AXIS A1001 & AXIS Entry Manager

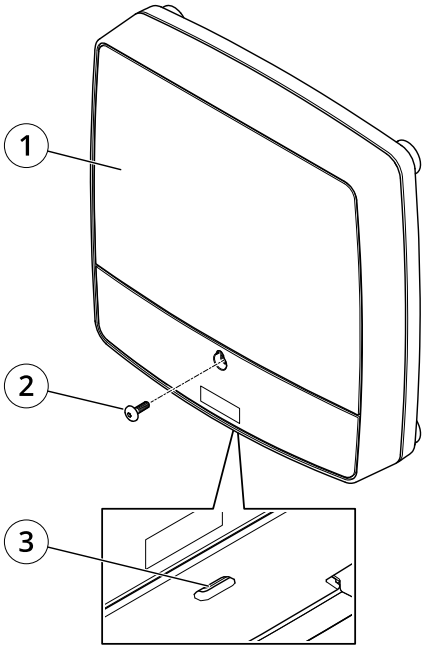
Руководство пользователя

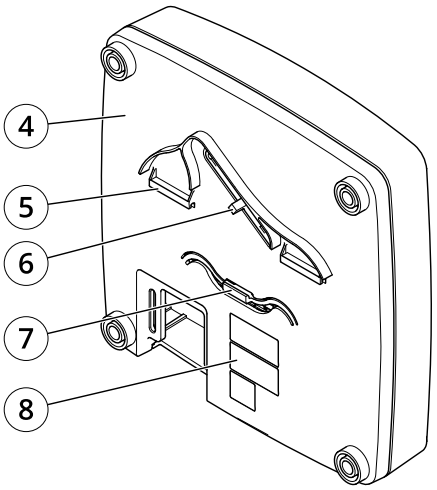
Содержание

Содержание

Общий вид устройства

Общий вид устройства

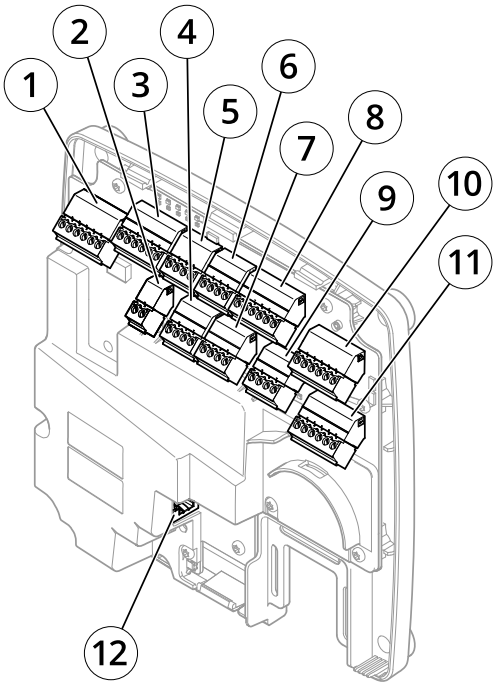




Оборудование, расположенное на передней и задней сторонах устройства:

1 *Крышка*
2 *Винт крышки*
3 *Прорезь для снятия крышки*
4 *Основание*
5 *DIN-скоба верхняя*
6 *Переключатель сигнала тревоги при несанкционированных действиях, расположенный на задней стороне устройства*
7 *DIN-скоба нижняя*
8 *Идентификационный номер (C/H) и серийный номер (C/H)*

Общий вид устройства



Интерфейс ввода-вывода:

1 Разъем данных считывателя (READER DATA 1)
10 Разъем данных считывателя (READER DATA 2)
3 Разъем ввода-вывода считывателя (READER I/O 1)
8 Разъем ввода-вывода считывателя (READER I/O 2)
4 Дверной разъем (DOOR IN 1)
7 Дверной разъем (DOOR IN 2)
6 Вспомогательный разъем (AUX)
5 Аудиоразъем (AUDIO) (не используется)

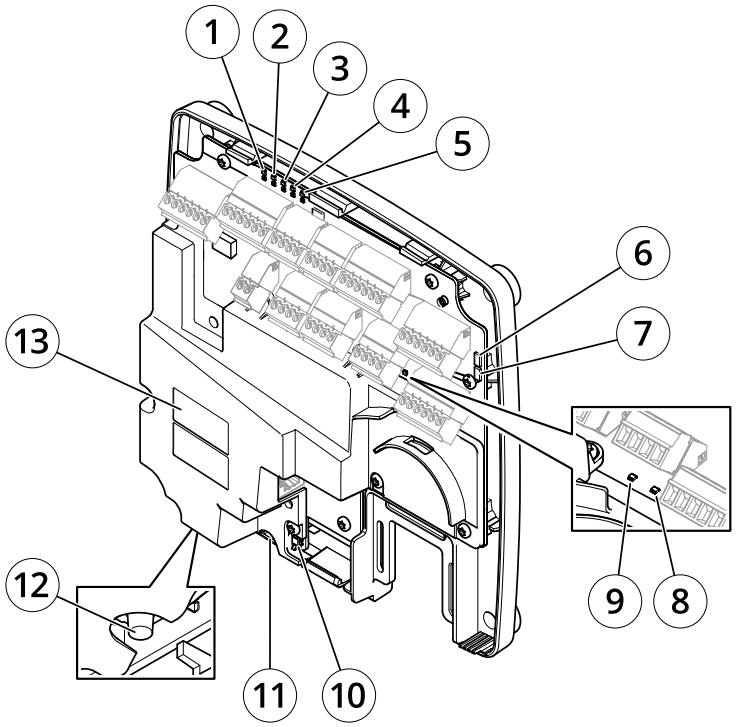
Внешние входы питания:

