

Руководство пользователя
Вызывная панель VTO3211D-P

V1.0.0

Содержание

Содержание	2
Декларация о безопасности в киберпространстве и рекомендации	1
Декларация о безопасности в киберпространстве	1
Рекомендации по информационной безопасности	1
1 Общие сведения об изделии	1
1.1 Характеристики устройства	1
1.2 Подключение к сети	1
2 Конструкция	2
2.1 Передняя панель	2
2.2 Задняя панель	3
3 Монтаж и наладка	5
3.1 Подключение устройства	5
3.2 Установка	5
3.2.1 Технические характеристики винтов	5
3.2.2 Установочные размеры	6
3.2.3 Порядок установки	7
3.3 Наладка	9
3.3.1 Подготовка к наладке	9
3.3.2 Установка вызывной панели	9
3.3.3 Внутреннее управление	10
3.3.4 Наладка	13
4 Настройка веб-интерфейса	1
4.1 Вход и выход из веб-интерфейса	1
4.1.1 Вход в систему	1
4.1.2 Выход из системы	1
4.2 Конфигурация системы	2
4.2.1 Локальная конфигурация	2

4.2.2	Конфигурация локальной сети (LAN).....	8
4.2.3	Внутреннее управление	9
4.2.4	Конфигурация сети.....	12
4.2.5	Настройка видео.....	1
4.2.6	Управление пользователем	3
4.2.7	IP-камера.....	5
4.2.8	Установка UPnP.....	6
4.3	Поиск информации	7
4.3.1	История вызовов	7
4.3.2	Запись при возникновении тревоги.....	7
4.3.3	Запись о снятии блокировки.....	8
4.4	Статистика статусов	8
4.4.1	Статус видеодомофона	8
5	Общие сведения о функциях.....	10
5.1	Просмотр	10
5.2	Разговор.....	10
5.3	Функция снятия блокировки	10
5.4	Восстановление	10
	Приложение 1. Технические характеристики	11

Декларация о безопасности в киберпространстве и рекомендации

Декларация о безопасности в киберпространстве

- Подключая ваше устройство к сети Интернет, вы несете ответственность за возникающие при этом риски, включая кибератаки, хакерские проникновения, компьютерные вирусы и вредоносное ПО и т. д. Принимайте необходимые меры для защиты ваших данных и персональной информации: изменяйте пароль, установленный по умолчанию, используйте в качестве пароля надежные комбинации, периодически обновляйте пароль, следите за актуальностью прошивки и т. д. Dahua не несет ответственности за нарушения в работе оборудования, утечку информации или прочие проблемы, обусловленные недостаточностью мер безопасности для защиты ваших устройств. Наша компания предоставляет услуги по техническому обслуживанию изделий.
- В той мере, в какой это допускается соответствующими законами, компания Dahua и ее сотрудники, лицензиаты и дочерние предприятия не несут ответственности за телесные повреждения или какие-либо случайные, преднамеренные, косвенные или сопутствующие убытки, включая (без ограничений) убытки в результате потери прибыли, коррупции или утраты данных, невозможности передать или получить те или иные данные, перерыва в производственной деятельности, а также любые другие коммерческие убытки или издержки, возникшие в результате использования настоящих продуктов и услуг или связанные с их использованием или невозможностью их использования, вне зависимости от того, чем она вызвана, а также причин и видов ответственности (договорной, внедоговорной или др.), даже если о возможности таких последствий было сообщено заранее. Некоторые системы юрисдикции не допускают исключения или ограничения ответственности за телесные повреждения, случайные или сопутствующие убытки, поэтому данное ограничение может не иметь к вам отношения.
- Ни при каких обстоятельствах сумма ответственности за все убытки (кроме случаев, обусловленных соответствующими законами в случаях, включающих телесные повреждения) не может превышать стоимости продуктов и услуг.

Рекомендации по информационной безопасности

Обязательные меры, которые должны быть приняты для обеспечения информационной безопасности

1. Изменение паролей и использование надежных паролей

Основная причина взлома систем – использование слабых паролей или паролей по умолчанию. Dahua рекомендует немедленно менять пароли по умолчанию и по возможности выбирать надежный пароль. Надежный пароль должен состоять как минимум из 8 символов и включать в себя специальные символы, цифры и буквы верхнего и нижнего регистра.

2. Обновление прошивки

Обновление прошивки – стандартная техническая процедура, которую мы рекомендуем для СВР, ЦВР и IP-камер, чтобы поддерживать последнюю версию системы с исправлениями и обновлениями безопасности.

Следите за актуальностью прошивки используемых вами устройств. Если прошивка была выпущена более 18 месяцев назад, обратитесь к сертифицированному дистрибьютору Dahua в вашем регионе или в отдел технической поддержки Dahua для получения доступных обновлений.

Дополнительные рекомендации по улучшению сетевой безопасности

1. Регулярно меняйте пароли

Регулярно меняйте учетные данные на своих устройствах, чтобы гарантировать, что только авторизованные пользователи смогут получить доступ к системе.

2. Измените HTTP и TCP-порты по умолчанию

- Измените порты HTTP и TCP, заданные по умолчанию для систем Dahua. Это два порта, которые используются для связи и просмотра видеопотоков в удаленном режиме.
- Этим портам может быть задан любой номер между 1025–65535. Избегая использования портов по умолчанию, вы снижаете риск того, что посторонние смогут угадать, какие порты вы используете.

3. Включите HTTPS/SSL

Установите SSL-сертификат, чтобы включить HTTPS. Это зашифрует всю связь между вашими устройствами и видеорегистратором.

4. Включите фильтр IP

Включение IP-фильтра предотвратит доступ всех пользователей, за исключением тех, кто использует указанные в системе IP-адреса.

5. Измените пароль ONVIF

На старой прошивке IP-камеры пароль ONVIF не изменяется при изменении учетных данных системы. Вам необходимо либо обновить прошивку камеры до последней версии, либо вручную изменить пароль ONVIF.

6. Перенаправляйте только необходимые порты

- Перенаправляйте только необходимые HTTP и TCP-порты. Не настраивайте перенаправление больших диапазонов портов на устройстве. Не помещайте IP-адрес устройства в демилитаризованную зону (DMZ).
- Не требуется перенаправлять порты отдельных камер, если все они подключены к регистратору на площадке; требуется перенаправить только адрес регистратора.

7. Отключите автоматический вход в SmartPSS

Если вы используете SmartPSS для просмотра своей системы и на компьютере, который используется несколькими людьми, то отключите автоматический вход в систему. Это

повысит уровень безопасности, так пользователи, не имеющие доступа к системе, не смогут войти в нее.

8. Используйте другое имя пользователя и пароль для SmartPSS

Если ваш аккаунт в социальных сетях, банке, электронной почте и т. д. был взломан, то злоумышленники могут попробовать использовать ваши учетные данные для входа в другие системы, например в систему видеонаблюдения. Использование другого имени пользователя и пароля в вашей системе безопасности предотвратит такой сценарий.

9. Ограничение прав гостевых аккаунтов

Если ваша система настроена для нескольких пользователей, убедитесь, что у каждого пользователя есть права на функции, которые им необходимы для выполнения их работы.

10. UPnP

- UPnP автоматически попытается перенаправить порты в маршрутизатор или модем. Обычно это целесообразно. Однако если ваша система автоматически перенаправляет порты, а вы оставляете учетные данные по умолчанию, в вашей системе могут оказаться нежелательные посетители.
- Если вы вручную перенаправляете порты HTTP и TCP в маршрутизатор / модем, эта функция должна быть отключена. Отключение UPnP рекомендуется, если функция не используется.

11. SNMP

Отключите SNMP, если вы его не используете. Если вы используете SNMP, следует включать его только на время отслеживания и тестирования.

12. Многоадресная рассылка

Многоадресная рассылка используется для обмена видеопотоками между двумя регистраторами. В настоящее время нет известных проблем, связанных с многоадресной рассылкой, но если вы не используете эту функцию, ее отключение может повысить безопасность вашей сети.

13. Проверка журнала

Если вы подозреваете, что кто-то получил несанкционированный доступ к вашей системе, вы можете посмотреть системный журнал. Системный журнал покажет вам, какие IP-адреса использовались для входа в систему и какие действия были совершены.

14. Физически ограничьте доступ к устройству

В идеале следует предотвратить любой несанкционированный доступ к вашей системе. Лучший способ достичь этого – установить регистратор в запирающийся ящик, ограничить доступ к серверной стойке или комнате с помощью замка и ключа.

15. Подключите IP-камеры к портам PoE на задней панели СВР

Камеры, подключенные к портам PoE на задней панели СВР, изолированы от внешнего мира и к ним невозможно получить доступ напрямую.

16. Изолируйте сетевые видеорегистраторы и сеть IP-камер

Ваши СВР и IP-камера не должны находиться в вашей общедоступной компьютерной сети. Это предотвратит доступ посетителей или злоумышленников к сети системы безопасности и обеспечит ее надлежащую работу.

Для получения более подробной информации о декларации Dahua о безопасности в киберпространстве и рекомендациях приглашаем вас посетить сайт www.dahuasecurity.com.

1 Общие сведения об изделии

1.1 Характеристики устройства

Металлическая вызывная панель отличается более легкой эксплуатацией и установкой и имеет следующие функции:

- предварительный просмотр в реальном времени на мобильном телефоне;
- звонок и двусторонняя связь с видеодомофоном;
- снятие блокировки двери с помощью карты;
- антивандальная сигнализация.

1.2 Подключение к сети

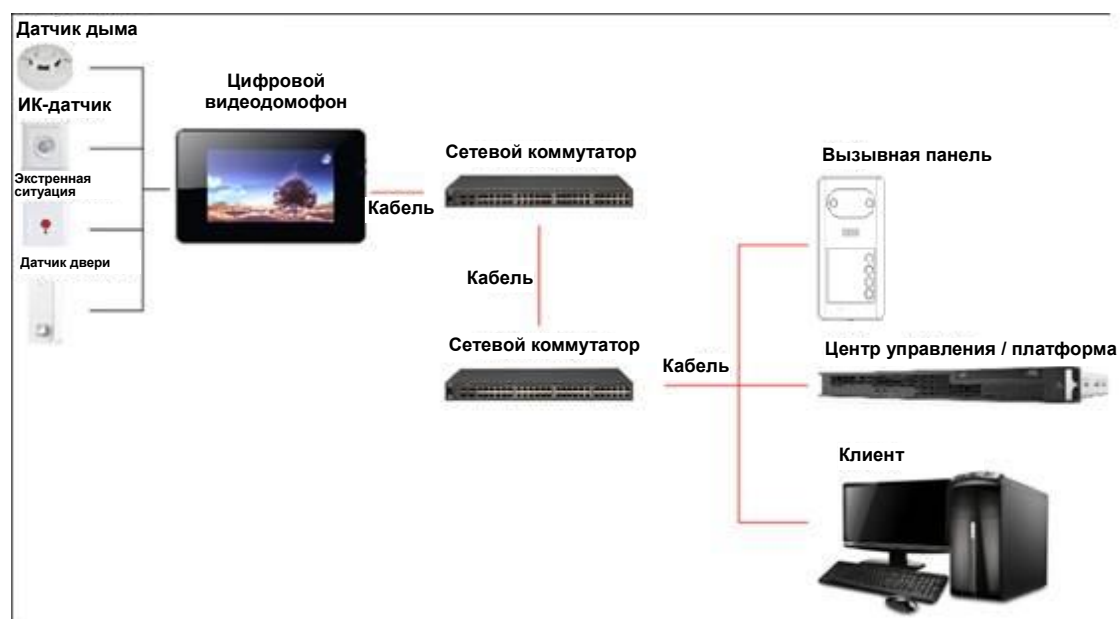


Рисунок 1-1

2 Конструкция

2.1 Передняя панель

Число кнопок на передней панели зависит от модели изделия. Например, модель VTO3211D-P2 имеет две кнопки; модель VTO3211D-P4 имеет четыре кнопки. В качестве примера ниже рассматривается модель VTO3211D-P2.

