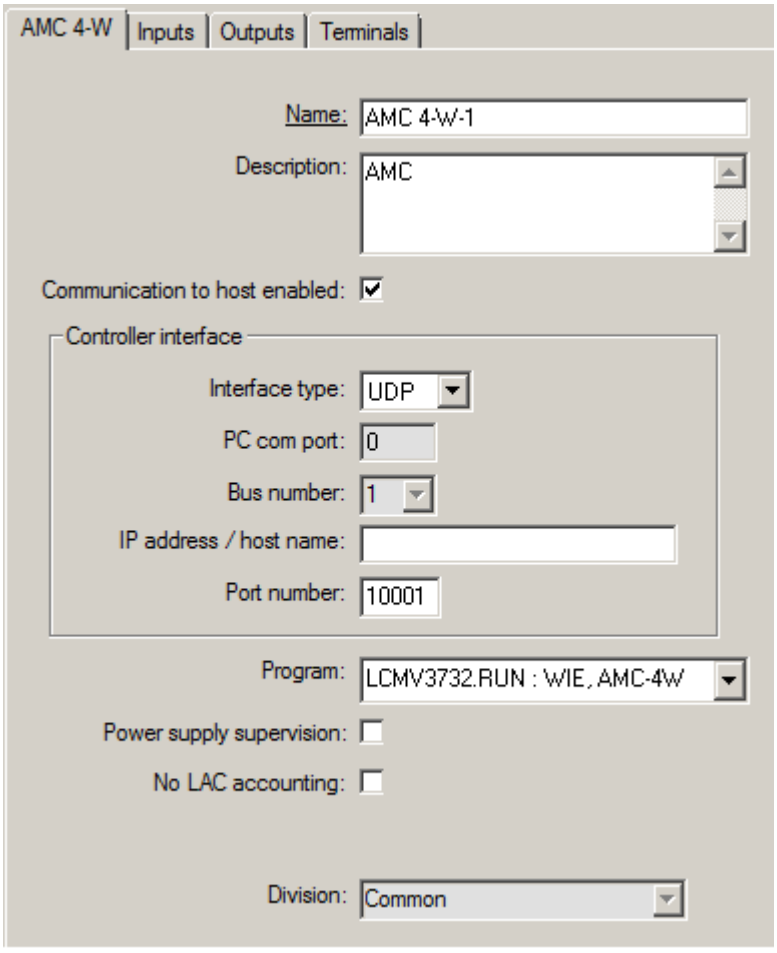
27.1 Авторизации для нескольких парковочных зон

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 LAC** в конфигурации AMC.



27.2 Отчет об автостоянке

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	--

27.3 Дополнительное управление парковкой

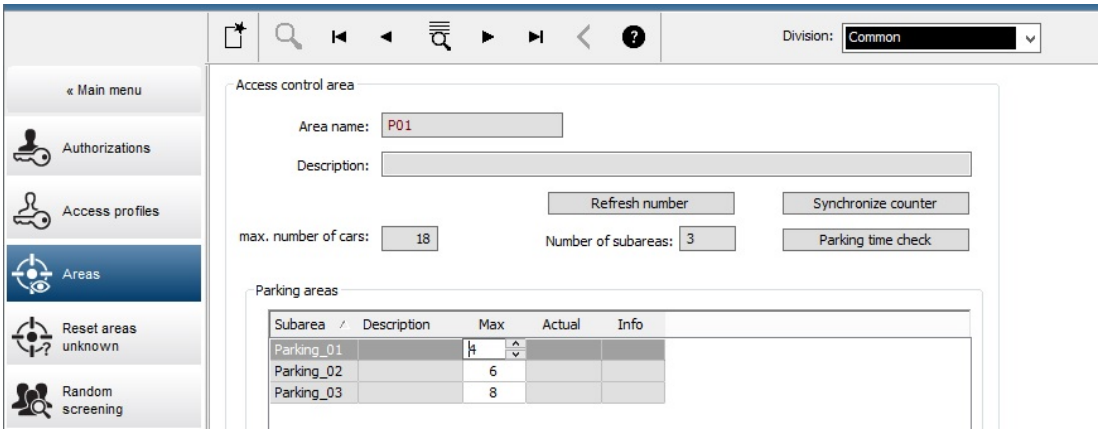
Введение

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.

Путь к диалоговому окну
Главное меню > **Системные данные** > **Области**

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



Примечания.
– Параметры, заданные в столбце **Макс.**, переопределяют параметры в конфигурации **Области**. См. раздел **Настройка областей для автомобилей** по ссылке ниже.
– Значение `0` в столбце **Макс.** означает, что количество парковочных мест неограниченно. В этом случае все подсчеты автомобилей отключены.

См.
– *Настройка областей для автомобилей, Страница 28*

28 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.