2 Разъем питания (DC IN)
12 Сетевой разъем (PoE)

Выходы питания:

9 Разъем питания замка (LOCK)
11 Разъем питания и реле (PWR, RELAY)

Общий вид устройства



Индикаторы, кнопки и прочее оборудование:

1 *Индикатор питания*
2 *Индикатор состояния*
3 *Индикатор сети*
4 *Индикатор считывателя Reader 2 (не используется)*
5 *Индикатор считывателя Reader 1 (не используется)*
6 *Контактная головка на передней стороне, служащая для оповещения при несанкционированных действиях (TF)*
7 *Контактная головка на задней стороне, служащая для оповещения при несанкционированных действиях (TB)*
8 *Индикатор замка*
9 *Индикатор замка*
10 *Датчик сигнала тревоги на передней стороне устройства для оповещения о несанкционированных действиях*
11 *Слот для карт SD (microSDHC) (не используется)*
12 *Кнопка управления*
13 *Идентификационный номер (P/N) и серийный номер (C/H)*

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.

Общий вид устройства

Питание	Зеленый	Нормальный режим работы.
	Желтый	Мигает зеленым и желтым во время обновления встроенного ПО.
Замок	Зеленый	Горит непрерывно, если нет подачи питания.
	Красный	Горит непрерывно при подключении к источнику питания.
	Не горит	Не подключен.

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)**.

Электрические соединители и кнопки

Интерфейс ввода-вывода

Разъемы данных считывателя
Две 6-контактные клеммные колодки с поддержкой стандарта RS485 и протоколов Wiegand для связи со считывателем. Для ознакомления с техническими характеристиками см. раздел *стр. 73*.

Разъемы ввода-вывода считывателя
Две 6-контактные клеммные колодки для входа и выхода считывателя. Помимо точки заземления 0 В пост. тока и питания (выход пост. тока), в разъем ввода-вывода считывателя включены следующие интерфейсы:

- Цифровой вход — например, для подключения сигналов тревоги в случае несанкционированных действий применительно к считывателю.
- Цифровой выход — например, для подключения устройства звуковой сигнализации и индикаторов считывателя.

Для ознакомления с техническими характеристиками см. раздел *стр. 73*.

Дверные разъемы
Две 4-контактные клеммные колодки для подключения устройств дверного мониторинга и устройств, обрабатывающих запросы на выход (REX-устройств). Для ознакомления с техническими характеристиками см. раздел *стр. 74*.

Дополнительный разъем
4-контактная настраиваемая клеммная колодка ввода-вывода. Используется для подключения внешних устройств, например для оповещения при несанкционированных действиях, активации определенных событий и уведомления о состоянии тревоги. Помимо точки заземления 0 В пост. тока и питания (выход пост. тока), вспомогательный разъем служит интерфейсом, который обеспечивает:

- Цифровой вход — вход сигнала тревоги для подключения устройств, которые способны размыкать и замыкать цепь, например пассивные ИК-датчики или детекторы разбивания стекла.
- Цифровой выход — для подключения внешних устройств, например сигнализации на случай взлома, сирен или световой сигнализации. Подключенные устройства можно активировать с помощью прикладного программного интерфейса VAPIX® или с помощью правила действия.

Для ознакомления с техническими характеристиками см. раздел *стр. 75*.

Внешние входы питания

ПРИМЕЧАНИЕ.

Устройство должно подключаться к сети с помощью экранированного сетевого кабеля (STP). Все кабели, с помощью которых устройство подключается к сети, должны быть предназначенными для данного варианта применения. Убедитесь, что сетевые устройства установлены согласно инструкциям производителя. Сведения о нормативных требованиях см. в разделе .

Общий вид устройства

Разъем питания
2-контактная клеммная колодка для подвода 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. Для ознакомления с техническими характеристиками см. раздел *стр. 76*.

Сетевой разъем
Разъем Ethernet RJ45. Поддерживает технологию Power over Ethernet (PoE). Для ознакомления с техническими характеристиками см. *стр. 76*.

Выходы питания

Разъем питания замка

4-контактная клеммная колодка для подключения одного или двух замков. Разъем замка также может использоваться для питания внешних устройств. Для ознакомления с техническими характеристиками см. раздел *стр. 76*.