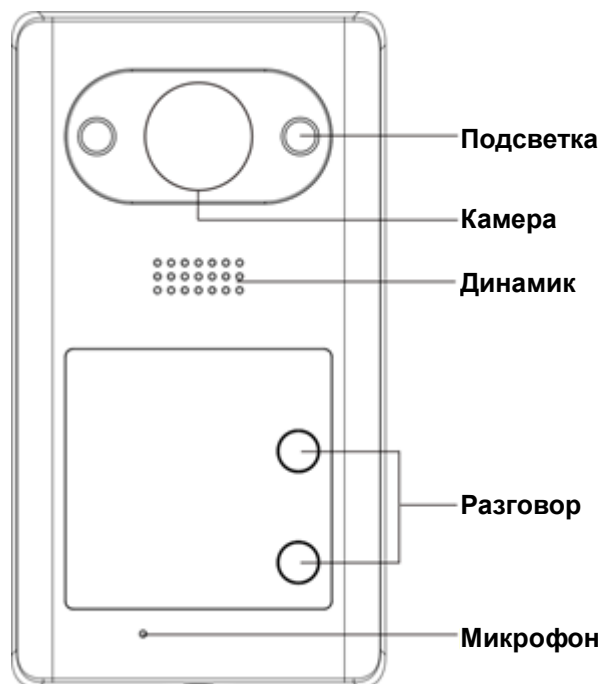


Рисунок 2-1

Название компонента	Описание
Инфракрасная подсветка	Инфракрасная подсветка в темное время суток
Камера	Просмотр зоны вызывной панели
Динамик	Выход звука
Кнопка «Разговор»	Начало разговора Примечание. Модель VTO3211D-P4 имеет 4 кнопки вызова. Две кнопки не отмечены, поэтому не функциональны
Микрофон	Аудиовход

Таблица 2-1

2.2 Задняя панель

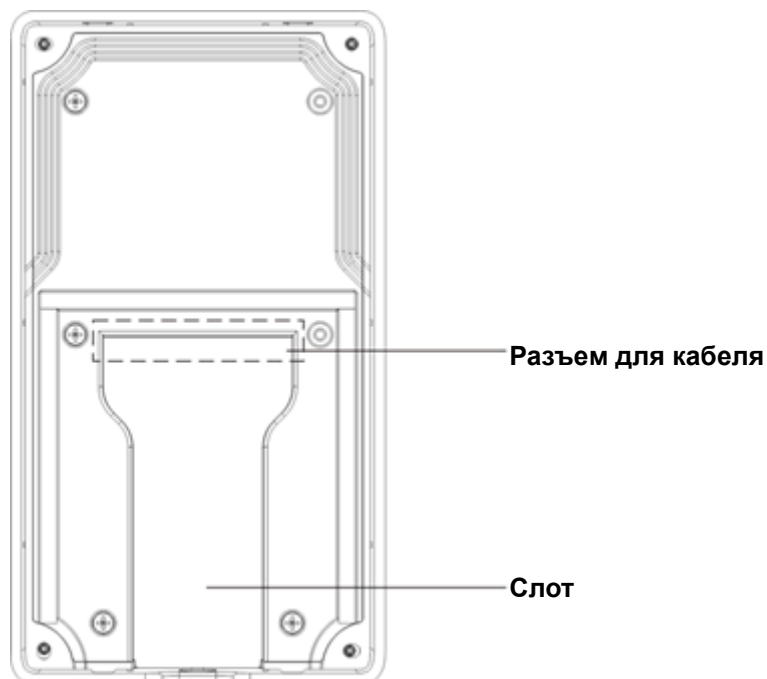


Рисунок 1-1

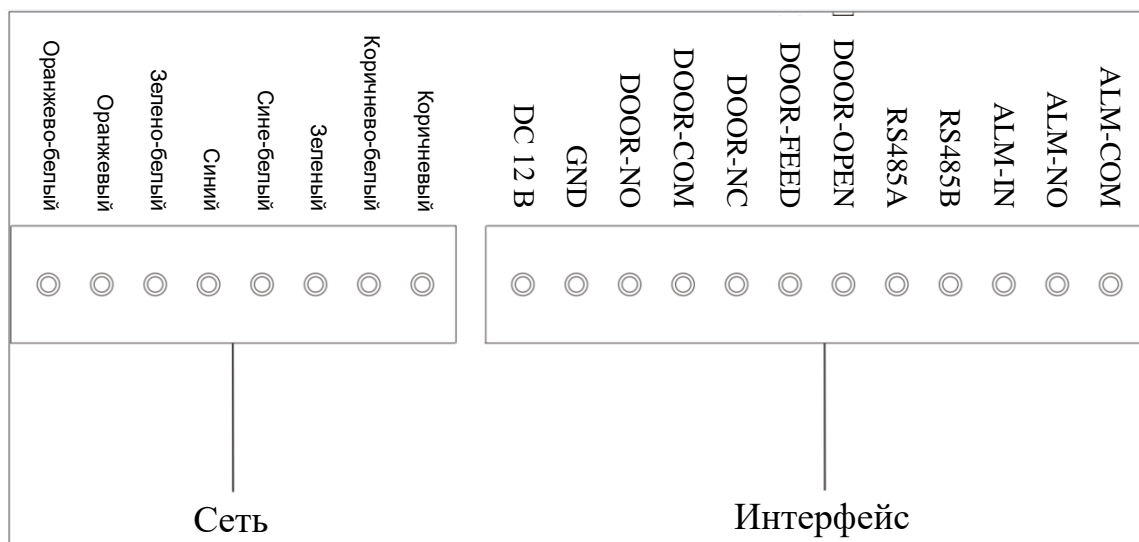


Рисунок 2-2

Маркировка	Примечание
DC 12 В	3 Разъем для кабеля питания 12 В

Маркировка	Примечание
	пост. тока
4 GND	5 Клемма заземления
6 DOOR-NO	7 Порт блокировки двери NO (нормально открытый)
8 DOOR-COM	Порт блокировки общего пользования
9 DOOR-NC	10 Порт блокировки NC (нормально закрытый)
DOOR-FEED	Датчик ОС блокировки двери
DOOR-OPEN	Кнопка снятия блокировки двери
RS485A	Канал передачи данных по интерфейсу RS485
RS485B	
ALM-IN	Тревожный вход
ALM-NO	Тревожный выход
ALM-COM	

Таблица 2-2

3 Монтаж и наладка

3.1 Подключение устройства

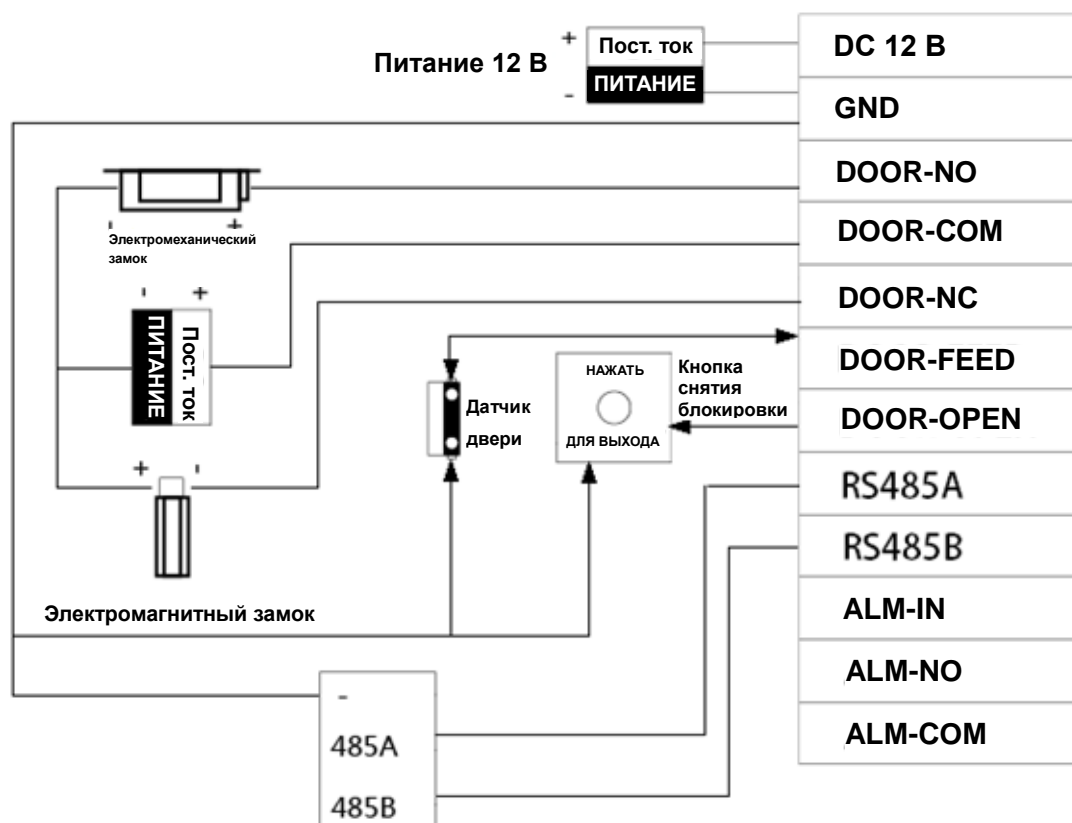


Рис. 3-1

3.2 Установка

Предупреждение

- Устройство должно быть защищено от воздействия неблагоприятных факторов, таких как выпадение конденсата, высокая температура, масляные загрязнения, пыль и т. д.
- Установка и отладка должны выполняться профессиональными сотрудниками. НЕ разбирайте устройство самостоятельно.

3.2.1 Технические характеристики винтов




Название компонента	Рисунок	Количество
Белый дюбель Ф6×30 мм		4
Саморез ST3×20		4
Механический винт М3×6		1

Таблица 3-1

3.2.2 Установочные размеры

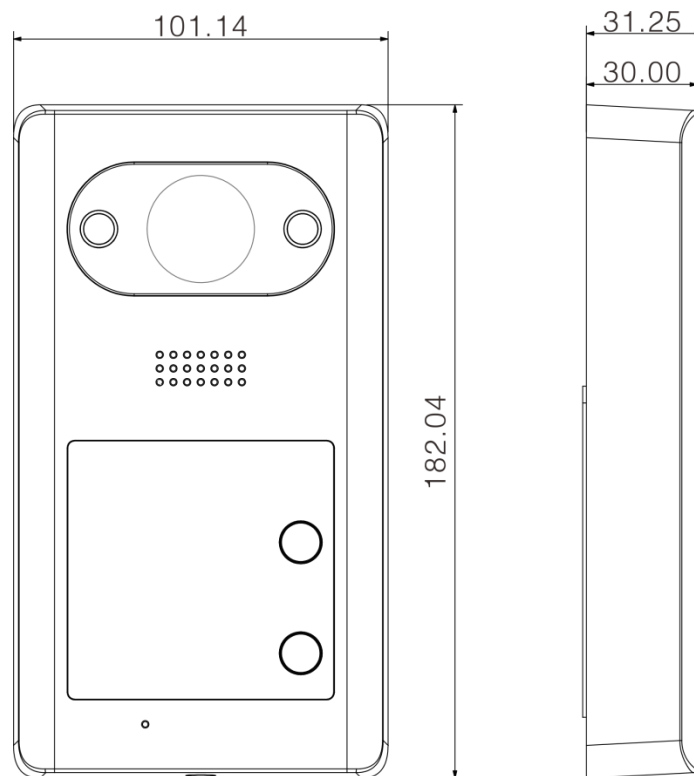


Рисунок 3-2

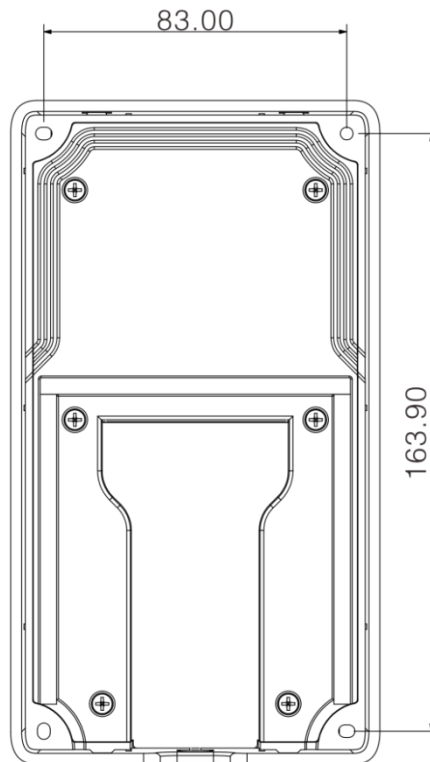


Рисунок 3-3

3.2.3 Порядок установки

Перед началом установки открутите механический винт М3*6 в нижней части устройства, снимите металлический корпус. См. Рисунок 3-4.

Шаг 1. Ориентируясь на расположение четырех отверстий на внутреннем корпусе устройства, просверлите отверстия в монтажной поверхности (например, в стене).

Шаг 2. Вставьте в отверстия дюбели.

Шаг 3. Закрепите внутренний корпус устройства в нужном положении с помощью четырех саморезов.

Шаг 4. Наложите внешний металлический корпус на внутренний в направлении сверху вниз.

Шаг 5. Закрепите защелкой внешний металлический корпус на внутреннем корпусе устройства в его нижней части.

Шаг 6. Зафиксируйте соединение внутреннего и внешнего корпусов устройства с помощью механического винта М3*6.

Примечание.

Рекомендуемая высота от центра устройства до уровня пола составляет от 1,4 до 1,6 м.

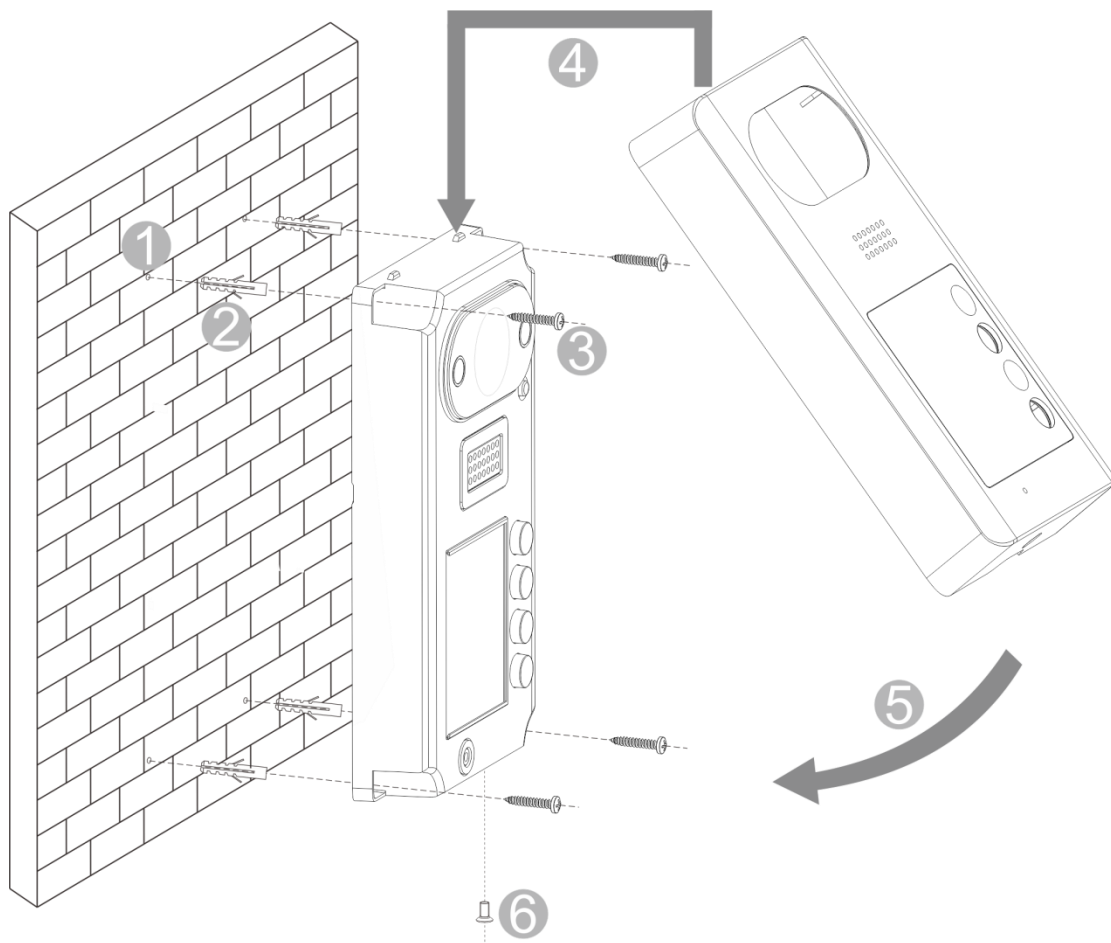


Рисунок 3-4

Вид после установки: Рисунок 3-5.