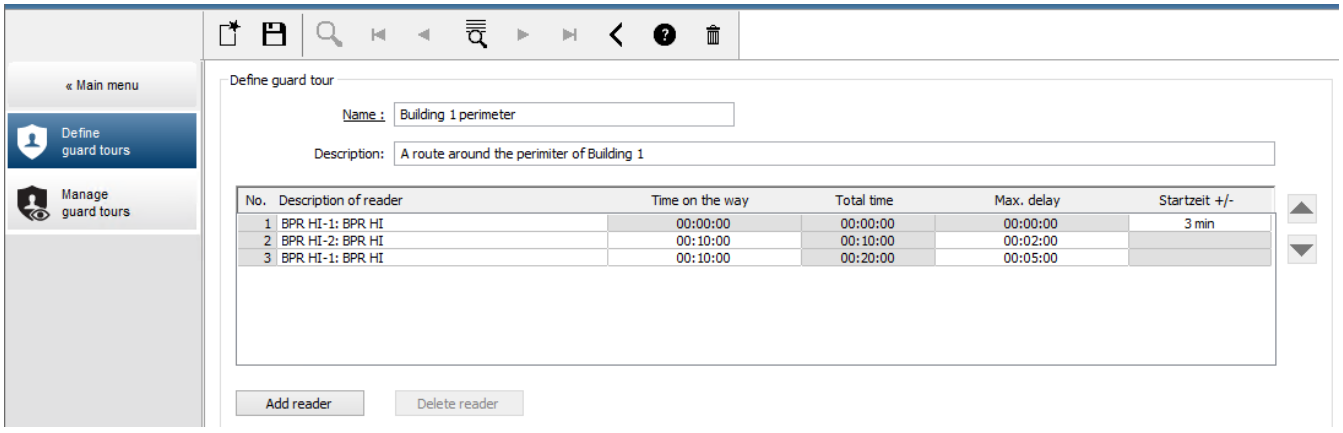
Маршрут патрулирования состоит из серии считывателей, для которых задано приблизительное временя, необходимое для того, чтобы дойти от одного считывателя к другому. Максимальное допустимое время задержки между считывателями и допустимое отклонение (+/-) от времени начала также являются параметрами маршрута 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.

28.1 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).

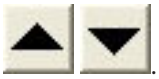
Добавление считывателей в маршрут патрулирования.

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  .

28.2 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.

28.3 Мониторинг маршрута (ранее «Контроль пути»)

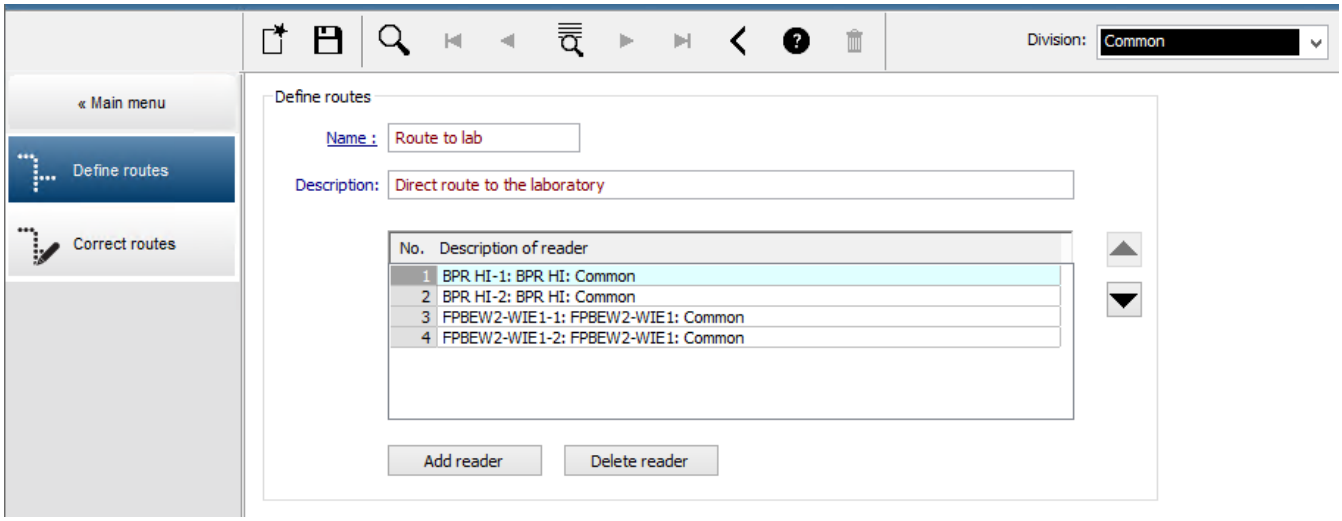
Введение

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**.

29 Случайный досмотр персонала

Порядок случайного досмотра

1. Держатель 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 отображаются индикаторы блокировки (красные), при этом мигают индикаторы случайного досмотра (фиолетовые).

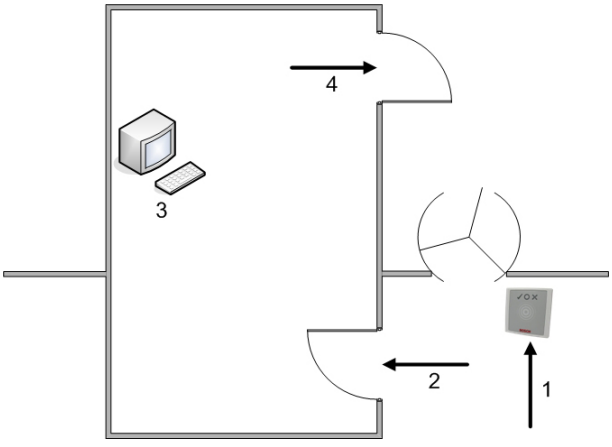
Замечание!

