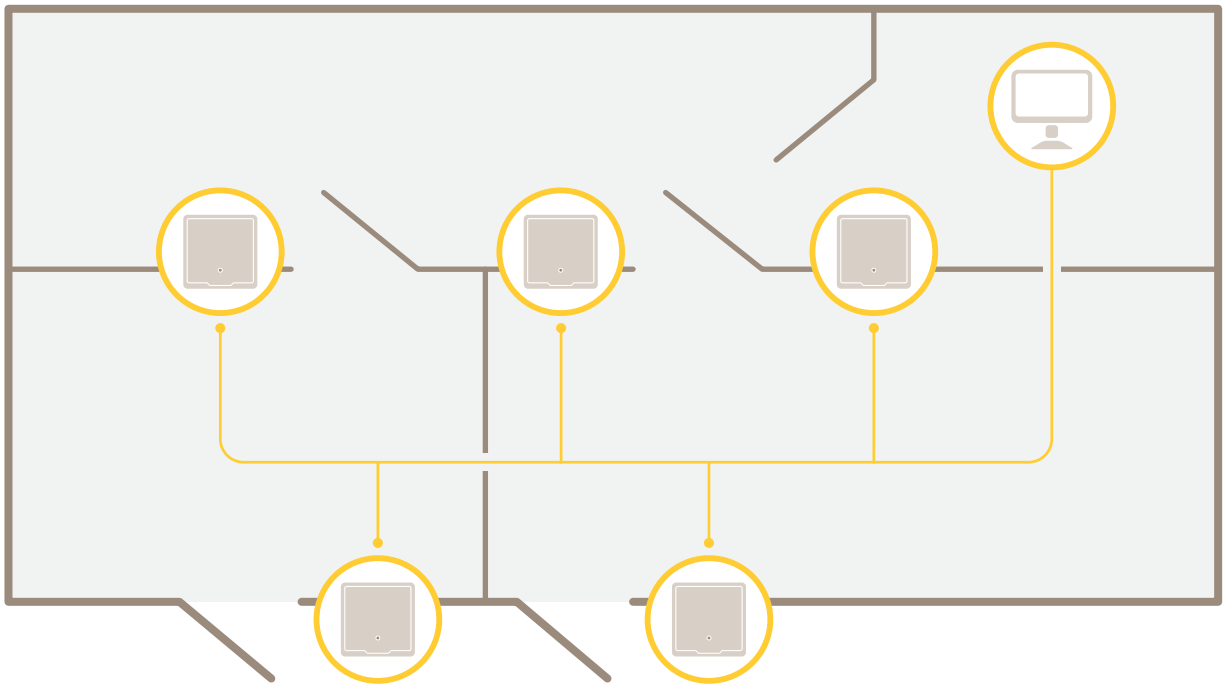
AXIS A1601 Network Door Controller

Руководство пользователя

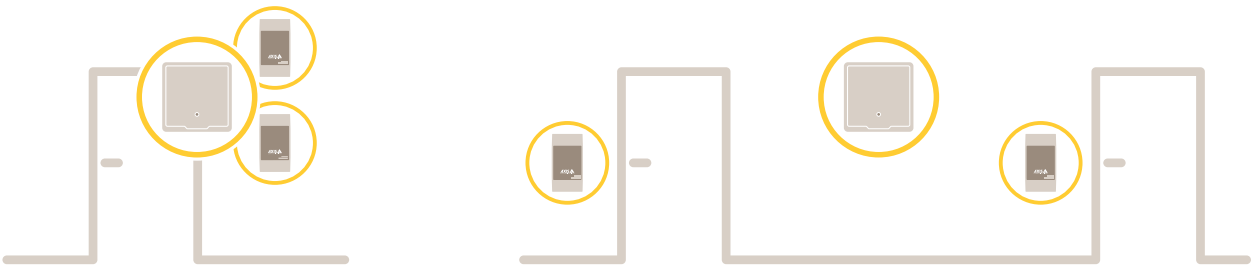
Содержание

Общие сведения о решении



Сетевой дверной контроллер легко подсоединить к существующей IP-сети, по которой он будет получать питание, что устраняет необходимость прокладки специальных кабелей.

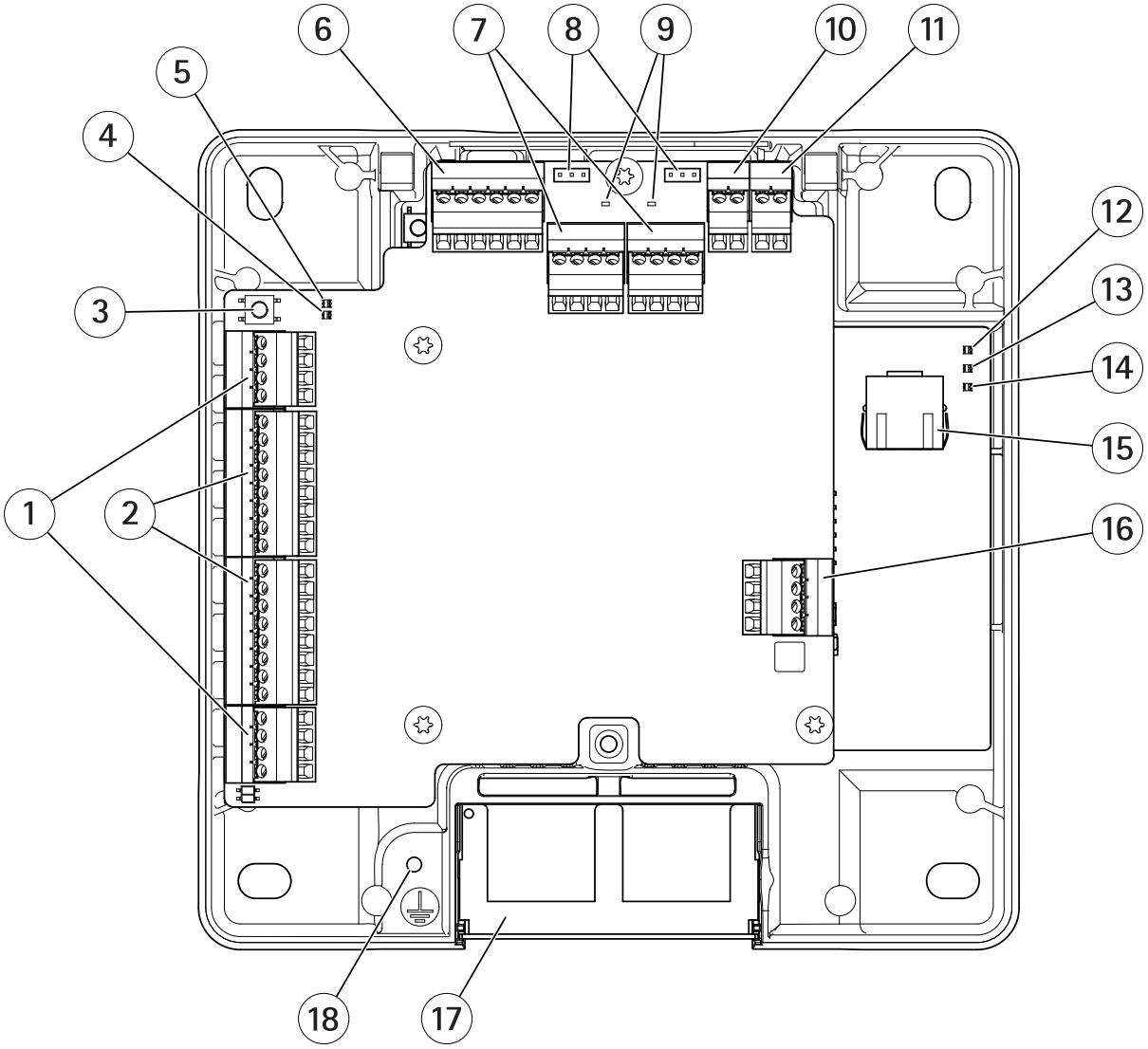
Общие сведения о решении



Каждый сетевой дверной контроллер представляет собой интеллектуальное устройство, которое нетрудно смонтировать рядом с дверью. Его можно использовать для питания и управления считывателями (не более двух).

Общий вид устройства

Общий вид устройства



1 *Разъем дверного датчика на стр. 44 (2 шт.)*
2 *Разъем считывателя на стр. 42 (2 шт.)*
3 *Кнопка управления на стр. 41*
4 *Индикатор перегрузки по току считывателя*
5 *Индикатор перегрузки по току реле*
6 *Вспомогательный разъем на стр. 45*
7 *Разъем реле на стр. 44 (2 шт.)*
8 *Перемычка реле (2 шт.)*
9 *Индикатор реле (2 шт.)*
10 *Входной разъем для подключения резервной батареи на стр. 47*
11 *Разъем питания на стр. 47*
12 *Индикатор питания*
13 *Индикатор состояния*

Общий вид устройства

14 *Светодиодный индикатор сети*
15 *Сетевой разъем на стр. 41*
16 *Внешний разъем на стр. 46*
17 *Двусторонний кабельный канал*
18 *Положение заземления*

Поиск устройства в сети

Для поиска устройств Axis в сети и назначения им IP-адресов в Windows® можно использовать приложение AXIS IP Utility или AXIS Device Manager. Оба эти приложения можно бесплатно скачать на странице *axis.com/support*.

Дополнительные сведения о поиске устройств и назначении IP-адресов см. в документе
How to assign an IP address and access your device (Как назначить IP-адрес и получить доступ к устройству).

Доступ к устройству

1. Откройте браузер и введите IP-адрес или имя хоста устройства Axis.

   Если вы не знаете IP-адрес, используйте утилиту AXIS IP Utility или приложение AXIS Device Manager, чтобы найти устройство в сети.

2. Введите имя пользователя и пароль. Для доступа к устройству в первый раз необходимо задать пароль root. См. .

3. В браузере откроется веб-страница устройства. Начальная страница называется Overview (Обзор).

Как получить доступ к устройству через Интернет

Сетевой маршрутизатор позволяет устройствам частной локальной сети совместно использовать единое подключение к Интернету. Для этого сетевой трафик из частной сети перенаправляется в Интернет.

Большинство маршрутизаторов по умолчанию настроены так, чтобы исключить возможность доступа к частной локальной сети из общедоступной сети (Интернета).

Если к устройству Axis, которое находится во внутренней локальной сети, нужно открыть доступ с внешней стороны NAT-маршрутизатора (из глобальной сети), необходимо включить функцию **NAT Traversal** (прохождение NAT). При должной настройке прохождения NAT весь HTTP-трафик, поступающий на внешний HTTP-порт NAT-маршрутизатора, будет перенаправляться на устройство.

Как включить функцию NAT Traversal

- Выберите последовательно **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Дополнительная настройка контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.
- Нажмите кнопку **Включить**.
- Вручную настройте NAT-маршрутизатор так, чтобы разрешить доступ из Интернета.

Примечание.

- В данном контексте под «маршрутизатором» понимается любое устройство сетевой маршрутизации, включая NAT-маршрутизатор, сетевой маршрутизатор, интернет-шлюз, широкополосный маршрутизатор, разделяемое широкополосное устройство или программное обеспечение, например, межсетевой экран.
- Функция NAT Traversal будет работать, только если она поддерживается маршрутизатором. Маршрутизатор также должен поддерживать технологию UPnP®.

Безопасные пароли

Важно!

Устройства Axis передают первоначально установленный пароль по сети в текстовом виде. Чтобы защитить свое устройство, после первого входа в систему настройте безопасное зашифрованное HTTPS-соединение, а затем измените пароль.

Поиск устройства в сети

Пароль устройства — это основное средство защиты ваших данных и сервисов. Для устройств Axis не предусмотрена собственная политика использования паролей, так как эти устройства могут входить в состав систем разного типа и назначения.

Для защиты данных мы настоятельно рекомендуем соблюдать указанные ниже правила.

- Используйте пароль длиной не менее 8 символов. Желательно создать пароль с помощью генератора паролей.
- Никому не сообщайте пароль.
- Периодически меняйте пароль — хотя бы раз в год.

Как настроить пароль пользователя root

Для получения доступа к устройству Axis необходимо задать пароль для администратора по умолчанию **root**. Сделать это можно в окне **Configure Root Password (Настройка пароля root)**, которое откроется при первой попытке доступа к устройству.

Для предотвращения перехвата данных пароль root можно настроить с использованием зашифрованного HTTPS-соединения, которое требует сертификат HTTPS. HTTPS (Hypertext Transfer Protocol over SSL) — протокол, используемый для шифрования трафика между веб-браузерами и серверами. Сертификат HTTPS обеспечивает зашифрованную передачу данными. См. *HTTPS на стр. 28*.

По умолчанию для администратора используется имя пользователя **root**. Изменить или удалить его невозможно. Если вы забудете пароль, необходимо произвести сброс параметров устройства к заводским установкам по умолчанию. См. *Сброс к заводским установкам на стр. 38*.

Чтобы задать пароль, введите его непосредственно в диалоговом окне.

Страница Overview (Обзор)

В разделе Overview (Обзор) на веб-странице устройства указано его название, MAC-адрес, IP-адрес и версия встроенного ПО Кроме того, с помощью этой страницы можно идентифицировать дверной контроллер в сети.

При первой попытке доступа к устройству Axis на странице Overview (Обзор) появится предложение настроить оборудование, установить дату и время, а также задать настройки сети. Дополнительные сведения о настройке системы см. в разделе *Пошаговая настройка на стр. 9* .

Чтобы вернуться на страницу Overview (Обзор) с любой другой веб-страницы устройства, выберите пункт **Overview (Обзор)** на панели меню.

Конфигурация системы

Чтобы открыть страницы настройки устройства, нажмите **Setup (Настройка)** в правом верхнем углу страницы Overview (Обзор).

Настройку устройства Axis производят администраторы. Дополнительные сведения о пользователях и администраторах см. в разделе *стр. 28*.

Пошаговая настройка

Прежде чем начать пользоваться системой контроля доступа, необходимо выполнить следующие этапы ее настройки.

1. Если английский не является вашим основным языком, то можно сделать так, чтобы на веб-странице устройства использовался другой язык. См. *Выбор языка на стр. 9*.
2. Установка даты и времени. См. *стр. 9*.
3. Настройка сетевых параметров. См. *стр. 10*.
4. Настройка дверного контроллера и подключенных устройств, среди которых считыватели, замки и устройства, обрабатывающие запросы на выход (REX-устройства). См. *Настройка оборудования на стр. 11*.
5. Проверка подключения оборудования. См. *стр. 18*.
6. Настройка карт и форматов. См. *стр. 19*.

Рекомендации по обслуживанию см. в разделе *Инструкции по обслуживанию на стр. 22*.

Выбор языка

По умолчанию на веб-странице устройства используется английский язык, но его можно сменить на любой из языков, включенных во встроенное ПО устройства. Дополнительные сведения о последней версии встроенного ПО см. на сайте *www.axis.com*.

Сменить язык можно на любой веб-странице устройства.

Чтобы сменить язык, нажмите значок  , чтобы открыть список, в котором можно выбрать язык. Все веб-страницы устройства и страницы справки будут отображаться на выбранном языке.

Примечание.

- При смене языка также меняется формат даты, чтобы обеспечить наилучшее соответствие выбранному языку. Действующий формат отображается в полях данных.
- После сброса устройства к заводским установкам по умолчанию веб-страница устройства будет вновь отображаться на английском языке.
- При восстановлении или перезапуске устройства, а также при обновлении встроенного ПО на веб-странице устройства будет по-прежнему использоваться выбранный язык.

Установка даты и времени

Чтобы настроить дату и время в устройстве Axis, перейдите в меню **Setup > Date & Time (Настройка > Дата и время)**.

Дату и время можно настроить следующими способами:

- Получение даты и времени от NTP-сервера. См. *стр. 10*.
- Установка даты и времени вручную. См. *стр. 10*.
- Получение даты и времени от компьютера. См. *стр. 10*.

Current controller time (Текущее время контроллера). Отображает текущие дату и время дверного контроллера (по 24-часовой шкале).

Те же параметры для даты и времени доступны на страницах System Options (Параметры системы). Перейдите в меню **Setup > Additional Controller Configuration > System Options > Date & Time (Настройка > Дополнительная настройка контроллера > Параметры системы > Дата и время)**.

Получение даты и времени от NTP-сервера

1. Выберите в меню **Setup > Date & Time (Настройка > Дата и время)**.
2. Выберите свой **Timezone (Часовой пояс)** из раскрывающегося списка.
3. Если в вашем регионе используется переход на летнее время, выберите **Adjust for daylight saving (Учитывать переход на летнее время)**.
4. Выберите **Synchronize with NTP (Синхронизировать с NTP-сервером)**.
5. Выберите адрес по умолчанию DHCP-сервера или введите адрес NTP-сервера.
6. Нажмите кнопку **Save (Сохранить)**.

При синхронизации с NTP-сервером дата и время постоянно обновляются, поскольку эти данные поступают от NTP-сервера в виде push-сообщений. Для получения сведений о настройках NTP-сервера см. раздел *Настройка NTP на стр. 32*.

Если для NTP-сервера используется имя хоста, то необходимо настроить DNS-сервер. См. *Настройка DNS на стр. 31*.

Установка даты и времени вручную

1. Выберите в меню **Setup > Date & Time (Настройка > Дата и время)**.
2. Если в вашем регионе используется переход на летнее время, выберите **Adjust for daylight saving (Учитывать переход на летнее время)**.
3. Выберите вариант **Set date & time manually (Установить дату и время вручную)**.
4. Введите нужные дату и время.
5. Нажмите кнопку **Save (Сохранить)**.

Данный способ служит для однократной установки даты и времени и не предполагает автоматическое обновление. Это означает, что при необходимости изменить дату или время изменения придется вводить вручную, так как подключение к внешнему NTP-серверу отсутствует.

Получение даты и времени от компьютера

1. Выберите в меню **Setup > Date & Time (Настройка > Дата и время)**.
2. Если в вашем регионе используется переход на летнее время, выберите **Adjust for daylight saving (Учитывать переход на летнее время)**.
3. Выберите вариант **Set date & time manually (Установить дату и время вручную)**.
4. Нажмите кнопку **Sync now and save (Синхронизировать сейчас и сохранить)**.

При использовании времени компьютера дата и время однократно синхронизируются с временем компьютера и не будут в дальнейшем обновляться автоматически. Это означает, что если вы измените дату или время на компьютере, который используется для управления системой, вам придется вновь синхронизировать эти данные.

Настройка сетевых параметров

Основные сетевые параметры настраиваются в меню **Setup > Network Settings (Настройка > Параметры системы)** или в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Основные)**.

