Контроллер доступа серии F-KD-1300

Руководство пользователя

Руководство пользователя

Настоящее руководство используется для контроллера доступа.

Наименование	Серия
Контроллер доступа	Контроллер доступа серии F-KD-1310
	Контроллер доступа серии F-KD-1320
	Контроллер доступа серии F-KD-1340

Руководство содержит инструкции по использованию продукта. Программное обеспечение, используемое в продукте, регулируется лицензионным соглашением пользователя, охватывающим этот продукт.

О руководстве

Данное руководство подлежит внутренней и международной защите авторских прав. iFLOW оставляет за собой все права на это руководство. Данное руководство пользователя (далее «Руководство») не подлежит воспроизведению, изменению, переводу или распространению, частично или целиком,
без предварительного разрешения iFLOW.

Торговые марки

Торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев. Права
на использование таких товарных знаков без явного разрешения не предоставляются.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, iFLOW НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ
ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, ПОМИМО ПРОЧЕГО, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ, В ОТНОШЕНИИ ДАННОГО РУКОВОДСТВА. iFLOW НЕ РУЧАЕТСЯ, НЕ ГАРАНТИРУЕТ И НЕ ДЕЛАЕТ НИКАКИХ ЗАЯВЛЕНИЙ ОТНОСИТЕЛЬНО ИСПОЛЬЗОВАНИЯ ДАННОГО РУКОВОДСТВА,
А ТАКЖЕ ПРАВИЛЬНОСТИ, ТОЧНОСТИ ИЛИ НАДЕЖНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НЕМ. ВЫ ИСПОЛЬЗУЕТЕ ДАННОЕ РУКОВОДСТВО И ПОЛНОСТЬЮ ПОЛАГАЕТЕСЬ
НА НЕГО НА СВОЙ СТРАХ И РИСК.
ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, НАША КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

ЗАКОНЫ, РЕГУЛИРУЮЩИЕ ВИДЕОНАБЛЮДЕНИЕ, ВАРЬИРУЮТСЯ В ЗАВИСИМОСТИ ОТ СТРАНЫ. ПРОВЕРЬТЕ ВСЕ СООТВЕТСТВУЮЩИЕ ЗАКОНЫ ВАШЕЙ СТРАНЫ ПЕРЕД ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ИСПОЛЬЗОВАНИЕ

ОБОРУДОВАНИЯ В НЕЗАКОННЫХ ЦЕЛЯХ. В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Поддержка

При возникновении каких-либо вопросов, обращайтесь к местному представителю.

Регулирующая информация

Информация о FCC

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, могут привести к аннулированию полномочий пользователя по работе с данным оборудованием.

Соответствие FCC: это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса B, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить необходимую защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:

— Изменить ориентацию или местоположение приемной антенны.

— Увеличить расстояние между оборудованием и приемником.

— Подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник.

— Обратиться к дилеру или опытному радио / телемастеру.

Условия FCC

Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. Эксплуатация допускается при соблюдении следующих двух условий.

1. Данное устройство не должно создавать вредных помех.
2. Данное устройство должно выдерживать возможные помехи, включая те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

Данный продукт и (если применимо) поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивой о радиооборудовании 1999/5/EC, директивой 2014/30/EC EMC, директивой 2014/35/EC LVD, директивой 2011/65/EC RoHS.

2012/19/EC (директива WEEE). Продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей переработки верните этот продукт своему местному поставщику при покупке эквивалентного нового оборудования или утилизируйте его в специально предназначенных точках сбора. За дополнительной

информацией обратитесь по адресу: www.recyclethis.info.

2006/66/EC (директива о батареях): данный продукт оснащен батареей, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb) или ртути (Hg).
Для надлежащей утилизации возвратите батарею своему поставщику либо избавьтесь от нее в специально предназначенных точках сбора. Подробная информация представлена по адресу: www.recyclethis.info.

Профилактические меры и предостерегающие советы

Перед подключением и эксплуатацией устройства, обратите внимание на следующие моменты.

- Убедитесь, что устройство установлено в хорошо проветриваемом, непыльном помещении.
- Не допускайте попадания жидкостей в устройство.
- Убедитесь, что условия окружающей среды соответствуют спецификациям производителя.
- Убедитесь, что устройство надежно закреплено на стойке или полке. Сильные удары или толчки устройства, полученные в результате падения, могут привести к повреждению чувствительной электроники устройства.
- Если позволяют условия, рекомендуется использовать устройство в комбинации с ИБП.
- Перед подключением и отключением аксессуаров и периферийных устройств необходимо отключить питание устройства.
- Для этого устройства следует использовать рекомендованный производителем жесткий диск.

Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем.

Инструкция по технике безопасности

Эта инструкция предназначена для того, чтобы пользователь мог использовать продукт правильно и избежать опасности или причинения вреда имуществу.

Меры предосторожности разделены на **«Предупреждения»** и **«Предостережения»**.

Предупреждения: игнорирование предупреждений может привести к тяжелым травмам или смерти.

Предостережения: игнорирование любого из предостережений может привести к травмам или порче оборудования.

Предупреждения: следуйте данным правилам для предотвращения серьезных травм и смертельных случаев.	**Предостережения:** следуйте мерам предосторожности, чтобы предотвратить возможные повреждения или материальный ущерб.

Предупреждения

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Если продукт не работает должным образом, необходимо обратиться к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. Компания не несет ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.

Предостережения

- Не бросайте устройство и не подвергайте его ударам или воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех. Рекомендуемая рабочая температура составляет от 0 до плюс 45 ℃, температура хранения: от минус 10 до плюс 55 ℃.
- Не подвергайте крышку устройства, предназначенного для использования внутри помещения, воздействию дождя или влаги.

- Не подвергайте устройство воздействию прямых солнечных лучей, не устанавливайте в местах с плохой вентиляцией или рядом с источником тепла таким, как обогреватель или радиатор (пренебрежение этим предостережением может привести к пожару).
- Запрещено направлять устройство на солнце или очень яркие источники света. Яркий свет может вызвать размытие или потерю четкости изображения (что не является признаком неисправности), а также повлиять на срок службы матрицы.
- Используйте прилагаемую перчатку во время демонтажа крышки устройства, избегайте прямого контакта с крышкой устройства, так как пот и жир с пальцев могут стать причиной разрушения защитного покрытия на поверхности устройства.
- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Сохраните упаковку после распаковки для использования в будущем. В случае сбоя работы устройство необходимо вернуть на завод (с оригинальной упаковкой). Транспортировка без оригинальной упаковки может привести к повреждению устройства и к дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Содержание

Раздел 1 Описание продукции 1
1.1 Общая информация 1
1.2 Основные характеристики 1
Раздел 2 Описание компонента 2
Раздел 3 Разъемы 3
3.1 Описание разъемов F-KD-1310 3
3.2 Описание разъемов F-KD-1320 5
3.3 Описание разъемов F-KD-1340 7
Раздел 4 Подключение внешних устройств 10
4.1 Подключение считывателя карт 10
4.1.1 Подключение считывателя карт Wiegand 10
4.1.2 Подключение считывателя карт серии F-KD-4301 11
4.2 Разъемы F-KD-1310 11
4.2.1 Установка катодного замка 11
4.2.2 Установка анодного замка 12
4.3 Подключение внешних тревожных устройств 12
4.4 Схема подключения кнопки открытия двери 13
4.5 Подключение магнитоконтактного датчика 13
4.6 Подключение источника питания 14
Раздел 5 Настройки 15
5.1 Инициализация аппаратной части 15
5.2 Релейный вход NO / NC 16
5.2.1 Релейный выход замка 16
5.2.2 Состояние тревожного релейного выхода 16
Раздел 6 Активация терминала доступа 19
6.1 Активация через ПО SADP 19
6.2 Активация через клиентское программное обеспечение 20
Раздел 7 Работа с клиентским ПО 23
7.1 Функциональный модуль 23
7.2 Регистрация пользователя и вход 23
7.3 Настройка системы 25
7.4 Управление контролем доступа 25
7.4.1 Добавление устройства контроля доступа 27
7.4.2 Отображение состояния устройства 36

7.4.3 Изменение основной информации ... 37
7.4.4 Удаленная настройка ... 37
7.5 Управление пользователями и картами ... 43
7.5.1 Управление организацией ... 44
7.5.2 Управление пользователями ... 45
7.6 Расписание и шаблон ... 54
7.6.1 Расписание рабочей недели ... 55
7.6.2 Группа выходных дней ... 56
7.6.3 Шаблон ... 58
7.7 Конфигурация разрешений ... 60
7.7.1 Добавление разрешений ... 61
7.7.2 Применение разрешений ... 62
7.8 Дополнительные функции ... 63
7.8.1 Параметры контроля доступа ... 64
7.8.2 Аутентификация с помощью считывателя карт ... 66
7.8.3 Открытие двери первой картой ... 67
7.8.4 Запрет двойного прохода по маршруту ... 69
7.8.5 Пароль аутентификации ... 71
7.8.6 Пользовательская настройка Wiegand ... 72
7.9 Поиск события контроля доступа ... 73
7.10 Настройка событий контроля доступа ... 74
7.10.1 Привязка событий контроля доступа ... 74
7.10.2 Привязка тревожного входа устройства контроля доступа ... 76
7.10.3 Привязка карты / события ... 77
7.10.4 Привязка различных устройств ... 79
7.11 Управление состоянием двери ... 80
7.11.1 Управление группой контроля доступа ... 80
7.11.2 Управление состоянием точки контроля доступа (дверь) ... 82
7.11.3 Настройка продолжительности состояния ... 83
7.11.4 Запись считывания карты в режиме реального времени ... 85
7.11.5 Тревога контроля доступа в режиме реального времени ... 86
7.12 Управление постановкой на охрану ... 87
Приложение А Голосовые предупреждения и индикаторы ... 88
Приложение Б Правила Wiegand ... 89

Раздел 1 Описание продукции

1.1 Общая информация

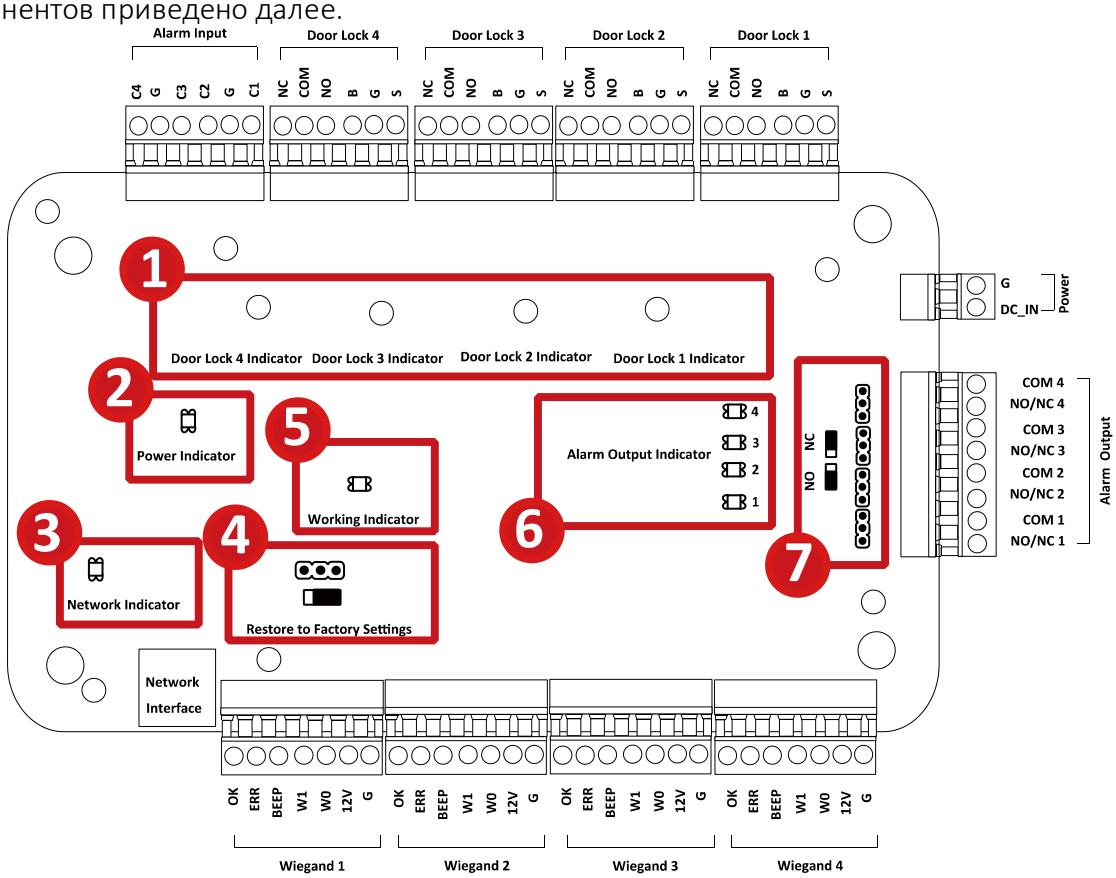
Контроллер доступа F-KD-1300 является эффективным и стабильным контроллером доступа, использующим логическую архитектуру. F-KD-1300 оснащен сетевым интерфейсом TCP / IP, данные связи зашифрованы. Контроллер может работать в автономном режиме. Поддержка детектора саботажа.

1.2 Основные характеристики

- Оснащен 32-битным высокоскоростным процессором.
- Передача данных по TCP / IP сети с адаптивным сетевым интерфейсом. Специальное шифрование данных связи для предотвращения утечки конфиденциальной информации.
- Распознавание и хранение номеров карт с максимальной длиной 20 символов.
- Хранение 10 000 записей о юридических картах и 50 000 записей считывания карт.
- Открытие двери первой картой, авторизация по первой карте, суперкарта, суперпароль, онлайн обновление и дистанционное управление дверьми.
- Поддержка Wiegand для доступа считывателя карт. Интерфейс Wiegand поддерживает W26 / W34 и бесшовное соединение, совместим со сторонним считывателем карт с интерфейсом Wiegand.
- Поддержка различных типов карт: обычные / заблокированные / патрульные / гостевые / по принуждению / суперкарты, карты с расширенными полномочиями и т. д.
- Автоматическая и ручная синхронизация времени при помощи NTP.
- Хранение записей, когда устройство находится офлайн, а также тревога при недостаточном пространстве для хранения.
- Контроллер доступа оснащен сторожевым таймером.
- После выключения контроллера доступа данные хранятся бессрочно.
- Привязка интерфейса входа / выхода и привязка событий.
- Тревога при офлайн событии (более 90 %).
- Несколько методов загрузки событий: канал, центральная группа и прослушивание.
- 500 групп кода аутентификации.
- Запрет двойного прохода.

Раздел 2 Описание компонента

В качестве примера представлено устройство F-KD-1340, схематическое изображение компонентов приведено далее.

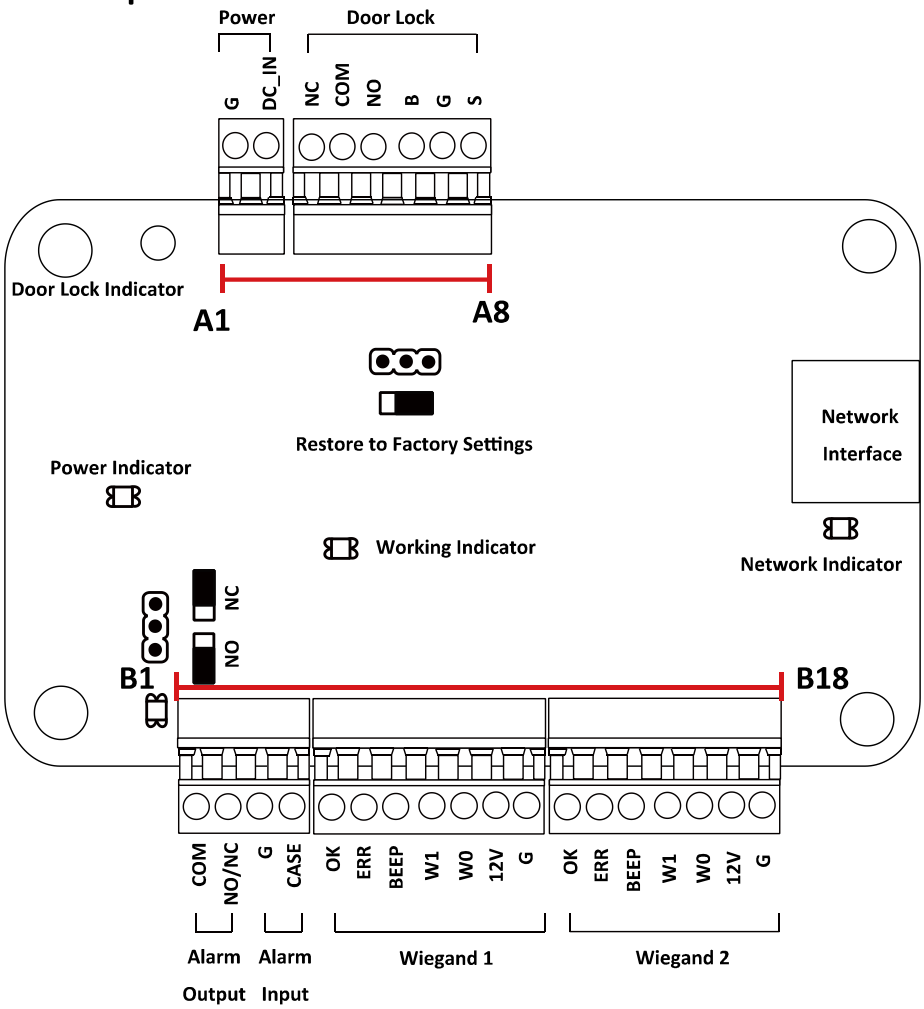


Описание компонентов F-KD-1300

№	Описание компонента		
	F-KD-1310	F-KD-1320	F-KD-1340
1	Индикатор дверного замка 1	Индикатор дверного замка 1 / 2	Индикатор дверного замка 1 / 2 / 3 / 4
2	Индикатор питания		
3	Индикатор сети		
4	Колпачковая перемычка для восстановления заводских настроек		
5	Индикатор рабочего состояния		
6	Индикатор тревожного выхода		
7	Колпачковая перемычка тревожного выхода (NO / NC)		

Раздел 3 Разъемы

3.1 Описание разъемов F-KD-1310

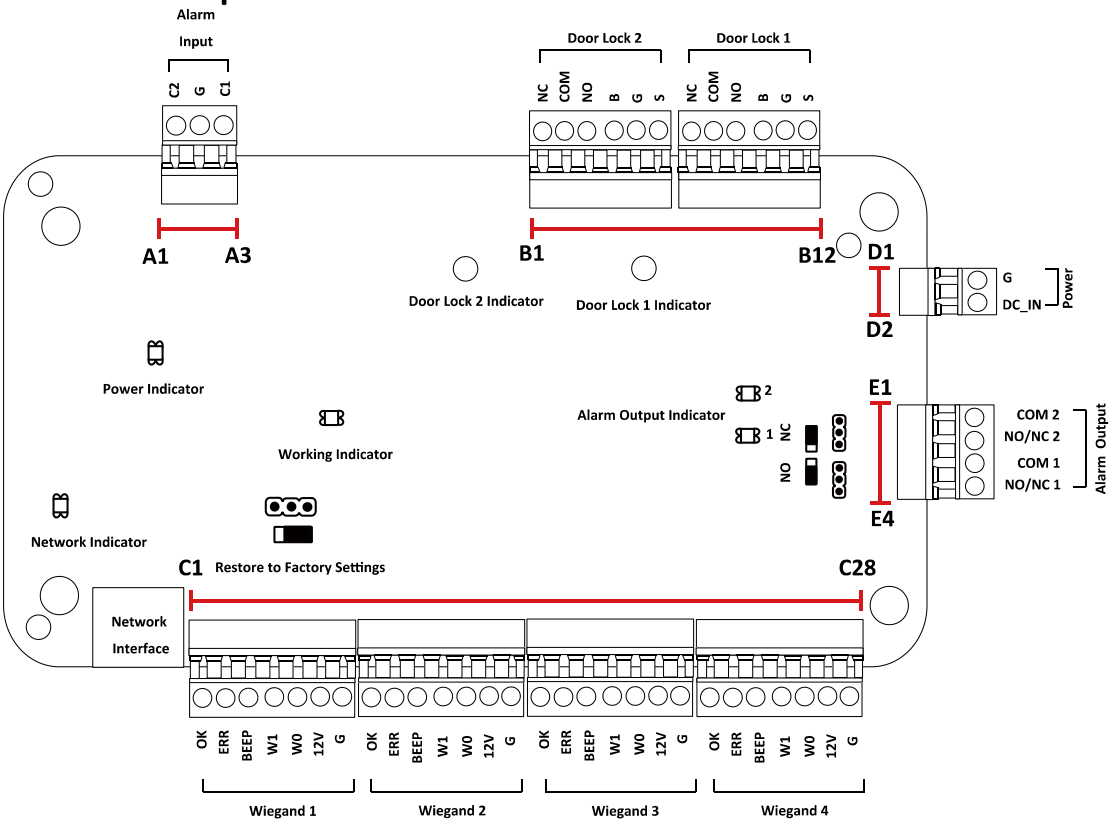


Описание разъемов F-KD-1310

№	F-KD-1310		
A1	Питание	GND	Заземление DC 12 В
A2		+12V	Входное напряжение DC 12 В
A3	Дверь	NC	Релейный выход дверного замка
A4		COM	
A5		NO	
A6		BUTTON	Вход кнопки открытия двери
A7		GND	Заземление
A8		SENSOR	Магнитоконтактный датчик
B1	Тревожный выход	COM	Тревожный релейный выход (сухой контакт)
B2		NO / NC	
B3	Тревожный вход	GND	Заземление

№	F-KD-1310		
B4		IN	Вход событий
B5	Считыватель карт Wiegand 1	OK	Индикатор управления выводом считывателя карт (прием карты)
B6		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B7		BZ	Вывод управления бипером считывателя карт
B8		W1	Интерфейс подключения Wiegand Data1
B9		W0	Интерфейс подключения Wiegand Data0
B10		PWR	Вывод питания считывателя карт
B11		GND	
B12	Считыватель карт Wiegand 2	OK	Индикатор управления выводом считывателя карт (прием карты)
B13		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B14		BZ	Вывод управления бипером считывателя карт
B15		W1	Интерфейс подключения Wiegand Data1
B16		W0	Интерфейс подключения Wiegand Data0
B17		PWR	Вывод питания считывателя карт
B18		GND	

3.2 Описание разъемов F-KD-1320

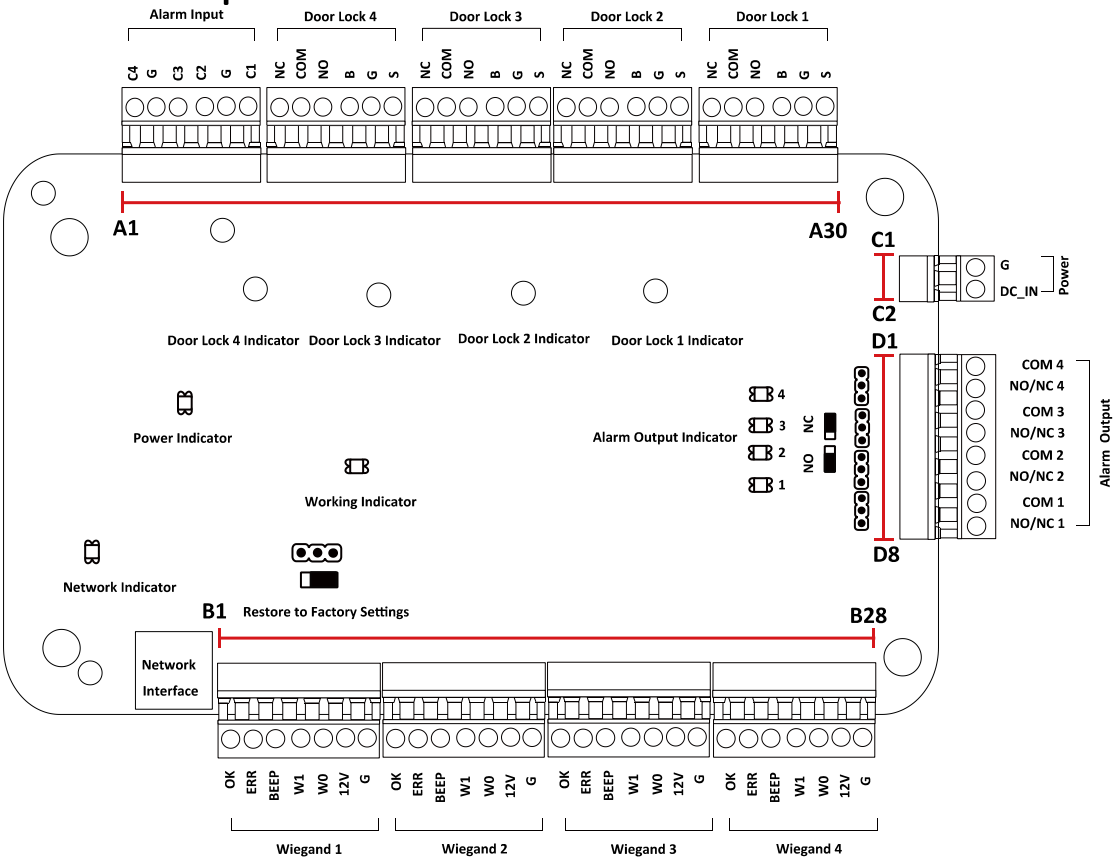


Описание разъемов F-KD-1320

№	F-KD-1320		
A1	Тревожный вход	IN2	Вход событий 2
A2		GND	Заземление
A3		IN1	Вход событий 1
B1	Дверь 2	NC	Релейный выход блокировки двери (сухой контакт)
B2		COM	
B3		NO	
B4		BUTTON	Вход кнопки открытия двери
B5		GND	Заземление
B6		SENSOR	Магнитоконтактный датчик
B7	Дверь 1	NC	Релейный выход блокировки двери (сухой контакт)
B8		COM	
B9		NO	
B10		BUTTON	Вход кнопки открытия двери
B11		GND	Заземление
B12		SENSOR	Магнитоконтактный датчик
D1	Питание	GND	Заземление DC 12 В
D2		+12V	Входное напряжение DC 12 В
E1	Тревожный выход 2	COM2	Тревожный релейный выход 2 (сухой контакт)
E2		NO/NC2	

№	F-KD-1320		
E3	Тревожный выход 1	COM1	Тревожный релейный выход 1 (сухой контакт)
E4		NO/NC1	
C1	Считыватель карт Wiegand 1	OK	Индикатор управления выводом считывателя карт (прием карты)
C2		ERR	Индикатор управления выводом считывателя карт (отказ карты)
C3		BZ	Вывод управления бипером считывателя карт
C4		W1	Интерфейс подключения Wiegand Data1
C5		W0	Интерфейс подключения Wiegand Data0
C6		PWR	Вывод питания считывателя карт
C7		GND	
C8	Считыватель карт Wiegand 2	OK	Индикатор управления выводом считывателя карт (прием карты)
C9		ERR	Индикатор управления выводом считывателя карт (отказ карты)
C10		BZ	Вывод управления бипером считывателя карт
C11		W1	Интерфейс подключения Wiegand Data1
C12		W0	Интерфейс подключения Wiegand Data0
C13		PWR	Вывод питания считывателя карт
C14		GND	
C15	Считыватель карт Wiegand 3	OK	Индикатор управления выводом считывателя карт (прием карты)
C16		ERR	Индикатор управления выводом считывателя карт (отказ карты)
C17		BZ	Вывод управления бипером считывателя карт
C18		W1	Интерфейс подключения Wiegand Data1
C19		W0	Интерфейс подключения Wiegand Data0
C20		PWR	Вывод питания считывателя карт
C21		GND	
C22	Считыватель карт Wiegand 4	OK	Индикатор управления выводом считывателя карт (прием карты)
C23		ERR	Индикатор управления выводом считывателя карт (отказ карты)
C24		BZ	Вывод управления бипером считывателя карт
C25		W1	Интерфейс подключения Wiegand Data1
C26		W0	Интерфейс подключения Wiegand Data0
C27		PWR	Вывод питания считывателя карт
C28		GND	

3.3 Описание разъемов F-KD-1340



Описание разъемов F-KD-1340

№	F-KD-1340		
A1	Тревожный вход	IN4	Вход событий 4
A2		GND	Заземление
A3		IN3	Вход событий 3
A4		IN2	Вход событий 2
A5		GND	Заземление
A6		IN1	Вход событий 1
A7	Дверь 4	NC	Релейный выход блокировки двери (сухой контакт)
A8		COM	
A9		NO	
A10		BUTTON	Вход кнопки открытия двери
A11		GND	Заземление
A12		SENSOR	Магнитоконтактный датчик
A13	Дверь 3	NC	Релейный выход блокировки двери (сухой контакт)
A14		COM	
A15		NO	
A16		BUTTON	Вход кнопки открытия двери
A17		GND	Заземление
A18		SENSOR	Магнитоконтактный датчик

№	F-KD-1340		
A19	Дверь 2	NC	Релейный выход блокировки двери (сухой контакт)
A20		COM	
A21		NO	
A22		BUTTON	Вход кнопки открытия двери
A23		GND	Заземление
A24		SENSOR	Магнитоконтактный датчик
A25	Дверь 1	NC	Релейный выход блокировки двери (сухой контакт)
A26		COM	
A27		NO	
A28		BUTTON	Вход кнопки открытия двери
A29		GND	Заземление
A30		SENSOR	Магнитоконтактный датчик
B1	Считыватель карт Wiegand 1	OK	Индикатор управления выводом считывателя карт (прием карты)
B2		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B3		BZ	Вывод управления бипером считывателя карт
B4		W1	Интерфейс подключения Wiegand Data1
B5		W0	Интерфейс подключения Wiegand Data0
B6		PWR	Вывод питания считывателя карт
B7		GND	
B8	Считыватель карт Wiegand 2	OK	Индикатор управления выводом считывателя карт (прием карты)
B9		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B10		BZ	Вывод управления бипером считывателя карт
B11		W1	Интерфейс подключения Wiegand Data1
B12		W0	Интерфейс подключения Wiegand Data0
B13		PWR	Вывод питания считывателя карт
B14		GND	
B15	Считыватель карт Wiegand 3	OK	Индикатор управления выводом считывателя карт (прием карты)
B16		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B17		BZ	Вывод управления бипером считывателя карт

№	F-KD-1340		
B18		W1	Интерфейс подключения Wiegand Data1
B19		W0	Интерфейс подключения Wiegand Data0
B20		PWR	Вывод питания считывателя карт
B21		GND	
B22	Считыватель карт Wiegand 4	OK	Индикатор управления выводом считывателя карт (прием карты)
B23		ERR	Индикатор управления выводом считывателя карт (отказ карты)
B24		BZ	Вывод управления бипером считывателя карт
B25		W1	Интерфейс подключения Wiegand Data1
B26		W0	Интерфейс подключения Wiegand Data0
B27		PWR	Вывод питания считывателя карт
B28		GND	
C1	Питание	GND	Заземление DC 12 В
C2		+12V	Входное напряжение DC 12 В
D1	Тревожный выход 4	COM4	Тревожный релейный выход 4 (сухой контакт)
D2		NO/NC4	
D3	Тревожный выход 3	COM3	Тревожный релейный выход 3 (сухой контакт)
D4		NO/NC3	
D5	Тревожный выход 2	COM2	Тревожный релейный выход 2 (сухой контакт)
D6		NO/NC2	
D7	Тревожный выход 1	COM1	Тревожный релейный выход 1 (сухой контакт)
D8		NO/NC1	

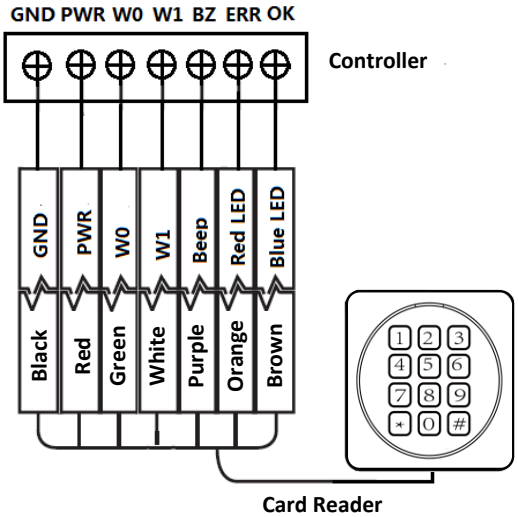
Примечания.

