

ASR1102A(V3)

Руководство пользователя



V1.0.2

Предисловие

Общий

Данное руководство описывает функции и работу считывателя доступа. Внимательно прочтите его перед использованием.
При использовании устройства сохраните инструкцию для дальнейшего использования.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
 DANGER	Указывает на высокую потенциальную опасность, которая, если её не избежать, приведёт к... смерти или серьезная травма.
 WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не избежать, может привести к... Привести к легким или умеренным травмам.
 CAUTION	Указывает на потенциальный риск, который, если его не избежать, может привести к повреждению имущества. повреждения, потеря данных, снижение производительности или непредсказуемые результаты.
 NOTE	Предоставляет дополнительную информацию в качестве дополнения к тексту.

История изменений

Версия	Содержание для пересмотра	Время выпуска
V1.0.2	Дополнительные требования к электропроводке.	Сентябрь 2024 г.
V1.0.1	Обновлено руководство.	Январь 2023 г.
V1.0.0	Первый релиз.	Февраль 2017 г.

Уведомление о защите конфиденциальности

Как пользователь устройства или оператор данных, вы можете собирать персональные данные других лиц, такие как их Лицо, аудиозапись, отпечатки пальцев и номерной знак автомобиля. Вам необходимо соблюдать местные правила. Законы и правила о защите конфиденциальности, призванные защищать законные права и интересы других лиц, путем внедрения мер, которые включают, помимо прочего: обеспечение четкой и наглядной информации. идентификация для информирования людей о существовании зоны наблюдения и предоставления необходимой информации. Контактная информация.

О руководстве пользователя

- Данное руководство носит исключительно справочный характер. Между руководством и другими документами могут быть обнаружены незначительные различия. продукт.
- Мы не несем ответственности за убытки, понесенные в результате эксплуатации продукта способами, не предусмотренными законом. соблюдение инструкций.
- Данное руководство будет обновляться в соответствии с последними законами и нормативными актами соответствующих юрисдикций.
Для получения подробной информации ознакомьтесь с бумажным руководством пользователя, воспользуйтесь нашим CD-ROM, отсканируйте QR-код или

Посетите наш официальный сайт. Данное руководство предназначено только для ознакомления. Между электронной и бумажной версиями могут быть незначительные различия.

- Все дизайнерские решения и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта. Возможно, будут некоторые расхождения между фактическим продуктом и руководством. Пожалуйста, свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации. • Возможны ошибки в печати или расхождения в описании функций, операций и технических данных. В случае возникновения каких-либо сомнений или споров мы оставляем за собой право окончательного толкования. • Если руководство (в формате PDF) не открывается, обновите программное обеспечение для чтения или попробуйте другое распространенное программное обеспечение для чтения. • Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в руководстве, являются собственностью их владельцев. соответствующих владельцев.
- В случае возникновения каких-либо проблем, пожалуйста, посетите наш веб-сайт, свяжитесь с поставщиком или службой поддержки клиентов. с использованием устройства. • В случае возникновения каких-либо неясностей или разногласий мы оставляем за собой право окончательного разъяснения.

Важные меры предосторожности и предупреждения

В этом разделе представлена информация о правильном обращении с устройством считывания карт, предотвращении опасностей и предотвращении повреждения имущества. Внимательно прочтите инструкцию перед использованием устройства считывания карт и соблюдайте ее правила при использовании.

Требования к транспорту



Транспортировать, использовать и хранить считыватель карт следует в пределах допустимых условий влажности и температуры.

Требования к хранению



Храните устройство для чтения карт в условиях допустимой влажности и температуры.

Требования к установке



- Не подключайте адаптер питания к считывателю карт, если адаптер включен. • Строго соблюдайте местные правила и стандарты электробезопасности. Убедитесь, что напряжение окружающей среды соответствует нормам. Стабильна и соответствует требованиям к электропитанию контроллера доступа.

- Не подключайте устройство чтения карт к двум или более типам источников питания, чтобы избежать его повреждения. Устройство для

чтения карт памяти. • Неправильное использование батареи может привести к возгоранию или взрыву.



- Персонал, работающий на высоте, должен принимать все необходимые меры для обеспечения личной безопасности, включая ношение каски и страховочных ремней.