Для получения дополнительных сведений о сетевых параметрах см. раздел *Сеть на стр. 30*

Настройка оборудования

До завершения настройки оборудования к устройству Axis можно подключить считыватели, замки и другие устройства. Однако проще будет подключить устройства после завершения настройки оборудования. Это связано с тем, что после завершения настройки будет доступна схема контактов оборудования. Схема контактов оборудования служит руководством при подсоединении устройств к контактам. С ней также можно сверяться в процессе обслуживания системы. Инструкции по обслуживанию см. в разделе *стр. 22*.

При первичной настройке оборудования выберите один из способов, описанных ниже.

- Импорт файла конфигурации оборудования. См. *стр. 11*.
- Создание новой конфигурации оборудования. См. *стр. 12*.

Примечание.

Если оборудование до этого не настраивалось или было удалено, в панели уведомлений на странице Overview (Обзор) будет доступен элемент **Hardware Configuration (Настройка оборудования)**.

Как импортировать файл конфигурации оборудования

Чтобы ускорить настройку оборудования для устройства Axis, можно импортировать файл конфигурации оборудования.

Экспортируя этот файл из одного устройства и импортируя его на другие устройства, можно несколько раз применить один и тот же вариант настройки оборудования, не повторяя каждый раз одни и те же шаги. Можно также хранить экспортированные файлы как резервные копии и использовать их для восстановления предыдущих конфигураций оборудования. Дополнительные сведения см. в разделе *Как экспортировать файл конфигурации оборудования на стр. 11*.

Импортирование файла настройки оборудования:

1. Перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)**.
2. Нажмите кнопку **Import hardware configuration (Импорт конфигурации оборудования)** или, если уже имеется настроенная конфигурация оборудования, кнопку **Reset and import hardware configuration (Сброс и импорт конфигурации оборудования)**.
3. В диалоговом окне выбора файла найдите и выберите файл настройки оборудования (*.json) на своем компьютере.
4. Нажмите кнопку **OK**.

Как экспортировать файл конфигурации оборудования

Чтобы несколько раз применить один и тот же вариант настройки оборудования, можно экспортировать файл конфигурации оборудования для устройства Axis. Можно также хранить экспортированные файлы как резервные копии и использовать их для восстановления предыдущих конфигураций оборудования.

Примечание.

Однако невозможно экспортировать файл конфигурации оборудования на этаже.

Настройки беспроводных замков не включаются в экспортируемый файл настройки оборудования.

Экспортирование файла настройки оборудования:

1. Перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)**.

2. Нажмите кнопку **Export hardware configuration (Экспортировать файл настройки оборудования**.
3. В зависимости от используемого браузера для завершения экспорта могут потребоваться какие-то действия в диалоговом окне.

   Если не указано иное, то экспортированный файл (*.json) сохраняется в папке загрузок по умолчанию. Папку загрузок можно выбрать в пользовательских настройках браузера.

Создание новой конфигурации оборудования

Следуйте инструкциям, соответствующим вашим конкретным требованиям:

- *Как создать новую конфигурацию оборудования без периферийных устройств на стр. 12*
- *Как создать новую конфигурацию оборудования для беспроводных замков на стр. 16*
- *Как создать новую конфигурацию оборудования с функцией управления лифтами (AXIS A9188) на стр. 16*

Как создать новую конфигурацию оборудования без периферийных устройств

1. Перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)** и нажмите кнопку **Start new hardware configuration (Создать новую конфигурацию оборудования)**.
2. Введите имя устройства Axis.
3. Выберите количество подключенных дверей и нажмите кнопку **Next (Далее)**.
4. Настройте дверные мониторы (датчики положения двери) и замки в соответствии со своими требованиями и нажмите кнопку **Next (Далее)**. Дополнительные сведения о доступных параметрах см. в разделе *Настройка замков и дверных мониторов на стр. 12*.
5. Настройте считыватели и REX-устройства, которые будут использоваться, затем нажмите кнопку **Finish (Готово)**. Дополнительные сведения о доступных параметрах см. в разделе *Как настроить считыватели и REX-устройства на стр. 14*.
6. Нажмите кнопку **Close (Закрыть)** или перейдите по ссылке для просмотра схемы контактов оборудования.

Настройка замков и дверных мониторов

После выбора параметров дверей в новой конфигурации оборудования можно перейти к настройке дверных мониторов и замков.

1. Если будет использоваться дверной монитор, выберите элемент **Door monitor (Дверной монитор)**, а затем выберите параметр, соответствующий организации цепей дверного монитора.
2. Если дверь должна блокироваться сразу же после открывания, выберите **Cancel access time once door is opened (Отменить время доступа после открывания двери)**.

   Если вы хотите отложить блокировку, установите время задержки в миллисекундах в **Relock time (Время блокировки)**.
3. Задайте временные параметры дверного монитора или, если дверной монитор не будет использоваться, — параметры для времени блокировки.
4. Выберите параметры, соответствующие организации цепей дверного монитора.
5. Если будет использоваться дверной монитор, выберите элемент **Lock monitor (Монитор блокировки)** и затем выберите параметры, соответствующие организации цепей монитора блокировки.
6. Если должны отслеживаться входные сигналы от считывателей, REX-устройств и дверных мониторов, выберите **Enable supervised inputs (Включить контроль входных сигналов)**.

   Дополнительные сведения см. в разделе *Как использовать контролируемые входы на стр. 15*.

Примечание.

- Большинство параметров замков, дверных мониторов и считывателей можно изменить без сброса и создания новой конфигурации оборудования. Перейдите в меню **Setup > Hardware Reconfiguration (Настройка > Повторная настройка оборудования)**.
- Для одного дверного контроллера можно подключить один монитор блокировки. Поэтому, если используются двери с двойной блокировкой, то монитором блокировки может быть снабжен только один замок. Если к одному дверному контроллеру подключены две двери, то нельзя использовать мониторы блокировки.

О дверном мониторе и параметрах времени

Для дверного монитора доступны следующие параметры:

- **Door monitor (Дверной монитор)** — выбран по умолчанию. Каждая дверь снабжена собственным дверным монитором, который, например, будет подавать сигнал тревоги, если дверь пытаются открыть силой или она слишком долго остается открытой. Отмените выбор этого элемента, если дверной монитор не будет использоваться.
  - **Open circuit = Closed door (Разомкнутая цепь = закрытая дверь)** — выберите этот элемент, если нормальным состоянием является разомкнутая цепь дверного монитора. При замыкании цепи дверной монитор подает сигнал тревоги, означающий, что дверь открыта. Когда цепь разомкнута, дверной монитор подает сигнал, означающий, что дверь закрыта.
  - **Open circuit = Open door (Разомкнутая цепь = открытая дверь)** — выберите этот элемент, если нормальным состоянием является замкнутая цепь дверного монитора. При размыкании цепи дверной монитор подает сигнал тревоги, означающий, что дверь открыта. Когда цепь замкнута, дверной монитор подает сигнал, означающий, что дверь закрыта.
- **Cancel access time once door is opened (Отменить время доступа после того, как дверь открыта)** — выберите этот параметр, чтобы предотвратить несанкционированный проход нескольких лиц. Как только дверной монитор укажет, что дверь была открыта, замок будет заблокирован.

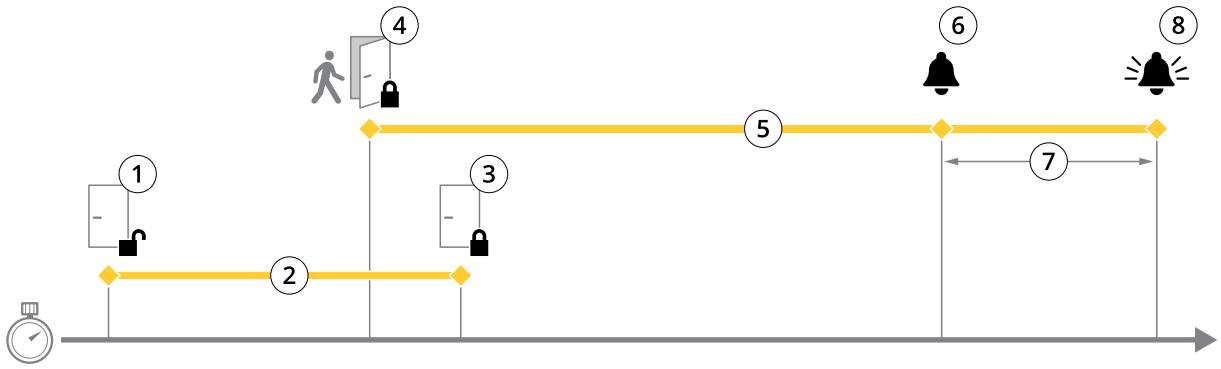
Для двери всегда доступны следующие параметры времени:

- **Access time (Время доступа)** — задайте количество секунд, в течение которых дверь должна оставаться разблокированной после предоставления доступа. Дверь остается разблокированной до момента открывания или пока не истечет заданное время. Дверь будет заблокирована, когда она закроется, независимо от того, истекло время доступа или нет.
- **Long access time (Длительное время доступа)** — задайте количество секунд, в течение которых дверь должна оставаться разблокированной после предоставления доступа. Значение параметра «Длительное время доступа» будет активировано для пользователей, у которых выбран этот параметр; его значение переопределяет уже заданное значение времени доступа.

Установите флажок у параметра **Door monitor (Дверной монитор)**, чтобы стали доступными следующие варианты для выбора времени:

- **Open too long time (Открыта слишком долго)** — задайте количество секунд, в течение которых дверь может оставаться открытой. Если дверь остается открытой по истечении заданного времени, то подается сигнал тревоги, соответствующий условию« Открыта слишком долго». Задайте правило для настройки действия, которое будет инициироваться событием "Открыта слишком долго".
- **Pre-alarm time (Время подачи предварительного сигнала)** — предварительный сигнал служит предупреждением, и он подается до истечения предельного времени, заданного параметром «Открыта слишком долго». Этот сигнал информирует администратора и предупреждает человека, входящего в дверь, о необходимости ее закрыть, иначе будет подан сигнал тревоги, соответствующий условию «Открыта слишком долго». Конкретное предупреждение зависит от того, как настроено правило действия. Задайте время (в секундах), когда система должна подать предварительный предупреждающий сигнал. По истечении этого времени будет активирован сигнал тревоги «Открыта слишком долго». Чтобы предварительный сигнал тревоги не подавался, задайте параметр «Время подачи предварительного сигнала» равным 0.

Конфигурация системы



1 *Доступ предоставлен — замок отпирается*
2 *Время доступа*
3 *Никаких действий не предпринято — замок запирается*
4 *Выполнено действие (открыта дверь) — замок запирается или остается незапертым до закрытия двери*
5 *Открыта слишком долго*
6 *Предварительный сигнал тревоги выключается*
7 *Время подачи предварительного сигнала*
8 *Сигнал тревоги «Открыта слишком долго» выключается*

Сведения о том, как настроить правило действия, см. в разделе *Как настроить правила действия на стр. 24*.

О вариантах блокировки

Для цепи блокировки доступны следующие параметры:

- Параметр **Relay (Реле)** можно использовать, только если на один дверной контроллер приходится один замок. Если к дверному контроллеру подключено две двери, то реле можно использовать только для замка второй двери.
- **None (Нет)** — доступно только для замка 2. Выберите данный вариант, если будет использоваться только один замок.

Для конфигурации с одной дверью доступны следующие параметры монитора блокировки:

- **Lock monitor (Монитор блокировки)** — выберите этот параметр, чтобы увидеть доступные элементы управления монитором блокировки. После этого выберите замок, который будет отслеживаться. Дверной монитор можно использовать только для дверей с двойной блокировкой и нельзя использовать, если к контроллеру подключено две двери.
  - **Open circuit = Locked (Разомкнутая цепь = заблокировано)** — выберите этот элемент, если нормальным состоянием является замкнутая цепь монитора блокировки. Когда цепь замкнута, монитор блокировки подает сигнал, означающий, что дверь разблокирована. Когда цепь разомкнута, монитор блокировки подает сигнал, означающий, что дверь заблокирована.
  - **Open circuit = UnLocked (Разомкнутая цепь = разблокировано)** — выберите этот элемент, если нормальным состоянием является разомкнутая цепь монитора блокировки. Когда цепь разомкнута, монитор блокировки подает сигнал, означающий, что дверь разблокирована. Когда цепь замкнута, монитор блокировки подает сигнал, означающий, что дверь заблокирована.

Как настроить считыватели и REX-устройства

После настройки дверных мониторов и замков в новой конфигурации оборудования можно приступить к настройке считывателей и REX-устройств (устройств, обрабатывающих запросы на выход).

1. Если будет использоваться считыватель, отметьте флажком соответствующее поле и выберите подходящие параметры для протокола связи считывателя.

2. Если будет использоваться REX-устройство (устройство, обрабатывающее запросы на выход), например, кнопка, датчик или толкающий рычаг, установите соответствующий флажок и выберите нужный параметр для соединения цепей REX-устройства.

   Если сигнал REX-устройства не влияет на открывание двери (например, для дверей с механическими рукоятками или толкающими рычагами), выберите **REX does not unlock door (REX-устройство не разблокирует дверь)**.

3. При подключении нескольких считывателей или REX-устройств к дверному контроллеру выполняйте предыдущие два шага для всех этих устройств, чтобы все считыватели или REX-устройства были настроены должным образом.

О параметрах считывателя и REX-устройства

Для считывателя доступны следующие параметры:

- **Wiegand** — выберите для считывателей, использующих протоколы Wiegand. Затем выберите управление светодиодами, поддерживаемое считывателем. Считыватели с управлением одним светодиодом, как правило, переключают цвет индикатора с красного на зеленый. Считыватели с управлением двумя светодиодами используют разные провода для красного и зеленого цветов. Это означает, что светодиоды управляются независимо друг от друга. Когда загораются оба светодиода, пользователь видит оранжевый цвет. Для получения сведений о типе управления светодиодами, поддерживаемом считывателем, см. инструкции производителя.
- **OSDP, RS485 half duplex (OSDP, полудуплекс RS485)** — выберите для считывателей RS485 с поддержкой полудуплекса. Для получения сведений о протоколе, поддерживаемом считывателем, см. инструкции производителя.

Для REX-устройства доступны следующие параметры:

- **Active low (Активный низкий уровень)** — выберите, если активация REX-устройства замыкает цепь.
- **Active high (Активный высокий уровень)** — выберите, если активация REX-устройства размыкает цепь.
- Если сигнал REX-устройства не влияет на открывание двери (например, для дверей с механическими рукоятками или толкающими рычагами), выберите **REX does not unlock door (REX-устройство не разблокирует дверь)**. Сигнал тревоги из-за принудительного открытия двери не будет активирован, если пользователь откроет дверь в отведенное время доступа. Снимите этот флажок, если дверь должна автоматически разблокироваться, когда пользователь активирует REX-устройство.

Примечание.

Большинство параметров замков, дверных мониторов и считывателей можно изменить без сброса и создания новой конфигурации оборудования. Перейдите в меню **Setup > Hardware Reconfiguration (Настройка > Повторная настройка оборудования)**.

Как использовать контролируемые входы

Контролируемые входы дают информацию о состоянии соединения между дверным контроллером и дверными мониторами. При нарушении соединения активируется событие.

Для использования контролируемых входов:

1. Установите резисторы на концах линии на все используемые контролируемые входы. Схему подключения см. на *стр. 43*.
2. Перейдите в меню **Setup > Hardware Reconfiguration (Настройка > Повторная настройка оборудования)** и выберите пункт **Enable supervised inputs (Активировать контролируемые входы)**. Кроме того, включить контролируемые входы можно при настройке оборудования.

О совместимости контролируемых входов

Для поддержки контролируемых входов служит следующая функция:

- Дверной монитор. См. *Разъем дверного датчика на стр. 44*.

Как создать новую конфигурацию оборудования для беспроводных замков

1. Перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)** и нажмите кнопку **Start new hardware configuration (Создать новую конфигурацию оборудования)**.
2. Введите имя устройства Axis.
3. В списке периферийных устройств выберите производителя беспроводного шлюза.
4. Если требуется подключить дверь с проводным интерфейсом, установите флажок **1 Door (1 дверь)** и нажмите кнопку **Next (Далее)**. Если дверь в конфигурацию не входит, нажмите кнопку **Finish (Готово)**.
5. В зависимости от производителя замка выполните соответствующие действия, которые указаны ниже.
   - **ASSA Aperio**: Нажмите ссылку для просмотра схемы контактов оборудования или нажмите кнопку **Close (Закрыть)** и перейдите в меню **Setup > Hardware Reconfiguration (Настройка > Повторная настройка оборудования)** для завершения настройки (см. раздел *Добавление дверей и устройств Assa Aperio™ на стр. 16*).
   - **SmartIntego**: Нажмите ссылку для просмотра схемы контактов оборудования или нажмите пункт **Click here to select wireless gateway and configure doors (Нажмите здесь, чтобы выбрать беспроводной шлюз и настроить двери)** для завершения настройки (см. раздел *Как настроить SmartIntego на стр. 22*).

Добавление дверей и устройств Assa Aperio™

Прежде чем добавить в систему дверь с беспроводным управлением, ее необходимо подключить с помощью концентратора Assa Aperio, используя Aperio PAP (прикладное средство программирования Aperio).

Добавление в систему двери с беспроводным управлением:

1. Перейдите в меню **Setup (Настройка)** > **Hardware Reconfiguration (Повторная настройка оборудования)**.
2. В меню Wireless Doors and Devices (Двери с беспроводным управлением и беспроводные устройства) нажмите кнопку **Add door (Добавить дверь)**.
3. В поле **Door name (Имя двери)** введите описательное имя.
4. В поле **ID (Идентификатор)** для пункта **Lock (Блокировать)** введите адрес устройства, которое вы хотите добавить, состоящий из 6 символов. Адрес устройства напечатан на его этикетке.
5. Можно также в разделе **Door position sensor (Датчик положения двери)** выбрать **Built in door position sensor (Встроенный датчик положения двери)** или **External door position sensor (Внешний датчик положения двери)**.

Примечание.

Если используется внешний датчик положения двери (DPS), перед настройкой убедитесь, что устройство блокировки Aperio поддерживает обнаружение состояния дверной ручки.

6. Можно также в поле **ID (Идентификатор)** раздела **Door position sensor (Датчик положения двери)** ввести адрес устройства, которое вы хотите добавить, состоящий из 6 символов. Адрес устройства напечатан на его этикетке.
7. Нажмите кнопку **Add (Добавить)**.

Как создать новую конфигурацию оборудования с функцией управления лифтами (AXIS A9188)

Важно!

Прежде чем создавать конфигурацию оборудования, необходимо добавить пользователя в сетевом релейном модуле ввода-вывода AXIS A9188 Network I/O Relay Module. Откройте веб-интерфейс модуля A9188 и выберите > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Настройки > Настройка дополнительного устройства > Базовая настройка > Пользователи > Добавить > Настройка пользователя)**.

Примечание.

Для каждого Axis Network Door Controller можно настроить не более двух модулей AXIS 9188 Network I/O Relay Module.