- Аппаратный интерфейс тревожного входа нормально разомкнут по умолчанию. Поэтому допускается только нормально открытый сигнал. Он может быть связан с бипером считывателя карт и контроллером доступа, релейным выходом тревоги и релейным выходом открытой двери.
- Контроллер доступа для одной двери: считыватели карт Wiegand 1 и 2 соответствуют входным и выходным считывателям карт двери 1. Контроллер доступа для двух дверей: считыватели карт Wiegand 1 и 2 соответствуют входным и выходным считывателям карт двери 1, а считыватели карт Wiegand 3 и 4 соответствуют входным и выходным считывателям карт двери 2. Контроллер доступа для четырех дверей: считыватели карт Wiegand 1, 2, 3 и 4 соответствуют входным считывателям карт дверей 1, 2, 3 и 4.

Раздел 4 Подключение внешних устройств

4.1 Подключение считывателя карт

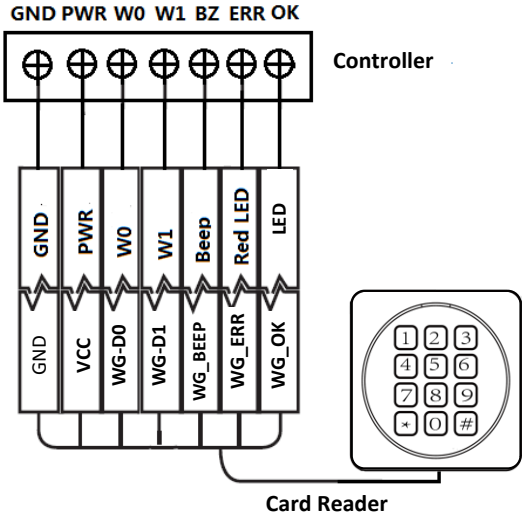
4.1.1 Подключение считывателя карт Wiegand



Английский	Русский
Controller	Контроллер
Card Reader	Считыватель карт
Black	Черный
GND	Заземление
Red	Красный
PWR	Питание
Green	Зеленый
W0	Интерфейс подключения Wiegand Data0
White	Белый
W1	Интерфейс подключения Wiegand Data1
Purple	Фиолетовый
Beep	Звуковой сигнал
Orange	Оранжевый
Red LED	Красный световой индикатор
Brown	Коричневый
Blue LED	Голубой световой индикатор

Примечание. При использовании контроллера доступа для управления светодиодом и бипером считывателя карт Wiegand необходимо подключить разъемы OK / ERR / BZ.

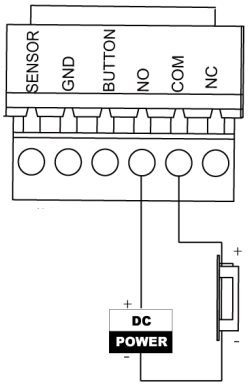
4.1.2 Подключение считывателя карт серии F-KD-4301



Английский	Русский
Controller	Контроллер
Card Reader	Считыватель карт

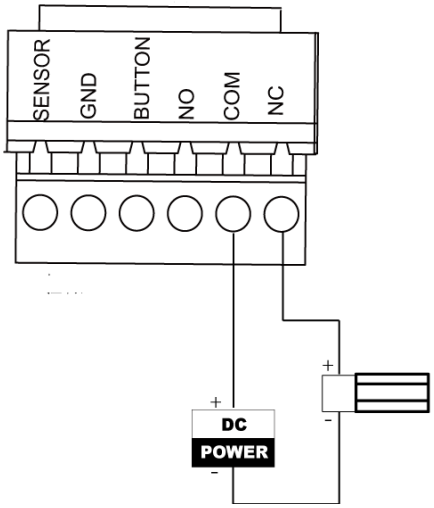
4.2 Разъемы F-KD-1310

4.2.1 Установка катодного замка



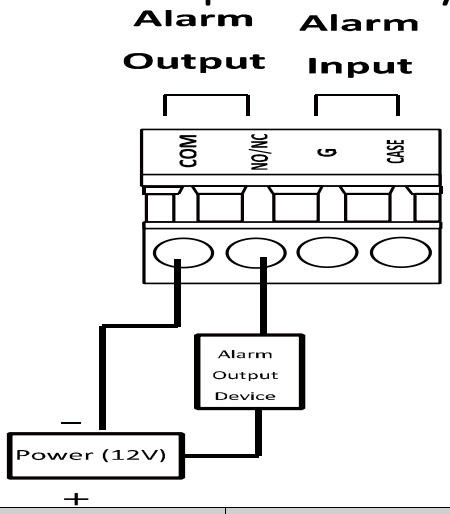
Английский	Русский
SENSOR	Магнитоконтактный датчик
GND	Заземление
BUTTON	Кнопка открытия двери
NO	Нормально открытый
COM	Общий
NC	Нормально закрытый

4.2.2 Установка анодного замка



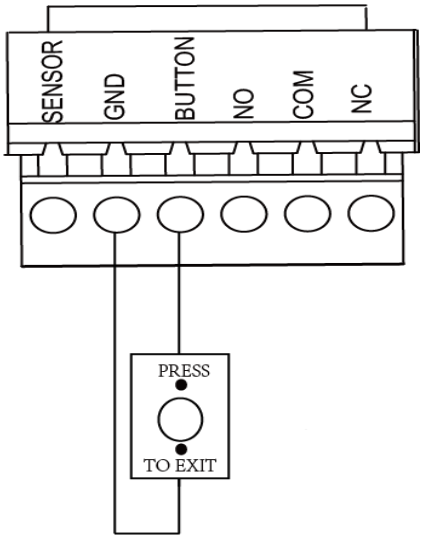
Английский	Русский
SENSOR	Магнитоконтактный датчик
GND	Заземление
BUTTON	Кнопка открытия двери
NO	Нормально открытый
COM	Общий
NC	Нормально закрытый

4.3 Подключение внешних тревожных устройств



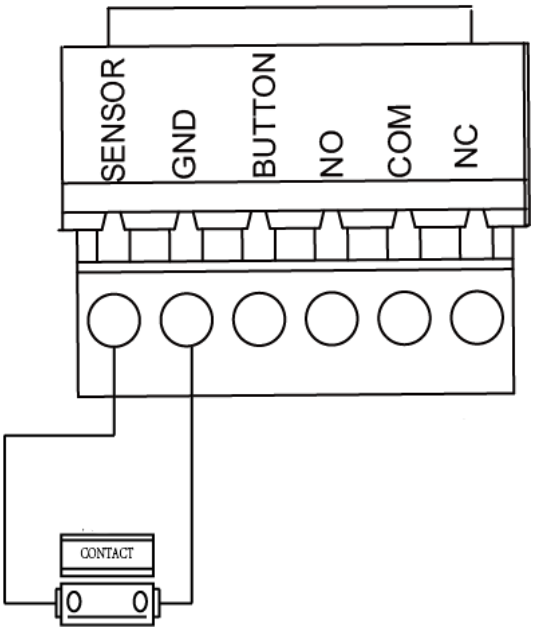
Английский	Русский
Alarm Output	Тревожный выход
Alarm Input	Тревожный вход
Alarm Output Device	Устройство тревожного выхода
Power (12 V)	Питание (12 В)
COM / NO/NC	Нормально открытый, общий, нормально закрытый

4.4 Схема подключения кнопки открытия двери

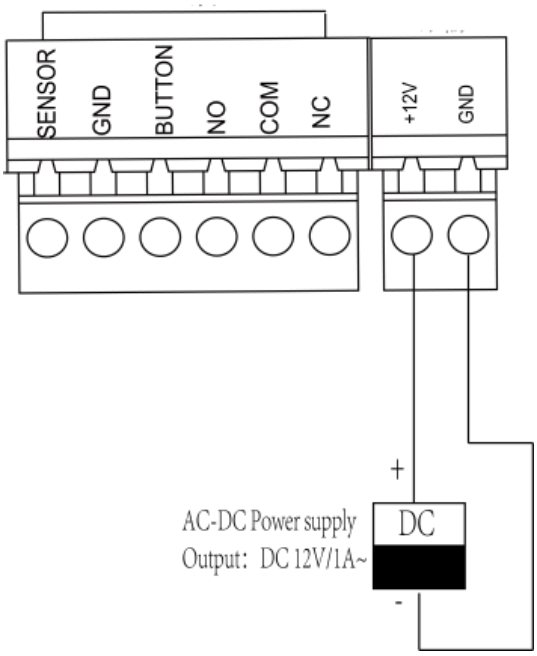


Английский	Русский
SENSOR	Магнитоконтактный датчик
GND	Заземление
BUTTON	Кнопка открытия двери
NO	Нормально открытый
COM	Общий
NC	Нормально закрытый
Press to exit	Нажмите для выхода

4.5 Подключение магнитоконтактного датчика



4.6 Подключение источника питания



Английский	Русский
SENSOR	Магнитоконтактный датчик
GND	Заземление
BUTTON	Кнопка открытия двери
NO	Нормально открытый
COM	Общий
NC	Нормально закрытый
AC-DC Power supply Output: DC 12V / 1A	Питание AC/DC Вывод: DC 12 В / 1 А

Раздел 5 Настройки

5.1 Инициализация аппаратной части

Вариант 1

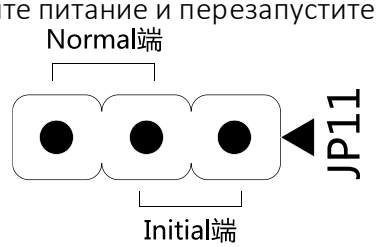
Шаги

1. Переведите колпачковую перемычку из положения **Normal** («Нормальное положение»).
2. Отключите питание и перезапустите контроллер доступа. Бипер контроллера издаст длинный звуковой сигнал.
3. Когда звуковой сигнал прекратится, верните колпачковую перемычку обратно в положение **Normal** («Нормальное положение»).
4. Отключите питание и перезапустите контроллер доступа.

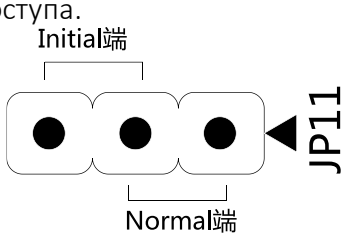
Вариант 2

Шаги

1. Переместите колпачковую перемычку из положения **Normal** («Нормальное положение») в положение **Initial** («Исходное положение»).
2. Отключите питание и перезапустите контроллер доступа. Бипер контроллера издаст длинный звуковой сигнал.
3. Когда звуковой сигнал прекратится, верните колпачковую перемычку обратно в положение **Normal** («Нормально положение»).
4. Отключите питание и перезапустите контроллер доступа.



Инициализация F-KD-1310



Инициализация F-KD-1320 / F-KD-1340

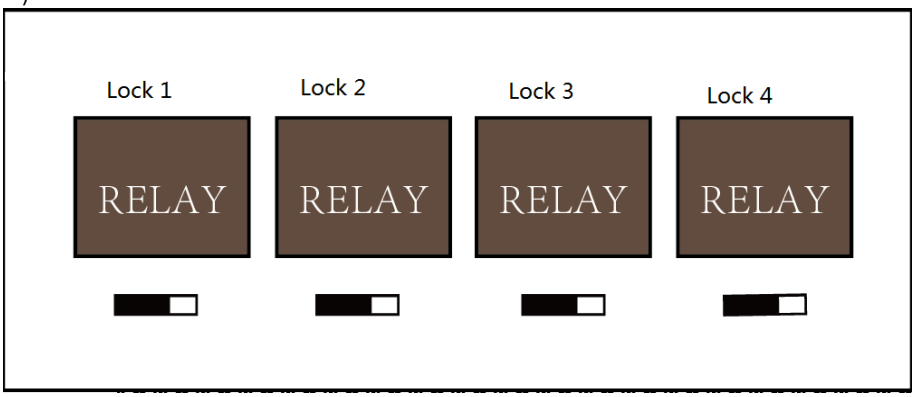
Английский	Русский
NORMAL	Нормальное
Initial	Исходное

Примечание. Инициализация устройства восстановит все параметры до значений по умолчанию, и все события устройства будут удалены.

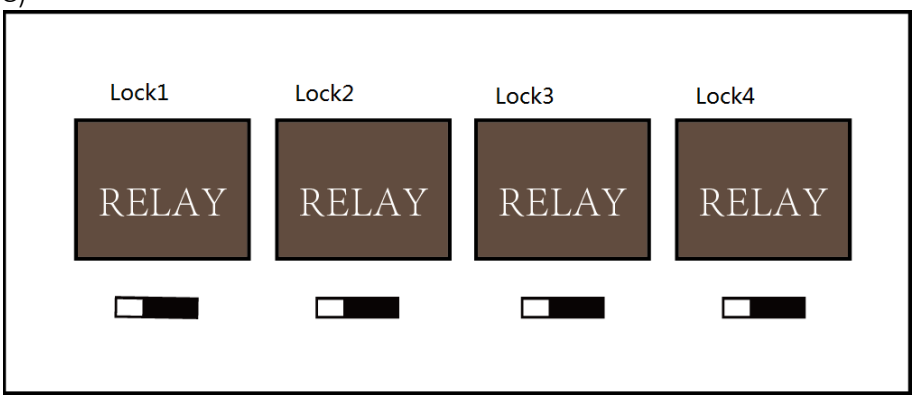
5.2 Релейный вход NO / NC

5.2.1 Релейный выход замка

Реле замка (NO)

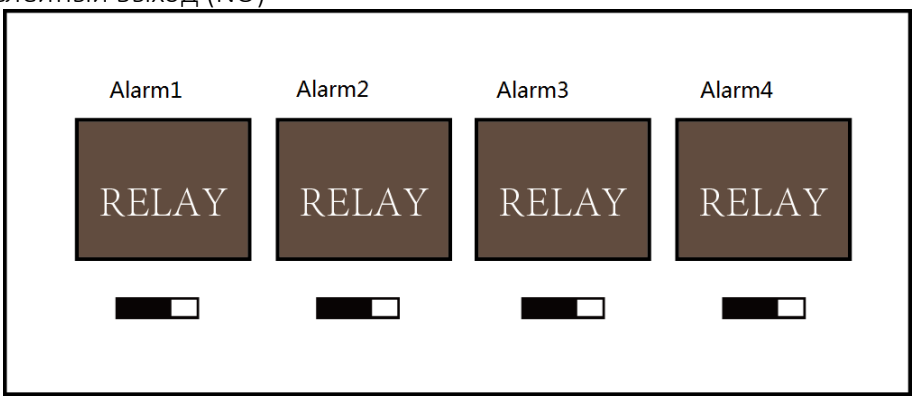


Реле замка (NC)



5.2.2 Состояние тревожного релейного выхода

Тревожный релейный выход (NO)



Тревожный релейный выход (NC)

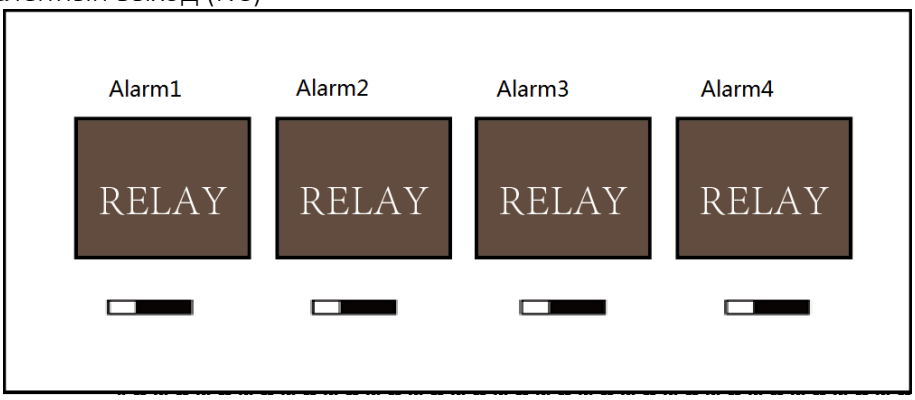
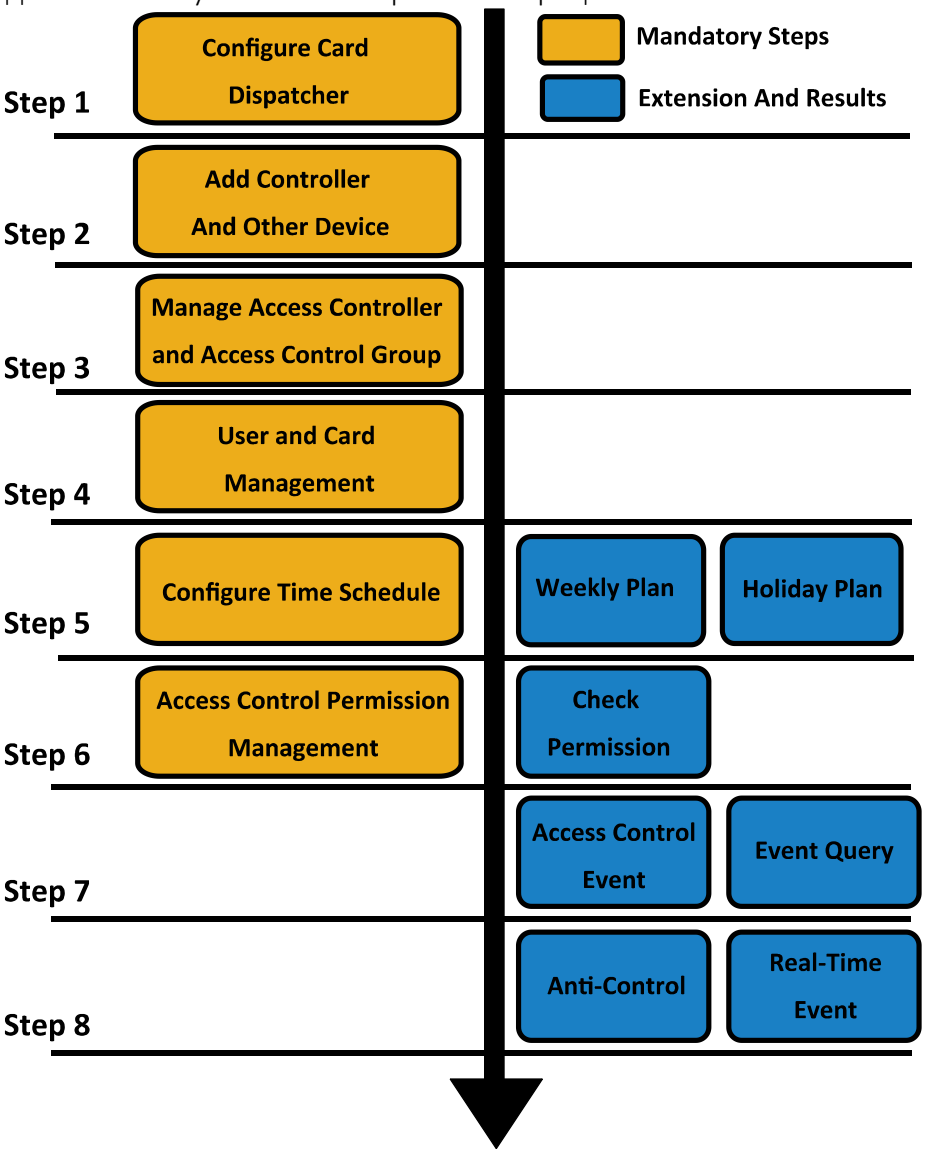


Схема рабочего процесса ПО

Подробная информация представлена в руководстве пользователя клиентского ПО. Далее представлена актуальная схема рабочего процесса.



Английский	Русский
Mandatory Steps	Обязательные шаги
Extension and Results	Расширенные функции и результаты
Configure Card Dispatcher	Настройка устройства для выпуска карт
Add Controller And Other Device	Добавление контроллера и другого устройства
Manage Access Controller and Access Controller Group	Привязка контроллера доступа к группе контроля доступа
User and Card Management	Управление пользователями и картами
Configure Time Schedule	Настройка расписания времени
Access Control Permission Management	Управление разрешениями контроля доступа
Weekly Plan	Еженедельный план
Holiday Plan	План выходных
Check Permission	Проверка разрешений
Access Control Event	Событие контроля доступа
Event Query	Поиск события
Anti-Control	Без управления
Real-Time Event	Событие в режиме реального времени

Раздел 6 Активация терминала доступа

Цель

Перед первым использованием устройства необходимо его активировать.
Поддерживается активация при помощи ПО SADP и при помощи клиентского ПО.
Значения по умолчанию для терминала контроля следующие.

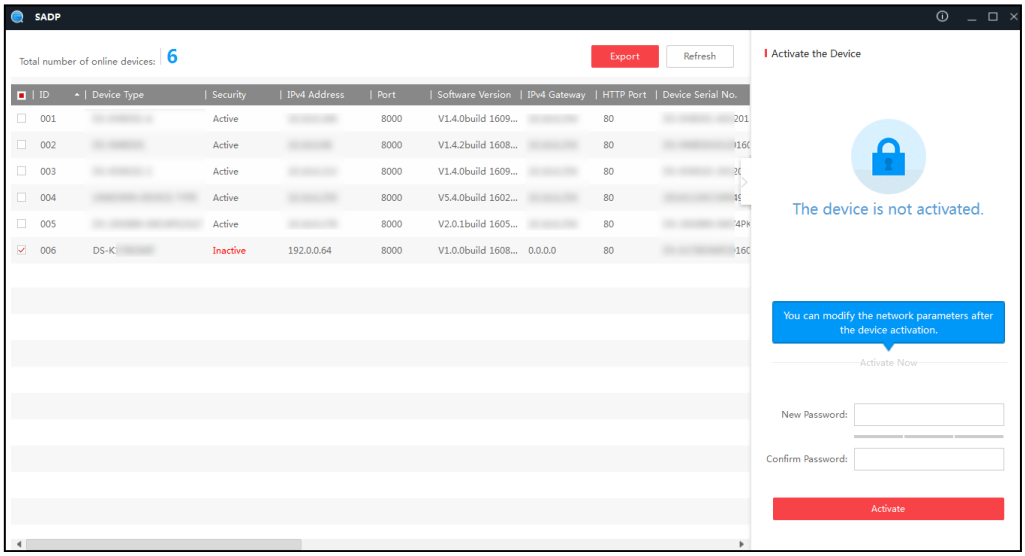
- IP-адрес по умолчанию: 192.0.0.64.
- № порта по умолчанию: 8000.
- Имя пользователя по умолчанию: admin.

6.1 Активация через ПО SADP

ПО SADP используется для обнаружения онлайн-устройств, активации устройства и смены пароля.
ПО SADP представлено на диске, входящем в комплект. Установите ПО SADP в соответствии с инструкцией. Выполните следующие шаги для активации панели управления.

Шаги

1. Запустите ПО SADP для поиска онлайн устройств.
2. Проверьте состояние устройства в списке устройств и выберите неактивное устройство.

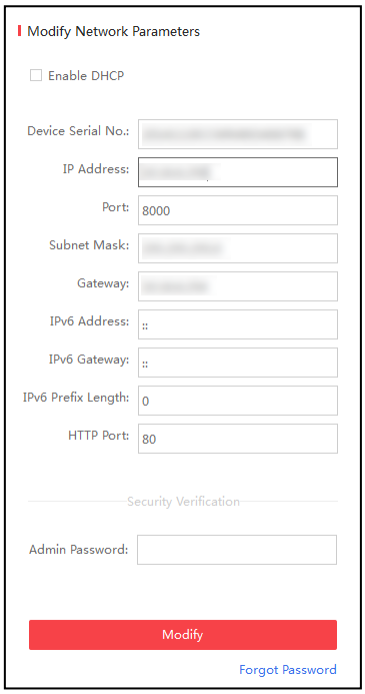


3. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его, нажав **Confirm Password** («Подтвердить пароль»).

<u>РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ</u> – *настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.*

4. Нажмите **Activate** («Активировать») для активации устройства.

5. Проверьте активированное устройство. Можно изменить IP-адрес устройства на адрес подсети вашего компьютера вручную или поставив галочку в поле **Enable DHCP** («Включить DHCP»).



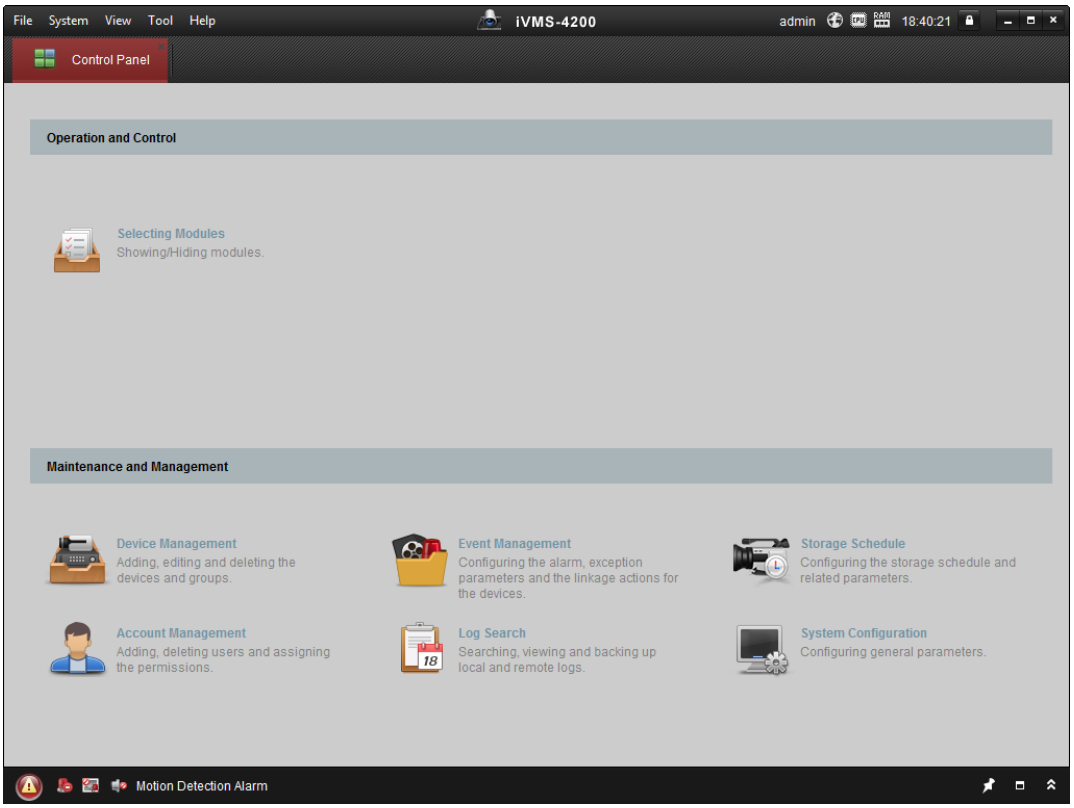
6. Введите пароль и нажмите кнопку **Modify** («Изменить») для изменения вашего IP-адреса.

6.2 Активация через клиентское программное обеспечение

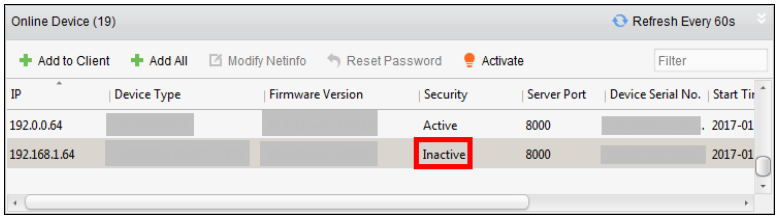
Клиентское программное обеспечение является универсальным программным обеспечением для управления видео и используется на различных типах устройств.
Клиентское ПО представлено на диске, входящем в комплект. Установите ПО в соответствии с инструкцией. Выполните следующие шаги для активации панели управления.

Шаги

1. Запустите клиентское программное обеспечение, появится панель управления программным обеспечением, как показано на рисунке ниже.



2. Нажмите **Device Management** («Управление устройством») для перехода в меню управления устройством.
3. Проверьте статус устройства в списке устройств и выберите неактивное устройство.



4. Для появления интерфейса активации нажмите **Activate** («Активировать»).
5. Во всплывающем окне создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердите пароль»).