- Не размещайте устройство чтения карт в местах, подверженных воздействию солнечных лучей или вблизи источников тепла. • Берегите устройство чтения карт от влаги, пыли и копоти. •

Установите устройство чтения карт на устойчивой поверхности, чтобы предотвратить его падение. • Установите устройство чтения карт в хорошо проветриваемом месте и не закрывайте вентиляционные отверстия. • Используйте адаптер или блок питания, предоставленный производителем. • Используйте кабели питания, рекомендованные для вашего региона и соответствующие номинальной мощности.

технические характеристики.

- Источник питания должен соответствовать требованиям стандарта ES1 в IEC 62368-1 и иметь мощность не выше PS2. Обратите внимание, что требования к источнику питания указаны на этикетке считывателя карт.

- Устройство чтения карт относится к электроприборам класса I. Убедитесь, что источник питания устройства чтения карт исправен. Считывающее устройство подключено к розетке с защитным заземлением.

Эксплуатационные требования



- Перед использованием проверьте правильность подключения блока питания.
- Не отключайте шнур питания сбоку считывателя карт, пока адаптер включен
 - Используйте считыватель карт в пределах допустимого диапазона входной и выходной мощности.
 - Используйте считыватель карт в допустимых условиях влажности и температуры.
 - Не допускайте попадания жидкости на считыватель карт и убедитесь, что на нем нет предметов, наполненных жидкостью, чтобы предотвратить попадание жидкости внутрь.
 - Не разбирайте считыватель карт без консультации специалиста.

Оглавление

Предисловие.....	Я
Важные меры предосторожности и предупреждения.....	III
1 Обзор продукта.....	1
1.1 Введение.....	1
1.2 Размеры.....	2
2. Проводка и монтаж.....	4
2.1 Требования к проводке.....	4
2.2 Процедура установки.....	4
3 Обновление системы.....	7
3.1 Обновление через SmartPSS	
Lite.....	7
Tool.....	7
3.2 Обновление через Config	
Приложение 1 Рекомендация по безопасности.....	8

1. Обзор продукта

1.1 Введение

В большинстве систем контроля доступа считыватель карт доступа представляет собой систему безопасности, требующую считывания идентификационной карты для подтверждения того, что человек, входящий в помещение/пространство, имеет право доступа. Он подходит для самых разных сценариев использования, таких как офисные здания, школы, комплексы, жилые районы, заводы, общественные места, бизнес-центры и правительственные здания.