Разъем питания и реле

6-контактная клеммная колодка для подключения питания и реле дверного контроллера к внешним устройствам, например, к замкам и датчикам. Для ознакомления с техническими характеристиками см. раздел *стр. 77*.

Кнопки и другое оборудование

Контактная головка, служащая для оповещения при несанкционированных действиях
Две 2-контактные головки для отключения сигналов тревоги при несанкционированных действиях, расположенные на передней и задней сторонах устройства. Для ознакомления с техническими характеристиками см. раздел *стр. 77*.

Кнопка управления
Кнопка управления служит для выполнения следующих действий.

- Сброс параметров изделия к заводским установкам. См. *стр. 69*.
- Подключение к службе видеохостинга AXIS Video Hosting System (AVHS). См. *стр. 62*. Для подключения нажмите и удерживайте кнопку примерно 1 секунду, пока индикатор состояния не начнет мигать зеленым цветом.
- Подключение к сервису AXIS Internet Dynamic DNS. См. *стр. 63*. Для подключения нажмите и удерживайте кнопку примерно 3 секунды.

Установка

Установка

Для просмотра видео откройте веб-версию данного документа.

www.axis.com/products/online-manual/19467#t10170589_ru

Видео с инструкциями по установке этого продукта.

Получение доступа к устройству

Сведения об установке устройства Axis см. в прилагаемом к нему руководстве по установке.

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 приложение AXIS Entry Manager. При использовании компьютера откроется страница Overview (Обзор). При использовании мобильного устройства откроется начальная страница для мобильного устройства.

О начальной странице для мобильных устройств

На начальной странице для мобильных устройств отображается состояние дверей и замков, подключенных к дверному контроллеру. Можно протестировать блокировку и разблокировку замков. Чтобы увидеть результат тестирования, нужно обновить страницу.

Для перехода в Axis Entry Manager воспользуйтесь ссылкой.

Примечание.

- Axis Entry Manager не поддерживается для мобильных устройств.
- Если вы продолжите работу в Axis Entry Manager, то не сможете вернуться на начальную страницу для мобильных устройств по причине отсутствия соответствующей ссылки.

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.

См. также сведения о службе AXIS Internet Dynamic DNS на веб-сайте *www.axiscam.net*.

Получение доступа к устройству

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®.

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. 58*.

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. 69*.

Чтобы задать пароль, введите его непосредственно в диалоговом окне.

Страница Overview (Обзор)

На странице Overview (Обзор) в AXIS Entry Manager для дверного контроллера указано его название, MAC-адрес, IP-адрес и версия встроенного ПО. Кроме того, с помощью этой страницы можно идентифицировать дверной контроллер в сети или в системе.

При первой попытке доступа к устройству Axis на странице Overview (Обзор) появится предложение настроить оборудование, установить дату и время, задать настройки сети и указать, является ли дверной контроллер частью системы или автономным устройством. Дополнительные сведения о настройке системы см. в разделе *Пошаговая настройка на стр. 12*.

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 разделах *стр. 34*, *стр. 44* и *стр. 58*.

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 в AXIS Entry Manager использовался другой язык. См. *Выбор языка на стр. 12*.
2. Установка даты и времени. См. *стр. 13*.
3. Настройка сетевых параметров. См. *стр. 14*.
4. Настройка дверного контроллера и подключенных устройств, среди которых считыватели, замки и устройства, обрабатывающие запросы на выход (REX-устройства). См. *Настройка оборудования на стр. 14*.
5. Проверка подключения оборудования. См. *стр. 22*.
6. Настройка карт и форматов. См. *стр. 23*.
7. Настройка системы дверных контроллеров. См. *Управление дверными сетевыми контроллерами на стр. 29*.

Сведения о настройке и управлении дверями, расписаниями, пользователями и группами в системе см. в разделе *Управление доступом на стр. 34*.

Рекомендации по обслуживанию см. в разделе *Инструкции по обслуживанию на стр. 33*.

Примечание.

Чтобы добавить или удалить дверные контроллеры, добавить, удалить или изменить пользователей или настроить оборудование, более половины дверных контроллеров в системе должны быть в состоянии **онлайн**. Для проверки состояния дверного контроллера выберите в меню **Setup > Manage Network Door Controllers in System (Настройка > Управление дверными сетевыми контроллерами в системе)**.

Выбор языка

По умолчанию в AXIS Entry Manager 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 в приложении AXIS Entry Manager вновь устанавливается английский язык.
- При восстановлении устройства в приложении AXIS Entry Manager будет по-прежнему использоваться выбранный язык.
- При перезапуске устройства в приложении AXIS Entry Manager будет по-прежнему использоваться выбранный язык.
- При обновлении встроенного ПО AXIS Entry Manager продолжит использовать выбранный язык.

Установка даты и времени

Если дверной контроллер является частью системы, настройки даты и времени будут общими для всех дверных контроллеров. Это означает, что параметры передаются другим контроллерам в системе, независимо от того, осуществляется ли синхронизация с NTP-сервером, устанавливаются ли дата и время вручную или сведения о дате и времени получаются от компьютера. Если изменения не отображаются, попробуйте обновить страницу в браузере. Дополнительные сведения об управлении системой дверных контроллеров см. в разделе *Управление дверными сетевыми контроллерами на стр. 29*.