<u>РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ</u> – *настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.*

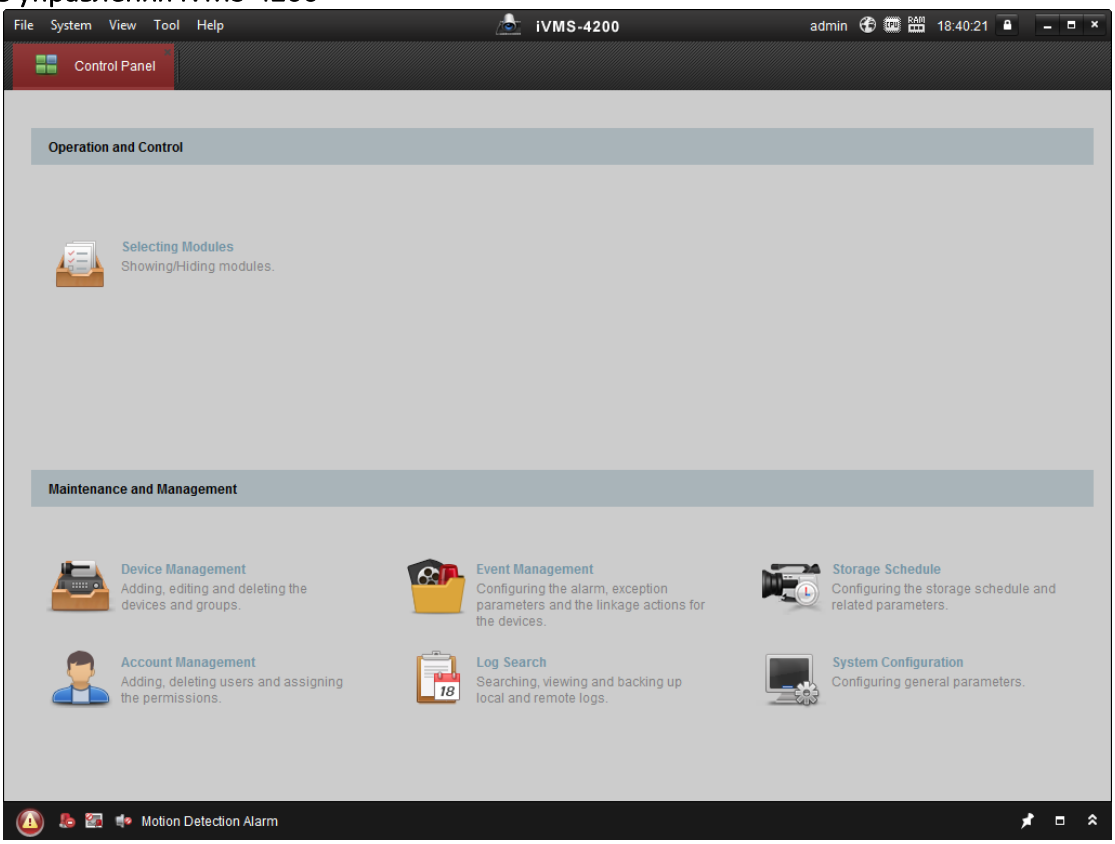
6. Нажмите OK, чтобы начать активацию.
7. Нажмите кнопку Modify Netinfo («Изменить сетевую информацию») для открытия интерфейса изменения сетевых параметров.
8. Измените вручную IP-адрес устройства на адрес подсети вашего компьютера.
9. Введите пароль и нажмите OK для сохранения настроек.

Раздел 7 Работа с клиентским ПО

Устройства контроля доступа можно настраивать и управлять ими через клиентское программное обеспечение. В данном разделе представлены операции устройства контроля доступа в клиентском программном обеспечении. Подробная информация об операциях представлена в *Руководстве пользователя клиентского ПО iVMS-4200.*

7.1 Функциональный модуль

Панель управления iVMS-4200

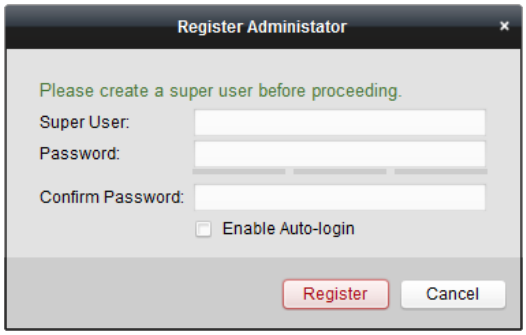


7.2 Регистрация пользователя и вход

При первом использовании клиентского ПО iVMS-4200 необходимо зарегистрировать учетную запись суперпользователя для входа в систему.

Шаги

1. Введите имя суперпользователя и пароль. ПО автоматически проверит надежность пароля. Настоятельно рекомендуется использовать надежный пароль для обеспечения безопасности данных.
2. Подтвердите пароль.
3. Опционально: нажмите **Enable Auto-login** («Включить автоматический вход в систему») для автоматического входа в ПО.
4. Нажмите **Register** («Регистрация»). Затем можно войти в ПО в качестве суперпользователя.

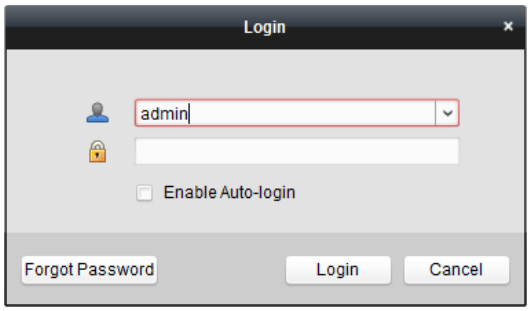


- *Имя пользователя не может содержать следующие символы: / \ : * ? “ < > |. Длина пароля должна превышать 6 символов.*
- *Для обеспечения безопасности системы, настоятельно рекомендуем изменить пароль на свой собственный (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы).*
- *Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.*

После регистрации при открытии iVMS-4200 можно войти в клиентское ПО, используя зарегистрированное имя пользователя и пароль.

Шаги

1. Введите зарегистрированное имя пользователя и пароль.
   Примечание. Если вы забыли пароль, нажмите **Forgot Password** («Забыли пароль») и запомните зашифрованную строку во всплывающем окне. Свяжитесь со дилером и отправьте ему зашифрованную строку для сброса пароля.
2. Опционально: нажмите **Enable Auto-login** («Включить автоматический вход в систему») для автоматического входа в ПО.
3. Нажмите **Login** («Вход»).



После запуска клиентского ПО можно открыть соответствующий мастер (в том числе мастер управления видео, мастер видеостены, мастер панели управления безопасностью, мастер управления доступом и видеодомофоном, мастер УРВ), который поможет добавить необходимое устройство и выполнить другие настройки и операции. Подробная информация о настройке мастеров представлена в *кратком руководстве пользователя iVMS-4200.*

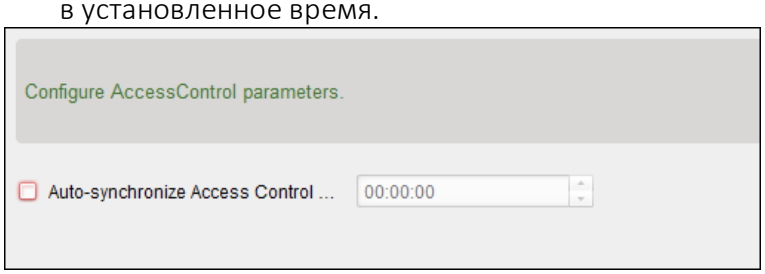
7.3 Настройка системы

Цель

Можно синхронизировать пропущенные события контроля доступа с клиентом.

Шаги

1. Нажмите **Tool** → **System Configuration** («Инструмент → Настройка системы»).
2. В окне настройки системы нажмите **Auto-synchronize Access Control Event** («Автоматическая синхронизация события контроля доступа»).
3. Настройте время синхронизации.
   Клиент автоматически синхронизирует пропущенное событие контроля доступа в установленное время.



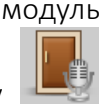
7.4 Управление контролем доступа

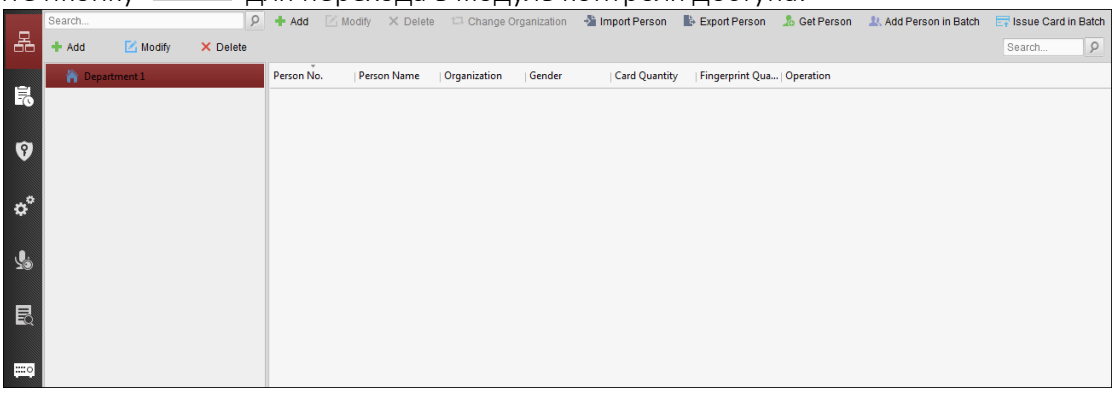
Цель

Модуль контроля доступа применим к устройствам контроля доступа и устройству видеодомофонии. Модуль реализует множество функций, включая управление записями сотрудников / посетителей и картами, настройку разрешений, управление состоянием устройств контроля доступа, видеодомофона, а также другие расширенные функции. Можно настроить события для устройств контроля доступа и отображать точки и зоны контроля доступа на электронной карте.

Примечание. Для пользователя с разрешениями модуля контроля доступа: он может войти в модуль **Access Control** («Контроль доступа») и управлять настройками доступа.

Нажмите на панели управления и нажмите **Access Control** («Контроль доступа»), чтобы добавить модуль контроля доступа в панель управления.

Нажмите иконку  для перехода в модуль контроля доступа.



Перед началом

При первом открытии модуля контроля доступа появится диалоговое окно, в котором потребуется выбрать сцену в соответствии с задачами.

Можно выбрать следующие сцены: Non-residence («Нежилая недвижимость») и Residence («Жилая недвижимость»).

Примечания.

- После выбора сценария применения, его невозможно изменить.
- В сценарии применения «Нежилая недвижимость» при добавлении пользователя нельзя настроить УРВ.

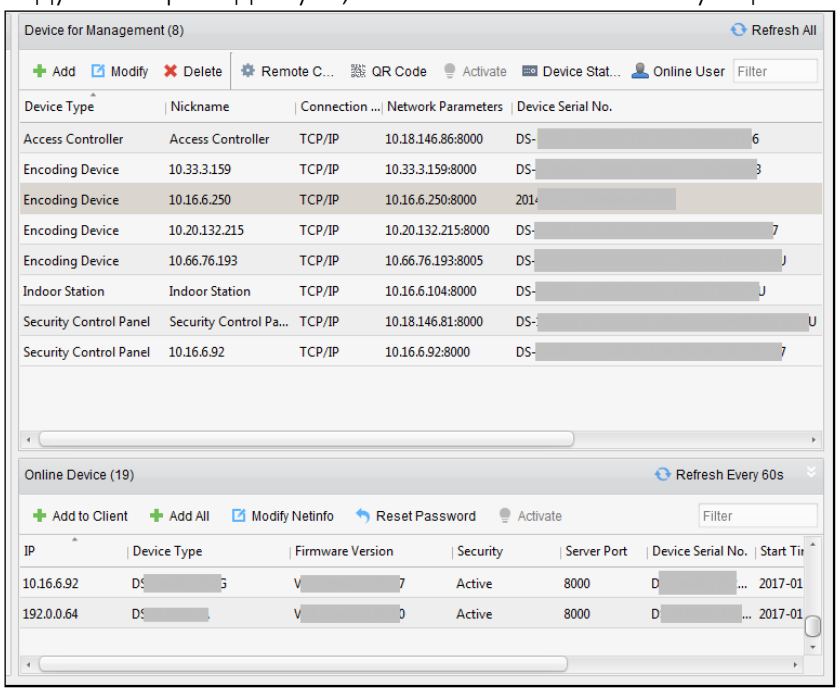
Модуль контроля доступа состоит из следующих дополнительных модулей.

	Person and Card («Пользователи и карты»)	Управление организациями, сотрудниками / посетителями и присвоение карт пользователям.
	Schedule and Template («Расписания и шаблоны»)	Настройка расписания рабочей недели, группы выходных дней и настройка шаблона.
	Permission («Разрешение»)	Назначение разрешений на контроль доступа пользователям и применение к устройствам.
	Advanced Function («Дополнительные функции»)	Реализация дополнительных функций, включая настройки параметров контроля доступа, аутентификацию считывателя карт, открытие двери первой картой, запрет двойного прохода, блокировку нескольких дверей и пароль аутентификации.
	Video Intercom («Видеодомофония»)	Видеодомофония между клиентом и жильцом, поиск в журнале набора и отправка уведомлений.
	Search («Поиск»)	Поиск по истории событий контроля доступа; поиск журналов вызовов, журналов открытия двери и уведомлений.
	Device Management («Управление устройствами»	Управление устройствами контроля доступа и устройствами видеодомофонии.

Примечание. В данной главе описаны только операции, связанные с контролем доступа.

7.4.1 Добавление устройства контроля доступа

Нажмите в модуле контроля доступа, чтобы войти в соответствующий интерфейс.



Примечание. После добавления устройства необходимо проверить состояние постановки устройства на охрану в **Tool → Device Arming Control** («Инструмент → Управление постановкой на охрану»). Если устройство не поставлено на охрану, необходимо поставить его на охрану, иначе события в клиентском ПО отображаться не будут. Подробная информация об управлении постановкой на охрану представлена в разделе *7.12 Управление постановкой* на охрану.

Создание пароля

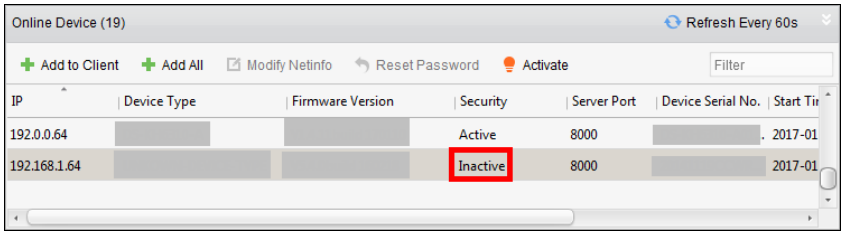
Цель

Для исправной работы некоторых устройств необходимо создать пароль активации, прежде чем добавлять их в систему.

Примечание. Устройство должно поддерживать данную функцию.

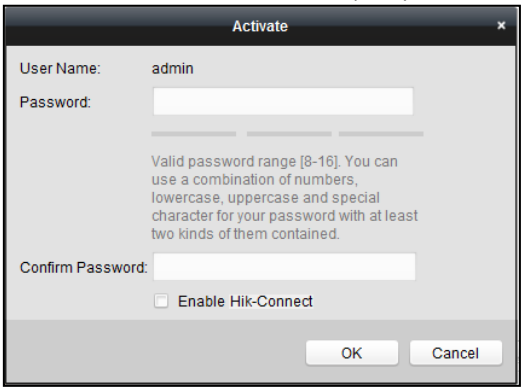
Шаги

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. В поле **Device for Management** («Устройство для управления») или **Online Device** («Онлайн устройство») проверьте состояние устройства (отображается в столбце **Security** («Безопасность») и выберите неактивное устройство.

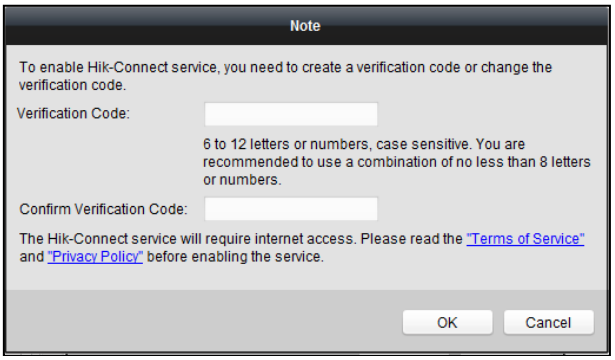


3. Для появления интерфейса активации нажмите **Activate** («Активировать»).
4. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).

<u>РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ</u> – *настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы).*
Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.



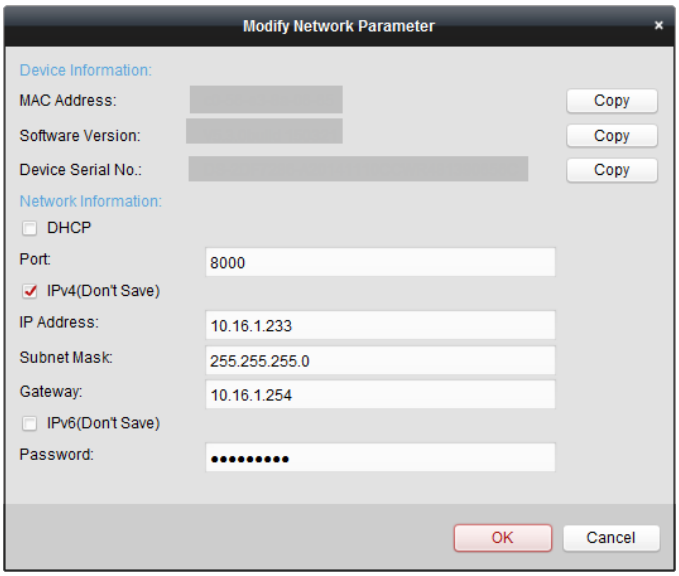
5. (Опционально) Включите Hik-Connect при активации устройства (устройство должно поддерживать функцию).
   1) Нажмите **Enable Hik-Connect** («Включить Hik-Connect»), чтобы открыть диалоговое окно примечаний.



   2) Создайте проверочный код.
   3) Подтвердите проверочный код.
   4) Нажмите **Terms of Service** («Условия предоставления услуг») и **Privacy Policy** («Политика конфиденциальности») и ознакомьтесь с условиями предоставления услуг и политикой конфиденциальности.

5) Нажмите **OK**, чтобы включить Hik-Connect.

6. Нажмите **OK** для активации устройства.
   После успешного введения пароля появится окно **The device is activated** («Устройство активировано»).
7. Нажмите **Modify Netinfo** («Изменить сетевую информацию»), чтобы открыть интерфейс изменения параметров сети.
   Примечание. Данная функция доступна только в поле **Online Device** («Онлайн устройство»). Если необходимо добавить устройство в ПО, измените IP-адрес устройства на ту же подсеть, что и компьютер.
8. Измените IP-адрес устройства на адрес в той же подсети, к которой подключен компьютер, вручную или поставив галочку **Enable DHCP** («Включить DHCP»).
9. Введите пароль, заданный в рамках шага 4, и нажмите **OK**, чтобы завершить настройки сети.

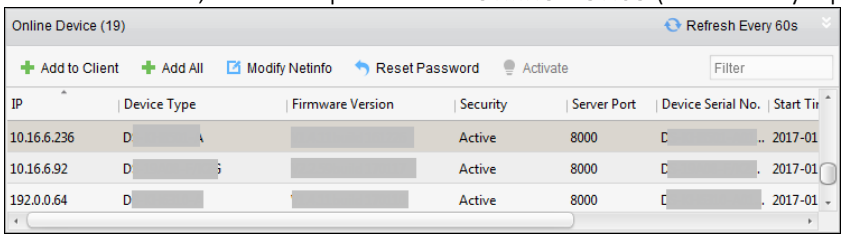


Добавление активных устройств

Цель

Активные устройства управления доступом, которые находятся в одной локальной подсети с клиентом, отображаются в области **Online Device** («Активные устройства»). Нажмите кнопку **Refresh Every 60s** («Обновлять каждые 60 с»), чтобы обновить информацию об активных устройствах.

Примечание. Можно нажать , чтобы скрыть поле **Online Device** («Онлайн устройство»)



Шаги

1. Выберите из списка устройства, которые нужно добавить.

Примечание. Прежде чем правильно добавить неактивное устройство необходимо создать для него пароль. Подробная инструкция представлена в *Chapter 6 Раздел 6 Активация* терминала доступа.

2. Нажмите **Add to Client** («Добавить в клиент»), чтобы открыть окно добавления устройства.
3. Введите необходимую информацию.

   Название: измените название устройства по своему выбору.

   Адрес: введите IP-адрес устройства. IP-адреса устройств получаются автоматически в данном режиме добавления.

   Порт: введите № порта устройства. Значение по умолчанию: *8000*.

   Имя пользователя: введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

   Пароль: введите пароль устройства.

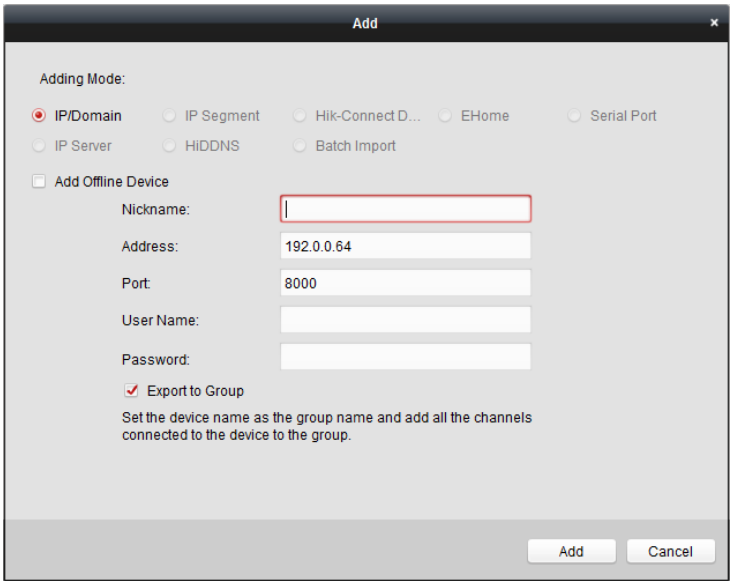
   Надежность пароля устройства может быть проверена ПО. Для обеспечения безопасности системы, настоятельно рекомендуем изменить пароль на свой собственный (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
4. Опционально: нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

   По умолчанию можно импортировать все каналы устройства в соответствующую группу.

   Примечание. С помощью iVMS-4200 можно также добавить автономные устройства.

   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
5. Нажмите **Add** («Добавить»), чтобы добавить устройство.

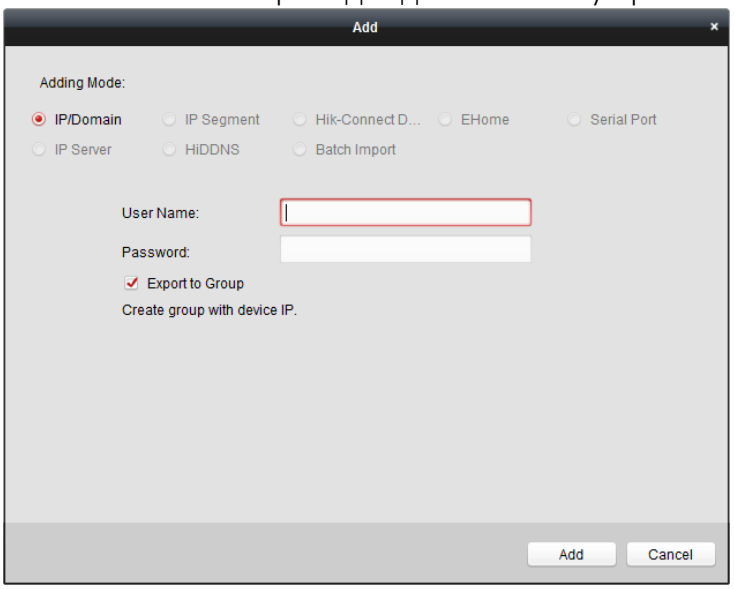


➢ Добавление нескольких онлайн устройств

Если хотите добавить несколько онлайн устройств в клиентское программное обеспечение, нажмите и удерживайте клавишу *Ctrl*, чтобы выбрать несколько устройств, и нажмите **Add to Client** («Добавить в клиент»), чтобы открыть диалоговое окно добавления устройства. Во всплывающем диалоговом окне введите имя пользователя и пароль для добавляемых устройств.

➢ Добавление всех онлайн устройств

Если хотите добавить все онлайн устройства в клиентское программное обеспечение, нажмите **Add All** («Добавить все») и нажмите **OK** во всплывающем диалоговом окне. Затем введите имя пользователя и пароль для добавляемых устройств.



Добавление устройств по IP-адресу или доменному имени

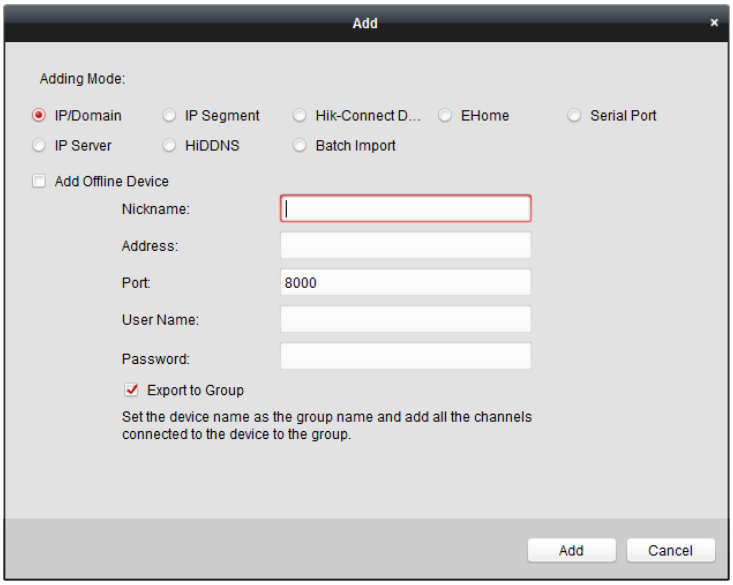
Шаги

1. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.

2. Выберите значение **IP/Domain** («IP/Домен») в поле **Adding Mode** («Режим добавления»).
3. Введите необходимую информацию.
   Название: Измените название устройства по своему выбору.
   Адрес: Введите IP-адрес устройства или доменное имя.
   Port («Порт»): Введите № порта устройства. Значение по умолчанию: 8000.
   User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).
   Password («Пароль»): Введите пароль устройства.

   Надежность пароля устройства может быть проверена ПО. Для обеспечения безопасности системы, настоятельно рекомендуем изменить пароль на свой собственный (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
4. Опционально: нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.
   По умолчанию можно импортировать все каналы устройства в соответствующую группу.
   Примечание. С помощью iVMS-4200 можно также добавить автономные устройства.
   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
5. Нажмите **Add** («Добавить»), чтобы добавить устройство.



Добавление устройств по сегменту IP-адресов

Шаги

1. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
2. Выберите **IP Segment** («Сегмент IP-адресов») в поле **Adding Mode** («Режим добавления»).
3. Введите необходимую информацию.

   Начальный сегмент IP-адреса: введите начальный сегмент IP-адреса.

   Конечный сегмент IP-адреса: введите конечный сегмент IP-адреса в том же сегменте сети, что и начальный IP-адрес.

   Порт: введите № порта устройства. Значение по умолчанию: 8000.

   Имя пользователя: введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

   Пароль: введите пароль устройства.

   Надежность пароля устройства может быть проверена ПО. Для обеспечения безопасности системы, настоятельно рекомендуем изменить пароль на свой собственный (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
4. Опционально: нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.

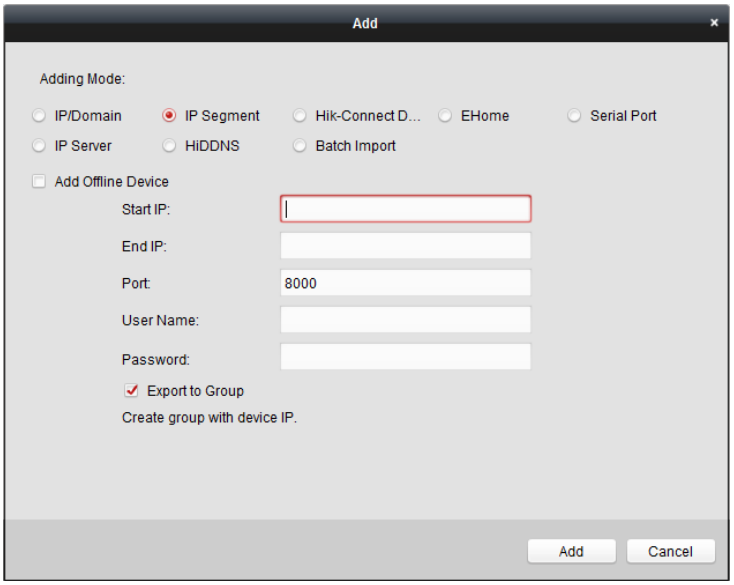
   По умолчанию можно импортировать все каналы устройства в соответствующую группу.

   Примечание. С помощью iVMS-4200 можно также добавить автономные устройства.

   1) Нажмите **Add Offline Device** («Добавление автономных устройств»).
   2) Введите необходимую информацию, в том числе номер канала устройства и номер тревожного входа.
   3) Нажмите **Add** («Добавить»).

   Когда автономное устройство подключается к сети, программное обеспечение подключает его автоматически.
5. Нажмите **Add** («Добавить»).

   В список устройств можно добавить устройство, IP-адрес которого находится между начальным и конечным IP-адресами.



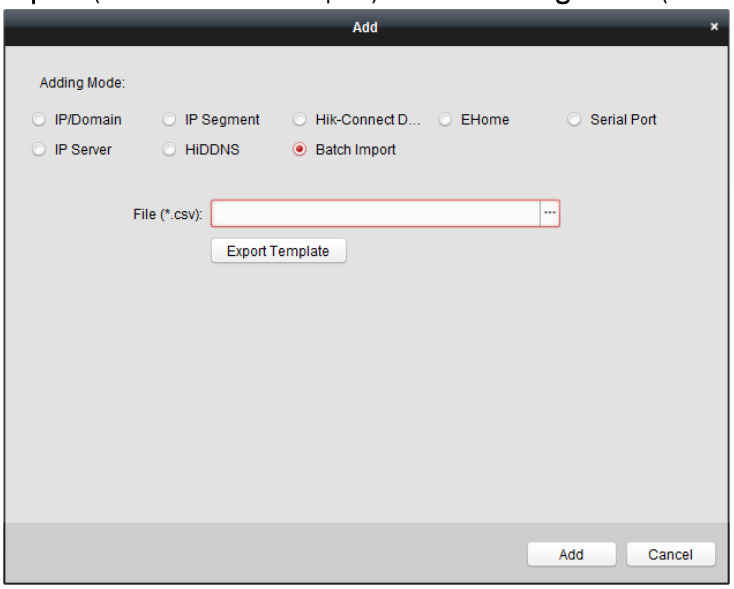
Импорт устройств в пакетном режиме

Цель

Устройства могут быть добавлены в ПО в пакетном режиме, для этого необходимо ввести информацию об устройствах в предварительно заданный файл CSV.

Шаги

1. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
2. Выберите **Batch Import** («Пакетный импорт») в поле **Adding Mode** («Режим добавления»).



3. Нажмите **Export Template** («Скачать шаблон») и сохраните предварительно выбранный шаблон (файл CSV) на компьютере.
4. Откройте экспортированный файл шаблона и введите необходимую информацию об устройствах, подлежащих добавлению, в соответствующие столбцы.
   Nickname («**Название**»): измените название устройства по своему выбору.
   Adding Mode («**Режим добавления**»): можно ввести значения 0, 2, 3, 4, 5 или 6, что означает разные режимы добавления.