1. Откройте веб-страницу дверного контроллера, перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)** и нажмите кнопку **Start new hardware configuration (Создать новую конфигурацию оборудования)**.
2. Введите имя устройства Axis.
3. В списке периферийных устройств выберите **Elevator control (Управление лифтом)**, чтобы включить в конфигурацию релейный модуль AXIS A9188 Network I/O Relay Module, а затем нажмите кнопку **Next (Далее)**.
4. Введите имя подключенного считывателя.
5. Выберите протокол считывателя, который будет использоваться, и нажмите кнопку **Finish (Готово)**.
6. Нажмите **Network Peripherals (Сетевые периферийные устройства)** для завершения настройки (см. раздел *Как добавить и настроить сетевые периферийные устройства на стр. 17*) или нажмите ссылку, чтобы перейти к схеме контактов оборудования.

Как добавить и настроить сетевые периферийные устройства

Важно!

- Прежде чем приступить к настройке сетевых периферийных устройств, необходимо добавить пользователя в сетевой релейный модуль ввода-вывода AXIS A9188 Network I/O Relay Module. Откройте веб-интерфейс модуля AXIS A9188 и выберите > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Настройки > Настройка дополнительного устройства > Базовая настройка > Пользователи > Добавить > Настройка пользователя)**.
- Не добавляйте еще один сетевой дверной контроллер AXIS A1001 Network Door Controller в качестве сетевого периферийного устройства.

1. Чтобы добавить устройство, перейдите к пункту меню **Setup > Network Periphals (Настройка > Сетевые периферийные устройства)**.
2. Найдите нужные устройства в разделе **Discovered devices (Обнаруженные устройства)**.
3. Нажмите кнопку **Add this device (Добавить это устройство)**.
4. Введите имя устройства.
5. Введите имя пользователя и пароль для релейного модуля AXIS A9188.
6. Нажмите кнопку **Add (Добавить)**.

Примечание.

Сетевые периферийные устройства можно добавить вручную, введя MAC-адрес или IP-адрес в диалоговом окне **Manually add device (Добавить устройство вручную)**.

Важно!

Если вы хотите удалить расписание, сначала убедитесь, что оно не используется сетевым релейным модулем ввода-вывода.

Настройка портов ввода-вывода и реле в сетевых периферийных устройствах

Важно!

Прежде чем приступить к настройке сетевых периферийных устройств, необходимо добавить пользователя в сетевой релейный модуль ввода-вывода AXIS A9188 Network I/O Relay Module. Откройте веб-интерфейс модуля AXIS A9188 и выберите > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Настройки > Настройка дополнительного устройства > Базовая настройка > Пользователи > Добавить > Настройка пользователя)**.

1. Перейдите в меню **Setup > Network Periphals (Настройка > Сетевые периферийные устройства)** и нажмите строку **Added devices (Добавленные устройства)**.

2. Выберите порты ввода-вывода и реле, которые будут заданы для определенного этажа.
3. Нажмите **Set as floor (Установить для этажа)** и введите имя.
4. Нажмите **Add (Добавить)**.

Проверка подключения оборудования

После завершения установки и настройки оборудования, а также в любой момент на протяжении срока службы дверного контроллера можно проверить функционирование подключенных дверных мониторов, сетевых релейных модулей ввода-вывода, замков и считывателей.

Чтобы проверить настройку и получить доступ к управлению проверкой, перейдите в меню **Setup > Hardware Connection Verification (Настройка > Проверка подключения оборудования)**.

Проверка дверного оборудования

- **Door state (Состояние двери)** — проверка текущего состояния дверного монитора, дверных сигналов тревоги и замков. Нажмите кнопку **Get current state (Получить данные о текущем состоянии)**.
- **Lock (Замок)** — Ручной переключатель замков. Будут задействованы основные и вспомогательные замки, если таковые есть. Нажмите кнопку **Lock (Закрыть)** или **Unlock (Открыть)**.
- **Lock (Замок)** — Ручной переключатель замков для проверки доступа. Будут задействованы только основные замки. Нажмите кнопку **Access (Доступ)**.
- **Reader: Feedback (Считыватель: обратная связь)** — проверка обратной связи считывателя (например, звуковых сигналов и светодиодных индикаторов) для разных команд. Выберите команду и нажмите кнопку **Test (Тест)**. Доступные виды обратной связи зависят от считывателя. Дополнительные сведения см. в разделе *Обратная связь со считывателем на стр. 27*. См. также инструкции производителя.
- **Reader: Tampering (Считыватель: несанкционированные действия)** — получение сведений о последней попытке несанкционированного доступа. Первая попытка несанкционированного доступа будет зарегистрирована при установке считывателя. Нажмите кнопку **Get last tampering (Получить данные о последних несанкционированных действиях)**.
- **Reader: Card swipe (Считыватель: использование карты)** — получение сведений о последней использованной карте или другом виде пользовательских жетонов, принимаемых считывателем. Нажмите кнопку **Get last credential (Получить последние учетные данные)**.
- **REX** — получение сведений о последнем использовании устройства, обрабатывающего запросы на выход (REX-устройства). Нажмите кнопку **Get last REX (Получить данные о последнем использовании REX-устройства)**.

Проверка этажного оборудования

- **Floor state (Состояние этажа)** — проверьте текущее состояние доступа на этаж. Нажмите кнопку **Get current state (Получить данные о текущем состоянии)**.
- **Floor lock & unlock (Блокировка и разблокировка доступа на этаж)** — ручной переключатель доступа на этаж. Будут задействованы основные и вспомогательные замки, если таковые есть. Нажмите кнопку **Lock (Закрыть)** или **Unlock (Открыть)**.
- **Floor access (Доступ на этаж)** — предоставление временного доступа на этаж в ручном режиме. Будут задействованы только основные замки. Нажмите кнопку **Access (Доступ)**.
- **Elevator Reader: Feedback (Считыватель лифта: обратная связь)** — проверка реакции считывателя (например, звуковых сигналов и светодиодных индикаторов) для разных команд. Выберите команду и нажмите кнопку **Test (Тест)**. Доступные виды обратной связи зависят от считывателя. Дополнительные сведения см. в разделе *Обратная связь со считывателем на стр. 27*. См. также инструкции производителя.
- **Elevator Reader: Tampering (Считыватель лифта: несанкционированные действия)** — получение сведений о последней попытке несанкционированного доступа. Первая попытка несанкционированного доступа будет

зарегистрирована при установке считывателя. Нажмите кнопку **Get last tampering (Получить данные о последних несанкционированных действиях)**.

- **Elevator Reader: Card swipe (Считыватель лифта: предъявленная карточка)** — получение сведений о последней предъявленной карточке или другом виде пользовательских устройств, пригодных для считывателя. Нажмите кнопку **Get last credential (Получить последние учетные данные)**.
- **REX** — получение сведений о последнем использовании устройства, обрабатывающего запросы на выход (REX-устройства). Нажмите кнопку **Get last REX (Получить данные о последнем использовании REX-устройства)**.

Настройка карт и форматов

Для дверного контроллера есть несколько готовых форматов карт, которые чаще всего применяются. Их можно непосредственно использовать или изменить так, как нужно. Можно также создать пользовательские форматы карт. Для каждого формата карты используется свой набор правил и расположение полей, определяющих то, каким образом организована информация, хранимая на карте. Задавая формат карты, вы сообщаете системе, как интерпретировать информацию, получаемую контроллером от считывателя. Для получения сведений о поддерживаемых считывателем форматах карт см. инструкции производителя.

Активация форматов карт:

1. Выберите в меню **Setup > Configure cards and formats (Настройка > Настройка карт и форматов)**.
2. Выберите один или несколько форматов карт, соответствующих тем форматам, которые используют подключенные считыватели.

Создание новых форматов карт:

1. Выберите в меню **Setup > Configure cards and formats (Настройка > Настройка карт и форматов)**.
2. Щелкните **Add card format (Добавить формат карты)**.
3. В диалоговом окне **Add card format (Добавить формат карты)** введите имя, описание и длину формата карты в битах. См. *Описание форматов карт на стр. 20*.
4. Щелкните **Add field map (Добавить расположение полей)** и введите в поля необходимые данные. См. *Схемы расположения полей на стр. 20*.
5. Чтобы добавить несколько схем расположения полей, повторите предыдущий шаг.

Чтобы развернуть элемент списка **Card Formats (Форматы карт)** и увидеть описания форматов карт и расположение полей, нажмите значок .

Чтобы изменить формат карты, щелкните и измените описания форматов карт и расположение полей соответствующим образом. Затем нажмите кнопку **Save (Сохранить)**.

Чтобы удалить схему расположения полей в диалоговом окне **Edit card format (Изменить формат карты)** или **Add card format (Добавить формат карты)**, нажмите значок .

Для удаления формата карты щелкните .

Важно!

- Вы можете активировать и деактивировать форматы карт только в том случае, если для данного дверного контроллера был настроен хотя бы один считыватель. См. *Настройка оборудования на стр. 11* и *Как настроить считыватели и REX-устройства на стр. 14*.
- Нельзя одновременно активировать два формата карт с одинаковой длиной в битах. Например, если вы определили два 32-битных формата карт — "Формат А" и "Формат Б" — и активировали "Формат А", то вы не можете активировать "Формат Б" без предварительной деактивации "Формата А".
- Если ни один формат карт не активирован, то для идентификации карты и предоставления доступа пользователям можно использовать типы идентификации **Card raw only (Только несформированные данные карты)** и **Card raw and PIN (Несформированные данные карты и PIN)**. Однако это не рекомендуется делать, поскольку разные производители считывателей или настройки считывателей могут создавать разные несформированные данные карты.

Описание форматов карт

- **Name (Имя)** (обязательное поле) — введите описательное имя.
- **Description (Описание)** — при желании введите дополнительную информацию. Эта информация будет видна только в окнах **Edit card format (Изменить формат карты)** и **Add card format (Добавить формат карты)**.
- **Bit length (Длина в битах)** (обязательное поле) — укажите длину формата карты в битах. Это должно быть число от 1 до 1000000000.

Схемы расположения полей

- **Name (Имя)** (обязательное поле) — введите без пробелов название схемы расположения полей, например, `OddParity`.

  Примеры распространенных схем расположения полей:

  - `Parity (Контроль четности)` — для обнаружения ошибок используются паритетные биты (биты четности). Биты четности обычно добавляют в начало или в конец строки в двоичном коде, и они указывают четность или нечётность количества единичных битов.
  - `EvenParity` — четные паритетные биты обеспечивают четное количество битов в строке. Считаются те биты, которые имеют значение 1. Если количество уже четное, то значение паритетного бита задается равным 0. Если количество нечетное, то значение паритетного бита четности задается равным 1, что делает общее количество четным числом.
  - `OddParity` — нечетные паритетные биты обеспечивают нечетное количество битов в строке. Считаются те биты, которые имеют значение 1. Если количество уже нечетное, то значение нечетного паритетного бита задается равным 0. Если количество четное, то значение паритетного бита задается равным 1, что делает общее количество нечетным числом.
  - `FacilityCode (Код объекта)` — коды объектов иногда используются для проверки того, что данные на жетоне (или другом устройстве для считывания) соответствуют заказанному пакету учетных данных конечного пользователя. В существовавших ранее системах контроля доступа код объекта использовался для нестрогого контроля, поскольку войти мог каждый сотрудник, который был указан в пакете учетных данных и имел зашифрованный код объекта. Данное имя схемы расположения полей, которое вводится с учетом регистра, необходимо для устройства, чтобы оно могло проверить код объекта.
  - `CardNr (Номер карты)` — номер карты или идентификатор пользователя представляет собой данные, которые наиболее часто проверяются в системах контроля доступа. Данное имя схемы расположения полей, которое вводится с учетом регистра, необходимо для устройства, чтобы оно могло номер карты.
  - `CardNrHex (Шестнадцатеричный номер карты)` — двоичные данные номера карты кодируются шестнадцатеричными числами в устройстве. В основном используется для устранения неполадок, если считыватель не выдает ожидаемый номер карты.

- **Range (Диапазон)** (обязательное поле) — введите диапазон битов схемы расположения полей, например 1, 2–17, 18–33, и 34.
- **Encoding (Кодирование)** (обязательное поле) — выберите тип кодирования каждого поля схемы расположения полей.
  - **BinLE2Int** — двоичные данные кодируются целыми числами с использованием прямого порядка битов (little endian). "Целое" означает, что это должно быть недробное число (без десятичных знаков). Прямой порядок битов (little endian) означает, что первый бит является наименьшим (наименее значимый).
  - **BinBE2Int** — двоичные данные кодируются целыми числами с использованием обратного порядка битов (big endian). "Целое" означает, что это должно быть недробное число (без десятичных знаков). Обратный порядок битов (big endian) означает, что первый бит является наибольшим (наиболее значимый).
  - **BinLE2Hex** — двоичные данные кодируются шестнадцатеричными числами с использованием прямого порядка битов (little endian). Шестнадцатеричная система, которую также называют системой счисления по основанию 16, состоит из 16 уникальных символов: числа от 0 до 9 и буквы от a до f. Прямой порядок битов (little endian) означает, что первый бит является наименьшим (наименее значимый).
  - **BinBE2Hex** — двоичные данные кодируются шестнадцатеричными числами с использованием обратного порядка байтов (big endian). Шестнадцатеричная система, которую также называют системой счисления по основанию 16, состоит из 16 уникальных символов: числа от 0 до 9 и буквы от a до f. Обратный порядок битов (big endian) означает, что первый бит является наибольшим (наиболее значимый).
  - **BinLEIBO2Int** — двоичные данные кодируются так же, как и для BinLE2Int, но здесь несформированные данные карты считываются в обратном порядке следования байтов в виде последовательности из нескольких байтов, а потом уже кодируются схемы расположения полей.
  - **BinBEIBO2Int** — двоичные данные кодируются так же, как и для BinBE2Int, но здесь несформированные данные карты считываются в обратном порядке следования байтов в виде последовательности из нескольких байтов, а потом уже кодируются схемы расположения полей.

Для получения информации о схеме расположения полей в вашей карте см. инструкции производителя.

Настройка служб

Выберите на странице Setup (Настройка) раздел Configure Services (Настройка служб), где можно настроить внешние службы для использования при работе дверного контроллера.

SmartIntego

SmartIntego — это беспроводное решение, позволяющее увеличить количество дверей, которые может обрабатывать дверной контроллер.

Предварительные требования для SmartIntego

Прежде чем приступать к настройке SmartIntego, необходимо выполнить перечисленные ниже предварительные требования.

- Необходимо создать csv-файл. Этот файл csv должен содержать информацию о том, какой шлюзовой узел и какие двери используются в вашем решении SmartIntego. Данный файл создается с помощью автономного программного обеспечения, предоставляемого партнером компании SimonsVoss.
- Произведена настройка оборудования для SmartIntego, см. раздел *Как создать новую конфигурацию оборудования для беспроводных замков на стр. 16*.

Примечание.

- Следует использовать средство настройки SmartIntego Configuration версии 2.1.6452.23485, сборка 2.1.6452.23485 (31.08.2017 13:02:50) или более поздней версии.
- Стандарт AES (Advanced Encryption Standard) не поддерживается для SmartIntego, поэтому его нужно отключить в средстве настройки SmartIntego Configuration.

Как настроить SmartIntego

Примечание.

- Убедитесь в том, что выполнены все перечисленные предварительные требования.
- Чтобы не пропустить момент ухудшения состояния батареи, перейдите в меню **Setup (Настройка)** > **Configure event and alarms logs (Настройка журналов событий и тревог)** и добавьте в качестве сигнала тревоги либо **Door — Battery alarm (Дверь — Сигнал тревоги батареи)**, либо **IdPoint — Battery alarm (IdPoint — Сигнал тревоги батареи)**.
- Настройки дверного монитора берутся из импортированного CSV-файла. В случае обычной установки не следует менять эти настройки.

1. Нажмите **Browse... (Обзор)**, выберите csv-файл и нажмите кнопку **Upload File (Загрузить файл)**.
2. Выберите GatewayNode (Шлюзовой узел) и нажмите кнопку **Next (Далее)**.
3. Будет показан предварительный вид новой конфигурации. При необходимости деактивируйте дверные мониторы.
4. Нажмите кнопку **Configure (Настроить)**.
5. Будет показана общая схема подключения дверей, входящих в конфигурацию. Нажмите **Settings (Настройки)**, чтобы настроить каждую дверь по отдельности.

Повторная настройка SmartIntego

1. Выберите **Setup (Настройка)** в верхнем меню.
2. Затем выберите **Configure Services (Настройка служб)** > **Settings (Параметры)**.
3. Нажмите кнопку **Re-configure (Настроить повторно)**.
4. Нажмите **Browse... (Обзор)**, выберите csv-файл и нажмите кнопку **Upload File (Загрузить файл)**.
5. Выберите GatewayNode (Шлюзовой узел) и нажмите кнопку **Next (Далее)**.
6. Будет показан предварительный вид новой конфигурации. При необходимости деактивируйте дверные мониторы.

Примечание.

Настройки дверного монитора берутся из импортированного CSV-файла. В случае обычной установки не следует менять эти настройки.

7. Нажмите кнопку **Configure (Настроить)**.
8. Будет показана общая схема подключения дверей, входящих в конфигурацию. Нажмите **Settings (Настройки)**, чтобы настроить каждую дверь по отдельности.

Инструкции по обслуживанию

Для поддержания бесперебойной работы системы контроля доступа компания Axis рекомендует проводить регулярное профилактическое обслуживание этой системы, включая дверные контроллеры и подключенные устройства.

Обслуживание должно выполняться хотя бы один раз в год. Предлагаемая процедура обслуживания включает в себя следующие проверки (не ограничиваясь этим):

- Убедитесь в надежности всех соединений между дверным контроллером и внешними устройствами.
- Проверьте все подключения оборудования. См. *Проверка дверного оборудования на стр. 18*.
- Проверьте правильность функционирования системы, включая подсоединенные к ней внешние устройства.
  - Воспользуйтесь карточкой доступа и проверьте работу считывателей, дверей и замков.
  - Если система содержит REX-устройства, датчики или другие устройства, проверьте их тоже.

- Проверьте сигналы тревоги при несанкционированных действиях, если они активированы.

Если результаты, полученные на любом из перечисленных выше этапов, указывают наличие неисправности или говорят о неправильной работе оборудования, предпримите указанные ниже действия:

- Протестируйте провода с помощью соответствующего оборудования, а также проверьте провода и кабели на наличие каких-либо повреждений.
- Замените все поврежденные или неисправные кабели и провода.
- После замены кабелей и проводов вновь проверьте все подключения оборудования. См. *Проверка дверного оборудования на стр. 18*.

- Если дверной контроллер ведет себя неожиданным образом, см. разделы *Устранение неполадок на стр. 38* и *Обслуживание на стр. 35* для получения дополнительной информации.