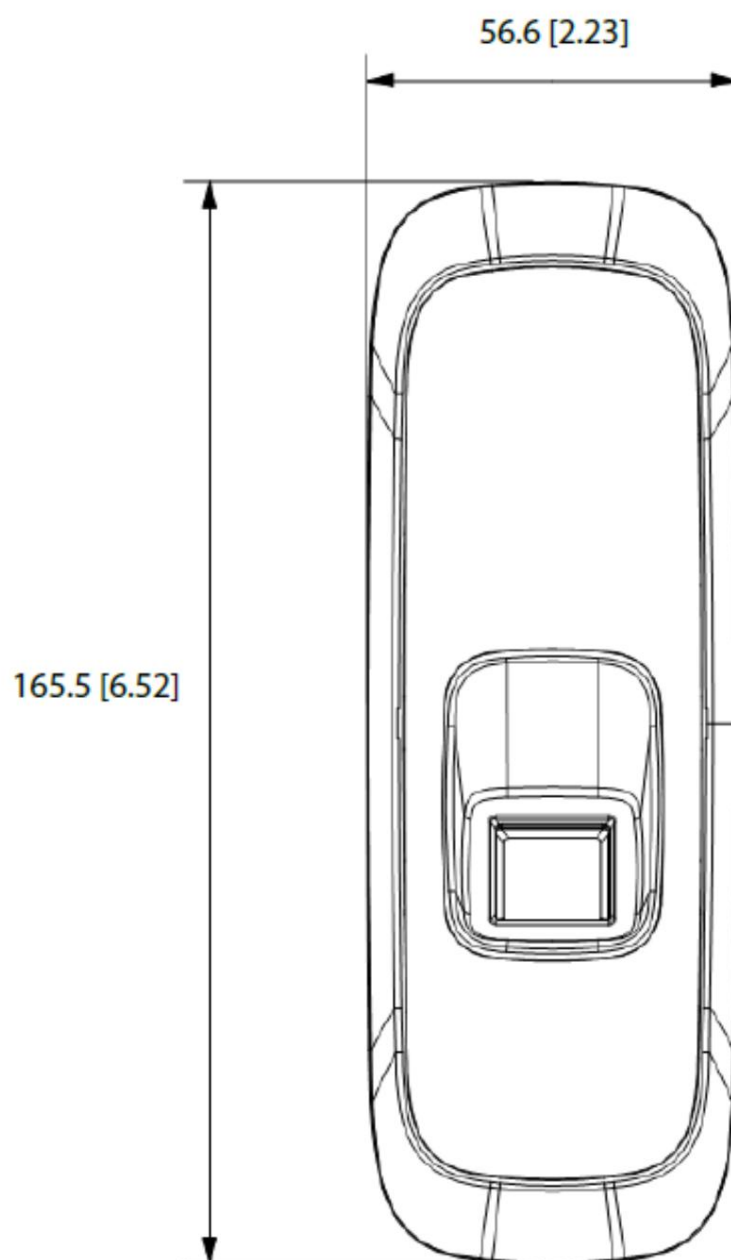
- Синий свет. •

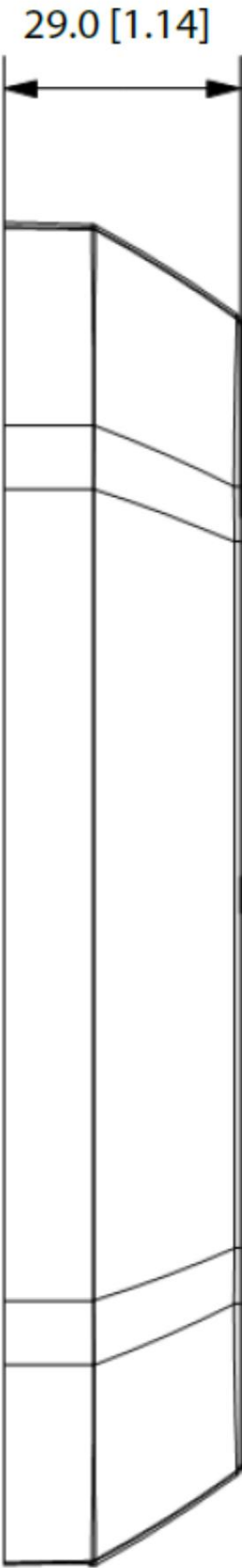
Бесконтактный считыватель (только чтение), расстояние считывания карты 3–5 см, время отклика < 0,3 с. • Время отклика при проверке отпечатков пальцев 0,5 с. • До 3000 отпечатков пальцев. • Поддержка протоколов

Wiegand и RS-485. Скорость передачи данных RS-485 составляет 9600 бит/с. • Расширенная служба управления ключами для снижения риска утечки данных и/или дублирования карт. • Режимы распознавания: карта, отпечаток пальца, карта + отпечаток пальца и карта/отпечаток пальца. • Поддержка сторожевого таймера и защиты от несанкционированного доступа. • Защита от статического электричества и короткого замыкания. • Онлайн-обновление. • Рабочая температура от -10 °C до +55 °C; рабочая влажность 95%. • Рабочее напряжение: 9–15 В постоянного тока, рабочий ток: 150 мА.

1.2 Размеры

Рисунок 1-1. Габариты считывателя карт (единица измерения: мм [дюйм])





2. Проводка и монтаж

2.1 Требования к проводке

- Подключите устройство чтения карт к портам Wiegand или RS-485 в зависимости от типа устройства.
Считыватель карт.
- Подберите подходящие провода в соответствии с требованиями к проводке.

Таблица 2-1. Обзор портов.

Цвет	Порт	Описание
Красный	12 В	Источник питания
Черный	GND	
Синий	ALARM_OUT	Выходные сигналы тревоги (для считывателя карт Wiegand)
Белый	D1	Сигналы передачи Виганда (для считывателя карт Wiegand)
Зеленый	D0	
Коричневый	LED/BELL_CTRL	Сигналы, реагирующие на Wiegand (для считывателя карт Wiegand)
Желтый	RS-485_B	считыватель карт RS-485
Фиолетовый	RS-485_A	

Таблица 2-2. Требования к подключению считывателя карт.