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.

30 Использование средства просмотра событий

Введение

Средство просмотра событий позволяет операторам с соответствующими полномочиями изучать события, записанные в системе, и составлять отчеты: выводить на экран, распечатывать или экспортировать в файлы `.CSV`.

Для извлечения и отображения нужных записей из базы данных журнала событий задайте критерии фильтрации и нажмите кнопку **Обновить**  . В зависимости от количества запрошенных данных этот процесс может занять несколько минут.

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

Предварительные требования

Вы вошли в диспетчер диалоговых окон.

Путь к диалоговому окну

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

30.1 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)
   - 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.

30.2 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)
   - 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.

30.3 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)
   - 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.

31 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.

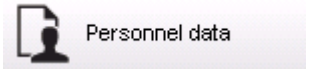
В окне предварительного просмотра есть собственная панель:

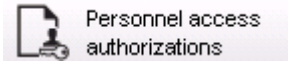
- Нажмите ✕, чтобы выйти из предварительного просмотра без печати.
- Используйте клавиши со стрелками ⏮ ◀ 2 of 17 ▶ ⏭ на панели инструментов предварительного просмотра для перемещения по документу или укажите номер нужной страницы.
- Нажмите  , чтобы распечатать документ немедленно, используя принтер 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.

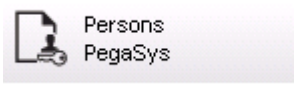
31.1 Отчеты: основные данные

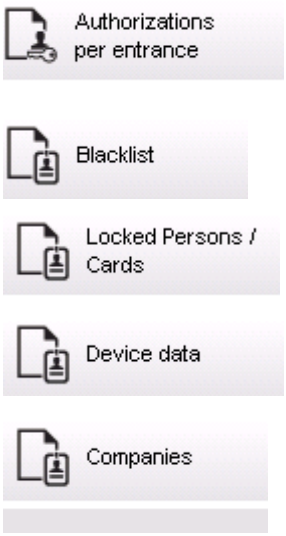
Обзор отчета: основные данные

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

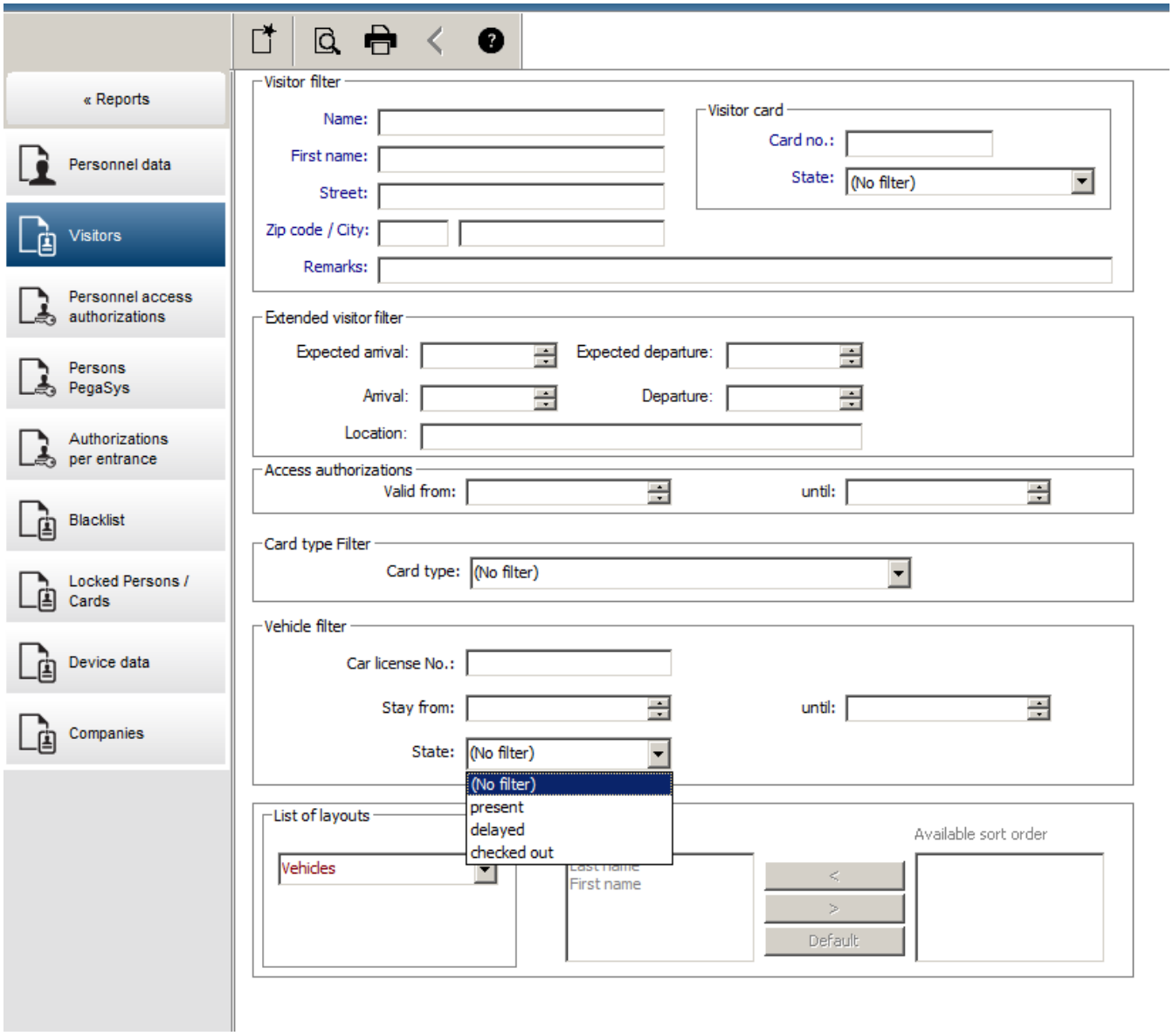
Диалоговое окно отчета «Компании» используется для сбора данных о компании. Используйте звездочки, чтобы найти компании с названием на определенную букву.

