



Контроллер доступа серии F-KD-13X1

Руководство пользователя

Правовая информация

Информация о документе

- Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначена только для ознакомления.
- Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. При использовании данного документа обращайтесь за помощью к профессионалам, обученным работе с продуктом.

О продукте

- Послепродажное обслуживание данного продукта возможно только в той стране или регионе, где была совершена покупка.
- Если выбранный вами продукт является видеопродуктом, сканируйте QR-код, чтобы ознакомиться с программой по использованию продукции видеомониторинга.

Признание прав интеллектуальной собственности

- iFLOW владеет авторскими правами и/или патентами, связанными с технологиями, реализуемыми в продукции и описанными в данном документе, которые могут включать лицензии, полученные от третьих лиц.
- Любая часть документа, включая текст, изображения, графику и т. д., принадлежит iFLOW. Никакая часть этого документа не может быть извлечена, скопирована, переведена или изменена полностью или частично любыми способами без письменного разрешения.
- Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Доступные модели

Наименование продукта	Модель
Контроллер доступа	F-KD-1311
	F-KD-1321
	F-KD-1341

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 В, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить достаточную 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

Данное оборудование следует устанавливать и использовать на расстоянии не менее 20 см между источником излучения и пользователем.

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. Устройство должно выдерживать возможные излучения, включая и 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 2014/30/EC EMC, директивой 2014/53/EC RE, директивой 2011/65/EC RoHS



2012/19/ЕС (директива WEEE): продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей утилизации верните продукт поставщику при покупке эквивалентного нового оборудования, либо избавьтесь от него в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info



2006/66/ЕС (директива о батареях): данный продукт содержит батарею, 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 или утилизируйте ее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу :www.recyclethis.info

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».

Предупреждение: игнорирование любого из предупреждений может привести к серьезным травмам или смерти.

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

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

Предупреждение:

- 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.
- Избегайте проглатывания батареи, существует опасность химического ожога. Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.

Храните новые и использованные батареи в недоступном для детей месте. Если отсек для батареи закрывается ненадежно, прекратите использование продукта и храните его в недоступном для детей месте. В случае проглатывания батареи или ее перемещения в какую-либо часть тела, немедленно обратитесь за медицинской помощью.

- 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.)

 Предостережение:

- Запрещено ронять устройство и подвергать 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.
- 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 Профилактические меры и предостерегающие рекомендации	1
Раздел 2 Описание устройства	2
Раздел 3 Описание основной платы управления	3
3.1 Описание основной платы управления контроллера доступа для одной двери	3
3.2 Описание основной платы управления контроллера доступа для двух дверей	4
3.2.1 Описание основной платы управления контроллера доступа для четырех дверей	5
3.3 Описание компонента	7
3.4 Плата зарядки батареи	8
Раздел 4 Описание разъемов	9
4.1 Описание разъемов контроллера доступа для одной двери	9
4.2 Описание разъемов контроллера доступа для двух дверей	12
4.3 Описание разъемов контроллера доступа для четырех дверей	15
Раздел 5 Установка	18
5.1 Установка на стену	18
Раздел 6 Подключение	20
6.1 Подключение основной платы	20
6.2 Подключение считывателя карт Wiegand	22
6.3 Подключение считывателя карт RS-485	23
6.4 Подключение катодного замка	24
6.5 Подключение анодного замка	24
6.6 Подключение тревожного выхода	25
6.7 Подключение кнопки выхода	25
6.8 Подключение дверного контакта	26
6.9 Подключение питания	27
Раздел 7 Настройки	28
7.1 Инициализация устройства (вариант 1)	28

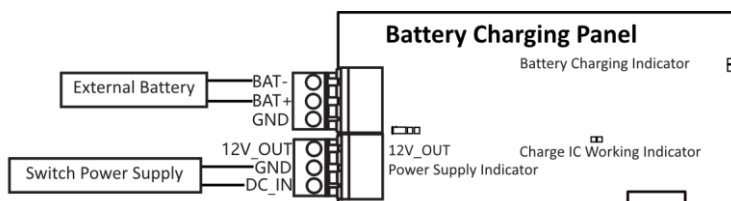
7.2 Инициализация устройства (вариант 2).....	28
7.3 Настройки релейного выхода NO/NC	29
7.3.1 Настройки релейного выхода замка	29
7.3.2 Настройки тревожного релейного выхода	30
Раздел 8 Активация.....	32
8.1 Активация через SADP	32
8.2 Активация устройства через клиентское ПО	33
Раздел 9 Настройка клиентского ПО.....	35
9.1 Схема настройки клиентского ПО	35
9.2 Управление устройством	36
9.2.1 Добавление устройства	36
9.2.2 Сброс пароля устройства	40
9.2.3 Управление добавленными устройствами	41
9.3 Управление группами	42
9.3.1 Добавление группы	42
9.3.2 Добавление ресурсов в группу.....	43
9.4 Управление сотрудниками / посетителями	43
9.4.1 Добавление организации.....	43
9.4.2 Импорт и экспорт информации о сотруднике / посетителе	44
9.4.3 Получение информации о пользователе с устройства контроля доступа	47
9.4.4 Выдача карт сотрудникам в пакетном режиме	48
9.4.5 Сообщить о потере карты.....	48
9.4.6 Настройка параметров выпуска карт	49
9.5 Настройка графиков и шаблонов.....	50
9.5.1 Добавление выходного дня	50
9.5.2 Добавление шаблона	51
9.6 Настройка группы контроля доступа для назначения разрешений на доступ	53
9.7 Настройка расширенных функций.....	54

9.7.1 Настройка оставить заблокированной / разблокированной	54
9.7.2 Настройка запрета двойного прохода	56
9.7.3 Настройка блокировки нескольких дверей	57
9.7.4 Настройка аутентификации в качестве первого пользователя	57
9.7.5 Настройка многофакторной аутентификации	59
9.7.6 Настройка аутентификации при помощи считывателя карт	61
9.7.7 Настройка параметров устройства	63
9.7.8 Настройка параметров устройства	67
9.8 Управление состоянием двери	68
9.8.1 Управление состоянием двери	68
9.8.2 Проверка записей о считывании карт в режиме реального времени	69
Приложение А. Рекомендации по сканированию отпечатков пальцев	71
Приложение В. Описание DIP-переключателей	73
Приложение С. Пользовательская настройка Wiegand	74
Приложение D. Коммуникационная матрица и команды устройства	Error! Bookmark not defined.

Раздел 1 Профилактические меры и предостерегающие рекомендации

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.
- Рекомендуется выбирать свинцово-кислотную батарею с напряжением 12 В, 7 А·ч, соответствующую стандарту IEC 60896. Способ подключения батареи показан на следующем изображении.



Раздел 2 Описание устройства

- Оснащен 32-битным высокоскоростным процессором.
- Поддержка TCP / IP. Специальное шифрование данных связи для предотвращения утечки конфиденциальной информации
- Поддержка распознавания и хранения номера карт с максимальной длиной 20 символов.
- Поддержка до 10 000 карт и 50 000 записей выдачи карт
- Поддержка функций: блокировка нескольких дверей, запрет двойного прохода, множественная аутентификация, открытие двери первой картой, суперпароль, шифрование M1-карты, онлайн обновление и дистанционное управление дверьми
- Обнаружение конфликта IP-адресов
- Поддержка RS-485 и интерфейса Wiegand для доступа к считывателю карт. Интерфейс Wiegand поддерживает W26, W34 и совместим со сторонним считывателем карт с интерфейсом Wiegand
- Устройство оснащено различными индикаторами для отображения различных состояний
- Поддержка функции хранения записей, когда устройство находится офлайн, и функции тревоги при недостаточном пространстве для хранения
- После выключения контроллера доступа данные хранятся бессрочно
- Поддержка привязки входа / выхода и привязки событий

Раздел 3 Описание основной платы управления

3.1 Описание основной платы управления контроллера доступа для одной двери

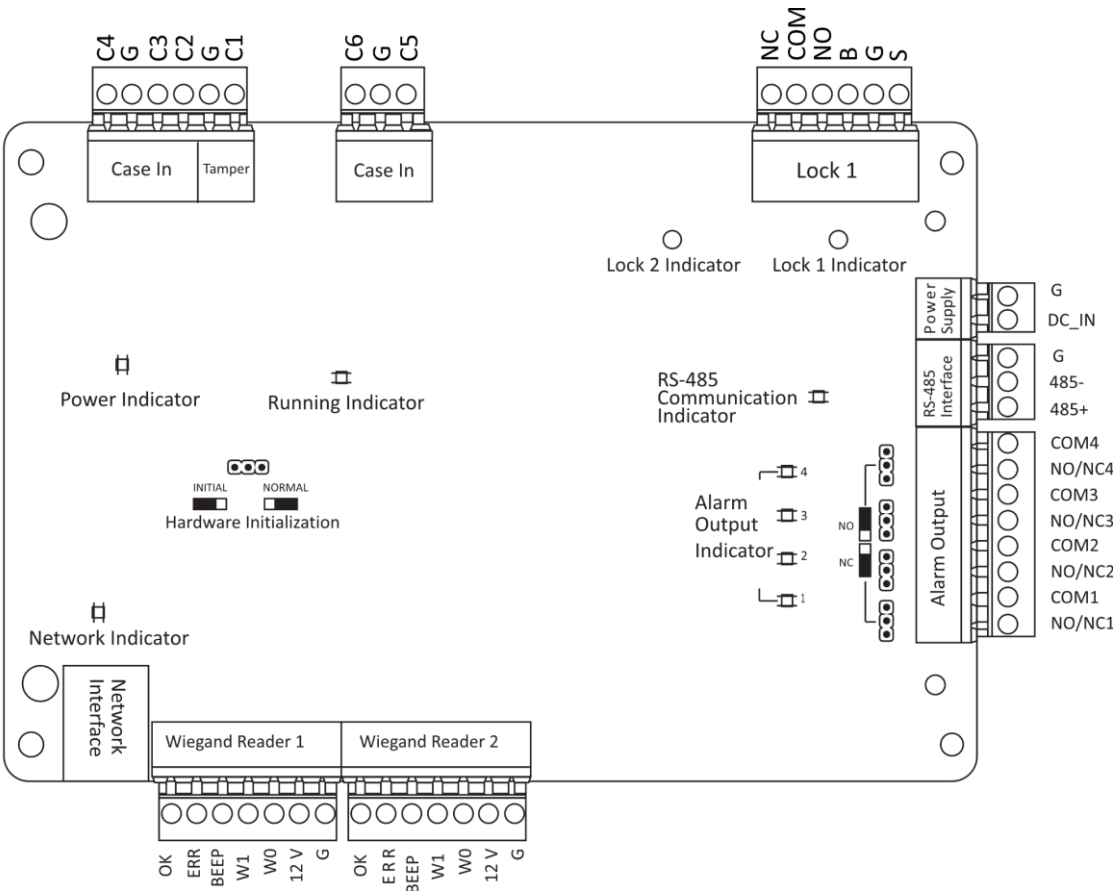


Рисунок 3-1. Основная плата управления контроллера доступа на 1 дверь

Английский язык	Русский язык
Wiegand Reader	Считыватель с Wiegand
Lock	Замок
Lock Indicator	Индикатор замка
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
RS-485 Interface	Интерфейс RS-485
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Indicator	Сетевой индикатор
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Running Indicator	Индикатор режима работы
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
Hardware initialization	Инициализация оборудования

3.2 Описание основной платы управления контроллера доступа для двух дверей

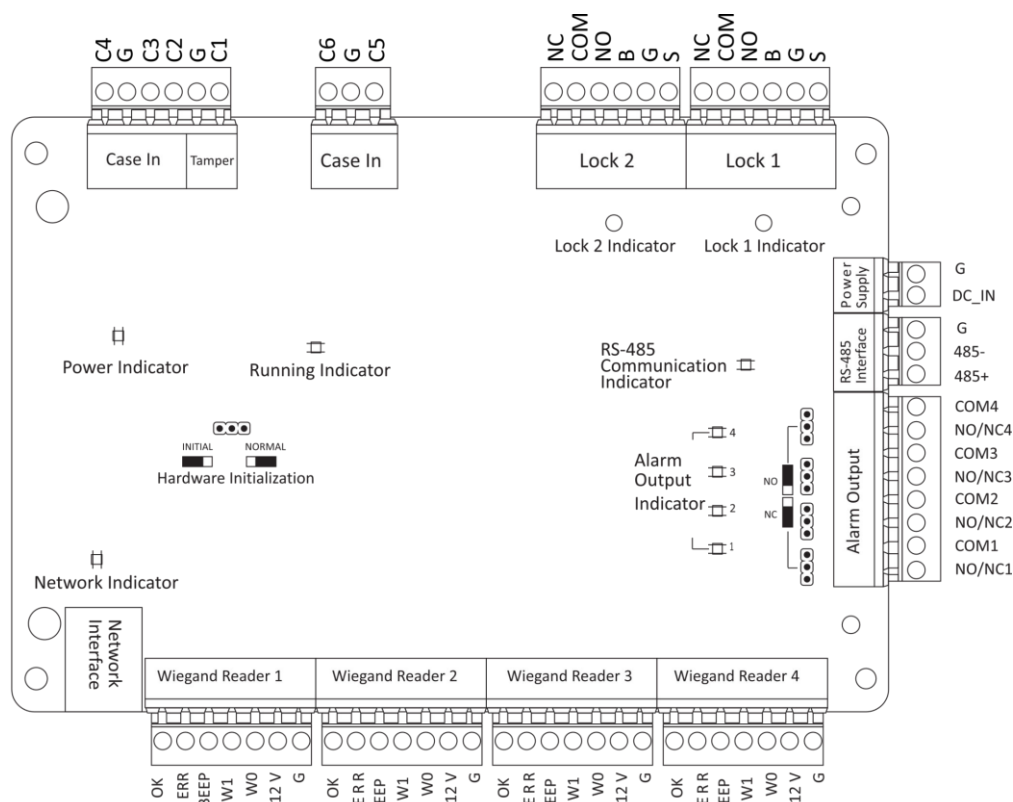


Рисунок 3-2. Основная плата управления контроллера доступа на 2 двери

Английский язык	Русский язык
Wiegand Reader	Считыватель с Wiegand
Lock	Замок
Lock Indicator	Индикатор замка
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
RS-485 Interface	Интерфейс RS-485
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Indicator	Сетевой индикатор
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Running Indicator	Индикатор режима работы
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
Hardware initialization	Инициализация оборудования

3.2.1 Описание основной платы управления контроллера доступа для четырех дверей

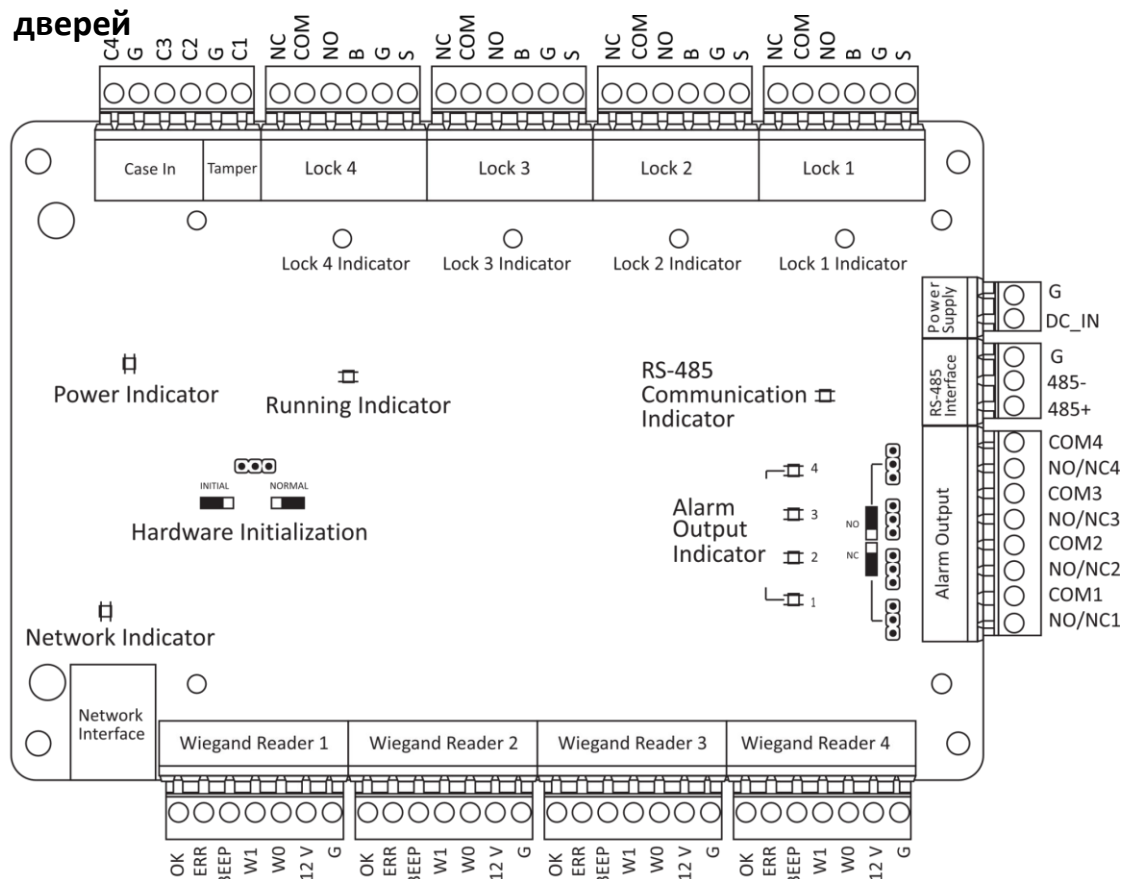


Рисунок 3-3. Основная плата управления контроллера доступа на 4 двери

Английский язык	Русский язык
Wiegand Reader	Считыватель с Wiegand
Lock	Замок
Lock Indicator	Индикатор замка
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
RS-485 Interface	Интерфейс RS-485
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Indicator	Сетевой индикатор
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Running Indicator	Индикатор режима работы
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
Hardware initialization	Инициализация оборудования

3.3 Описание компонента

В данном документе представлены компоненты устройства с описаниями.
В качестве примера далее представлена схема компонентов контроллера доступа на 4 двери.