0: устройство добавлено по IP-адресу или доменному имени;
2: устройство добавлено через IP-сервер;
3: устройство добавлено через HiDDNS;
4: устройство добавлено по протоколу EHome;
5: устройство добавлено через серийный интерфейс;
6: устройство добавлено через Hik-Connect.

Address («Адрес»): измените адрес устройства. Если установить 0 в поле режима добавления, необходимо ввести IP-адрес или доменное имя устройства; если установить 2 в поле режима добавления, необходимо ввести IP-адрес ПК, на котором установлен IP-сервер; если установить 3 в поле режима добавления, необходимо ввести www.hik-online.com.

Port («Порт»): введите № порта устройства. Значение по умолчанию: 8000.

Device Information («**Информация об устройстве»)**: если установить 0 в поле режима добавления, заполнение данного поля не обязательно; если установить 2 в поле режима добавления, необходимо ввести идентификатор устройства, зарегистрированного на IP-сервере; если установить 3 в поле режима добавления, необходимо ввести доменное имя устройства, зарегистрированное на сервере HiDDNS; если установить 4 в поле режима добавления, необходимо ввести данные учетной записи EHome; если установить 6 в поле режима добавления, необходимо ввести серийный номер устройства.

User Name («Имя пользователя»): введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

Password («Пароль»): введите пароль устройства.

Надежность пароля устройства может быть проверена ПО. Для обеспечения безопасности системы, настоятельно рекомендуем изменить пароль на свой собственный (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

Add Offline Device («Добавление автономных устройств»): введите ***1***, чтобы разрешить добавление автономного устройства, а затем программное обеспечение автоматически подключит его, когда автономное устройство подключится к сети. Если выбрано значение 0, значит функция отключена.

Export to Group («Экспорт в группу»): введите 1, чтобы создать группу по названию устройства. Все каналы устройства будут импортированы в соответствующую группу по умолчанию. Если выбрано значение 0, значит функция отключена.

Channel Number («Номер IP-канала»): если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***1***, необходимо ввести номер канала устройства. Если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***0***, заполнение данного поля не обязательно.

Alarm Input Number («Номер тревожного входа»): если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение ***1***, необходимо ввести номер тревожного входа устройства.

Если в поле **Add Offline Device** («Добавление неактивных устройств») установлено значение *0*, заполнение данного поля не обязательно.

Serial Port No. («Номер серийного интерфейса»): если в поле режима добавления установлено значение *5*, необходимо ввести номер серийного интерфейса для устройства контроля доступа.

Baud Rate («Скорость передачи данных»): если в поле режима добавления установлено значение *5*, необходимо ввести скорость передачи данных (в бодах) для устройства контроля доступа.

DIP («Адрес DIP-переключателя»): если в поле режима добавления установлено значение *5*, необходимо ввести DIP-адрес для устройства контроля доступа.

Hik-Connect Account («Учетная запись Hik-Connect»): если в поле режима добавления установлено значение *6*, необходимо ввести данные учетной записи Hik-Connect.

Hik-Connect Password («Пароль Hik-Connect»): если в поле режима добавления установлено значение *6*, необходимо ввести пароль учетной записи Hik-Connect.

5. Нажмите ··· и выберите файл шаблона.
6. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

После успешного добавления устройства будут отображаться в списке устройств для управления. Можно проверить использование ресурсов, состояние жесткого диска, состояние записи и другую информацию о добавленных устройствах в списке. Нажмите **Refresh All** («Обновить все»), чтобы обновить информацию обо всех добавленных устройствах. Также можно ввести имя устройства в поле фильтра для поиска.

7.4.2 Отображение состояния устройства

В списке устройств можно выбрать устройство, а затем нажать кнопку **Device Status** («Состояние устройства»), чтобы просмотреть его состояние.

Примечание. Интерфейс может отличаться от изображения, представленного выше. При использовании этой функции ориентируйтесь на фактический интерфейс клиента.

Door Status («Состояние двери»): состояние подключенной двери.

Host Status («Состояние хоста»): состояние хоста, включая напряжение питания аккумуляторной батареи, состояние источника питания устройства, состояние блокировки нескольких дверей, состояние запрета обратного прохода и состояние детектора саботажа.

Card Reader Status («Состояние считывателя карт»): состояние считывателя карт.

Примечание. Состояние считывателя карт RS-485 можно просматривать онлайн и офлайн. Состояние считывателя карт Wiegand можно просматривать офлайн.

Alarm Output Status («Состояние тревожного выхода»): состояние тревожного выхода каждого порта.

Event Sensor Status («Состояние датчика события»): состояние датчика событий каждого порта.

Arming Status («Состояние постановки на охрану»): состояние устройства.

7.4.3 Изменение основной информации

Цель

После добавления устройства контроля доступа можно изменить основную информацию об устройстве.

Шаги

1. Выберите устройство из списка устройств.
2. Нажмите **Modify** («Изменить»), чтобы открыть окно изменения информации устройства.
3. Нажмите вкладку **Basic Information** («Основная информация»), чтобы войти в интерфейс основной информации.

4. Можно изменить информацию об устройстве, включая режим добавления, имя устройства, IP-адрес устройства, номер порта, имя пользователя и пароль.

7.4.4 Удаленная настройка

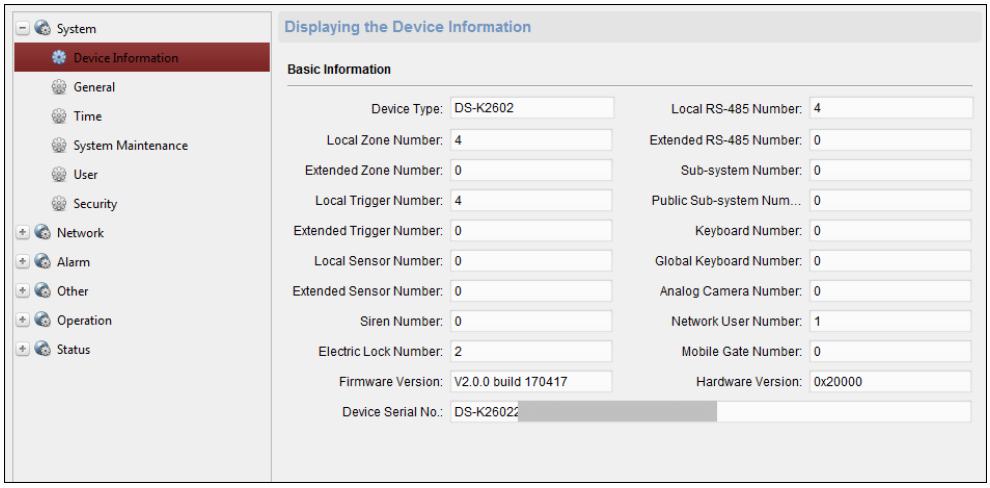
Цель

В списке устройств выберите устройство и нажмите **Remote Configuration** («Удаленная настройка») для перехода в интерфейс удаленной настройки. Можно задать подробные параметры выбранного устройства.

Проверка информации об устройстве

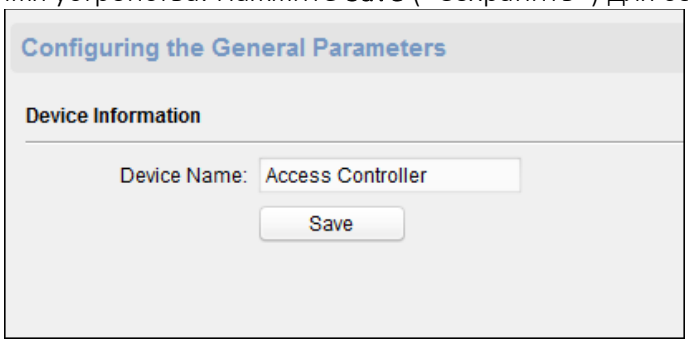
Шаги

1. В списке устройств выберите устройство и нажмите **Remote Configuration** («Удаленная настройка») для перехода в интерфейс удаленной настройки.
2. Нажмите **System → Device Information** («Система → Информация об устройстве»), чтобы проверить основную информацию об устройстве и информацию о версии устройства.



Редактирование имени устройства

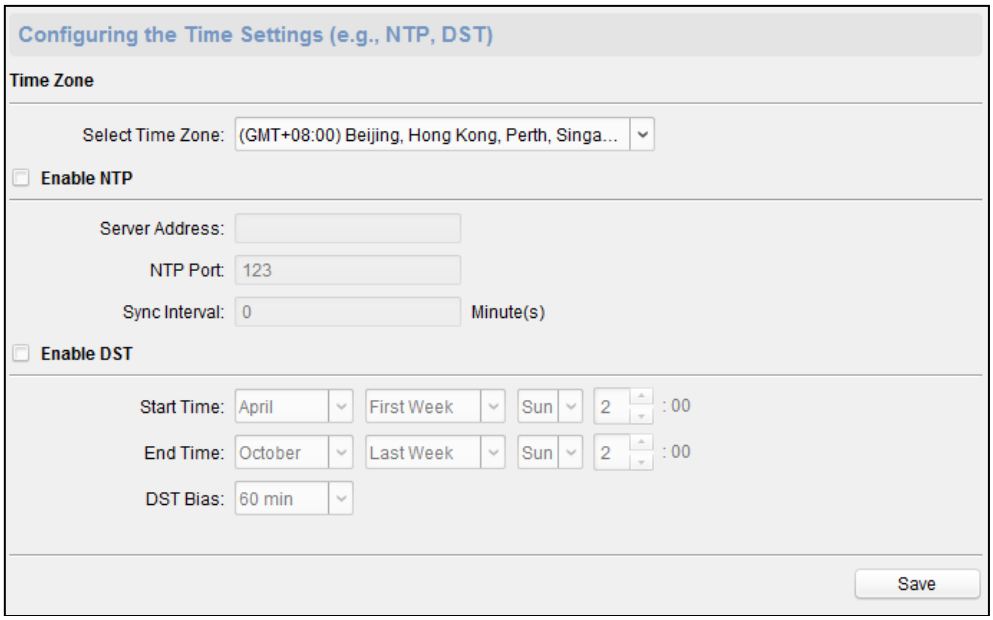
В интерфейсе удаленной настройки нажмите **System → General** («Система → Основное»), чтобы редактировать имя устройства. Нажмите **Save** («Сохранить») для сохранения настроек.



Редактирование времени

Шаги

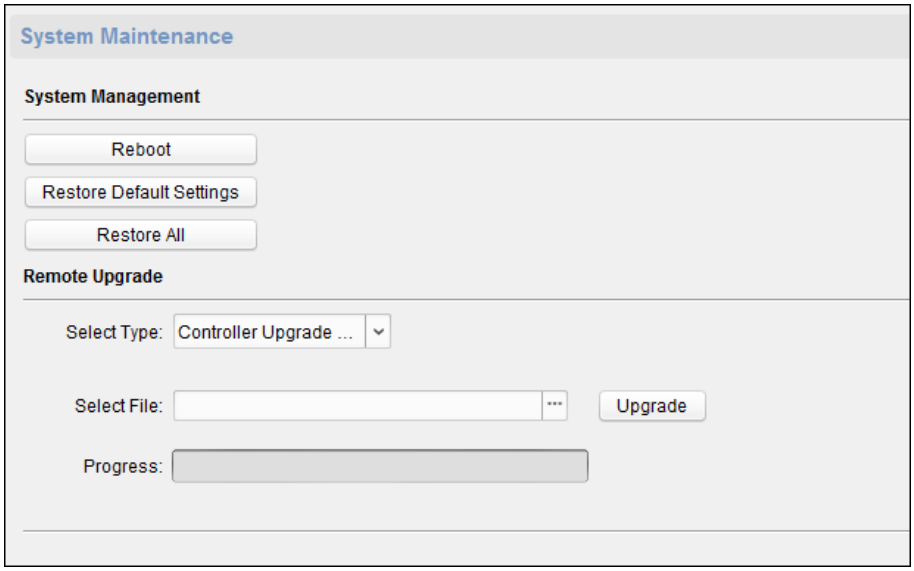
1. В интерфейсе удаленной настройки нажмите **System → Time** («Система → Время»), чтобы настроить часовой пояс.
2. (Необязательно) Нажмите **Enable NTP** («Включить NTP») и настройте адрес сервера NTP (или домен сервера), порт NTP и интервал синхронизации.
3. (Опционально) Нажмите **Enable DST** («Включить DST») и настройте время перехода на летнее время, время окончания и параметры смещения.
4. Нажмите **Save** («Сохранить») для сохранения настроек.



Настройка обслуживания системы

Шаги

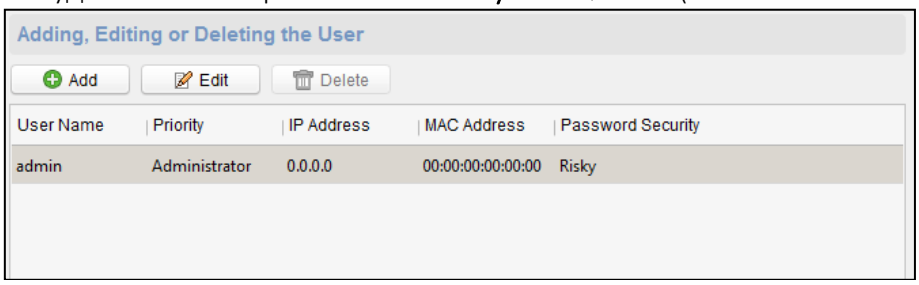
1. В интерфейсе удаленной настройки нажмите **System** → **System Maintenance** («Система → Обслуживание системы»).
2. Нажмите **Reboot** («Перезагрузка») для перезагрузки устройства.
   Или нажмите **Restore Default Settings** («Восстановление настроек по умолчанию»), чтобы восстановить настройки устройства по умолчанию, за исключением IP-адреса.
   Или нажмите **Restore All** («Восстановить все»), чтобы восстановить параметры устройства по умолчанию. После восстановления настроек необходимо активировать устройство.
   Примечание. В файле конфигурации содержится информация о параметрах устройства.
3. Устройство также можно обновить удаленно.
   1) В поле **Remote Upgrade** («Удаленное обновление») выберите тип файла обновления в раскрывающемся списке.
      В раскрывающемся списке можно выбрать файл обновления контроллера или обновление считывателя карт.
   2) Нажмите ..., чтобы выбрать файл обновления.
   3) Нажмите **Upgrade** («Обновить»), чтобы начать обновление.
      Примечание. Обновить можно только считыватели карт, подключенные через RS-485. Контроллер доступа серии F-KD-1300 поддерживает только считыватель карт Wiegand.



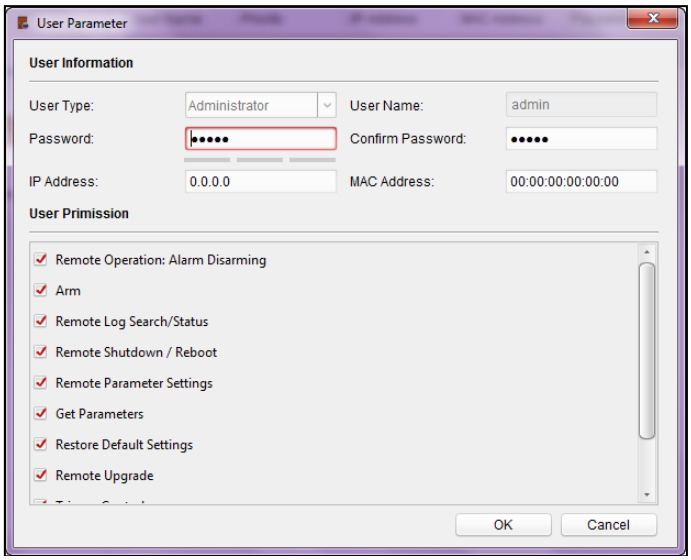
Управление пользователями

Шаги

1. В интерфейсе удаленной настройки нажмите **System → User** («Система → Пользователь»).



2. Нажмите **Add** («Добавить») для добавления пользователя.
   Или выберите пользователя в списке пользователей и нажмите **Edit** («Изменить»), чтобы редактировать информацию о пользователе. Можно редактировать пароль пользователя, IP-адрес, MAC-адрес и права пользователя. Нажмите **OK**, чтобы подтвердить редактирование.



Настройка безопасности

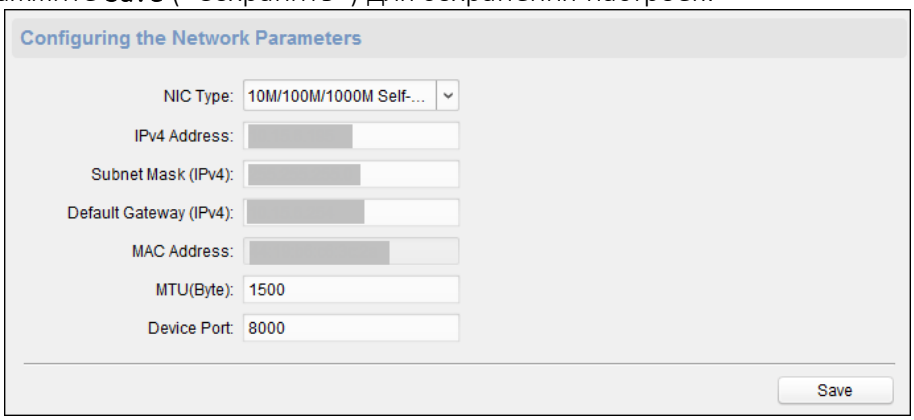
Шаги

1. Нажмите **System → Security** («Система → Безопасность»).

2. В раскрывающемся списке выберите режим шифрования.
   Можно выбрать **Compatible Mode** («Режим совместимости») или **Encryption Mode** («Режим шифрования»).
3. Нажмите **Save** («Сохранить») для сохранения настроек.

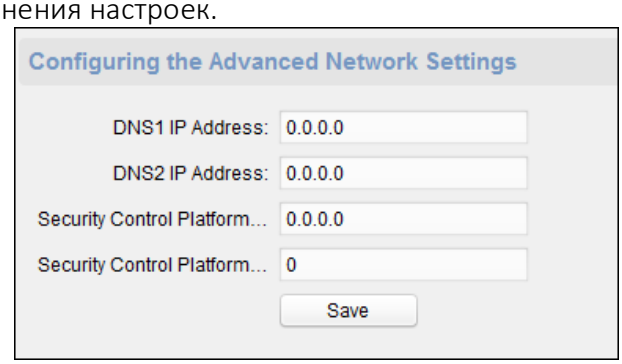
Настройка параметров сети

Перейдите в меню **Network → General** («Сеть → Общие»). Можно настроить тип сетевой карты, адрес IPv4, маску подсети (IPv4), шлюз по умолчанию (IPv4), адрес MTU, MTU и порт устройства. Нажмите **Save** («Сохранить») для сохранения настроек.



Расширенные настройки сети

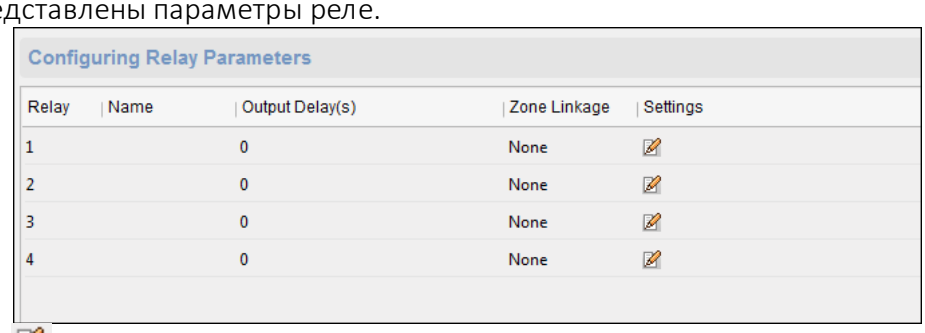
Нажмите **Network → Advanced Settings** («Сеть → Расширенные настройки»). Можно настроить DNS-адрес 1, DNS-адрес 2, IP-адрес хоста тревоги и порт хоста тревоги. Нажмите **Save** («Сохранить») для сохранения настроек.



Настройка параметров реле

Шаги

1. Нажмите **Alarm → Relay** («Тревога → Реле»).
   Здесь представлены параметры реле.



2. Нажмите , чтобы открыть окно настройки параметров реле.
3. Настройте имя реле и параметры задержки вывода.
4. Нажмите **Save** («Сохранить») для сохранения настроек.
   Или нажмите **Copy to...** («Копировать в...»), чтобы скопировать информацию о реле в каналы других реле.

Настройка параметров контроля доступа

Шаги

1. В интерфейсе удаленной настройки нажмите **Other → Access Control Parameters** («Другое → Параметры контроля доступа»).
2. Нажмите **Press Key to Input Card No.** («Введение номера карты нажатием кнопки»).
3. Нажмите **Save** («Сохранить») для сохранения настроек.

Настройка параметров детекции лиц

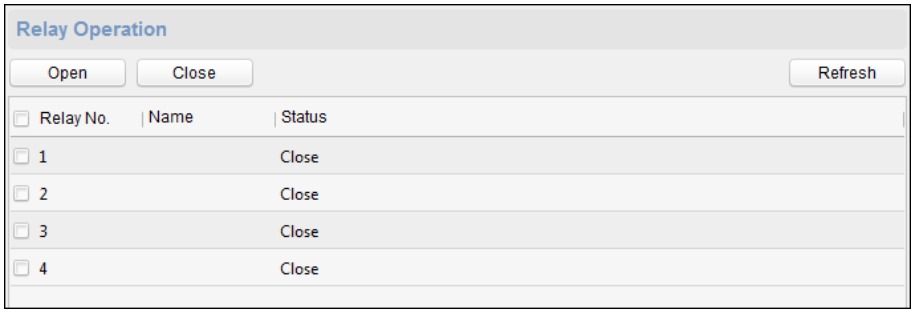
Нажмите **Other → Face Detection** («Другое → Детекция лиц»). Можно нажать **Enable** («Включить»), чтобы включить функцию детекции лица на устройстве.

Примечание. Данную функцию поддерживают только устройства с функцией управления видео.

Управление реле

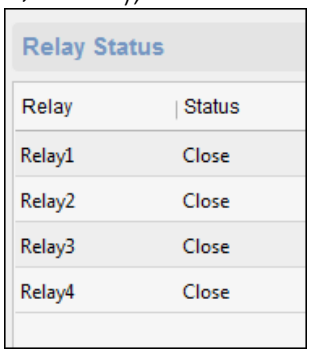
Шаги

1. Нажмите **Operation → Relay** («Управление → Реле»).
   Здесь показано состояние реле.
2. Выберите поле необходимого реле.
3. Нажмите **Open** («Открыть») или **Close** («Закрыть»), чтобы открыть / закрыть реле.
4. (Опционально) Нажмите **Refresh** («Обновить») для обновления состояния реле.



Просмотр состояния реле

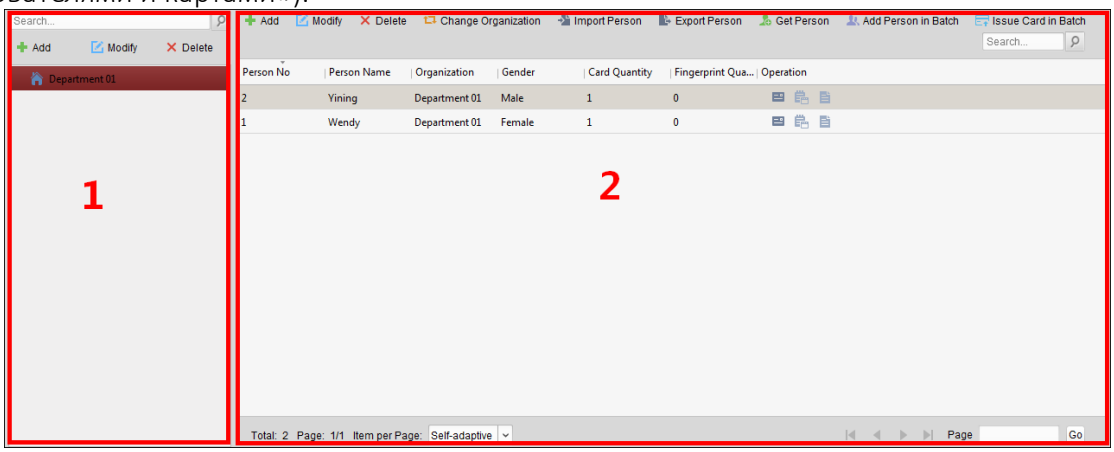
Нажмите **Status → Relay** («Состояние → Реле»), чтобы посмотреть состояние реле.



7.5 Управление пользователями и картами

Можно добавлять, изменять или удалять организации по вашему желанию в модуле **Person and Card Management** («Управление пользователями и картами»).

Нажмите вкладку для перехода в меню **Person and Card Management** («Управление пользователями и картами»).



Интерфейс разделен на две части: управление организацией и управление людьми.

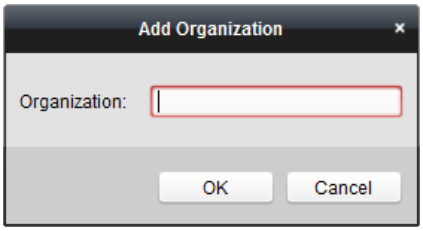
1	Управление организацией	Можно добавлять, редактировать или удалять организацию по своему усмотрению.
2	Управление пользователями	После добавления организации Можно добавить сотрудника в организацию и выдать карты сотрудникам для дальнейшего управления.

7.5.1 Управление организацией

Добавление организации

Шаги

1. В списке организаций слева вы должны добавить верхнюю организацию как головную организацию для всех организаций.
   Нажмите кнопку **Add** («Добавить»), чтобы появилось всплывающее окно добавления организации.



2. Введите **Organization Name** («Имя организации») по вашему усмотрению.
3. Нажмите **OK** для подтверждения добавления.
4. Можно добавить несколько уровней организаций в соответствии с фактическими потребностями.
   Чтобы добавить дочернюю организацию, выберите родительскую организацию и нажмите **Add** («Добавить»).
   Повторите *Шаг 2* и *3* для добавления дочерней организации.
   Тогда добавленная организация станет дочерней для организации верхнего уровня.

Примечание. Можно создать до 10 уровней организации.

Изменение и удаление организации

Можно выбрать добавленную организацию и нажать **Modify** («Изменить») для изменения ее имени.

Можно выбрать добавленную организацию и нажать **Delete** («Удалить») для ее удаления.

Примечание.

- Если удалить организацию верхнего уровня, организации нижнего уровня тоже будут удалены.
- Организация не может быть удалена, если ранее добавлены сотрудники.

7.5.2 Управление пользователями

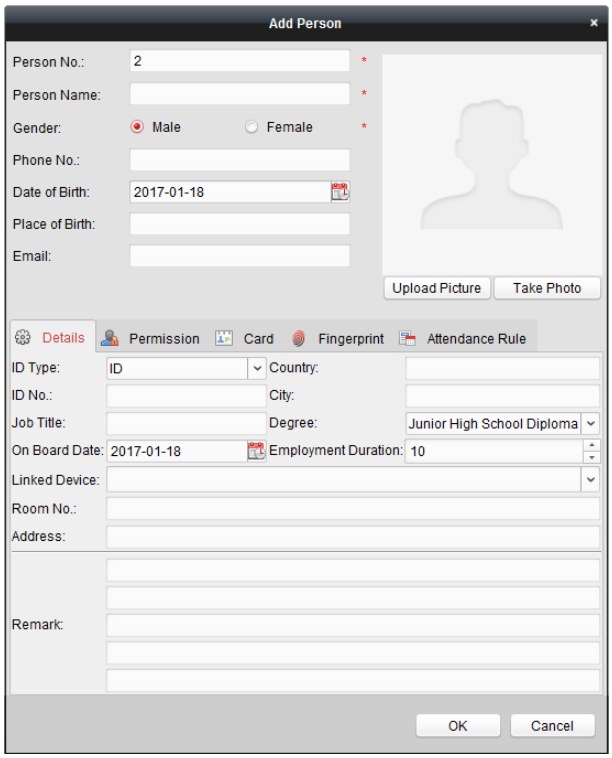
После добавления организации Можно добавить пользователя в организацию и управлять добавленными пользователями, например, выпускать карты в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.
Примечание. Может быть добавлено до 10000 пользователей или карт.

Добавление пользователя

Добавление пользователя (основная информация)

Шаги

1. Выберите организацию в списке организаций и нажмите кнопку **Add** («Добавить») на панели **Person** («Пользователь») для появления всплывающего окна добавления пользователя.

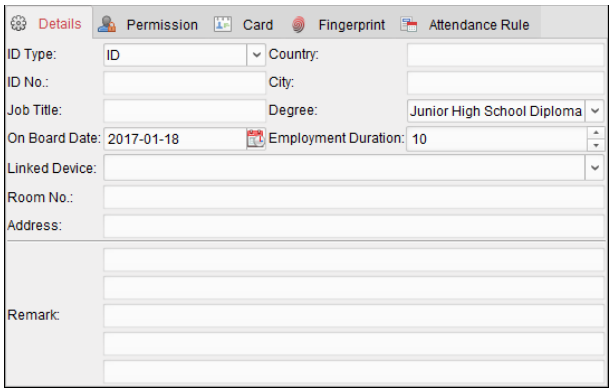


2. **Person No.** («№ пользователя») будет сгенерирован автоматически и не может быть изменен.
3. Введите основную информацию, включая **person name** («имя сотрудника»), **gender** («пол»), **phone No.** («№ телефона»), **birthday details** («детали рождения») и **email**.
4. Нажмите **Upload Picture** («Загрузить изображение») для выбора изображения сотрудника из папки на локальном ПК и загрузки в клиент.
   Примечание. Изображение должно быть в формате *.jpg.
5. (Опционально) Также можете нажать **Take Photo** («Сделать фото») для того, чтобы сделать фото пользователя при помощи камеры ПК.
6. Нажмите **OK** для завершения добавления.

Добавление пользователя (подробная информация)

Шаги

1. В меню добавления пользователя нажмите вкладку **Details** («Детали»).



2. Введите подробную информацию о сотруднике, включая **ID type** («тип ID»), **ID No.** («ID номер»), **country** («страна») и др.
   - **Linked Device («Связанные устройства»):** можете привязать видеодомофон к пользователю.

     Примечание. Если вы выбрали значение **Analog Indoor Station** («Аналоговый видеодомофон») в поле **Linked Device** («Привязка устройства»), тогда будет отображено поле **Door Station** («Вызывная панель»), и вам необходимо будет выбрать вызывную панель для связи с аналоговым видеодомофоном.
   - **№ помещения:** можете ввести номер помещения для пользователя.
3. Нажмите **OK** для сохранения настроек.