Настройка событий

Происходящие в системе события — например, когда пользователь подносит карту к считывателю или активируется REX-устройство — заносятся в журнал событий.

- Просмотр журнала событий. См. *стр. 24*.
- Экспорт журнала событий. См. .
- Настройка журнала событий. См. *Настройка журнала событий на стр. 24*.

Просмотр журнала событий

Для просмотра занесенных в журнал событий выберите **Event Log (Журнал событий)**.

Чтобы развернуть запись в журнале событий и просмотреть подробные сведения об этом событии, щелкните .

Применение фильтров к журналу событий позволяет легче найти конкретные события. Чтобы отфильтровать список, выберите один или несколько фильтров журнала событий и нажмите кнопку **Apply filters (Применить фильтры)**. Дополнительные сведения см. в разделе *Фильтры журнала событий на стр. 24*.

Для администратора некоторые события могут представлять больший интерес, чем прочие. Поэтому можно выбрать, какие события должны заноситься в журнал событий. Дополнительные сведения см. в разделе *Параметры журнала событий на стр. 24*.

Фильтры журнала событий

Можно уменьшить количество заносимых в журнал событий за счет применения одного или нескольких из представленных ниже фильтров:

- User (Пользователь) — фильтр для событий, связанных с выбранным пользователем.
- Door & floor (Дверь и этаж) — фильтр для событий, связанных с конкретной дверью или этажом.
- Topic (Тема) — фильтр для типа событий.
- Date and time (Дата и время) — фильтрация событий в журнале для заданного диапазона дат и времени.

Настройка журнала событий

На странице настройки журнала событий можно задать события, которые должны заноситься в журнал.

Параметры журнала событий

Чтобы задать события, которые должны регистрироваться в журнале событий, перейдите в меню **Setup > Configure Event Logs (Настройка > Настройка журнала событий)**.

Предусмотрены следующие варианты занесения событий в журнал:

- **No logging (Без занесения в журнал)** — занесение события в журнал отключено. Данное событие не будет зарегистрировано или занесено в журнал событий.
- **Log for all sources (Заносить в журнал для всех источников)** активировано занесение событий в журнал. Данное событие будет зарегистрировано и занесено в журнал событий.

Как настроить правила действия

Страницы Event (Событие) позволяют настроить устройство Axis так, чтобы при возникновении разных событий выполнялись те или иные действия. Набор условий, определяющих как и когда запускается то или иное действие, называется правилом действия. Если задано несколько условий, то для запуска соответствующего действия необходимо соблюдение всех условий.

Дополнительные сведения о доступных триггерах и действиях см. во встроенной справке устройства.

В следующем примере описано, как настроить правило действия, состоящее в активации выходного порта, если дверь открыта с приложением силы.

1. Выберите в меню последовательно **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Настройка > Дополнительная настройка контроллера > Параметры системы > Порты и устройства > Порты ввода-вывода)**.
2. Выберите **Output (Выход)** для нужного элемента **I/O Port Type (Тип порта ввода-вывода)**, представленного в раскрывающемся списке, и введите **Name (Имя)**.
3. Выберите для порта ввода-вывода (I/O port) **Normal state (Нормальное состояние)** и нажмите кнопку **Save (Сохранить)**.
4. Перейдите в меню **Events > Action Rules (События > Правила действия)** и нажмите кнопку **Add (Добавить)**.
5. Выберите **Door (Дверь)** из раскрывающегося списка **Trigger (Инициирующее событие)**.
6. Выберите **Door Alarm (Сигнал при несанкционированном открывании двери)** из раскрывающегося списка.
7. Выберите нужную дверь из раскрывающегося списка.
8. Выберите **DoorForcedOpen (Открывание двери силой)** из раскрывающегося списка.
9. В качестве альтернативного варианта можно выбрать **Schedule (Расписание)** и **Additional conditions (Дополнительные условия)**. См. раздел ниже.
10. В меню **Actions (Действия)**, выберите **Output Port (Выходной порт)** из раскрывающегося списка **Type (Тип)**.
11. Выберите нужный выходной порт из раскрывающегося списка **Port (порт)**.
12. Задайте состояние **Active (Активный)**.
13. Выберите **Duration (Длительность)** и **Go to opposite state after (Затем перейти в исходное состояние)**. Введите желаемую длительность действия.
14. Нажмите кнопку **OK**.

Чтобы использовать более одного инициирующего события для правила действия, выберите **Additional conditions (Дополнительные условия)** и нажмите кнопку **Add (Добавить)** для добавления дополнительных инициирующих событий. Если используется несколько условий, то для запуска соответствующего действия необходимо соблюдение всех условий.

Чтобы предотвратить повторный запуск какого-либо действия, можно задать время ожидания **Wait at least (Подождать не менее)**. Введите интервал времени в часах, минутах и секундах, в течение которого инициирующее событие должно игнорироваться, и лишь по прошествии указанного времени правило действия может быть вновь активировано.

Для получения более подробной информации см. встроенную в устройство справку.

Как добавить получателей

Устройство может отправлять сообщения, уведомляющие получателей о событиях и сигналах тревоги. Однако, чтобы устройство смогло отправлять уведомления, необходимо указать одного или нескольких получателей. Сведения о доступных вариантах см. в разделе .

Чтобы добавить получателя:

1. Перейдите в меню **Setup > Additional Controller Configuration > Events > Recipients (Настройка > Дополнительная настройка контроллера > События > Получатели)** и нажмите кнопку **Add (Добавить)**.

2. Введите описательное имя.
3. Выберите тип получателя в разделе **Type (Тип)**.
4. Введите информацию, необходимую для типа получателя.
5. Нажмите кнопку **Test (Тест)**, чтобы проверить связь с получателем.
6. Нажмите кнопку **OK**.

Как настроить получателей электронной почты

Чтобы настроить получателей электронной почты, надо выбрать одного поставщика услуг электронной почты из указанных в списке, либо указать SMTP-сервер, порт и способ проверки подлинности, который применяется, например, на корпоративном почтовом сервере.

Примечание.

Некоторые поставщики услуг электронной почты ставят фильтры безопасности, которые не позволяют пользователям получать или просматривать вложения большого объема, а также не позволяют получать письма по расписанию и тому подобное. Поинтересуйтесь политикой безопасности выбранного поставщика услуг электронной почты, чтобы избежать проблем с доставкой писем и с заблокированными учетными записями электронной почты.

Настройка получателя электронной почты с помощью одного из поставщиков услуг, представленных в списке:

1. Перейдите в меню **Events > Recipients (События > Получатели)** и нажмите кнопку **Add (Добавить)**.
2. Введите **Name (Имя)** и выберите **Email** из списка **Type (Тип)**.
3. Введите адреса электронной почты, по которым следует отправлять письма, в поле **To (Кому)**. При вводе нескольких адресов разделяйте их запятыми.
4. Выберите поставщика услуг электронной почты из списка **Provider (Поставщик услуг)**.
5. Введите идентификатор пользователя и пароль для учетной записи электронной почты.
6. Нажмите кнопку **Test (Проверка)**, для отправки проверочного письма.

Чтобы настроить получателя электронной почты, используя, например, корпоративный почтовый сервер, следуйте приведенным выше инструкциям, но выберите **User defined (Задаваемый пользователем)** в качестве **Provider (Поставщик услуг)**. Введите адрес электронной почты, который должен отобразиться в качестве адреса отправителя, в поле **From (От кого)**. Выберите **Advanced settings (Расширенные настройки)** и укажите адрес SMTP-сервера, порт и способ проверки подлинности. При желании можно выбрать **Use encryption (Использовать шифрование)** для отправки писем электронной почты по зашифрованному соединению. Сертификат сервера можно проверить с помощью сертификатов, которые имеются в устройстве Axis. Сведения о том, как загрузить сертификаты, см. в разделе *Сертификаты на стр. 29*.

Создание расписаний

Расписания могут использоваться в качестве запускающего фактора правил действия или в качестве дополнительных условий. Используйте одно из предустановленных расписаний или создайте новое расписание в соответствии с инструкциями ниже.

Для создания нового расписания:

1. Перейдите в меню **Setup > Additional Controller Configuration > Events > Schedules (Настройка > Дополнительная настройка контроллера > События > Расписания)** и нажмите кнопку **Add (Добавить)**.
2. Введите описательное имя и сведения, необходимые для ежедневного, еженедельного, ежемесячного или ежегодного расписания.
3. Нажмите кнопку **OK**.

Чтобы использовать расписание в правиле действия, сначала выберите расписание в раскрывающемся списке **Schedule (Расписание)** на странице Action Rule Setup (Настройка правила действия).

Как настроить периодичность

Периодичность используется для повторного запуска правил действия, например, каждые 5 минут или каждый час.

Чтобы настроить периодичность:

1. Перейдите в меню **Setup > Additonal Controller Configuration > Events > Recurrences (Настройка > Дополнительная настройка контроллера > События > Периодичность)** и нажмите кнопку **Add (Добавить)**.
2. Введите описательное имя и укажите периодичность.
3. Нажмите кнопку **OK**.

Чтобы использовать периодичность в правиле действия, сначала выберите значение **Time (Время)** в раскрывающемся списке **Trigger (Триггер)** на странице Action Rule Setup (Настройка правила действия), а затем выберите периодичность во втором раскрывающемся списке.

Чтобы изменить или удалить периодичность, выберите нужное значение в **Recurrences List (Список периодичности)** и нажмите кнопку **Modify (Изменить)** или **Remove (Удалить)**.

Обратная связь со считывателем

Считыватели передают информационные сообщения пользователю (человеку, который получил или пытается получить доступ к двери) с помощью индикаторов и звуковых сигналов. Дверной контроллер может вызвать разные информационные сообщения, некоторые из которых уже настроены в дверном контроллере и поддерживаются большинством считывателей.

Считыватели могут использовать индикаторы разными способами, но, как правило, это разные последовательности горящих и мигающих световых сигналов красного, зеленого и оранжевого цветов.

Некоторые считыватели также используют для передачи сообщений однотонные звуковые сигналы: разную последовательность коротких и длинных сигналов.

В таблице ниже приведены события, которые, в соответствии с уже заданными настройками дверного контроллера, вызывают сообщения считывателей, а также соответствующие им типичные сигналы считывателей. Информационные сигналы считывателей AXIS описаны в руководстве по установке, которое поставляется вместе со считывателем AXIS.

Событие	Двойной светодиод Wiegand	Одиночный светодиод Wiegand	OSDP	Последователь-ность звуковых сигналов	Состояние
Idle (Простой)[1]	Off (Выкл.)	Красный	Красный	Тишина	Нормальное
Требуется PIN-код	Мигает красным / зеленым	Мигает красным / зеленым	Мигает красным / зеленым	Два коротких звуковых сигнала	Требуется PIN-код
Доступ получен	Зеленый	Зеленый	Зеленый	Звуковой сигнал	Доступ получен
В доступе отказано	Красный	Красный	Красный	Звуковой сигнал	В доступе отказано

1. Состояние простоя вводится в том случае, если дверь закрыта и замок заблокирован.

Другие информационные сообщения необходимо настроить в клиенте, таком как система управления доступом, посредством прикладного программного интерфейса VAPIX®, который поддерживает эту функцию, при использовании считывателей, способных обеспечить необходимые сигналы. Дополнительные сведения см. в руководстве разработчика системы управления доступом и производителя считывателя.

Параметры системы

Безопасность

Пользователи

Контроль доступа пользователей включен по умолчанию. Настроить его можно в меню **Setup > Additional Controller Configuration > System Options > Security > Users (Настройка > Дополнительная настройка контроллера > Параметры системы > Безопасность > Пользователи)**. Администратор может задать настройки для других пользователей, назначив для них имена и пароли.

В списке пользователей отображаются авторизованные пользователи и группы пользователей (уровни доступа):

- **Администраторы** имеют неограниченный доступ ко всем настройкам. Администратор может добавлять, изменять и удалять других пользователей.

Примечание.

Отметим, что при выборе параметра **Encrypted & unencrypted (Зашифровано и незашифровано)** веб-сервер будет зашифровывать пароль. Это значение задано по умолчанию для нового устройства или устройства после сброса параметров к заводским установкам.

Разрешенный тип пароля следует выбрать в разделе **HTTP/RTSP Password Settings (Настройки пароля HTTP/RTSP)**. Возможно, вам потребуется разрешить пароли без шифрования, если используются клиенты просмотра, которые не поддерживают шифрование, или вы обновили встроенное ПО, и существующие клиенты поддерживают шифрование, но для того, чтобы использовать эту функцию, они должны заново войти в систему, и их необходимо заново настроить.

ONVIF

ONVIF — это открытый отраслевой форум, который основан с целью разработки и продвижения стандартных интерфейсов для эффективного взаимодействия IP-устройств, обеспечивающих физическую безопасность.

Создавая пользователя, вы автоматически включаете ONVIF-связь. Используйте это имя пользователя и пароль для любой ONVIF-связи с устройством. Дополнительные сведения смотрите на сайте *www.onvif.org*

Фильтр IP-адресов

Выберите в меню **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Фильтр IP-адресов)**, чтобы перейти на страницу настройки фильтра IP-адресов. После активации списка указанные в нем IP-адреса смогут получить доступ к устройству Axis или, наоборот, им будет отказано в доступе к этому устройству. Выберите в списке **Allow (Разрешить)** или **Deny (Отказать)**, затем нажмите кнопку **Apply (Применить)**, чтобы включить фильтрацию IP-адресов.

Администратор может добавить в список до 256 записей с IP-адресами (каждая запись может содержать несколько IP-адресов).

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer или HTTP over SSL) — это веб-протокол, используемый для просмотра зашифрованных веб-страниц. HTTPS также могут применять пользователи и клиенты для проверки того, что доступ осуществлен к нужному устройству. Уровень безопасности, обеспечиваемый протоколом HTTPS, считается достаточным для большинства случаев обмена коммерческой информацией.

Устройство Axis можно настроить для обязательного применения HTTPS при входе в систему администраторов.

Для использования HTTPS необходимо сначала установить сертификат HTTPS. Для установки и управления сертификатами перейдите в меню **Setup > Additional Controller Configuration > System Options > Security > Certificates (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Сертификаты)**. См. *Сертификаты на стр. 29*.

Включение HTTPS для устройства Axis:

1. Выберите в меню последовательно **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Настройка > Дополнительная настройка контроллера > Параметры системы > Безопасность > HTTPS)**.
2. Выберите из списка установленных сертификатов сертификат HTTPS.
3. Можно также нажать кнопку **Ciphers (Шифрование)** и выбрать, какие алгоритмы шифрования будут применяться для SSL.
4. Задайте **HTTPS Connection Policy (Политика подключения по HTTPS)** для других групп пользователей.
5. Чтобы настройки вступили в силу, нажмите кнопку **Save (Сохранить)**.

Для получения доступа к устройству Axis с использованием нужного протокола введите в адресное поле браузера `https://` для протокола HTTPS или `http://` в случае протокола HTTP.

Порт HTTPS можно изменить на странице **System Options > Network > TCP/IP > Advanced (Параметры системы > Сеть > TCP/IP > Дополнительно)**.

IEEE 802.1X

IEEE 802.1X — стандарт для технологии контроля доступа в сеть с использованием портов, обеспечивающий проверку подлинности проводных и беспроводных сетевых устройств. Стандарт IEEE 802.1X основан на протоколе EAP (Extensible Authentication Protocol).

Для получения доступа к сети, защищенной по стандарту IEEE 802.1X, устройства должны пройти проверку подлинности. Проверка подлинности выполняется сервером проверки подлинности. Как правило, это **RADIUS-сервер**, примерами которого являются FreeRADIUS и Служба Microsoft проверки подлинности в Интернете.

В реализации Axis устройство Axis и сервер проверки подлинности идентифицируют себя с помощью цифровых сертификатов, используя протокол EAP-TLS (Extensible Authentication Protocol — Transport Layer Security). Сертификаты предоставляются **центром сертификации** (ЦС). Вам требуется:

- сертификат ЦС для проверки удостоверения сервера проверки подлинности;
- сертификат клиента, подписанный ЦС, для проверки подлинности сетевого устройства.

Для создания и установки сертификатов перейдите в меню **Setup > Additional Controller Configuration > System Options > Security > Certificates (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Сертификаты)**. См. *Сертификаты на стр. 29*.

Предоставление устройству доступа к сети, защищенной по стандарту IEEE 802.1X:

1. Выберите в меню последовательно **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (Настройка > Дополнительная настройка контроллера > Параметры системы > Безопасность > IEEE 802.1X)**.
2. Выберите из списка установленных сертификатов **CA Certificate (ЦС-сертификат)** и **Client Certificate (Сертификат клиента)**.
3. В меню **Settings (Настройки)** выберите версию EAPOL и укажите свое EAP-удостоверение, связанное с сертификатом клиента.
4. Установите флажок, чтобы включить IEEE 802.1X, и нажмите кнопку **Save (Сохранить)**.

Примечание.

Проверка подлинности пройдет должным образом только в том случае, если параметры даты и времени устройства Axis синхронизируются с NTP-сервером. См. .

Сертификаты

Сертификаты служат для проверки подлинности устройств в сети. Как правило, для этого применяется шифрование веб-страниц (HTTPS), сетевая защита согласно стандарту IEEE 802.1X и отправка уведомляющих сообщений, например, по электронной почте. Для устройств Axis можно использовать два типа сертификатов:

Сертификаты сервер/клиент – служат для проверки подлинности устройства Axis. Сертификат **Server/Client (Сервер/Клиент)** может быть самозаверяющим или может быть выдан Центром сертификации (ЦС). Самозаверяющий сертификат дает ограниченную защиту, и его можно использовать до получения сертификата, выданного Центром сертификации.

Сертификаты ЦС – служат для проверки подлинности сертификатов соседей в сетке узлов (peer certificates), например, сертификата сервера проверки подлинности, если устройство Axis подключено к сети с защитой по стандарту IEEE 802.1X. Устройство Axis поставляется с несколькими предустановленными ЦС-сертификатами.

Примечание.

- При сбросе параметров устройства к заводским настройкам по умолчанию все установленные сертификаты будут удалены, за исключением предустановленных сертификатов ЦС.
- При сбросе параметров устройства к заводским настройкам по умолчанию все предустановленные сертификаты ЦС, которые были удалены, будут установлены вновь.

Как создать самозаверяющий сертификат

1. Для установки и управления сертификатами перейдите в меню **Setup > Additional Controller Configuration > System Options > Security > Certificates (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Сертификаты)**.
2. Нажмите кнопку **Create self-signed certificate (Создать самозаверяющий сертификат)** и укажите необходимые данные.