31.1.1 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.

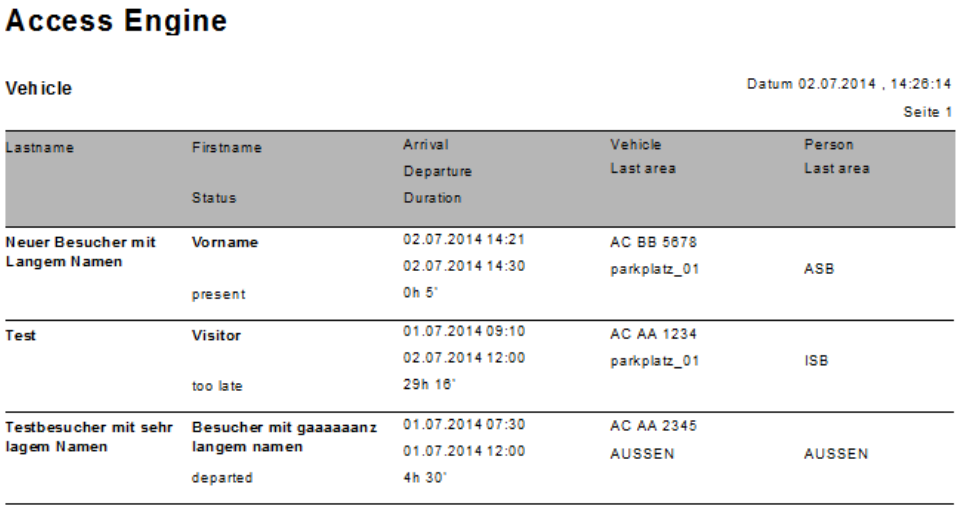


Отчет об автомобилях можно составить только для посетителей, потому что в таблице **Посетители** базы данных ожидаемая дата прибытия, ожидаемая дата убытия, дата прибытия и дата убытия доступны только для посетителей.

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

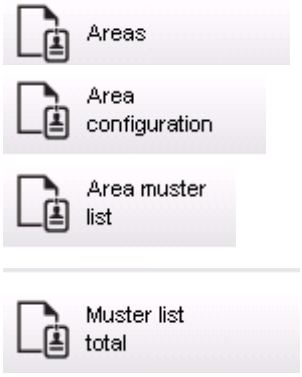
Seite 1

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

31.2 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.

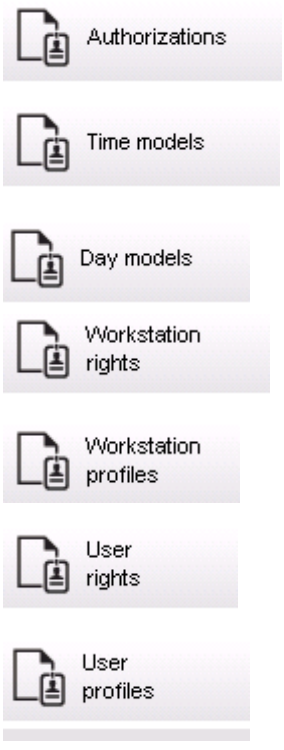
Отчет: "Конфигурация областей"
Определенные области и их подобласти с отмеченными флажками автостоянками и максимальным числом пользователей или автомобилей.

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.

31.3 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.

32 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 144*.

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 144*

32.1 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.

32.2 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 149*

32.3 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 215*

33 Использование Swipe ticker

Введение

Swipe ticker — это инструмент, помогающий операторам Map View в реальном времени отслеживать, кто входит на территорию или покидает ее.

Обзор

Swipe ticker — это приложение в AMC Map View, в котором отображаются последние 10 минут событий доступа в динамическом прокручиваемом списке. Отображаются до 50 событий доступа, а события старше 10 минут удаляются из списка автоматически. Оператор может отслеживать все считыватели в системе или может выбрать подмножество устройств.

Каждая запись в списке содержит подробные сведения о событии и используемых учетных данных, например:

- Имя владельца карты и сохраненная фотография для визуального подтверждения личности.
- Временная метка.
- Название компании и (или) подразделения, если оно сохранено.
- Проход и считыватель, на которых были использованы учетные данные.
- Категория события с цветовой меткой:
  - Зеленый цвет: завершенный доступ с действительными учетными данными
  - Желтый цвет: незавершенный доступ с действительными учетными данными, например владелец карты перезапустил блокировку, но не открыл дверь.
  - Красный цвет: неудачная попытка доступа с недействительными учетными данными. Отображается тип недействительности, например, учетные данные добавлены в черный список, неизвестны или срок их действия истек.

