Серия ASI1212M / ASI1201M

Краткое руководство пользователя

V1.0.2

Содержание

1 Конструкция

Схема предоставлена для справки. Конструкция и размеры могут отличаться в зависимости от фактической модели.

Рис. 1-1 Габаритные размеры (единица измерения: мм [дюйм])

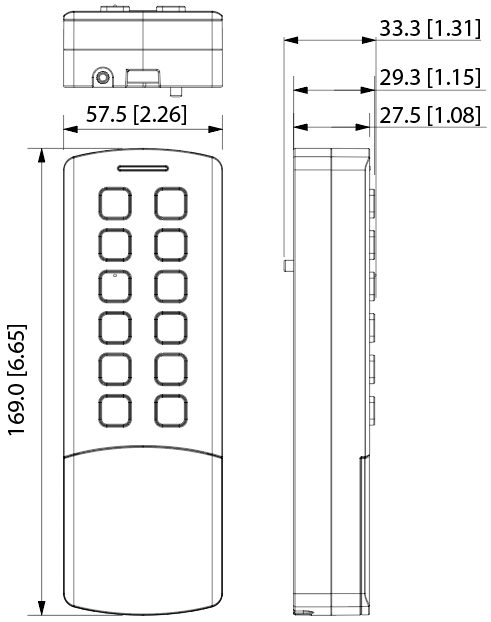
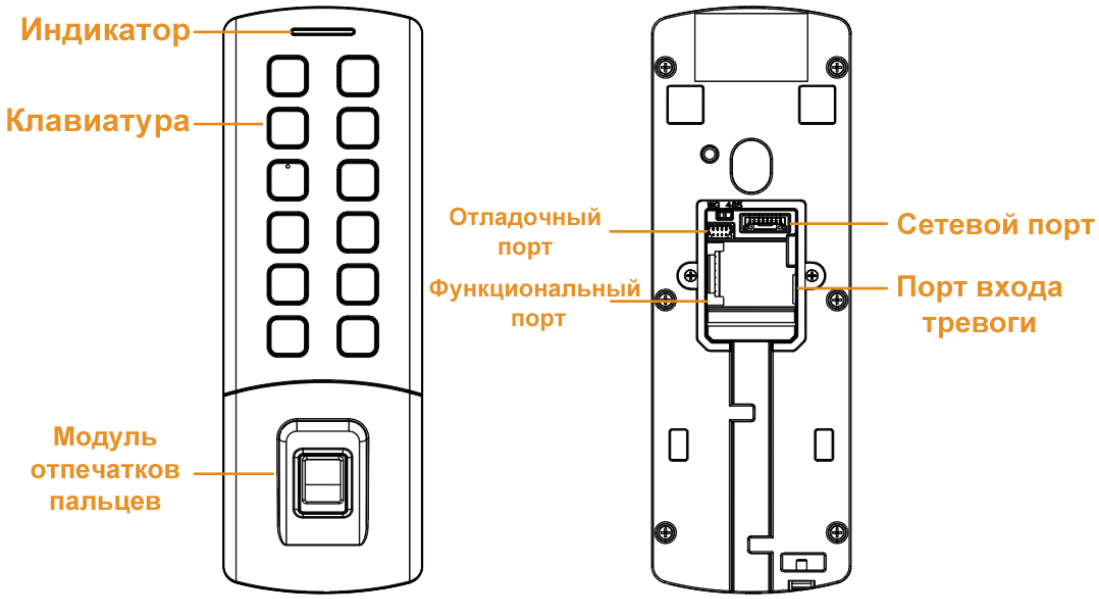


Рис. 1-2 Конструкция



Функция распознавания отпечатков пальцев доступна только в отдельных моделях.

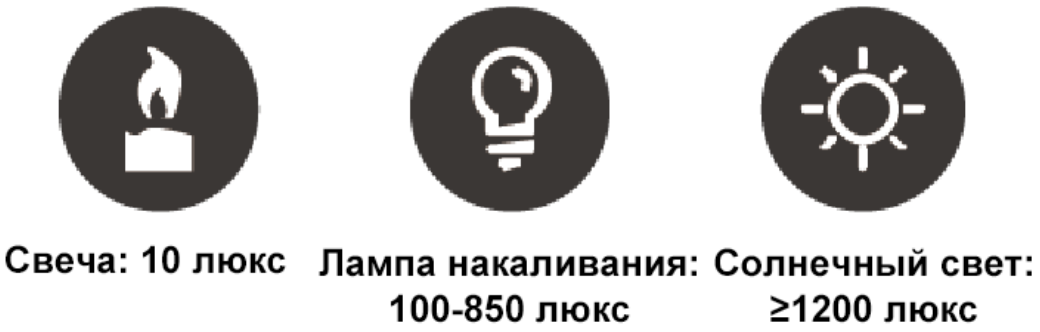
2 Подключение и установка

2.1 Требования к установке

- Рекомендуемая высота установки (от индикатора до земли) — 1,4 м.
- Освещённость на расстоянии 0,5 метра от устройства должна быть не менее 100 Люкс.
- Рекомендуется устанавливать устройство внутри помещений, на расстоянии не менее 3 метров от окон и дверей и не менее 2 метров от источников света.
- Следует избегать контрового света, прямого солнечного света, близко расположенных источников света и падающего под углом света.

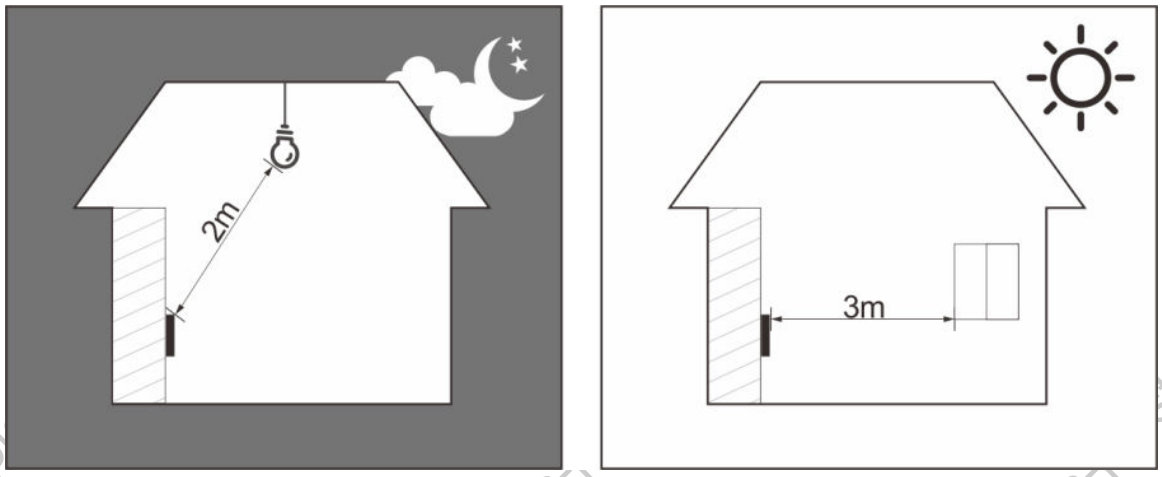
Требования к освещению

Рис. 2-1 Требования к окружающему освещению



Рекомендуемое место установки

Рис. 2-2 Рекомендуемое место установки



Нерекомендуемые места установки

Рис. 2-3 Нерекомендуемые места установки

2.2 Подключение проводов

Конфигурация портов может отличаться в зависимости от модели изделия.