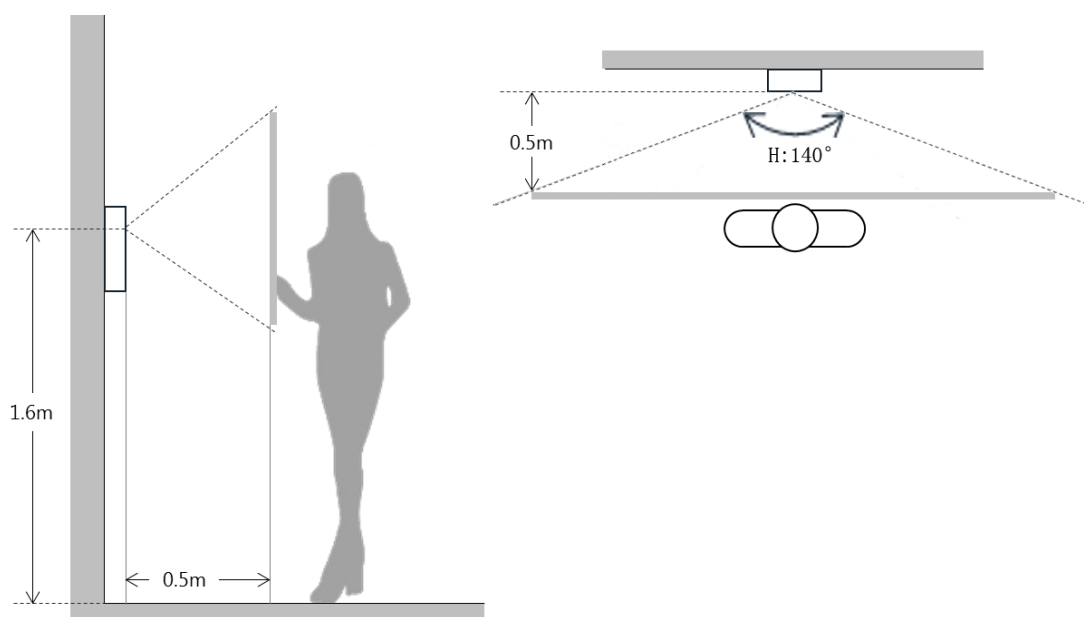


Рисунок 3-5

3.3 Наладка

3.3.1 Подготовка к наладке

Ниже описаны подготовительные действия перед наладкой VTH5221D и видеодомофона с дисплеем 7 дюймов.

- Перед наладкой специалисты должны ознакомиться с порядком установки, подключения и эксплуатации устройства.
- Перед наладкой необходимо проверить проводку на отсутствие короткого замыкания или обрыва в цепи.
- Убедитесь в нормальной работе видеодомофона.

3.3.2 Установка вызывной панели

IP-адрес вызывной панели по умолчанию: 192.168.1.110. Прежде чем приступить к эксплуатации вызывной панели, необходимо изменить IP-адрес на другой, находящийся в одном сегменте с видеодомофоном.

Шаг 1. Подключите питание вызывной панели.

Шаг 2. В поле адреса в браузере введите IP-адрес по умолчанию (192.168.1.110). См. Рисунок 3-6.



Рисунок 3-6

Шаг 3. Введите имя пользователя и пароль, нажмите Login (Войти в систему).

Примечание.

Имя пользователя и пароль по умолчанию – admin и admin. После первого входа в систему измените пароль как можно быстрее. См. п. 4.2.6.3.

Шаг 4. System Config > Network Config > TCP/IP (Конфигурация системы > Конфигурация сети > TCP/IP). См. Рисунок 3-7. Измените IP-адрес вызывной панели на необходимый. См. п. 4.2.4.1.

После завершения модификации произойдет перезагрузка страницы системы и переход по новому IP-адресу для входа в систему.

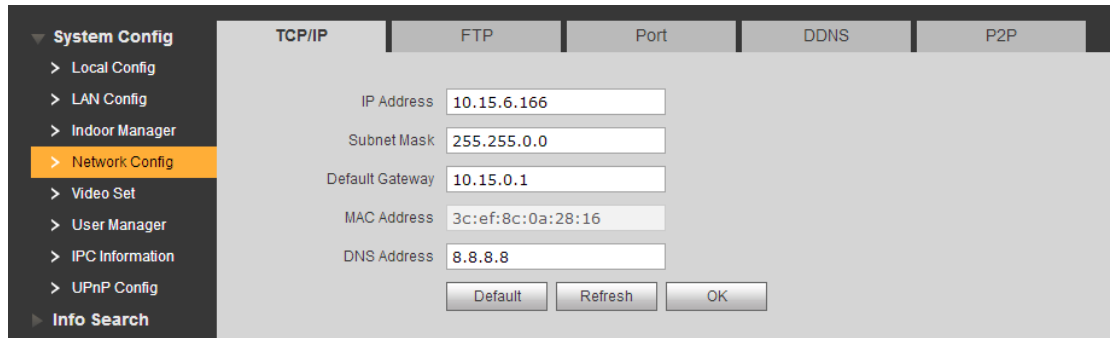


Рисунок 3-7

Шаг 5. Выберите System Config > Indoor Manager > Indoor Manager (Конфигурация системы > Внутреннее управление > Внутреннее управление). См. Рисунок 3-8. Нажмите Add (Добавить) для добавления информации о видеодомофоне.

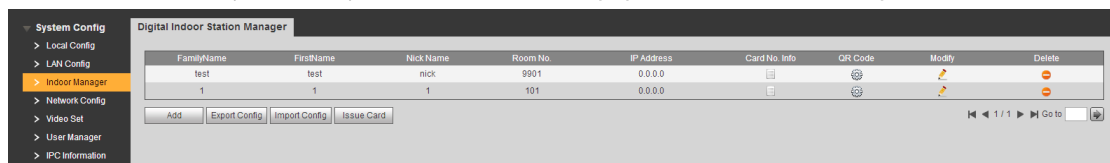


Рисунок 3-8

Шаг 6. Выберите System Config > Local Config > Facase Layout (Конфигурация системы > Локальная конфигурация > План фасада), нажмите на область белого цвета слева и выберите номер помещения видеодомофона. См. Рисунок 3-9.

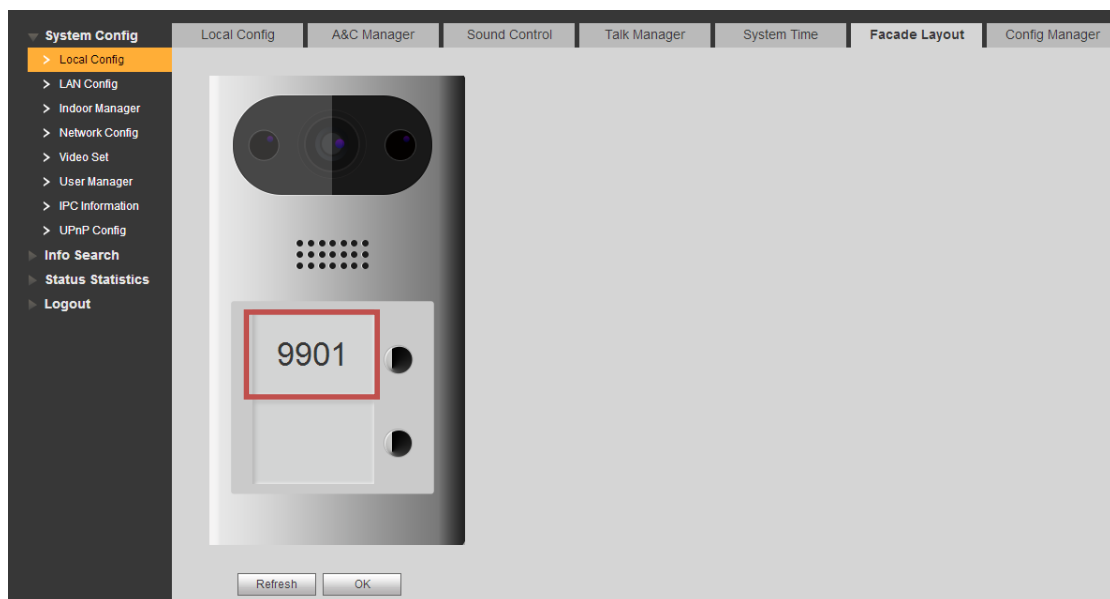


Рисунок 3-9

3.3.3 Внутреннее управление

Шаг 1. Находясь на начальной странице видеодомофона, удерживайте кнопку Setup (Настройки) в течение 6 секунд.

Шаг 2. Введите пароль в интерфейсе проекта видеодомофона.

Шаг 3. Нажмите Network Setup (Настройка сети) для подключения к сети видеодомофона. См.

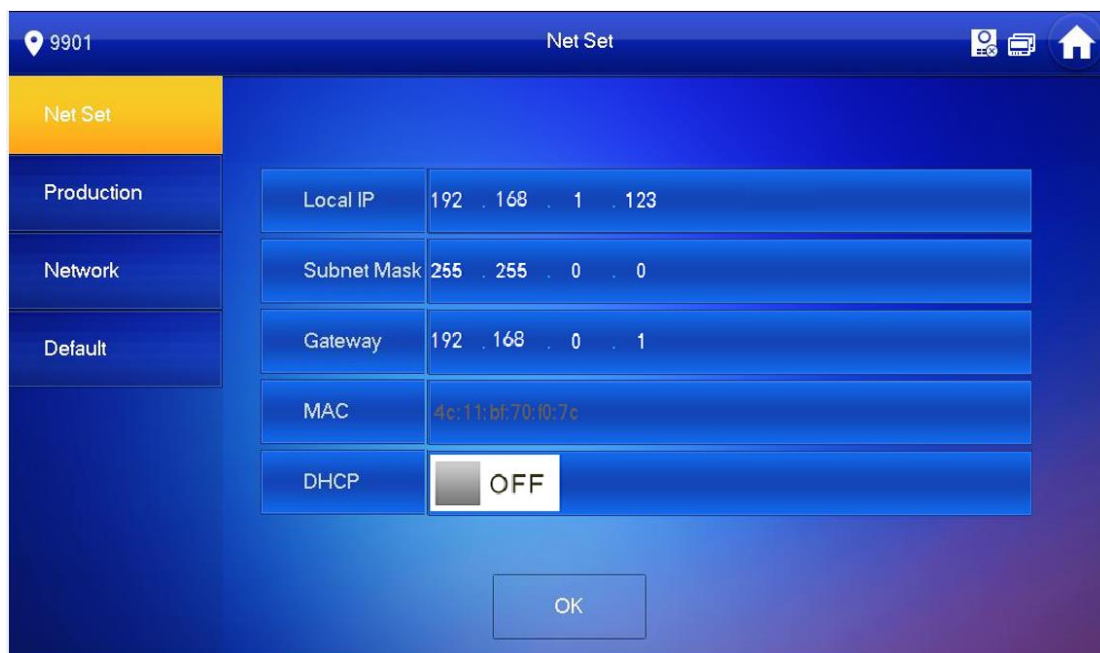



Рисунок 3-10

1. Введите локальный IP-адрес, маску подсети и шлюз видеодомофона.
2. Нажмите ОК.

В правом верхнем углу главной страницы появится значок , означающий успешно установленное соединение.

Примечание.

Вы можете выбрать функцию DHCP для автоматического получения IP-адреса, маски подсети и шлюза. Затем нажмите ОК.

Шаг 4. Нажмите Local Info (Локальная информация) для установки номера помещения видеодомофона.

См. Рисунок 3-11.

Примечание.

Номер помещения видеодомофона должен совпадать с коротким номером видеодомофона. Выполните настройку в сети вызывной панели, см. п. 4.2.3.