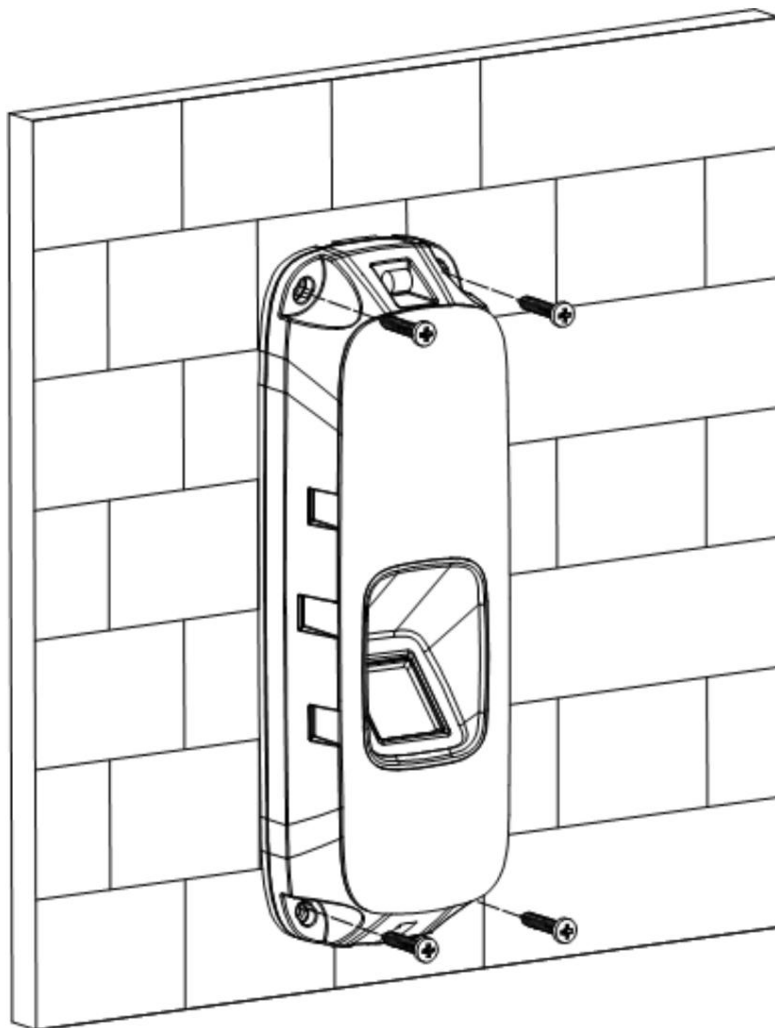
Тип	Требования к импедансу	Требования к длине
считыватель карт RS485	Соединяет провода RS-485, импеданс отдельного провода должно быть 10 Ом.	100 м. Выше стандарта UL1061 24AWG экранированные провода рекомендуется.
считыватель карт Wiegand	Соединяет провода Wiegand и импеданс отдельного провода должно быть 2 Ом.	80 м. Выше стандарта UL1061 18AWG экранированные провода рекомендуется.

2.2 Процедура установки

Процедура

Шаг 1. Снимите переднюю крышку устройства, а затем прикрепите устройство к стене.
винты.