Создание и установка ЦС-сертификата

1. Сведения о создании самозаверяющего сертификата см. в разделе .
2. Перейдите к пункту **Setup > Additional Controller Configuration > System Options > Security > Certificates (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Сертификаты)**.
3. Нажмите кнопку **Create certificate signing request (Создать запрос на подписание сертификата)** и укажите необходимые данные.
4. Скопируйте этот запрос в формате PEM и отправьте его в выбранный ЦС.
5. После возвращения подписанного сертификата нажмите кнопку **Install certificate (Установить сертификат)** и загрузите сертификат.

Как установить дополнительные ЦС-сертификаты

1. Для установки и управления сертификатами перейдите в меню **Setup > Additional Controller Configuration > System Options > Security > Certificates (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > Сертификаты)**.
2. Нажмите кнопку **Install certificate (Установить сертификат)** и загрузите сертификат.

Сеть

Основные настройки TCP/IP

Устройство Axis поддерживает протокол IP версии 4 (IPv4) и IP версии 6 (IPv6).

Устройство Axis может получить IP-адрес следующими способами:

- **Динамический IP-адрес** — по умолчанию выбран вариант **Obtain IP address via DHCP (Получить IP-адрес с помощью DHCP)**. Это означает, что предусмотрено автоматическое получение IP-адреса устройством Axis с помощью протокола DHCP.

Протокол DHCP позволяет администраторам сетей автоматизировать назначение IP-адресов сетевым устройствам, а также централизованно управлять этим процессом.

- **Статический IP-адрес** — для использования статического IP-адреса выберите элемент **Use the following IP address (Использовать следующий IP-адрес)** и укажите IP-адрес, маску подсети и маршрутизатор по умолчанию. Затем нажмите кнопку **Save (Сохранить)**.

Протокол DHCP следует включать только при использовании уведомления о назначении динамического IP-адреса или если с помощью DHCP можно обновить данные DNS-сервера, который обеспечивает доступ к устройству Axis по имени (имя хоста).

Если DHCP включен, но доступа к устройству нет, запустите AXIS IP Utility для поиска в сети подключенных устройств Axis или сбросьте настройки устройства к заводским настройкам, а затем выполните установку заново. Сведения о том, как выполнить сброс к заводским настройкам, см. в разделе *стр. 38*.

Система размещения видео AXIS (AVHS)

Система AVHS, используемая вместе с сервисом AVHS, обеспечивает простой и безопасный доступ через Интернет к управлению контроллерами, а также к журналам, где бы вы ни находились. Для получения дополнительных сведений и справки о местоположении локального поставщика услуг AVHS перейдите на страницу www.axis.com/hosting.

Чтобы настроить параметры AVHS, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Основные)**. Возможность подключения к службе AVHS включена по умолчанию. Для отключения снимите флажок в поле **Enable AVHS (Включить AVHS)**.

Включение одним щелчком мыши – Нажмите и удерживайте в нажатом положении кнопку управления устройством (см. раздел *Общий вид устройства на стр. 5*) в течение примерно 3 секунд, чтобы подключиться к сервису AVHS через Интернет. После регистрации будет активирован экранный элемент **Always (Всегда)**, что означает постоянное подключение к сервису AVHS устройства Axis. Если в течение 24 часов после нажатия кнопки устройство не будет зарегистрировано, то оно будет отключено от сервиса AVHS/

Always (Всегда) – Устройство Axis будет постоянно пытаться подключиться к службе AVHS через Интернет. После регистрации устройство будет постоянно подключено к этой службе. Этот вариант можно использовать, когда устройство уже установлено, и нет возможности или неудобно использовать установку одним щелчком.

Примечание.

Поддержка AVHS зависит от пакетов услуг, подписки на которые предлагает ваш поставщик.

Сервис AXIS Internet Dynamic DNS

Сервис AXIS Internet Dynamic DNS служит для назначения имени хоста, чтобы упростить доступ к устройству. Дополнительные сведения см. на сайте *www.axiscam.net*.

Чтобы зарегистрировать устройство Axis с помощью службы AXIS Internet Dynamic DNS Service, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Основные)**. Выбрав **Services (Службы)**, нажмите кнопку **Настройки** для AXIS Internet Dynamic DNS Service (требуется доступ к Интернету). Текущее имя домена, зарегистрированное для данного устройства в сервисе AXIS Internet Dynamic DNS, можно удалить в любой момент.

Примечание.

Для работы сервиса AXIS Internet Dynamic DNS требуется IPv4.

Расширенные настройки TCP/IP

Настройка DNS

DNS (служба доменных имен) обеспечивает перевод имен узлов в IP-адреса. Чтобы задать параметры DNS, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

Выберите элемент **Obtain DNS server address via DHCP (Получить адрес DNS-сервера от DHCP-сервера)**, чтобы использовать параметры DNS-сервера, предоставленные DHCP-сервером.

Чтобы задать настройки вручную, выберите **Use the following DNS server address (Использовать следующий адрес DNS-сервера)** и укажите следующие данные:

Имя домена - Укажите домены, в которых будет проведен поиск имени хоста, используемого устройством Axis. Можно указать несколько доменов, разделив их точкой с запятой. Имя хоста — это всегда первая часть полного доменного имени; например `myserver` — имя хоста в полном доменном имени `myserver.mycompany.com`, где `mycompany.com` — имя домена.

Основной/Дополнительный DNS-сервер - Введите IP-адреса основного и дополнительного DNS-серверов. Наличие дополнительного DNS-сервера не является обязательным — он будет использоваться, если недоступен основной DNS-сервер.

Настройка NTP

NTP (Network Time Protocol) — протокол, используемый для синхронизации времени устройств в сети. Чтобы задать параметры NTP, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

Выберите элемент **Obtain NTP server address via DHCP (Получить адрес NTP-сервера от DHCP-сервера)**, чтобы использовать параметры NTP, предоставленные DHCP-сервером.

Чтобы ввести параметры вручную, выберите элемент **Use the following NTP server address (Использовать следующий адрес NTP-сервера)** и введите имя хоста или IP-адрес NTP-сервера.

Настройка имени хоста

К устройству Axis можно получить доступ с помощью имени хоста вместо IP-адреса. Как правило, имя хоста соответствует назначенному DNS-имени. Чтобы задать имя хоста, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

Выберите элемент **Obtain host name via IPv4 DHCP (Получить имя хоста с помощью IPv4 DHCP)**, чтобы использовать имя хоста, которое дает DHCP-сервер, применяющий протокол IPv4.

Чтобы задать имя хоста вручную, выберите **Use the host name (Использовать имя хоста)**.

Для динамического обновления имен локальных DNS-серверов при любых изменениях IP-адреса устройства Axis, выберите **Enable dynamic DNS updates (Включить динамическое обновление DNS-серверов)**. Дополнительные сведения можно найти в онлайн-справке.

Локальный IPv4-адрес

Параметр **Link-Local Address (Локальный адрес)** включен по умолчанию и означает назначение устройству Axis дополнительного IP-адреса, который можно использовать для доступа к устройству с других хост-компьютеров в том же сегменте локальной сети. Устройство может одновременно иметь локальный IP-адрес и статический IP-адрес, получаемый от DHCP-сервера.

Чтобы отключить эту функцию, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

HTTP

HTTP-порт, используемый устройством Axis, можно изменить в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**. Помимо значения 80, которое задано по умолчанию, можно использовать любой порт в диапазоне 1024–65535.

HTTPS

HTTP-порт, используемый устройством Axis, можно изменить в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Дополнительная настройка контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**. Помимо значения 443, которое задано по умолчанию, можно использовать любой порт в диапазоне 1024–65535.

Чтобы включить HTTPS, выберите в меню последовательно **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Настройка > Настройка дополнительного контроллера > Параметры системы > Безопасность > HTTPS)**. Дополнительные сведения см. в разделе *HTTPS на стр. 28*.

Прослеживание NAT (сопоставление портов) для IPv4

Сетевой маршрутизатор позволяет устройствам частной (локальной) сети совместно использовать единое подключение к Интернету. Для этого сетевой трафик из частной сети переадресуется во "внешнюю" сеть, то есть в Интернет. Безопасность частной (локальной) сети повышается, так как настройки большинства маршрутизаторов широкополосной связи предотвращают попытки доступа к частной (локальной) сети из общедоступной сети (Интернета).

Используйте функцию **NAT Traversal**, если камера расположена в интрасети (локальной сети), и вы хотите открыть к ней доступ с внешней стороны NAT-маршрутизатора (из глобальной сети). При должной настройке прохождения NAT весь HTTP-трафик, поступающий на внешний HTTP-порт NAT-маршрутизатора, будет перенаправляться на устройство.

Чтобы настроить функцию NAT Traversal, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

Примечание.

- Технология NAT Traversal будет работать только в том случае, если она поддерживается маршрутизатором. Маршрутизатор также должен поддерживать технологию UPnP®.
- В данном контексте маршрутизатор означает любое устройство сетевой маршрутизации, включая NAT-маршрутизатор, сетевой маршрутизатор, интернет-шлюз, маршрутизатор широкополосной связи, разделяемое устройство широкополосной связи или программное обеспечение, например, межсетевой экран.

Enable/Disable (Включение и выключение) – Если эта функция включена, устройство Axis попытается настроить сопоставление портов в NAT-маршрутизаторе вашей сети с помощью UPnP. Обратите внимание, что в устройстве необходимо включить UPnP (см. **Setup > Additional Controller Configuration > System Options > Network > UPnP (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > UPnP)**).

Выбор NAT-маршрутизатора вручную – Выберите этот пункт, чтобы вручную выбрать NAT-маршрутизатор, и введите IP-адрес маршрутизатора в соответствующее поле. Если маршрутизатор не указан вручную, устройство будет автоматически вести поиск NAT-маршрутизатора в сети. Если обнаружено несколько маршрутизаторов, будет выбран маршрутизатор, указанный по умолчанию.

Alternative HTTP port (Альтернативный HTTP-порт) – Выберите этот пункт, чтобы вручную задать внешний HTTP-порт. Введите номер порта в диапазоне 1024–65535. Если поле порта оставлено пустым или содержит значение по умолчанию (0), номер порта автоматически выбирается при включении прослеживания NAT.

Примечание.

- Альтернативный HTTP-порт может использоваться или быть активным даже при отключенном прослеживании NAT. Это полезно, если ваш NAT-маршрутизатор не поддерживает UPnP, и вам необходимо вручную настроить порт переадресации в NAT-маршрутизаторе.
- Если выбранный вручную порт уже используется, другой порт будет выбран автоматически.
- Если порт выбирается автоматически, он отображается в этом поле. Чтобы изменить его, введите новый номер порта и нажмите кнопку **Save (Сохранить)**.

FTP

FTP-сервер, работающий в устройстве Axis, обеспечивает загрузку нового встроенного ПО, приложений пользователя и т. д. FTP-сервер можно отключить в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**.

RTSP

RTSP-сервер, запущенный в устройстве Axis, позволяет подключившемуся клиенту запустить передачу данных о событиях. Номер порта RTSP можно изменить в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Настройка > Дополнительная настройка контроллера > Параметры системы > Сеть > TCP/IP > Дополнительно)**. Номер порта по умолчанию — 554.

Примечание.

Передача данных о событиях будет недоступна, если RTSP-сервер отключен.

SOCKS

SOCKS — прокси-протокол организации сети. В параметрах устройства Axis можно настроить использование SOCKS-сервера для обращения к сетям по другую сторону от межсетевого экрана или прокси-сервера. Эта функциональность полезна, если устройство Axis расположено в локальной сети за межсетевым экраном, а уведомления, отправка, сигналы тревоги и т. д. необходимо отправлять в пункт назначения за пределами локальной сети (например, в Интернет).

SOCKS можно настроить в меню **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > SOCKS)**. Дополнительные сведения можно найти в онлайн-справке.

Стандарт Quality of service (QoS)

Стандарт Quality of Service (QoS) гарантирует обеспечение определенного уровня указанных ресурсов для выбранного трафика в сети. Сеть с QoS назначает приоритет сетевому трафику и обеспечивает увеличенную надежность сети, благодаря управлению нагрузкой на полосу пропускания, которую может использовать приложение.

Параметры QoS настраиваются в разделе **Setup > Additional Controller Configuration > System Options > Network > QoS (Настройка > Дополнительная настройка контроллера >Параметры системы > Сеть > QoS)**. С помощью значений DSCP (Differentiated Services Codepoint) устройство Axis отмечает трафик событий и сигналов тревоги и трафик управления.

SNMP

Протокол SNMP (Simple Network Management Protocol) позволяет осуществлять удаленное управление сетевыми устройствами. Сообщество SNMP — группа устройств и управляющая станция, работающая по SNMP. Имена сообществ служат для идентификации групп.

Чтобы включить и настроить SNMP в устройстве Axis, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > SNMP (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > SNMP)**.

В зависимости от требуемого уровня защиты выберите нужную версию SNMP.

Ловушки используются устройством Axis для отправки сообщений системе управления при важных событиях или изменениях состояния. Установите флажок **Enable traps (Включить ловушки)** и введите IP-адрес, на который будут отправляться сообщения ловушки. Укажите сообщество, которое будет получать сообщение, в поле **Trap community (Сообщество ловушки)**.

Примечание.

Если протокол HTTPS включен, протоколы SNMP v1 и SNMP v2c необходимо отключить.

Traps for SNMP v1/v2 (Ловушки для SNMP v1/v2) используются устройством Axis для отправки сообщений системе управления при важных событиях или изменениях состояния. Установите флажок **Enable traps (Включить ловушки)** и введите IP-адрес, на который будут отправляться сообщения ловушки. Укажите сообщество, которое будет получать сообщение, в поле **Trap community (Сообщество ловушки)**.

Доступны следующие ловушки:

- Cold start. Холодный запуск.
- Warm start. Горячий запуск.
- Link up. Соединение установлено.
- Authentication failed. Проверка подлинности не пройдена.

SNMP v3 обеспечивает шифрование и надежные пароли. Для использования ловушек с SNMP v3 требуется приложение управления SNMP v3.

Чтобы использовать SNMP v3, необходимо активировать HTTPS. См. раздел *HTTPS на стр. 28*. Чтобы включить SNMP v3, установите флажок и задайте исходный пароль пользователя.

Примечание.

Исходный пароль можно задать только один раз. Если вы забудете пароль, необходимо произвести сброс параметров устройства Axis к заводским установкам по умолчанию. См. раздел *Сброс к заводским установкам на стр. 38*.

UPnP

В устройстве Axis реализована поддержка UPnP®. Стандарт UPnP по умолчанию включен, поэтому устройство автоматически обнаруживается операционными системами и клиентами, которые поддерживают этот протокол.

UPnP можно отключить в меню **Setup > Additional Controller Configuration > System Options > Network > UPnP (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > UPnP)**.

Bonjour

В устройстве Axis реализована Bonjour. Стандарт Bonjour по умолчанию включен, поэтому устройство может быть автоматически обнаружено операционными системами и клиентами, которые поддерживают этот протокол.

Bonjour можно отключить в меню **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > Bonjour)**.

Порты и устройства

Порты ввода-вывода

Благодаря дополнительному разъему имеется четыре настраиваемых порта ввода и вывода для подключения внешних устройств.

Внешний разъем обеспечивает два настраиваемых порта ввода и вывода для подключения внешних устройств.

Для настройки портов ввода-вывода перейдите в меню **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Настройка > Настройка дополнительного контроллера >Параметры системы > Порты и устройства > Порты ввода-вывода)**. Выберите направление передачи данных для порта (**Input (Вход)** или **Output (Выход)**). Портам можно давать описательные имена, а в качестве значения параметра **Normal states (Нормальные состояния)** можно задать для них состояние **Open circuit (Разомкнутая цепь)** или **Grounded circuit (Заземленная цепь)**.

Состояние портов

Выбрав в меню **System Options > Ports & Devices > Port Status (Параметры системы > Порты и устройства > Состояние портов)**, вы увидите список, в котором будет отображено состояние входных и выходных портов устройства.

Обслуживание

В устройстве Axis предусмотрено несколько функций обслуживания. Для доступа к ним выберите **Setup > Additional Controller Configuration > System Options > Maintenance (Настройка > Настройка дополнительного контроллера > Параметры системы > Обслуживание)**.

Нажмите кнопку **Restart (Перезапуск)**, чтобы правильно выполнить перезагрузку системы, если устройство Axis ведет себя неожиданным образом. Это не повлияет ни на какие текущие параметры.

Примечание.

Перезагрузка очищает все записи в отчете сервера.

Для сброса большинства параметров к заводским установкам нажмите кнопку **Restore (Восстановить)**. Сброс не затрагивает следующие параметры:

- протокол изначальной загрузки (DHCP или статический);
- статический IP-адрес;
- маршрутизатор по умолчанию;
- маска подсети;
- системное время;
- настройки, соответствующие стандарту IEEE 802.1X;

Для сброса всех параметров, включая IP-адрес, к заводским установкам нажмите кнопку **Default (По умолчанию)**. Этой кнопкой следует пользоваться с осторожностью. Для сброса параметров устройства Axis к заводским установкам также можно использовать кнопку управления, см. раздел *Сброс к заводским установкам на стр. 38*.

Сведения об обновлении встроенного ПО см. в разделе *Как обновить встроенное ПО на стр. 38*.

Поддержка

Обзор поддержки

Страница **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Настройка > Настройка дополнительного контроллера > Параметры системы > Поддержка > Обзор поддержки)** содержит информацию об устранении неполадок, а также контактные данные на случай, если вам понадобится техническая помощь.

См. также *Устранение неполадок на стр. 38*.

Обзор системы

С обзором состояния и настроек устройства Axis можно ознакомиться в меню **Setup > Additional Controller Configuration > System Options > Support > System Overview (Настройка > Настройка дополнительного контроллера > Параметры системы > Поддержка > Обзор системы)**. Среди указанных здесь сведений: версия встроенного ПО, IP-адрес, настройки сети, безопасности, событий, а также последние записи в журнале.

Журналы и отчеты

Выбрав в меню **Настройка > Настройка дополнительного контроллера > Параметры системы > Поддержка > Журналы и отчеты**, вы откроете страницу, где можно создать журналы и отчеты, которые полезны для анализа системы, диагностики и устранения неисправностей. При обращении в службу поддержки Axis приложите к своему запросу отчет сервера.

Системный журнал – Он содержит сведения о системных событиях.

Журнал доступа – В нем фиксируются все неудачные попытки доступа к устройству. Журнал доступа также можно настроить таким образом, чтобы в нем были представлены все подключения к данному устройству (см. ниже).

Просмотр отчета сервера – В этом отчете представлена информация о статусе устройства (в открывающемся окне). В отчет сервера автоматически включается журнал доступа.

Скачать отчет сервера – При скачивании создается файл .zip, который содержит полный отчет сервера в виде текстового файла формата UTF–8. Чтобы включить в отчет моментальный снимок, сделанный в режиме живого просмотра на устройстве,

выберите **Include snapshot from Live View (Включить моментальный снимок в режиме живого просмотра)**. При обращении в службу поддержки всегда следует прикладывать файл .zip.