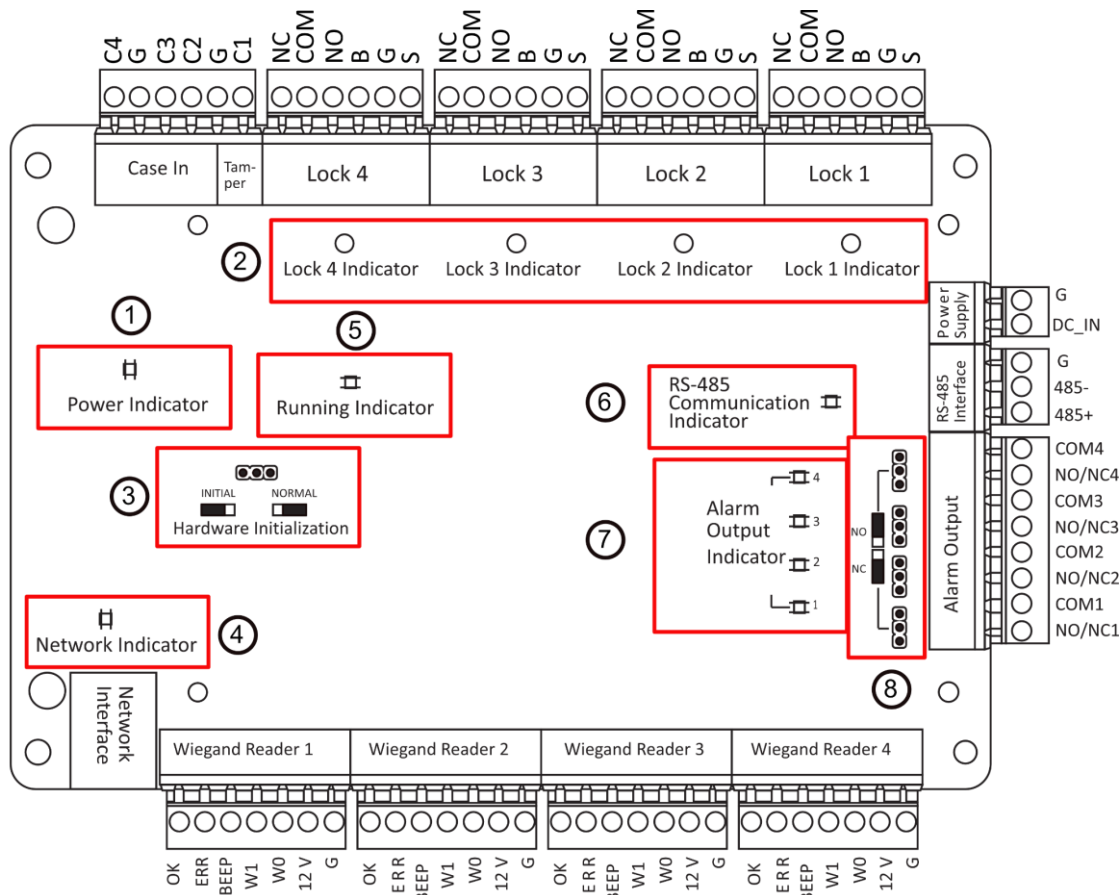


Рисунок 3-4. Схема компонентов контроллера доступа на 4 двери

Таблица 3-1. Описание компонентов контроллера доступа на 4 двери

№	Описание компонента
1	Индикатор питания
2	Индикатор замка
3	Инициализация оборудования и выбор стандартного режима работы
4	Индикатор сети
5	Индикатор режима работы
6	Индикатор связи RS-485
7	Индикатор тревожного выхода
8	Выбор состояния тревожного релейного выхода (NC / NO)

3.4 Плата зарядки батареи

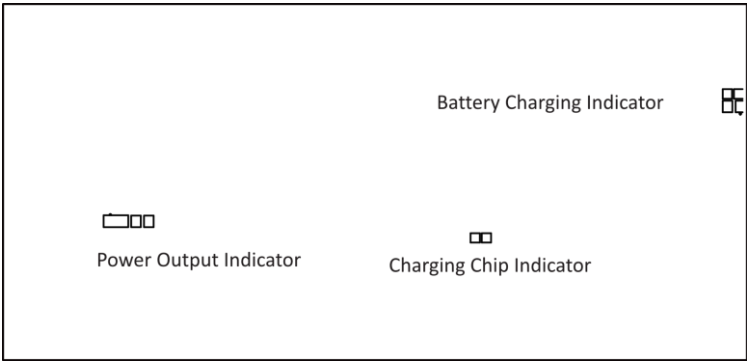


Рисунок 3-5 Плата зарядки батареи

Английский язык	Русский язык
Power Output Indicator	Индикатор выхода питания
Charging Chip Indicator	Индикатор зарядного чипа
Battery Charging Indicator	Индикатор зарядки батареи



Примечание

Платы для зарядки батареи предназначены только для устройств, поддерживающих батареи.

Раздел 4 Описание разъемов

4.1 Описание разъемов контроллера доступа для одной двери

Далее представлено описание разъемов контроллера доступа на 1 дверь.

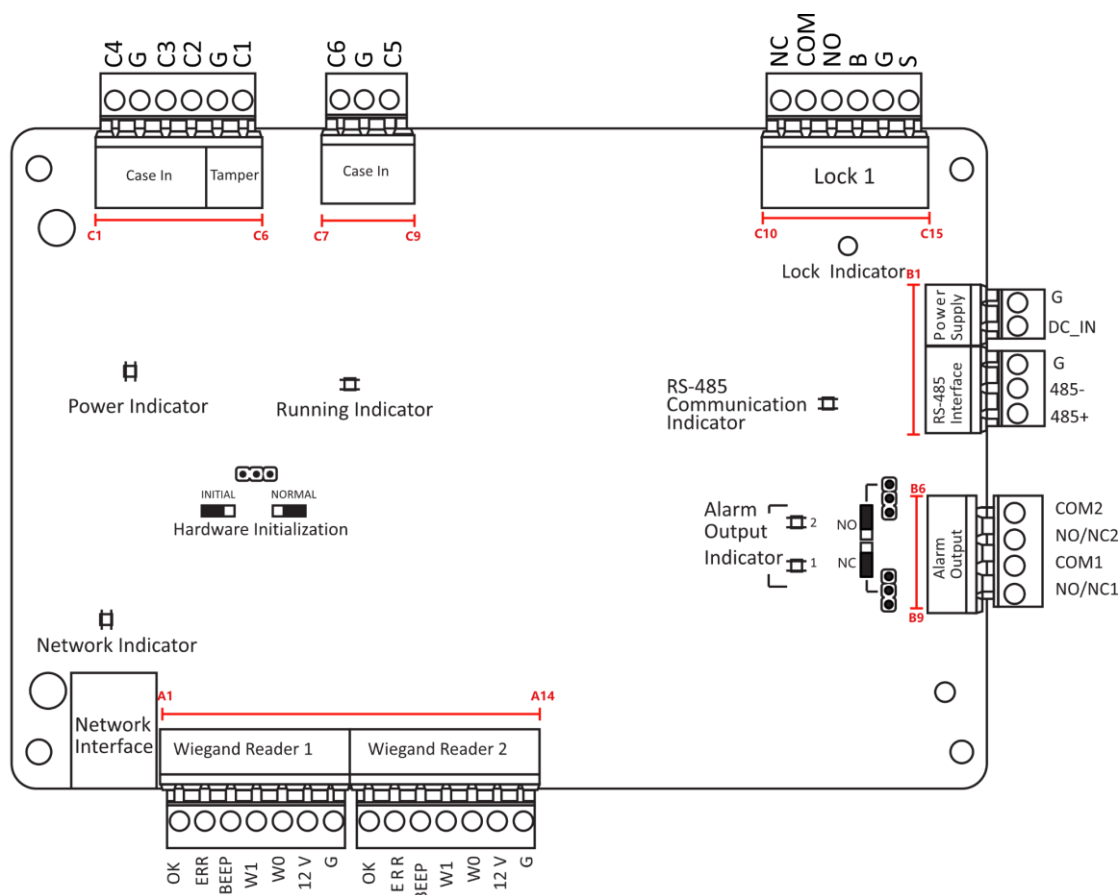


Рисунок 4-1. Основная плата управления контроллера доступа на 1 дверь

Таблица 4-1. Описание разъемов контроллера доступа на 1 дверь

№	Контроллер доступа на 4 двери		
A1~A28	Считыватель с Wiegand 1~4	OK	Индикатор управления выводом считывателя карт (прием карты)
		ERR	Индикатор управления выводом считывателя карт (отказ карты)
		BEEP	Вывод управления бипером считывателя карт
		W1	Интерфейс чтения входных данных Wiegand 1
		W0	Интерфейс чтения входных данных Wiegand 0
		+12 В	Интерфейс чтения входных данных Wiegand 0
		G	Заземление
B1	Питание	G	Заземление
B2		DC_IN	Вход питания
B3	RS-485	G	Заземление
B4		485-	Считыватель карт 485-
B5		485+	Считыватель карт 485+
B6~B13	Тревожный выход	COM4	Тревожный релейный выход 4 (сухой контакт)
		NO / NC4	
		COM3	Тревожный релейный выход 3 (сухой контакт)
		NO / NC3	
		COM2	Тревожный релейный выход 2 (сухой контакт)
		NO / NC2	
		COM1	Тревожный релейный выход 1 (сухой контакт)
		NO / NC1	
C1	Вход события	C4	Вход события 4
C2		G	Заземление

№	Контроллер доступа на 4 двери		
C3		C3	Вход события 3
C4	Детектор саботажа	C2	Зарезервировано
C5		G	Заземление
C6		C1	Детектор саботажа
C7	Вход события	C6	Вход события 6
C8		G	Заземление
C9		C5	Вход события 5
C10~C15	Замок 1	NC	Релейный выход блокировки (сухой контакт)
		COM	
		NO	
		B	Вход кнопки выхода
		G	Заземление
		S	Дверной контакт



Примечание

- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 2. В приведенной ниже таблице показана связь номера двери и идентификатора.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход

- Для контроллера доступа на 1 дверь связь между считывателем карт Wiegand и дверью по умолчанию следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	2	Выход

4.2 Описание разъемов контроллера доступа для двух дверей

Далее представлено описание разъемов контроллера доступа на 2 двери.

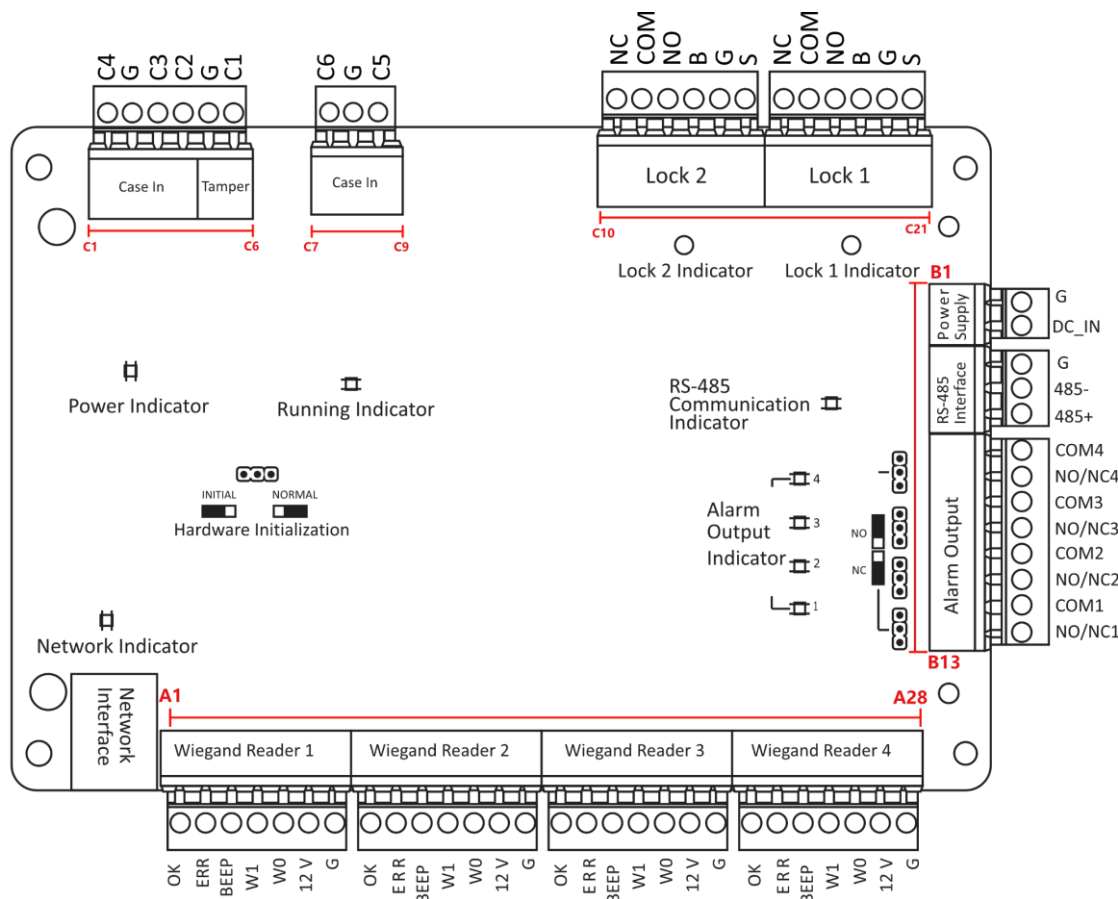


Рисунок 4-2. Основная плата контроллера доступа на 2 двери

Таблица 4-2. Описание разъемов контроллера доступа на 2 двери

№	Контроллер доступа на 4 двери		
A1~A28	Считыватель с Wiegand 1~4	OK	Индикатор управления выводом считывателя карт (прием карты)
		ERR	Индикатор управления выводом считывателя карт (отказ карты)
		BEEP	Вывод управления бипером считывателя карт
		W1	Интерфейс чтения входных данных Wiegand 1

№	Контроллер доступа на 4 двери		
		W0	Интерфейс чтения входных данных Wiegand 0
		+12 В	Интерфейс чтения входных данных Wiegand 0
		G	Заземление
B1	Питание	G	Заземление
B2		DC_IN	Вход питания
B3	RS-485	G	Заземление
B4		485-	Считыватель карт 485-
B5		485+	Считыватель карт 485+
B6~B13	Тревожный выход	COM4	Тревожный релейный выход 4 (сухой контакт)
		NO / NC4	
		COM3	Тревожный релейный выход 3 (сухой контакт)
		NO / NC3	
		COM2	Тревожный релейный выход 2 (сухой контакт)
		NO / NC2	
		COM1	Тревожный релейный выход 1 (сухой контакт)
		NO / NC1	
C1	Вход события	C4	Вход события 4
C2		G	Заземление
C3		C3	Вход события 3
C4	Детектор саботажа	C2	Зарезервировано
C5		G	Заземление
C6		C1	Детектор саботажа
C7	Вход события	C6	Вход события 6
C8		G	Заземление
C9		C5	Вход события 5
C10~C21	Замок 1 ~ замок 2	NC	Релейный выход блокировки (сухой контакт)
		COM	

№	Контроллер доступа на 4 двери		
		NO	
		B	Вход кнопки выхода
		G	Заземление
		S	Дверной контакт

 Примечание

- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 8.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход

- Для контроллера доступа на 2 двери связь между считывателем карт Wiegand и дверью по умолчанию следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход

4.3 Описание разъемов контроллера доступа для четырех дверей

Далее представлено описание разъемов контроллера доступа на 4 двери.