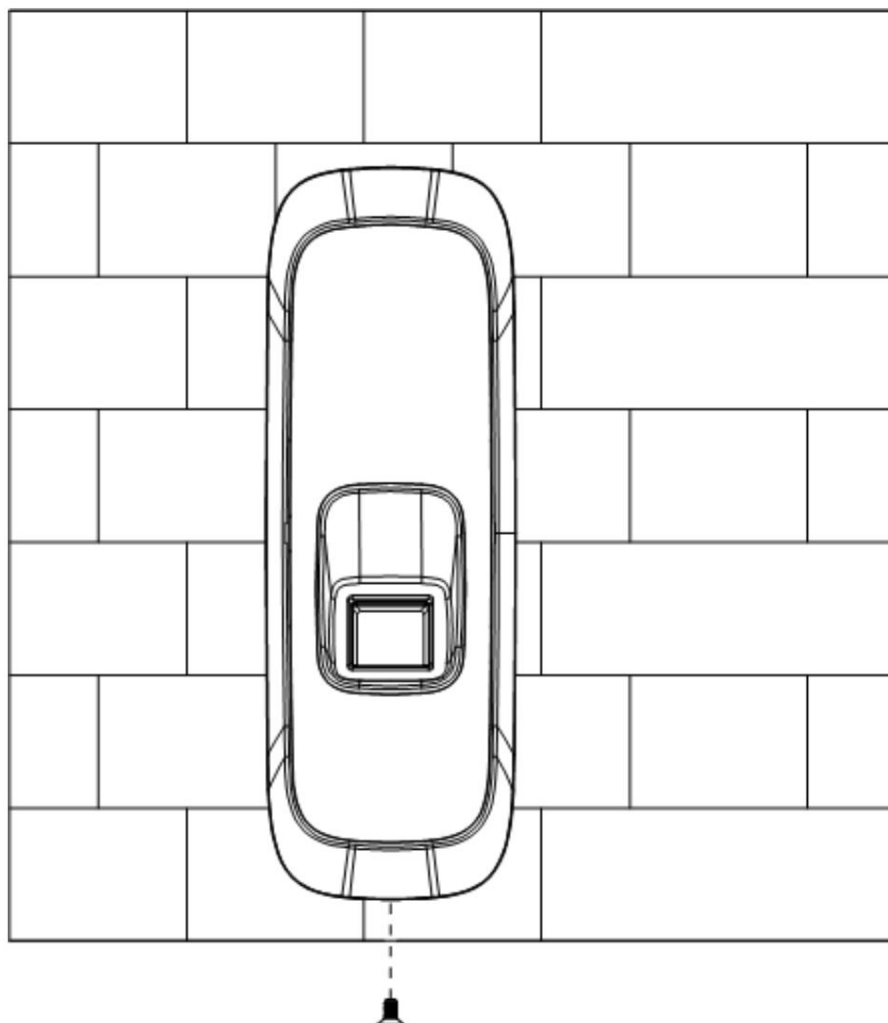
Рисунок 2-1. Отверстия для сверления (единица измерения: мм [дюйм])



Шаг 2. Прикрепите переднюю крышку к устройству.

Шаг 3. Вкрутите один винт снизу, чтобы закрепить устройство.

Рисунок 2-2. Отверстия для сверления (единица измерения: мм [дюйм])



3. Обновление системы

3.1 Обновление через SmartPSS Lite

Предварительные требования

- Считыватель карт был подключен к контроллеру доступа через интерфейс RS-485.
- Контроллер доступа и считыватель карт включены.

Процедура

Шаг 1 Установите SmartPSS Lite и войдите в систему, затем выберите «Диспетчер устройств».

Шаг 2. Нажмите .

Рисунок 3-1. Выберите контроллер доступа.

☒	No.	Name	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
☒	1	Device01	172.16.1.100	Access Controller	ASC2208C-S	37777	010/8/8	Online	6H029E1YAJ5FD7D	   

Шаг 3. Нажмите и выберите файл обновления.

Шаг 4. Нажмите «Обновить».

Индикатор устройства чтения карт мигает синим цветом до завершения обновления, после чего устройство чтения карт автоматически перезапускается.

3.2 Обновление через инструмент конфигурации

Предварительные требования

- Считыватель карт был подключен к контроллеру доступа через интерфейс RS-485.
- Контроллер доступа и считыватель карт включены.

Процедура

Шаг 1 Установите и откройте Configtool, затем выберите пункт «Обновление устройства».

Шаг 2. Щелкните по контроллеру доступа, а затем щелкните Шаг 3. .

Щелкните «Обновить».

Индикатор устройства чтения карт мигает синим цветом до завершения обновления, после чего устройство чтения карт автоматически перезапускается.

Приложение 1. Рекомендации по безопасности.

Управление учетными записями

1. Используйте сложные пароли.