Список параметров – В списке представлены параметры устройства и их текущие значения. Это может оказаться полезным при поиске неполадок или при обращении в службу поддержки Axis.

Список подключений – В списке перечислены все клиенты, которые в данный момент имеют доступ к различным потокам данных.

Отчет об отказах системы – Создается архив с информацией об отладке. Для создания отчета требуется несколько минут.

Уровни журнала для системного журнала и журнала доступа настраиваются в меню **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Настройка > Настройка дополнительного контроллера > Параметры системы > Поддержка > Журналы и отчеты > Конфигурация)**. Журнал доступа можно настроить таким образом, чтобы в нем были представлены все подключения к данному устройству (для этого следует выбрать параметры Critical (Критические), Warnings (Предупреждения) и Info (Сведения)).

Дополнительно

Сценарии

У опытных пользователей есть возможность создавать и использовать собственные сценарии.

ПРИМЕЧАНИЕ.

Неправильное использование может привести к неожиданному поведению и даже вызвать потерю соединения с устройством Axis.

Axis настоятельно рекомендует использовать эту функцию только в том случае, если вы отдаете себе полный отчет в возможных последствиях. Служба поддержки Axis не оказывает помощь в решении проблем, связанных с пользовательскими сценариями.

Чтобы открыть редактор сценариев, перейдите в меню **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Настройка > Настройка дополнительного контроллера > Параметры системы > Дополнительно > Создание сценариев)**. Если сценарий вызывает проблемы, сбросьте параметры устройства к заводским установкам по умолчанию. См. *стр. 38*.

Дополнительные сведения см. на сайте *www.axis.com/developer*.

Загрузка файлов

Файлы, в частности, веб-страницы и изображения, можно загрузить в устройство Axis и использовать в качестве пользовательских настроек. Чтобы загрузить файл, выберите в меню **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Настройка > Настройка дополнительного контроллера > Параметры системы > Дополнительно > Загрузка файла)**.

Загруженные файлы доступны по адресу `http://<ip address>/local/<user>/<file name>`, где `<user>` — это выбранная группа пользователей (administrator (администратор)) загруженного файла.

Устранение неполадок

Сброс к заводским установкам

Важно!

Следует с осторожностью выполнять сброс к заводским установкам. Сброс к заводским установкам приведет к возврату всех параметров (включая IP-адрес) к принимаемым по умолчанию значениям.

Для сброса параметров изделия к заводским установкам:

1. Отсоедините питание устройства.
2. Нажмите и удерживайте кнопку управления, одновременно подключив питание. См. *Общий вид устройства на стр. 5* .
3. Удерживайте кнопку управления в нажатом положении в течение 25 секунд, пока индикатор состояния во второй раз не загорится желтым светом.
4. Отпустите кнопку управления. Процесс завершен, когда индикатор состояния становится зеленым. Произошел сброс параметров устройства к заводским установкам по умолчанию. Если в сети нет доступного DHCP-сервера, то IP-адресом по умолчанию будет `192.168.0.90`.
5. С помощью программных средств установки и управления назначьте IP-адрес и задайте пароль, чтобы получить доступ к устройству.

Сброс параметров к заводским установкам также можно выполнить с помощью веб-интерфейса. Выберите последовательно **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Настройка > Конфигурация дополнительного контроллера > Настройка > Параметры системы > Обслуживание)** и выберите **Default (По умолчанию)**.

Как узнать текущую версию встроенного ПО

Встроенное ПО определяет функциональность сетевых устройств. При возникновении неполадок в первую очередь необходимо проверить текущую версию встроенного ПО. Последняя версия может содержать исправление, устраняющее вашу проблему.

Текущая версия встроенного ПО для устройства Axis отображается на странице Overview (Обзор).

Как обновить встроенное ПО

Важно!

- Ваш дилер оставляет за собой право взимать плату за любой ремонт, связанный с неправильным обновлением встроенного ПО пользователем.
- При обновлении встроенного ПО ранее измененные настройки будут сохранены при условии наличия тех же функций в новой версии встроенного ПО, хотя Axis Communications этого не гарантирует.
- Если вы устанавливаете предыдущую версию встроенного ПО, необходимо будет после этого восстановить заводские установки по умолчанию.

Примечание.

- После завершения обновления устройство автоматически перезапускается. Если вы производите перезапуск вручную после обновления, подождите 5 минут, даже если вы подозреваете, что обновление завершилось неудачно.
- Первый запуск после обновления встроенного ПО может занять несколько минут, поскольку после встроенного ПО обновляется база данных пользователей, групп, учетных данных и другие сведения. Продолжительность запуска зависит от объемов данных.
- После обновления встроенного ПО до последней версии на устройстве Axis становятся доступны новые функции. Перед обновлением встроенного ПО всегда читайте инструкции по обновлению и примечания к выпуску.

1. Последнюю версию встроенного ПО можно бесплатно загрузить на свой компьютер со страницы *www.axis.com/support*
2. Перейдите в меню **Setup > Additional Controller Configuration > System Options > Maintenance (Настройка > Настройка дополнительного контроллера > Параметры системы > Обслуживание)** на веб-страницах устройства.
3. В разделе **Upgrade Server (Сервер обновления)** нажмите кнопку **Choose file (Выбрать файл)** и найдите нужный файл на своем компьютере.
4. Если требуется, чтобы устройство после обновления автоматически производило сброс к заводским установкам по умолчанию, установите флажок **Default (По умолчанию)**.
5. Нажмите кнопку **Upgrade (Обновить)**.
6. Подождите примерно 5 минут, пока устройство обновляется и перезапускается. Затем очистите кэш браузера.
7. Войдите в систему устройства.

Симптомы, возможные причины и меры по их устранению

Проблемы при обновлении встроенного ПО	
Сбой при обновлении встроенного ПО	Если при обновлении встроенного ПО происходит сбой, устройство вновь загружает предыдущую версию этого ПО. Проверьте файл встроенного ПО и повторите попытку.

Проблемы с заданием IP-адреса	
При использовании ARP/Ping	Попробуйте выполнить установку еще раз. IP-адрес должен быть задан в течение двух минут после подключения питания устройства. Убедитесь в том, что заданная длина ping-пакета составляет 408. Инструкции см. в руководстве по установке на странице устройства на сайте *www.axis.com*.
Устройство расположено в другой подсети	Если IP-адрес, предназначенный для устройства, и IP-адрес компьютера, используемого для получения доступа к устройству, расположены в разных подсетях, вы не сможете настроить IP-адрес. Свяжитесь с сетевым администратором, чтобы получить соответствующий IP-адрес.
IP-адрес используется другим устройством.	Отключите устройство Axis от сети. Запустите команду Ping (в командной строке или сеансе DOS введите `ping` и IP-адрес устройства): • Если вы получите следующий ответ: `Reply from <IP-адрес>: bytes=32; time=10...` — это означает, что данный IP-адрес, возможно, уже используется другим устройством в сети. Получите новый IP-адрес от сетевого администратора и переустановите устройство. • Если вы получите следующий ответ: `Request timed out`, это означает, что данный IP-адрес доступен для использования устройством Axis. В этом случае проверьте все кабели и переустановите устройство.
Возможный конфликт с IP-адресом другого устройства в той же подсети	Перед тем, как DHCP-сервер установит динамический адрес, в устройстве Axis используется статический IP-адрес. Таким образом, если тот же статический IP-адрес используется другим устройством, при доступе к устройству Axis могут возникнуть проблемы.

К устройству нет доступа из браузера	
Не удается войти в систему.	Если протокол HTTPS включен, убедитесь, что при попытке входа в систему используется правильный протокол (HTTP или HTTPS). Возможно, вам придется вручную ввести `http` или `https` в поле адреса браузера. Если утерян пароль для пользователя root, необходимо произвести сброс параметров устройства к заводским установкам по умолчанию. См. *Сброс к заводским установкам на стр. 38*.

Устранение неполадок

IP-адрес изменен DHCP-сервером.	IP-адрес, получаемый от DHCP-сервера, является динамическим и может меняться. Если IP-адрес изменился, используйте утилиту AXIS IP Utility или AXIS Device Manager, чтобы найти устройство в сети. Устройство можно идентифицировать по модели, серийному номеру или DNS-имени (если это имя задано). При необходимости можно вручную назначить статический IP-адрес. Инструкции см. в документе *How to assign an IP address and access your device (Как назначить IP-адрес и получить доступ к устройству)* на странице данного устройства на *axis.com*
Ошибка сертификата при использовании IEEE 802.1X	Проверка подлинности пройдет должным образом только в том случае, если параметры даты и времени устройства Axis синхронизируются с NTP-сервером. См. .

Устройство доступно локально, но не из внешней сети.

Настройка маршрутизатора	Чтобы маршрутизатор пропускал входящий трафик данных к устройству Axis, включите функцию NAT Traversal, которая попытается автоматически настроить маршрутизатор для получения доступа к устройству Axis. См. раздел *Прослеживание NAT (сопоставление портов) для IPv4 на стр. 33*. Маршрутизатор должен поддерживать технологию UPnP®.
Защита с помощью межсетевого экрана	Попросите сетевого администратора проверить настройки межсетевого экрана.
Требуются настройки маршрутизатора по умолчанию.	Проверьте, нужно ли настроить параметры маршрутизатора в меню **Setup > Network Settings (Настройка > Настройки сети)** или в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Основные)**.

Характеристики

Текст с пометкой **UL** действителен только для систем, соответствующих стандарту UL 293 или UL 294.

Светодиодные индикаторы

Индикатор	Цвет	Индикация
Сеть	Зеленый	Горит непрерывно — подключение к сети 100 Мбит/с. Мигает — осуществляется обмен данными по сети.
	Желтый	Горит непрерывно — подключение к сети 10 Мбит/с. Мигает — осуществляется обмен данными по сети.
	Не горит	Сетевое подключение отсутствует.
Состояние	Зеленый	Непрерывно горит зеленым — нормальный режим работы.
	Желтый	Горит непрерывно во время запуска и при восстановлении настроек.
	Красный	Медленно мигает — ошибка обновления.
Питание	Зеленый	Нормальный режим работы.
	Желтый	Мигает зеленым и желтым во время обновления встроенного ПО.
Перегрузка реле по току	Красный	Горит непрерывно в случае короткого замыкания или при обнаружении перегрузки по току.
	Не горит	Нормальный режим работы.
Перегрузка считывателя по току	Красный	Горит непрерывно в случае короткого замыкания или при обнаружении перегрузки по току.
	Не горит	Нормальный режим работы.
Реле	Зеленый	Реле активно. [1]
	Не горит	Реле не активно.

1. Реле активно при соединении контактов COM и NO.

Примечание.

- Индикатор состояния можно настроить так, чтобы он мигал, пока событие активно.
- Индикатор состояния можно настроить так, чтобы он мигал при идентификации устройства. Выберите в меню последовательно **Setup > Additional Controller Configuration > System Options > Maintenance (Настройка > Дополнительная настройка контроллера > Параметры системы > Обслуживание)**.

Кнопки

Кнопка управления

Кнопка управления служит для выполнения следующих действий.

- Сброс параметров изделия к заводским установкам. См. *Сброс к заводским установкам на стр. 38*.

Разъемы

Сетевой разъем

Разъем RJ45 Ethernet с поддержкой технологии Power over Ethernet Plus (PoE+).

Характеристики

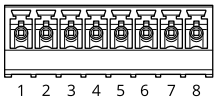
UL: Питание по технологии Power over Ethernet (PoE) должно осуществляться с использованием инжектора ограниченной мощности, который внесен в реестр UL 294, обеспечивает напряжение питания 44–57 В пост. тока и мощность 15,4 Вт/30 Вт и соответствует стандарту Power over Ethernet IEEE 802.3af/802.3at, тип 1, класс 3 либо стандарту Power over Ethernet Plus (PoE+) IEEE 802.3at, тип 2, класс 4. Питание по технологии Power over Ethernet (PoE) было проверено компанией UL с применением AXIS T8133 Midspan 30 W 1-port.

Разъем считывателя

Две 8-контактные клеммные колодки с поддержкой стандарта RS485 и протоколов Wiegand для связи со считывателем.

Указанные значения выходной мощности являются общими для двух портов считывателя. Это означает, что для всех считывателей, подключенных к дверному контроллеру, в сумме может быть обеспечен ток 486 мА при напряжении 12 В пост. тока.

Выберите протокол для использования на веб-странице устройства.



Настроено для RS485

Функция	Контакт	Примечание.	Технические характеристики
Заземление пост. тока (GND)	1		0 В пост. тока
Выход питания пост. тока (+12 В)	2	Подача питания на считыватель.	12 В пост. тока, макс. 486 мА в сумме для обоих считывателей
RX/TX	3–4	Полный дуплекс: RX. Полудуплекс: RX/TX.	
TX	5–6	Полный дуплекс: TX.	
Настраиваемый (вход или выход)	7–8	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 30 В пост. тока
		Цифровой выход: при подключении индуктивной нагрузки, например реле, параллельно нагрузке должен включаться диод для защиты от переходных напряжений.	От 0 до макс. 30 В пост. тока, с открытым стоком, 100 мА

Важно!

- Когда питание считывающего устройства обеспечивается контроллером, допустимая длина кабеля составляет до 30 метров.
- Если питание считывающего устройства не обеспечивается контроллером, длина кабеля считывающего устройства может составлять до 200 метров при следующих требованиях к кабелю: 1 витая пара с экраном, AWG 24, сопротивление 120 Ом.

Настроено для Wiegand

Характеристики

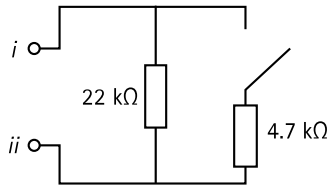
Функция	Контакт	Примечание	Технические характеристики
Заземление по пост. току (GND)	1		0 В пост. тока
Выход питания пост. тока (+12 В)	2	Подача питания на считыватель.	12 В пост. тока, макс. 486 мА в сумме для обоих считывателей
D0	3		
D1	4		
O	5–6	Цифровой выход, с открытым стоком	
Настраиваемый (вход или выход)	7–8	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 30 В пост. тока
		Цифровой выход: при подключении индуктивной нагрузки, например реле, параллельно нагрузке должен включаться диод для защиты от переходных напряжений.	От 0 до макс. 30 В пост. тока, с открытым стоком, 100 мА

Важно!

- Когда питание считывающего устройства обеспечивается контроллером, допустимая длина кабеля составляет до 30 метров.
- Если питание считывающего устройства не обеспечивается контроллером, длина кабеля считывающего устройства может составлять до 150 метров при следующих требованиях к кабелю: AWG 22.

Контролируемые входы

Чтобы использовать контролируемые входы, подключите оконечные резисторы, как показано на схеме ниже.



i Вход

ii 0 В пост. тока (-)

UL: проверка контролируемых входов на возможность применения в системе охранной сигнализации компанией UL не производилась. Только дверной монитор и устройство запроса выхода (REX) поддерживают контроль с использованием оконечных резисторов.

Примечание.

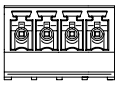
Рекомендуется использовать экранированные кабели с витыми парами. Экранирующую оплетку следует подсоединить к цепи 0 В пост. тока.

Характеристики

Разъем дверного датчика

Две 4-контактные клеммные колодки для устройств дверного мониторинга (цифровой вход).

Только дверной монитор осуществляет контроль благодаря резисторам на концах линии. При нарушении подключения раздается сигнал тревоги. Чтобы использовать контролируемые входы, установите резисторы на концах линии. Для контролируемых входов используйте схему подключения. См. *стр. 43*.



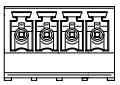
Функция	Контакт	Примечания	Технические характеристики
Заземление пост. тока	1, 3		0 В пост. тока
Вход	2, 4	Для обмена данными с дверным монитором. Цифровой вход или контролируемый вход — подсоедините к контакту 1 или 3, чтобы, соответственно, активировать или деактивировать (оставить свободным, то есть неподсоединенным).	От 0 до макс. 30 В пост. тока

Важно!

Допустимая длина кабеля составляет до 30 метров при соблюдении следующих требований: AWG 24.

Разъем реле

Две 4-контактные клеммные колодки для реле типа C, которые можно использовать, например, для управления замком или интерфейсом для ворот.



Функция	Контакт	Примечания	Технические характеристики
DC ground (GND) (Заземление пост. тока)	1		0 В пост. тока
NO	2	Нормально разомкнутые. Для подключения релейных устройств. Подключите отказоустойчивую блокировку между контактами NO и DC ground. Два релейных контакта гальванически отделены от остальной части схемы, если не используются перемычки.	Макс. ток = 2 А на реле Макс. напряжение = 30 В пост. тока
COM	3	Общие	
NC	4	Нормально замкнутые. Для подключения релейных устройств. Подключите отказоустойчивую блокировку между контактами NC и DC ground. Два релейных контакта гальванически отделены от остальной части схемы, если не используются перемычки.	

Характеристики

Перемычка для питания реле

Установленная перемычка для питания реле соединяет контакт «COM» реле с цепью 12 В пост. тока или 24 В пост. тока.

Ее можно использовать для подключения замка между контактом «GND» и нормально разомкнутым контактом («NO») или между контактом «GND» и нормально замкнутым контактом («NC»).

Блок питания	Макс. мощность при 12 В пост. тока[1]	Макс. мощность при 24 В пост. тока[1]
Вход пост. тока	1 600 мА	800 мА
PoE	800 мА	400 мА

1. Питание подается на два реле и на дополнительные входы-выходы (12 В пост. тока).

ПРИМЕЧАНИЕ.

Если применяется неполяризованный замок, рекомендуется добавить внешний диод обратной цепи.

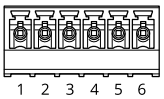
Вспомогательный разъем

Используйте вспомогательный разъем для подключения внешних устройств в сочетании, например, с детектором движения, устройством подачи сигнала тревоги, а также с устройством, запускаемым определенными событиями. Помимо точки заземления 0 В пост. тока и питания (выход пост. тока), вспомогательный разъем служит интерфейсом, который обеспечивает:

Цифровой вход – Для подключения устройств, которые способны размыкать и замыкать цепь, как, например, пассивные ИК-датчики, дверные/оконные контакты и детекторы разбивания стекла.

Цифровой выход – Для подключения внешних устройств, например реле и светодиодных индикаторов. Подключенные устройства можно активировать с помощью прикладного программного интерфейса API VAPIX® или на веб-странице устройства.