- Провода RS485A и WG_D0 объединены. Провода RS485B и WG_D1 объединены.
- Когда DIP-переключатель установлен в положение WG, объединенные провода могут быть подключены к устройству с протоколом Wiegand. Когда DIP-переключатель установлен в положение 485, объединенные провода могут быть подключены к устройству с протоколом RS-485.
- Если вы выбираете «**Door Control Module**» (Модуль управления дверью) через «**Communication Settings**» (Настройки связи) > «**RS-485 Config**» (Конфигурация RS-485), модуль безопасности управления дверью необходимо приобрести отдельно. Модуль безопасности требует отдельного источника питания.
- Когда функция модуля безопасности активирована, кнопка выхода, управление замком и тревожная сигнализация становятся неактивными.

Рис. 2-4 Схема подключения

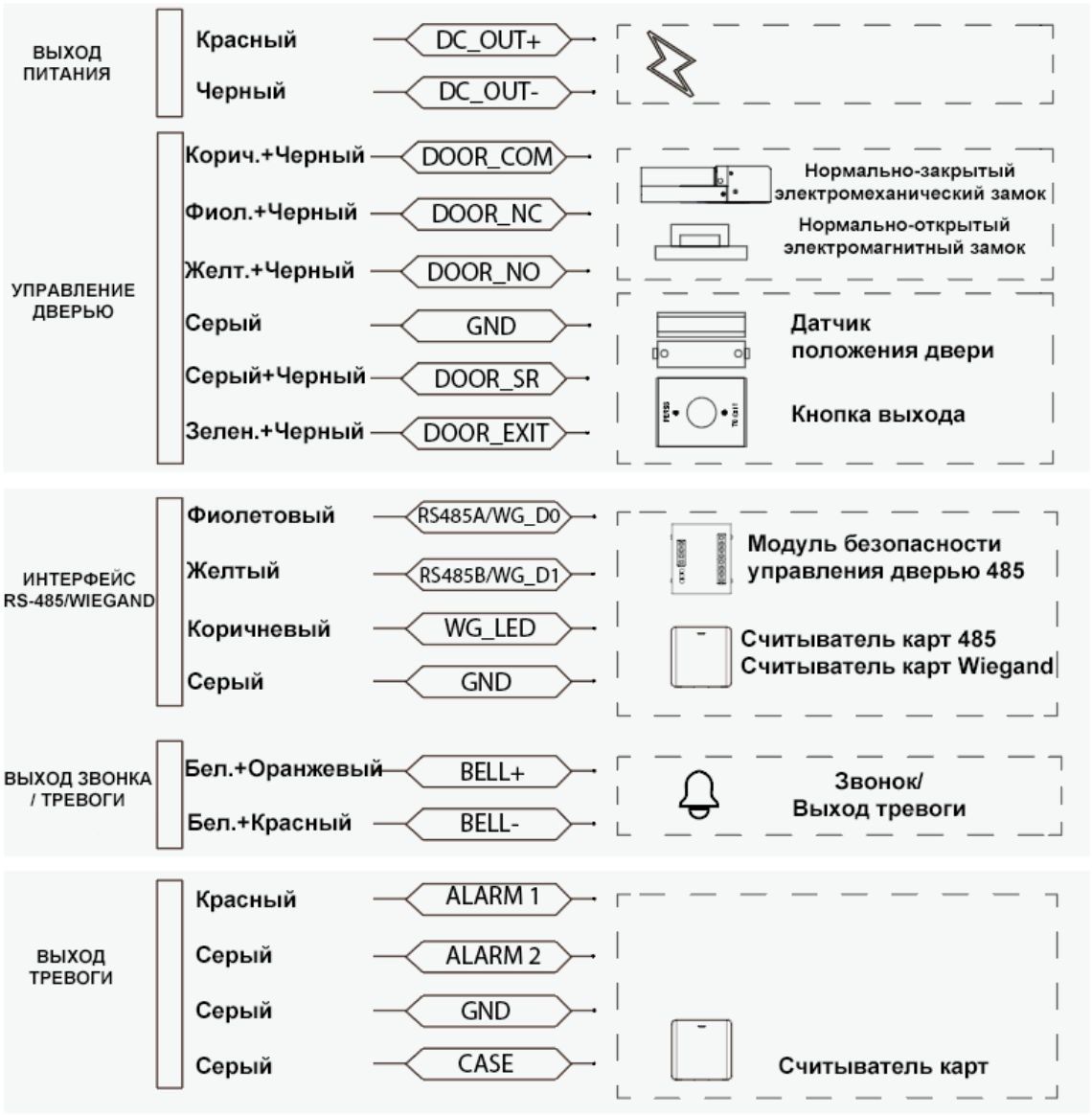


Рис. 2-5 Схема подключения стандартного устройства

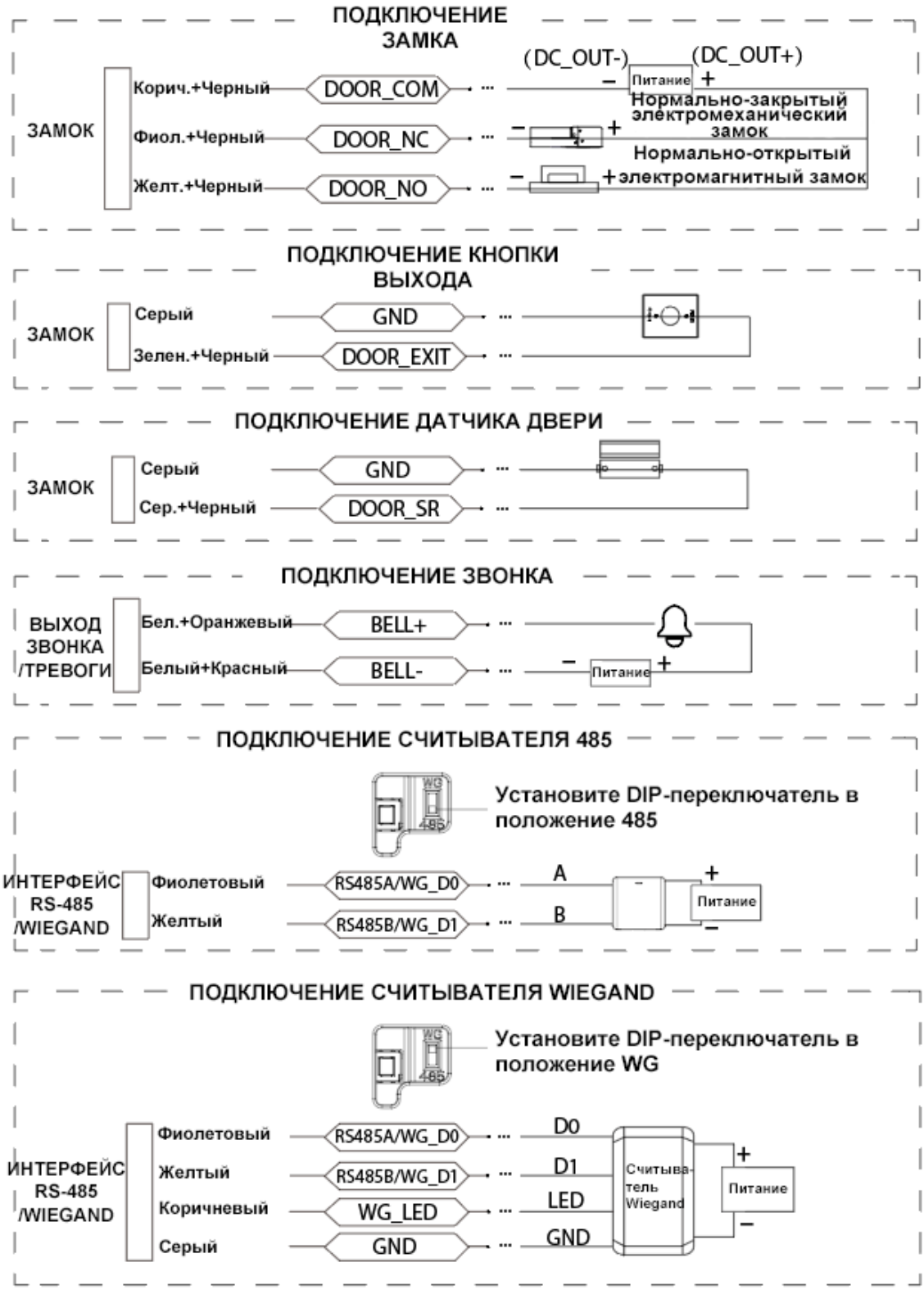


Рис. 2-6 Схема подключения модуля безопасности управления дверью

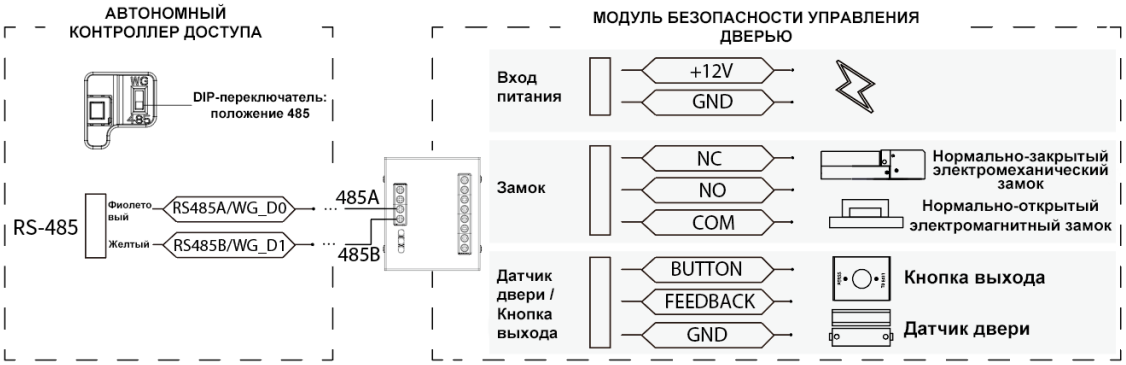


Рис. 2-7 Схема подключения питания

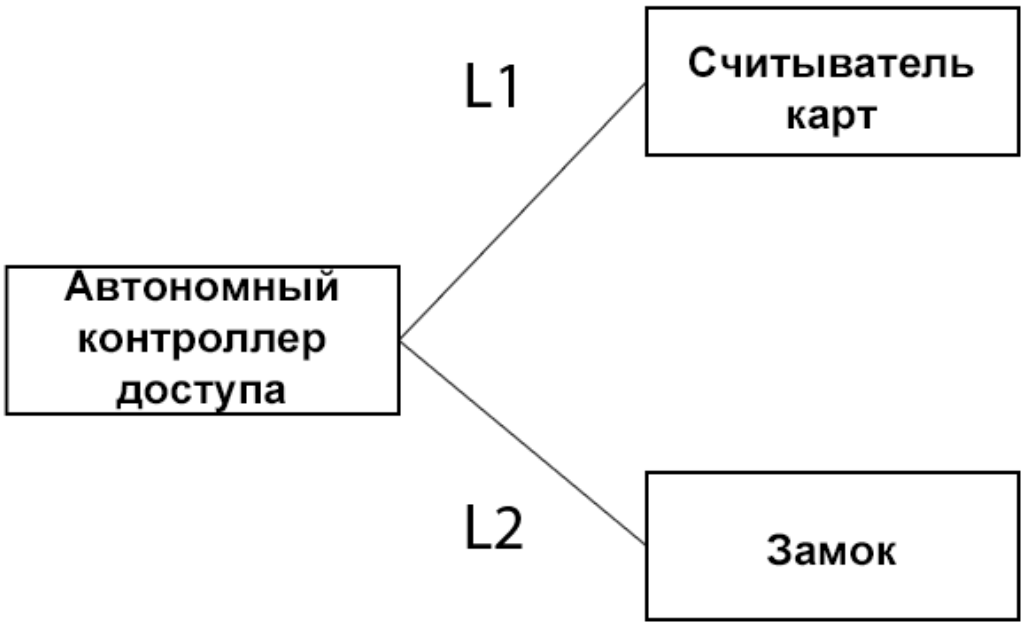


Таблица 2-1 Описание спецификации кабелей

№	Название	Рекомендуемая модель и спецификации	Рекомендуемая макс. длина для питания и связи
L1	Кабель считывателя	● RVV 0.5 мм² (сопр. пост. току ≤ 39.0 Ом/км) ● RVV 1.0 мм² (сопр. пост. току ≤ 19.5 Ом/км) ● RVV 1.5 мм² (сопр. пост. току ≤ 13.3 Ом/км) ● CAT5E (сопр. на 100 м ≤ 9 Ом)	● **RVV 0.5 мм²:** - Считыватель RS-485: ≤ 200 м - Считыватель Wiegand: ≤ 120 м ● **CAT5E (одна жила):** - Считыватель RS-485: ≤ 120 м - Считыватель Wiegand: ≤ 50 м