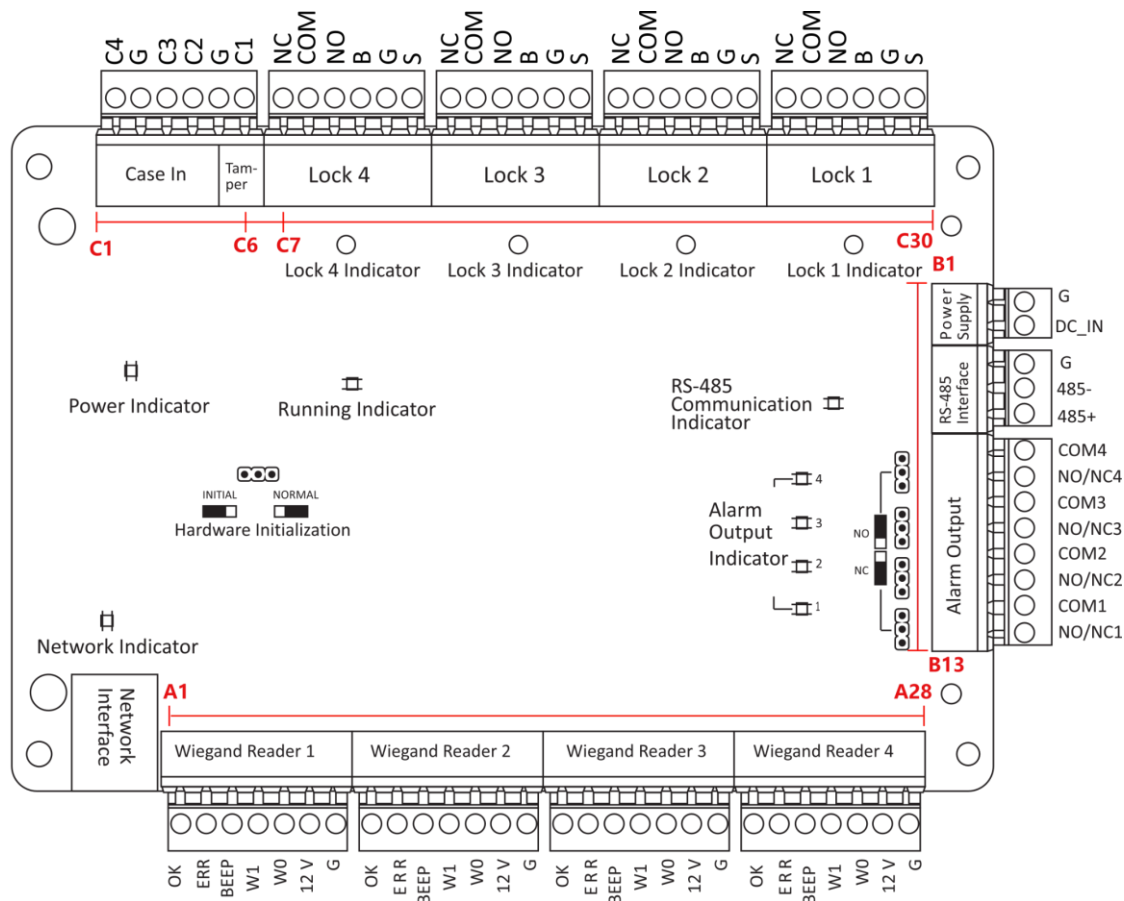


Рисунок 4-3. Основная плата управления контроллера доступа на 4 двери

Таблица 4-3. Описание разъемов контроллера доступа на 4 двери

№	Контроллер доступа на 4 двери		
A1~A28	Считыватель с Wiegand 1~4	OK	Индикатор управления выводом считывателя карт (прием карты)
		ERR	Индикатор управления выводом считывателя карт (отказ карты)
		BEEP	Вывод управления бипером считывателя карт
		W1	Интерфейс чтения входных данных Wiegand 1

№	Контроллер доступа на 4 двери		
		W0	Интерфейс чтения входных данных Wiegand 0
		+12 В	Интерфейс чтения входных данных Wiegand 0
		G	Заземление
B1	Питание	G	Заземление
B2		DC_IN	Вход питания
B3	RS-485	G	Заземление
B4		485-	Считыватель карт 485-
B5		485+	Считыватель карт 485+
B6~B13	Тревожный выход	COM4	Тревожный релейный выход 4 (сухой контакт)
		NO / NC4	
		COM3	Тревожный релейный выход 3 (сухой контакт)
		NO / NC3	
		COM2	Тревожный релейный выход 2 (сухой контакт)
		NO / NC2	
		COM1	Тревожный релейный выход 1 (сухой контакт)
		NO / NC1	
C1	Вход события	C4	Вход события 4
C2		G	Заземление
C3		C3	Вход события 3
C4	Детектор саботажа	C2	Зарезервировано
C5		G	Заземление
C6		C1	Детектор саботажа
C7~C30	Замок 1~4	NC	Релейный выход блокировки (сухой контакт)
		COM	
		NO	
		B	Вход кнопки выхода

№	Контроллер доступа на 4 двери		
		G	Заземление
		S	Дверной контакт



Примечание

- Идентификатор считывателя карт RS-485 должен быть в диапазоне от 1 до 8.

Номер двери	Идентификатор считывателя карт (RS-485)	Описание
Дверь 1	1	Вход
	2	Выход
Дверь 2	3	Вход
	4	Выход
Дверь 3	5	Вход
	6	Выход
Дверь 4	7	Вход
	8	Выход

- Для контроллера доступа на 4 двери связь между считывателем карт Wiegand и дверью по умолчанию следующая.

Номер двери	Считыватель карт Wiegand	Описание
Дверь 1	1	Вход
	/	Выход
Дверь 2	2	Вход
	/	Выход
Дверь 3	3	Вход
	/	Выход
Дверь 4	4	Вход
	/	Выход

Раздел 5 Установка

5.1 Установка на стену

Контроллер доступа можно устанавливать на стену.

Шаг 1

 Примечание

В процессе установки после прокладки кабеля через отверстие, само отверстие следует заделать огнестойким материалом или заглушкой класса V-1.

Откройте и снимите дверцу корпуса.

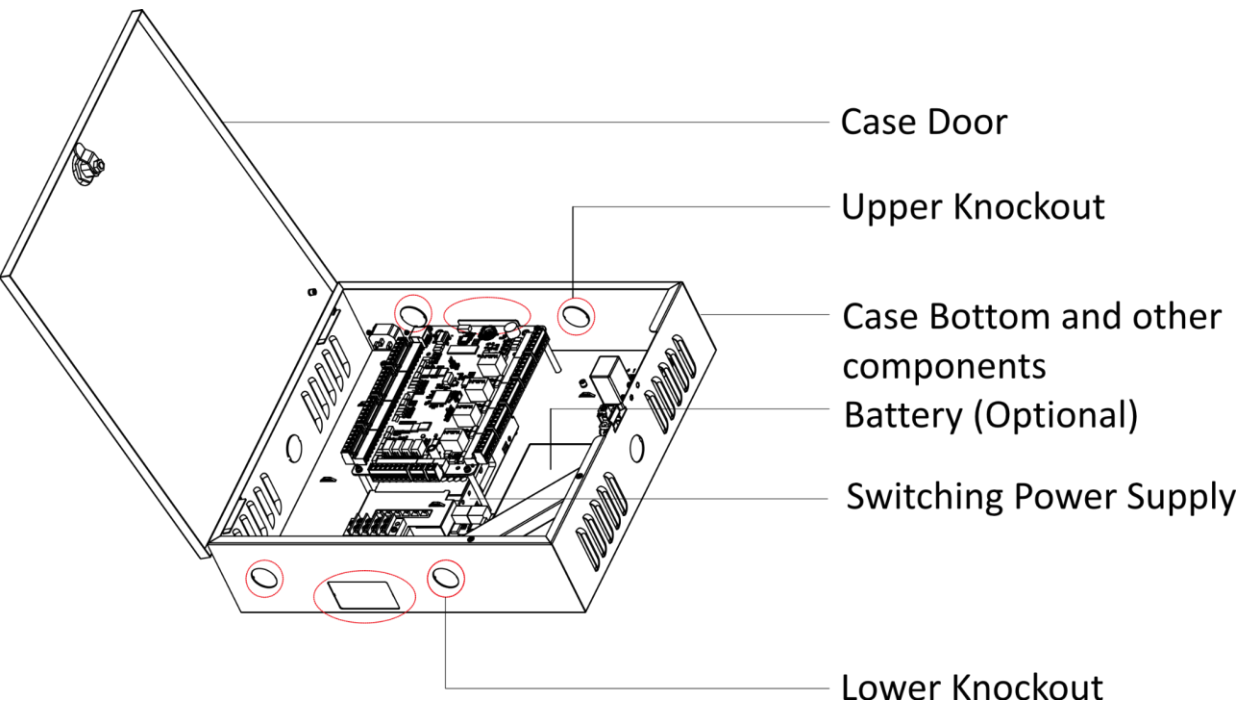


Рисунок 5-1 Откройте дверцу корпуса

Английский язык	Русский язык
Case door	Дверца корпуса
Upper knockout	Верхнее отверстие
Case bottom and other components	Корпус и другие компоненты
Battery (optional)	Батарея (опционально)
Switching power supply	Переключение питания
Lower knockout	Нижнее отверстие

2. Закрепите устройство на стене с помощью установочных винтов.

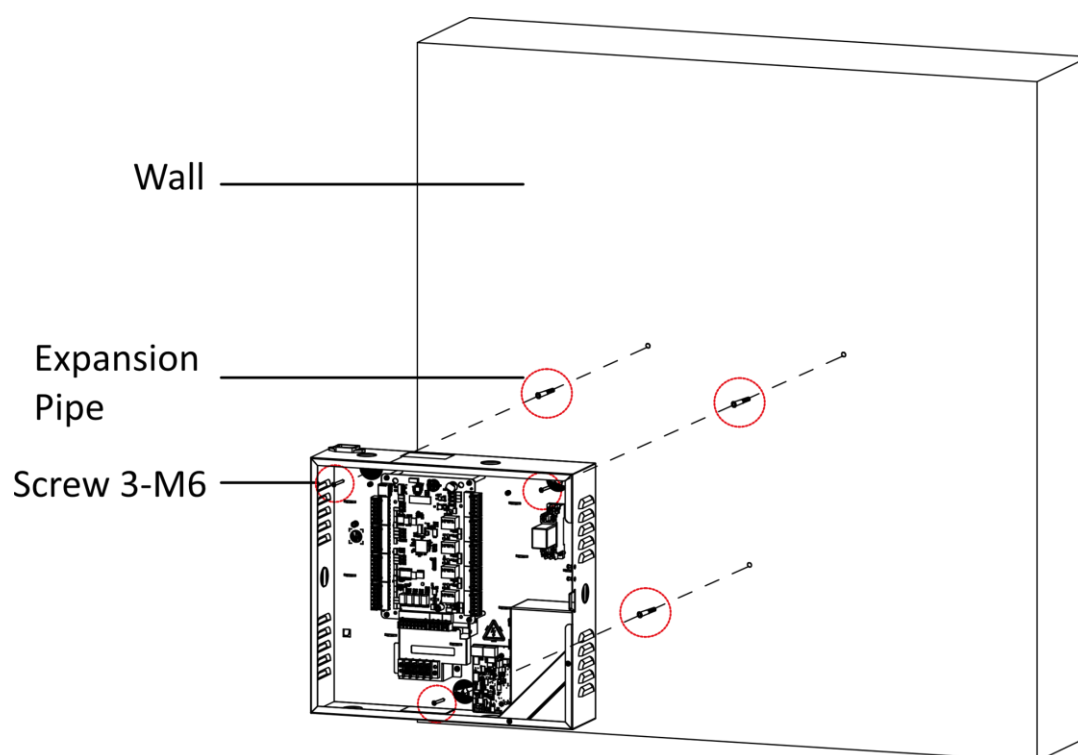


Рисунок 5-2 Фиксация устройства

Английский язык	Русский язык
Wall	Стена
Expansion pipe	Дюбель
Screw	Винт

- 3.** После подключения устройства установите дверцу и нижнюю панель корпуса.
При прокладке кабелей можно использовать нижние отверстия.

Раздел 6 Подключение

Описание подключения контроллера доступа.

6.1 Подключение основной платы

Ниже представлена схема подключения основной платы.

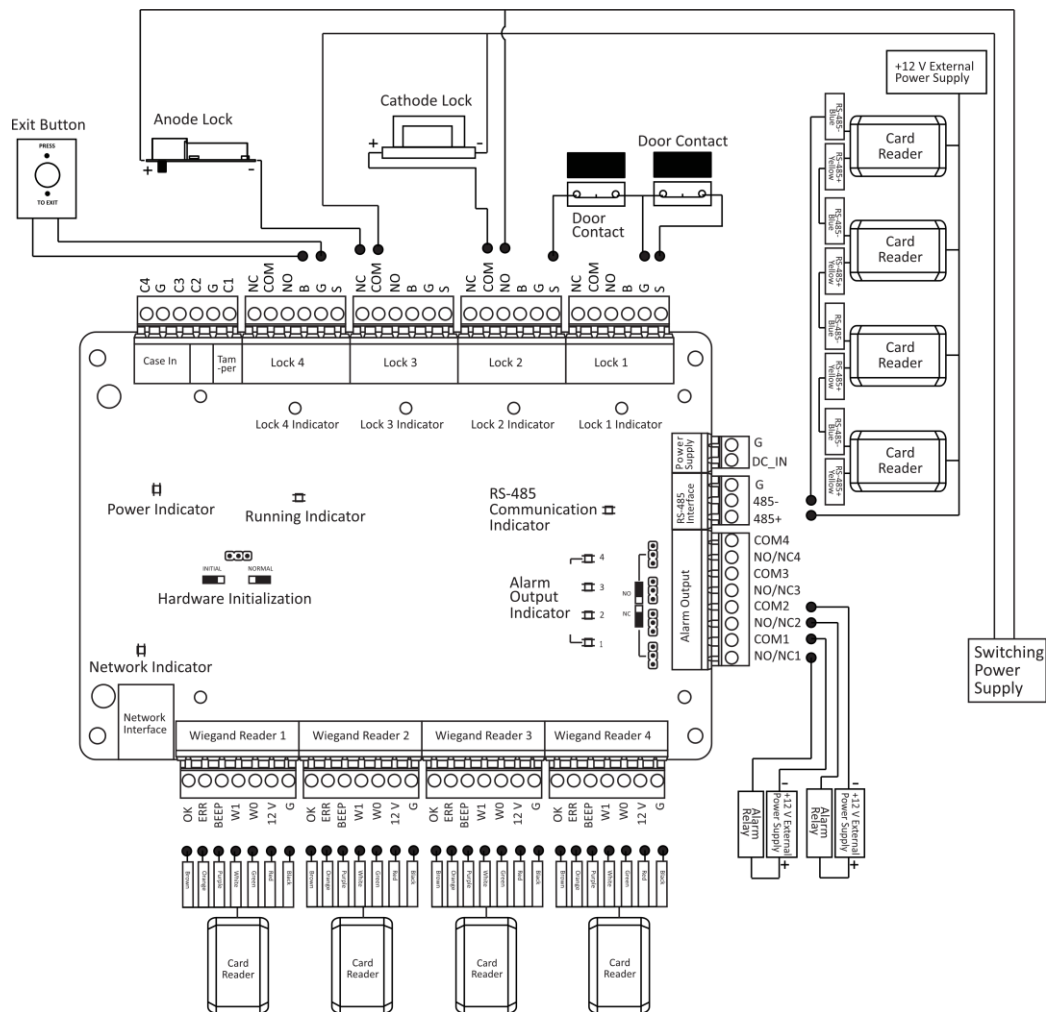


Рисунок 6-1 Подключение основной платы контроллера доступа

Английский язык	Русский язык
Exit button	Кнопка выхода
Anode lock	Анодный замок
Cathode lock	Катодный замок
Door contact	Дверной контакт
External power supply	Внешний источник питания
Card reader	Считыватель карт
Lock	Замок
Lock indicator	Индикатор замка
Wiegand Reader	Считыватель с Wiegand
Network Interface	Сетевой интерфейс
Alarm Output	Тревожный выход
RS-485 Interface	Интерфейс RS-485
Power Supply	Питание
NO	Нормально разомкнутый контакт
NC	Нормально замкнутый контакт
Network Indicator	Сетевой индикатор
RS-485 Communication Indicator	Индикатор связи RS-485
Power Indicator	Индикатор питания
Running Indicator	Индикатор режима работы
Normal	Нормальное положение
Initial	Исходное положение
Alarm Output Indicator	Индикатор тревожного выхода
Hardware initialization	Инициализация оборудования
Switching power supply	Переключение питания
Alarm relay	Реле тревоги

6.2 Подключение считывателя карт Wiegand

Далее представлена схема подключения считывателя карт Wiegand.