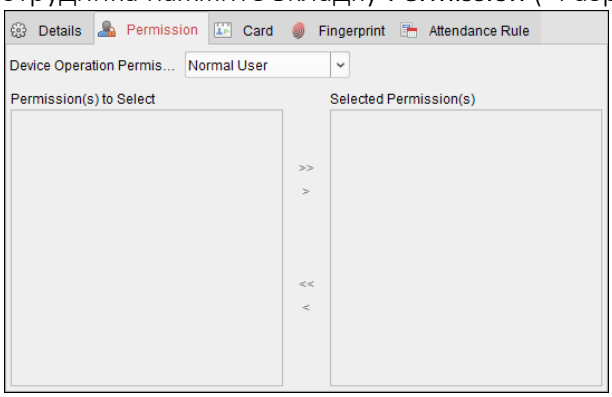
Добавление сотрудника (разрешения)

Можно назначать разрешения (включая разрешения на операции устройства контроля доступа и разрешения контроля доступа) пользователю при его добавлении.

Примечание. Подробная информация о разрешениях контроля доступа представлена в *разделе 7.7 Конфигурация разрешений.*

Шаги

1. В меню добавления сотрудника нажмите вкладку **Permission** («Разрешения»).



2. В поле **Device Operation Role** («Роль для работы с устройством») выберите роль для работы с устройством контроля доступа.

   Normal User («Обычный пользователь»): пользователь имеет разрешение на отметку о входе / выходе в устройстве, на проход через контрольные точки доступа и др.

Administrator («Администратор»): у администратора есть разрешения обычного пользователя, а также разрешение на конфигурацию устройства, включая добавление обычных пользователей и др.

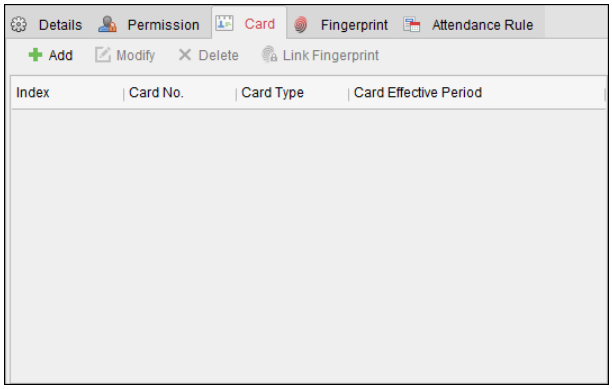
3. В списке **Permission(s) to Select** («Разрешения для выбора») отображаются все сконфигурированные разрешения.
   Поставьте галочку (-и) напротив разрешений и нажмите **>** для их добавления в список **Selected Permission(s)** («Выбранные разрешения»).
   (Опционально) Можно нажать **>>** для добавления всех отображенных разрешений в список **Selected Permission(s)** («Выбранные разрешения»).
   (Опционально) В списке **Selected Permission(s)** («Выбранные разрешения») выберите разрешения и нажмите кнопку **<** для их удаления из данного списка. Также можете нажать **<<** для удаления всех выбранных разрешений.
4. Нажмите **OK** для сохранения настроек.

Добавление пользователя (карта)

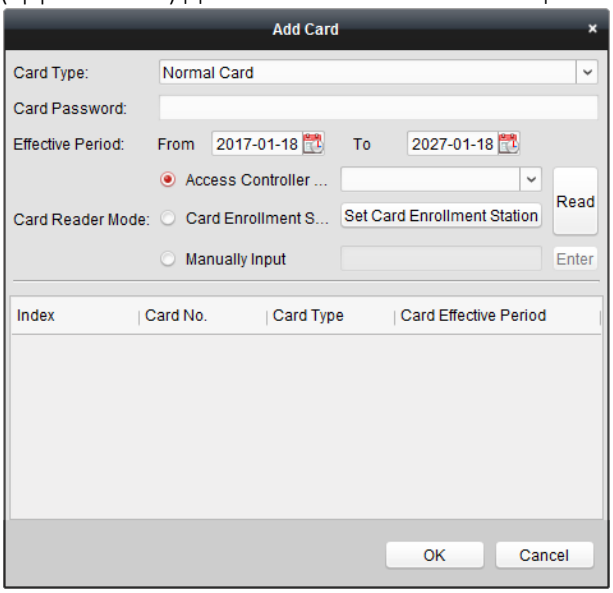
Можно добавлять карты и выдавать их людям.

Шаги

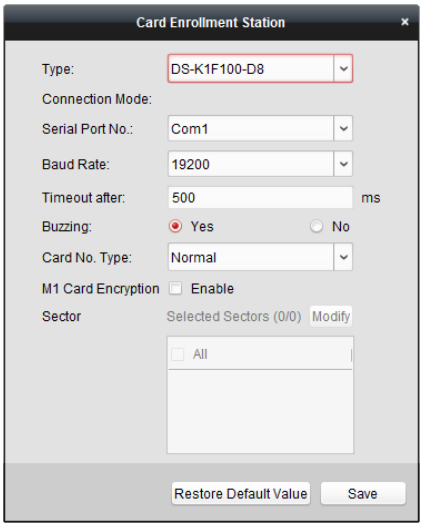
1. В меню добавления сотрудника нажмите вкладку **Card** («Карта»).



2. Нажмите кнопку **Add** («Добавить») для появления всплывающего окна добавления карты.



3. Выберите тип карты.
   - Normal Card («Обычная карта»)
   - Card for Door Extended Opening («Карта с расширенными полномочиями»)
     Дверь останется открытой в течение заданного периода времени для владельца данной карты.
   - Card in Blocklist («Карта из черного списка»)
     Действие считывания карты будет загружено в систему, и дверь не будет открыта.
   - Patrol Card («Патрульная карта»)
     Считывание карты позволяет персоналу инспектирования проверить рабочее состояние устройства. Разрешения доступа для персонала инспектирования могут быть настроены в зависимости от задач проекта.
   - Duress Card («Принудительная карта»)
     Дверь может быть открыта при помощи считывания принудительной карты.
     При этом клиент может создает уведомление о событии принуждения.
   - Super Card («Суперкарта»)
     Карта действительна для всех дверей контроллера
     в течение заданного в расписании времени.
   - Visitor Card («Карта посетителя»)
     Карта предназначена для посетителей. Для карты посетителя можно установить параметр Max. Swipe Times («Макс. число проводок»).
     Примечания.
     - Параметр Max. Swipe Times («Макс. число проводок») должен быть задан числом в промежутке от 0 до 255. Если длительность считывания карты превышает настроенное время, считывание карты считается недействительным.
     - При установке значения «0» количество считываний карты не ограничено.
4. Введите пароль от самой карты в поле Card Password («Пароль карты»). Пароль карты должен содержать от 4 до 8 цифр.
   Примечание. Пароль будет необходим, когда держатель карты проведет картой для входа или выхода через дверь, если включены такие режимы аутентификации считывателя карт как Card and Password («Карта и Пароль»), Password and Fingerprint («Пароль и Отпечаток пальца»), Card («Карта»), Password («Пароль») и Fingerprint («Отпечаток пальца»). Подробная информация приведена в *разделе 7.8.2 Аутентификация с помощью* считывателя карт.
5. Нажмите для установки времени действия и истечения действия карты.
6. Выберите Card Reader Mode («Режим считывателя карт») для считывания номера карты.
   - Считыватель карт контроллера доступа: Поместите карту на считыватель контроллера доступа и нажмите Read («Считать») для получения номера карты.
   - Настольный считыватель карт: Поместите карту на настольный считыватель и нажмите Read («Считать») для получения номера карты.
     Примечание. Настольный считыватель карт должен быть подключен к ПК с запущенным клиентом. Можно нажать Set Card Enrollment Station («Установить настольный считыватель карт») для перехода в следующее меню.



2) Выберите тип настольного считывателя карт.

   Примечание. Поддерживаемые типы считывателей карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

3) Задайте номер серийного интерфейса, скорость передачи данных, значение лимита времени, параметры бипера или тип № карты.

   Примечание. Контроллер доступа серии F-KD-1300 не поддерживает функцию шифрования карты M1.

4) Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

Можно нажать кнопку **Restore Default Value** («Восстановить значение по умолчанию») для восстановления значений по умолчанию.

- **Ввод вручную:** введите номер карты и нажмите **Enter** для внесения номера карты.

7. Нажмите **OK**, чтобы выдать карту сотруднику.
8. (Опционально) Можно выбрать добавленную карту и нажать **Edit** («Изменить») или **Delete** («Удалить») для редактирования или удаления карты.
9. Нажмите **OK** для сохранения настроек.

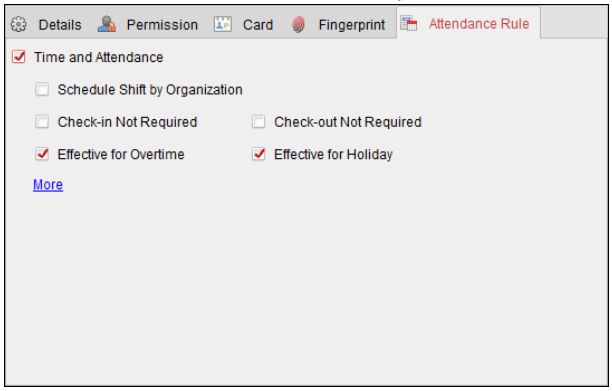
Добавление пользователя (правило УРВ)

Можно настроить правило УРВ для сотрудника.

Примечание. Эта вкладка отображается, если при первом запуске программного обеспечения выбран режим **Non-Residence** («Нежилая недвижимость»).

Шаги

1. В меню добавления пользователя нажмите вкладку **Attendance Rule** («Правило УРВ»).



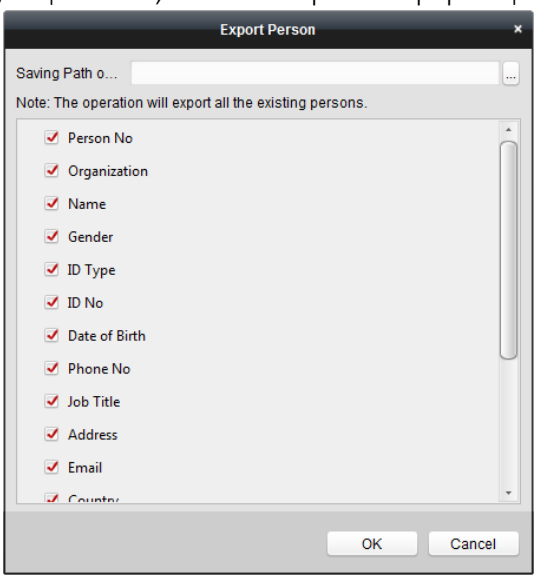
2. Если для пользователя необходимо настроить УРВ, нажмите **Time and Attendance** («Учет рабочего времени»), чтобы включить эту функцию. Записи считывания карты сотрудника будут записаны и проанализированы в рамках УРВ.
   Для получения подробной информации об УРВ нажмите **More** («Подробнее»), чтобы перейти к модулю УРВ.
3. Нажмите **OK** для сохранения настроек.

Импорт и экспорт информации пользователя

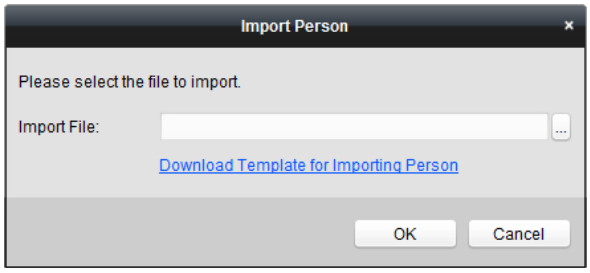
Информация пользователя может быть импортирована и экспортирована в пакетном режиме.

Шаги

1. **Экспорт пользователя:** можно экспортировать информацию о добавленных пользователях в формате Excel на локальный ПК.
   1) После добавления пользователя можно нажать **Export Person** («Экспорт пользователя») во вкладке **Person and Card** («Пользователь и карта») для появления следующего окна.
   2) Нажмите ... для выбора пути сохранения экспортированного файла Excel.
   3) Нажмите соответствующее поле, чтобы выбрать информацию для экспорта.



   4) Нажмите **OK**, чтобы начать экспорт.
2. **Импорт пользователя:** можно импортировать файл Excel с информацией пользователей в пакетном режиме с локального ПК.
   1) Нажмите **Import Person** («Импортировать пользователя») на вкладке **Person and Card** («Пользователь и карта»).



   2) Можно нажать **Download Template for Importing Person** («Скачать шаблон для импорта пользователей»), чтобы скачать шаблон.

3) Введите информацию о пользователе в загруженный шаблон.
4) Нажмите ... для выбора Excel файла с информацией о пользователе.
5) Нажмите **OK**, чтобы начать импорт.

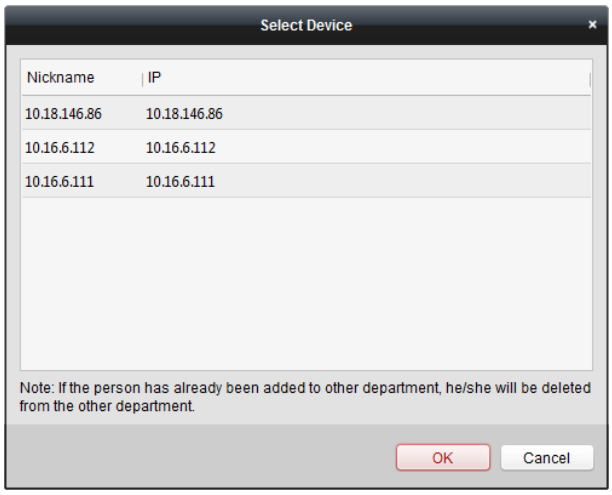
Получение информации о пользователе с устройства контроля доступа

Если в добавленном устройстве контроля доступа была настроена информация о пользователе (включая подробную информацию о пользователе, отпечаток пальца, информацию о выданной карте), можно получить информацию с устройства и импортировать ее в клиент для дальнейшей работы.

Примечание. Эта функция поддерживается только устройством, которое было добавлено при помощи TCP / IP.

Шаги

1. В списке организаций слева выберите организацию для импорта пользователей.
2. Нажмите **Get Person** («Получить информацию пользователя») для появления следующего диалогового окна.



3. Будут отображены добавленные устройства контроля доступа.
4. Нажмите устройство, чтобы выбрать его, а затем нажмите **OK**, чтобы начать получать информацию о пользователе с устройства.
   Или дважды нажмите имя устройства, чтобы начать получать информацию о пользователе с устройства.

Примечание.

- Информация о пользователе, включая подробную информацию о пользователе, информацию об отпечатках пальцев (если настроены) и картах (если настроены), будет импортирована в выбранную организацию.
- Если в информации о пользователе, хранящейся на устройстве, в поле **Name** («Имя») не указаны данные, то это поле будет заполнено номером выданной карты после импорта в клиентское ПО.
- По умолчанию задан пол: **Male** («Мужской»).
- Можно импортировать до 10 000 пользователей, по 5 карт на каждого пользователя.

Управление пользователями

Изменение информации пользователя и удаление пользователя

Чтобы изменить информацию пользователя и правило УРВ, нажмите или в столбце **Operation** («Операции») или выберите пользователя и нажмите **Modify** («Изменить»), чтобы открыть диалоговое окно изменения информации пользователя.

Можно нажать , чтобы просмотреть записи считывания карт.

Для удаления пользователя, выберите его и нажмите **Delete** («Удалить»).

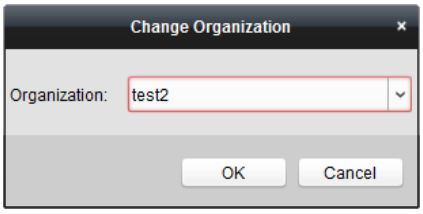
Примечание. Если карта выдана текущему пользователю, привязка будет недействительна после его удаления.

Перемещение пользователя в другую организацию

При необходимости Можно переместить пользователя в другую организацию.

Шаги

1. Выберите пользователя из списка и нажмите **Change Organization** («Изменить организацию»).



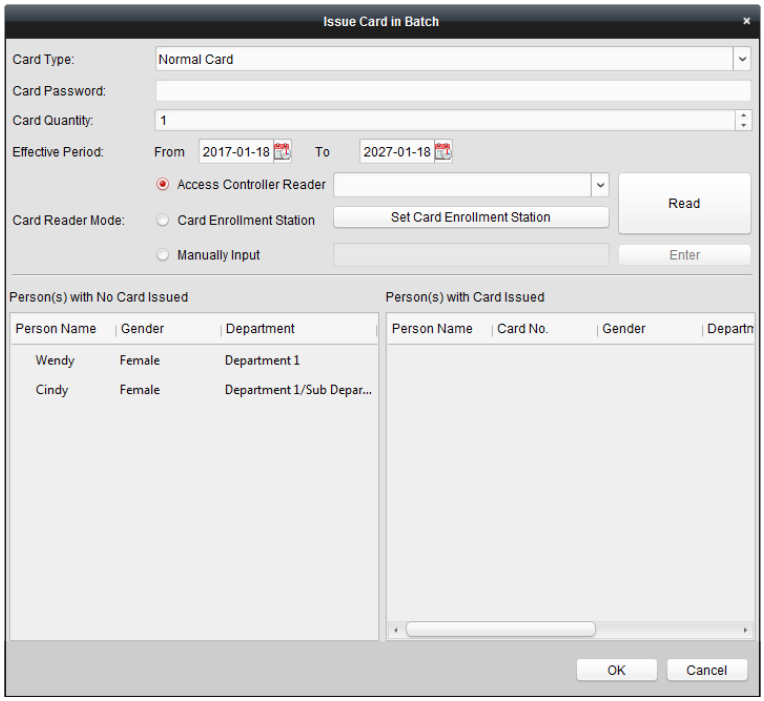
2. Выберите организацию, в которую нужно переместить пользователя.
3. Нажмите **OK** для сохранения настроек.

Выдача карт в пакетном режиме

Можно выдать несколько карт пользователю, у которого нет карты.

Шаги

1. Нажмите **Issue Card in Batch** («Выдача карт в пакетном режиме»), чтобы открыть следующее диалоговое окно.
   Все добавленные пользователи, которым не были выданы карты, будут отображены в списке **Person(s) with No Card Issued** («Пользователи, которым не выданы карты»).



2. Выберите тип карты.

   Примечание. Подробная информация о типах карты представлена в разделе *Добавление пользователя*.

3. Введите пароль от самой карты в поле **Card Password** («Пароль карты»). Пароль карты должен содержать от 4 до 8 цифр.

   Примечание. Пароль будет необходим, когда держатель карты проведет картой для входа или выхода через дверь, если включены такие режимы аутентификации считывателя карт как **Card and Password** («Карта и Пароль»), **Password and Fingerprint** («Пароль и Отпечаток пальца»), **Card** («Карта»), **Password** («Пароль») и **Fingerprint** («Отпечаток пальца»). Подробная информация представлена в разделе *7.8.2Аутентификация с помощью* считывателя карт.

4. Введите количество карт, выданных на каждого пользователя.

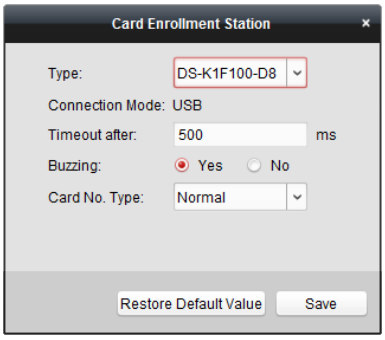
   Например, если выдано 3 карты, можно ввести три № карты для каждого пользователя.

5. Нажмите для установки времени действия и истечения действия карты.

6. Выберите **Card Reader Mode** («Режим считывателя карт») для считывания номера карты.

   - **Считыватель карт контроллера доступа:** поместите карту на считыватель контроллера доступа и нажмите **Read** («Считать») для получения номера карты.
   - **Настольный считыватель карт:** поместите карту на настольный считыватель и нажмите **Read** («Считать») для получения номера карты.

     Примечание. Настольный считыватель карт должен быть подключен к ПК с запущенным клиентом. Можно нажать **Set Card Enrollment Station** («Установить настольный считыватель карт») для перехода в следующее меню.



1) Выберите тип настольного считывателя карт.
   Примечание. Поддерживаемые типы считывателей карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.
2) Установите параметры для подключенного настольного считывателя карт.
3) Нажмите кнопку **Save** («Сохранить») для сохранения настроек.
   Можно нажать кнопку **Restore Default Value** («Восстановить значение по умолчанию») для восстановления значений по умолчанию.

- **Ввод вручную:** введите номер карты и нажмите **Enter** для внесения номера карты.

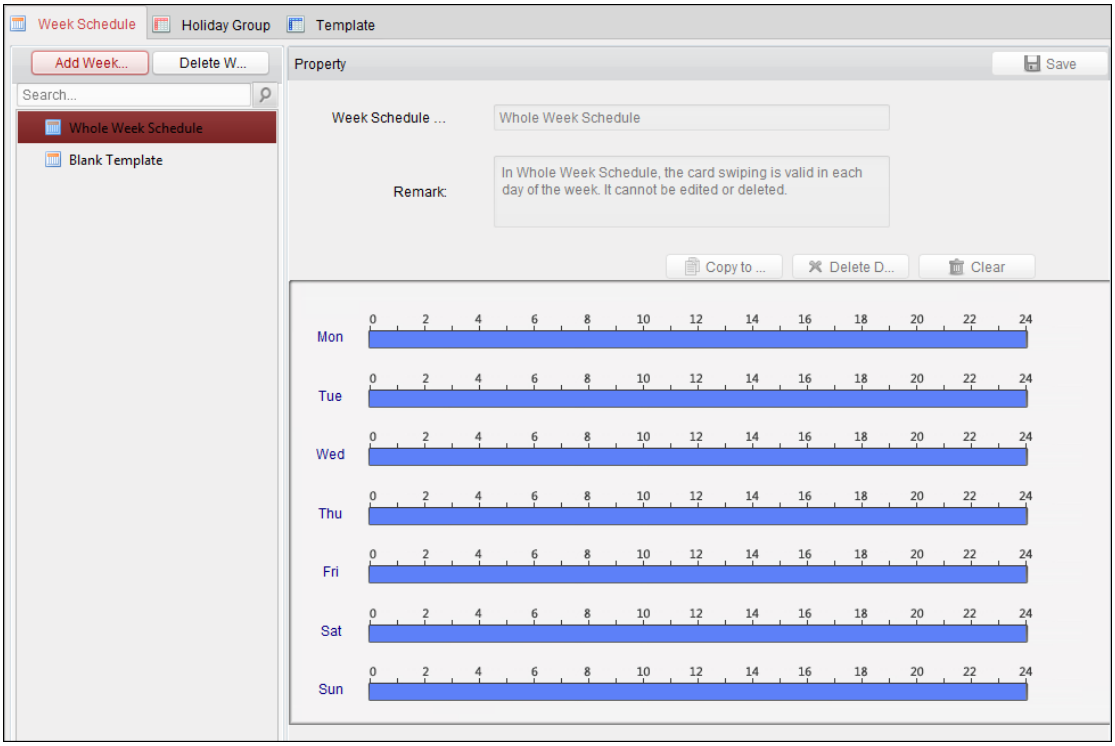
7. После выдачи карты пользователю, информация о нем и о карте будет отображена в списке **Person(s) with Card Issued** («Пользователи, которым выданы карты»).
8. Нажмите **OK** для сохранения настроек.

7.6 Расписание и шаблон

Цель

Настройте шаблон, в том числе недельный расписание работы и расписание выходных дней. После настройки шаблонов, их можно использовать для настройки разрешений контроля доступа.

Нажмите для входа в интерфейс расписаниеов и шаблонов.



Можно управлять расписанием разрешений контроля доступа, включая расписание рабочей недели, расписание выходных дней и шаблон. Подробная информация о разрешениях представлена в разделе *7.7 Конфигурация разрешений.*

7.6.1 Расписание рабочей недели

Нажмите **Week Schedule** («Расписание рабочей недели»), чтобы перейти на соответствующую страницу.

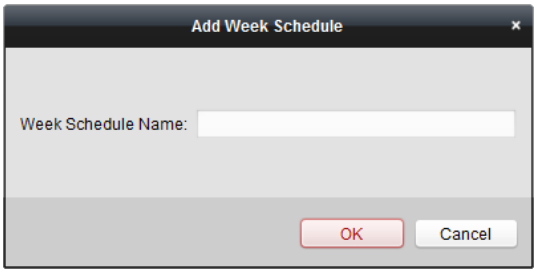
По умолчанию клиент определяет два типа плана недели: **Whole Week Schedule** («Расписание на всю неделю») и **Blank Schedule** («Незаполненное расписание»), нельзя изменить или удалить.

- **Whole Week Schedule («Расписание на всю неделю»):** считывание карты действительно каждый день недели.
- **Blank Schedule («Незаполненное расписание»):** считывание карты недействительно каждый день недели.

Можно выполнить следующие шаги, чтобы настроить индивидуальные расписания.

Шаги

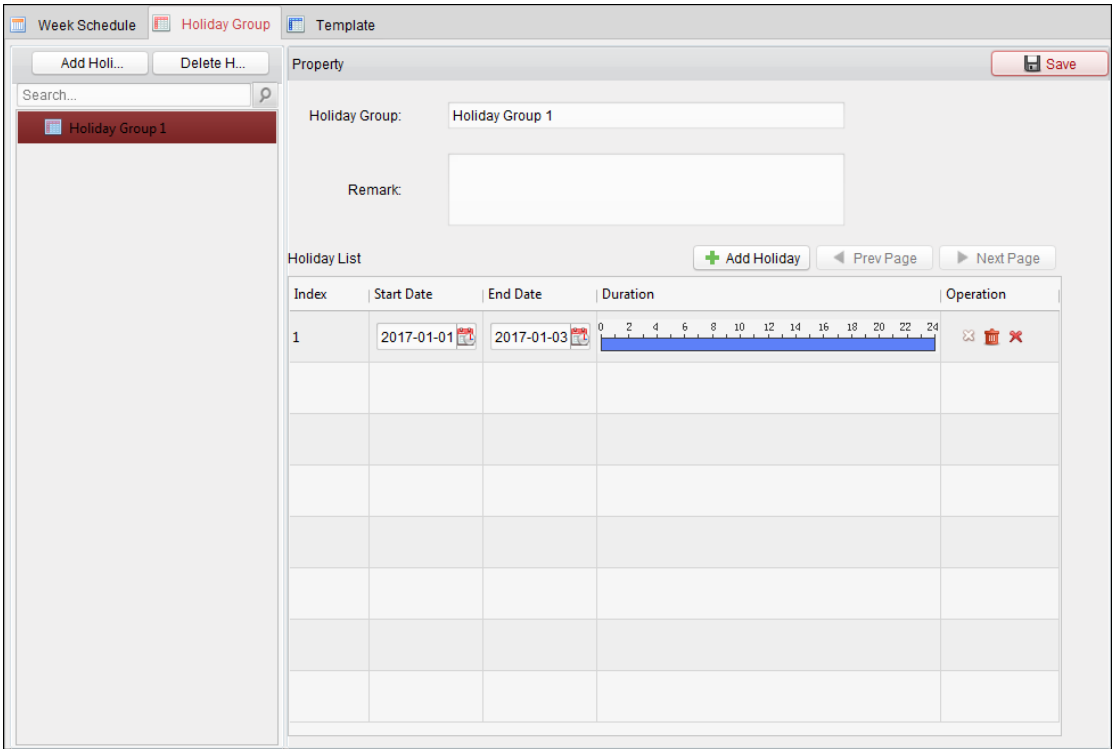
1. Нажмите **Add Week Schedule** («Добавить расписание рабочей недели»), чтобы появилось всплывающее окно добавления расписания.



2. Введите имя расписания рабочей недели и нажмите кнопку **OK**, чтобы добавить расписание.
3. Выберите добавленное расписание рабочей недели в списке расписаний, свойства расписания представлены справа.
   Можно изменить название расписания недели и добавить примечания.
4. Чтобы задать расписание нажмите и перетащите день, это означает, что в этот период времени активируется настроенное разрешение.
   Примечание. Для каждого дня в расписании можно установить до 8 периодов времени.
5. Когда вид курсора изменится на , можно переместить только что отредактированный период времени. Также можно редактировать отображаемый момент времени, чтобы с точностью настроить период времени.
   Когда вид курсора изменится на , можно увеличить или уменьшить выбранный период времени.
6. Опционально: можно выбрать шкалу времени расписания,
   а затем нажать **Delete Duration** («Удалить продолжительность»), чтобы удалить выбранную шкалу времени.
   Нажмите **Clear** («Очистить»), чтобы удалить все шкалы времени.
   Выберите **Copy to Week** («Применить ко всем дням недели»), чтобы применить эти настройки ко всем дням недели.
7. Нажмите **Save** («Сохранить») для сохранения настроек.

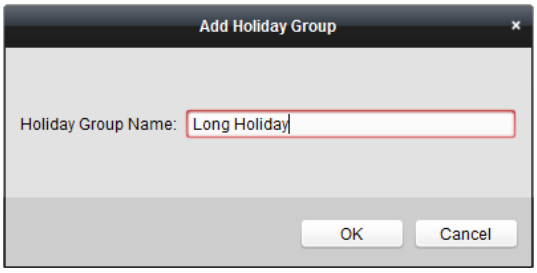
7.6.2 Группа выходных дней

Нажмите вкладку **Holiday Group** («Группа выходных дней») для перехода в меню управления группой выходных дней.



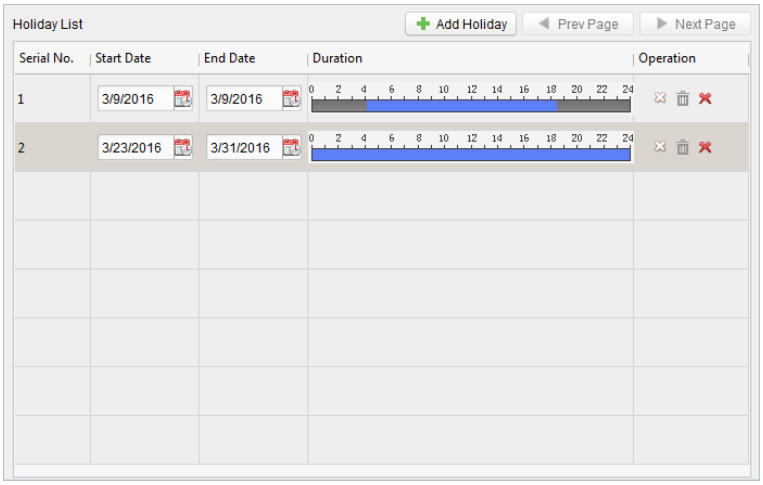
Шаги

1. Нажмите **Add Holiday Group** («Добавить группу выходных дней») слева, чтобы открыть интерфейс добавления группы выходных дней.