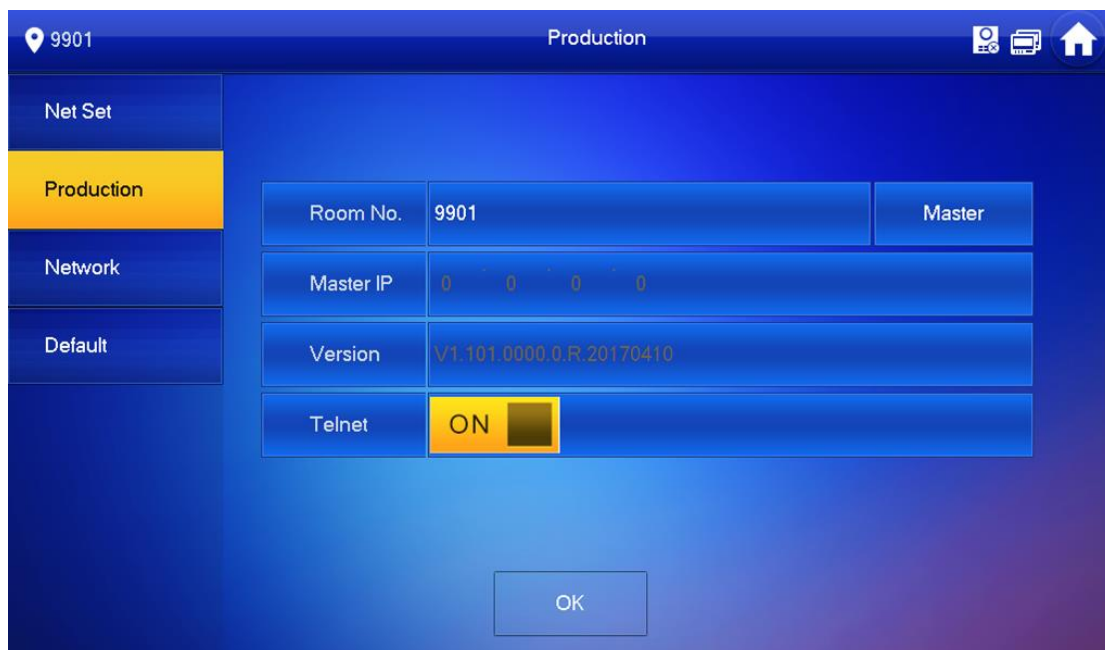


Рисунок 3-11

- Если данный видеодомофон установлен в качестве главного, выберите хост. Введите номер помещения, нажмите OK, чтобы сохранить изменения. См. Рисунок 3-11.
 - Если данный видеодомофон установлен в качестве дополнительного, выберите дополнение. Введите номер помещения дополнения и IP-адрес хоста. Нажмите OK для сохранения.
- Шаг 5. Для настройки информации о вызывной панели нажмите Network (Сеть). См. Рисунок 3-12.

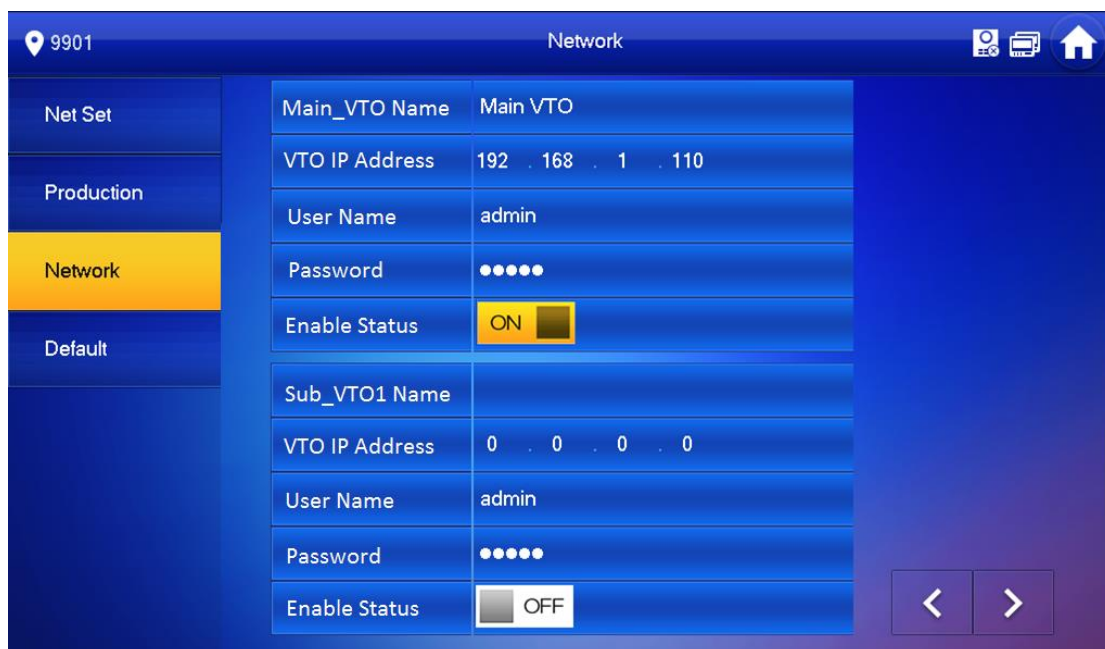


Рисунок 3-12

1. Введите имя и IP-адрес вызывной панели, чтобы установить хост / дополнение.
2. Измените статус на ВКЛ.

3.3.4 Наладка

Нажмите кнопку на вызывной панели для привязки к видеодомофону и позвоните на этот видеодомофон. На дисплее видеодомофона появятся кнопки просмотра видео и управления, см. Рисунок 3-13. Теперь наладка успешно завершена.



Рисунок 3-13

4 Настройка веб-интерфейса

В настоящем разделе описан веб-интерфейс вызывной панели и его параметры, а также порядок их конфигурации.

4.1 Вход и выход из веб-интерфейса

4.1.1 Вход в систему

Шаг 1. В поле адреса в браузере ПК введите необходимый IP-адрес. См. Рисунок 4-1.

Примечание.

IP-адрес вызывной панели по умолчанию: 192.168.1.110. См. п. 4.2.4.



Рисунок 4-1

Шаг 2. Введите имя пользователя и пароль.

Примечание.

Имя пользователя и пароль по умолчанию – admin и admin. После первого входа в систему измените первоначальный пароль. См. п. 4.2.6.3.

Шаг 3. Для входа в систему нажмите Login (Войти).

4.1.2 Выход из системы

Шаг 1. Выберите Logout > Logout > Logout (Выход > Выход > Выход). См. Рисунок 4-2.

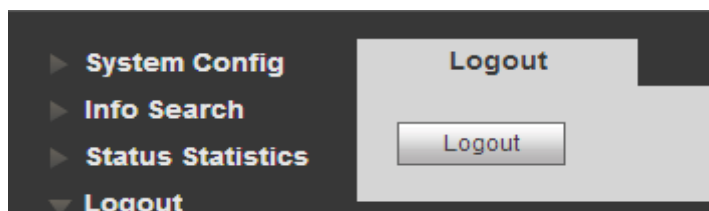


Рисунок 4-2

Шаг 2. Нажмите Logout (Выход).

Вы также можете перезагрузить систему, выбрав Logout > Reboot Device > Reboot Device (Выход > Перезагрузить устройство > Перезагрузить устройство).

4.2 Конфигурация системы

4.2.1 Локальная конфигурация

4.2.1.1 Локальная конфигурация

Выбрав интерфейс System Config > Local Config > Local Config (Конфигурация системы > Локальная конфигурация > Локальная конфигурация), вы можете настроить светочувствительность, яркость и т. д.

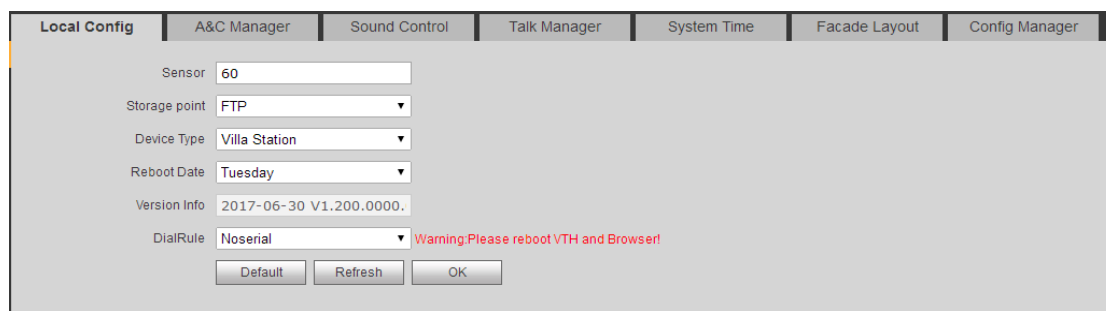


Рисунок 4-1

Параметр	Примечание
Sensor (Датчик)	В темное время суток датчик автоматически активирует подсветку
Storage Point (Место хранения)	Место хранения записей и изображений. Вы можете выбрать FTP-сервер или SD-карту. Установка FTP-сервера описана в п.4.2.4.2
Device Type (Тип устройства)	Выберите тип используемого устройства, например, вызывная панель для загородного дома
Reboot Date (Дата перезагрузки)	Установите дату перезагрузки. По умолчанию это 2:00 каждый вторник
Version Info (Данные версии)	Просмотр номера версии ПО устройства
Dial Rule (Правила набора)	Номер помещения видеодомофона имеет возможность постоянного или прерывистого соединения
Default (По умолчанию)	Нажмите Default для восстановления стандартных настроек всех параметров на этой странице
Refresh (Обновить)	Нажмите Refresh для обновления информации текущего интерфейса
OK	Нажмите OK для сохранения настроек

Таблица 4-1

Параметр	Примечание
Sensor (Датчик)	Настройка светового порога компенсации
Device Type (Тип устройства)	Отображение типа устройства
Reboot Date (Дата перезагрузки)	При наступлении указанной даты произойдет автоматическая перезагрузка устройства
Version Info (Данные версии)	Отображение информации о версии устройства
Default (По умолчанию)	Восстановление только текущей страницы Local Config (Локальная конфигурация) до настроек по умолчанию
Language (Язык)	Доступен выбор из восьми языков

Таблица 4-2

4.2.1.2 Автоматика и контроль

Функция A&C (Автоматика и контроль) главным образом отвечает за контроль интервала отклика при снятии блокировки, периода снятия блокировки и контрольного времени датчика двери.

Рисунок 4-2

Параметр	Примечание
Lock No. (Номер блокировки)	Локальная блокировка и блокировка 485
Unlock Responding Interval (Интервал отклика при снятии блокировки)	Интервал между текущей и последующей блокировкой, измеряется в секундах
Unlock Period (Период разблокировки)	Период, в течение которого дверь остается разблокированной, измеряется в секундах
Door Sensor Check Time (Контрольное время датчика двери)	При использовании только датчика двери отметьте Door Sensor Signal перед блокировкой и установите Door Sensor Check Time для активации.
Отметьте Door Sensor Signal (Проверка сигнала датчика двери) перед блокировкой	Если дверь остается разблокированной в течение времени, превышающего установленное контрольное время датчика двери, срабатывает сигнализация
Auto Snapshot (Автоматический мгновенный снимок)	Выберите Enable (Активировать), и при считывании карты дважды будет выполнена моментальная съемка с загрузкой изображений на FTP или SD-карту
Issue Card (Выдача карты)	Авторизация IC-карты для использования, поддержка до 10 000 карт. См. п. 4.2.1.3
Default (По умолчанию)	Восстановление только текущей страницы A&C (Автоматика) и контроль до настроек по умолчанию
Refresh (Обновить)	Нажмите Refresh для обновления страницы

Таблица 4-3

4.2.1.3 Управление картами

Примечание.

Перед выдачей карты добавьте видеодомофон в соответствии с п. 4.2.3.1.

Шаг 1. System Config > Local Config > A&C (Конфигурация системы > Локальная конфигурация > Автоматика и контроль).

Шаг 2. Нажмите Issue Card (Выдача карты) и приложите IC-карту к считывателю карт. См. Рисунок 4-3.

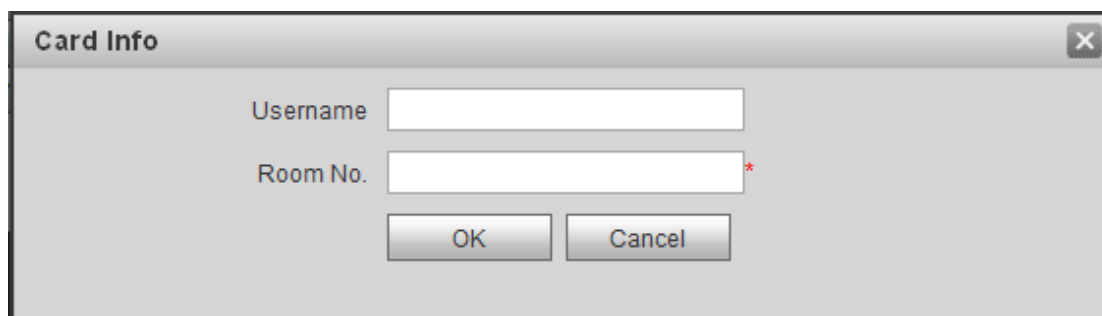



Рисунок 4-3

Шаг 3. Введите соответствующее имя пользователя и номер помещения IC-карты и нажмите OK.

Примечание.

Номер помещения карты должен совпадать с номером помещения на видеодомофоне.

Шаг 4. Нажмите OK. Вы можете выбрать System Config > Indoor Manager > Digital Indoor Station Manager (Конфигурация системы > Внутреннее управление > Управление внутренней цифровой станцией) и нажать  для просмотра.

4.2.1.4 Управление звуком

Выбрав System Config > Local Config > Sound Control (Конфигурация > Локальная конфигурация > Управление звуком), вы можете включить или отключить звук звонка, снятия блокировки, сигнализации и голоса.