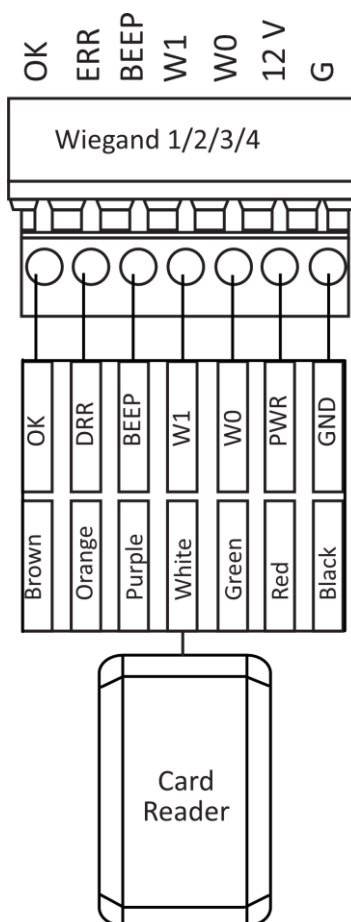


Рисунок 6-2 Схема подключения считывателя карт Wiegand



Примечание

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

6.3 Подключение считывателя карт RS-485

Далее представлена схема подключения считывателя карт RS-485.

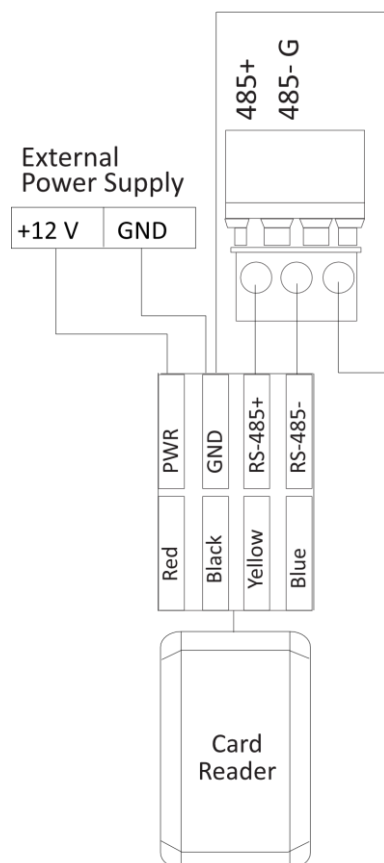


Рисунок 6-3 Схема подключения считывателя карт RS-485



Примечание

Если считыватель карт установлен слишком далеко от контроллера доступа, можно использовать внешний источник питания.

6.4 Подключение катодного замка

Далее представлена схема подключения катодного замка.

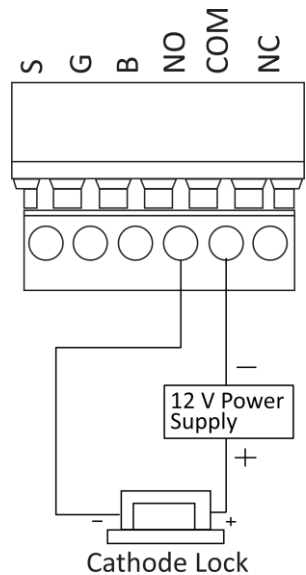


Рисунок 6-4 Схема подключения катодного замка

6.5 Подключение анодного замка

Далее представлена схема подключения анодного замка.

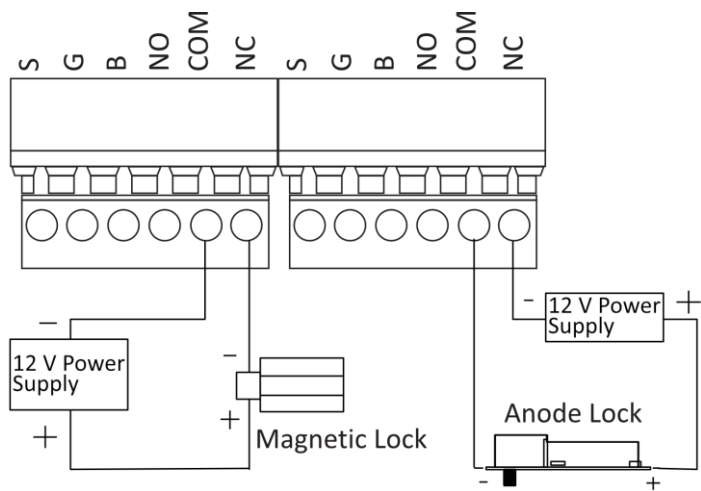


Рисунок 6-5 Схема подключения анодного замка

Английский язык	Русский язык
Anode lock	Анодный замок
Magnetic lock	Электромагнитный замок
Power Supply	Питание

6.6 Подключение тревожного выхода

Ниже представлена схема подключения тревожного выхода.

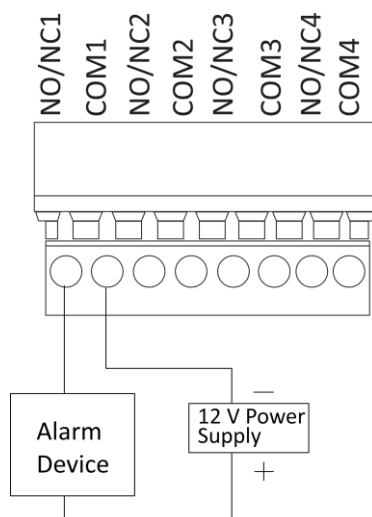


Рисунок 6-6 Подключение тревожного выхода

6.7 Подключение кнопки выхода

Далее представлена схема подключения кнопки выхода.

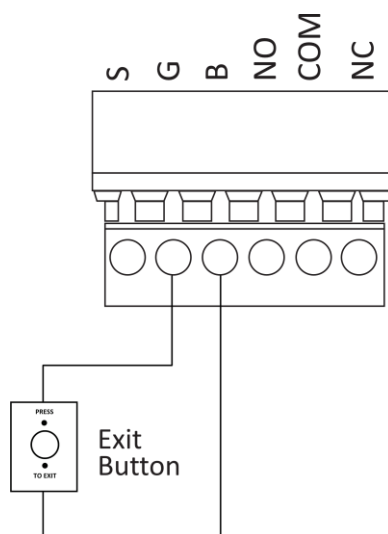


Рисунок 6-7 Подключение кнопки выхода

6.8 Подключение дверного контакта

Далее представлена схема подключения дверного контакта.

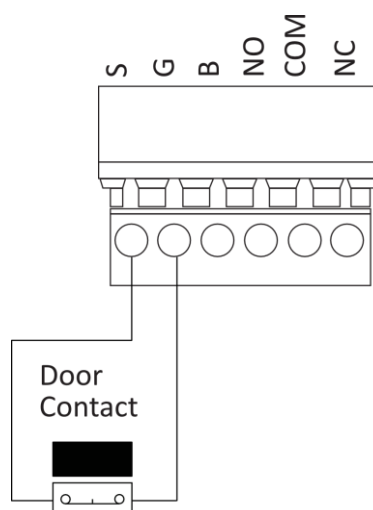


Рисунок 6-8 Подключение дверного контакта

6.9 Подключение питания

Далее представлена схема подключения источника питания.

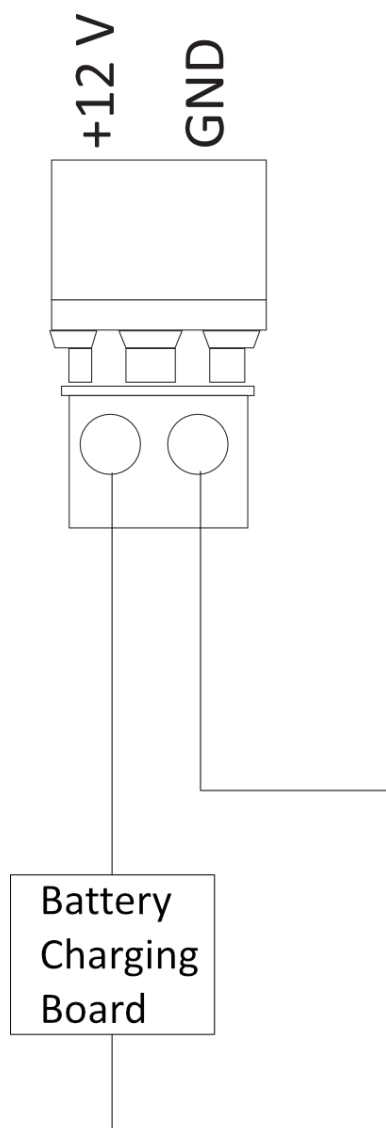


Рисунок 6-9 Подключение питания

Раздел 7 Настройки

7.1 Инициализация устройства (вариант 1)

Инициализацию устройства можно выполнить с помощью колпачковой переключки.

Шаги

1. Переведите колпачковую переключку 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 переключку обратно в положение **Normal** («Нормальное положение»).
4. Отключите питание и перезапустите контроллер доступа.

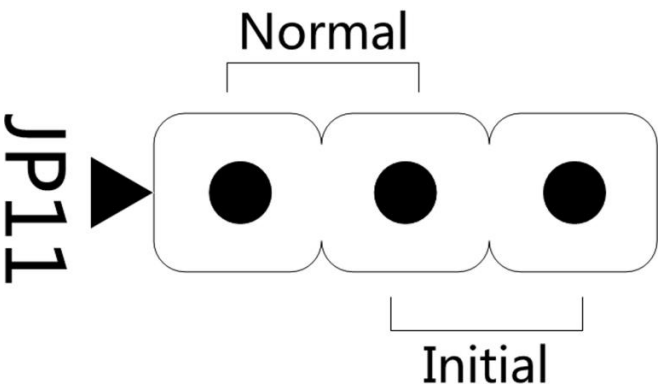


Рисунок 7-1 Колпачковая переключка контакта инициализации

Английский язык	Русский язык
Normal	Нормальное положение
Initial	Исходное положение



Примечание

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

7.2 Инициализация устройства (вариант 2)

Инициализацию устройства можно выполнить с помощью колпачковой переключки.

Шаги

1. Переместите колпачковую переключку 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 переключку обратно в положение **Normal** («Норма»).

4. Отключите питание и перезапустите контроллер доступа.

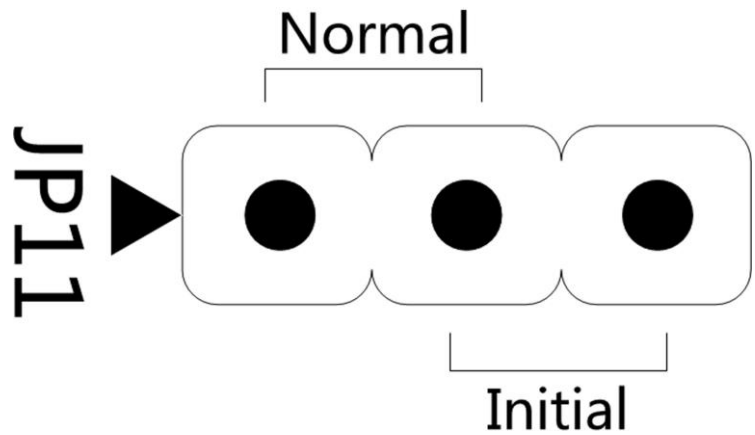


Рисунок 7-2 Колпачковая переключатель контакта инициализации

Английский язык	Русский язык
Normal	Нормальное положение
Initial	Исходное положение



Примечание

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

7.3 Настройки релейного выхода NO/NC

7.3.1 Настройки релейного выхода замка

Далее представлено состояние подключения релейного выхода замка (NO / NC).

Состояние подключения реле замка (NO)

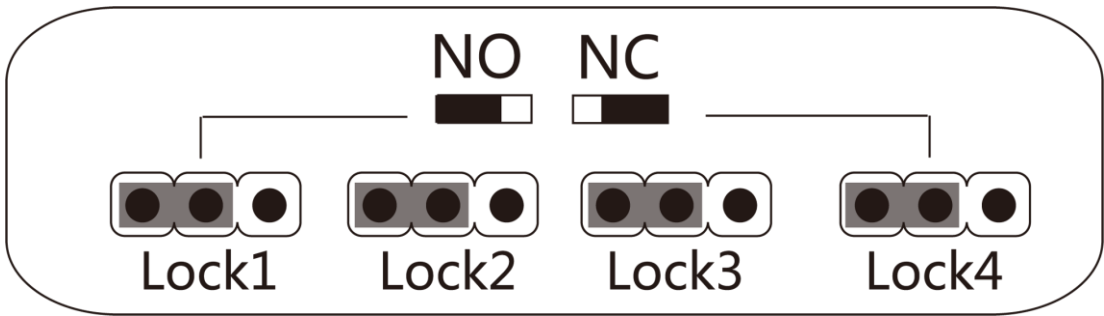


Рисунок 7-3 Состояние NO

Английский язык	Русский язык
Lock	Замок

Состояние подключения реле замка (NC)

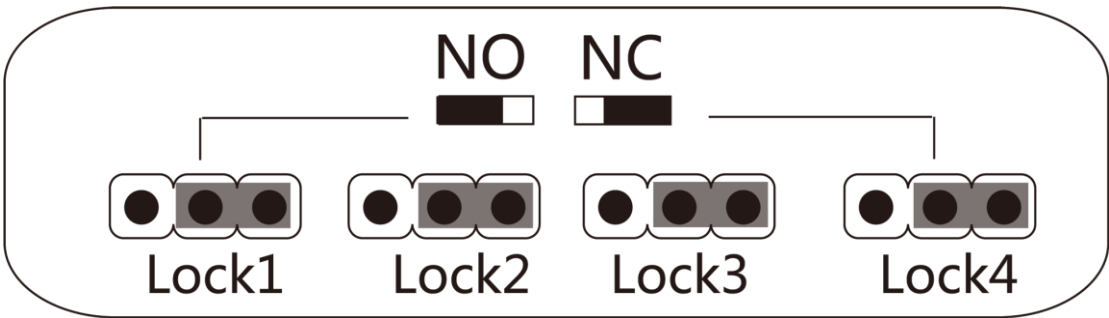


Рисунок 7-4 Состояние NC

Английский язык	Русский язык
Lock	Замок

7.3.2 Настройки тревожного релейного выхода

Далее представлено состояние подключения релейного выхода замка (NO / NC).

Состояние подключение тревожного релейного выхода (NO)

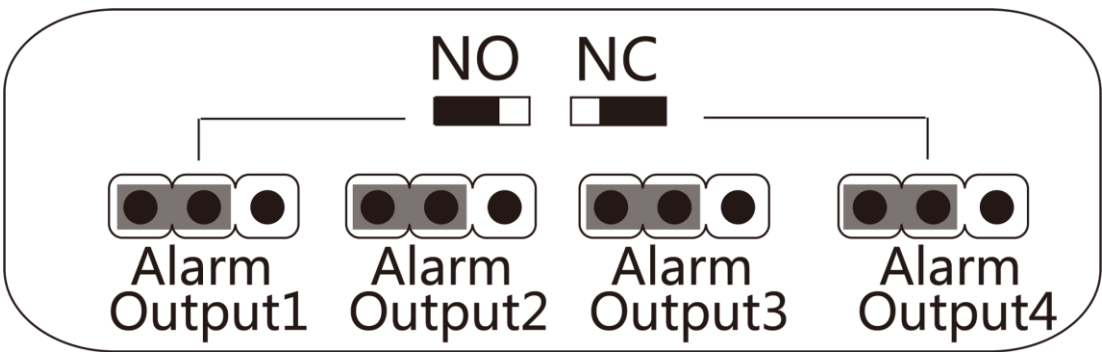


Рисунок 7-5 Состояние NO

Английский язык	Русский язык
Alarm Output	Тревожный выход

Состояние тревожного релейного выхода (NC)

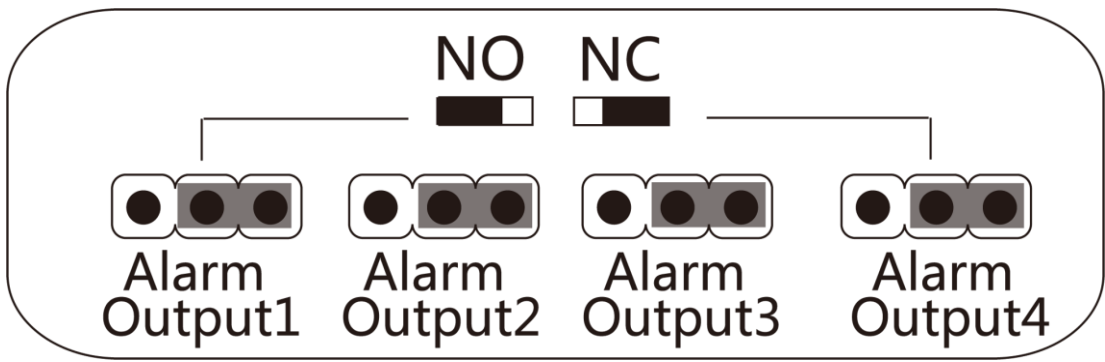


Рисунок 7-6 Состояние NC

Английский язык	Русский язык
Alarm Output	Тревожный выход

Раздел 8 Активация

Перед первым входом в систему необходимо активировать устройство. После включения устройства система переключится на страницу активации устройства.