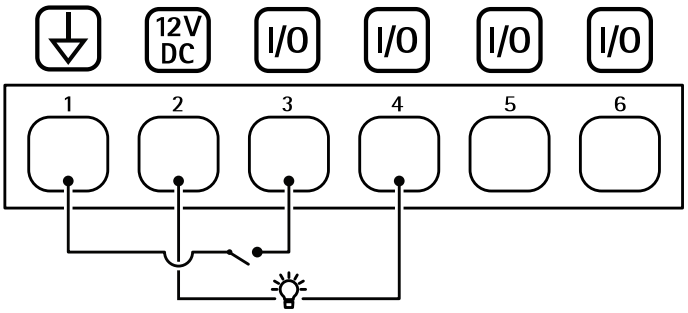
6-контактная клеммная колодка



Функция	Кон-такт	Примечания	Технические характеристики
Заземление пост. тока	1		0 В пост. тока
Выход питания пост. тока	2	Может использоваться для питания дополнительного оборудования. Примечание. Этот контакт может использоваться только для подачи питания на внешние устройства.	12 В пост. тока Макс. нагрузка = 50 мА для каждого входа-выхода.

Характеристики

Настраиваемый (вход или выход)	3–6	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 30 В пост. тока
		Цифровой выход: в активном состоянии соединен с контактом 1 («земля» пост. тока) через внутреннюю цепь, в неактивном состоянии ни с чем не соединен. При подключении индуктивной нагрузки, например реле, параллельно нагрузке следует включить диод для защиты от переходных напряжений. Каждый вход-выход способен подавать питание 12 В пост. тока, 50 мА (макс.) на внешнюю нагрузку, если используется выход внутреннего напряжения 12 В пост. тока (контакт 2). В случае применения схемы подключения с открытым стоком в сочетании с внешним источником питания входы-выходы способны работать при напряжении 0–30 В пост. тока и максимальном токе 100 мА.	От 0 до макс. 30 В пост. тока, с открытым стоком, 100 мА

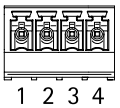


1 *«Земля» по пост. току*
2 *Выход питания пост. тока +12 В*
3 *Вход-выход настроен как вход*
4 *Вход-выход настроен как выход*
5 *Настраиваемый вход-выход*
6 *Настраиваемый вход-выход*

Внешний разъем

4-контактная клеммная колодка для подключения внешних устройств, например детектора разбивания стекла или детектора пожара.

UL: проверка разъема на возможность применения в системе охранной или пожарной сигнализации компанией UL не производилась.



Функция	Контакт	Примечания	Технические характеристики
Заземление пост. тока	1, 3		0 В пост. тока

Настраиваемый (вход или выход)	2, 4	Цифровой вход: для активации подключить к контакту 1 или 3, для деактивации оставить свободным (неподключенным).	От 0 до макс. 30 В пост. тока
		Цифровой выход: для активации подключить к контакту 1 или 3, для деактивации оставить свободным (неподключенным). При подключении индуктивной нагрузки, например реле, параллельно нагрузке должен включаться диод для защиты от переходных напряжений.	От 0 до макс. 30 В пост. тока, с открытым стоком, 100 мА.

Разъем питания

2-контактная клеммная колодка для ввода питания пост. тока. В целях безопасности используйте сверхнизковольтный (SELV) источник ограниченной мощности (LPS), у которого либо номинальная выходная мощность не превышает 100 Вт, либо номинальный выходной ток не превышает 5 А.

Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1		0 В пост. тока
Вход питания пост. тока	2	Для питания контроллера без использования технологии Power over Ethernet. Примечание. Этот контакт может использоваться только для подачи питания от внешнего источника.	10,5–28 В пост. тока, макс. 36 Вт

UL: питание постоянного тока должно поступать от источника питания, сертифицированного на соответствие UL 294, UL 293 или UL 603, с номинальными параметрами, соответствующими целям применения.

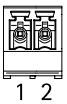
Входной разъем для подключения резервной батареи

Служит для резервного питания от аккумулятора со встроенным зарядным устройством. Вход напряжения питания 12 В пост. тока.

UL: проверка разъема компанией UL не производилась.

Важно!

При использовании входа батареи необходимо последовательно подключить внешний плавкий предохранитель на 3 А с задержкой срабатывания.



Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1		0 В пост. тока
Вход батареи	2	Для питания дверного контроллера, если другие источники питания недоступны. Примечание. Этот контакт можно использовать только для подачи питания на батарею. Только для подключения к ИБП.	11–13,7 В пост. тока, макс. 36 Вт

Сведения по безопасности

Уровни опасности

⚠ОПАСНО

Опасная ситуация, которая, если ее не устранить, приведет к смерти или опасным травмам.

⚠ВНИМАНИЕ!

Опасная ситуация, которая, если ее не устранить, может привести к смерти или опасным травмам.

⚠ОСТОРОЖНО

Опасная ситуация, которая, если ее не устранить, может привести к травмам незначительной или средней тяжести.

ПРИМЕЧАНИЕ.

Опасная ситуация, которая, если ее не устранить, может вызвать повреждение имущества.

Прочие уведомления

Важно!

Означает существенную информацию, которая важна для правильной работы изделия.

Примечание.

Означает полезную информацию, которая помогает использовать все возможности изделия.

Интерфейс устройства

Вход в интерфейс устройства осуществляется путем ввода IP-адреса в веб-браузере на устройстве.

Примечание.

Этот раздел относится только к контроллеру AXIS A1601 Network Door Controller со встроенным ПО AXIS Camera Station Secure Entry.

 Показать или скрыть основное меню.

 Доступ к справке по продукту.

 Изменить язык.

 Установка светлой или темной темы.

 Просмотр информации о пользователе, который вошел в систему.

 Контекстное меню содержит следующие команды:

- **Analytics data (Данные аналитики)**. Нажмите «Принять», чтобы разрешить передачу неперсональных данных просмотра веб-страниц.
- **Feedback (Обратная связь)**. Отправка отзывов, которые помогут нам повысить удобство работы пользователей.
- **Legal (Юридическая информация)**. Просмотр информации о файлах cookie и лицензиях.
- **About (О системе)**. Просмотр информации об устройстве, включая версию встроенного ПО и серийный номер.
- **Старый интерфейс устройства**: Измените интерфейс устройства на старый интерфейс устройства.

Состояние

Синхронизация по NTP

Отображение информации о синхронизации по протоколу NTP, в том числе о том, синхронизировано ли устройство с NTP-сервером, и о том, сколько времени осталось до следующей синхронизации.

NTP settings (Параметры NTP). Нажмите для перехода на страницу Date and time (Дата и время), где можно изменить параметры NTP.

Информация об устройстве

Отображение информации об устройстве, включая его серийный номер и версию встроенного ПО.

Upgrade firmware (Обновить встроенное ПО). Нажмите для перехода на страницу Maintenance (Обслуживание), где можно выполнить обновление встроенного ПО.

Контроль доступа

Тревоги

Device motion (Движение устройства): В системе при обнаружении движения устройства в дверном контроллере по умолчанию срабатывает сигнал тревоги.

Casing open (Вскрытие корпуса): В системе при обнаружении вскрытия корпуса в дверном контроллере по умолчанию срабатывает сигнал тревоги.

External tamper (Внешние несанкционированные действия): Подключается к порту ввода-вывода 13. Включите этот параметр, чтобы в системе при обнаружении внешних несанкционированных действий срабатывал сигнал тревоги. Например, при открытии или закрытии внешнего шкафа.

Supervised input (Контролируемый вход): Включите контроль входного состояния и настройте резисторы на концах линии.

- Чтобы использовать параллельное соединение, выберите пункт **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Параллельное соединение с параллельным резистором 22 кОм и последовательным резистором 4,7 кОм)**.
- Чтобы использовать последовательное подключение, выберите **Serial first connection (Последовательное соединение)** и укажите значение резистора, выбрав его в раскрывающемся списке **Resistor values (Значения резистора)**.

Периферийные устройства

Upgrade readers (Обновление считывателей): Щелкните, чтобы обновить встроенное ПО на считывателях до новой версии. При наличии подключения к сети можно обновить только считыватель AXIS A4020-E Reader.

Система

Дата и время

Формат времени зависит от языковых настроек веб-браузера.

Примечание.

Рекомендуется синхронизировать дату и время устройства с NTP-сервером.

Synchronization (Синхронизация). Выберите способ синхронизации даты и времени устройства.

- **Automatic date and time (NTP server using DHCP) (Автоопределение даты и времени (NTP-сервер, использующий DHCP))**. Синхронизация с NTP-сервером, подключенным к серверу DHCP.
- **Automatic date and time (manual NTP server) (Автоопределение даты и времени (через NTP-сервер вручную))**. Синхронизация с выбранным вами NTP-сервером.
  - **Primary NTP server (Основной NTP-сервер)** и **Secondary NTP server (Резервный NTP-сервер)**. Введите IP-адрес одного или двух NTP-серверов. При использовании двух NTP-серверов устройство синхронизирует и подстраивает свое время на основании вводимых данных на обоих серверах.
- **Custom date and time (Пользовательская настройка даты и времени)**. Установка даты и времени вручную. Нажмите **Get from system (Получить из системы)**, чтобы однократно получить настройки даты и времени с вашего компьютера или мобильного устройства.

Time zone (Часовой пояс). Выберите часовой пояс, который будет использоваться. Время будет автоматически корректироваться с учетом летнего времени и зимнего времени.

Примечание.

Система использует настройки даты и времени во всех записях, журналах и системных параметрах.

Сеть

IPv4 and IPv6 (IPv4 и IPv6)

IPv4

- **Automatic IP (DHCP) and DNS (DHCP) (Автоматический IP-адрес (DHCP) и DNS (DHCP))**: Рекомендуемый параметр для большинства сетей. Текущие настройки обновляются автоматически.
- **Automatic IP (DHCP) and manual DNS (Автоматическое назначение IP-адреса (DHCP) и назначение DNS вручную)**: Обратитесь к администратору сети, чтобы задать настройки вручную. Текущие автоматические настройки обновляются автоматически.
- **Manual IP and DNS (Назначение IP-адреса и DNS вручную)**: Обратитесь к администратору сети, чтобы задать настройки вручную.

IP address (IP-адрес). Укажите уникальный IP-адрес устройства. В изолированных сетях можно случайным образом назначать статические IP-адреса при условии, что каждый адрес является уникальным. Во избежание конфликтов настоятельно рекомендуется обратиться к администратору сети, прежде чем назначить статический IP-адрес.

Subnet mask (Маска подсети). Укажите маску подсети.

Router (Маршрутизатор). Укажите IP-адрес маршрутизатора (шлюза), который по умолчанию используется для подключения устройств, находящихся в разных сетях и разных сегментах сети.

Hostname (Имя хоста). Введите имя хоста.

Search domains (Поиск по доменам). При использовании неполного имени хоста нажмите **Add search domain (Добавить поисковый домен)** и введите домен, в котором будет осуществляться поиск имени хоста, используемого устройством.

DNS servers (DNS-серверы). Нажмите **Add DNS server (Добавить DNS-сервер)** и введите IP-адрес основного DNS-сервера. Этот сервер обеспечивает преобразование имен хостов в IP-адреса в вашей сети.

IPv6

Assign IPv6 automatically (Назначить IPv6 автоматически). Выберите этот пункт, чтобы сетевой маршрутизатор автоматически назначил IP-адрес устройству.

HTTP and HTTPS (HTTP и HTTPS).

Allow access through (Разрешить доступ через). Выберите этот вариант, если пользователю разрешено подключаться к устройству через **HTTP**, **HTTPS** или оба протокола **HTTP and HTTPS (HTTP и HTTPS)**.

HTTPS — это протокол, обеспечивающий шифрование запросов страниц от пользователей и страниц, возвращаемых веб-сервером. Обмен зашифрованной информацией регулируется использованием сертификатов HTTPS, которые гарантируют надежность и безопасность сервера.

Чтобы на устройстве можно было использовать протокол HTTPS, необходимо установить сертификат HTTPS. Для создания и установки сертификатов перейдите в меню **System > Security (Система > Безопасность)**.

Примечание.

При просмотре зашифрованных веб-страниц по протоколу HTTPS возможно снижение производительности, особенно если вы запрашиваете страницу в первый раз.

HTTP port (Порт HTTP). Введите номер HTTP-порта, который будет использоваться. Допустимыми вариантами являются порт 80 или любой порт в диапазоне 1024-65535. Если вы вошли в систему от имени администратора, можете ввести любой порт в диапазоне 1-1023. Если используете порт в этом диапазоне, вы получите предупреждение.

HTTPS port (Порт HTTPS). Введите номер HTTPS-порта, который будет использоваться. Допустимыми вариантами являются порт 443 или любой порт в диапазоне 1024-65535. Если вы вошли в систему от имени администратора, можете ввести любой порт в диапазоне 1-1023. Если используете порт в этом диапазоне, вы получите предупреждение.

Certificate (Сертификат). Выберите сертификат, чтобы включить протокол HTTPS для данного устройства.

Friendly name (Понятное имя)

Bonjour®. Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

Bonjour name (Имя для протокола Bonjour). Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

Use UPnP® (Использовать UPnP®). Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

UPnP name (Имя в службе UPnP). Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

One-click cloud connection (Подключение к облаку одним щелчком)

Подключение к облаку в одно нажатие (O3C) совместно с сервисом O3C обеспечивает простой и безопасный доступ через Интернет к живому и записанному видео отовсюду, где бы вы ни находились. Дополнительные сведения см. на странице *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Разрешить O3C):

- **One-click (Одно нажатие)**. Значение по умолчанию. Нажмите и удерживайте нажатой кнопку управления, чтобы подключиться к службе O3C через Интернет. После нажатия кнопки управления необходимо зарегистрировать устройство в службе O3C в течение 24 часов. В противном случае, устройство будет отключено от службы O3C. После регистрации будет активирован параметр **Always (Всегда)** и устройство будет постоянно подключено к службе O3C.
- **Always (Всегда)**. Устройство будет постоянно пытаться подключиться к службе O3C через Интернет. После регистрации устройство будет постоянно подключено к службе O3C. Используйте этот вариант, если кнопка управления находится вне досягаемости.
- **No (Нет)**. Отключает службу O3C.

Proxy settings (Настройки прокси-сервера): Если требуется, задайте параметры прокси-сервера для подключения к серверу HTTP.

Host (Хост). Укажите адрес прокси-сервера.

Port (Порт). Введите номер порта, используемого для получения доступа.

Login (Логин) и **Password (Пароль)**. При необходимости введите имя пользователя и пароль для прокси-сервера.

Authentication method (Способ проверки подлинности).

- **Basic (Базовая)**. Этот способ является самой совместимой схемой проверки подлинности для протокола HTTP. Метод **Digest (Дайджест-авторизация)** безопаснее, так как в данном случае имя пользователя и пароль передаются серверу без шифрования.
- **Digest (Дайджест-авторизация)**. Этот способ является более безопасным, так как при его использовании пароль всегда передается по сети в зашифрованном виде.
- **Auto (Автоматически)** Этот вариант позволяет устройству выбирать способ проверки подлинности автоматически в зависимости от поддерживаемого способа. Приоритет отдается способу **Digest (Дайджест-авторизация)**, а не **Basic (Базовая)**.

Owner authentication key (OAK) (Ключ аутентификации владельца (OAK)): Нажмите **Get key (Получить ключ)**, чтобы получить ключ авторизации владельца. Это возможно только в том случае, если устройство подключено к Интернету без межсетевого экрана или прокси-сервера.

SNMP

Протокол SNMP (Simple Network Management Protocol) позволяет осуществлять удаленное управление сетевыми устройствами.

SNMP: Выберите версию SNMP для использования.

- **v1 and v2c (v1 и v2c)**.
  - **Read community (Сообщество для чтения)**. Укажите имя сообщества с уровнем доступа только для чтения ко всем поддерживаемым объектам SNMP. Значение по умолчанию: **public**.
  - **Write community (Сообщество для записи)**. Укажите имя сообщества с уровнем доступа для чтения и записи ко всем поддерживаемым объектам SNMP (кроме объектов, доступных только для чтения). Значение по умолчанию: **write**.
  - **Activate traps (Активировать ловушки)**. Включите данный параметр, чтобы активировать отчеты по ловушкам. Ловушки используются устройством для отправки сообщений системе управления при важных событиях или изменениях состояния. В интерфейсе устройства можно настроить ловушки для протоколов SNMP v1 и v2c. Ловушки автоматически отключаются, если вы перейдете на SNMP v3 или отключите SNMP. При использовании протокола SNMP v3 ловушки нужно настраивать с помощью приложения управления SNMP v3.
  - **Trap address (Адрес ловушки)**. Укажите адрес или имя хоста, присвоенные серверу управления.
  - **Trap community (Сообщество ловушки)**. Укажите сообщество, которое будет использоваться при отправке устройством сообщения ловушки в систему управления.
  - **Traps (Ловушки)**:
  - **Cold start (Холодный запуск)**. При запуске устройства отправляется сообщение ловушки.
  - **Warm start (Горячий запуск)**. При изменении настроек SNMP отправляется сообщение ловушки.
  - **Link up (Соединение установлено)**. Отправка сообщения ловушки при изменении статуса «соединение не установлено» на «соединение установлено».
  - **Authentication failed (Проверка подлинности не пройдена)**. Отправка сообщения ловушки при неудачной попытке авторизации.

Примечание.

Все ловушки AXIS Video MIB включаются при включении ловушек SNMP v1 и v2c. Дополнительные сведения см. в разделе *Axis OS Portal > SNMP*.

- **v3**: SNMP v3 — это более надежная версия протокола, обеспечивающая шифрование и надежные пароли. Для использования протокола SNMP v3 рекомендуется активировать протокол HTTPS, чтобы использовать HTTPS для передачи пароля. Это также поможет предотвратить несанкционированный доступ к незашифрованным ловушкам протоколов SNMP v1/v2c. При использовании протокола SNMP v3 ловушки нужно настраивать с помощью приложения управления SNMP v3.
  - **Password for the account "initial" (Пароль для учетной записи initial)**: Введите пароль SNMP для учетной записи с именем initial. Хотя пароль можно отправить без активации HTTPS, мы так поступать не рекомендуем. Пароль SNMP v3 можно задать лишь один раз, при этом рекомендуется включить протокол HTTPS. После установки пароля поле для ввода пароля больше не отображается. Для повторной установки пароля необходимо выполнить сброс устройства к заводским установкам.

Connected clients (Подключенные клиенты)

В списке отображаются все клиенты, подключенные к устройству.

Update (Обновление). Нажмите, чтобы обновить список.

Безопасность

Сертификаты

Сертификаты служат для проверки подлинности устройств в сети. Устройство поддерживает два типа сертификатов:

- **Сертификаты клиента/сервера**
  Сертификат клиента/сервера удостоверяет подлинность устройства. Он может быть самозаверяющим или может быть выдан Центром сертификации (ЦС). Самозаверяющий сертификат дает ограниченную защиту, и его можно использовать до получения сертификата, выданного Центром сертификации.
- **Сертификаты ЦС**
  Сертификат, выданный Центром сертификации (ЦС), можно использовать для подтверждения подлинности сертификата узла, например для идентификации сервера проверки подлинности, когда устройство подключается к сети, защищенной по стандарту IEEE 802.1X. Устройство поставляется с несколькими предустановленными сертификатами ЦС.