Swipe ticker не сохраняет собственные архивы; он извлекает и отображает события доступа из системной базы данных. Динамическую прокрутку можно приостановить для подробного изучения или открыть в отдельном окне для параллельного использования с другими приложениями Map View.

Замечание!

Задержка после редактирования

Для распространения изменений идентификационных фотографий и других данных держателя карты из AMC в Swipe ticker обычно требуется несколько минут. Во время синхронизации Swipe ticker продолжает реагировать в реальном времени на старые данные.

Предварительные требования

Профиль пользователя оператора требует наличия специальной авторизации для запуска Swipe ticker.

1. В главном приложении AMC перейдите в меню: **Конфигурация** > **Профили пользователей**.
2. Загрузите имя профиля нужного оператора.
3. В таблице выберите **Приложения Map системы Access Manager** > **Специальные функции** > Swipe ticker .

Запуск Swipe ticker

- В Map View щелкните  , чтобы запустить инструмент.

Выбор считывателей для наблюдения

Если считыватели еще не выбраны или вы хотите изменить выбор, выполните следующие действия:

1. В окне Swipe ticker нажмите кнопку  (Настройки).
   Откроется окно **Фильтр устройств**.
2. В дереве устройств установите флажки напротив проходов или считывателей, которые требуется отслеживать. Флажки работают следующим образом:
   Если выбрать проход, по умолчанию будут выбраны все подчиненные устройства. Флажки отдельных подчиненных устройств затем можно снять, если они не требуются.
   Если выбраны **все** дочерние элементы родительского устройства, флажок родительского объекта отображается белым цветом. Если выбрана только **часть** элементов, флажок родительского объекта отображается серым цветом.
3. Нажмите кнопку **ОК**, чтобы завершить выбор считывателей и закрыть окно **Фильтр устройств**.

Отображение выбранных считывателей на карте

- Дважды щелкните запись в Swipe ticker.
- ⇨ Swipe ticker автоматически приостанавливается.
- ⇨ В главном окне отобразится Map view, первая соответствующая сцена карты в иерархии карт, и будет выделен считыватель, который вы дважды щелкнули.

Приостановка Swipe ticker

- В окне Swipe ticker щелкните  или дважды щелкните запись в списке, чтобы приостановить динамическое отображение.
- ⇨ Динамическое отображение будет приостановлено. Входящие записи событий помещаются в буфер, но не отображаются.
- ⇨ В начало списка добавляется уведомление о том, что поток событий приостановлен.

Возобновление приостановленного Swipe ticker

- В окне Swipe ticker нажмите  , чтобы возобновить динамическое отображение.
- ⇨ Динамический список отображает в хронологическом порядке (сначала самые новые) все события доступа, произошедшие на выбранных считывателях за последние 10 минут (максимум 50).
- ⇨ События доступа, которые старше 50 самых новых или старше 10 минут, удаляются из списка.
- ⇨ Новые события доступа снова отображаются в реальном времени по мере их появления.

Дублирование Swipe ticker в отдельном окне

Обратите внимание, что в каждый момент времени можно открыть только одно окно дубликата Swipe ticker.

1. В окне Swipe ticker щелкните  (Дополнительное окно).
   Отдельное окно является дубликатом и **не** зависит от Swipe ticker в главном окне. Оно подчиняется тем же настройкам.
   Другие приложения Map View, такие как список тревог, теперь можно использовать параллельно в главном окне.
2. После завершения работы с отдельным окном используйте строку заголовка, чтобы закрыть его.

33.1 Особые случаи

Приложение Swipe ticker в Map View и двери с модулями B901

Для предоставления правильной информации приложению **Swipe ticker** в представлении AMS Map View идентификаторы дверей с модулями B901 должны совпадать с идентификаторами их дверных точек. Например, дверь 1 должна быть назначена дверной точке 1, дверь 2 дверной точке 2 и т. д.

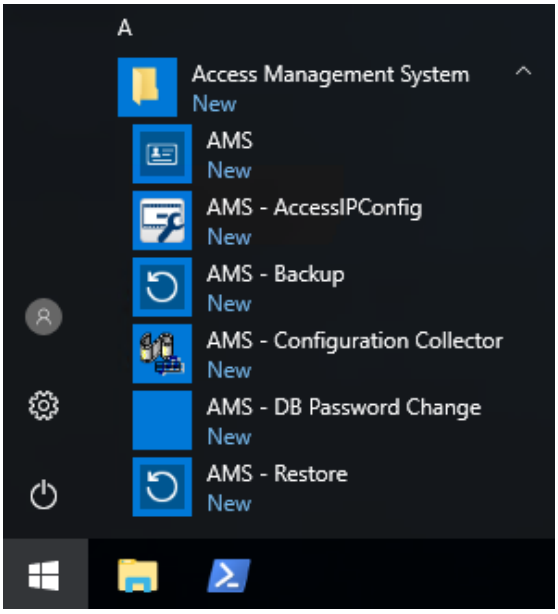
Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Эти назначения для контроллера дверей B901 выполняются в инструменте RPS для настройки охранных панелей и контроллеров.