Поддерживается активация через само устройство, активация при помощи ПО SADP и при помощи клиентского ПО. Значения по умолчанию для устройства следующие:

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

8.1 Активация через SADP

Программное обеспечение SADP — это инструмент для обнаружения, активации и изменения IP-адреса устройства через локальную сеть.

Перед началом

- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Для получения подробной информации о пакетной активации и изменении IP-адресов смотрите *Руководство пользователя ПО SADP*.

Шаги

1. Запустите ПО SADP для поиска онлайн устройств.
2. Найдите и выберите устройство в списке онлайн устройств.
3. Введите новый пароль (пароль администратора) и подтвердите его.



Предостережение

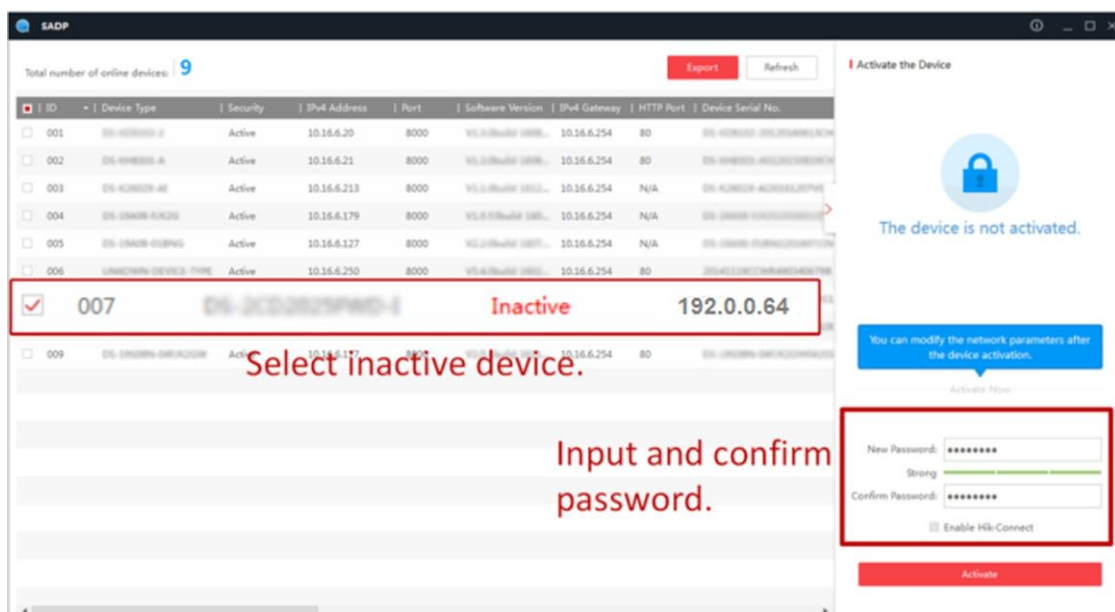
РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит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



Примечание

Символы содержащие admin и nimda не могут быть использованы для активации пароля.

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



После успешной активации статус устройства изменится на **Active** («Активно»).

5. Измените IP-адрес устройства.

- 1) Выберите устройство.
- 2) Измените IP-адрес устройства на адрес в той же подсети, к которой подключен компьютер вручную или поставив галочку **Enable DHCP** («Включить DHCP»).
- 3) Введите пароль администратора и нажмите **Modify** («Изменить») для изменения IP-адреса.

8.2 Активация устройства через клиентское ПО

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

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите  в правой части экрана на странице **Device Management** («Управление устройством») и выберите **Device** («Устройство»).
3. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств. Искомые онлайн устройства отобразятся в списке.
4. Проверьте состояние устройства (отображено в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.



Примечание

Символы содержащие admin и nimda не могут быть использованы для активации пароля.

7. Для активации устройства нажмите **ОК**.

Раздел 9 Настройка клиентского ПО

Можно позвонить на горячую линию, чтобы получить установочный пакет клиентского ПО iVMS-4200.

9.1 Схема настройки клиентского ПО

Следуйте приведенной ниже схеме для настройки клиентского ПО.

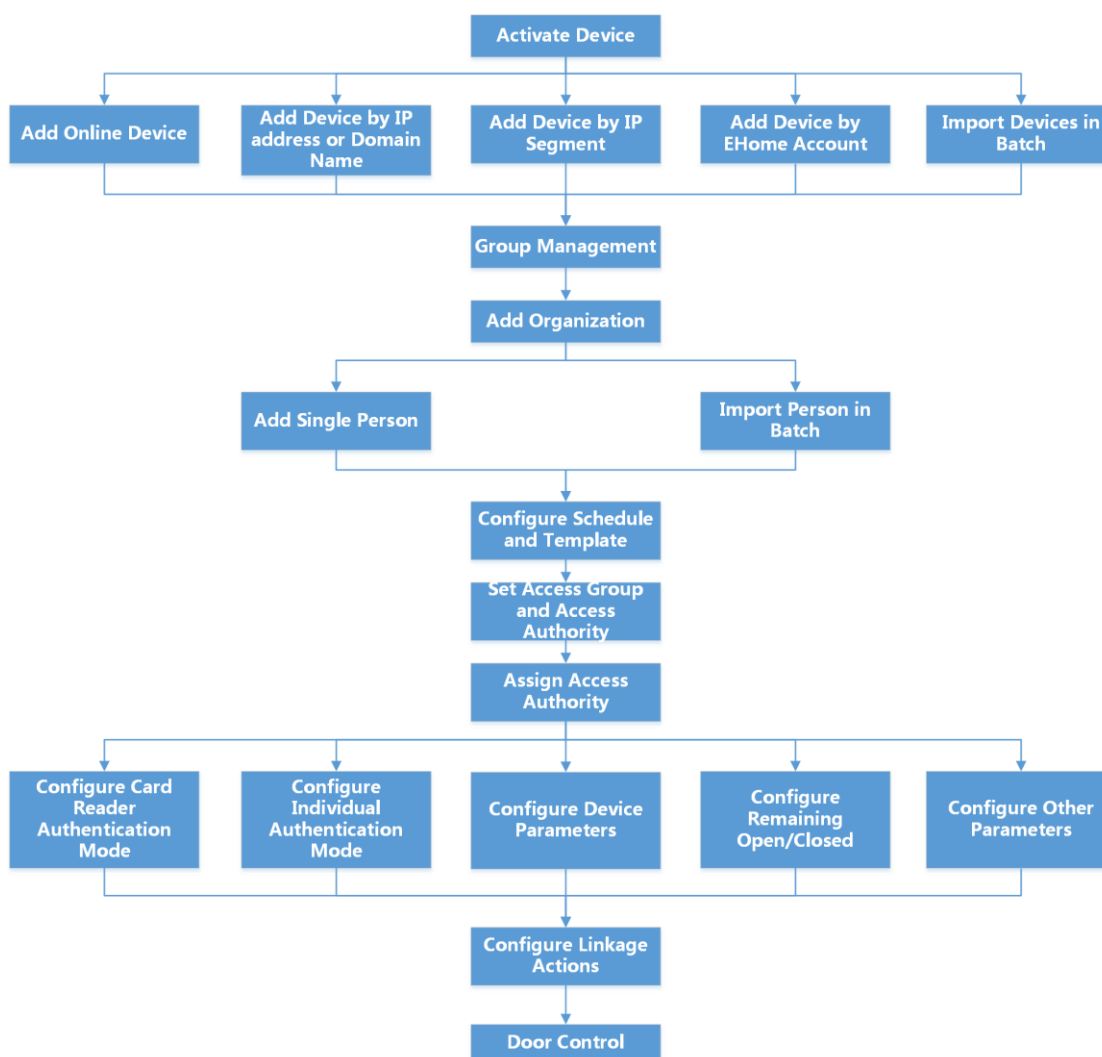


Рисунок 9-1 Схема настройки клиентского ПО

Английский язык	Русский язык
Activate Device	Активировать устройство
Add Online Device	Добавить устройство онлайн
Add Device by IP Address or Domain Name	Добавить устройство по IP-адресу или доменному имени
Add Device by EHome Account	Добавить устройство по учетной записи EHome
Import Devices in Batch	Импортировать устройства в пакетном режиме
Group Management	Управление группами
Add Organization	Добавить организацию
Add Single Person	Добавить одного пользователя
Import Person in Batch	Импорт пользователя в пакетном режиме
Configure Schedule and Template	Настроить расписание и шаблон
Set Access Group and Access Authority	Настроить группу доступа и права доступа
Assign Access Authority	Назначить права доступа
Configure Card Reader	Настроить считыватель карт
Configure Individual Authentication Mode	Настроить индивидуальный режим аутентификации
Configure Device Parameters	Настроить параметры устройства
Configure Remaining Open / Closed	Настроить состояние «Оставить открытым / закрытым»
Configure Other Parameters	Настроить другие параметры
Configure Linkage Actions	Настроить действия привязки
Door Control	Управление дверью

9.2 Управление устройством

Поддержка устройств контроля доступа и устройств видеодомофонии.

Пример

После добавления устройств контроля доступа в клиентское ПО доступно управление въездом и выездом, управление УРВ, видеодомофония с использованием вызывной панели, установленной внутри или снаружи помещений.

9.2.1 Добавление устройства

После запуска клиента к клиенту следует добавить устройства для удаленной настройки и управления.

После добавления устройств можно выбрать устройство и нажать **Remote Configuration** («Удаленная настройка»), чтобы при необходимости настроить дополнительные параметры выбранного устройства.



Примечание

Для некоторых моделей устройств можно открыть окно настройки общих или дополнительных параметров. Чтобы открыть исходное окно удаленной настройки, нажмите **CTRL** и выберите **Remote Configuration** («Удаленная настройка»).

После добавления устройств контроля доступа можно выбрать устройство из списка и нажать **Device Status** («Состояние устройства»), чтобы просмотреть состояние устройства.

Добавление устройства по IP-адресу или доменному имени

Добавьте устройство по IP-адресу или доменному имени.

Для добавления устройств по IP-адресу или доменному имени необходимо выполнить следующие действия.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device** («Устройство») и выберите **Device** («Устройство») в качестве необходимого устройства.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
4. Выберите значение **IP/Domain** («IP-адрес / домен») в поле **Adding Mode** («Режим добавления»).
5. Введите необходимую информацию, включая название, IP-адрес, номер порта, имя пользователя и пароль.

Адрес

Введите IP-адрес устройства или доменное имя.

Порт

Введите № порта устройства. Значение по умолчанию: 8000.

Имя пользователя

Введите имя пользователя устройства. По умолчанию имя пользователя: admin.

Пароль

Введите пароль устройства.



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее. Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально.** После добавления устройства в клиентское ПО нажмите **Synchronize Device Time** («Синхронизировать время устройства»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО.
7. **Опционально.** Нажмите **Export to Group** («Экспортировать в группу»), чтобы создать группу по названию устройства.



Примечание

По умолчанию можно импортировать все каналы устройства в соответствующую группу.

8. **Опционально.** Добавьте автономные устройства.
 - 1) Нажмите **Add Offline Device** («Добавление неактивных 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.
9. Нажмите **Add** («Добавить») для добавления устройств.

Импорт устройств в пакетном режиме

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

Для импорта устройств в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите **Device** → **Add** («Устройство → Добавить»), чтобы открыть окно добавления устройства.
3. Выберите **Batch Import** («Пакетный импорт») в поле **Adding Mode** («Режим добавления»).
4. Нажмите **Export Template** («Скачать шаблон») и сохраните предварительно выбранный шаблон (файл CSV) на компьютере.

5. Откройте экспортированный файл шаблона и введите необходимую информацию об устройствах, подлежащих добавлению, в соответствующие столбцы.

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;

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.

Порт

Введите № порта устройства. Значение по умолчанию: 8000.

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.

Имя пользователя

Введите имя пользователя устройства. По умолчанию имя пользователя: admin.

Пароль

Введите пароль устройства.



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее. Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

Добавление неактивного устройства

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.

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.

Количество IP-каналов

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.

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.

Номер серийного интерфейса

Если в поле режима добавления установлено значение **5**, необходимо ввести номер серийного интерфейса для устройства контроля доступа.

Скорость передачи данных

Если в поле режима добавления установлено значение **5**, необходимо ввести скорость передачи данных (в бодах) для устройства контроля доступа.

DIP

Если в поле режима добавления установлено значение **5**, необходимо ввести DIP-адрес для устройства контроля доступа.

6. Нажмите  и выберите файл шаблона.

7. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

9.2.2 Сброс пароля устройства

Если пользователь забыл пароль обнаруженных онлайн устройств, пароль устройства можно сбросить через клиентское ПО.

Шаги

1. Откройте страницу **Device Management** («Управление устройством»).
2. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств. Все онлайн устройства, находящиеся в одной подсети, будут отображены в списке.
3. Выберите устройство из списка и нажмите  в столбце **Operation** («Операции»).

4. Сбросьте пароль устройства.

- Нажмите **Generate** («Создать»), чтобы открыть окно QR-кода, затем нажмите **Download** («Загрузить»), чтобы сохранить QR-код на компьютере. Также можно сфотографировать QR-код и сохранить его на телефон. Отправьте изображение в нашу службу технической поддержки.

**Примечание**

Для выполнения следующих операций по сбросу пароля обратитесь в службу технической поддержки.

**Предостережение**

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

9.2.3 Управление добавленными устройствами

После добавления устройств вы можете управлять добавленными устройствами, в том числе: редактировать параметры устройства, выполнять удаленную настройку устройства, просмотреть состояние устройства и т. д.

Таблица 9-1 Управление добавленными устройствами

Редактирование устройства	Нажмите  , чтобы изменить информацию об устройстве, включая имя устройства, адрес, имя пользователя, пароль и т. д.
Удаление устройства	Выберите одно или более устройств, затем нажмите Delete («Удалить»), чтобы удалить выбранные устройства.
Удаленная настройка	На странице списка устройств нажмите  в столбце Operation («Операции»), чтобы выполнить удаленную настройку устройства.  находится в крайнем правом столбце страницы устройства. Подробная информация представлена в руководстве пользователя устройства.
Просмотр состояния устройства	Нажмите  , чтобы просмотреть состояние устройства, включая наименование двери, номер, статус и т. д.  Примечание Доступная информация о состоянии устройства зависит от модели фактического устройства.
Просмотр пользователей в сети	Нажмите  , чтобы просмотреть подробную информацию о пользователях в сети, которые имеют доступ к устройству, включая имя пользователя, тип пользователя, IP-адрес и время входа в систему.

Обновление информации об устройстве	Нажмите  , чтобы обновить и получить последнюю информацию об устройстве.
Обновление устройства	Просмотрите статус устройства в столбце Firmware Upgrade («Обновление прошивки»), отметьте одно или несколько обновляемых устройств и нажмите Upgrade Device Firmware («Обновить прошивку устройства»), чтобы обновить выбранные устройства.
Получение событий с устройства	Отметьте одно устройство и нажмите Get Events from Device («Получить события с устройства»), чтобы синхронизировать события.
Экспорт устройства	Нажмите Export Device («Экспорт устройства»), укажите путь сохранения и выберите тип устройства, чтобы экспортировать сведения об устройстве (например, тип устройства, IP-адрес и номер порта) на локальный компьютер.  Примечание Суперпользователь может включить защиту паролем и ввести пароль, после чего экспортированный файл с информацией об устройстве будет зашифрован.

9.3 Управление группами

Клиентское ПО предоставляет области для управления добавленными ресурсами в разных группах. Ресурсы можно сгруппировать в разные группы в зависимости от расположения ресурсов.

Пример

Например, на первом этаже установлено 16 дверей, 64 тревожных входа и 16 тревожных выходов. Эти ресурсы можно организовать в одну группу (с именем «1-й этаж») для удобного управления. Можно контролировать состояние двери и выполнять другие операции с устройствами, объединив ресурсы по группам.

9.3.1 Добавление группы

Добавьте группы для удобного управления устройствами.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
3. Создайте группу.
 - Нажмите **Add Group** («Добавить группу») и введите желаемое название группы.
 - Нажмите **Create Group by Device Name** («Создать группу по названию устройства») и выберите добавленное устройство, чтобы создать новую группу по имени выбранного устройства.

Примечание

Ресурсы (такие как тревожные входы / выходы, точки доступа и т. д.) устройства будут импортированы в группу по умолчанию.

9.3.2 Добавление ресурсов в группу

Импортируйте ресурсы устройства (такие как тревожные входы / выходы, точки доступа и т. д.) в добавленную группу в пакетном режиме.

Перед началом

Добавьте группу для управления устройствами. Подробная информация представлена в разделе **Добавление группы**.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
3. Выберите группу и тип ресурса из списка: **Access Point** («Точка доступа»), **Alarm Input** («Тревожный вход»), **Alarm Output** («Тревожный выход») и т. д.
4. Нажмите **Import** («Импорт»).
5. Выберите миниатюры / названия ресурсов для отображения в списке.

Примечание

Нажмите  или  чтобы переключить режим отображения ресурса на режим просмотра миниатюр или списка.

6. Нажмите **Import** («Импорт») для импорта выбранных ресурсов в группу.