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. 13*.
- Установка даты и времени вручную. См. *стр. 13*.
- Получение даты и времени от компьютера. См. *стр. 14*.

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. 63*.

Если для NTP-сервера используется имя хоста, то необходимо настроить DNS-сервер. См. *Настройка DNS на стр. 63*.

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. 61*

Настройка оборудования

Управление дверями и доступом на этажи возможно только после настройки оборудования на страницах Hardware Configuration (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. 33*.

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

- Импорт файла конфигурации оборудования. См. *стр. 14*.
- Создание новой конфигурации оборудования. См. *стр. 15*.

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. 15*.

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. 15*
- *Как создать новую конфигурацию оборудования для беспроводных замков на стр. 19*
- *Как создать новую конфигурацию оборудования с функцией управления лифтами (AXIS A9188) на стр. 20*

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. 16*.

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. 18*.

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. 19*.

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.
- Замки с электроприводом должны настраиваться как вспомогательные.

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.

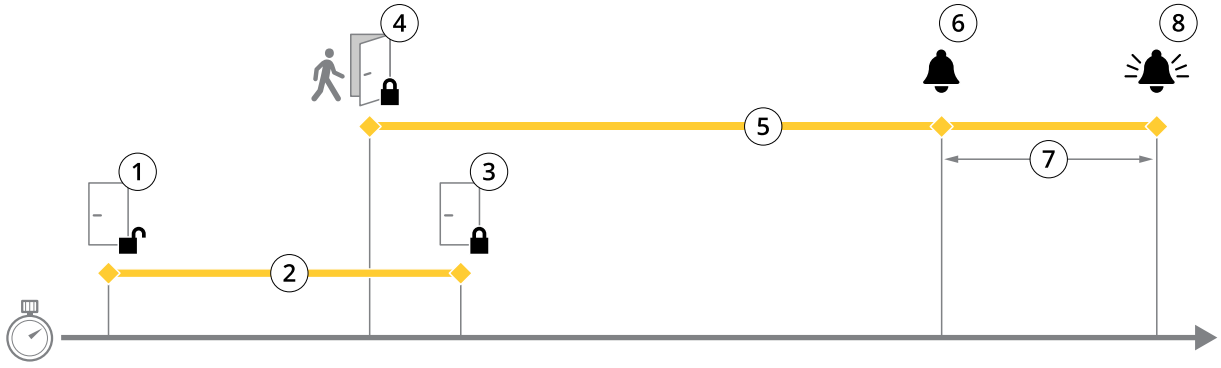
- **Cancel access time once door is opened (Отменить время доступа после того, как дверь открыта)** — выберите этот параметр, чтобы предотвратить несанкционированный проход нескольких лиц. Как только дверной монитор укажет, что дверь была открыта, замок будет заблокирован.

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, см. *Учетные данные пользователя на стр. 44*

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.



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. 50*.

О вариантах блокировки

Для цепи блокировки доступны следующие параметры:

- **12 В**
  - **Fail-secure (Защита от перебоев питания)** — выберите этот вариант для замков, которые остаются заблокированными при отключении питания. При подаче электрического тока замок разблокируется.
  - **Fail-safe (Безопасность)** — выберите для замков, которые разблокируются при отключении питания. При подаче электрического тока замок заблокируется.
- 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.
  - **Relay open = Locked (Размыкание реле = заблокировано)** — выберите для замков, которые остаются заблокированными при размыкании реле (защита от перебоев питания). При замыкании реле замок разблокируется.
  - **Relay open = Unlocked (Разомкнутое реле = разблокировано)** — выберите для замков, которые разблокируются при отключении питания (безопасность). При замыкании реле замок заблокируется.
- **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 считывателями, REX-устройствами 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. 78*.
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

Следующие разъемы поддерживают контролируемые входы:

- Разъем ввода-вывода считывателя — сигнал несанкционированных действий. См. *стр. 73*.
- Разъем дверного датчика. См. *стр. 74*.

Считыватели и переключатели, которые могут использоваться с контролируемыми входами, включают:

- HID-считыватели с внутренним сопротивлением 1 кОм и повышением напряжения до 5 В.
- Считыватели и переключатели с внутренним сопротивлением 1 кОм и повышением напряжения до 5 В.
- Считыватели и переключатели без внутреннего повышения напряжения.

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. 20*).

   - **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. 29*).

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 сетевого дверного контроллера Axis Network Door Controller можно настроить не более двух модулей AXIS 9188 Network I/O Relay Module.

1. В контроллере A1001 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. 21*) 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)**.

Теперь этаж будет отображаться на вкладке **Floor (Пол)** ниже элемента **Access Management (Управление доступом)**.

Примечание.

В AXIS Entry Manager можно добавить не более 16 этажей.