2. Введите имя группы выходных дней в текстовое поле и нажмите кнопку **OK**, чтобы добавить группу выходных дней.
3. Выберите добавленную группу выходных дней, чтобы изменить имя группы и добавить примечания.
4. Нажмите **Add Holiday** («Добавить выходной день»), чтобы добавить период выходных дней в список и настроить продолжительность выходных дней.

   Примечание. Для одной группы выходных дней можно добавить до 16 выходных дней.



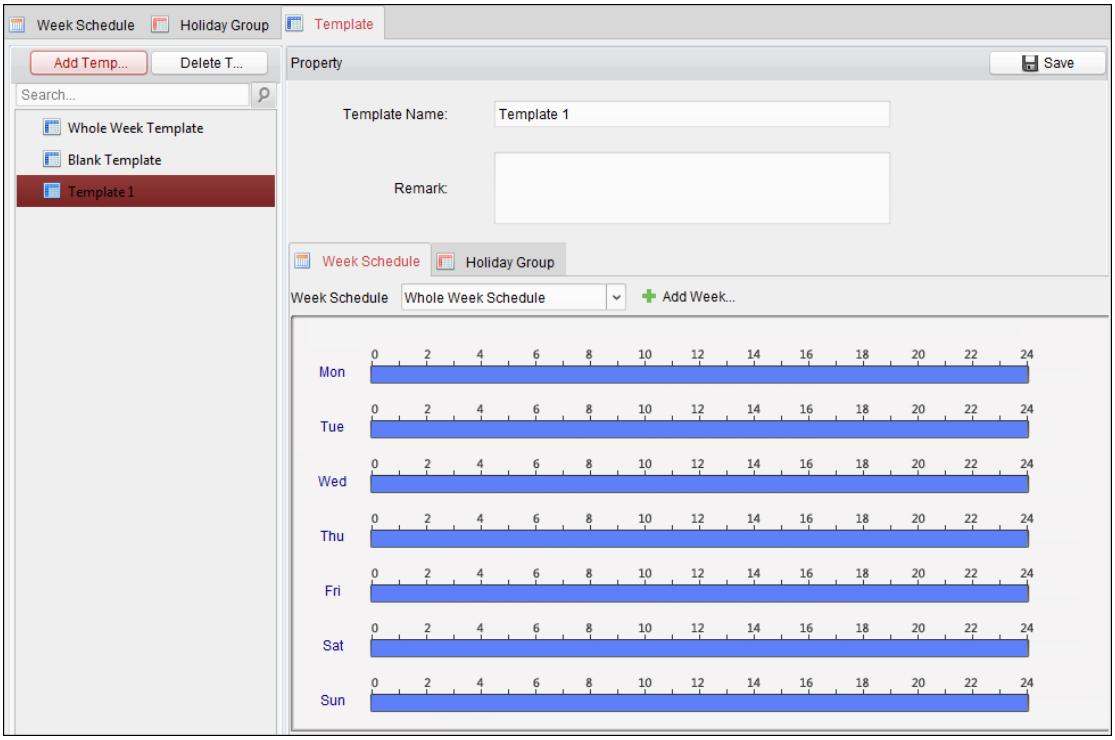
1) Чтобы задать период нажмите и перетащите день, что означает, что в этот период времени активируется настроенное разрешение.
   Примечание. Для каждого периода в расписании можно установить до 8 временных интервалов.
2) Когда вид курсора изменится на , можно переместить только что отредактированный период времени. Также можно редактировать отображаемый момент времени, чтобы с точностью настроить период времени.
3) Когда вид курсора изменится на , можно увеличить или уменьшить выбранный период времени.
4) Опционально: можно выбрать шкалу времени расписания, а затем нажать , чтобы удалить выбранную шкалу времени,
   Нажмите , чтобы удалить все шкалы времени выходных дней.
   Или нажмите , чтобы удалить выходной день непосредственно.

5. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание. Выходные дни не должны пересекаться.

7.6.3 Шаблон

После настройки расписания рабочей недели и группы выходных дней можно настроить шаблон, который содержит расписание рабочей недели и расписание группы выходных дней.
Примечание. Приоритет группы выходных дней выше, чем приоритет расписания рабочей недели.
Нажмите вкладку **Template** («Шаблон») для перехода в меню управления шаблонами.



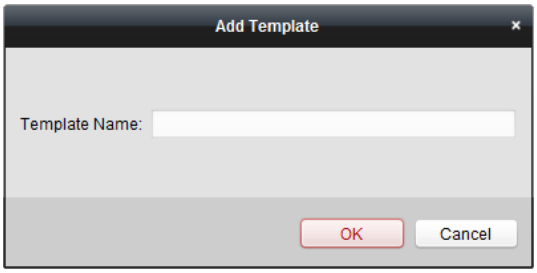
По умолчанию существует два шаблона: **Whole Week Template** («Шаблон на всю неделю») и **Blank Template** («Незаполненный шаблон»), которые нельзя изменить или удалить.

- **Whole Week Template («Шаблон на всю неделю»):** считывание карты действительно каждый день недели, группа выходных дней отсутствует.
- **Blank Template («Незаполненный шаблон»):** считывание карты недействительно каждый день недели, группа выходных дней отсутствует.

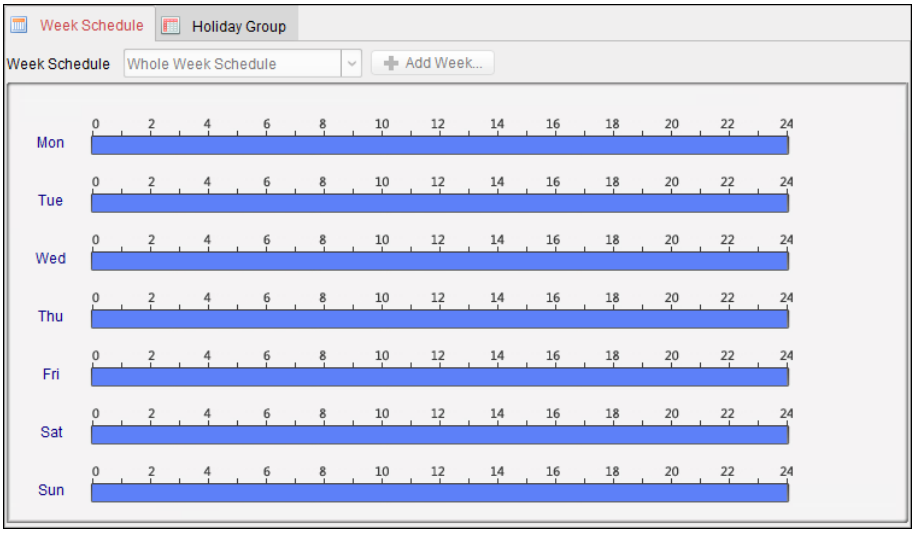
Шаблон можно заполнить в соответствии с задачами проекта.

Шаги

1. Нажмите **Add Template** («Добавить шаблон»), чтобы появилось всплывающее окно добавления шаблона.

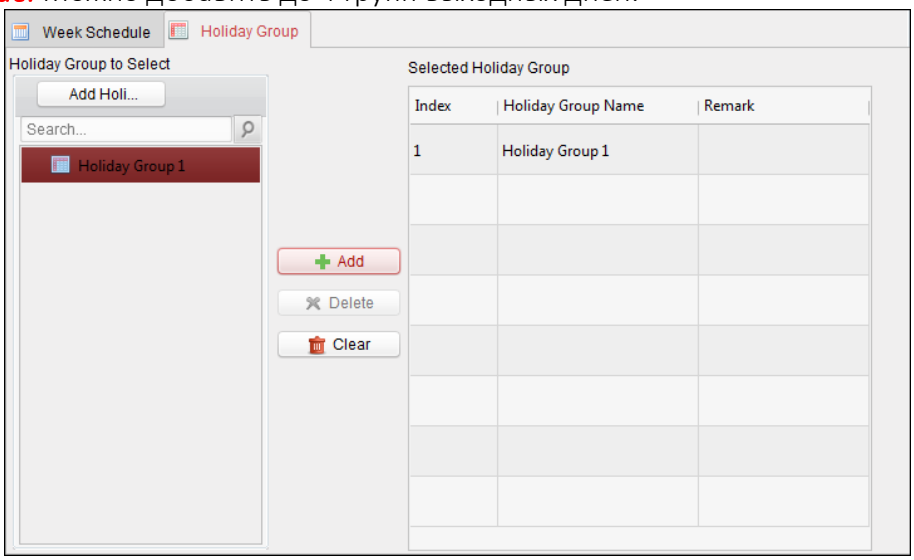


2. Введите имя шаблона в текстовое поле и нажмите кнопку **OK**, чтобы добавить шаблон.
3. Выберите добавленный шаблон, свойства шаблона представлены справа. Можно изменить название шаблона и добавить примечания.
4. Выберите шаблон и примените его к расписанию.
   Нажмите вкладку **Week Schedule** («Расписание рабочей недели») и выберите расписание в раскрывающемся списке.
   Нажмите **Add Week Schedule** («Добавить расписание рабочей недели») для добавления нового расписания рабочей недели. Подробная информация представлена в разделе *7.6.1 Расписание рабочей* недели.



5. Выберите группу выходных дней и примените ее к расписанию.

   Примечание. Можно добавить до 4 групп выходных дней.



   Выберите группу выходных дней в списке, и нажмите **Add** («Добавить»), чтобы добавить ее в шаблон. Нажмите **Add Holiday Group** («Добавить группу выходных дней») для добавления новой группы. Подробная информация представлена в разделе *7.6.2Группа выходных* дней.

   Можно выбрать добавленную группу выходных в списке справа и нажать **Delete** («Удалить»), чтобы удалить ее.

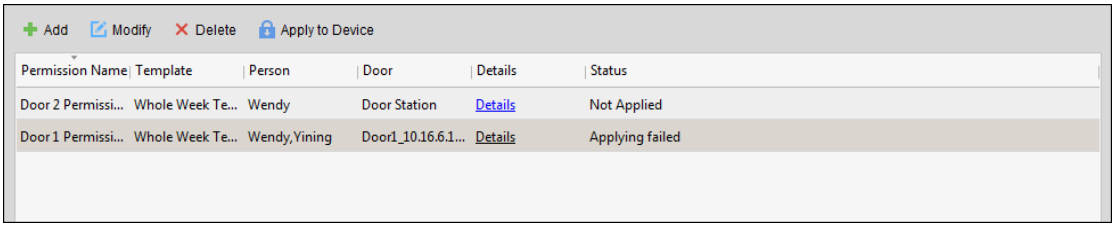
   Можно нажать **Clear** («Очистить»), чтобы удалить все добавленные группы выходных дней.

6. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

7.7 Конфигурация разрешений

В модуле конфигурации разрешений Можно добавлять, изменять и удалять разрешения контроля доступа, и затем применять настройки разрешений к устройству.

Нажмите , чтобы войти в интерфейс разрешений контроля доступа.



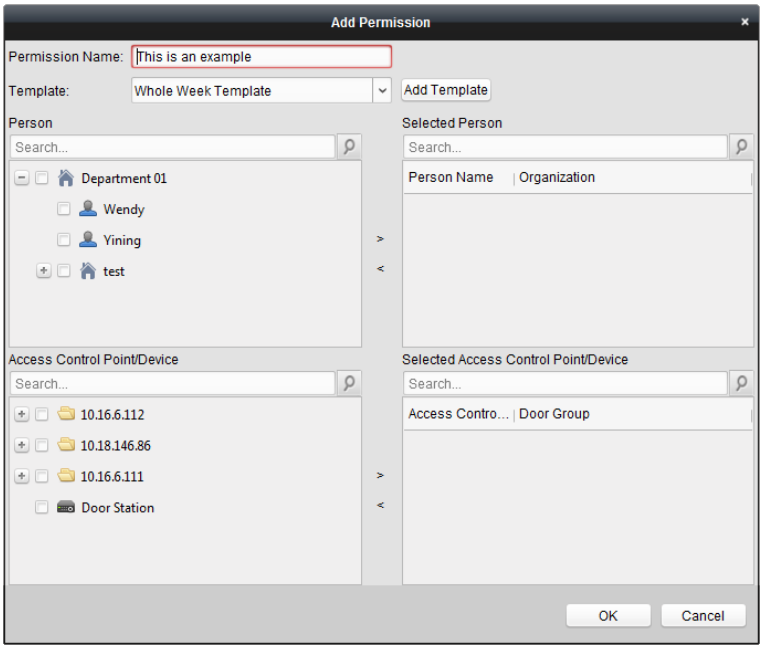
7.7.1 Добавление разрешений

Цель

Можно назначать разрешения для людей на вход / выход через контрольные точки (двери) в этом разделе.

Шаги

1. Нажмите **Add** («Добавить») для перехода в следующее меню.



2. В поле **Permission Name** («Имя разрешения») введите желаемое имя для разрешения.
3. Нажмите выпадающий список в поле **Template** («Шаблон») для выбора шаблона для разрешения.

   Примечание. Перед настройкой разрешений необходимо настроить шаблон. Можно нажать кнопку **Add Template** («Добавить шаблон») для добавления шаблона. Подробная информация представлена в разделе *7.6 Расписание и шаблон*.
4. В поле **Person List** («Список пользователей») отображаются все добавленные пользователи. Поставьте галочку (-и) для выбора пользователем и нажмите **>** для их добавления в список **Selected Person** («Выбранные пользователи»).

   (Опционально) Можно выбрать пользователя в списке **Selected Person** («Выбранные пользователи») и нажать **<** для отмены выбора пользователя.
5. В списке **Access Control Point/Device** («Точка контроля доступа/Устройство») будут отображены все добавленные точки контроля доступа (двери) и вызывные панели.

Поставьте галочку (-и) для выбора дверей или вызывных панелей и нажмите **>** для их добавления в список выбранных устройств.
(Опционально) Можно выбрать дверь или вызывную панель в списке выбранных устройств и нажать **<** для отмены выбора.

6. Нажмите кнопку OK для завершения добавления разрешений. Выбранные люди будут иметь разрешения на вход/выход через выбранные двери/вызывные панели при помощи привязанных карт или отпечатков пальцев.
7. (Опционально) После добавления разрешения, можно нажать Details («Детали») просмотра деталей. Или можно выбрать разрешение и нажать Modify («Изменить») для его изменения.
   Можно выбрать добавленное разрешение из списка и нажать Delete («Удалить») для его удаления.

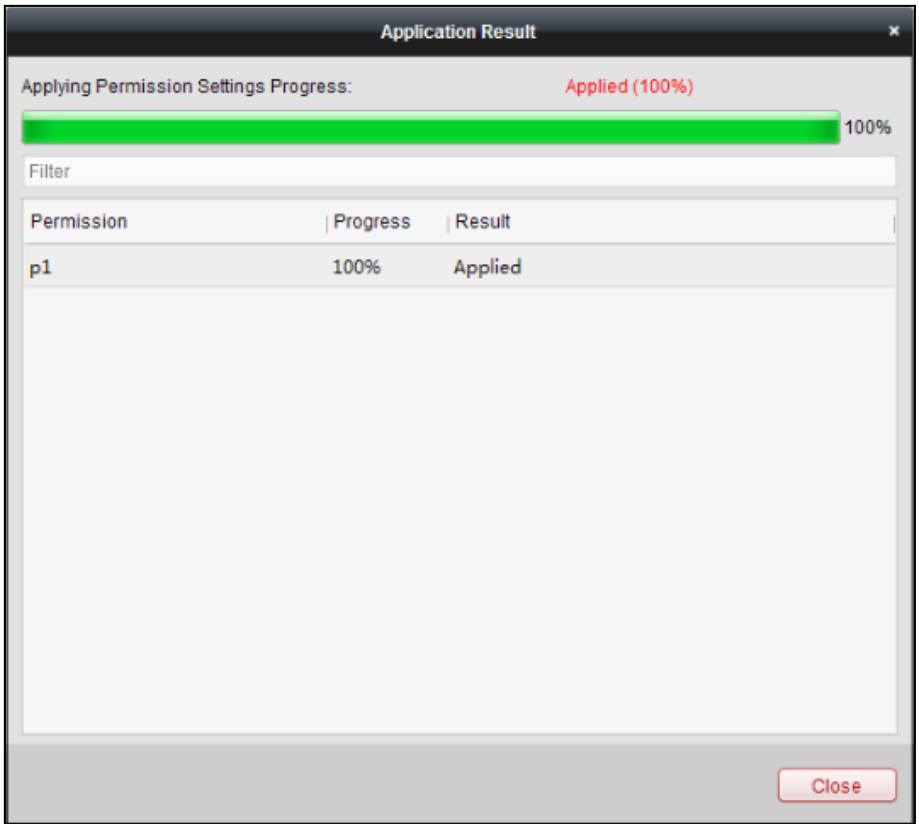
7.7.2 Применение разрешений

Цель

После настройки разрешений вы должны применить добавленные разрешения к устройствам контроля доступа.

Шаги

1. Выберите разрешения, которые вы хотите применить к устройству контроля доступа.
   Для выбора нескольких разрешений удерживайте клавиши *Ctrl* или Shift.
2. Нажмите Apply to Device («Применить к устройству») для начала применения выбранных разрешений к устройству контроля доступа или вызывной панели.
3. Появится следующее всплывающее окно, показывающее результат применения разрешений.



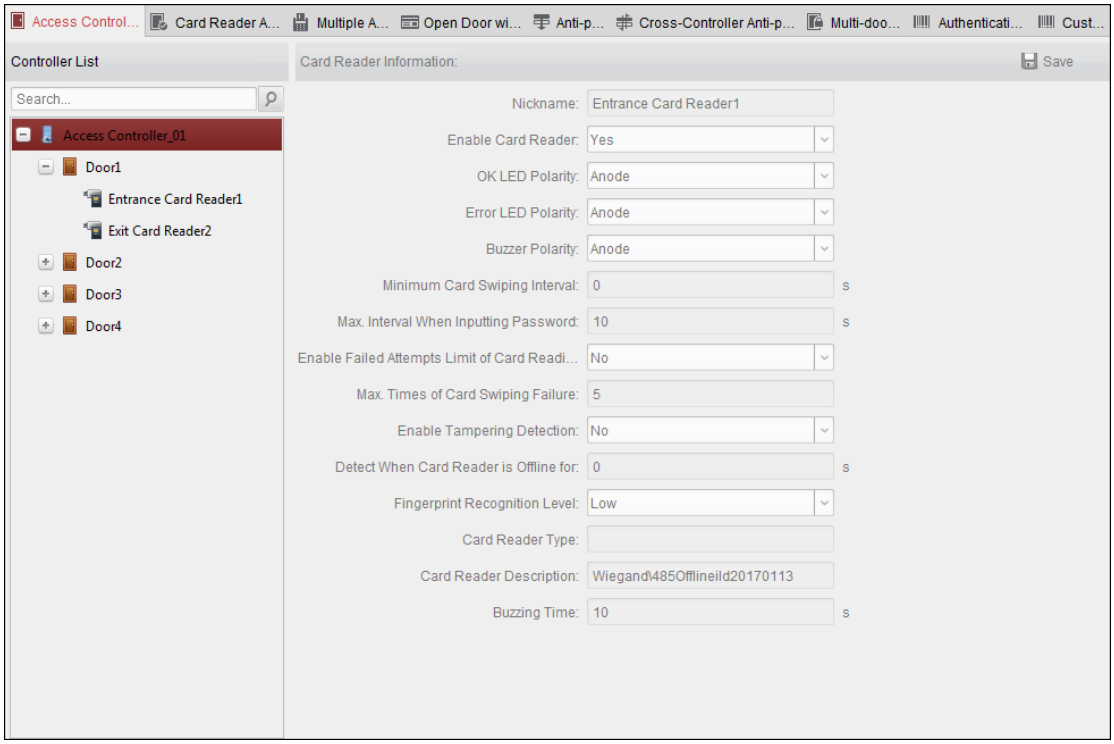
7.8 Дополнительные функции

Цель

После настройки данных пользователя, шаблона и разрешений контроля доступа можно настроить дополнительные параметры приложения контроля доступа.

Примечание. Устройство должно поддерживать возможность использования расширенных функций.

Нажмите иконку для перехода в следующее меню.



7.8.1 Параметры контроля доступа

Цель

После настройки данных пользователя, шаблона и разрешений контроля доступа можно настроить дополнительные параметры приложения контроля доступа.

Нажмите вкладку **Access Control Parameters** («Параметры контроля доступа») для входа в меню настройки параметров.

Параметры двери

Шаги

1. В списке контроллеров слева нажмите , чтобы развернуть информацию устройства контроля доступа, выберите дверь (точку контроля доступа), и вы сможете отредактировать информацию о выбранной двери справа.
2. Также можно настроить следующие параметры:

   Магнитоконтактный датчик: магнитоконтактный датчик находится в состоянии **Remain Closed** («Оставить дверь закрытой») (за исключением особых условий).

   Тип кнопки выхода: тип кнопки выхода находится в состоянии **Remain Open** («Оставить дверь открытой») (за исключением особых условий).

   Время до закрытия двери: после считывания обычной карты и срабатывания реле запускается таймер для блокировки двери.

   Продолжительность открытого состояния двери при использовании карты с расширенными полномочиями: Магнитоконтактный датчик двери может быть включен с соответствующей задержкой после того, как пользователь считает карту.

   Тревога тайм-аута открытой двери: тревога сработает, если дверь не будет закрыта

в течение заданного периода времени.

Включить блокировку двери при закрытии двери (зарезервировано): дверь может быть заблокирована после ее закрытия, даже если порог блокировки двери не достигнут.

Код принуждения: дверь может быть открыта при помощи кода принуждения. При этом клиент может создает уведомление о событии принуждения.

Суперпароль: пользователь может открыть дверь с помощью суперпароля.

Код отклонения: введите код отклонения, чтобы отключить бипер считывателя карт.

Примечания.

- Код отклонения, суперпароль и код принуждения должны отличаться.
- Код отклонения, суперпароль и код принуждения должны отличаться от пароля аутентификации.
- Код отклонения, суперпароль и код отклонения должны содержать от 4 до 8 цифр.

3. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

Параметры считывателя карт

Шаги

1. В списке устройств слева нажмите , чтобы раскрыть параметры двери. Выберите имя считывателя карт, чтобы редактировать параметры считывателя карт.
2. Также можно настроить следующие параметры:

Nickname («Наименование»)

Выберите наименование считывателя карт по своему выбору.

Enable Card Reader («Включить считыватель карт»)

Выберите **Yes** («Да»), чтобы включить считыватель карт.

OK LED Polarity («Полярность светодиода OK»)

Выберите полярность светодиода OK на материнской плате считывателя карт.

Error LED Polarity («Полярность светодиода Error»)

Выберите полярность светодиода Error на материнской плате считывателя карт.

Buzzer Polarity («Полярность бипера»)

Выберите полярность светодиода бипера на материнской плате считывателя карт.

Minimum Card Swiping Interval («Мин. интервал считывания карты»)

Если интервал считывания одной и той же карты меньше установленного значения, считывание карты будет недействительным. Можно задать данное значение в диапазоне от 0 до 255.

Max. Interval When Inputting Password («Макс. интервал времени при вводе пароля»)

Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

Enable Failed Attempts Limit of Card Reading («Активировать предел неудачных попыток считывания карты»)

Можно включить функцию сообщения о тревоге при достижении максимального количества неудачных попыток считывания карты.

Max. Times of Card Swiping Failure («Максимальное количество сбоев при считывании

карты»)
Установите максимальное количество неудачных попыток считывания карты.
Enable Tampering Detection («Включение тревоги тампера»)
Включите детектор саботажа на считывателе карт.
Примечание. Контроллер доступа серии F-KD-1300 не поддерживает данную функцию.
Detect When Card Reader is Offline for («Определить, когда считыватель карт находится в автономном режиме»): если устройство контроля доступа не может подключиться к считывателю карт в течение установленного времени, считыватель карт отключится автоматически.
Примечание. Контроллер доступа серии F-KD-1300 не поддерживает данную функцию.
Время бипера: настройте время зуммера для считывателя карт. Доступный диапазон времени: от 0 до 5 999 с. 0 представляет непрерывную работу бипера.
Описание считывателя карт: отображение информации о считывателе карт.

3. Нажмите кнопку Save («Сохранить») для сохранения настроек.

7.8.2 Аутентификация с помощью считывателя карт

Цель

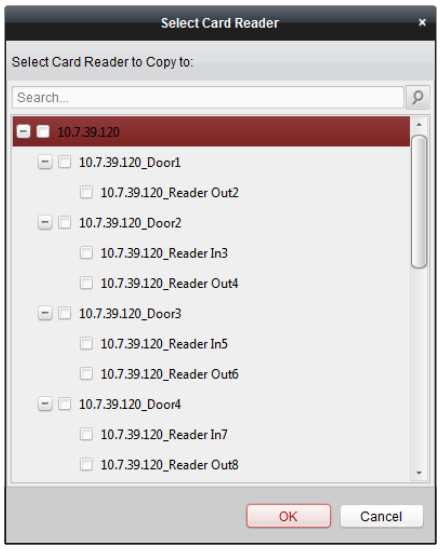
Установите правила прохождения через контрольные пункты для считывателя карт устройства контроля доступа.

Шаги

1. Нажмите Card Reader Authentication («Аутентификация с помощью считывателя карт») и выберите считыватель карт.
2. Выберите режим аутентификации считывателя карт. Доступные режимы аутентификации зависят от типа считывателя карт:
   - Карта и пароль: дверь можно открыть при помощи ввода пароля или считывания карты.
     Примечание. Пароль представляет собой пароль карты, установленный при выдаче карты. Подробная информация представлена в разделе *7.5.2 Управление пользователями*.
   - Карта или пароль аутентификации: дверь можно открыть при помощи ввода пароля аутентификации или считывания карты.
     Примечание. Пароль аутентификации — это пароль, установленный для открытия двери. Подробная информация представлена в разделе *7.8.5 Пароль аутентификации.*
   - Карта: дверь можно открыть только считыванием карты.
3. Перемещайте ползунок шкалы времени, чтобы нарисовать цветную полосу в расписаниее. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи считывателя карт.
4. Повторите этот шаг для установки других отрезков времени.
   Выберите настроенный день и нажмите Copy to Week («Применить ко всем дням недели»), чтобы применить эти настройки ко всем дням недели.

(Опционально) Можно нажать **Delete** («Удалить»), чтобы удалить выбранный период времени, или **Clear** («Очистить»), чтобы удалить все настроенные периоды времени.

5. (Опционально) Нажмите **Copy to (**«Копировать в...»), чтобы копировать настройки в другие считыватели карт.



6. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

7.8.3 Открытие двери первой картой

Цель

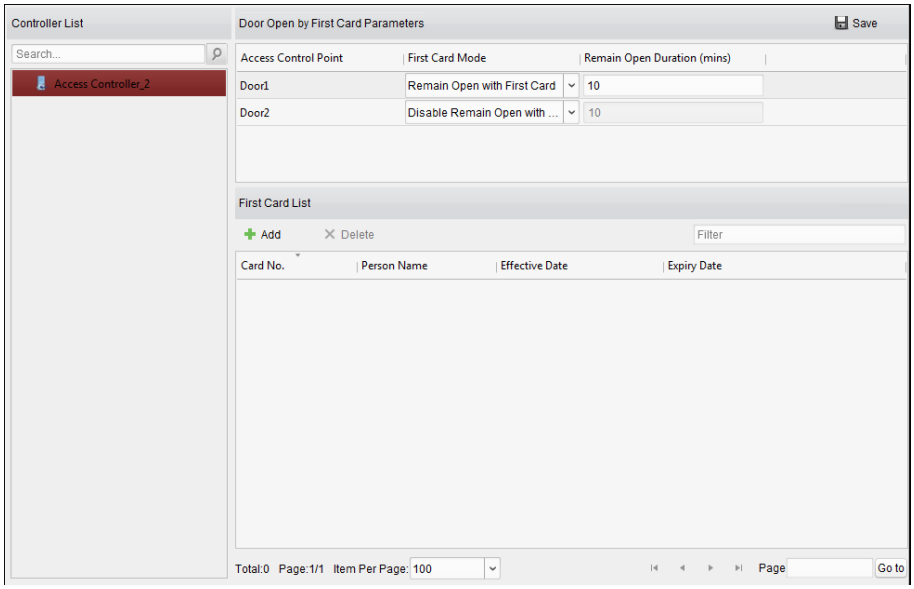
Для одной точки контроля доступа можно назначить несколько первых карт. После первого считывания карты несколько других пользователей получат доступ к дверям и разрешения на другие действия. Варианты режимов при считывании первой карты: **Remain Open with First Card** («Оставить дверь открытой при считывании первой карты»), **Disable Remain Open with First Card** («Не оставлять дверь открытой при считывании первой карты») и **First Card Authorization** («Авторизация первой карты»).

Remain Open with First Card («Оставить дверь открытой при считывании первой карты»): После считывания первой карты дверь остается открытой в течение заданного промежутка времени и до истечения оставшегося времени открытия.

Авторизация первой карты: Все режимы аутентификации (за исключением авторизации суперкарты, принудительной карты и кода принуждения) доступны только после авторизации первой карты.

Шаги

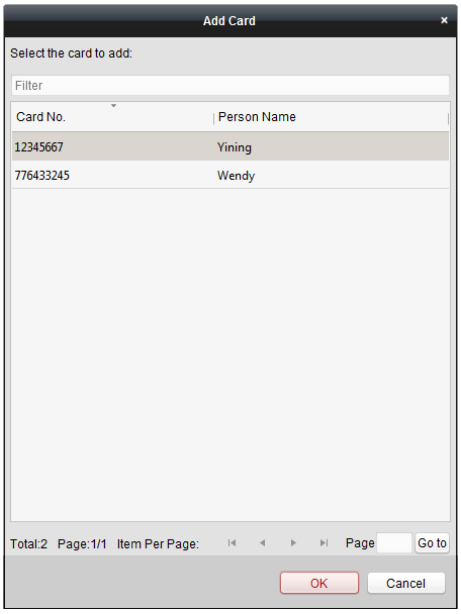
1. Нажмите **Open Door with First Card** («Открытие двери первой картой»), чтобы перейти в соответствующий интерфейс.



2. Выберите устройство контроля доступа из списка слева.
3. Для точки контроля доступа выберите режим считывания первой карты в раскрывающемся списке.
4. (Опционально) При выборе **Remain Open with First Card** («Оставить дверь открытой при считывании первой карты») необходимо задать продолжительность открытия.

   Примечание.