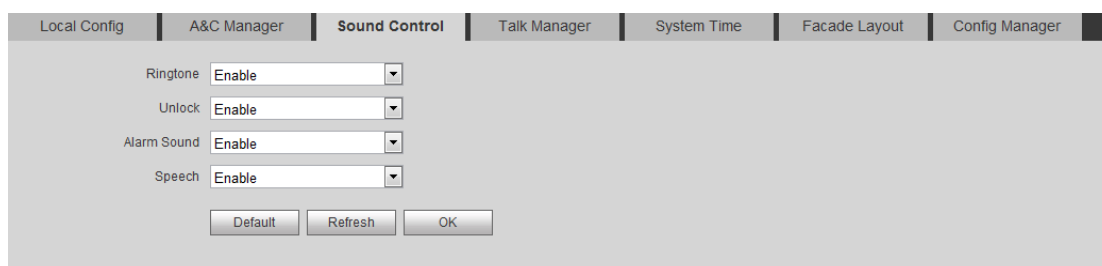


Рисунок 4-4

4.2.1.5 Управление разговором

Устройство поддерживает функцию управления разговором. Вы можете включить или отключить передачу записи разговора, функцию сообщений и автоматического мгновенного снимка.

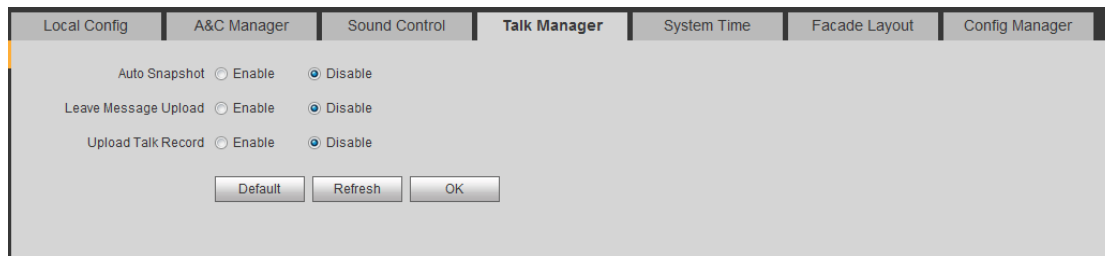


Рисунок 4-5

Параметр	Примечание
Auto Snapshot (Автоматический мгновенный снимок)	Выберите Enable (Активировать), и во время звонка трижды будет выполнена моментальная съемка с загрузкой изображений на FTP или SD-карту
Leave Message Upload (Загрузка оставленного сообщения)	Выберите Enable, и при поступлении с вызывной панели звонка на видеодомофон, если никто не отвечает, вы сможете оставить сообщение, воспользовавшись подсказками. Файл сообщения сохраняется на SD-карте и доступен для просмотра на видеодомофоне. Примечание. Если установлено время 0 секунд, запись сообщения невозможна. При другом значении настройки система предложит оставить сообщение
Upload Talk Record (Загрузка записи разговора)	Выберите Enable для загрузки записи разговора. Вы можете просмотреть запись, выбрав Info Search > Unlock Record > Call Record (Поиск информации > Запись о снятии блокировки > Запись звонка)

Таблица 4-4

4.2.1.6 Системное время

В данном меню вы можете настроить формат даты, формат времени (24 часа и 12 часов) и ввести значения системной даты и времени. Вы также можете нажать Sync PC (Синхронизация с ПК) для синхронизации системного времени со временем ПК. Здесь также можно настроить переход на летнее время.

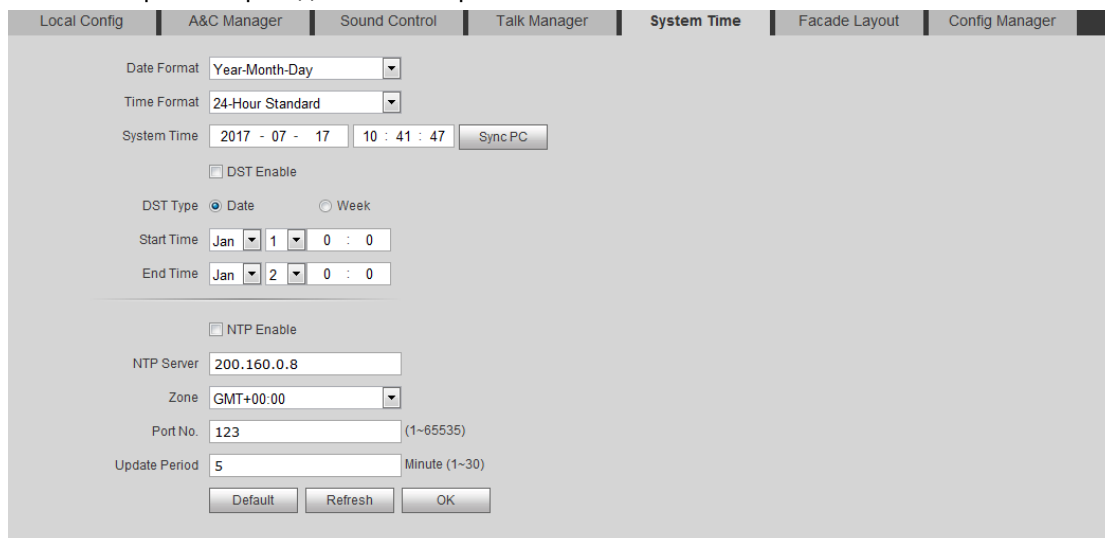


Рисунок 4-3

Параметр	Примечание
Date Format (Формат даты)	Настройка режима отображения даты
Time Format (Формат времени)	Настройка режима отображения времени в формате 12 ч или 24 ч
System Time (Системное время)	Настройка отображения системного времени
Sync PC (Синхронизация с ПК)	Нажмите Sync PC (Синхронизация с ПК) для синхронизации времени с локальным ПК
DST Enable (Включить функцию летнего времени)	Отметьте DST Enable для активации летнего времени. Установите дату начала и конца периода летнего времени
DST Type (Тип летнего времени)	
Start Time (Начальное время)	
End Time (Конечное время)	
NTP Enable (Включить NTP)	Отметьте NTP Enable (Включить NTP) для подключения NTP-сервера. Вы можете настроить ввод IP, часового пояса, номера порта и интервала сервера, где установлен NTP. Настройте синхронизацию времени
NTP Server (Сервер NTP)	
Zone (Зона)	
Port No. (№ порта)	
Update Period (Период обновления)	
Default (По умолчанию)	Нажмите Default для восстановления всех параметров на этой странице до стандартных.
Refresh (Обновить)	Нажмите Refresh для обновления текущей страницы

Таблица 4-5

4.2.1.7 План фасада

Выбрав System Config > Local Config > (Конфигурация системы > Локальная конфигурация >), вы можете определить кнопку для привязки видеодомофона.

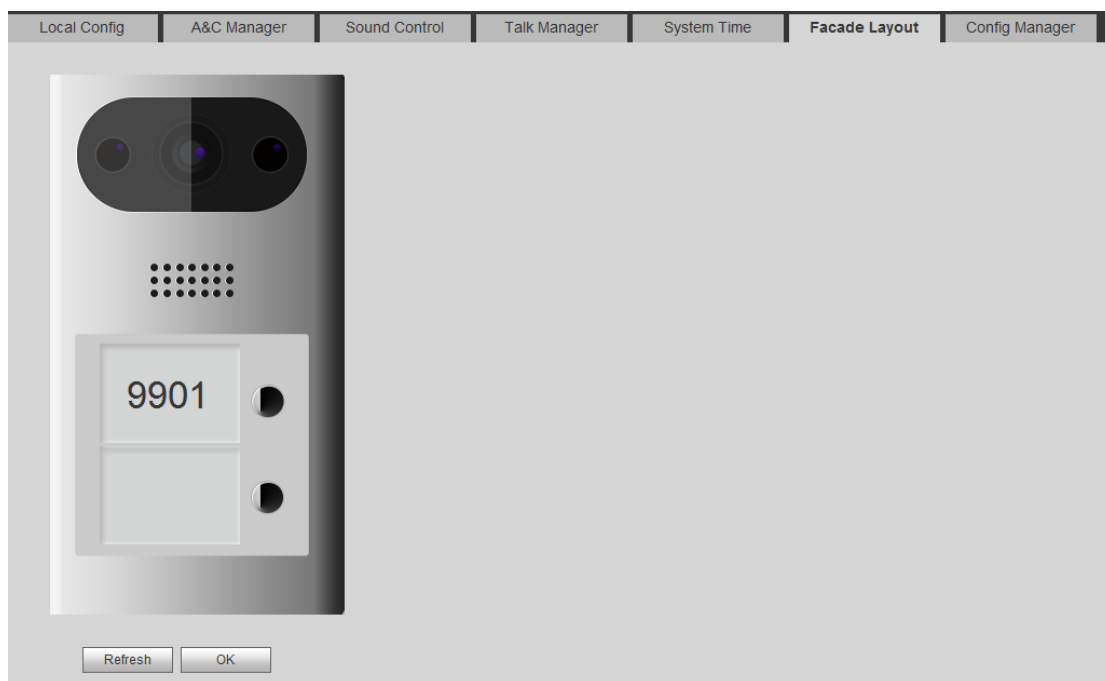


Рисунок 4-6

Нажмите на область белого цвета слева от каждой кнопки, см. . Выберите привязку

помещения видеодомофона к этой кнопке (короткий номер видеодомофона) и нажмите ОК. После привязки, если вы не активировали функцию звонка в центр управления во вкладке LAN Config (Конфигурация LAN), нажмите на эту кнопку для вызова видеодомофона. См. п. 4.2.2.

Примечание.

Нажмите Clear (Очистить) для удаления привязки.

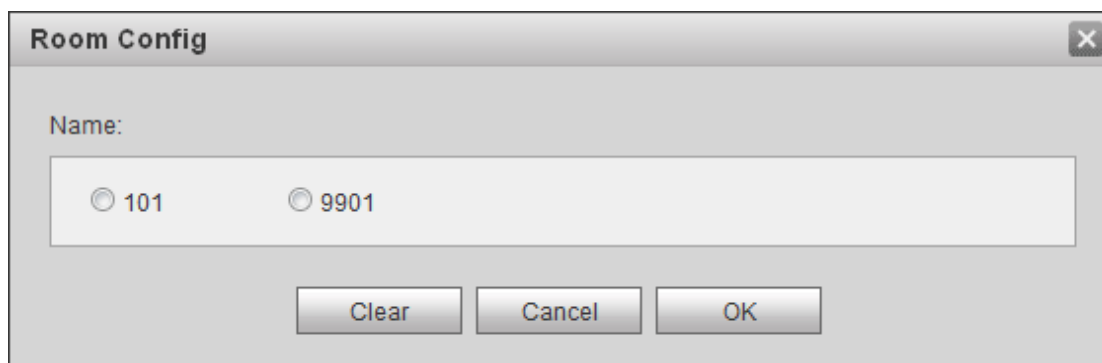


Рисунок 4-7

4.2.1.8 Управление конфигурацией

System Config > Local Config > Config Manager (Конфигурация системы > Локальная конфигурация > Управление конфигурацией).

Вам доступен импорт и экспорт конфигурации или восстановление настроек по умолчанию.

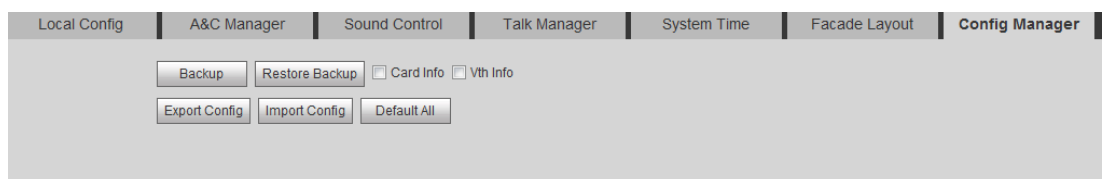


Рисунок 4-4

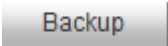
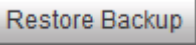
Параметр	Примечание
Backup (Резервирование)	Отметьте card no. (Номер карты) и VTH info (Данные вызывной панели) и нажмите  , чтобы зарезервировать номер карты и данные вызывной панели
Restore Backup (Восстановление и резервирование)	Отметьте параметры card no. и VTH info и нажмите  , чтобы восстановить номер карты и данные вызывной панели. Примечание. Каждый час видеодомофон автоматически сохраняет номер карты и данные видеодомофона в системе, поэтому, если необходимо их восстановить, сделайте это как можно быстрее
Export (Экспорт)	Экспорт файла конфигурации (резервирование конфигурации)
Import (Импорт)	Импорт файла конфигурации
Default (По умолчанию)	Восстановление всех параметров до статуса Default (По умолчанию)

Таблица 4-6

4.2.2 Конфигурация локальной сети (LAN)

Выбрав System Config > LAN Config > LAN Config (Конфигурация системы > Конфигурация LAN > Конфигурация LAN), вы можете настроить номер здания вызывной панели, номер вызывной панели и зарегистрироваться в центре управления. См. Рисунок 4-8.

После завершения конфигурации нажмите Reboot Device (Перезагрузить устройство), перейдя на вкладку Logout > Reboot Device > Reboot Device (Выйти > Перезагрузить устройство > Перезагрузить устройство).

LAN Config

Building No.

Building Unit No.

VTO No.

Max Extension Index Group Call

MGT Centre IP Address Register to the MGT Centre

MGT Port No.

Call VTS Time : To : Call VTS Or Not

NoAnswer Transfer MGT Centre Enable Disable

Alarm Out Enable Disable

Warning:The device needs reboot after modifying the config above.
If extensionCount changed,need reboot VTH and init VTH information again!