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. 56*. 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. 56*. 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. 24*.
4. Щелкните **Add field map (Добавить расположение полей)** и введите в поля необходимые данные. См. *Схемы расположения полей на стр. 24*.
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!

- Любые изменения, внесенные в форматы карт, относятся ко всей системе дверных контроллеров.
- Вы можете активировать и деактивировать форматы карт только в том случае, если хотя бы для одного дверного контроллера в системе уже был настроен считыватель. См. *Настройка оборудования на стр. 14* и *Как настроить считыватели и REX-устройства на стр. 18*.
- 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.

Предустановленный код объекта

Для проверки соответствия устройства идентификации системе контроля доступа на данном объекте иногда используются коды объектов. Часто бывает так, что устройства идентификации, выпущенные для одного объекта, имеют одинаковый код объекта. Введите предустановленный код объекта, чтобы упростить регистрацию пакета карт в ручном режиме. При добавлении пользователей предустановленный код объекта вставляется автоматически, см. *Учетные данные пользователя на стр. 44*

Чтобы задать предустановленный код объекта:

1. Выберите в меню **Setup > Configure cards and formats (Настройка > Настройка карт и форматов)**.
2. В разделе **Preset facility code (Предустановленный код объекта)** введите код объекта.
3. Нажмите кнопку **Set facility code (Задать код объекта)**.

Настройка служб

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

HID Mobile Access

Приложение HID Mobile Access расширяет возможности контроля доступа благодаря использованию мобильного устройства в качестве учетных данных.

Необходимые условия для HID Mobile Access

Прежде чем приступать к настройке HID Mobile Access для дверного контроллера, необходимо выполнить перечисленные ниже требования:

- Должна быть создана учетная запись HID. Для настройки учетной записи обратитесь к местному партнеру HID.
- Выделите номер (для своих учетных данных для мобильного доступа), связанный с вашей учетной записью HID.
- Устройство должно иметь доступ к облачным серверам HID Mobile Access посредством исходящей HTTPS-связи. Соответствующим образом обновите свою ИТ-инфраструктуру. В результате это должно обеспечить подключение к DNS-серверу.

Настройка мобильного доступа HID

1. Выберите **Setup (Настройка)** в верхнем меню.
2. Затем выберите **Configure Services (Настройка служб)** > **Settings (Параметры)**.
3. Введите свой идентификатор клиента и пароль для HID.
4. При необходимости укажите параметры прокси-сервера и выберите в меню **Connect (Подключить)**.
5. Выберите **Set as current (Установить как текущий номер)**, чтобы указать выделенный номер, который вы хотите использовать для данной установки.
6. Способы добавить мобильный доступ HID Mobile Access для пользователей:
   - Создание и изменение пользователей вручную (см. раздел *Создание и изменение пользователей на стр. 44* на странице *стр. 44*).
   - Импортирование пользователей (см. раздел *Импортирование пользователей на стр. 45* на странице *стр. 45*).

Примечание.

Каждый пользователь, которому предоставляется доступ к HID Mobile Access, получает по электронной почте ссылку на приложение, чтобы продолжить установку на своем устройстве.