   - Допустимый диапазон длительности открытого состояния двери: от 0 до 1440 минут. По умолчанию, значение составляет 10 минут.
   - В режиме авторизации первой карты можно получить доступ к двери при помощи считывания суперкарты, карты принуждения или посредством кода принуждения (при этом не выполнять считывание первой карты).
   - Чтобы отключить режим первой карты, необходимо считать первую карту еще раз.
   - Авторизация первой карты действует только в текущий день. Срок действия авторизации истекает после 24:00 текущего дня.
5. В списке **First Card** («Первая карта») нажмите **Add** («Добавить»), чтобы открыть соответствующее диалоговое окно.



1) Выберите карты, которые нужно добавить в качестве первой карты для двери.
   Примечание. Сначала необходимо настроить разрешения карты и применить разрешения к устройству контроля доступа. Подробная информация представлена в разделе *7.7 Конфигурация разрешений*.
2) Нажмите **OK** для подтверждения добавления карты.

6. Можно нажать **Delete** («Удалить»), чтобы удалить карту из списка первых карт.
7. Нажмите **Save** («Сохранить»), чтобы сохранить и применить новые настройки.

7.8.4 Запрет двойного прохода по маршруту

Цель

Можно установить запрет двойного прохода для считывателей карт одного контроллера доступа. Считайте карту в соответствии с настроенным маршрутом считывания карты. Только один пользователь может пройти точку контроля доступа после считывания карты.

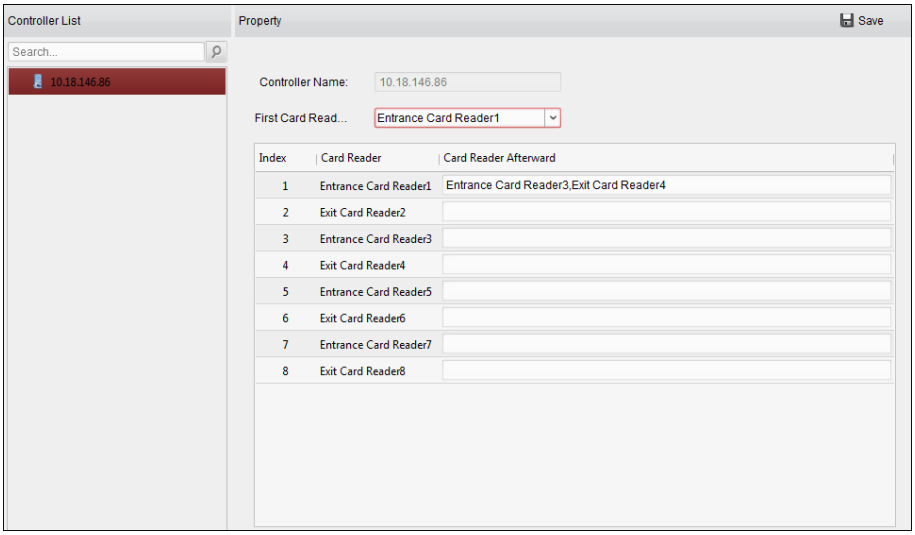
Примечания.

- Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей.
- Сначала необходимо включить функцию запрет двойного прохода по маршруту на устройстве контроля доступа.

Настройка маршрута считывания карт (порядок срабатывания считывателя карт)

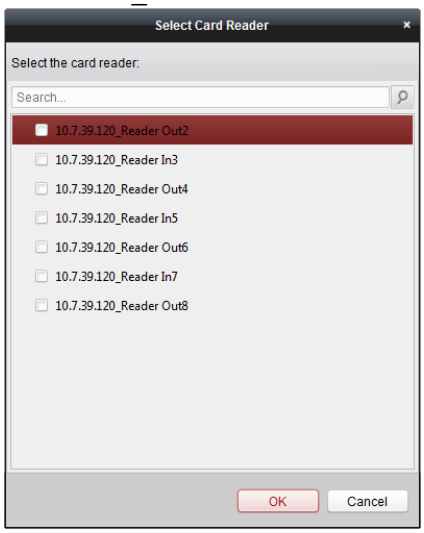
Шаги

1. Нажмите вкладку **Anti-passing Back** («Запрет двойного прохода по маршруту») для перехода в следующее меню.



2. Выберите устройство контроля доступа из списка устройств слева.
3. В поле **First Card Reader** («Первый считыватель карт») выберите считыватель карт в качестве первого считывателя карт на маршруте.
4. В списке нажмите **Card Reader Afterward** («Последующий считыватель карт») и выберите считыватель карт.

   Пример: выберите Reader In_01 в качестве начала маршрута, а Reader In_02, Reader Out_04 в качестве связанных считывателей карт. После этого пользователь сможет пройти через точку контроля доступа, считав карту в следующей последовательности: Reader In_01, Reader In_02 и Reader Out_04.



   Примечание. Для одного считывателя карт можно добавить до 4 последующих считывателей карт.
5. (Опционально) Можно снова войти в диалоговое окно **Select Card Reader** («Выбор считывателя карт»), чтобы изменить последующие считыватели карт.
6. Нажмите **Save** («Сохранить»), чтобы сохранить и применить новые настройки.

7.8.5 Пароль аутентификации

Цель

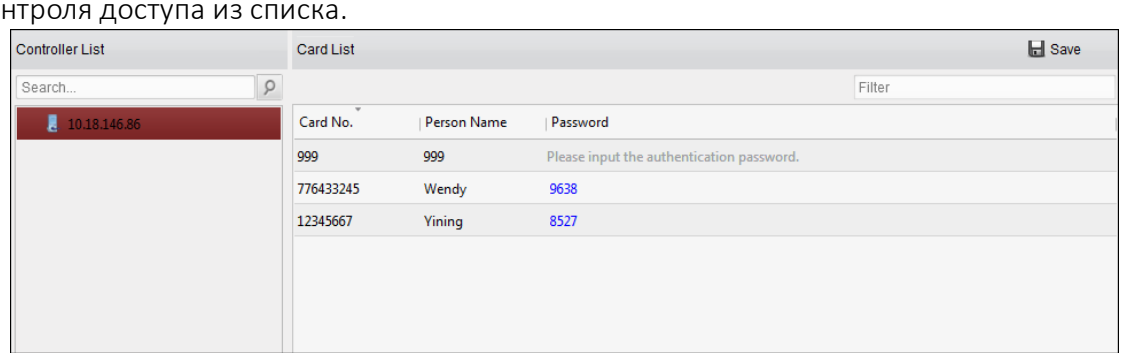
После настройки пароля аутентификации дверь можно открыть дверь посредством ввода пароля аутентификации на клавиатуре считывателя карт.

Примечания.

- Функция пароля аутентификации действительна только во время расписания, когда режим аутентификации считывателя карт для устройства контроля доступа установлен как **Card or Authentication Password** («Карта или пароль аутентификации»). Подробная информация представлена в разделе *7.8.2 Аутентификация с помощью* считывателя карт.
- Устройства контроля доступа должно поддерживать данную функцию.

Шаги

1. Нажмите **Authentication Password** («Пароль аутентификации») и выберите устройство контроля доступа из списка.



   Будут отображены все карты и пользователи, связанные с устройством.

   Примечание. Подробная информация о настройке и применении разрешений представлена в разделе *7.7 Конфигурация разрешений.*

2. Нажмите поле **Password** («Пароль») и введите пароль аутентификации для карты.

   Примечание. Пароль аутентификации должен содержать от 4 до 8 цифр.

3. После настройки пароля аутентификации функция пароля аутентификации карты будет включена по умолчанию.
4. (Опционально) Для поиска можно ввести ключевые слова, такие как номер карты, имя пользователя или пароль аутентификации.

Примечания.

- К одному устройству контроля доступа можно добавить до 500 карт с паролем аутентификации.
- Пароль должен быть уникальным и не может совпадать с суперпаролем, кодом принуждения и кодом отклонения в параметрах контроля доступа.

7.8.6 Пользовательская настройка Wiegand

Цель

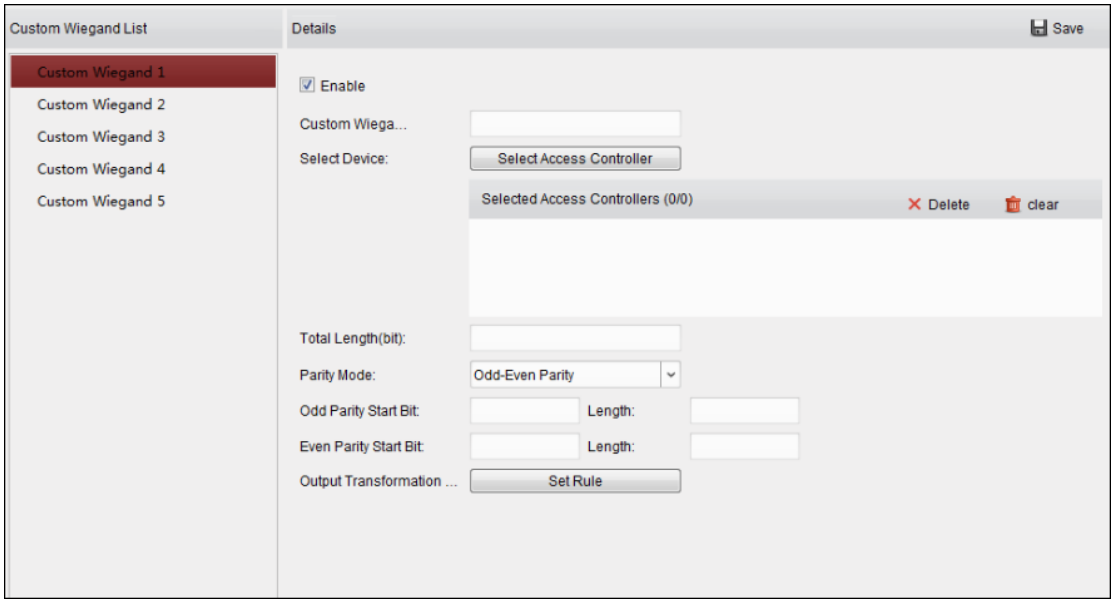
Основываясь на знании правил загрузки для стороннего Wiegand, можно установить несколько настраиваемых правил Wiegand для связи между контроллером и сторонними считывателями карт.

Перед началом

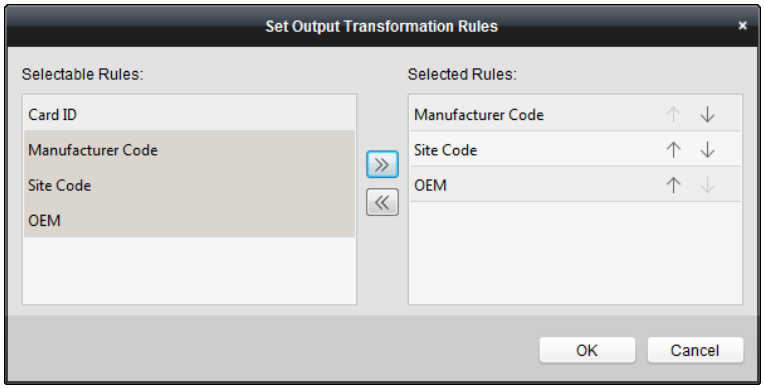
Подключите сторонние считыватели карт к контроллеру.

Шаги

1. Нажмите **Custom Wiegand** («Пользовательская настройка Wiegand»), чтобы перейти на соответствующую страницу.



2. Выберите настраиваемый Wiegand слева.
3. Нажмите **Enable** («Включить»), чтобы включить пользовательскую настройку Wiegand.
4. Настройте имя Wiegand.
5. Выберите устройство.
   1) Нажмите **Select Device** («Выбрать устройство»).
   2) Выберите устройство, на котором выполняется пользовательская настройка Wiegand.
   3) Нажмите **OK** для сохранения настроек.
6. Введите общую длину и выберите режим четности в раскрывающемся списке.
   При выборе **Odd-Even Parity** («Контроль четности / нечетности») необходимо настроить старт-бит контроля нечетности и длину, старт-бит контроля четности и длину.
   При выборе четности XOR необходимо настроить старт-бит четности XOR, длину каждой группы и общую длину.
   При выборе варианта **None** («Нет») режим четности настраивать не нужно.
7. Установите правило преобразования выходного сигнала.
   1) Нажмите **Set Rule** («Установить правило»), чтобы открыть окно установки правила преобразования выходного сигнала.



2) Выберите правила в левом списке.
   Примечание. Нажмите *Shift*, чтобы выбрать несколько правил.
3) Нажмите , чтобы переместить выбранные правила в список справа.
4) (Опционально) Нажмите или , чтобы изменить порядок правил.
5) (Опционально) Выберите правила в списке **Selected Rule** («Выбранное правило») и нажмите , чтобы удалить правило из списка справа.
6) Нажмите **OK** для сохранения настроек.
7) На вкладке настраиваемого Wiegand установите старт-бит правила, длину и десятичную цифру.

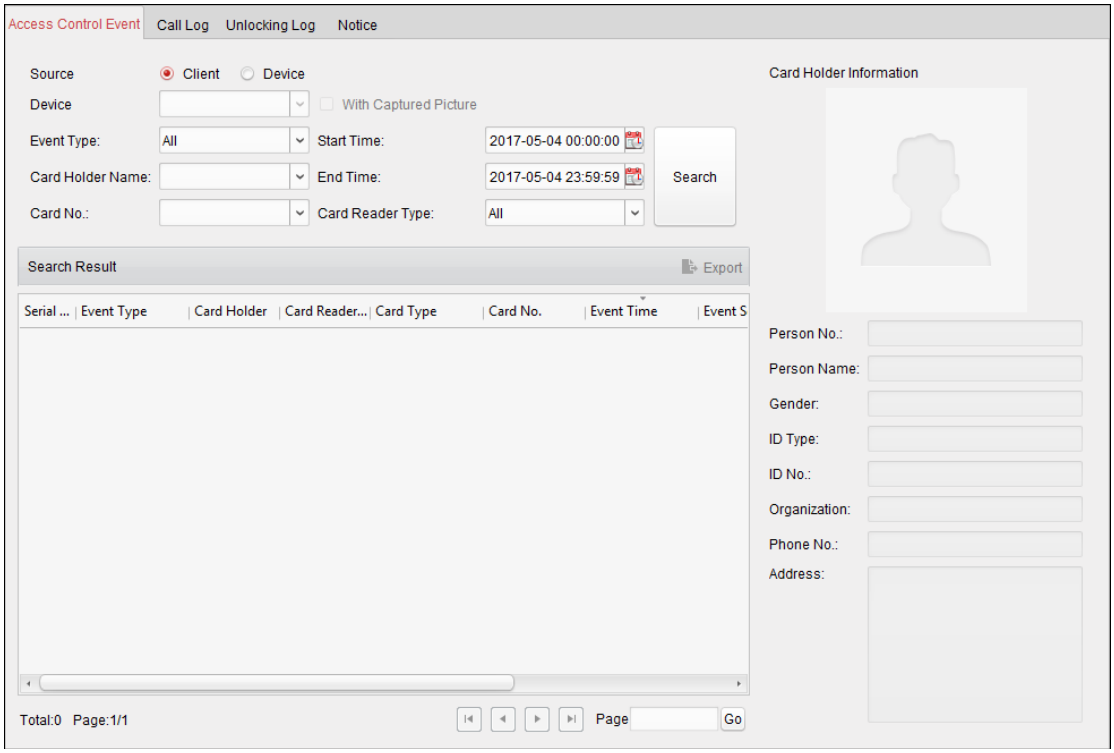
8. Нажмите **Save** («Сохранить») в правом верхнем углу для сохранения настроек.
   Примечания.
   - По умолчанию устройство отключает настраиваемую функцию Wiegand.
   - Если функция пользовательской настройки Wiegand включена, все интерфейсы Wiegand в устройстве будут использовать настроенный протокол Wiegand.
   - Можно указать до 5 настраиваемых Wiegand.
   - Имя настраиваемого Wiegand может содержать до 32 символов.
   - Общая длина может достигать 80 бит.
   - Старт-бит и длина нечетности и старт-бит и длина четности находятся в диапазоне от 1 до 80 бит.
   - Старт-бит ID карты, кода производителя, кода сайта и производителя оборудования должны находиться в диапазоне от 1 до 80 бит.
   - Подробная информация о пользовательской настройке Wiegand представлена в приложении.

7.9 Поиск события контроля доступа

Цель

Можно искать события истории контроля доступа, включая событие исключения устройства, событие двери, срабатывание тревожного входа и событие считывателя карт.

Нажмите и перейдите на вкладку **Access Control Event** («Событие контроля доступа»), чтобы войти в соответствующий интерфейс.



Шаги

1. Выберите источник.
   Можно выбрать **Client** («Клиент») или **Device** («Устройство»).
2. Введите условие поиска (источник, тип события, имя владельца карты, № карты, захват, время начала и окончания).
3. Нажмите **Search** («Поиск») для получения результатов поиска.
4. Просмотрите информацию о событии в списке событий.
5. Нажмите событие, чтобы просмотреть информацию о держателе карты на панели **Card Holder Information** («Информация о держателе карты») в левой части страницы.
6. Можно нажать **Export** («Экспорт») для экспорта результатов поиска на локальный ПК.

7.10 Настройка событий контроля доступа

Цель

Для добавленного устройства контроля доступа можно настроить привязку действий, включая привязку событий контроля доступа, привязку тревожного входа, привязку карты событий и привязку различных устройств.

Нажмите на панели управления.

Или нажмите **Tools → Event Management** («Инструменты → Управление событиями») для открытия страницы управления событиями.

7.10.1 Привязка событий контроля доступа

Цель

Можно назначить действия в соответствии с событием контроля доступа, настроив правило.

Например, при обнаружении события контроля доступа появляется звуковое предупреждение или выполняются другие настроенные действия.

Примечание. Привязка в данном контексте означает привязку действий клиентского ПО.

Шаги

1. Нажмите вкладку **Access Control Event** («Событие контроля доступа»).
2. Добавленные устройства контроля доступа отобразятся в панели устройств контроля доступа слева.
   Выберите устройство контроля доступа, тревожный вход, точку контроля доступа (дверь) или считыватель карт, чтобы настроить привязку событий.
3. Выберите тип события, чтобы настроить привязку.
4. Выберите камеру для привязки. Когда произойдет выбранное событие, появится изображение или видео с камеры.
   Чтобы сделать захват снимка камеры, можно установить расписание захвата и путь хранения во вкладке **Storage Schedule** («Расписание хранения»).
5. Нажмите соответствующее поле, чтобы активировать действия по привязке. Подробная информация представлена в *таблице 14.1 Действия привязки для события контроля доступа.*
6. Нажмите **Save** («Сохранить») для сохранения настроек.
7. Можно нажать **Copy to** («Копировать в...»), чтобы скопировать событие контроля доступа на другое устройство контроля доступа, тревожный вход, точку контроля доступа или считыватель карт.
   Выберите параметры для копирования, выберите цель для копирования и нажмите **OK** для подтверждения.

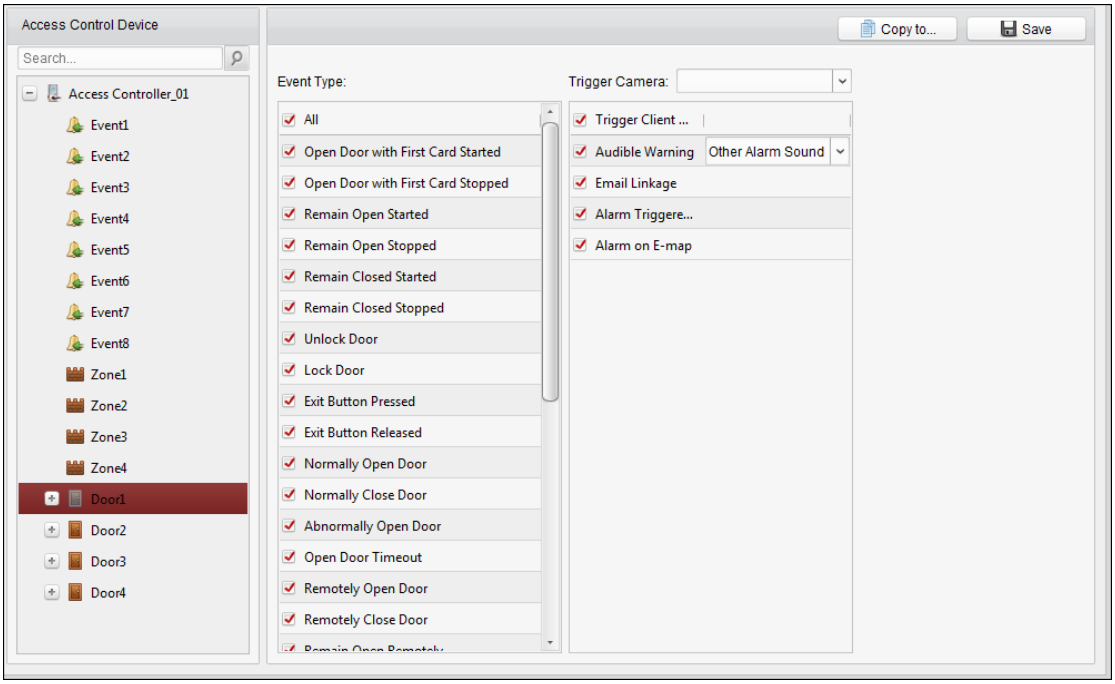


Таблица 7-1 Действия привязки для события контроля доступа

Действия привязки	Описание
Audible Warning («Звуковое предупреждение»)	Клиентское программное обеспечение выдает звуковое предупреждение при срабатывании тревоги. Выберите сигнал для звукового предупреждения.
Email Linkage («Привязка Email»)	Отправьте электронное уведомление о тревоге одному или нескольким получателям.
Alarm on E-map («Тревога на электронной карте»)	Отображение информации о тревоге на электронной карте. *Примечание.* Привязка доступна только для точки контроля доступа и тревожного входа.
Alarm Triggered Pop-up Image («Всплывающее изображение при срабатывании тревоги»)	При срабатывании тревоги появляется изображение с информацией о тревоге.

7.10.2 Привязка тревожного входа устройства контроля доступа

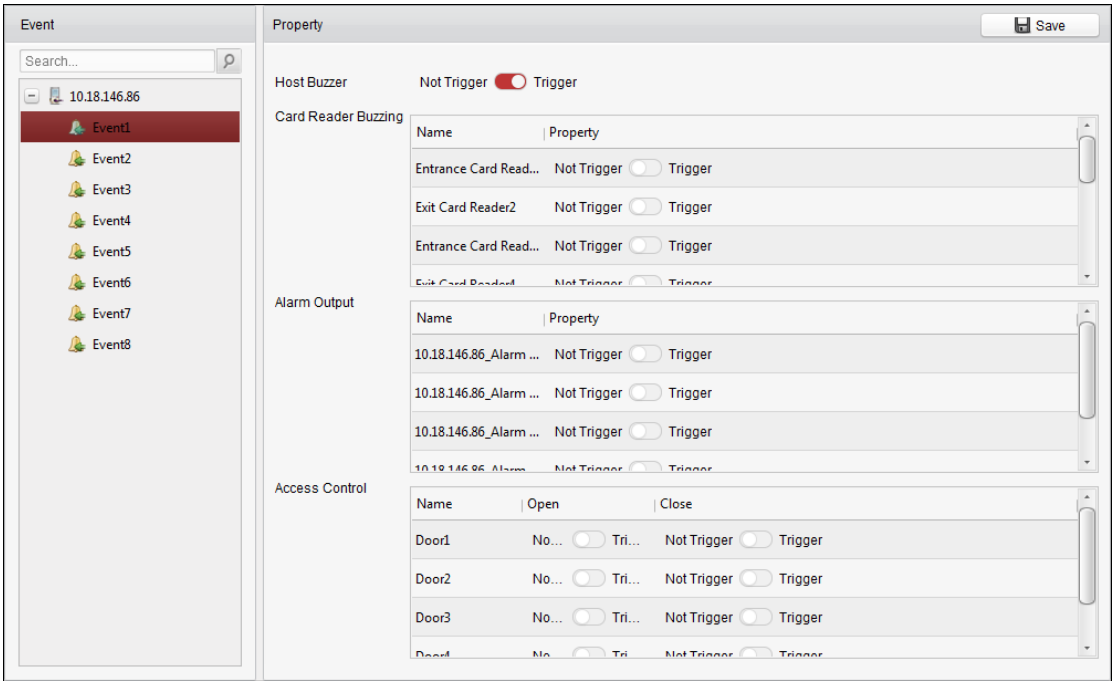
Цель

Тревожные входы устройств контроля доступа могут быть связаны с некоторыми действиями (например, срабатывание тревожного выхода, бипера хоста).

Примечание. Привязка в данном контексте означает привязку действий клиентского ПО.

Шаги

1. Нажмите вкладку **Access Control Alarm Input** («Тревожный вход устройства контроля доступа») для входа в соответствующее меню.



2. В списке событий слева выберите тревожный вход.
3. Переместите ползунок с положения на положение , чтобы включить это действие.

   Бипер хоста: контроллер доступа выдаст звуковое предупреждение.

   Бипер считывателя карт: считыватель карт выдаст звуковое предупреждение.

   Тревожный выход: тревожный выход будет активирован для уведомления.

   Точка контроля доступа (открытие / закрытие): при срабатывании тревоги входа событий дверь закроется или откроется.

   Примечание. Необходимо выбрать один параметр двери при настройке: закрытая или открытая.
4. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

7.10.3 Привязка карты / события

Нажмите вкладку **Event / Card Linkage** («Привязка карты / события») для перехода в соответствующее меню.

Примечания.

- Привязка карты / события должна поддерживаться устройством.
- Привязка в данном контексте означает привязку действий клиентского ПО.

Выберите устройство контроля доступа из списка слева.

Нажмите кнопку **Add** («Добавить») для добавления новой привязки. Можно выбрать в качестве **Event source** («Источник события») значение **Event Linkage** («Привязка события»).

Привязка события

При привязке событий тревожное событие можно разделить на четыре типа: событие устройства, тревожный вход, событие двери и событие считывания карт.

Шаги

1. Выберите значение **Event Linkage** («Привязка события»), и выберите тип события из выпадающего списка **Event type** («Тип события»).
   - Для события устройства: выберите тип события из выпадающего списка.
   - Для тревожного входа: выберите тип как тревожный сигнал или восстановление после тревоги и выберите имя тревожного входа из таблицы.
   - Для события двери: выберите тип события и выберите дверь из таблицы.
   - Для события считывателя карт: выберите тип события и выберите считыватель карт из таблицы.
2. Настройте цель привязки и переместите ползунок с положения на положение , чтобы включить это действие.
   - **Бипер хоста:** звуковое предупреждение контроллера доступа будет включено / отключено.
   - **Захват:** будет включен захват изображений в режиме реального времени.
   - **Бипер считывателя карт:** звуковое предупреждение считывателя карт будет включено / отключено.
   - **Тревожный выход:** тревожный выход будет включен / отключен для уведомления.
   - **Точка контроля доступа:** будет включено одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

     Примечания.
     - Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.
     - Целевая дверь и дверь, используемая в качестве источника, не могут являться одной дверью.
3. Нажмите **Save** («Сохранить»), чтобы сохранить и применить новые настройки.

Привязка карты

Шаги

1. Выберите тип привязки **Card Linkage** («Привязка карты»).
2. Введите номер карты или выберите карту из выпадающего списка.
3. Выберите считыватель карт из таблицы.
4. Настройте цель привязки и переместите ползунок с положения на положение , чтобы включить это действие.
   - **Host Buzzer («Бипер хоста»)**

     Звуковое предупреждение контроллера доступа будет включено / отключено.
   - **Capture («Захват»)**

     Будет включен захват изображений в режиме реального времени.
   - **Card Reader Buzzer («Бипер считывателя карт»)**

     Звуковое предупреждение считывателя карт будет включено / отключено.
   - **Alarm Output («Тревожный выход»)**

     Тревожный выход будет включен / отключен для уведомления.

- Access Control Point («Точка контроля доступа»)
  Будет включено одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.

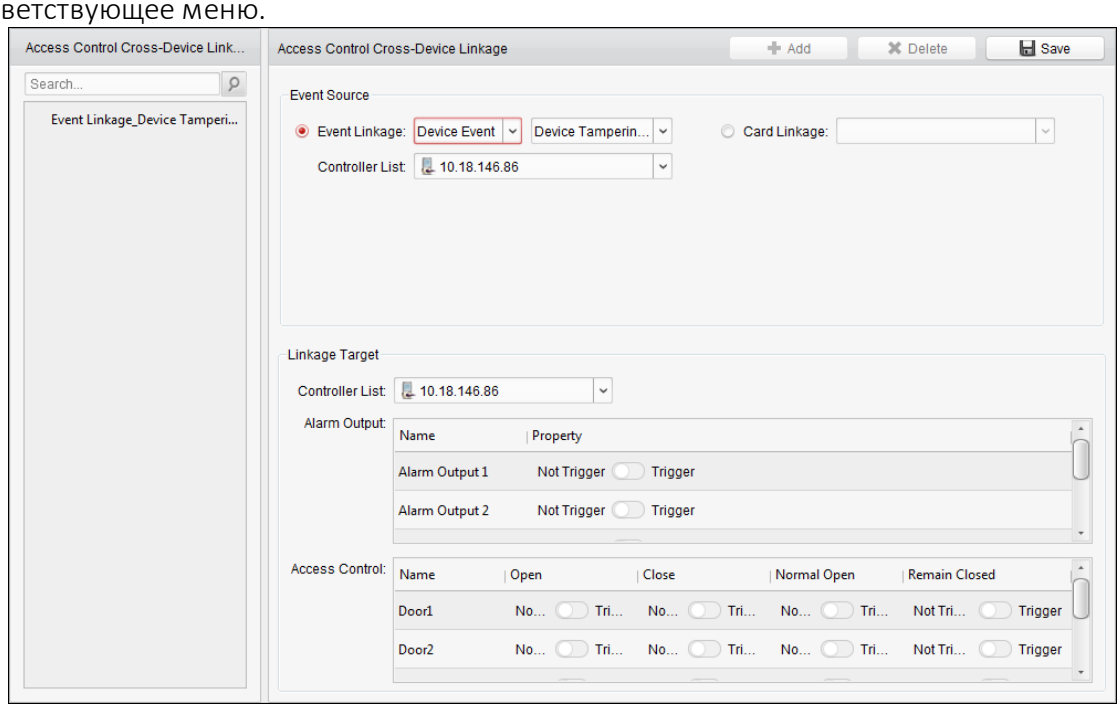
5. Нажмите **Save** («Сохранить»), чтобы сохранить и применить новые настройки.

7.10.4 Привязка различных устройств

Цель

Можно назначить запуск действия другого устройства контроля доступа при тревожном событии, установив соответствующее правило.

Нажмите вкладку **Cross-Device Linkage** («Привязка различных устройств») для перехода в соответствующее меню.