34 Резервное копирование и восстановление

Функция **Резервное копирование и восстановление** позволяет переносить систему вместе с ее данными в систему AMS новой версии или на новый компьютер.
Резервное копирование и восстановление может выполняться только на компьютере с установленным сервером AMS. В меню «Пуск» Windows имеются два ярлыка:

- **AMS — резервное копирование** — для создания резервной копии
- **AMS — восстановление** — для восстановления из резервной копии:

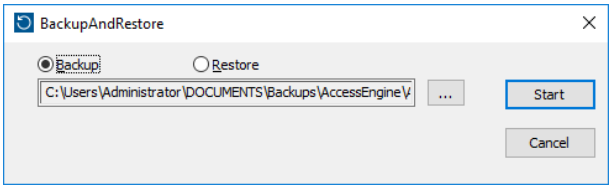


34.1 Создание резервной копии системы

В этом разделе описывается, как создать резервную копию приложения AMS и как найти файлы резервной копии SQL Server.

Создание резервной копии приложения AMS

1. В меню «Пуск» Windows щелкните правой кнопкой мыши **AMS — резервное копирование** и выберите **Запуск от имени администратора**.
   - Запустится инструмент **Резервное копирование и восстановление** с уже выбранным режимом **Резервное копирование**.



2. Укажите путь для сохранения файла `.GZ`.
3. Нажмите **Пуск**, чтобы запустить резервное копирование.
   - Инструмент **Резервное копирование и восстановление** создаст один файл `.GZ`, отображая ход выполнения во всплывающем окне.
4. Скопируйте этот файл в безопасное место на другом компьютере. Чтобы не потерять данные, **не оставляйте** единственную копию на сервере DMS.

Поиск и копирование файлов резервной копии SQL Server

1. Используя Проводник на компьютере сервера AMS, перейдите к папке, в которой SQL Server хранит файлы `.BAK`.

- Путь к файлу выглядит следующим образом, где <version> и <instance name> — переменные, зависящие от вашей системы:
  C:
  \Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\
- Имена файлов имеют следующий формат:
  acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
  Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
  Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
  Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
  Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
  Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak

2. Скопируйте **все** файлы .BAK в безопасное место на своем компьютере. Чтобы не потерять данные, **не** оставляйте единственные копии на сервере DMS.

Замечание!
Путь по умолчанию к журналу событий AMS:
C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\