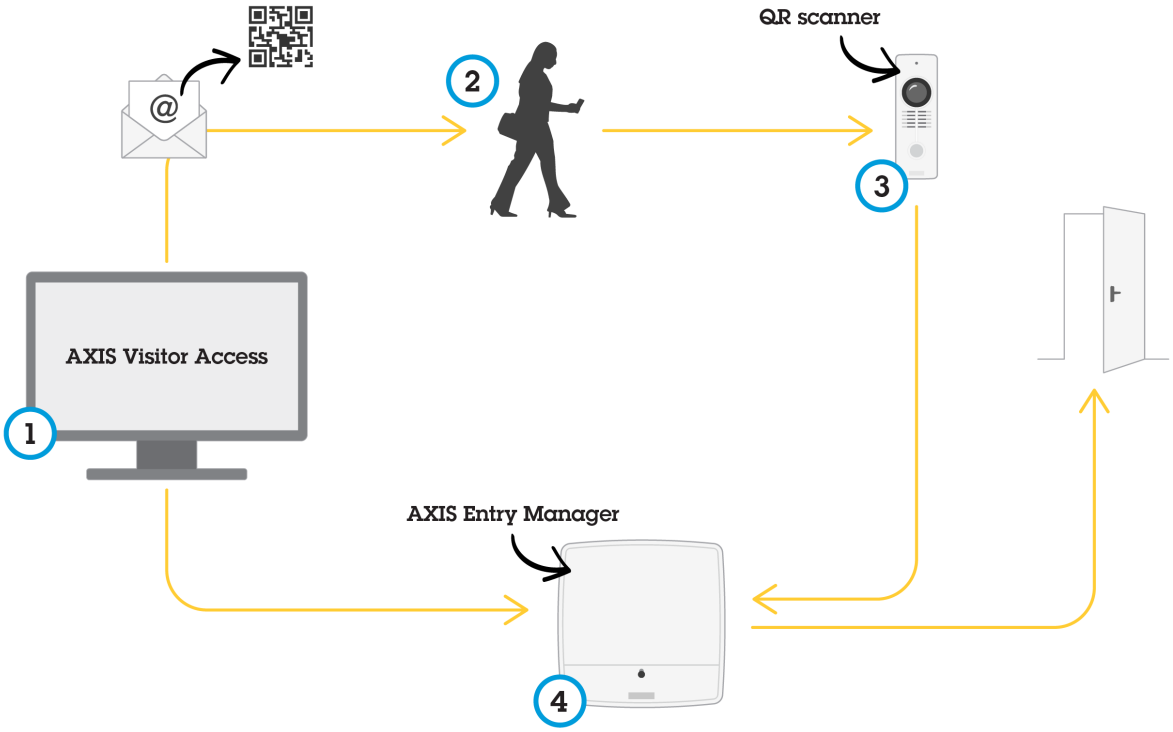
AXIS Visitor Access

Приложение AXIS Visitor Access позволяет создавать временные учетные данные в виде QR-кода. Сетевая камера Axis или домофон, подключенные к системе контроля доступа, проверяют QR-код.

В состав службы входят:

- дверной контроллер Axis с установленным приложением AXIS Entry Manager и встроенным ПО версии 1.65.2 или выше;
- сетевая камера или домофон Axis с установленным приложением сканера QR-кодов;
- ПК с ОС Windows®, на котором установлено приложение AXIS Visitor Access.

Конфигурация системы



Использование службы AXIS Visitor Access

Пользователь создает приглашение в приложении AXIS Visitor Access (1) и отправляет приглашение на адрес электронной почты посетителя. Одновременно создаются учетные данные для разблокировки двери, которые хранятся в подключенном дверном контроллере Axis (4). Посетитель предъявляет приложенный к приглашению QR-код сетевой камере или домофону (3), и на дверной контроллер (4) поступает сигнал для разблокировки двери для данного посетителя.

QR Code — это зарегистрированный товарный знак компании Denso Wave, inc..

Предварительные требования для использования AXIS Visitor Access

Прежде чем использовать службу AXIS Visitor Access, необходимо:

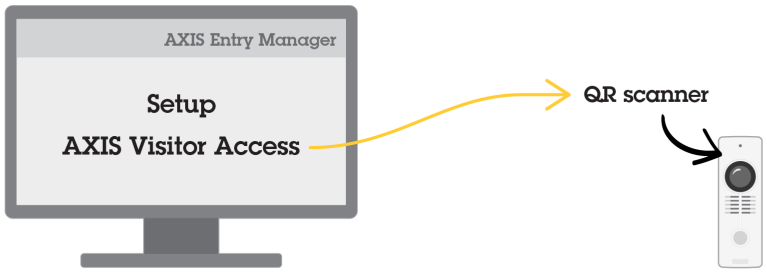
- настроить оборудование дверного контроллера;
- подключить сетевую камеру или домофон Axis к той же сети, в которой находится дверной контроллер, и разместить в доступном для посетителя месте возле двери;
- иметь в наличии установочный пакет AXIS Visitor Access (его можно найти на сайте *axis.com*);
- наличие двух дополнительных учетных записей пользователей в дверном контроллере, которые будут использоваться только службой AXIS Visitor Access. Одна из них требуется для приложения AXIS Visitor Access, а вторая — для приложения сканера QR-кодов. О том, как создавать учетные записи пользователей, см. в разделе *Пользователи на стр. 58*.

Конфигурация системы

Важно!

- Службу AXIS Visitor Access можно подключить только к одному дверному контроллеру во всей системе.
- Службу AXIS Visitor Access можно использовать только для тех дверей, которыми управляет подключенный дверной контроллер. Для других дверей в системе ее использовать невозможно.
- Для изменения и удаления посетителей используйте приложение AXIS Visitor Access. Не используйте AXIS Entry Manager.
- Если вы изменяете пароль для учетной записи пользователя, которая используется для AXIS Visitor Access, его также необходимо обновить в приложении AXIS Visitor Access.
- Если вы изменяете пароль учетной записи пользователя, которая используется для приложения сканера QR-кодов, необходимо заново настроить сканер QR-кодов.

Настройка AXIS Visitor Access



Приложение сканера QR-кодов устанавливается на сетевую камеру или домофон Axis при настройке службы AXIS Visitor Access. Никакой отдельной установки выполнять не требуется.

1. На веб-странице дверного контроллера выберите **Setup > Configure Services > Settings (Настройка > Настройка служб > Настройки)**.
2. Нажмите кнопку **Start a new setup (Начать новую настройку)**.
3. Следуйте инструкциям на экране для завершения установки.

Важно!

Если вы хотите применить HTTPS, убедитесь в том, что дверной контроллер обменивается данными по протоколу HTTPS. В противном случае, приложение не сможет взаимодействовать с дверным контроллером.

4. На компьютере, который будет использоваться для создания временных учетных данных, установите и настройте приложение AXIS VisitorAccess.