№	Название	Рекомендуемая модель и спецификации	Рекомендуемая макс. длина для питания и связи
L2	Кабель замка		• **RVV 0.5 мм²** Электромагнитный замок 280 кг (одна дверь): ≤ 60 м • **RVV 1.0 мм²** Электромагнитный замок 280 кг (одна дверь): ≤ 100 м • **RVV 1.5 мм²** Электромагнитный замок 280 кг (одна дверь): ≤ 140 м

- Если считыватель карт питается от автономного контроллера доступа, рекомендуется выбирать считыватель с максимальным потребляемым током не более 200 мА. Выбранный считыватель должен поддерживать работу в широком диапазоне напряжений, при этом минимальное рабочее напряжение не должно превышать 9 В.
- Если замок питается от автономного контроллера доступа, рекомендуется выбирать замок с максимальным потребляемым током не более 500 мА. Выбранный замок должен поддерживать работу в широком диапазоне напряжений, при этом минимальное рабочее напряжение не должно превышать 10 В.
- Длина линий L1 и L2 зависит от напряжения источника питания и сечения кабеля. При фактическом монтаже необходимо обеспечивать, чтобы напряжение питания не опускалось ниже минимального рабочего напряжения автономного контроллера, считывателя и замка. Кроме того, линии L1 и L2 не должны прокладываться в одном кабеле.
- При использовании кабеля CAT5e (сопротивление на 100 м ≤ 9 Ом) для питания замков или считывателей рекомендуется равномерно распределить все свободные жилы, помимо необходимых сигнальных, для подачи питания, чтобы минимизировать потери.
- Фактические данные могут отличаться в зависимости от конкретных условий эксплуатации.