9.4 Управление сотрудниками / посетителями

Добавьте информацию о сотруднике / посетителе в систему для дальнейших операций, таких как контроль доступа, видеодомофония, настройка времени, УРВ и т. д. Здесь можно управлять добавленными пользователями, например, выпускать карточки в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.

9.4.1 Добавление организации

Добавьте организацию и импортируйте информацию о сотруднике/посетителе в организацию для эффективного управления персоналом. Также можно добавить подчиненную организацию для добавленной организации.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите головную организацию в левом столбце и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию.

3. Создайте имя для добавленной организации.



Примечание

Можно добавить до 10 уровней организаций.

4. **Опционально.** Выполните следующие операции.

Изменение

организации

Наведите указатель мыши на добавленную организацию и нажмите , чтобы изменить ее название.

Удаление

организации

Наведите указатель мыши на добавленную организацию и нажмите , чтобы удалить ее.



Примечание

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

Отображение

персонала

подчиненной

организации

Нажмите **Show Persons in Sub Organization** («Отображение персонала подчиненной организации») и выберите организацию, чтобы показать персонал подчиненной организации.

9.4.2 Импорт и экспорт информации о сотруднике / посетителе

Можно импортировать информацию о нескольких пользователях в клиентское ПО в пакетном режиме. Также информацию о пользователях можно экспортировать и сохранить на компьютере.

Импорт информации о сотруднике / посетителе

Можно импортировать информацию о нескольких пользователях (включая идентификационную информацию, данные отпечатков пальцев и номер карты, привязанной к отпечатку пальца) в клиентское ПО в пакетном режиме посредством импорта файла Excel с локального ПК.

Для импорта данных в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control → Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Import Person** («Импортировать пользователя») и выберите **Person Information** («Информация о сотруднике / посетителе») в качестве данных для импорта.
3. Во всплывающем окне нажмите **Download Template for Importing Person** («Скачать шаблон для импорта сотрудника / посетителя»), чтобы скачать шаблон.
4. Введите информацию о пользователе в загруженный шаблон.

От f1 до f10

Данные отпечатков пальцев.

От f1-карты до f10-карты

Номер карты, привязанной к отпечатку пальца. Если привязка карты не выполнена, поле можно не заполнять.



Примечание

Если у пользователя несколько карт, разделите каждый номер карты точкой с запятой.

5. Войдите в **Access Control** → **Person and Card** («Контроль доступа → Управление пользователями и картами»), нажмите **Import Person** («Импортировать пользователя») и выберите файл Excel с информацией о сотруднике / посетителе.
6. Нажмите **ОК** для запуска импорта.



Примечание

Если номер сотрудника / посетителя уже существует в базе данных клиентского ПО, информация после импорта будет автоматически заменена.

Импорт изображений сотрудников / посетителей

После импорта изображений лиц в клиентское ПО, пользователи на изображениях могут быть идентифицированы с помощью терминала доступа с функцией распознавания лиц. Можно импортировать изображения пользователей по одному или импортировать несколько изображений одновременно.

Перед началом

Не забудьте заранее импортировать информацию о пользователе в клиентское ПО.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите добавленную организацию из списка и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию, затем выберите эту организацию.
3. Нажмите **Import** («Импорт»), чтобы открыть соответствующую панель, затем выберите **Face** («Лицо»).
4. **Опционально.** Включите функцию **Verify by Device** («Проверка устройством»), чтобы проверить способность устройства распознавания лиц на клиентском ПО распознать лицо на фотографии.
5. Нажмите , чтобы выбрать файл с изображением лица.



Примечание

- Папка с изображениями лиц должна быть в формате ZIP.
- Изображение должно быть в формате JPG. Размер изображения не должен превышать 200 КБ.

- Название файла изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_Имя». Идентификатор пользователя должен совпадать с идентификатором импортированного пользователя.

6. Нажмите **Import** («Импорт») для начала импорта.

Прогресс и результат импорта будут отображены на экране.

Экспорт информации о сотруднике / посетителе

Экспортируйте данные о добавленном пользователе на локальный ПК в формате Excel. Для экспорта информации пользователей в пакетном режиме необходимо выполнить следующие действия.

Шаги

1. Нажмите **Access Control** → **Person and Card** («Контроль доступа → Управление пользователями и картами»).
2. Нажмите **Export Person** («Импортировать пользователя») и выберите **Person Information** («Информация о сотруднике / посетителе») в качестве данных для экспорта.
3. Выберите путь сохранения экспортированного Excel файла.
4. Выберите элементы информации о сотруднике / посетителе, которые необходимо экспортировать.
5. Нажмите **OK**, чтобы начать экспорт.

От f1 до f10

Данные отпечатков пальцев.

От f1-карты до f10-карты

Номер карты, привязанной к отпечатку пальца. Если привязка карты не выполнена, поле можно не заполнять.

Экспорт изображений сотрудников / посетителей

Экспортируйте файл с изображением лиц добавленных сотрудников и сохраните его на компьютере.

Перед началом

- Убедитесь, что пользователи и изображения их лиц добавлены в организацию.
 - Убедитесь, что включена функция **Export Person Information** («Экспорт информации о сотруднике / посетителе»), чтобы отобразить кнопку **Export** («Экспорт»).
- Подробная информация представлена в соответствующем разделе.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. **Опционально.** Выберите организацию из списка.



Примечание

Если не выбрать конкретную организацию, будут экспортированы изображения лиц всех пользователей.

3. Нажмите **Export** («Экспорт») в главном меню.
4. Введите имя суперпользователя и пароль для проверки. Откроется панель экспорта.
5. Выберите **Face** («Лицо») в качестве контента для экспорта.
6. Нажмите **Export** («Экспорт») и установите ключ шифрования для шифрования экспортируемого файла.



Примечание

- Файл будет экспортирован в формате ZIP.
- Название файла экспортированного изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_имя_0» («0» — для лица, видимого во всех деталях).

9.4.3 Получение информации о пользователе с устройства контроля доступа

Если добавленное устройство контроля доступа было дополнено информацией о пользователе (включая подробную информацию о пользователе, об отпечатках пальцев и выданной карте), данную информацию можно получить с устройства и импортировать ее в клиент для дальнейшей работы.

Шаги



Примечание

- 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.
- Если номер карты или идентификатор пользователя (идентификатор сотрудника), который хранится на устройстве, уже существует в клиентской базе данных, пользователь с таким номером карты или идентификатором не будет импортирован в клиентское ПО.

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите организацию для импорта сотрудников.
3. Нажмите **Get from Device** («Получить из устройства»).
4. Выберите добавленное устройство контроля доступа или настольный считыватель карт из выпадающего списка.



Примечание

При выборе настольного считывателя карт, нажмите **Login** («Войти»), затем установите IP-адрес, номер порта, имя пользователя и пароль.

5. Выберите **Getting Mode** («Режим получения»).



Примечание

Режим получения может различаться в зависимости от устройства. Устройство контроля доступа поддерживает получение личной информации о пользователе с помощью ID сотрудника. Могут быть указаны до 5 ID сотрудников.

-
6. Нажмите **Import** («Импорт») для начала импорта информации о пользователе в клиент.
-



Примечание

Можно импортировать до 2000 пользователей и до 5000 карт.

Информация пользователя, включая подробную информацию, информацию об отпечатках пальцев (если настроены) и связанных картах (если настроены), будет импортирована в выбранную организацию.

9.4.4 Выдача карт сотрудникам в пакетном режиме

В клиентском ПО предусмотрена возможность выпустить сразу несколько карт в пакетном режиме.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Нажмите **Batch Issue Cards** («Выпуск карт в пакетном режиме»).
Будут отображены все добавленные пользователи, для которых карты еще не были выпущены.
3. Настройка параметров выпуска карт. Подробная информация представлена в разделе **Настройка параметров выпуска карт**.
4. Нажмите **Initialize** («Инициализировать»), чтобы инициализировать считыватель карт и подготовить его к выдаче карт.
5. Нажмите на колонку **Card No.** («Номер карты») и введите номер карты.
 - Поместите карту на настольный считыватель.
 - Считайте карту через считыватель карт.
 - Введите номер карты вручную и нажмите клавишу **Enter** на клавиатуре.Номер карты считывается автоматически, и карта будет выпущена сотруднику в списке.
6. Повторите вышеизложенные шаги для выпуска карт сотрудникам в списке в последовательном порядке.

9.4.5 Сообщить о потере карты

В случае утери карты необходимо сообщить о потере для деактивации доступа с помощью утерянной карты.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите сотрудника, о потере карты которого необходимо сообщить, и нажмите **Edit** («Редактировать»), чтобы открыть соответствующее окно.

3. На панели **Credential** → **Card** («Учетные данные → Карта»), нажмите  на добавленную карту, чтобы изменить ее статус на **Lost card** («Утерянная карта»).

После уведомления об утере карты авторизация доступа по этой карте будет недействительной и неактивной. Если картой решит воспользоваться другой пользователь, он не сможет получить доступ к дверям, используя утерянную карту.

4. **Опционально.** Нажмите , чтобы отменить рапорт о потере карты, если карта найдена.

После отмены уведомления об утере карты, авторизация доступа по этой карте будет действительной и активной.

5. Если утерянная карта добавлена в группу доступа, которая применена к устройству, после сообщения об утере карты или отмене уведомления об утере карты появится окно с уведомлением о необходимости применить изменения к устройству. После применения к устройству эти изменения будут задействованы на устройстве.

9.4.6 Настройка параметров выпуска карт

Предусмотрено два режима считывания номера карты: с помощью настольного считывателя карт или считывателя карт устройства контроля доступа. Подключите настольный считыватель карт к ПК, на котором работает клиент, через USB или COM-интерфейс, затем поместите карту на настольный считыватель карт. При отсутствии настольного считывателя карт считайте карту через считыватель карт добавленного устройства контроля доступа, чтобы получить номер карты. Перед выпуском карты для пользователя необходимо установить параметры выпуска карты, в том числе режим выпуска карт и сопутствующие параметры.

При добавлении карточки нажмите **Settings** («Настройки»), чтобы открыть соответствующее окно.

Локальный режим: выпуск карт с помощью настольного считывателя карт

Подключите настольный считыватель карт к ПК, на котором работает клиент. Приложите карту к настольному считывателю для получения номера карты.

Настольный считыватель карт

Выберите модель подключенного настольного считывателя карт

Примечание

В настоящее время поддерживаются следующие модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

Тип карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8E или DS-K1F180-D8E.

Выберите тип карты: EM-карта или IC-карта в соответствии с фактическим типом карты.

Серийный интерфейс

Это поле доступно только для модели считывателя карт DS-K1F100-M. Выберите COM-интерфейс, к которому будет подключен настольный считыватель карт.

Бипер

После успешного считывания номера карты включите или выключите бипер.

Тип номера карты

Выберите необходимый тип номера карты.

Шифрование M1-карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8, DS-K1F100-D8E или DS-K1F180-D8E.

Если используется карта M1 и нужно активировать функцию ее шифрования, выберите соответствующий сектор.

Удаленный режим: выпуск карт с помощью считывателя карт

Выберите устройство контроля доступа, добавленное в клиент, и считайте карту через считыватель карт, чтобы получить ее номер.

9.5 Настройка графиков и шаблонов

Настройте шаблон, в том числе недельный график работы и график выходных дней. После настройки шаблона, его можно использовать для настройки групп доступа, чтобы настройки указанной группы доступа были действительны во время действия шаблона.

Примечание

Подробная информация о настройке группы контроля доступа представлена в разделе ***Настройка группы контроля доступа для назначения разрешений на доступ***.

9.5.1 Добавление выходного дня

Здесь можно установить выходные дни и настроить параметры выходных дней, в том числе дату начала, дату окончания и продолжительность указанного периода.

Шаги

Примечание

Можно добавить до 64 групп выходных дней.

1. Нажмите **Access Control → Schedule → Holiday** («Контроль доступа → Графики → Выходные дни»), чтобы перейти на соответствующую страницу.
 2. На панели слева нажмите **Add** («Добавить»).
 3. Создайте название для выходного дня.
 4. **Опционально.** Введите описание или уведомления об этом выходном дне в поле **Remark** («Замечания»).
 5. Добавьте период и настройте продолжительность выходных дней.
-

Примечание

Для одной группы выходного дня можно добавить до 16 периодов.

- 1) Нажмите **Add** («Добавить») в поле списка выходных дней.
- 2) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.



Примечание

Для одного периода выходных может быть установлено до 8 временных интервалов.

- 3) **Опционально.** Для изменения временных интервалов выполните следующие действия.
 - Когда вид курсора изменится на , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
 - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
 - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
 - 4) **Опционально.** Выберите отрезок времени, который необходимо удалить, а затем нажмите  в столбце **Operation** («Операции»), чтобы удалить его.
 - 5) **Опционально.** Нажмите кнопку , чтобы удалить все отрезки времени нерабочих дней.
 - 6) **Опционально.** Или нажмите кнопку , чтобы удалить конкретный нерабочий день.
6. Нажмите **Save** («Сохранить»).

9.5.2 Добавление шаблона

Шаблон может содержать недельный график работы и график выходных дней. Установите недельный график работы и назначьте время авторизации доступа для конкретного пользователя или группы. Также можно выбрать добавленные выходные дни и включить их в шаблон.

Шаги

Примечание

Можно добавить до 255 шаблонов.

1. Нажмите **Access Control → Schedule → Template** («Контроль доступа → Графики → Шаблон»), чтобы перейти на соответствующую страницу.

Примечание

По умолчанию предусмотрено два вида шаблонов: **All-Day Authorized** («Авторизован в течение всего дня») и **All-Day Denied** («Доступ запрещен в течение всего дня»). Указанные шаблоны не подлежат редактированию или удалению.

All-Day Authorized («Авторизован в течение всего дня»)

Авторизация действует в каждый день недели и не предусматривает выходных дней.

All-Day Denied («Доступ запрещен в течение всего дня»)

Авторизация не действует в течение недели и не предусматривает выходных дней.

2. На панели слева нажмите **Add** («Добавить»), чтобы создать новый шаблон.
3. Создайте имя для шаблона.
4. Введите описание или уведомления об этом шаблоне в поле **Remark** («Замечания»).

5. Внесите изменения в недельный график и примените их к шаблону.

- 1) Перейдите на вкладку **Week Schedule** («Недельный график работы») на панели снизу.
- 2) Выберите день недели и укажите продолжительность на шкале времени.



Примечание

Для каждого дня в недельном графике может быть установлено до 8 временных интервалов.

- 3) **Опционально.** Для изменения временных интервалов выполните следующие действия.
 - Когда вид курсора изменится на , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
 - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
 - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
- 4) Повторите два последних действия выше, чтобы задать несколько временных интервалов в другие дни недели.

6. Добавьте выходной день и примените его к шаблону.



Примечание

В один шаблон можно добавить до 4 выходных дней.

- 1) Нажмите на вкладку **Holiday** («Выходной день»).
- 2) Выберите выходной день из списка слева, чтобы добавить его в выбранный список на панели справа.
- 3) **Опционально.** Нажмите **Add** («Добавить») для добавления нового выходного.



Примечание

Подробная информация о добавлении выходных представлена в разделе **Добавление выходных.**

- 4) **Опционально.** Выберите выходной день и нажмите , чтобы удалить его, или нажмите **Clear** («Очистить»), чтобы удалить все выбранные выходные дни из списка справа.

7. Нажмите **Save** («Сохранить») для сохранения настроек и завершите добавление шаблона.

9.6 Настройка группы контроля доступа для назначения разрешений на доступ

После добавления пользователя и настройки его учетных данных можно создать группы контроля доступа, чтобы предоставить доступ к дверям для определенных пользователей. После этого необходимо применить группу контроля доступа к устройству контроля доступа, чтобы измененные настройки были задействованы.

Шаги

- Для одного сотрудника: можно добавить до 4 групп доступа на одну контрольную точку доступа на одном устройстве.
 - Всего можно добавить до 128 групп доступа.
 - После изменения настроек группы доступа необходимо снова применить эти группы доступа к устройствам, чтобы изменения вступили в силу. Изменения в группе доступа включают в себя изменения шаблона, настроек группы доступа, настроек группы доступа пользователя и сведений о связанных лицах (включая № карты, отпечатки пальцев, изображения лиц, привязку № карты и отпечатков пальцев, пароль карты, срок действия карты и др.).
1. Нажмите **Access Control** → **Access Group** («Контроль доступа → Группа доступа»), чтобы перейти на соответствующую страницу.
 2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
 3. В текстовом поле **Name** («Имя») введите имя для группы доступа по своему выбору.
 4. Выберите шаблон для группы доступа.



Примечание

Необходимо настроить шаблон перед настройкой группы доступа. Подробная информация представлена в разделе **Настройка графиков и шаблонов**.