34.2 Восстановление из резервной копии

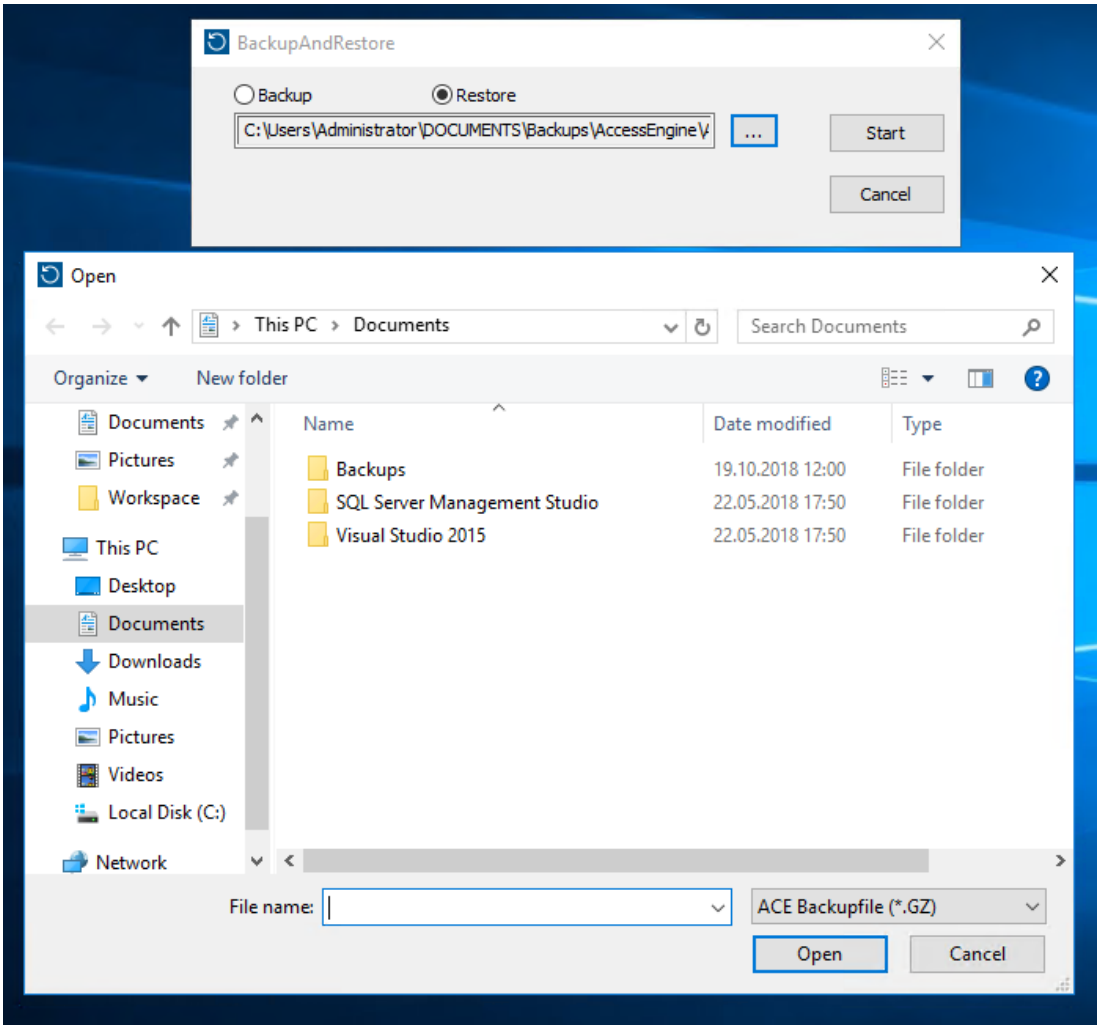
Предварительные требования

- Наличие файла GZ, созданного инструментом **Резервное копирование и восстановление**.
- Наличие файлов .BAK, созданных сервером SQL Server и сохраненных вами во время процедуры резервного копирования.
- Учетная запись SQL с правами **системного администратора**, например sa.
- Должным образом подготовленный целевой компьютер со всеми необходимыми **лицензиями** и **сертификатами**:
  - **Лицензии**. На целевом компьютере (на котором вы восстанавливаете данные из резервной копии) как минимум должны присутствовать лицензии, эквивалентные тем, что были на компьютере, на котором создавалась резервная копия.
  - **Сертификаты**. Для любых клиентов на целевом компьютере потребуются новые сертификаты, созданные в ходе установки на целевом компьютере, а не те, чтобы были созданы при установке на исходном компьютере.
    Информацию о создании и установке сертификатов клиентов см. в **Руководстве по установке AMS**.

Процедура

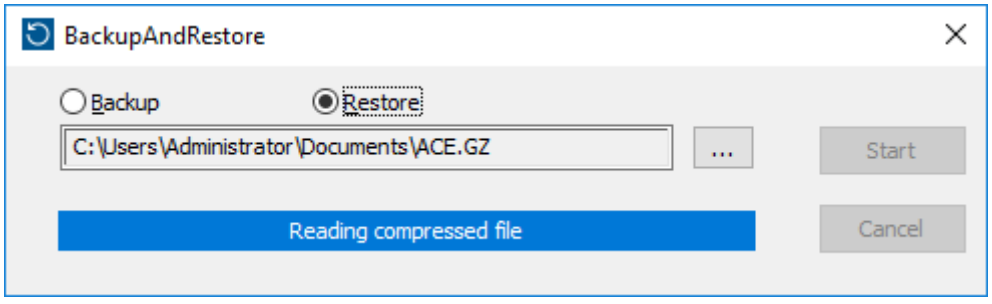
1. В программе AMS нажмите **Файл** > **Выход**, чтобы остановить приложение AMS.
2. Когда работа программы будет завершена, запустите приложение **Службы Windows** и убедитесь, что все службы Access Engine и Access Management System остановлены. В противном случае остановите их там же.
3. **Если и только если** вы используете RMAC (резервный MAC) со своим основным MAC или 1. MAC, перейдите к следующему подразделу и выполните описанную там процедуру, прежде чем выполнять этот шаг.

4. Скопируйте сохраненные вами файлы `.BAK` MSSQL с исходного компьютера по аналогичному пути на новом компьютере.
   – Путь к файлу выглядит следующим образом, где `<version>` и `<instance name>` — переменные, зависящие от вашей системы:
   `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
5. В меню «Пуск» Windows щелкните правой кнопкой мыши **AMS — восстановление** и выберите **Запуск от имени администратора**.
   – Запустится инструмент **Резервное копирование и восстановление** с уже выбранным режимом **Восстановление**.
6. Нажмите кнопку **[...]**, чтобы найти файл резервной копии `GZ` в файловой системе, и нажмите **Открыть**, чтобы выбрать его.



7. Нажмите **Пуск**, чтобы начать процесс восстановления.
8. При отображении запроса учетных данных для сервера введите учетные данные пользователя MSSQL с правами системного администратора, например `sa`, а не учетные данные для входа на компьютер сервера.

– Начнется процесс восстановления.



9. По завершении процесса восстановления запустите приложение **Службы Windows** и вручную перезапустите все службы `Access Engine` и `Access Management System`.
10. Запустите программу настройки сервера `AMS Server Setup.exe` от имени администратора, чтобы повторно синхронизировать резервную копию данных с текущими данными системы.

См.

– *Создание резервной копии системы, Страница 258*

34.2.1 Восстановление RMAC в новой установке

Примечание. Эта процедура применима только в случае, когда вы восстанавливаете на другом оборудовании систему с MAC и RMAC из резервной копии.

Введение

Если вы восстанавливаете систему из резервной копии на новых компьютерах, то вместо прежних IP-адресов MAC и RMAC, сохраненных в файл резервной копии, нужно задать IP-адреса нового оборудования. Для этого нужно запустить инструмент MACInstaller на новом оборудовании.

Инструмент MACInstaller находится в папке `\AddOns\MultiMAC\MACInstaller.exe` на установочном носителе.

Работа с инструментом MACInstaller подробно описывается в главе *Использование средства установки MAC, Страница 57*.