2.3 Порядок установки

Устройство поддерживает настенный монтаж и имеет два способа прокладки кабелей: наружный и скрытый (в стене).

Порядок монтажа

Шаг 1. По разметке монтажного кронштейна просверлите 6 отверстий и 1 канал для кабеля в стене.

Примечание: Канал в стене не требуется для наружной прокладки кабеля.

Шаг 2. Вставьте дюбели в отверстия и закрепите кронштейн на стене.

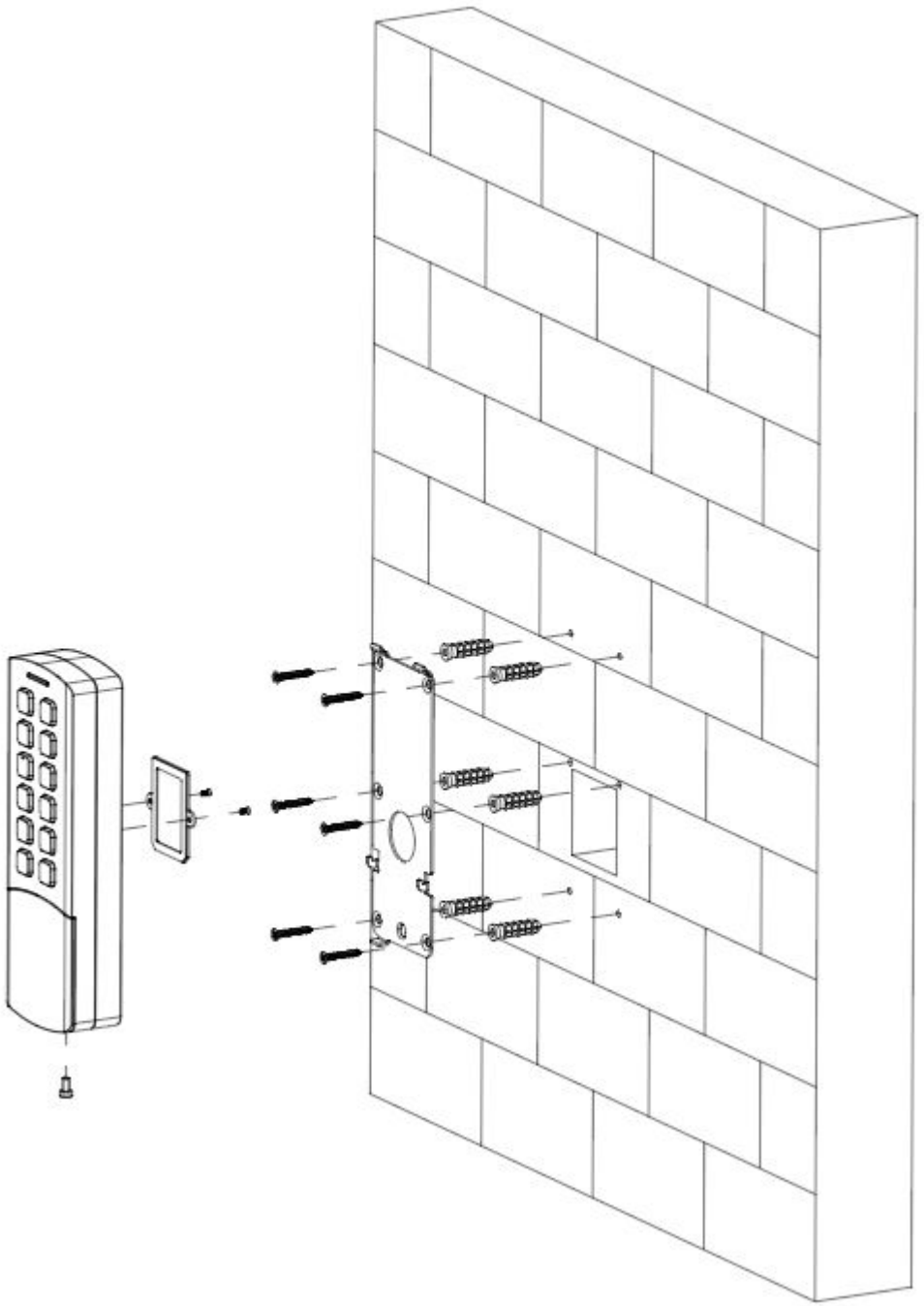
Шаг 3. Подключите кабели устройства. Подробности см. в разделе «2.2 Подключение».

- При скрытой прокладке пропустите кабель через заднюю панель и канал в стене.
- При наружной прокладке прокладка кабеля через заднюю панель не требуется.

Шаг 4. Установите устройство на кронштейн задней панели.

Шаг 5. Заверните винт в нижней части устройства.

Рис. 2-8 Монтаж



3 Локальная конфигурация

Процедура локальной настройки может отличаться в зависимости от модели контроллера доступа.

3.1 Инициализация

После первого включения питания устройства необходимо установить пароль администратора. Пароль администратора используется для входа в главное меню устройства.

Порядок действий

Шаг 1. Подключите питание устройства. Индикатор медленно мигает красным.

Шаг 2. Нажмите **#**, введите пароль администратора и снова нажмите **#**.

- Длина пароля должна составлять от 1 до 8 символов.
- Постоянный синий свет индикатора означает, что устройство инициализировано.

После инициализации доступны только функции на самом устройстве. Для входа на веб-интерфейс устройства необходимо выполнить его инициализацию через веб-страницу или с помощью ConfigTool.

Связанные операции

- При инициализации непосредственно на устройстве пароль учетной записи администратора может состоять только из цифр.
- При инициализации через платформу ConfigTool пароль учетной записи администратора может содержать цифры, буквы и другие символы.

После завершения инициализации на самом устройстве выполнение операций возможно только на нем самом. Если необходимо подключить устройство к сети, используйте ConfigTool или платформу для его инициализации.

При использовании ConfigTool или платформы для инициализации устройства, после настройки сетевой учетной записи и пароля устройство автоматически завершит инициализацию и перейдет в режим ожидания. Локальный пароль администратора преобразуется из сетевого пароля. Если пароль превышает 8 символов, сохраняются только первые 8 символов. Буквы преобразуются в цифры в соответствии со стандартом E.161. Преобразование пароля нечувствительно к регистру, а все остальные символы преобразуются в 0.