5. Слева в поле **Select Person** («Выбрать сотрудника / посетителя») выберите сотрудника / пользователя, и он будет добавлен в выбранный список.
6. Слева в поле **Select Door** («Выбрать дверь») выберите дверь или вызывную панель(и) для доступа выбранным пользователям, и выбранная дверь или вызывная панель будет добавлена в выбранный список.
7. Нажмите **OK**.
8. После добавления группы доступа необходимо применить их к устройству контроля доступа, чтобы изменения были задействованы.
 - 1) Выберите группы доступа, которые необходимо применить к устройству контроля доступа.
Для выбора нескольких групп доступа удерживайте клавиши **Ctrl** или **Shift**.
 - 2) Нажмите **Apply All to Devices** («Применить все к устройствам») для до начала применения выбранных групп доступа к устройству контроля доступа или вызывной панели.



Предостережение

- Нажатие **Apply All to Devices** («Применить все к устройствам») очистит все группы доступа выбранных устройств, а затем применит новую группу доступа.
- Можно нажать **Apply Changes to Devices** («Применить изменения к устройствам»), чтобы применить только измененную часть выбранной группы доступа к устройству.

3) Присвоенный статус отображается в столбце **Status** («Статус»). Также можно нажать **Applying Status** («Присвоенный статус»), чтобы просмотреть все примененные группы доступа.

Выбранные пользователи будут иметь разрешения на вход/выход через выбранные двери/вызывные панели при помощи привязанных карт или отпечатков пальцев.

9. Опционально. При необходимости нажмите  для редактирования групп доступ.

9.7 Настройка расширенных функций

Настройте расширенные функции контроля доступа в соответствии со сценой наблюдения.



Примечание

- При использовании функций, связанных с картами (с картами контроля доступа), во время добавления карт будут перечислены только карты с примененной группой доступа.
- Устройство должно поддерживать возможность использования расширенных функций.
- Наведите курсор на **Advanced Function** («Расширенная функция»), затем нажмите  для настройки расширенной функции.

9.7.1 Настройка оставить заблокированной / разблокированной

Настройте состояние двери как «разблокирована» или «заблокирована», а также настройте контроллер лифта как «свободный» и «контролируемый». Например, можно перевести дверь в состояние «заблокирована» в праздничные дни, или в состояние «разблокирована» в указанный рабочий день.

Перед началом

Добавьте устройство контроля доступа в систему.

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Remain Locked/Unlocked** («Контроль доступа → Расширенные функции → Оставить заблокированной / разблокированной»), чтобы перейти на соответствующую страницу.
2. На панели слева выберите дверь и контроллер лифта, которые необходимо настроить.
3. Для настройки контроллера лифта и двери в течение рабочего дня нажмите **Week Schedule** («График рабочей недели») и выполните следующие действия.
 - 1) Нажмите **Remain Unlocked** («Оставить разблокированным») или **Remain Locked** («Оставить заблокированным»).

- 2) Для контроллера лифта выберите значение: **Free** («Свободный») или **Controlled** («Контролируемый»).
- 3) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.



Примечание

Для каждого дня в недельном графике может быть установлено до 8 временных интервалов.

- 4) **Опционально.** Для изменения временных интервалов выполните следующие действия.
 - Когда вид курсора изменится на , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
 - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
 - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
- 5) Нажмите **Save** («Сохранить»).

Сопутствующие операции

**Применить
ко всей
неделе**

Выберите временной интервал на шкале времени и нажмите **Copy to Whole Week** («Применить ко всей неделе»), чтобы применить настройки ко всем дням недели.

**Удалить
выбранные интервалы**

Выберите временной интервал на шкале времени и нажмите **Delete Selected** («Удалить выбранные интервалы»), чтобы удалить временной интервал.

Очистить

Нажмите **Clear** («Очистить»), чтобы очистить все настройки временных интервалов в недельном графике.

4. Для настройки состояния двери в течение выходного дня нажмите **Holiday** («Выходной день») и выполните следующие действия.
 - 1) Нажмите **Remain Unlocked** («Оставить разблокированным») или **Remain Locked** («Оставить заблокированным»).
 - 2) Нажмите **Add** («Добавить»).
 - 3) Введите дату начала и дату окончания периода.
 - 4) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.



Примечание

Для одного периода выходных может быть установлено до 8 временных интервалов.

- 5) Для изменения временных интервалов выполните следующие действия.
 - Когда вид курсора изменится на , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.

- Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
- Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
- 6) **Опционально.** Выберите отрезок времени, который необходимо удалить, а затем нажмите  в столбце **Operation** («Операции»), чтобы удалить его.
- 7) **Опционально.** Нажмите кнопку , чтобы удалить все отрезки времени нерабочих дней.
- 8) **Опционально.** Или нажмите кнопку , чтобы удалить конкретный нерабочий день.
- 9) Нажмите **Save** («Сохранить»).
- 5. **Опционально.** Нажмите **Copy to** («Скопировать на»), чтобы применить состояние двери к этой двери и к другим дверям.

9.7.2 Настройка запрета двойного прохода

Установите контрольный пункт проверки доступа, через который возможен проход одного человека после считывания карты.

Перед началом

Включите функцию запрета двойного прохода по маршруту.

Для настройки функции запрета двойного прохода выполните следующие действия.

Шаги

Примечание

Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Подробная информация о блокировке нескольких дверей представлена в разделе **Настройка блокировки нескольких дверей**.

1. Нажмите **Access Control → Advanced Function → Anti-Passback** («Контроль доступа → Расширенные функции → Запрет двойного прохода»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа на панели слева.
3. Выберите считыватель карт в качестве точки начала маршрута в поле **First Card Reader** («Первый считыватель карт»).
4. Нажмите  на выбранный считыватель карт в колонке **Card Reader Afterward** («Следующий считыватель карт»), чтобы открыть выбранный считыватель карт.
5. Выберите считыватель карт, который следует за первым считывателем карт.

Примечание

Для одного считывателя карт можно добавить до 4 последующих считывателей карт.

6. В диалоговом окне нажмите **OK**, чтобы сохранить выбранные настройки.
7. На странице функции запрета двойного прохода нажмите **Save** («Сохранить») для сохранения настроек и их применения в устройстве.

Пример

Установите маршрут считывания карты.

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.

9.7.3 Настройка блокировки нескольких дверей

Вы можете установить блокировку нескольких дверей для нескольких дверей одного контроллера доступа. Чтобы открыть одну из дверей, другие двери должны оставаться закрытыми. Это означает, что в блокировке комбинированной группы дверей одновременно может открываться до одной двери.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает функцию блокировки нескольких дверей.

Шаги**Примечание**

- Функция блокировки нескольких дверей поддерживается только устройством контроля доступа, которое имеет более одной точки контроля доступа (дверей).
- Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Информация о настройке функции запрета двойного прохода представлена в разделе **Настройка запрета двойного прохода**.

1. Нажмите **Access Control → Advanced Function → Multi-door Interlocking** («Контроль доступа → Расширенные функции → Блокировка нескольких дверей»).
2. Выберите устройство контроля доступа на панели слева.
3. Нажмите **Add** («Добавить») на панели **Multi-door Interlocking List** («Список блокировки нескольких дверей»), чтобы открыть **Add Access Control Point** («Добавить точку контроля доступа») и открыть окно добавления.
4. Выберите как минимум две точки (двери) контроля доступа из списка.

**Примечание**

В одну комбинацию блокировки нескольких дверей можно добавить до четырех дверей.

5. Нажмите **OK**, чтобы добавить выбранные точки контроля доступа для блокировки. Настроенная комбинация блокировки нескольких дверей будет отображаться на панели **Multi-door Interlocking List** («Список блокировки нескольких дверей»).
6. **Опционально.** Выберите из списка добавленную комбинацию блокировки нескольких дверей и нажмите **Delete** («Удалить»), чтобы удалить комбинацию.
7. Нажмите **Apply** («Применить»), чтобы применить настройки к устройству контроля доступа.

9.7.4 Настройка аутентификации в качестве первого пользователя

Для одной точки контроля доступа можно назначить несколько первых пользователей.

После авторизации первого пользователя несколько других пользователей получают доступ к дверям и разрешения на другие действия.

Перед началом

- Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает функцию аутентификации первого пользователя.
- Добавьте сотрудника/пользователя и задайте параметры авторизации доступа. Подробная информация представлена в разделах **Управление сотрудниками / посетителями** и **Настройка группы контроля доступа для назначения разрешений на доступ**.

Шаги

1. Нажмите **Access Control → Advanced Function → First Person In** («Контроль доступа → Расширенные функции → Аутентификация в качестве первого пользователя»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка слева.
3. Из выпадающего списка выберите режим для каждого устройства: **Enable Remaining Open after First Person** («Активировать функцию, при которой дверь остается открытой после аутентификации первого пользователя») или **Disable Remaining Open after First Person** («Деактивировать функцию, при которой дверь остается открытой после аутентификации первого пользователя»).

Активация функции, при которой дверь остается открытой после аутентификации первого человека

После авторизации первого человека дверь остается открытой в течение заданного промежутка времени и до истечения оставшегося времени открытия. Чтобы выбрать этот режим, необходимо установить время последовательной аутентификации и интервал последовательной аутентификации.



Примечание

Допустимый диапазон длительности открытого состояния двери: от 0 до 1440 минут. По умолчанию длительность открытого состояния составляет 10 минут.

Выключение функции, при которой дверь остается открытой после аутентификации первого пользователя

Выключение функции аутентификации первого пользователя.

Авторизация после первого лица

Все режимы аутентификации (за исключением авторизации суперкарты, суперпароля, принудительной карты и кода принуждения) доступны только после авторизации первого лица.



Примечание

Чтобы отключить режим авторизации после первого лица, необходимо выполнить повторную авторизацию первого лица.

4. В списке **First Person** («Первый пользователь») нажмите **Add** («Добавить»).
5. Выберите пользователей из списка слева, чтобы добавить их к выбранным пользователям в качестве первого пользователя дверей.
Добавленные первые пользователи будут перечислены в списке первых пользователей.

6. **Опционально.** Выберите пользователя из списка и нажмите **Delete** («Удалить»), чтобы удалить пользователя из списка первых пользователей.
7. Нажмите **Save** («Сохранить»).

9.7.5 Настройка многофакторной аутентификации

Настройте управление пользователями по группам и установите аутентификацию для нескольких пользователей в одной точке контроля доступа (двери).

Перед началом

Установите группу доступа и примените ее к устройству контроля доступа. Подробная информация представлена в разделе **Настройка группы контроля доступа для назначения разрешений на доступ.**

Выполните следующие действия, чтобы настроить аутентификацию сразу нескольких карт для одной точки контроля доступа (двери).

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Multi-Factor Auth** («Контроль доступа → Расширенные функции → Многофакторная аутентификация»).
2. Выберите устройство контроля доступа из списка слева.
3. Добавьте пользователя / группу карт для устройства контроля доступа.
 - 1) На панели справа нажмите **Add** («Добавить»).
 - 2) Создайте имя для группы своему усмотрению.
 - 3) Укажите время начала и время окончания периода действия разрешения пользователя / группы карт.
 - 4) Выберите доступных членов группы и карты из списка, чтобы добавить их в выбранный список.



Примечание

Карта должна быть предварительно выпущена для пользователя.

Предварительно установите группу доступа и примените ее к устройству контроля доступа.

- 5) Нажмите **Save** («Сохранить»).
- 6) **Опционально.** Выберите пользователя / группу карт, затем нажмите **Delete** («Удалить»), чтобы удалить их.
- 7) **Опционально.** Выберите пользователя / группы карт и нажмите **Apply** («Применить»), чтобы повторно применить группу доступа, которую ранее не удалось применить к устройству контроля доступа.
4. Выберите точку контроля доступа (дверь) выбранного устройства на панели слева.
5. Введите максимальный интервал времени при вводе пароля.
6. Добавьте группу аутентификации для выбранной точки контроля доступа.
 - 1) На панели **Authentication Groups** («Группы аутентификации») нажмите **Add** («Добавить»).

- 2) Из выпадающего списка выберите настроенный шаблон в качестве шаблона аутентификации.



Примечание

Информация о настройке шаблона представлена в разделе **Настройка графиков и шаблонов**.

- 3) Выберите тип аутентификации группы из выпадающего списка **Local Authentication** («Локальная аутентификация»), **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») или **Local Authentication and Super Password** («Локальная аутентификация и пароль суперпользователя»).

Локальная аутентификация

Аутентификация с помощью устройства контроля доступа.

Локальная аутентификация и удаленное открытие двери

Аутентификация через устройство контроля доступа и клиентское ПО. После считывания карты появится окно. Дверь может быть разблокирована через клиентское ПО.

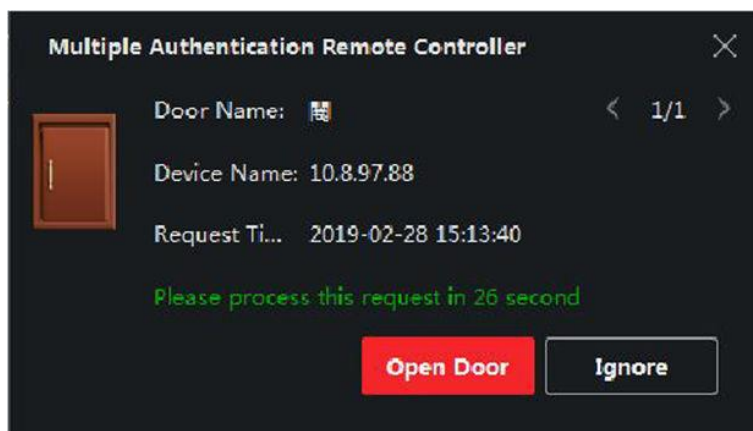


Рисунок 9-2 Удаленное открытие двери



Примечание

Выберите **Offline Authentication** («Автономная аутентификация»), чтобы активировать функцию аутентификации по суперпаролю, если устройство контроля доступа было отключено от клиентского ПО.

Локальная аутентификация и суперпароль

Аутентификация с помощью устройства контроля доступа и суперпароля.

- 4) Выберите добавленного пользователя / группу карт из списка слева внизу экрана, чтобы добавить его в список в качестве группы аутентификации.
 - 5) Нажмите на добавленную группу аутентификации в списке справа, чтобы установить количество попыток аутентификации в столбце **Auth Times** («Количество попыток считывания карты»).
-



Примечание

Количество попыток считывания карты должно быть больше 0 и не превышать количество добавленных пользователей в соответствующей группе.

- 6) Нажмите **Save** («Сохранить»).
-



Примечание

- Для каждой точки контроля доступа (двери) можно добавить до 4 групп аутентификации.
 - В группу аутентификации с типом **Local Authentication** («Локальная аутентификация») можно добавить до восьми пользователей / групп карт.
 - В группу аутентификации с типом **Local Authentication and Super Password** («Локальная аутентификация и пароль суперпользователя») или **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») можно добавить до 7 групп карт.
-

7. Нажмите **Save** («Сохранить»).

9.7.6 Настройка аутентификации при помощи считывателя карт

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

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Authentication** («Контроль доступа → Расширенные функции → Аутентификация»), чтобы перейти на соответствующую страницу.
2. На панели слева выберите считыватель карт, который необходимо настроить.
3. Установите режим аутентификации для считывателя карт.
 - 1) Нажмите на кнопку **Configuration** («Настройки»).