Для установки паролей воспользуйтесь следующими рекомендациями:

- Длина не должна быть меньше 8 символов;
- Включать как минимум два типа символов: прописные и строчные буквы, цифры и символы;
- Не содержать название счета или название счета в обратном порядке;
- Не использовать непрерывные символы, такие как 123, abc и т. д.;
- Не использовать повторяющиеся символы, такие как 111, aaa и т. д.

2. Периодически меняйте пароли.

Рекомендуется периодически менять пароль устройства, чтобы снизить риск его угадывания или взлома.

3. Распределите учетные записи и права доступа надлежащим образом.

Добавляйте пользователей в соответствии с требованиями к обслуживанию и управлению и назначайте им минимальные наборы прав доступа.

4. Включите функцию блокировки учетной записи.

Функция блокировки учетной записи включена по умолчанию. Рекомендуется оставить ее включенной для защиты безопасности учетной записи. После нескольких неудачных попыток ввода пароля соответствующая учетная запись и исходный IP-адрес будут заблокированы.

5. Своевременно устанавливайте и обновляйте информацию для сброса пароля.

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

Конфигурация службы

1. Включите HTTPS.

Рекомендуется включить протокол HTTPS для доступа к веб-сервисам через защищенные каналы.

2. Зашифрованная передача аудио и видео.

Если ваши аудио- и видеоданные очень важны или конфиденциальны, рекомендуется использовать функцию зашифрованной передачи, чтобы снизить риск перехвата ваших аудио- и видеоданных во время передачи.

3. Отключите некритичные службы и используйте безопасный режим.

Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точки доступа и т. д., чтобы уменьшить поверхность атаки.

При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, помимо прочего, следующие сервисы:

- SNMP: Выберите SNMP v3 и настройте надежное шифрование и пароли аутентификации.
- SMTP: Выберите TLS для доступа к серверу почтовых ящиков.
- FTP: Выберите SFTP и настройте сложные пароли.
- Точка доступа: Выберите режим шифрования WPA2-PSK и настройте сложные пароли.

4. Измените порты 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 его подбора злоумышленниками.

Сетевая конфигурация

1. Включите список разрешенных .

Рекомендуется включить функцию списка разрешенных IP-адресов и разрешить доступ к устройству только IP-адресам из этого списка. Поэтому обязательно добавьте IP-адрес вашего компьютера и IP-адрес вашего устройства в список разрешенных.

2. Привязка MAC-адреса

Рекомендуется привязать IP-адрес шлюза к MAC-адресу устройства, чтобы снизить риск подмены ARP-адреса.

3. Создайте безопасную сетевую среду.

Для повышения уровня безопасности устройств и снижения потенциальных киберрисков рекомендуется следующее:

- Отключите функцию переадресации портов маршрутизатора, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети;
- Разделите сеть в соответствии с фактическими потребностями: если между двумя подсетями нет потребности в обмене данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети с целью достижения сетевой изоляции;
- Внедрить систему аутентификации доступа 802.1x для снижения риска несанкционированного доступа терминалов к частной сети.

Аудит безопасности

1. Проверьте пользователей сети.

Рекомендуется регулярно проверять пользователей в сети, чтобы выявлять нелегальных пользователей.

2. Проверьте журнал устройства.

Просмотрев журналы, вы можете узнать об IP-адресах, которые пытались войти в систему устройства, и о ключевых операциях авторизованных пользователей.

3. Настройка сетевого журнала

Из-за ограниченной емкости памяти устройств объем сохраняемых журналов ограничен. Если вам необходимо сохранять журналы в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию критически важных записей с сервером сетевого журнала для трассировки.

Безопасность программного обеспечения

1. Своевременно обновляйте прошивку.

В соответствии со стандартными отраслевыми требованиями, для обеспечения актуальности функций и безопасности устройства необходимо своевременно обновлять его прошивку до последней версии. Если устройство подключено к общедоступной сети, рекомендуется включить функцию автоматического обнаружения онлайн-обновлений, чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.

2. Своевременно обновляйте клиентское программное обеспечение.

Рекомендуется загрузить и использовать последнюю версию клиентского программного обеспечения.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных), например, разместить устройство в специально отведенном машинном помещении и шкафу, а также установить систему контроля доступа.

а также внедрена система управления ключами для предотвращения повреждения оборудования и других периферийных устройств (например, USB-накопителей, последовательных портов) посторонними лицами.