- После инициализации, если вы измените сетевой пароль, локальный пароль администратора не будет затронут.
- Если сначала выполнить инициализацию через устройство, а затем через ConfigTool или платформу, локальный пароль администратора не изменится.

Рис. 3-1 Стандарт E.161 (T9-клавиатура)

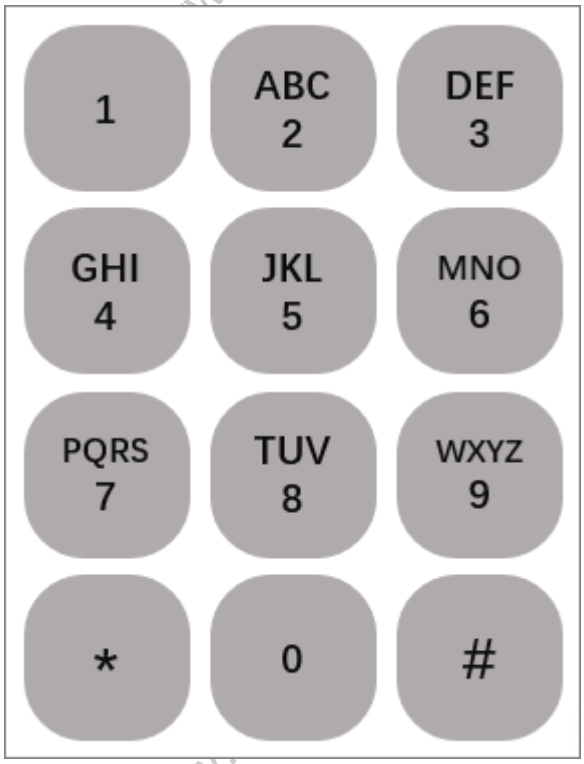


Таблица 3-1 Пример преобразования

Сетевой пароль	Локальный пароль администратора
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

3.2 Главное меню

Вход в главное меню

Нажмите **#**, введите пароль администратора, затем снова нажмите **#**.

- Медленное мигание синим индикатором означает, что вы вошли в главное меню.
- Однократное мигание красным индикатором и 3 звуковых сигнала зуммера с последующим постоянным синим светом означают, что пароль неверен.

Связанные индикации

- Однократное мигание зеленым индикатором и 1 звуковой сигнал зуммера означают успешное выполнение операции или проверки доступа.
- Однократное мигание красным индикатором и 3 звуковых сигнала зуммера означают сбой операции или проверки доступа.
- Медленное мигание красным индикатором означает, что устройство не инициализировано.

- Постоянный синий свет индикатора означает, что устройство находится в режиме ожидания.
- Мигание синим индикатором означает, что устройство вошло в главное меню.
- Клавиатура подсвечивается белым при работе с устройством. Если в течение 10 секунд не производится никаких действий, подсветка выключается и устройство выходит из текущего экрана.

3.3 Добавление пользователей

- Для одного пользователя можно добавить только одну карту, один пароль или один отпечаток пальца. Необходимо добавить хотя бы один метод: карту, пароль или отпечаток пальца.
- Функция распознавания отпечатков пальцев доступна только в отдельных моделях.

Порядок действий

Шаг 1. Нажмите **#,** введите пароль администратора, затем снова нажмите **#.**

Войдите в главное меню (индикатор мигает синим).

Шаг 2. Нажмите **1**, затем **#** для добавления пользователей.

Шаг 3. Введите идентификатор пользователя (**ID**), затем нажмите **#.**

- Если индикатор не загорается и раздается звуковой сигнал, идентификатор пользователя успешно добавлен.
- Если индикатор мигает красным и раздается звуковой сигнал, не удалось добавить идентификатор пользователя. Возможная причина: идентификатор уже существует. Попробуйте использовать другой идентификатор.

На устройстве для идентификатора (ID) можно вводить только цифры.

Шаг 4. После прикладывания карты нажмите #, чтобы добавить карту.

Если не требуется добавлять карту, нажмите #, чтобы пропустить этот шаг.

Шаг 5. Введите пароль пользователя и нажмите #.

Если вам не нужно устанавливать пароль пользователя, нажмите #, чтобы пропустить этот шаг.

Длина пароля должна составлять от 1 до 8 символов.

Шаг 6. Добавьте отпечаток пальца, затем нажмите #.

Если вам не нужно добавлять отпечаток пальца, нажмите #, чтобы пропустить этот шаг.

Эта функция доступна только в отдельных моделях.

Шаг 7. Повторите шаги со 2 по 6, чтобы добавить других пользователей.

После добавления пользователя нажмите ***** для возврата в главное меню, затем снова нажмите ***** для возврата в режим ожидания.

4 Работа с SmartPSS Lite

4.1 Установка

Обратитесь в техническую поддержку или посетите официальный сайт, чтобы получить дистрибутив SmartPSS Lite. После получения программного пакета установите и запустите программу в соответствии с инструкциями на странице.

4.2 Инициализация

При первом входе в SmartPSS Lite необходимо выполнить инициализацию, включающую установку пароля для входа и контрольных вопросов для его восстановления.

Порядок действий

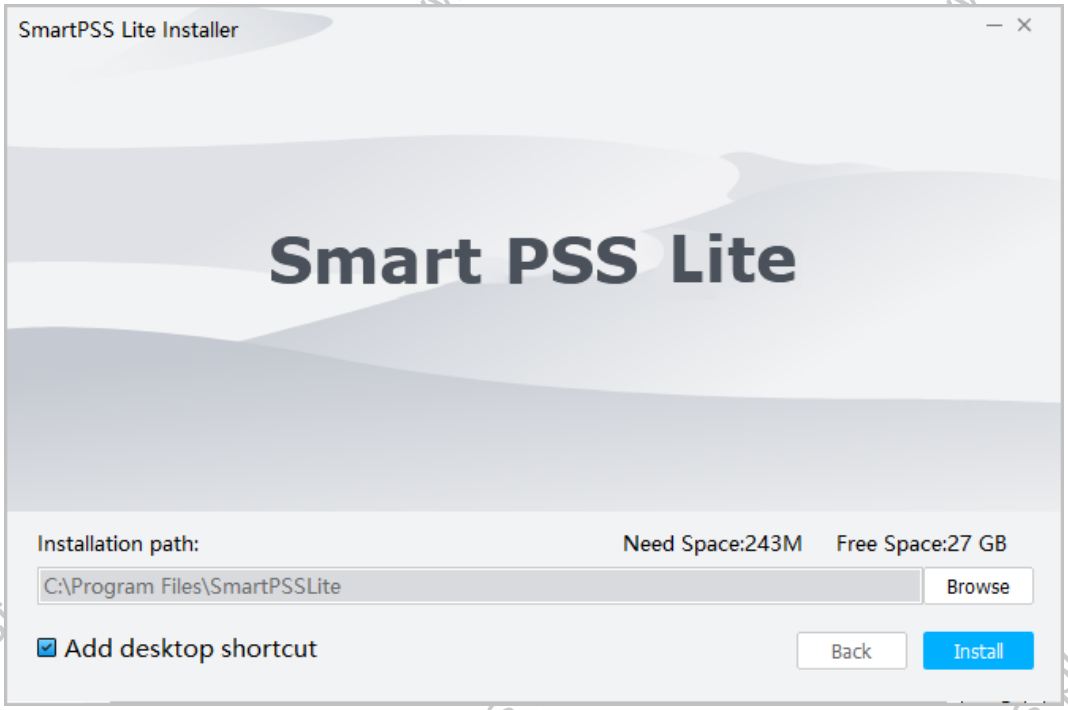
Шаг 1 Дважды щелкните файл **SmartPSSLite.exe**.