Рисунок 4-8

Параметр	Примечание
Building No. (Номер здания)	Укажите номер здания видеодомофона и номер квартиры
Building Unit No. (Номер квартиры)	
VTO No. (Номер вызывной панели)	Номер данной вызывной панели по умолчанию: 6901. При подключении одного видеодомофона к нескольким вызывным панелям вы можете присвоить им номера 6901, 6902, 6903...
Max Extension Index (Максимальный индекс дополнительного устройства)	К одному главному видеодомофону относятся номера дополнительных устройств, максимальным из которых является 5. Предупреждение. После изменения этого параметра вам будет необходимо перезагрузить устройство и настроить информацию о

Параметр	Примечание
	видеодомофоне
Group Call (Групповой вызов)	Отметьте поле group call (Групповой вызов), чтобы звонить на все видеодомофоны в этом помещении
MGT Center IP Address (IP-адрес центра управления)	Введите IP-адрес и номер порта центра управления, отметьте register to MGT center (Зарегистрироваться в центре управления) для регистрации устройства
Register to MGT Center (Зарегистрироваться в центре управления)	
MGT Port No. (Номер порта центра управления)	
Call VTS Time (Время вызова VTS)	После регистрации в центре управления установите период вызова и активируйте функцию звонка в центр управления
Call VTS (Вызов VTS)	Во время установленного периода совершить вызов в центр управления можно будет с помощью любой кнопки. Примечание. В модели VTO3211D-P4 для вызова могут использоваться только кнопки 2 и 4 сверху
No Answer Transfer MGT (Переадресация в центр управления)	Выберите Enable (Активировать), и звонок с вызывной панели на видеодомофон будет переадресован в центр управления, если не получен ответ. Примечание. Если вы активируете эту функцию и установите значение, отличное от нуля, при отсутствии ответа видеодомофона вызов будет направлен в центр управления без записи сообщения
(Default) По умолчанию	Нажмите Default (По умолчанию) для восстановления всех параметров на этой странице до стандартных
Refresh (Обновить)	Нажмите Refresh (Обновить) для обновления текущей страницы

Таблица 4-7

4.2.3 Внутреннее управление

В интерфейсе Indoor Manager (Внутреннее управление) вы можете добавлять, удалять и изменять видеодомофон (внутреннюю цифровую станцию).

4.2.3.1 Добавить видеодомофон

К примеру, чтобы добавить цифровой видеодомофон:

Шаг 1. Во вкладках выберите System Config > Indoor Manager > Digital Indoor Station Manager (Конфигурация системы > Внутреннее управление > Управление внутренней цифровой станцией).

Шаг 2. Нажмите .

Шаг 3. Введите основную информацию о цифровом видеодомофоне. См. Рисунок 4-5.

Рисунок 4-5

Примечание.

Поля, отмеченные *, обязательны для заполнения.

Параметр	Примечание
(Family Name) Фамилия	Ввести имя пользователя
First Name (Имя)	
Nick Name (Сетевое имя)	
VTH Short No. (Короткий номер видеодомофона)	Видеодомофон является внутренним устройством, номер видеодомофона
IP Address (IP-адрес)	Добавить IP-адрес видеодомофона

Шаг 4. Нажмите .

При добавлении видеодомофона будет вызван соответствующий интерфейс системы. См. Рисунок 4-6.

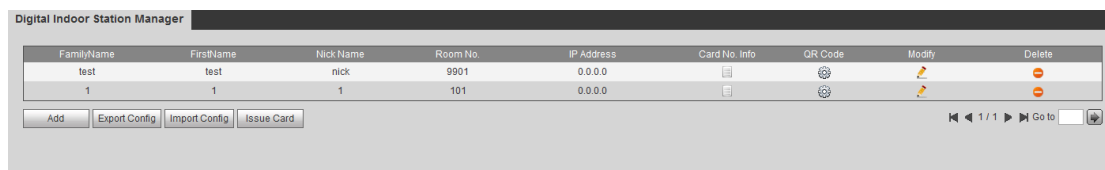





Рисунок 4-6

4.2.3.2 Изменение видеодомофона

- Нажмите  и измените информацию о видеодомофоне во всплывающем окне изменения.
- Нажмите  для удаления цифрового видеодомофона.

4.2.3.3 Просмотр данных карты

См. п. 4.2.1.3.

Нажмите  для просмотра всех авторизованных карт для данного видеодомофона, см. Рисунок 4-9.

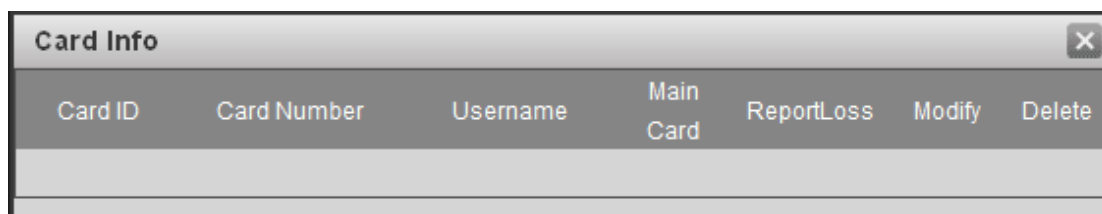


Рисунок 4-9




Параметр	Примечание
Card ID (Идентификация карты)	Отображение номера IC-карты, имени пользователя и номера помещения
Card Number (Номер карты)	
Username (Имя пользователя)	
Main Card (Главная карта)	Отметьте поле main card (Главная карта) и определите данную IC-карту в качестве главной. Примечание. С помощью главной карты проводится авторизация других карт, однако данное устройство не поддерживает эту функцию
Report Loss (Уведомление об утере)	В случае утери IC-карты нажмите  для уведомления об утере. С помощью указанной карты невозможно будет снять блокировку
Modify (Изменить)	Нажмите  для изменения имени пользователя IC-карты
Delete (Удаление)	Нажмите  для удаления этой IC-карты

Таблица 4-8

4.2.3.4 QR-код

Каждый видеодомофон имеет один QR-код, посредством которого пользователь может соединиться с клиентом мобильного телефона посредством P2P, и каждое сообщение может быть передано клиенту.


Нажмите , введите имя пользователя и пароль (по умолчанию имя пользователя и пароль – admin и admin), нажмите ОК для просмотра QR-кода и серийного номера видеодомофона. См. Рисунок 4-10.



Рисунок 4-10

Предупреждение.

После сканирования QR-кода мобильным телефоном и добавления устройством потребуется активация функции P2P вызывной панели. См. п. 4.2.4.5.

4.2.3.5 Импорт / экспорт конфигурации

Вам доступен импорт / экспорт конфигурации видеодомофона или данных карты.

- Нажмите Export Config (Экспорт конфигурации) для экспорта существующей конфигурации видеодомофона или данных карты.
- Нажмите Import Config (Импорт конфигурации) для импорта существующей конфигурации видеодомофона или данных карты.

4.2.4 Конфигурация сети

4.2.4.1 TCP/IP

Вы можете установить параметр IP локальной сети.

Выберите System Config > Network > TCP/IP (Конфигурация системы > Сеть > TCP/IP).

Введите IP-адрес локальной сети, маску подсети и шлюз по умолчанию.

См. Рисунок 4-7.

Рисунок 4-7

Параметр	Примечание
IP Address (IP-адрес)	Введите IP-адрес
Subnet Mask (Маска подсети)	В зависимости от фактической ситуации установите префикс маски подсети в виде номера 1~255, чтобы отметить особое соединение сети, включающее, как правило, одноуровневую структуру
Default Gateway (Шлюз по умолчанию)	В зависимости от фактической ситуации шлюз должен находиться в одном сегменте с IP-адресом
MAC Address (MAC-адрес)	Отображение MAC-адреса устройства
DNS Address (Адрес DNS)	Введите необходимый IP-адрес сервера DNS
Default (По умолчанию)	Нажмите Default (По умолчанию) для восстановления стандартных настроек всех параметров на этой странице
Refresh (Обновить)	Нажмите Refresh (Обновить) для обновления информации текущего интерфейса

Таблица 4-9

4.2.4.2 FTP

Сервер FTP используется для хранения записей, моментальных снимков и т. д. Пользователь может зарегистрироваться на сервере FTP для просмотра и получения фотографий или изображений.

Примечание.

Необходимо приобрести или скачать инструмент FTP и установить ПО на ПК.

Шаг 1. Вы можете перейти на вкладку System Config > Network > FTP (Конфигурация системы > Сеть > FTP), чтобы настроить локальные сетевые параметры FTP.

См. Рисунок 4-8.

Рисунок 4-8

Шаг 2. Настройте параметры интерфейса, см.

Параметр	Примечание
IP Address (IP-адрес)	Установите IP-адрес хоста FTP-сервера
Port No. (№ порта)	По умолчанию: 21
Username (Имя пользователя)	Имя пользователя и пароль для доступа к FTP-серверу
Password (Пароль)	

Таблица 4-10

Шаг 3. Нажмите ОК.

4.2.4.3 Порт

Вы можете установить значение каждого порта.

Шаг 1. System Config > Network > FTP (Конфигурация системы > Конфигурация сети > Порт), см. Рисунок 4-11.

Рисунок 4-11

Шаг 2. Установите значение каждого порта.

Параметр	Примечание
Порт TCP	Протокол связи TCP обеспечивает обслуживание через этот порт. Пользователь может настроить его, значение по умолчанию: 37777
Порт UDP	Порт протокола данных пользователя. Пользователь может настроить его, значение по умолчанию: 37778

Параметр	Примечание
Порт WEB	<p>Настройте порт WEB вызывной панели, значение по умолчанию: 80.</p> <p>Если номер порта занят, вы можете использовать любой порт от 1025 до 65535.</p> <p>Войдите в браузер для доступа к порту WEB вызывной панели</p>
Порт RTSP	<ul style="list-style-type: none"> ● Номер порта RTSP по умолчанию: 554, если не допускается расширение. Пользователи могут применять следующий формат при использовании плагина браузера Apple QuickTime или VLC для просмотра в реальном времени. BlackBerry также имеет поддержку данного параметра. ● Поточковый протокол реального времени: формат URL потока, запрос потока просмотра в реальном времени, передача мультимедийных потоков RTSP. URL должен быть указан в номере канала запроса, тип потока, если требуется информация аутентификации, также необходимо указать имя пользователя и пароль. ● При использовании BlackBerry для доступа режим кодировки потока устанавливается как H.264B, разрешение CIF, аудио отключено. <p>Формат URL определяется следующим образом:</p> <p>Rtsp: // username: password @ ip: port / cam / realmonitor? Channel = 1 & subtype = 0</p> <ul style="list-style-type: none"> ● Username: имя пользователя, например, admin. ● password: пароль, например, admin. ● ip: IP-адрес устройства, например, 10.7.8.122. ● Port: номер порта RTSP по умолчанию: 554, если не допускается расширение. ● channel: номер канала, начиная с 1. Например, номер канала – 2, тогда channel = 2 ● subtype: тип потока, основной поток – 0 (т. е. subtype = 0), дополнительный поток – 1 (т. е. subtype = 1). <p>К примеру, запрос канала 2 потока устройства выглядит следующим образом:</p> <p>Rtsp: // admin: admin@10.12.4.84: 554 / cam / realmonitor? Channel = 2 & subtype = 1</p> <p>Если аутентификация не требуется, имя пользователя и пароль указывать не обязательно, можно использовать следующий формат:</p> <p>Rtsp: // ip: port / cam / realmonitor? Channel = 1 & subtype = 0</p>

Таблица 4-11

Шаг 3. Нажмите ОК.

4.2.4.4 Конфигурация DDNS

DDNS (Динамический сервер доменных имен), динамическое обновление доменного имени и IP-адреса сервера DNS, при котором происходит частая смена IP-адреса. Таким образом, пользователю гарантируется доступ посредством доменного имени.

Предупреждение

- Перед конфигурацией убедитесь, что устройство поддерживает тип DNS, и войдите в

систему, используя соответствующее имя пользователя DDNS, пароль и т. д.

- Пользователь регистрируется на сайте DDNS и входит в систему, а затем получает возможность просмотра всех данных подключенных устройств пользователя.

Шаг 1. Выберите System Config > Network Config > DDNS (Конфигурация системы > Конфигурация сети > DDNS). См. Рисунок 4-12.

Рисунок 4-12

Шаг 2. Отметьте Enable (Включить), чтобы включить функцию сервера DDNS.

Шаг 3. Настройте параметры по таблице ниже.

Параметр	Примечание
Server Type (Тип сервера)	Имя и адрес провайдера DDNS, см. ниже. Адрес Dyndns DDNS: members.dyndns.org
Server Name (Имя сервера)	Адрес DDNS NO-IP: dynupgrade.no-ip.com Поскольку тип сервера должен быть NO-IP DDNS, указывается имя сервера dynupgrade.no-ip.com
Server Port (Порт сервера)	Порт сервера DDNS
Domain (Домен)	Домен зарегистрированного пользователя на сайте провайдера сервера DDNS
User (Пользователь)	Введите имя пользователя и пароль, полученные от провайдера сервера DDNS. Пользователь должен зарегистрироваться на сайте провайдера сервера DDNS (с именем пользователя и паролем)
Password (Пароль)	
DDNS Live Time (Время жизни информации DDNS)	Время жизни информации DDNS

Шаг 4. Нажмите OK для завершения настройки сервера DDNS.

В сетевом браузере ПК введите доменное имя и нажмите Enter (Ввод). Отображение страницы устройства означает успешную работу. Если страница не отобразилась, произошел сбой настройки.