Нажмите кнопку **Add** («Добавить»), чтобы добавить привязку нового клиента. Можно выбрать в качестве **Event source** («Источник события») значение **Event Linkage** («Привязка события»).

Привязка события

При привязке событий тревожное событие можно разделить на четыре типа: событие устройства, тревожный вход, событие двери и событие считывания карт.

Шаги

1. Нажмите **Event Linkage** («Привязка события»), выберите устройство контроля доступа в качестве устройства-источника события и выберите тип события из выпадающего списка **Event type** («Тип события»).
   - Для события устройства: выберите тип события из выпадающего списка.
   - Для тревожного входа: выберите тип как тревожный сигнал или восстановление после тревоги и выберите имя тревожного входа из таблицы.
   - Для события двери: выберите тип события и выберите дверь из таблицы.

- Для события считывателя карт: выберите тип события и выберите считыватель карт из таблицы.

2. Настройте цель привязки, выберите устройство контроля доступа из списка в качестве цели привязки и переместите ползунок с положения на положение , чтобы включить это действие.
   - **Alarm Output («Тревожный выход»):** тревожный выход будет активирован для уведомления.
   - **Access Control Point («Точка контроля доступа»):** возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.
     Примечание. Возможно только одно из следующих состояний двери: открыта / закрыта, оставить открытой / оставить закрытой.
3. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

Привязка карты

Шаги

1. Выберите тип привязки **Card Linkage** («Привязка карты»).
2. Выберите карту из списка и выберите устройство контроля доступа в качестве устройства-источника события.
3. Выберите считыватель карт из таблицы.
4. Настройте цель привязки, выберите устройство контроля доступа из списка в качестве цели привязки и переместите ползунок с положения на положение , чтобы включить это действие.
   Alarm Output («Тревожный выход»): Тревожный выход будет активирован для уведомления.
5. Нажмите кнопку **Save** («Сохранить») для сохранения настроек.

7.11 Управление состоянием двери

Цель

Состояние двери точки контроля доступа устройства будет отображаться в режиме реального времени. Можно проверить состояние двери и соответствующие события выбранной двери. Можно управлять состоянием двери и устанавливать продолжительность состояния.

7.11.1 Управление группой контроля доступа

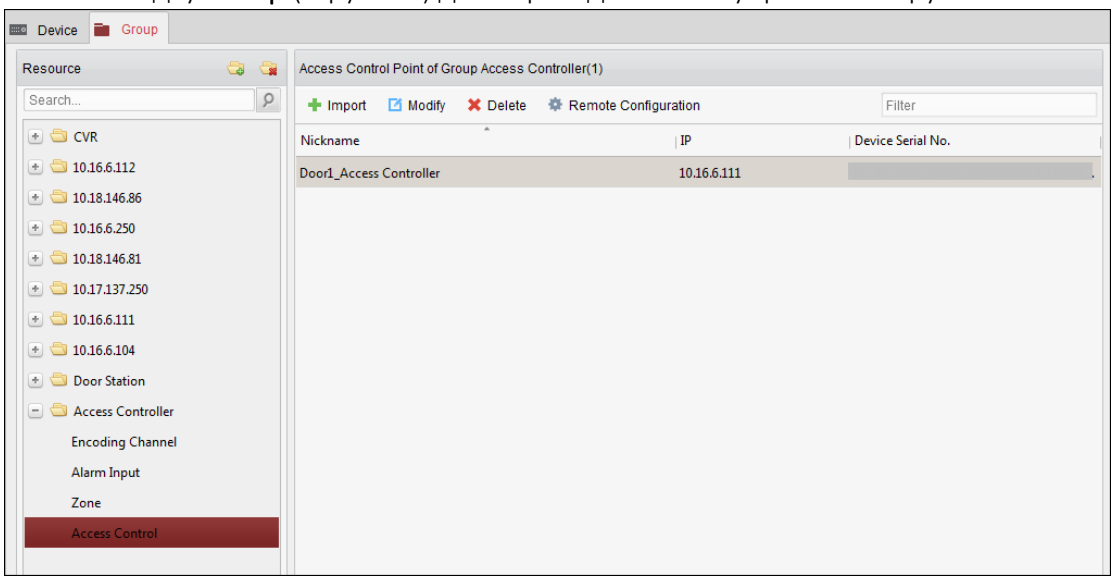
Цель

Перед тем, как контролировать состояние двери и установить продолжительность состояния, вам необходимо организовать ее в группу для удобного управления.
Выполните следующие шаги, чтобы создать группу для устройства контроля доступа.

Шаги

1. Нажмите на панели управления для открытия страницы управления устройствами.

2. Нажмите вкладку **Group** («Группа») для перехода в меню управления группами.



3. Выполните следующие шаги для добавления группы.
   1) Нажмите , чтобы открыть диалоговое окно добавления группы.
   2) Введите **group name** («имя группы») по вашему желанию.
   3) Нажмите **OK** для добавления новой группы в список групп.

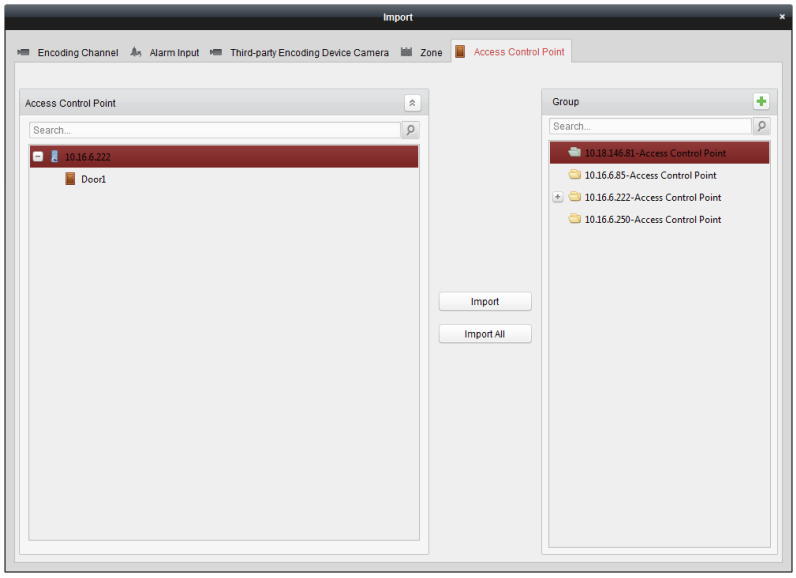
   Также можете поставить галочку **Create Group by Device Name** («Создать группу по имени устройства») для создания новой группы с именем, совпадающим с именем выбранного устройства.

4. Выполните следующие шаги, чтобы импортировать точки контроля доступа в группу:
   1) Нажмите **Import** («Импорт») в меню **Group Management** («Управление группой»), а затем нажмите вкладку **Access Control** («Контроль доступа») для перехода на страницу **Import Access Control** («Импорт контроля доступа»).

   Примечание.

   - Также можете выбрать вкладку **Alarm Input** («Тревожный вход») и импортировать тревожные входы в группу.
   - Для видео терминала доступа можно добавить камеры в качестве канала кодирования в группу.

   2) Выберите имена точек контроля доступа в списке.
   3) Выберите группу из списка групп.
   4) Нажмите **Import** («Импорт») для импорта выбранных точек контроля доступа в группу. Также можете нажать **Import All** («Импортировать все») для импорта всех точек контроля доступа в выбранную группу.



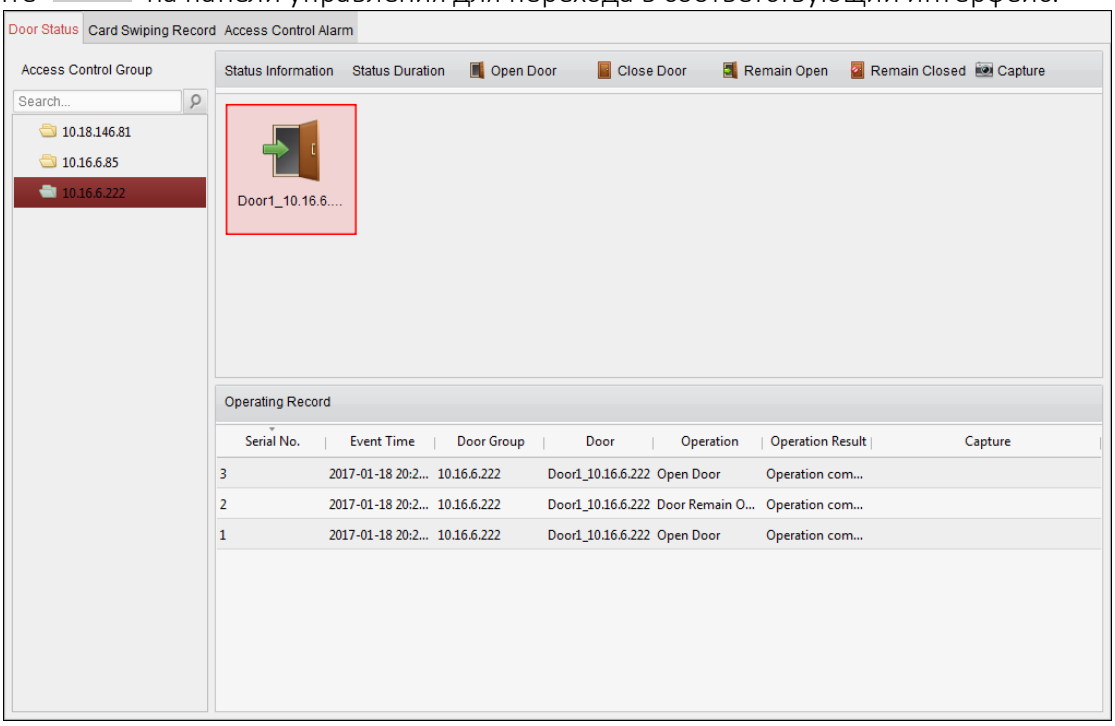
5. После импорта точек контроля доступа в группу можно нажать или дважды щелкнуть по имени группы / точки контроля доступа для ее редактирования.

7.11.2 Управление состоянием точки контроля доступа (дверь)

Цель

Можно управлять состоянием отдельной точки контроля доступа (дверь): открыть дверь, закрыть дверь, оставить дверь открытой и оставить дверь закрытой.

Нажмите на панели управления для перехода в соответствующий интерфейс.



Шаги

1. Выберите группу контроля доступа на панели слева. Подробная информация о группе контроля доступа представлена в *разделе 7.11.1 Управление группой контроля доступа.*
2. Точки контроля доступа выбранной группы контроля доступа будут отображаться справа.

   Нажмите на панели информации о состоянии, чтобы выбрать дверь.
3. Нажмите кнопки, представленные на панели информации о состоянии, чтобы управлять дверью.

   Open Door: открытие двери один раз.

   Close Door: закрытие двери один раз.

   Remain Open: оставить дверь открытой.

   Remain Closed: оставить дверь закрытой.

   Capture: захват вручную.
4. Можно просмотреть результат операции контроля в панели **Operation Log** («Журнал операций»).

Примечания.

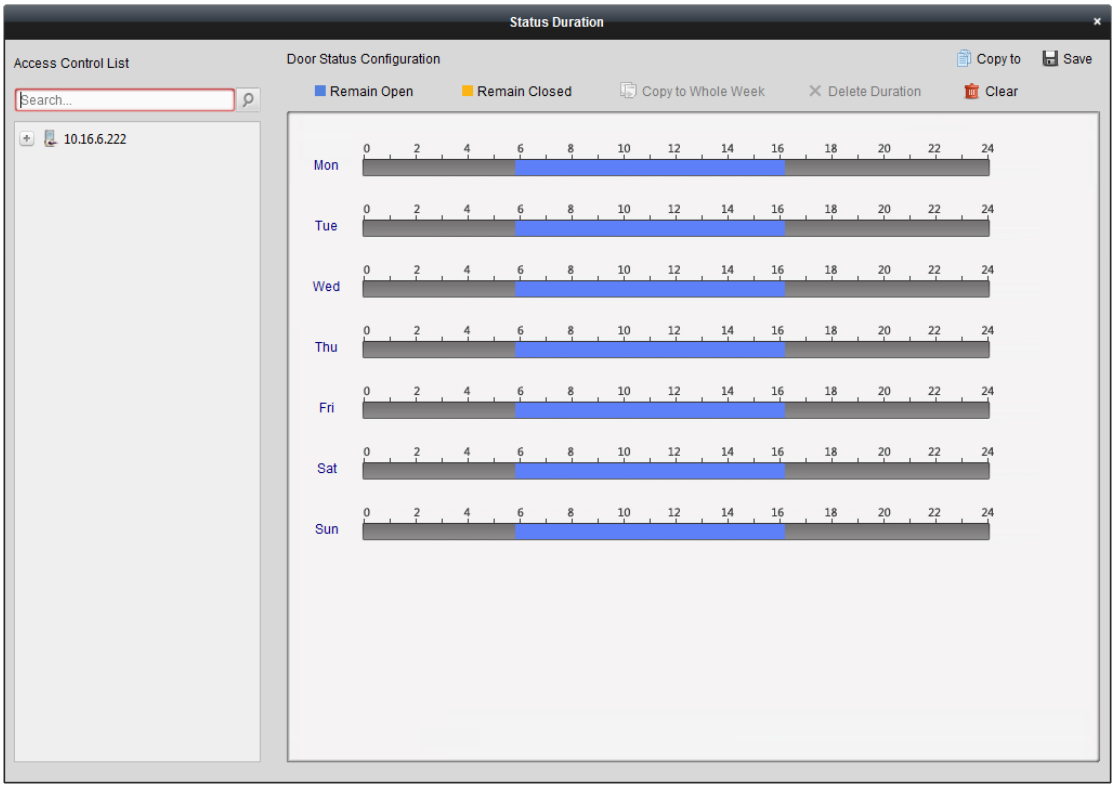
- При выборе состояния **Remain Open/Remain Closed** («Оставить открытой / Оставить закрытой»), дверь будет оставаться открытой / закрытой до тех пор, пока не будет задана новая команда контроля.
- Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата изображений. Функцию невозможно реализовать, пока не настроен сервер хранения.
- Если состояние двери — «оставить закрытой», открыть дверь можно только при помощи суперкарты или через клиентское ПО.

7.11.3 Настройка продолжительности состояния

Цель

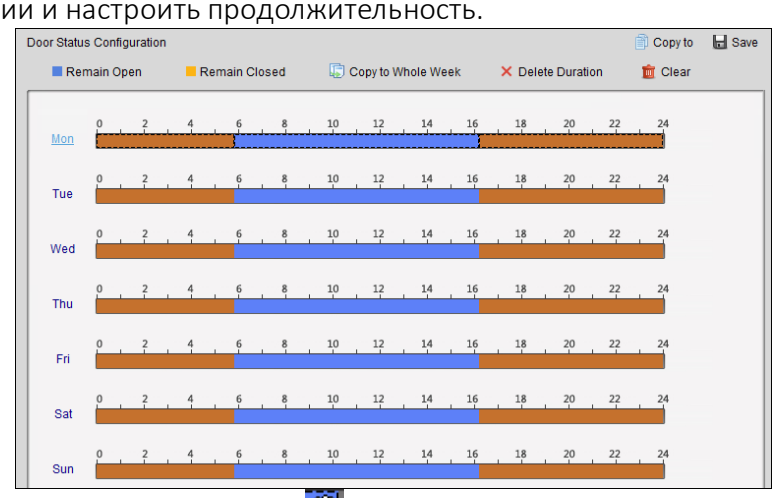
Можно настроить расписание на неделю для контрольной точки (двери) устройства контроля доступа, чтобы дверь оставалась открытой / закрытой в течение заданного промежутка времени.

В модуле **Door Status** («Состояние двери») нажмите **Status Duration** («Продолжительность состояния»), чтобы войти в соответствующий интерфейс.



Шаги

1. Выберите дверь из списка устройств контроля доступа слева.
2. На панели **Door Status Configuration** («Настройка состояния двери») справа задайте расписание для выбранной двери.
   1) Выберите состояние Remain Open или Remain Closed.
      Оставить дверь открытой: дверь будет оставаться открытой в течение заданного периода времени. Цвет кисти .
      Оставить дверь закрытой: дверь будет оставаться закрытой в течение заданного периода времени. Цвет кисти .
   2) Перемещайте ползунок шкалы времени, чтобы нарисовать цветную полосу в расписании и настроить продолжительность.



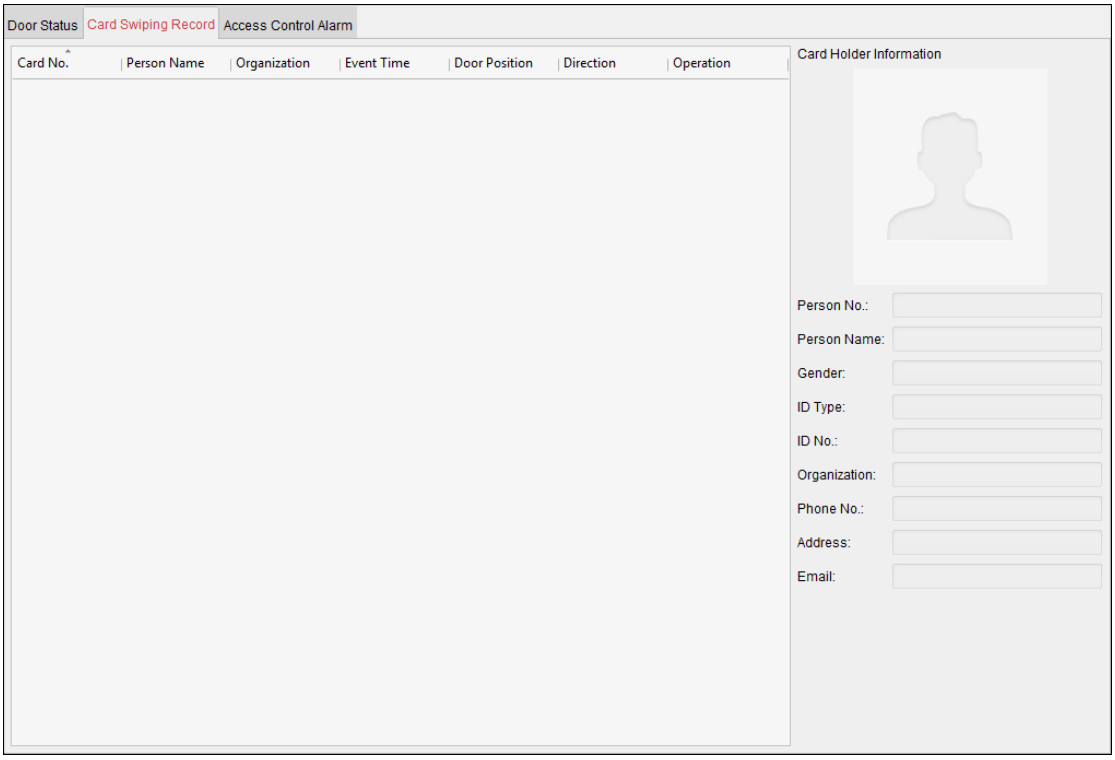
   3) Когда вид курсора изменится на , можно переместить только что отредактированный период времени.

Также можно редактировать отображаемый момент времени, чтобы с точностью настроить период времени.
Когда вид курсора изменится на , можно увеличить или уменьшить выбранный период времени.

3. (Опционально) Выберите период времени и нажмите **Copy to Whole Week** («Применить ко всей неделе»), чтобы скопировать настройки расписания и времени на другие дни недели.
4. Можно выбрать шкалу времени, а нажать **Delete Duration** («Удалить продолжительность»), чтобы удалить выбранный период времени.
   Можно нажать **Clear** («Очистить»), чтобы очистить все настроенные значения продолжительности в расписании.
5. Нажмите **Save** («Сохранить») для сохранения настроек.
6. Можно нажать **Copy to** («Копировать в...»), чтобы скопировать расписание на другие двери.

7.11.4 Запись считывания карты в режиме реального времени

Нажмите вкладку **Card Swiping Record** («Запись считывания карты»), чтобы войти в соответствующий интерфейс.



Будут отображены журналы считывания карт всех устройств контроля доступа в режиме реального времени. Можно просмотреть подробную информацию о событии считывания карты, включая номер карты, имя пользователя, организацию, время события и т. д.

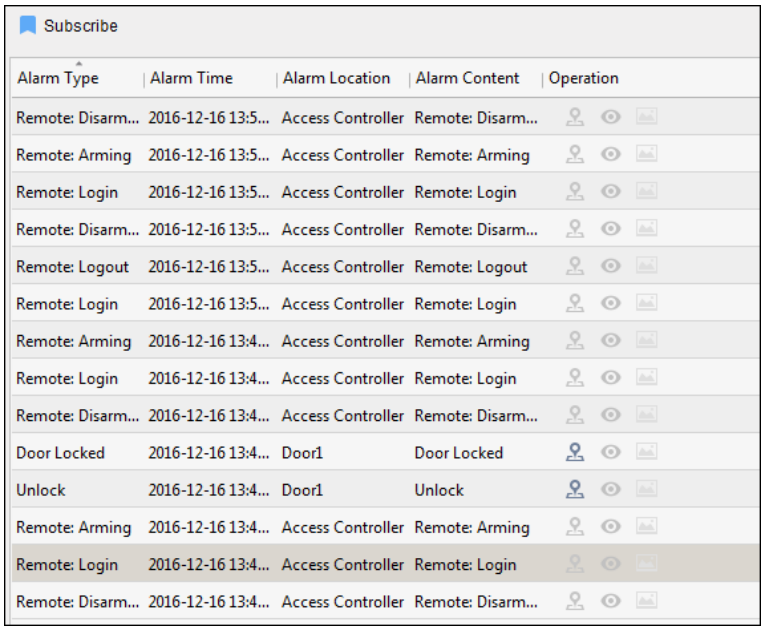
Можно нажать событие, чтобы просмотреть сведения о держателе карты, включая номер пользователя, имя пользователя, организацию, телефон, контактный адрес и т. д.

7.11.5 Тревога контроля доступа в режиме реального времени

Цель

Журналы событий контроля доступа будут отображаться в режиме реального времени, включая исключения устройства, события двери, события считывателя карт и события тревожного входа.

Нажмите вкладку **Access Control Alarm** («Тревога контроля доступа») для входа в соответствующее меню.

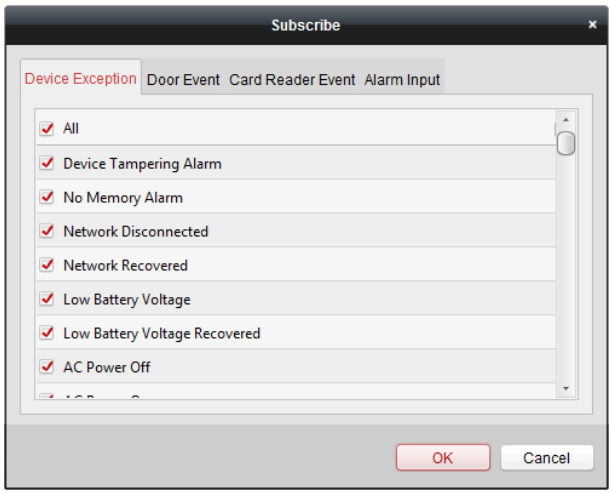


Subscribe

Alarm Type	Alarm Time	Alarm Location	Alarm Content	Operation
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Arming	2016-12-16 13:5...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Logout	2016-12-16 13:5...	Access Controller	Remote: Logout	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	
Door Locked	2016-12-16 13:4...	Door1	Door Locked	
Unlock	2016-12-16 13:4...	Door1	Unlock	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	

Шаги

1. Все тревоги контроля доступа будут отображаться в списке в режиме реального времени. Можно просмотреть тип тревоги, время тревоги, местоположение и т. д.
2. Нажмите , чтобы просмотреть тревогу на электронной карте.
3. При возникновении тревожного события нажмите или для просмотра сцены в режиме реального времени или просмотра захваченного изображения.
   Примечание. Подробная информация о срабатывании камеры представлена в *разделе 7.10.1 Привязка событий контроля доступа*.
4. Нажмите **Subscribe** («Подписаться»), чтобы выбрать тревогу, которую клиент может получить при возникновении тревожного события.



1) Выберите тревоги, включая тревогу исключения устройства, тревогу двери, тревогу считывателя карт и тревожный вход.
2) Нажмите **OK** для сохранения настроек.

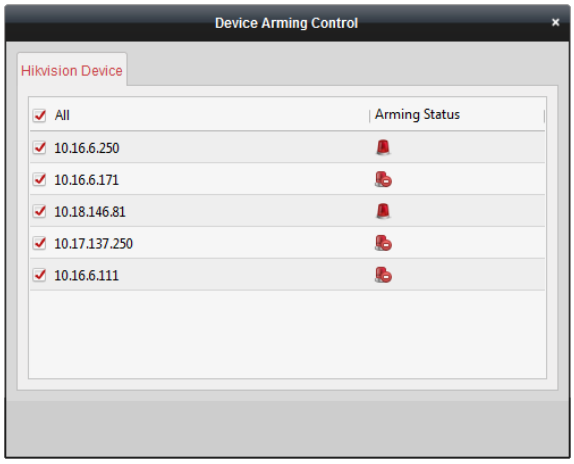
7.12 Управление постановкой на охрану

Цель

Включите постановку на охрану или снятие устройства с охраны. После постановки устройства на охрану клиент может получать информацию о тревоге с устройства.

Шаги

1. Нажмите **Tool → Device Arming Control** («Инструменты → Управление постановкой на охрану»), чтобы открыть соответствующий интерфейс.
2. Чтобы поставить устройство на охрану, нажмите соответствующее поле.
   При возникновении тревожной ситуации информация о тревоге будет автоматически загружена в клиентское ПО.



Приложение А Голосовые предупреждения и индикаторы

После включения считывателя карт LED-индикатор загорится синим и замигает 1 раз. Затем он загорится красным и замигает 3 раза. Затем появится звуковой сигнал бипера, указывающий, что процесс запуска завершен.

При использовании считывателя карт, вы услышите разные звуковые предупреждения, а LED-индикатор будет указывать на различные состояния. Более подробная информация представлена в таблицах далее.

Таблица 1 Описание звуковых оповещений

Голосовое предупреждение	Описание
Один звуковой сигнал	Протокол RS-485: Оповещение нажатия клавиш; сканирования карты; истечения времени для нажатия клавиш или считывания карты. Протокол Wiegand: Уведомление нажатия клавиш; сканирования карты
Два коротких звуковых сигнала	Действие нажатия клавиш или считывания карты допустимо.
Три длинных звуковых сигнала	Действие нажатия клавиш или считывания карты недопустимо.
Короткие повторяющиеся звуковые сигналы	Тревожный сигнал датчика контроля вскрытия.
Длинные продолжительные сигналы	Данные считывателя карт не зашифрованы.

Таблица 2 Описание LED-индикаторов

Состояние LED-индикатора	Описание
Зеленый, мигает	Считыватель карт работает в стандартном режиме.
Горит зеленым	Действие нажатия клавиш или считывания карты допустимо.
Горит красным	Действие нажатия клавиш или считывания карты недопустимо.
Красный, мигает	Протокол RS-485: сбой регистрации или считыватель карт находится в режиме офлайн. Сбой получения ключевых файлов PSAM-карты; сбой обнаружения PSAM-карты.
Красный, быстро мигает	Доступно для чтения файлов в режиме CPU-карты: PSAM-карта не введена или не обнаружена.

Приложение Б Правила Wiegand

В качестве примера используйте Wiegand 44 со следующими значениями настроенных параметров Custom Wiegand («Настраиваемый Wiegand»):

Имя настраиваемого Wiegand:	Wiegand 44				
Общая длина	44				
Правило преобразования (десятичный знак)	По правилу формата [4]=[1][4][0][0]				
Режим четности	Четность XOR				
Старт-бит контроля нечетности		Длина			
Старт бит контроля четности		Длина			
Старт-бит четности XOR	0	Длина каждой группы	4	Общая длина	40
Старт-бит ID-карты	0	Длина	32	Десятичный знак	10
Старт-бит кода объекта		Длина		Десятичный знак	
Старт-бит OEM		Длина		Десятичный знак	
Старт-бит кода производителя	32	Длина	8	Десятичный знак	3

Данные Wiegand = действительные данные + данные четности

Общая длина

Длина данных Wiegand.

Правило комбинации 4 байтов

Будут отображены комбинированные типы допустимых данных. В примере отображается комбинация идентификатора карты и кода производителя. Допустимые данные могут быть одним правилом или комбинацией нескольких правил.

Режим четности

Действительный паритет для данных Wiegand. Выберите четные или нечетные данные.

Старт-бит контроля нечетности и длина

Если выбрать Odd Parity («Контроль нечетности»), данные элементы будут доступны.
Если старт-бит контроля нечетности равен 1, а длина равна 12, тогда система начнет расчет проверки нечетности с бита 1. Она посчитает 12 битов. Результат будет в бите 0.
(Бит 0 – первый бит).

Старт-бит контроля четности и длина

Если выбрать Even Parity («Контроль на четность»), данные элементы будут доступны.
Если старт-бит контроля четности равен 12, а длина равна 12, система начнет расчет проверки четности с бита 12. Она посчитает 12 битов. Результат будет в стоп-бите.

Четность XOR, длина каждой группы, длина четности

Если выбрать XOR Parity («Четность XOR»), данные элементы будут доступны. Основываясь на таблице выше, старт-бит равен 0, длина каждой группы равна 4, а длина четности равна 40.

Это означает, что система выполнит расчет каждого 4 бита, начиная с бита 0, что в итоге даст 40 битов (10 групп). Результат будет в последних 4 битах. (Итоговая длина аналогична длине каждой группы).

Старт-бит ID-карты, длина и десятичный знак
Данные параметры доступны при использовании правила преобразования. Основываясь на таблице выше, старт-бит ID-карты равен 0, длина равна 32 и десятичный знак равен 10. Это означает, что, начиная с бита 0, 32 бита представляют собой ID-карту. (Здесь длина рассчитана по биту). А длина десятичного знака равна 10 битов.

Старт-бит кода объекта, длина и десятичный знак
Данные параметры доступны при использовании правила преобразования. Подробная информация представлена в описании ID-карты.

Старт-бит OEM, длина и десятичный знак
Данные параметры доступны при использовании правила преобразования. Подробная информация представлена в описании ID-карты.

Старт-бит кода производителя, длина и десятичный знак
Данные параметры доступны при использовании правила преобразования. Основываясь на таблице выше, старт-бит кода производителя равен 32, длина равна 8 и десятичный знак равен 3. Это означает, что, начиная с бита 32, 8 битов представляют собой код производителя. (Здесь длина рассчитана по биту). А длина десятичного знака равна 3.

020000001080620

See Far, Go Further

RU05668B-D