Шаг 2 Выберите язык из раскрывающегося списка, установите флажок "**Я прочитал и принимаю лицензионное соглашение**" (I have read and agree the software agreement), затем нажмите "**Далее**" (Next).

Рис. 4-1 Выбор языка

Шаг 3 Нажмите «**Обзор**» (Browse) для выбора пути установки, затем нажмите «**Установить**» (Install).

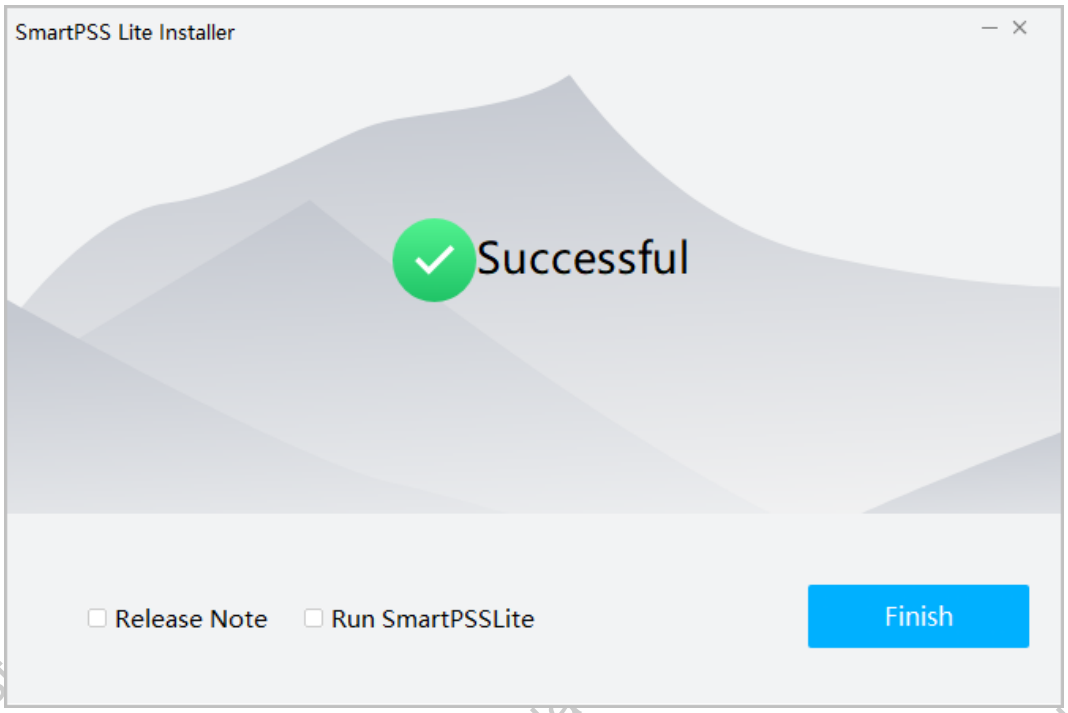
Рис. 4-2 Выбор пути установки



Нажмите «**Готово**» (Finish) для завершения установки.

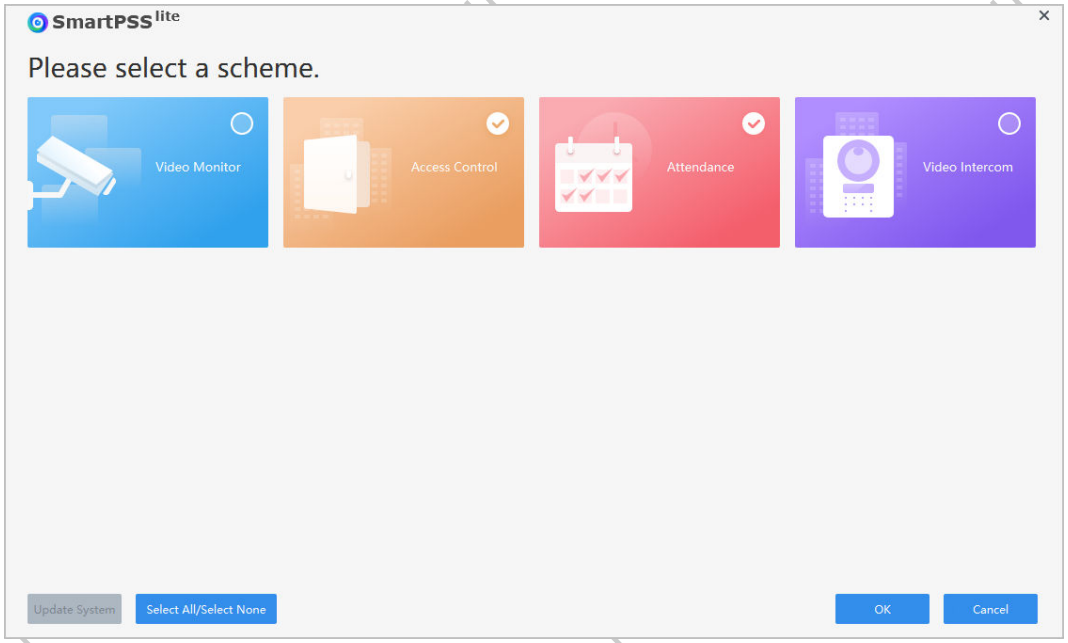
Выберите опцию «**Запустить SmartPSSLite**» (Run SmartPSSLite) для старта приложения SmartPSS Lite.

Рис. 4-3 Установка завершена



Шаг 5 Выберите сценарии применения, которые вы хотите добавить, и нажмите «**OK**».

Рис. 4-4 Выбор сценариев применения



Шаг 6. Нажмите «**Принять и продолжить**» (Agree and Continue), чтобы согласиться с Лицензионным соглашением и Политикой конфиденциальности продукта.

Шаг 7. На странице «**Инициализация**» (Initialization) установите пароль и нажмите «**Далее**» (Next).