4.2.4.5 P2P

После активации функции P2P клиент мобильного телефона сканирует QR-код в интерфейсе Indoor Manage (Внутреннее управление) для получения серийного номера. Добавьте все домофоны для совместного управления, и вы сможете разговаривать, просматривать записи, снимать блокировку, делать моментальные снимки и записи на клиенте. Вы можете сканировать QR-код для скачивания приложения на мобильный телефон, см. Рисунок 4-13.



Рисунок 4-13

Перейдя на вкладку System Config > Network Config > P2P interface (Конфигурация системы > Конфигурация сети > P2P), выберите Enable P2P server (Активировать сервер P2P) и просматривайте информацию, отсканировав двухмерный код в нижней части интерфейса. См. Рисунок 4-14.

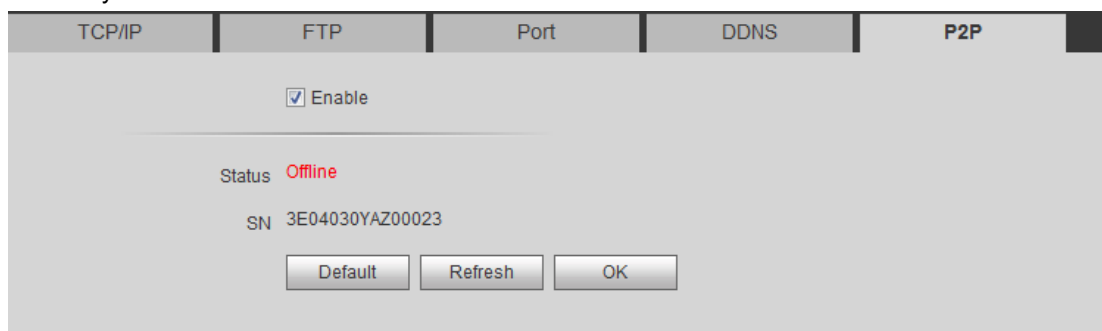


Рисунок 4-14

4.2.5 Настройка видео

4.2.5.1 Настройка видео

Вы можете перейти в интерфейс System Config > Video Set interface (Конфигурация системы > Настройка видео) для настройки видео и аудио.

Выберите System Config > Video Set > Video Set (Конфигурация системы > Настройка видео > Настройка видео).

Отрегулируйте параметры видеозаписи. См. Рисунок 4-15.

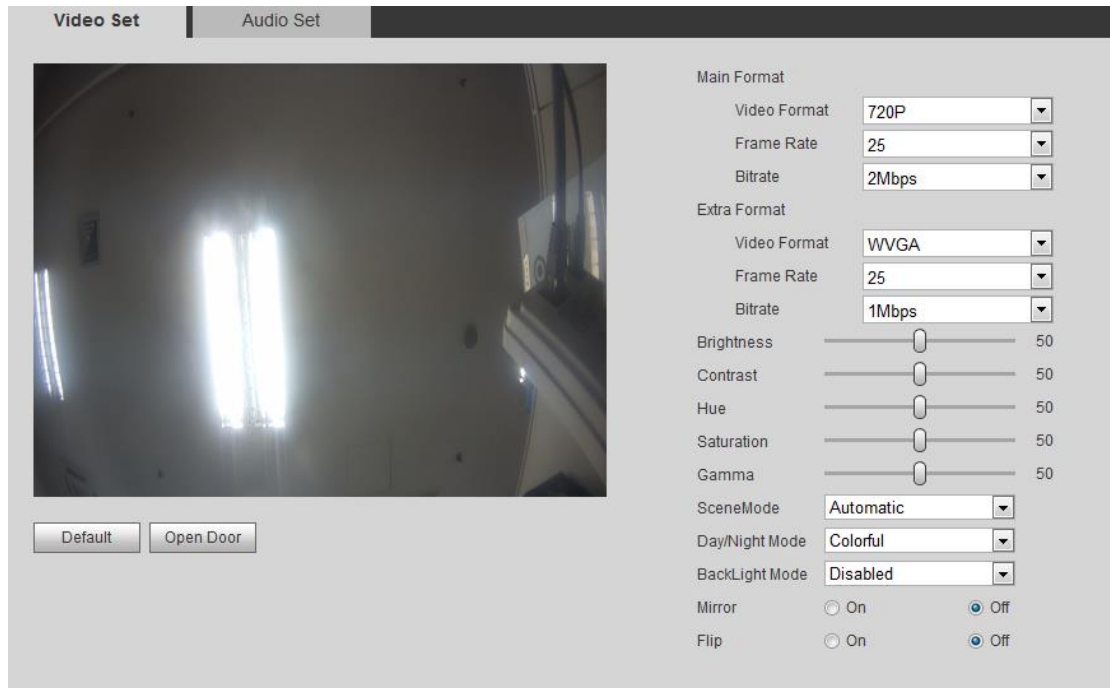


Рисунок 4-15

Примечание.

Если у вас не установлен плагин, установите его с помощью следующих инструкций.

Параметр		Примечание
Main Format (Главный формат)	Video Format (Формат видео)	Настройте разрешение видеоизображения: 720P, WVGA и D1
	Frame Rate (Частота кадров)	Настройте скорость передачи видеоизображения: 3fps, 25fps и 30fps
	Bit Rate (Скорость передачи данных)	С учетом фактического ввода данных устройства выберите скорость передачи данных: 256 кбит/с, 512 кбит/с, 1 Мбит/с, 2 Мбит/с и 3 Мбит/с
Extra Format (Дополнительный формат)	Video Format	Настройте разрешение видеоизображения: WVGA, D1 и QVGA
	Frame Rate	Настройте скорость передачи видеоизображения: 3fps, 25fps и 30fps
	Bit Rate	С учетом фактического ввода данных устройства выберите скорость передачи данных: 256 кбит/с, 512 кбит/с, 1 Мбит/с, 2 Мбит/с и 3 Мбит/с
Brightness (Яркость)		Настройте яркость видео, рекомендуемое значение: 40~60, диапазон: 0~100
Contrast (Контрастность)		Настройте контрастность видео, рекомендуемое значение: 40~60, диапазон: 0~100
Hue (Тон)		Настройте тон и насыщенность изображения
Saturation (Насыщенность)		Настройте насыщенность цвета видео, рекомендуемое значение: 40~60, диапазон: 0~100
Gamma (Гамма)		Настройте отображение нелинейным методом в качестве дополнения к яркости и контрастности

Параметр	Примечание
Scene Mode (Режим сцены)	Выберите режим: automatic, sunny, night («Авто», «Солнце», «Ночь») и т. д.
Day/Night Mode (Режим «День / ночь»)	Включает: цвет, авто и B/W
Back Light Mode (Режим задней подсветки)	Включает: ВЫКЛ, подсветка, WDR, HLC
Mirror (Зеркальное отображение)	Зеркальное отображение изображения
Flip (Поворот)	Горизонтальный поворот изображения
Default (По умолчанию)	Сброс настроек видео и аудио до стандартных
Unlock (Снятие блокировки)	Снятие блокировки через сеть

Таблица 4-12

4.2.5.2 Настройки аудио

Выбрав интерфейс System Config > Video Set > Audio Set interface (Конфигурация системы > Настройка видео > Настройка аудио), вы можете отрегулировать звук микрофона и зуммера. См. Рисунок 4-16.

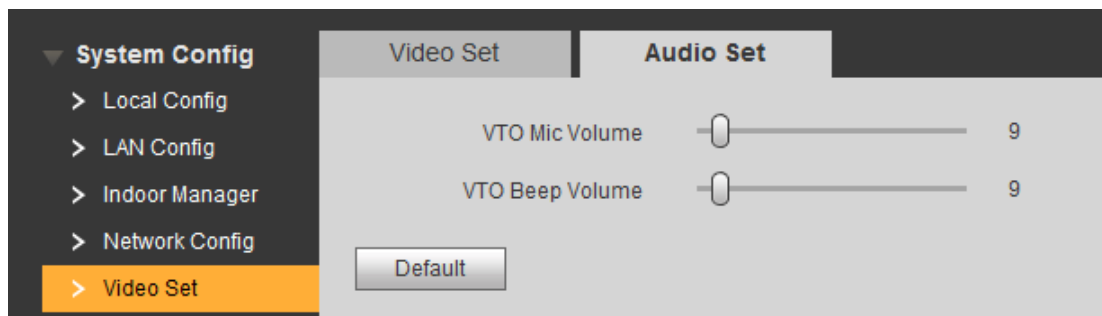


Рисунок 4-16

4.2.6 Управление пользователем

Только зарегистрировавшись в качестве администратора, вы получаете доступ к добавлению, изменению, удалению и просмотру данных пользователя в интерфейсе Управление пользователем.

4.2.6.1 Добавить пользователя

Шаг 1. Выберите System Config > User Manager > User Manager (Конфигурация системы > Управление пользователем > Управление пользователем), и откроется интерфейс User Manager (Управление пользователем).

Шаг 2. Нажмите Add (Добавить).

Шаг 3. Настройте информацию о пользователе, которого добавляете. См. Рисунок 4-17.

Рисунок 4-17

Примечание.

В данное время система поддерживает два типа пользователей: администратор и пользователь.

- Администратор имеет расширенные права и полный спектр рабочих возможностей.
- Пользователь имеет только возможность просмотра конфигурации системы, снятия блокировки, экспорта записи, публикации информации и изменения пароля пользователя.

Шаг 4. Нажмите .

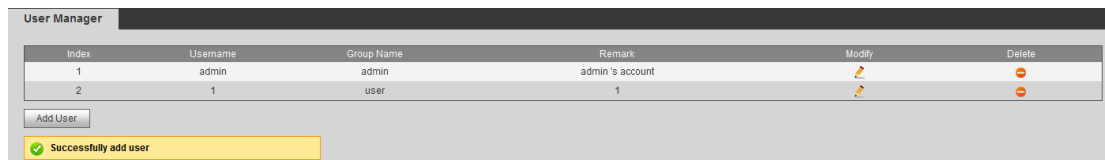




Рисунок 4-18

4.2.6.2 Удалить пользователя

В интерфейсе User Manager нажмите  для удаления пользователя.

4.2.6.3 Изменить пользователя

Шаг 1. Выберите пользователя, которого хотите изменить, и нажмите . См. Рисунок 4-19.

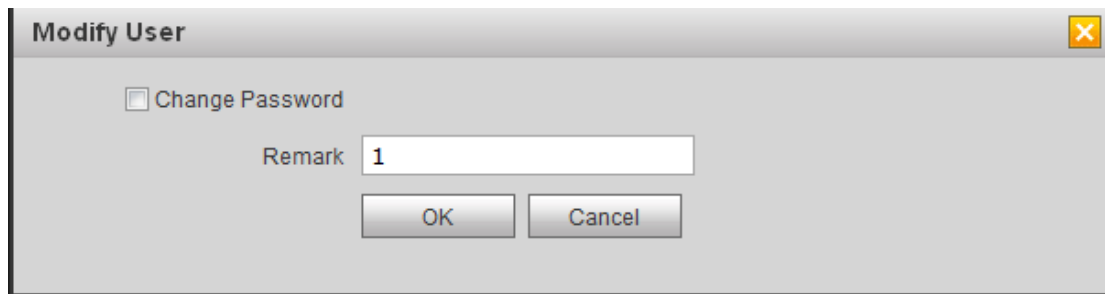


Рисунок 4-19

Шаг 2. Отметьте поле Change Password (Изменить пароль) для просмотра старого пароля, ввода нового пароля и подтверждения.

Шаг 3. Установите параметр.

Шаг 4. Нажмите ОК.

4.2.7 IP-камера

Вы можете добавить до 64 IP-камер, первые 32 канала могут быть изменены. Добавленные камеры будут автоматически синхронизированы с видеодомофоном.

Чтобы добавить IP-камеру:

Шаг 1. Вы можете перейти в интерфейс System Config > IPC info interface (Конфигурация системы > Данные IP-камеры), чтобы просматривать и изменять данные IP-камеры.

Шаг 1. Выберите System Config > IPC information > IPC information (Конфигурация системы > Данные IP-камеры > Данные IP-камеры).

Шаг 2. Нажмите .

Измените данные IP-камеры. См. Рисунок 4-9.

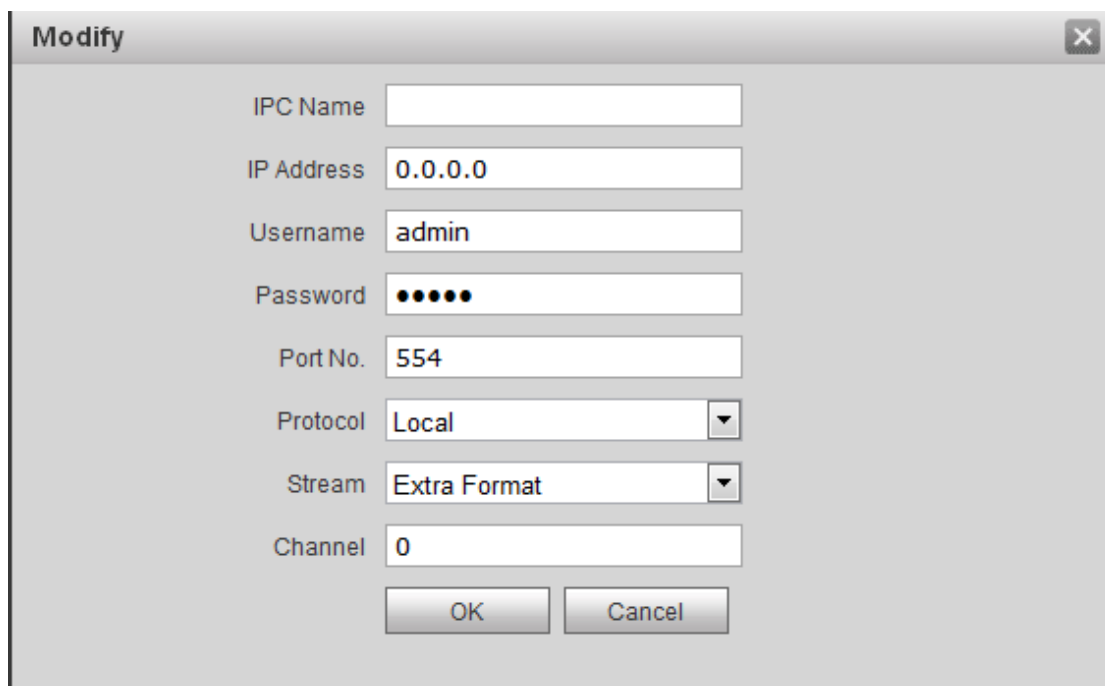


Рисунок 4-9

Шаг 3.