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. 19*.

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.

Управление дверными сетевыми контроллерами

В разделе Manage Network Door Controllers (Управление дверными сетевыми контроллерами) на странице System (Система) представлена информация о дверном контроллере, его системном статусе, а также о других дверных контроллерах, которые являются компонентами системы. Кроме того, указанный раздел позволяет администратору изменить настройку системы путем добавления или удаления дверных контроллеров.

Важно!

Все дверные контроллеры в системе должны быть подключены к одной и той же сети и настроены для использования на одном объекте.

Для управления дверными контроллерами выберите в меню **Setup > Manage Network Door Controllers in System (Настройка > Управление дверными сетевыми контроллерами в системе)**.

Страница Manage Network Door Controllers in System (Управление дверными сетевыми контроллерами в системе) содержит следующие панели:

- **System status of this controller (Состояние данного контроллера в системе)** – отображение системного статуса данного дверного контроллера и переключение между режимом работы в составе системы и автономным режимом. Дополнительные сведения см. в разделе *Состояние системы дверного контроллера на стр. 30*.
- Панель **Network door controllers in system (Дверные сетевые контроллеры в системе)** – отображение сведений о дверных контроллерах в системе, а также возможность добавления и удаления контроллера из системы. Дополнительные сведения см. в разделе *Подключенные к системе дверные контроллеры на стр. 30*.

Состояние системы дверного контроллера

Состояние системы определяет, может ли дверной контроллер быть частью системы дверных контроллеров. Состояние системы дверного контроллера отображается на панели **System status for this controller (Состояние системы для этого контроллера)**.

Если дверной контроллер не находится в автономном режиме и вы хотите защитить его от добавления в систему, нажмите кнопку **Activate standalone mode (Активировать автономный режим)**, чтобы запустить автономный режим.

Если дверной контроллер находится в автономном режиме, но вы хотите добавить его в систему, нажмите кнопку **Deactivate standalone mode (Отключить автономный режим)**, чтобы выйти из автономного режима.

Режимы системы

- **This controller is not part of a system and not in standalone mode (Данный контроллер не является частью системы и не находится в автономном режиме)** – дверной контроллер не включен ни в одну систему и не находится в автономном режиме. Это означает, что дверной контроллер доступен и может быть добавлен в систему любым другим дверным контроллером в той же сети. Чтобы защитить дверной контроллер от добавления в систему, активируйте автономный режим.
- **This controller is set to standalone mode (Контроллер работает в автономном режиме)** – дверной контроллер не входит ни в одну систему. Другие контроллеры в сети не могут добавить его в систему, и он не может добавлять другие дверные контроллеры. Автономный режим, как правило, используется в небольших помещениях с одним дверным контроллером и одной или двумя дверями. Чтобы разрешить добавление дверного контроллера в систему, отключите автономный режим.
- **This controller is part of a system (Контроллер входит в систему)** – дверной контроллер является частью распределенной системы. В распределенной системе пользователи, группы, двери и расписания являются общими для всех подключенных контроллеров.

Подключенные к системе дверные контроллеры

Панель **Network door controllers in system (Дверные сетевые контроллеры в системе)** позволяет контролировать следующие изменения, вносимые в систему:

- Добавление дверных контроллеров в систему, см. раздел *Добавление дверных контроллеров в систему на стр. 31*.
- Удаление дверных контроллеров из системы, см. раздел *Удаление дверных контроллеров из системы на стр. 32*.

Список подключенных дверных контроллеров

Панель **Network door controllers in system (Дверные сетевые контроллеры в системе)** также содержит список, в котором представлены следующие идентификаторы и сведения о статусе подключенных дверных контроллеров в системе:

- **Name (Имя)** – заданное пользователем имя дверного контроллера. Если администратор не задал имени при настройке оборудования, то будет отображаться имя по умолчанию.
- **IP address (IP-адрес)**
- **MAC address (MAC-адрес)**
- **Status (Статус)** – дверной контроллер, откуда вы осуществляете доступ к системе, будет иметь статус **This controller (Этот контроллер)**. Остальные дверные контроллеры в системе будут иметь статус **Online (Онлайн)**.
- **Firmware version (Версия встроенного ПО)**

Чтобы открыть веб-страницы другого дверного контроллера, щелкните его IP-адрес.

Для обновления списка нажмите кнопку **Refresh the list of controllers (Обновить список контроллеров)**.

Примечание.

Все контроллеры в системе всегда должны иметь одну и ту же версию встроенного ПО. Чтобы одновременно обновить встроенное ПО для всех контроллеров в целой системе, используйте приложение Axis Device Manager.

Добавление дверных контроллеров в систему

Важно!

При подключении дверных контроллеров будут удалены все настройки управления доступом для контроллера добавленной двери и вместо них будут заданы системные параметры управления доступом.