Рис. 4-5 Установка пароля

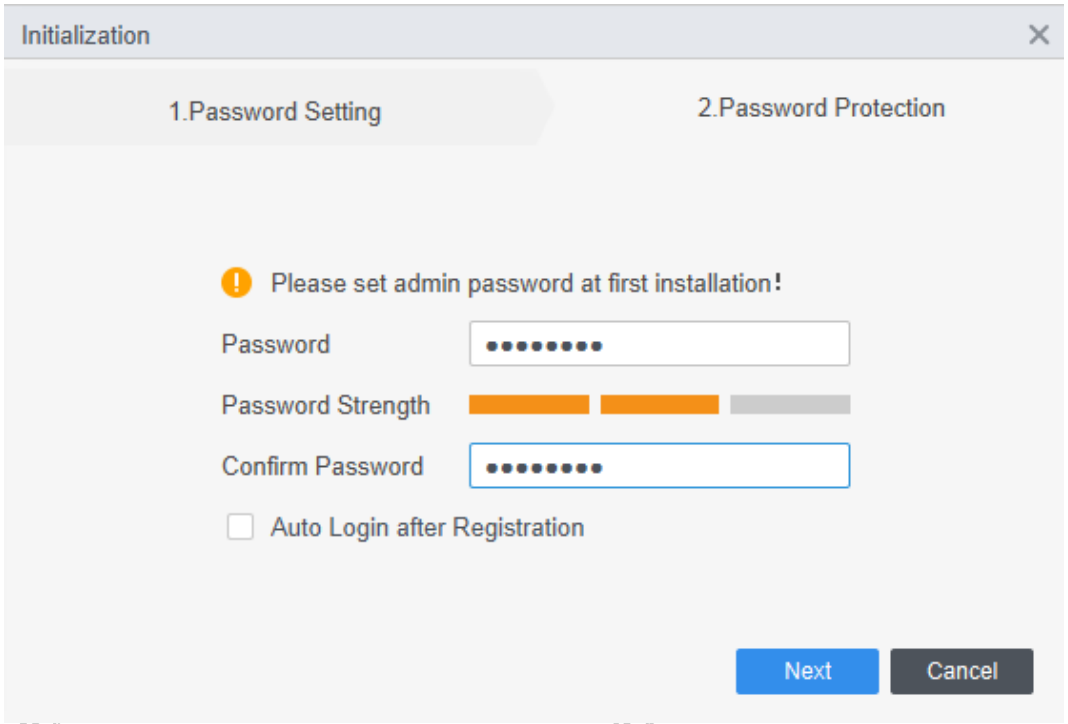
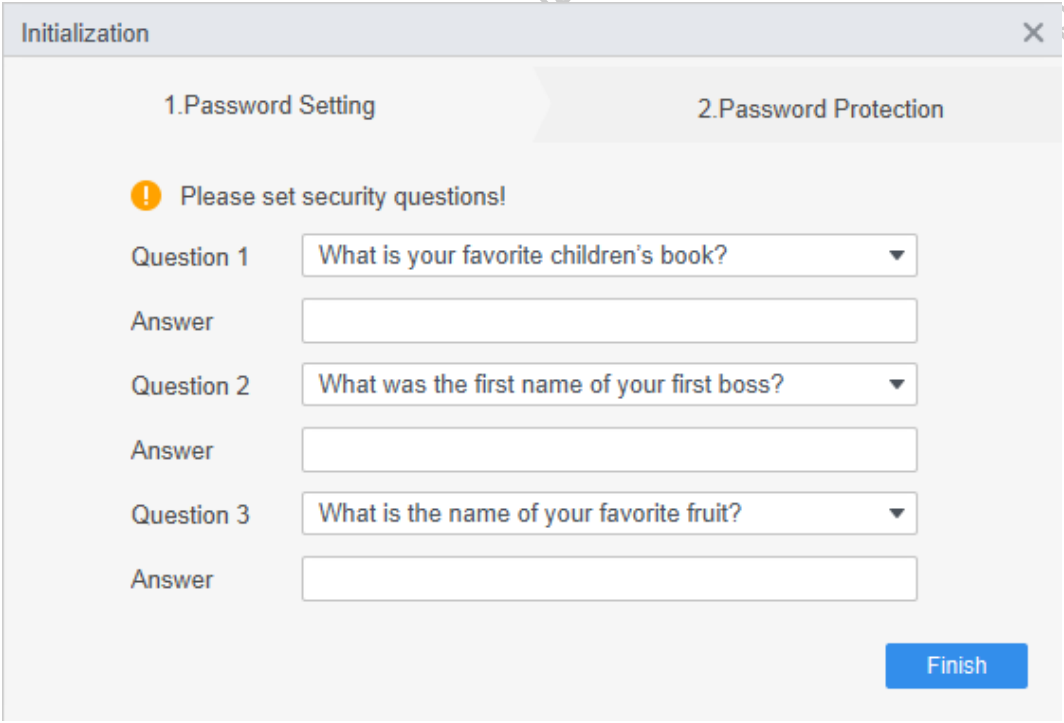


Таблица 4-1 Параметры инициализации

Параметр	Описание
Пароль	Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа символов из следующих: заглавные буквы, строчные буквы, цифры и специальные символы (исключая ' " ; : &).
Надежность пароля	Отображает устойчивость пароля к угадыванию или перебору. Зеленый индикатор означает, что пароль достаточно надежен, красный — что надежность недостаточна. Установите пароль высокого уровня безопасности в соответствии с подсказкой о надежности.
Подтверждение пароля	Повторно введите пароль для подтверждения.
Автоматический вход после регистрации	Включите опцию **Auto Login after Registration**, чтобы SmartPSS Lite автоматически выполнял вход после инициализации; в противном случае будет отображаться страница входа.

Шаг 8. Установите контрольные вопросы и нажмите «**Готово**» (Finish).

Рис. 4-6 Настройка контрольных вопросов



4.3 Вход в систему

Порядок действий

Шаг 1. Дважды щелкните файл SmartPSSLite.exe.

Шаг 2. Введите имя пользователя и пароль, затем нажмите «**Вход**» (Login).

Если на вашем компьютере доступно несколько сетей, вы можете выбрать одну из них.