Процедура

1. Запустите инструмент MACInstaller на компьютере, на котором работает 1.MAC. Этот компьютер может быть сервером DMS или выделенным сервером для 1.MAC.
   – В инструменте настройте новые IP-адреса основного MAC (текущий компьютер) и RMAC.
2. Запустите инструмент MACInstaller на компьютере, на котором работает RMAC.
   – В инструменте настройте новые IP-адреса основного MAC и RMAC (текущий компьютер).
3. Вернитесь к шагу, на котором вы прервали выполнение **Процедуры восстановления**.

См.

– *Использование средства установки MAC, Страница 57*

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.

ACS

Общий термин для системы управления доступом Bosch, например AMS (Access Management System) или ACE (BIS Access Engine).

CSN

Выборы номера карты.

DCP

Пароль, из которого система управления доступом создает главный ключ, используемый для шифрования сетевого подключения ко всем подчиненным локальным контроллерам доступа (как правило, это устройства AMC).

DSN

Имя источника данных. Имя источника данных в Open Database Connectivity (ODBC).

DTLS

Datagram Transport Layer Security — это безопасный протокол связи, который защищает от подслушивания и взлома.

IDS

Система охранной сигнализации, которую также называют системой обнаружения вторжения.

MAC (главный контроллер доступа)

В системах контроля и управления доступом серверная программа, которая координирует работу локальных контроллеров доступа (как правило, это модульные контроллеры доступа (AMC)) и управляет ими.

REX

«Запрос на выход». Сигнал запроса на отпирание двери изнутри для обеспечения выхода. Обычно сигнал инициируется нажатием кнопки или ручки с внутренней части прохода, а иногда — детектором движения.

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.

RPS (Remote Programming Software)

Программное обеспечение удаленного программирования. Программа, которая управляет пожарными или охранными панелями управления в сети.

SmartIntego

Цифровая система блокировки от Simons Voss Technologies. SmartIntego интегрируется с некоторыми системами контроля доступа Bosch.

Аппаратный ключ AMC

Внутренний код проверки подлинности, который AMC создает на основе определенных параметров оборудования. Он не отображается пользователям.

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.

Главный ключ

Код, созданный системой из пароля связи с устройством (DCP) и используемый для защиты устройств управления доступом. Главный ключ не отображается пользователям.

группа лифта

Группа лифтов, которые совместно обслуживают одни и те же этажи. Каждая группа лифтов управляется сервером ввода направлений (Destination Entry Server - DES).

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.

Инструмент IPConfig

Отдельная дополнительная программа для настройки параметров сети и сетевой безопасности в системе управления доступом.

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.

Надежность пароля

Надежность пароля измеряется на основе таких факторов, как случайность, число доступных символов и фактическое количество используемых символов.

Нормальный режим

В нормальном режиме, в отличие от офисного, доступ предоставляется только лицам, предъявившим считывателю действительные учетные данные.

Область (постановка на охрану)

Группирование проходов в рамках модели прохода 14 в системе управления доступом. Постановка охранной системы на охрану или снятие ее с охраны на любом из этих проходов приведет к такому же действию в отношении всех остальных проходов, у которых параметр «Область постановки на охрану» имеет такое же однобуквенное обозначение.

Офисный режим

Приостановка контроля доступа на входе в рабочее время.

Перенаправитель ввода направлений (DER)

Компьютер на том же уровне, что и сервер ввода направлений (DES) в системе Otis CompassPlus. Он подключается ко всем группам лифта; его задача — это повышение эффективности устройств DES.

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.

Режим конфигурирования

Состояние по умолчанию устройств управления доступом в редакторе устройств. Изменения вступают в силу и передаются в подчиненные устройства немедленно.

Режим работы

Состояние устройства управления доступом в редакторе устройств, когда оно отвечает на команды, посылаемые вне редактора устройств. Изменения конфигурации вступают в силу только после завершения режима работы и восстановления режима конфигурирования.

Сервер MAC

Оборудование: компьютер A (кроме сервера DMS) в системе Access Engine (ACE) или системе управления доступом (AMC), где работает контроллер MAC или RMAC.

Сервер ввода направлений (DES)

Компьютер, который управляет лифтовым холлом для оптимизации времени поездок.

Система диспетчеризации направлений (Destination Dispatching System - DDS)

также известная как система управления направлениями (Destination Management System), но следует использовать только аббревиатуру DDS. Otis CompassPlus — это разновидность DDS.

Система управления данными (DMS)

Процесс верхнего уровня для управления данными контроля доступа в системе. DMS передает данные главным контроллерам доступа (MAC), которые, в свою очередь, предоставляют данные локальным контроллерам доступа (как правило, AMC).

Случайный ключ ЖК-дисплея

Временный буквенно-цифровой код, который AMC создает заново при каждой загрузке. Ключ может быть отображен на жидкокристаллических дисплеях (ЖК-дисплеях) AMC и может запрашиваться программными средствами для аутентификации сетевых соединений.

Терминал ввода направлений (Destination Entry Terminal - DET)

Устройство, на котором пассажир лифта может ввести место назначения для группы лифтов.

Точка

Датчик для обнаружения вторжения в охраняемую область. В некоторых случаях вместо термина «точка» может употребляться термин «зона» или «датчик».

Точка сбора

Место, где, согласно инструкции, должны собраться и ждать люди после эвакуации здания.

шунт

для подавления тревоги при определенных обстоятельствах.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309211038