Поддерживаются следующие форматы:

- Форматы сертификатов: .PEM, .CER и .PFX
- Форматы закрытых ключей: PKCS#1 и PKCS#12

Важно!

При сбросе параметров устройства к заводским установкам все сертификаты удаляются. Любые предустановленные сертификаты ЦС будут установлены повторно.

Фильтрация сертификатов в списке.

Add certificate (Добавление сертификата). Нажмите эту кнопку, чтобы добавить сертификат.

Контекстное меню содержит следующие команды:

- **Certificate information (Информация о сертификате)**. Просмотр свойств установленного сертификата.
- **Delete certificate (Удалить сертификат)**. Удаление сертификата.
- **Create certificate signing request (Создать запрос подписи сертификата)**. Создание запроса на подписание сертификата для его отправки в регистрационный орган и подачи заявления на получение цифрового удостоверения личности.

IEEE 802.1x

IEEE 802.1x — стандарт для технологии контроля доступа в сеть с использованием портов, обеспечивающий проверку подлинности проводных и беспроводных сетевых устройств. Стандарт IEEE 802.1x основан на протоколе EAP (Extensible Authentication Protocol).

Для получения доступа к сети, защищенной IEEE 802.1x, сетевые устройства должны пройти проверку подлинности. Проверка подлинности выполняется сервером проверки подлинности. Как правило, это RADIUS-сервер, примерами которого являются FreeRADIUS и сервер Microsoft для проверки подлинности в Интернете (IAS).

Сертификаты

Если сертификат ЦС не был настроен, проверка сертификата сервера будет отключена и устройство будет проверять собственную подлинность независимо от того, к какой сети оно подключено.

При использовании сертификата в установке Axis устройство и сервер аутентификации авторизуются с помощью цифровых сертификатов через протокол EAP-TLS.

Чтобы обеспечить устройству доступ к сети, защищенной с помощью сертификатов, на устройстве должен быть установлен подписанный клиентский сертификат.

Client certificate (Сертификат клиента): Выберите сертификат клиента для использования IEEE 802.1x. Сервер проверки подлинности использует сертификат для подтверждения подлинности сервера аутентификации.

CA certificate (Сертификат ЦС): Выберите сертификат ЦС для проверки удостоверения сервера проверки подлинности. Если сертификат не выбран, устройство попытается пройти проверку подлинности независимо от того, к какой сети оно подключено.

EAP identity (Идентификатор EAP). Введите удостоверение пользователя, связанное с сертификатом клиента.

EAPOL version (Версия EAPOL). Выберите версию протокола EAPOL, используемую в сетевом коммутаторе.

Use IEEE 802.1x (Использовать IEEE 802.1x): Выберите этот пункт, чтобы использовать протокол IEEE 802.1x.

Prevent brute-force attacks (Предотвращение атак методом подбора)

Blocking (Блокировка): Включите, чтобы блокировать атаки методом подбора пароля. При таких атаках злоумышленник пытается угадать данные для входа в систему или ключи шифрования, перебирая разные варианты.

Blocking period (Период блокировки): Введите количество секунд, в течение которых будет блокироваться атака методом подбора пароля.

Blocking conditions (Блокирующие условия): Введите количество сбоев проверки подлинности в секунду, вызывающее блокировку. Можно задать количество ошибок, разрешенных как на уровне страницы, так и на уровне устройства.

IP address filter (Фильтр IP-адресов)

Use filter (Использовать фильтры): Выберите этот пункт, чтобы отфильтровать IP-адреса, которым разрешен доступ к устройству.

Policy (Политика): Укажите, следует ли **Allow (Разрешить)** доступ или **Deny (Запретить)** доступ для определенных IP-адресов.

Addresses (Адреса): Введите IP-адреса, которым разрешен или запрещен доступ к устройству. Можно также использовать формат CIDR.

Custom-signed firmware certificate (Сертификат для встроенного ПО с пользовательской подписью)

Для установки тестового встроенного ПО или другого пользовательского встроенного ПО от компании Axis на устройстве необходимо использовать сертификат для встроенного ПО с пользовательской подписью. Сертификат проверяет, одобрено ли встроенное ПО как владельцем устройства, так и компанией Axis. Встроенное ПО может работать только на определенном устройстве, которое идентифицируется по его уникальному серийному номеру и идентификатору микросхемы. Сертификаты для встроенного ПО с пользовательской подписью может создавать только компания Axis, поскольку она является владельцем ключа для подписания таких сертификатов.

Нажмите **Install (Установить)**, чтобы установить сертификат. Перед установкой встроенного ПО необходимо установить сертификат.

Пользователи

+ **Add user (Добавить пользователя)**. Нажмите, чтобы добавить нового пользователя. Можно добавить до 100 пользователей.

Username (Имя пользователя). Введите уникальное имя пользователя.

New password (Новый пароль). Введите пароль для пользователя. Длина паролей должна составлять от 1 до 64 символов. В пароле можно использовать только печатные ASCII-символы (с кодами от 32 до 126), например буквы, цифры, знаки пунктуации и некоторые другие символы.

Repeat password (Повторите ввод пароля). Введите тот же самый пароль еще раз.

Role (Роль).

- **Administrator (Администратор)**. Имеет неограниченный доступ ко всем настройкам. Администраторы также могут добавлять, обновлять и удалять других пользователей.
- **Operator (Оператор)**. Эти пользователи обладают правом доступа ко всем настройкам, кроме следующих:
  - Все **System (Системные)** настройки.
  - Добавление приложений.
- **Viewer (Наблюдатель)**. Не может изменять настройки.

Контекстное меню содержит следующие команды:

Update user (Обновить пользователя): Изменение свойств пользователя.

Delete user (Удалить пользователя). Удаление пользователя. Пользователя root удалить нельзя.

MQTT

MQTT (Message Queuing Telemetry Transport) — это стандартный протокол обмена сообщениями для Интернета вещей (IoT). Он был разработан с целью упростить интеграцию IoT и используется в самых разных отраслях для подключения удаленных устройств с небольшим объемом кода и требующих минимальной пропускной способности сети. Клиент MQTT, встроенный в микропрограмму устройства Axis, позволяет упростить интеграцию данных и событий устройства в другие системы, которые не являются системами управления видео (VMS).

Настройте устройство в качестве клиента MQTT. Связь по протоколу MQTT происходит между двумя участниками: клиентом и брокером. Клиенты могут отправлять и принимать сообщения. Брокер отвечает за маршрутизацию сообщений между клиентами.

Более подробно о протоколе MQTT можно узнать на странице *AXIS OS Portal*.

MQTT client (Клиент MQTT)

Connect (Подключение). Позволяет включить или выключить клиент MQTT.

Status (Состояние). Отображает текущее состояние клиента MQTT.

Broker (Брокер)

Host (Хост). Введите имя хоста или IP-адрес сервера MQTT.

Protocol (Протокол). Выберите протокол, который будет использоваться.

Port (Порт). Введите номер порта.

- 1883 — это значение по умолчанию для **MQTT по протоколу TCP**
- 8883 — это значение по умолчанию для **MQTT по протоколу SSL**
- 80 — это значение по умолчанию для **MQTT по протоколу WebSocket**
- 443 — это значение по умолчанию для **MQTT по протоколу WebSocket Secure**

Username (Имя пользователя). Введите имя пользователя, которое клиент будет использовать для доступа к серверу.

Password (Пароль). Введите пароль для имени пользователя.

Client ID (Идентификатор клиента). Введите идентификатор клиента. Идентификатор клиента, передаваемый на сервер, когда клиент подключается к серверу.

Clean session (Очистка сеанса). Определяет поведение во время подключения и отключения. Если этот параметр включен, информация о состоянии при подключении и отключении отклоняется.

Keep alive interval (Интервал поддержания активности соединения). С помощью параметра Keep alive interval (Интервал поддержания активности соединения) клиент может определять, что сервер больше не доступен, не ожидая долго тайм-аута TCP/IP.

Timeout (Тайм-аут). Промежуток времени в секундах, в течение которого должно быть выполнено соединение. Значение по умолчанию: 60

Префикс темы устройства: Используется в значениях по умолчанию для раздела в Connect message (Сообщение о подключении) и LWT message (Сообщение «завещания») на вкладке **клиента MQTT**, а также в условиях публикации на вкладке **публикация MQTT**.

Reconnect automatically (Переподключаться автоматически). Указывает, должен ли клиент автоматически переподключаться при непреднамеренном отключении.

Connect message (Сообщение о подключении)

Указывает, следует ли отправлять сообщение при установлении подключения.

Send message (Отправить сообщение). Включите этот параметр для отправки сообщений.

Use default (Использовать по умолчанию). Выключите этот параметр, если вы хотите ввести собственное сообщение для использования по умолчанию.

Topic (Тема). Введите тему для сообщения по умолчанию.

Payload (Полезные данные). Введите содержание сообщения по умолчанию.

Retain (Сохранять). Выберите, чтобы сохранить состояние клиента для данной темы (**Topic (Тема)**).

QoS. Позволяет изменить уровень QoS для потока пакетов.

Last Will and Testament message (Сообщение последнего распоряжения)

С помощью параметра Last Will Testament (Завещание) клиент при подключении к брокеру может вместе со своими учетными данными предоставить распоряжение («завещание»). Это позволит брокеру отправить сообщение другим клиентам, если впоследствии данный клиент будет некорректно отключен (например, из-за отсутствия питания). Сообщение «завещания» имеет ту же форму, что и обычное сообщение, и отправляется с использованием тех же механизмов.

Send message (Отправить сообщение). Включите этот параметр для отправки сообщений.

Use default (Использовать по умолчанию). Выключите этот параметр, если вы хотите ввести собственное сообщение для использования по умолчанию.

Topic (Тема). Введите тему для сообщения по умолчанию.

Payload (Полезные данные). Введите содержание сообщения по умолчанию.

Retain (Сохранять). Выберите, чтобы сохранить состояние клиента для данной темы (**Topic (Тема)**).

QoS. Позволяет изменить уровень QoS для потока пакетов.

MQTT publication (Публикация MQTT)

Use default condition prefix (Использовать префикс условия по умолчанию). Выберите использование префикса условия по умолчанию, который задается с помощью префикса темы устройства на вкладке **MQTT client (Клиент MQTT)**.

Include condition name (Включить имя условия). Выберите этот параметр, если в тему MQTT нужно включить темы, описывающее условие.

Include condition namespaces (Включить пространства имен условия). Выберите этот параметр, если в тему MQTT нужно включить пространства имен темы ONVIF.

Include serial number (Включить серийный номер): Выберите этот параметр, если в полезные данные MQTT нужно включить серийный номер устройства.

+ **Add condition (Добавить условие)**. Нажмите, чтобы добавить условие.

Retain (Сохранять). Определяет, какие сообщения MQTT отправляются как сохраняемые.

- **None (Нет)**. Отправлять все сообщения как несохраняемые.

- **Property (Свойство)**. Отправлять в качестве сохраняемых только сообщения с сохранением состояния.
- **All (Все)**. Отправлять в качестве сохраняемых сообщения с сохранением и без сохранения состояния.

QoS. Выберите требуемый уровень для публикации MQTT.

MQTT subscriptions (Подписки MQTT)

Add subscription (Добавить подписку). Нажмите, чтобы добавить новую подписку MQTT.

Subscription filter (Фильтр подписок). Введите тему MQTT, на которую вы хотите подписаться.

Use device topic prefix (Использовать префикс темы устройства). Добавьте фильтр подписки в качестве префикса к теме MQTT.

Subscription type (Тип подписки).

- **Stateless (Без сохранения состояния)**. Выберите этот вариант для преобразования сообщений MQTT в сообщения без сохранения состояния.
- **Stateful (С сохранением состояния)**. Выберите этот вариант для преобразования сообщений MQTT в условие. Полезные данные используются в качестве состояния.

QoS. Выберите требуемый уровень для подписки MQTT.

Принадлежности

I/O ports (Порты ввода-вывода)

Используйте цифровой вход для подключения внешних устройств, способных размыкать и замыкать электрическую цепь, таких как пассивные ИК-датчики, дверные или оконные контакты и детекторы разбивания стекла.

Цифровой выход служит для подключения внешних устройств, например таких как реле и светодиодных индикаторов. Подключенные устройства можно активировать с помощью VAPIX® Application Programming Interface или в интерфейсе устройства.

Port (Порт)

Name (Имя): Чтобы переименовать порт, измените текст.

Direction (Направление): указывает, что порт является входным портом. указывает на то, что это порт вывода. Если порт настраиваемый, то нажмите на значки для переключения между входом и выходом.

Нормальное состояние: Нажмите для разомкнутой цепи и для замкнутой цепи.

Текущее состояние: Показывает текущее состояние порта. Вход или выход активен, когда его текущее состояние отличается от нормального. Входная цепь устройства разомкнута, когда вход не подсоединен или при наличии напряжения выше 1 В пост. тока.

Примечание.

Во время перезапуска выходная цепь разомкнута. После завершения перезапуска цепь возвращается в обычное положение. При изменении каких-либо параметров на этой странице выходные цепи вернутся в обычное положение, даже если в этот момент будут активны какие-либо триггеры.

Контролируемый : Включите этот параметр для обнаружения и запуска действий при несанкционированных действиях с подключением к цифровым устройствам ввода-вывода. Помимо обнаружения разомкнутых или замкнутых входных цепей, можно также обнаруживать несанкционированные действия с ними (например, при обрыве или замыкании). Реализация этой функции требует дополнительного оборудования (резисторы на концах линии) во внешней петле ввода-вывода.

Журналы

Отчеты и журналы

Reports (Отчеты)

- **View the device server report (Просмотр отчета сервера устройства)**. Нажмите, чтобы просмотреть информацию о состоянии устройства (во всплывающем окне). В отчет сервера автоматически добавляется журнал доступа.
- **Download the device server report (Загрузить отчет сервера устройства)**. Нажмите, чтобы скачать отчет сервера. При скачивании отчета сервера создается файл ZIP, который содержит полный отчет сервера в виде текстового файла в формате UTF–8, а также моментальный снимок текущего изображения живого просмотра. При обращении в службу поддержки всегда прикладывайте файл ZIP с отчетом сервера.
- **Download the crash report (Загрузить отчет о сбоях в работе сервера)**. Нажмите, чтобы скачать архив с подробной информацией о состоянии сервера. Отчет об отказах системы содержит сведения, включенные в отчет сервера, а также подробную информацию для отладки. Этот отчет может содержать конфиденциальную информацию, например трассировку сети. Для формирования отчета может потребоваться несколько минут.

Logs (Журналы)

- **View the system log (Просмотр журнала системных событий)**. Нажмите, чтобы показать информацию о системных событиях, таких как запуск устройства, предупреждения и важные сообщения.
- **View the access log (Просмотр журнала запросов на получение доступа)**. Нажмите, чтобы отобразить все неудачные попытки доступа к устройству, например при использовании неверного пароля для входа в систему.

Network trace (Трассировка сети)

Важно!

Файл трассировки сети может содержать конфиденциальную информацию, например сертификаты или пароли.

В файле трассировки сети регистрируются совершаемые в сети операции, что может помочь в поиске и устранении неполадок. Выберите продолжительность трассировки в секундах или минутах и нажмите **Download (Скачать)**.

Remote system log (Удаленный системный журнал)

Системный журнал (syslog) — это стандартный способ регистрации сообщений. С его помощью можно разделить программное обеспечение, которое генерирует сообщения, систему, в которой они хранятся, и программное обеспечение, которое сообщает о них и анализирует их. Каждое сообщение помечается кодом объекта, обозначающим тип программного обеспечения, создавшего сообщение. Также сообщению назначается уровень серьезности.

+ **Server (Сервер)**. Нажмите, чтобы добавить новый сервер.

Host (Хост). Введите имя хоста или IP-адрес сервера.

Format (Форматировать): Выберите формат сообщений в системном журнале.

- RFC 3164
- RFC 5424

Protocol (Протокол). Выберите протокол и порт для использования:

- UDP (по умолчанию используется порт 514)
- TCP (по умолчанию используется порт 601)
- TLS (по умолчанию используется порт 6514)

Severity (Степень серьезности). Выберите, какие сообщения будут отправляться при срабатывании триггера.

CA certificate set (Набор сертификатов ЦС). Просмотр текущих настроек или добавление сертификата.

Обслуживание

Restart (Перезапуск). Перезапуск устройства. Это не повлияет на какие-либо текущие параметры. Работающие приложения перезапустятся автоматически.

Restore (Восстановить). Возврат *большинства* настроек к заводским установкам. После этого необходимо перенастроить устройство и приложения, переустановить все приложения, которые не были предустановлены, и воссоздать любые события и предустановленные положения PTZ.

Важно!

Единственными настройками, которые сохраняются после восстановления, являются следующие:

- Boot protocol (DHCP or static) (Протокол загрузки (DHCP или статический))
- Static IP address (Статический IP-адрес)
- Default router (Маршрутизатор по умолчанию)
- Subnet mask (Маска подсети)
- Параметры 802.1X
- Параметры O3C

Factory default (Заводские установки). Возврат *всех* настроек к заводским установкам. После этого необходимо сбросить IP-адрес, чтобы обеспечить возможность доступа к устройству.

Примечание.

Чтобы гарантировать то, что на вашем устройстве выполняется установка только проверенного встроенного ПО, все встроенное ПО для устройств Axis сопровождается цифровой подписью. Это еще больше повышает общий минимальный уровень кибербезопасности устройств Axis. Для получения дополнительной информации см. технический документ «Встроенное ПО с цифровой подписью, режим безопасной загрузки и защита закрытых ключей» на веб-сайте *axis.com*.

Firmware upgrade (Обновление встроенного ПО). Обновление до новой версии встроенного ПО. Новые выпуски встроенного ПО могут содержать улучшенную функциональность, исправление ошибок или совершенно новые функции. Рекомендуется всегда использовать самую последнюю версию. Чтобы скачать последнюю версию, перейдите на страницу *axis.com/support*.

В ходе обновления можно выбрать один из трех вариантов:

- **Standard upgrade (Стандартное обновление)**. Обновление до новой версии встроенного ПО.
- **Factory default (Заводские установки)**. Обновление и возврат всех настроек к заводским установкам по умолчанию. При выборе этого варианта после выполнения обновления вернуться к предыдущей версии встроенного ПО будет нельзя.
- **Autorollback (Автооткат)**. Обновление и подтверждение обновления в течение указанного срока. Если не выполнить подтверждение, устройство вернется к предыдущей версии встроенного ПО.

Firmware rollback (Откат встроенного ПО). Выполнение отката к установленной ранее версии встроенного ПО.

Руководство пользователя
AXIS A1601 Network Door Controller

Версия M10.2
Дата: Май 2022
Артикул T10125657