Рис. 4-7 Вход в систему

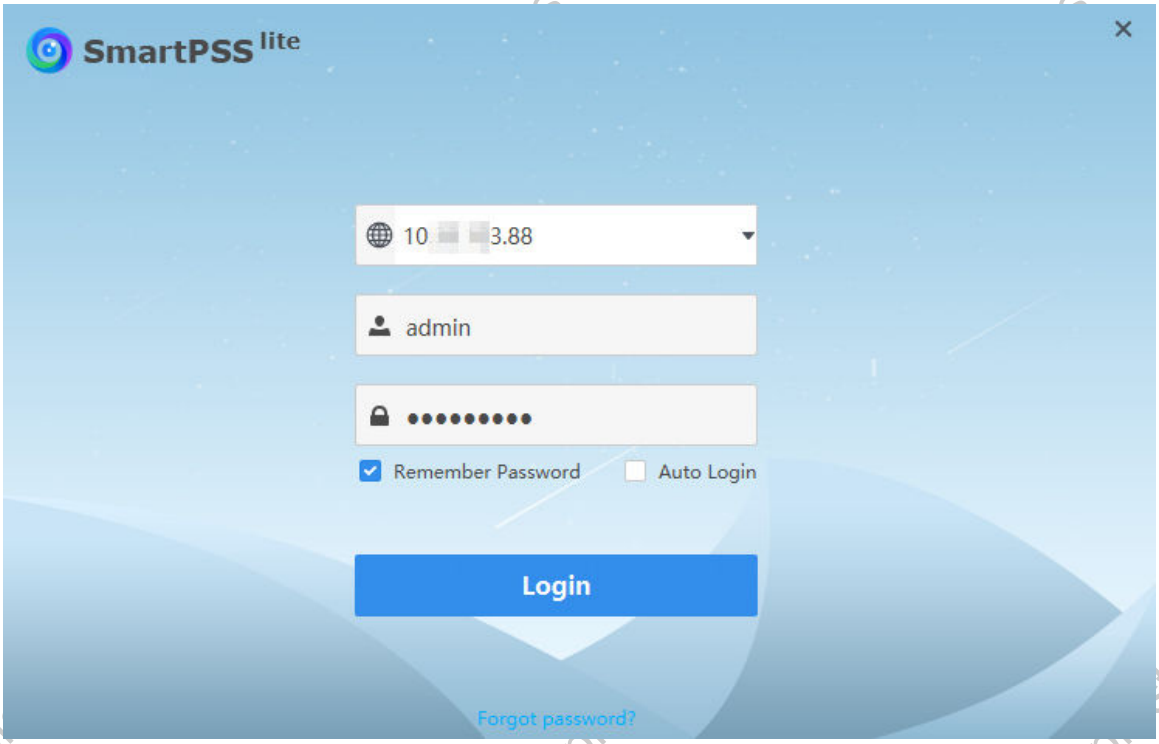


Таблица 4-2 Параметры входа

Параметр	Описание
Запомнить пароль	Включите опцию "**Запомнить пароль**" (Remember Password), чтобы не вводить пароль повторно при следующем входе в систему.
Автоматический вход	Включите опцию "**Автоматический вход**" (Auto Login), чтобы SmartPSS Lite автоматически выполнял вход при следующем использовании под той же учетной записью.
Забыли пароль?	Нажмите "**Забыли пароль?**" (Forgot password?), чтобы сбросить пароль с помощью контрольных вопросов, если вы его забыли.

Приложение 1 Рекомендации по безопасности

Управление учетными записями

1. **Использование сложных паролей**

   При установке паролей рекомендуется следовать следующим правилам:

   - Длина пароля должна быть не менее 8 символов;
   - Пароль должен содержать как минимум два типа символов: заглавные и строчные буквы, цифры и специальные знаки;
   - Пароль не должен содержать имя учетной записи или его запись в обратном порядке;
   - Не используйте последовательные символы, такие как 123, abc и т.д.;
   - Не используйте повторяющиеся символы, такие как 111, aaa и т.д.
2. **Регулярная смена паролей**

   Рекомендуется периодически менять пароли устройств, чтобы снизить риск их угадывания или взлома.
3. **Рациональное распределение учетных записей и прав доступа**

   В зависимости от служебных и управленческих требований следует добавлять пользователей и назначать им минимально необходимые наборы прав.
4. **Активация функции блокировки учетной записи**

   Функция блокировки учетной записи включена по умолчанию. Рекомендуется сохранять её включенной для защиты учетной записи. После нескольких неудачных попыток ввода пароля соответствующая учетная запись и IP-адрес источника будут заблокированы.
5. **Своевременная настройка и обновление информации для сброса пароля**

   Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции злоумышленниками, при изменении информации необходимо своевременно её обновлять. При настройке контрольных вопросов рекомендуется не использовать легко угадываемые ответы.

Конфигурация служб

1. **Активация HTTPS**

   Рекомендуется включить протокол HTTPS для доступа к веб-службам через защищённые каналы.
2. **Шифрование передачи аудио и видео**

   Если содержимое ваших аудио- и видеоданных является важным или конфиденциальным, рекомендуется использовать функцию шифрования передачи, чтобы снизить риск перехвата данных во время передачи.
3. **Отключение необязательных служб и использование безопасного режима**

   При отсутствии необходимости рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точка доступа AP и др., чтобы сократить поверхность атаки.
4. При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, но не ограничиваясь следующими службами:

   - SNMP: Выбирайте SNMP v3 и настраивайте стойкое шифрование и пароли аутентификации.
   - SMTP: Выбирайте TLS для доступа к почтовому серверу.
   - FTP: Выбирайте SFTP и устанавливайте сложные пароли.
   - Точка доступа AP: Выбирайте режим шифрования WPA2-PSK и устанавливайте сложные пароли.
5. **Изменение портов HTTP и других служб по умолчанию**

   Рекомендуется изменить порт по умолчанию для HTTP и других служб на любой порт в диапазоне от 1024 до 65535, чтобы снизить риск их угадывания злоумышленниками.

Настройка сети

1. **Активация белого списка (Allowlist)**
   Рекомендуется включить функцию белого списка и разрешить доступ к устройству только IP-адресам, внесенным в этот список. Обязательно добавьте в белый список IP-адрес вашего компьютера и IP-адреса поддерживаемых устройств.
2. **Привязка MAC-адресов**
   Рекомендуется выполнить привязку IP-адреса шлюза к MAC-адресу на устройстве, чтобы снизить риск ARP-спуфинга.
3. **Создание безопасной сетевой среды**
   Для обеспечения повышенной безопасности устройств и снижения потенциальных сетевых рисков рекомендуется следующее:
   - Отключите функцию проброса портов (port mapping) на маршрутизаторе, чтобы исключить прямой доступ к устройствам внутренней сети из внешней сети;
   - В соответствии с фактическими сетевыми потребностями сегментируйте сеть: если между двумя подсетями не требуется обмен данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети и обеспечения её изоляции;
   - Внедрите систему контроля доступа по стандарту 802.1x, чтобы снизить риск несанкционированного доступа терминалов в приватную сеть.

Аудит безопасности

1. **Проверка пользователей в сети**
   Рекомендуется регулярно проверять список активных пользователей для выявления несанкционированных подключений.
2. **Просмотр журналов устройства**
   Анализ журналов позволяет отслеживать IP-адреса, с которых выполнялись попытки входа на устройство, а также ключевые действия авторизованных пользователей.
3. **Настройка сетевого журналирования**
   Из-за ограниченного объема памяти устройства возможности хранения журналов ограничены. Для длительного сохранения записей рекомендуется активировать функцию сетевого журналирования, чтобы критически важные логи синхронизировались с сетевым сервером для последующего анализа.

Безопасность программного обеспечения

1. **Своевременное обновление прошивки**
   В соответствии с отраслевыми стандартами эксплуатации прошивку устройств необходимо своевременно обновлять до последней версии, чтобы обеспечить наличие новейших функций и исправлений уязвимостей. Если устройство подключено к публичной сети, рекомендуется включить функцию автоматической проверки обновлений в режиме онлайн для своевременного получения информации о выпускаемых производителем обновлениях прошивки.
2. **Своевременное обновление клиентского программного обеспечения**
   Рекомендуется загружать и использовать последние версии клиентского программного обеспечения.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных). Для этого следует размещать оборудование в специализированных серверных комнатах и стойках, а также внедрить систему контроля доступа и управления ключами, чтобы предотвратить несанкционированный доступ персонала, который может привести к повреждению аппаратного обеспечения и периферийного оборудования (например, USB-накопителей, последовательных портов).