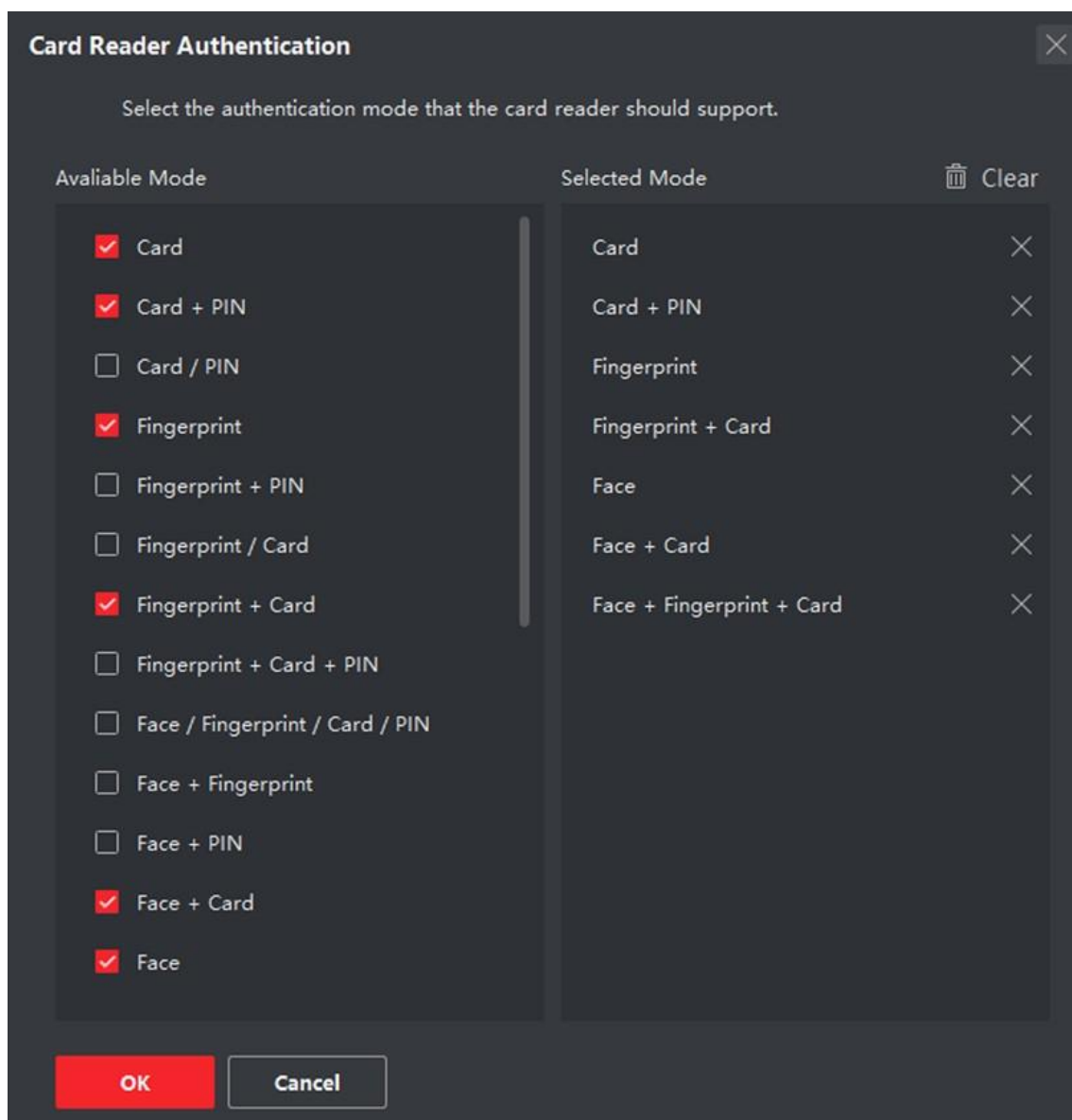


Рисунок 9-3 Выбор режима аутентификации для считывателя карт

- 2) Выберите режим из списка доступных режимов, чтобы добавить его в список выбранных режимов.
- 3) Нажмите **ОК**.

После завершения процедуры выбора режимов, они будут отображаться на экране в виде значков.

4. Нажмите на значок, чтобы выбрать режим аутентификации устройства для считывания карт. Проведите курсором мыши по определенному дню, чтобы нарисовать цветную полосу в графике. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи устройства для считывания карт.
5. Повторите этот шаг для установки других отрезков времени.
6. **Опционально.** Выберите настроенный день и нажмите кнопку **Copy to Week** («Применить ко всем дням недели»), чтобы применить эти настройки ко всем дням недели.

7. **Опционально.** Нажмите **Copy to** («Копировать в»), для копирования настроек в другие считыватели карт.
8. Нажмите **Save** («Сохранить»).

9.7.7 Настройка параметров устройства

После добавления устройства контроля доступа можно настроить параметры устройства контроля доступа и точки управления доступом.

Настройка параметров устройства контроля доступа

После добавления устройства контроля доступа можно настроить его параметры, в том числе наложить пользовательскую информацию на изображение, загрузить изображения после захвата, сохранить захваченные изображения и т. д.

Перед началом

Добавьте устройство контроля доступа в клиент.

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).

Примечание

Выберите **Device Parameter** («Параметры устройства») в списке расширенных функций, наведите курсор, а затем нажмите  чтобы отобразить параметры устройства.

2. Выберите устройство контроля доступа, чтобы отобразить его параметры на странице справа .
3. Нажмите **ON** («Вкл.»), чтобы включить соответствующую функцию.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Включить ANR

После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

Включение распознавания M1-карты

После активации этой функции устройство сможет распознавать M1-карты. Поднесите M1-карту к устройству.

Активация распознавания EM-карты

После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

Активация распознавания CPU-карты

Зарезервировано. После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

Активация распознавания ID-карты

Зарезервировано. После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

4. Нажмите **ОК**.

5. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Настройка параметров двери

После добавления устройства контроля доступа можно настроить параметры его точки доступа (двери).

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Выберите устройство контроля доступа на панели слева, а затем нажмите , чтобы показать двери или этажи выбранного устройства.
3. Выберите дверь или этаж, чтобы отобразить его параметры в правой части экрана.
4. Измените параметры двери или этажа.



Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Название

Выберите наименование считывателя карт по своему выбору.

Дверной контакт

Установите датчик двери в режим **Remaining closed** («Оставить открытым») или **Remaining open** («Оставить закрытым»). По умолчанию активирован режим **Remaining closed** («Оставить открытым»).

Тип кнопки выхода

Установите кнопку выхода в режим **Remaining closed** («Оставить открытым») или **Remaining open** («Оставить закрытым»). По умолчанию активирован режим **Remaining open** («Оставить закрытым»).

Длительность открытого состояния

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Тревога тайм-аута открытой двери

Тревога срабатывает, если дверь не будет закрыта в течение заданного периода времени. Тревога не срабатывает, если установлено значение «0».

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

5. Нажмите **Advanced** («Расширенные настройки»), чтобы настроить дополнительные параметры.

Увеличение длительности открытого состояния

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Код принуждения

Дверь может быть открыта при помощи кода принуждения. При этом клиент может создать уведомление о событии принуждения.

Включение блокировки двери при закрытии двери

Дверь может быть заблокирована после ее закрытия, даже если порог блокировки двери не достигнут.

Код отклонения

Создайте код отклонения, который можно использовать для отключения зуммера считывателя карт (путем ввода кода отклонения на клавиатуре).



Примечание

- Суперпароль должен отличаться от кода принуждения.
- Суперпароль и код принуждения должны отличаться от пароля аутентификации.
- Длина суперпароля и кода принуждения установлена устройством. Обычно пароль должен содержать от 4 до 8 цифр.

-
6. Нажмите **ОК**.

7. **Опционально.** Нажмите **Copy to** («Копировать на») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.



Примечание

Настройки состояния двери и этажа будут также применены к выбранной двери.

Настройка параметров считывателя карт

После добавления устройства контроля доступа можно настроить параметры его считывателя карт.

Шаги

1. Нажмите **Access Control** → **Advanced Function** → **Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Выберите устройство контроля доступа на панели слева, а затем нажмите , чтобы показать двери или этажи выбранного устройства.

3. Затем измените основные параметры данного устройства, приведенные на соответствующей странице.



Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа. Ниже приведены некоторые параметры. Подробная информация представлена в руководстве пользователя устройства.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Название

Выберите наименование считывателя карт по своему выбору.

Интервал аутентификации по карте

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.

Активация предела неудачных попыток аутентификации

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

Тип считывателя карт / описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

4. Нажмите **Advanced** («Расширенные настройки») и настройте другие параметры.

Включение считывателя карт

Включите функцию для их использования на считывателе карт.

Правильная полярность светодиода / Ошибочная полярность светодиода / Полярность бипера

Настройте **OK LED Polarity** («Правильная полярность светодиода») / **Error LED Polarity** («Ошибочная полярность светодиода») / **Buzzer Polarity** («Полярность бипера») основной платы в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

Полярность бипера

Настройте **Buzzer Polarity** («Полярность бипера») основной платы в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

Время зуммера

Настройте время зуммера для считывателя карт. Доступный диапазон времени: от 0 до 5 999 с. 0 представляет непрерывный зуммер.

Максимальный 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.

Тревога тампера

Включите детектор саботажа на считывателе карт.

Связь с панелью управления

Если устройство контроля доступа не может подключиться к считывателю карт в течение установленного времени, считыватель карт отключится автоматически.

Уровень распознавания отпечатков пальцев

Из выпадающего списка выберите уровень распознавания отпечатков пальцев.

5. Нажмите **ОК**.

6. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите считыватель карт, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Настройка параметров тревожного выхода

Настройте параметры тревожного выхода после добавления устройства контроля доступа.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает тревожный выход.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»), чтобы перейти на соответствующую страницу.
2. Нажмите кнопку  в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, выберите тревожный вход и настройте его параметры на панели справа.
3. Настройте параметры тревожного выхода.

Имя

Выберите наименование считывателя карт по своему выбору.

Время работы тревожного выхода

Время работы тревожного выхода после активации.

4. Нажмите **ОК**.

5. **Опционально.** Установите переключатель в верхнем правом углу в положение ON («Вкл.»), чтобы активировать тревожный выход.

9.7.8 Настройка параметров устройства

После добавления устройства контроля доступа можно настроить параметры его сети.

Включить шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Шаги



Примечание

Устройство контроля доступа и считыватель карт должны поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **M1 Card Encryption** («Шифрование карты M1»), чтобы открыть страницу «Шифрование карты M1».
4. Установите переключатель в положение **On** («Вкл.»), чтобы включить функцию шифрования M1-карты.
5. Установите идентификатор сектора.
Диапазон яркости от 1 до 100.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

9.8 Управление состоянием двери

Состояние двери добавленного устройства контроля доступа будет отображаться в режиме реального времени в модуле **Monitoring** («Мониторинг») добавленного устройства контроля доступа. Также можно управлять дверью, например, открывать / закрывать дверь или оставлять дверь открытой / закрытой удаленно через клиентское ПО. События доступа отображаются в этом модуле в режиме реального времени. Здесь можно просматривать информацию о допуске и данные пользователей.



Примечание

Пользователь с разрешением на управление дверью может войти в модуль мониторинга и осуществлять управление дверью. Для других пользователей панель управления устройством отображаться не будет. Подробная информация о настройке разрешения пользователя представлена в разделе **Управление пользователями**.

9.8.1 Управление состоянием двери

Можно контролировать состояние одной двери, включая открытие двери, закрытие двери, оставление двери открытой и оставление двери закрытой.

Шаги

1. Нажмите **Monitoring** («Мониторинг») для перехода на соответствующую страницу.

2. В правом верхнем углу выберите группу точки доступа.



Примечание

Подробная информация об управлении группой точек доступа представлена в разделе *Управление группами* Руководства пользователя клиентского программного обеспечения.

На экране будут отображены двери в выбранной группе контроля доступа.

3. Нажмите на значок двери, чтобы выбрать ее, или нажмите **Ctrl** и выберите несколько дверей.
4. Нажимайте следующие кнопки, чтобы управлять дверью.

Открыть дверь

Разблокируйте дверь, чтобы открыть ее на определенный промежуток времени. По истечении заданного времени дверь будет автоматически заблокирована.

Закрыть дверь

Когда дверь открыта, заблокируйте ее. Пользователь с соответствующим разрешением может получить доступ к двери с помощью учетных данных.

Оставить дверь открытой

Дверь будет разблокирована (из открытого или закрытого состояния). Для доступа к двери не требуется предъявление учетных данных.

Оставить дверь закрытой

Дверь будет закрыта и заблокирована. Дверь будет недоступна даже для пользователей с соответствующими разрешениями, за исключением суперпользователей.

Захват

Захват изображения вручную.



Примечание

Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата изображений. Изображение сохраняется на компьютере, на котором работает клиентское ПО. Для настройки параметров сохранения обратитесь к разделу *Настройка звукового сигнала* руководства пользователя клиентского программного обеспечения.

Результат

Иконки дверей изменятся в режиме реального времени, если операция завершена успешно.

9.8.2 Проверка записей о считывании карт в режиме реального времени

Записи доступа будут отображаться в режиме реального времени, включая записи считывания карт, записи сравнения отпечатков пальцев и т. д. Можно просмотреть информацию о сотруднике / посетителях и просмотреть изображение, сделанное во время получения доступа.

Шаги

1. Нажмите **Monitoring** («Мониторинг») и выберите группу из списка в правом верхнем углу. Записи событий доступа, сработавших на дверях в выбранной группе, будут отображаться в режиме реального времени. Здесь можно просмотреть подробную информацию о записях, включая номер карты, имя сотрудника, организацию, время события и т. д.

2. **Опционально.** Выберите тип и статус события, чтобы отобразить их в списке при обнаружении событий. События, тип и состояние которых не установлены, не будут отображаться в списке.
 3. **Опционально.** Установите флажок **Show Latest Event** («Показать последнее событие»), и последняя запись доступа будет выбрана и отображена в верхней части списка записей.
 4. **Опционально.** Нажмите на событие, чтобы просмотреть сведения о пользователе, в том числе изображения пользователя (захваченное изображение и изображение профиля), номер карты пользователя, имя пользователя, наименование организация, телефон, контактный адрес и т. д.
-



Примечание

Дважды нажмите на захваченное изображение, чтобы увеличить его и рассмотреть в деталях.

5. **Опционально.** Нажмите правой кнопкой мыши на название колонки события доступа в таблице, чтобы отобразить или скрыть колонку.

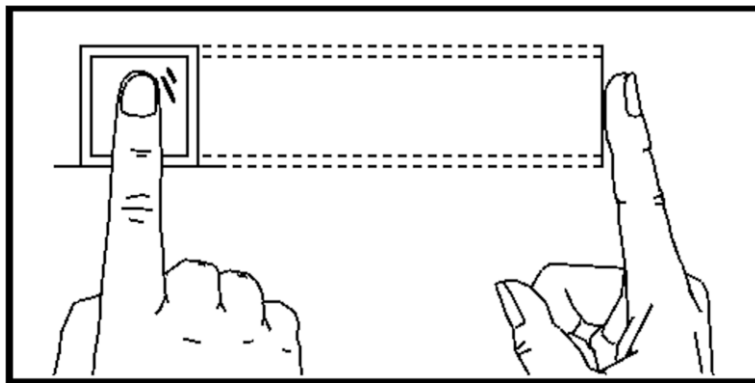
Приложение А. Рекомендации по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

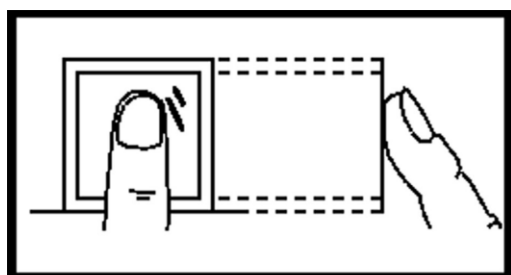
На рисунке ниже показан правильный способ сканирования пальца:



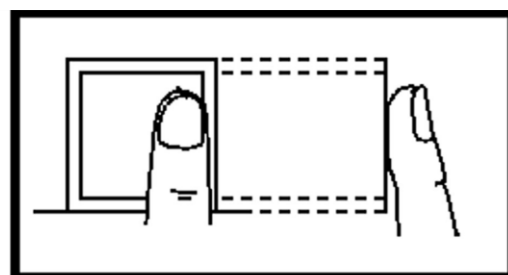
Вы должны прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

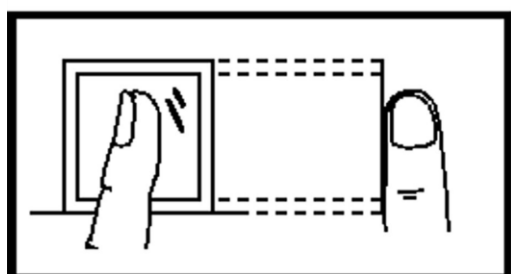
Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



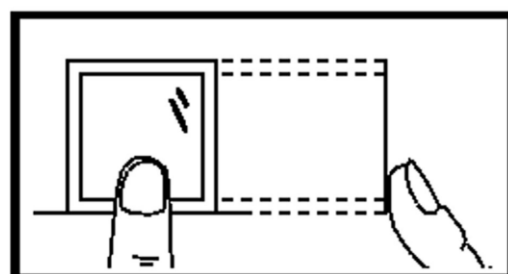
Vertical



Edge I



Side



Edge II

Английский язык	Русский язык
Vertical	Вертикально
Edge	Край
Side	Боковая поверхность

Окружающая среда

Не подвергайте сканер воздействию прямых солнечных лучей, высоких температур, влажных условий и дождя. Когда палец сухой, сканер может не распознать отпечаток пальца. Можно подуть на палец и снова приложить его к сканеру.

Другое

Если у вас неглубокий отпечаток пальца или его сложно сканировать, рекомендуется использовать другие методы аутентификации.

Если на сканируемом пальце есть травмы, сканер может его не распознать. Можно использовать другой палец и повторить попытку снова.

Приложение В. Описание DIP-переключателей

Расположение переключателей от № 1 до № 8 означает расположение от младшего бита к старшему.



Когда переключатель находится в положении **ON** («ВКЛ.»), это означает, что переключатель включен, в противном случае переключатель выключен. Если вы установите DIP-переключатели, как показано на рисунке ниже, двоичное значение будет равно 00001100, а десятичное значение равно 12.



Приложение С. Пользовательская настройка Wiegand

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

Имя настраиваемого Wiegand	Wiegand 44				
Общая длина	4444				
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

Данные Wiegand = действительные данные + данные четности

Общая длина

Длина данных Wiegand.

Правило комбинации

4 байта. 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 и длина контроля нечетности

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

Контроль на четность и длина

Если выбрать **Even Parity** («Контроль на четность»), данные элементы будут доступны. Если старт-бит контроля четности равен 12, а длина равна 12, тогда система начнет расчет проверки четности с бита 12. Будет вычислено 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.