Параметр	Примечание
IPC Name (Имя IP-камеры)	Имя IP-камеры
IP Address (IP-адрес)	IP-адрес IP-камеры
Username (Имя пользователя)	Имя пользователя и пароль для входа на WEB-страницу IP-камеры
Password (Пароль)	

Таблица 4-13

Шаг 4. Нажмите .

4.2.8 Установка UPnP

Предупреждение

- Зайдите в настройки роутера, установите IP-адрес порта WAN при соединении с WAN.
- Роутер активирует функцию UPnP.
- Подключите устройство к порту LAN роутера для создания частной сети.

С помощью протокола UPnP установите соответствие между частной и внешней сетью. Пользователь внешней сети может подключаться к устройству в LAN по внешнему IP-адресу.

Шаг 1. Выберите System Config > UPnP Setup > UPnP (Конфигурация системы > Установка UPnP > UPnP).

Шаг 2. Отметьте поле UPnP Enable (Включить UPnP), чтобы включить функцию UPnP.

Шаг 3. Нажмите Add (Добавить). См. Рисунок 4-20.

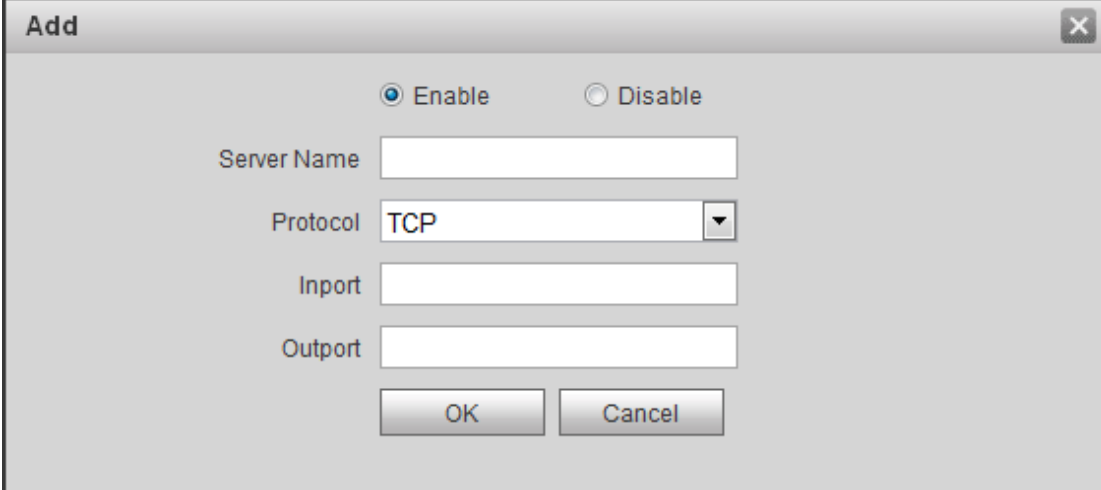


Рисунок 4-20

Шаг 4. Включите функцию UPnP. Выберите Enable (Активировать), см. таблицу ниже.

Параметр	Примечание
Server Name (Имя сервера)	Имя сервера
Protocol Type (Тип протокола)	Выберите тип протокола, TCP или UDP
Inport (Входной порт)	Порт для преобразования
Output (Выходной порт)	Порт, распределенный на роутере

Таблица 4-14

Примечание.

- Настраивая выходной порт распределения роутера, старайтесь использовать порт в диапазоне 1024~5000, избегая распространенных портов 1~255 и системных портов 256~1023.
- При подключении нескольких устройств к одному порту LAN предусмотрите распределение порта, чтобы ограничить преобразование множества устройств к одному внешнему порту.
- В ходе преобразования порта убедитесь, что порт не занят и не ограничен.
- Внутренние и внешние порты TCP/UDP должны быть одинаковы и не могут быть изменены.

Шаг 5. Нажмите ОК для завершения настройки UPnP.

В браузере перейдите по адресу *http://WAN IP: WAN port no.*, чтобы попасть к номеру соответствующего порта роутера частного устройства.

4.3 Поиск информации

Вы можете искать и экспортировать записи о снятии блокировки вызывной панели, вызовах и тревогах в интерфейсе Info Search (Поиск информации).

4.3.1 История вызовов

Вы можете найти историю вызовов вызывной панели в интерфейсе Call History (История вызовов), рассчитанном на хранение до 1024 записей.

См. Рисунок 4-21.

Index	Call Type	Room No.	Begin Time	Talk Time(min)	End State
1	Outgoing	9901	2000-01-04 23:18:29	00:00	Missed
2	Outgoing	9901	2000-01-04 23:17:28	00:00	Missed
3	Outgoing	9901	2000-01-04 23:13:52	00:00	Missed
4	Outgoing	9901	2000-01-04 23:12:51	00:00	Missed
5	Outgoing	9901	2000-01-04 23:11:50	00:00	Missed
6	Outgoing	9901	2000-01-04 23:10:49	00:00	Missed
7	Outgoing	9901	2000-01-04 23:09:48	00:00	Missed
8	Outgoing	9901	2000-01-04 23:08:47	00:00	Missed
9	Outgoing	9901	2000-01-04 23:07:46	00:00	Missed
10	Outgoing	9901	2000-01-04 23:06:45	00:00	Missed
11	Outgoing	9901	2000-01-04 23:05:44	00:00	Missed
12	Outgoing	9901	2000-01-04 23:04:43	00:00	Missed
13	Outgoing	9901	2000-01-04 23:03:42	00:00	Missed
14	Outgoing	9901	2000-01-04 23:02:41	00:00	Missed
15	Outgoing	9901	2000-01-04 23:01:40	00:00	Missed
16	Outgoing	9901	2000-01-04 23:00:39	00:00	Missed
17	Outgoing	9901	2000-01-04 22:59:38	00:00	Missed
18	Outgoing	9901	2000-01-04 22:58:37	00:00	Missed
19	Outgoing	9901	2000-01-04 22:57:36	00:00	Missed
20	Outgoing	9901	2000-01-04 22:56:35	00:00	Missed

Рисунок 4-21

Нажмите Export Record (Экспорт записи) для экспорта истории вызовов.

4.3.2 Запись при возникновении тревоги

Хранение до 1024 записей, включая записи при срабатывании сигнализации датчика двери, антивандальной сигнализации и т. д.

Выберите интерфейс Info Search > Alarm Record > Alarm Record (Поиск > Запись при возникновении тревоги > Запись при возникновении тревоги). Вы можете найти сигнализацию вызывной панели квартиры, в т. ч. номер комнаты, статус сигнализации и т. д., см. Рисунок 4-22.

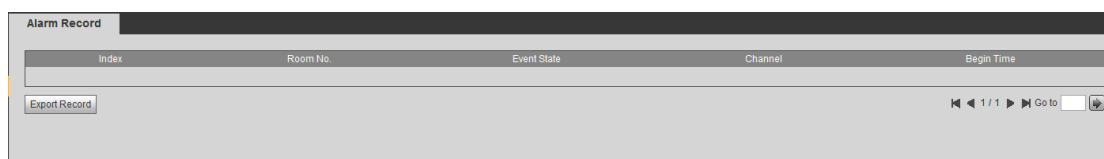


Рисунок 4-22

Нажмите Export Record (Экспорт записи) для экспорта записи при срабатывании сигнализации вызывной панели.

4.3.3 Запись о снятии блокировки

Вы можете найти записи о снятии блокировки вызывной панели в интерфейсе Unlock Record (Запись о снятии блокировки) вызывной панели, рассчитанном на хранение до 1000 записей. Он включает записи о снятии блокировок дистанционным способом, нажатием кнопки и картой.

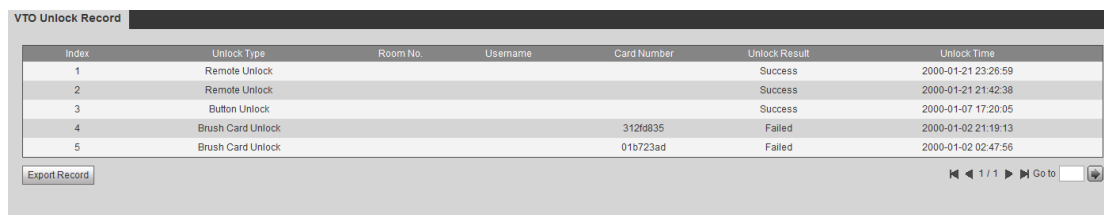


Рисунок 4-10

Нажмите Export Record (Экспорт записи) для экспорта записи при срабатывании сигнализации вызывной панели.

4.4 Статистика статусов

4.4.1 Статус видеодомофона

Предупреждение

Если видеодомофон ни разу не был онлайн, вы не сможете найти статусы в меню Status Statistics > VTH Status > VTH Status (Статистика статусов > Статус видеодомофона > Статус видеодомофона).

В меню VTH status (Статус видеодомофона) вы можете просмотреть статусы подключений видеодомофона. См. Рисунок 4-23.

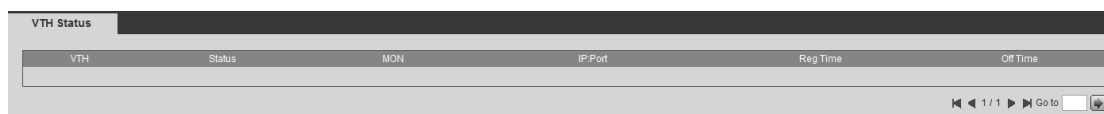


Рисунок 4-23

- Статус

Offline (Офлайн): соединение между вызывной панелью и видеодомофоном отсутствует; вы не можете звонить, просматривать видео и разговаривать.

Online (Онлайн): соединение между вызывной панелью и видеодомофоном настроено; вы можете звонить, просматривать видео и разговаривать.

- Статус просмотра

Unmon: наблюдение не ведется.

Onmon: наблюдение ведется.

5 Общие сведения о функциях

Вызывная панель поддерживает снятие блокировки с помощью карты, звонка в центр управления одним нажатием и видеодомофона, а центр управления может связаться с видеодомофоном.

5.1 Просмотр

Скачайте приложение через мобильный телефон и зарегистрируйтесь, чтобы просматривать видеозаписи видеодомофона в удаленном режиме. См. п. 4.2.4.5.

5.2 Разговор

Нажмите кнопку вызова на устройстве, чтобы позвонить в центр управления или на видеодомофон.

См. п. 4.2.2

5.3 Функция снятия блокировки

Снятие блокировки IC-картой

Проведите авторизованной IC-картой в поле считывания вызывной панели, и после верификации дверь откроется. См. п. 4.2.1.3.

Снятие блокировки из центра

При входящем или исходящем звонке центра или в режиме просмотра центр имеет возможность дистанционно снять блокировку двери. Вызывная панель будет оставаться в режиме ожидания после завершения звонка или обратного отсчета.

Снятие блокировки от домофона

При входящем или исходящем звонке центра или в режиме просмотра видеодомофон имеет возможность дистанционно снять блокировку двери. Вызывная панель будет оставаться в режиме ожидания после завершения звонка или обратного отсчета.

5.4 Восстановление

См. п. 4.2.1.8.

Приложение 1. Технические характеристики

Модель		VTO3211D-P	VTO3211D
Система	Главный процессор	Встроенный микроконтроллер	
	Операционная система	Встроенная система Linux	
Видео	Стандарт сжатия видео	H.264	
Аудио	Стандарт аудио	G.711	
	Вход	Однонаправленный микрофон	
	Выход	Встроенный динамик	
	Разговор	Поддержка двусторонней голосовой связи	
Режим работы	Вход	Механический ключ	
Тревожная сигнализация	Вход	1-кан. кнопка снятия блокировки, 1-кан. датчик ОС блокировки двери	
	Выход	1-кан. релейный выход	
	Фронтальная камера	2,0 МП	
Сеть	Ethernet	10М/100М Мбит/с, самонастройка	
Другие параметры	485 BUS	1-кан.	
	Внешняя TF-карта	Макс. 64 Гб	
Общие параметры	Питание	12 В пост. тока или стандартное питание по Ethernet	12 В пост. тока
	Защита	IK08	
	Водонепроницаемость	IP65	
	Потребляемая мощность	В режиме ожидания ≤ 1 Вт; в работе ≤ 7 Вт	
	Размеры (ДхШхВ)	182 мм * 101 мм * 30 мм	

Примечание.

- Данное руководство предназначено только для справки. В интерфейсе пользователя могут содержаться небольшие отличия.
- Все проектные решения и программы могут меняться без предварительного письменного оповещения.
- Другие торговые марки и зарегистрированные торговые марки, упоминаемые в данном документе, являются собственностью соответствующих владельцев.
- Если вы нашли неточность или противоречие, см. наши последние разъяснения.
- Посетите наш веб-сайт или обратитесь за дополнительной информацией к инженеру местной сервисной службы.