Чтобы добавить в систему дверной контроллер из списка дверных контроллеров, выполните следующие действия:

1. Выберите в меню **Setup > Manage Network Door Controllers in System (Настройка > Управление дверными сетевыми контроллерами в системе)**.
2. Нажмите кнопку **Add controllers to system from list (Добавить контроллеры в систему из списка)**.
3. Выберите дверной контроллер, который вы хотите добавить.
4. Нажмите кнопку **Add (Добавить)**.
5. Если нужно еще добавить контроллеры в систему, повторите описанные выше шаги.

Чтобы добавить в систему дверной контроллер, зная его IP-адрес или MAC-адрес, выполните следующие действия:

1. Перейдите в раздел **Manage Devices (Управление устройствами)**.
2. Нажмите кнопку **Add controller to system by IP or MAC address (Добавить контроллер в систему по его IP или MAC-адресу**.
3. Введите IP-адрес или MAC-адрес.
4. Нажмите кнопку **Add (Добавить)**.
5. Если нужно еще добавить контроллеры в систему, повторите описанные выше шаги.

По завершении подключения все дверные контроллеры в системе имеют полную информацию о пользователях, дверях, расписаниях и группах.

Для обновления списка нажмите кнопку **Refresh list of controllers (Обновить список контроллеров)**.

Удаление дверных контроллеров из системы

Важно!

- Перед удалением дверного контроллера из системы сбросьте настройку оборудования. Если пропустите этот шаг, все двери, связанные с удаленным дверным контроллером, останутся в системе, и удалить их будет невозможно.
- При удалении дверного контроллера из системы с двумя контроллерами оба дверных контроллера автоматически переключаются в автономный режим.

Чтобы удалить дверной контроллер из системы:

1. Получите доступ к системе через дверной контроллер, который вы хотите удалить, и перейдите в меню **Setup > Hardware Configuration (Настройка > Настройка оборудования)**.
2. Нажмите кнопку **Сброс настройки оборудования**.
3. После сброса настройки оборудования выберите в меню **Setup > Manage Network Door Controllers in System (Настройка > Управление дверными сетевыми контроллерами в системе)**.
4. В списке **Network door controllers in system (Дверные сетевые контроллеры в системе)** найдите дверной контроллер, который вы хотите удалить, и нажмите кнопку **Remove from system (Удалить из системы)**.
5. Откроется диалоговое окно с напоминанием о сбросе настроек оборудования для дверного контроллера. Нажмите кнопку **Remove controller (Удалить контроллер)** для подтверждения.
6. Откроется диалоговое окно с просьбой подтвердить удаление дверного контроллера. Нажмите кнопку **OK** для подтверждения. Удаленный дверной контроллер переключится в автономный режим.

Примечание.

- При удалении из системы дверного контроллера удаляются все его настройки управления доступом.
- Удалить можно только дверные контроллеры, которые находятся в сети.

Режим настройки

Режим настройки — это стандартный режим при первом обращении к устройству. При отключении режима настройки большинство функций настройки для данного устройства будут скрыты.

Важно!

Не следует рассматривать отключение режима настройки в качестве меры обеспечения безопасности. Этот режим предназначен для исправления ошибок при настройке, а не для того, чтобы злоумышленники не могли изменить важнейшие параметры.

Как отключить режим настройки

1. Выберите **Setup (Настройка)** > **Disable Configuration Mode (Отключить режим настройки)**.
2. Введите ПИН-код и нажмите **OK**.

Примечание.

PIN-код не является обязательным параметром.

Как включить режим настройки

1. Выберите **Setup (Настройка)** > **Enable Configuration Mode (Включить режим настройки)**.
2. Введите ПИН-код и нажмите **OK**.

Примечание.

Если вы не помните свой PIN-код, то можно включить режим настройки, введя `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

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. 22*.
- 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. 22*.

- Убедитесь в актуальности данных всех расписаний доступа, дверей, групп и пользователей.
- Если дверной контроллер ведет себя неожиданным образом, см. разделы *Устранение неполадок на стр. 70* и *Обслуживание на стр. 67* для получения дополнительной информации.

Управление доступом

О пользователях

Пользователями приложения AXIS Entry Manager являются те, кто зарегистрирован в качестве владельца одного или нескольких устройств идентификации (типов идентификации). У каждого человека должен быть уникальный профиль пользователя, чтобы ему был предоставлен доступ к дверям в системе контроля доступа. Профиль пользователя — это учетные данные, по которым система опознает пользователя, а также определяет, когда и как ему был предоставлен доступ к дверям. Дополнительные сведения см. в разделе *Создание и изменение пользователей на стр. 44*.

В данном контексте пользователей не следует путать с администраторами. Администраторы имеют неограниченный доступ ко всем настройкам. Однако в контексте управления системой контроля доступа и веб-страницами устройства (AXIS Entry Manager) администраторов тоже иногда называют пользователями. Дополнительные сведения см. в разделе *Пользователи на стр. 58*.

Страница Access Management (Управление доступом)

Страница Access Management (Управление доступом) позволяет настроить и управлять пользователями, группами, дверями и расписаниями системы. Чтобы открыть эту страницу, выберите пункт **Access Management (Управление доступом)**.

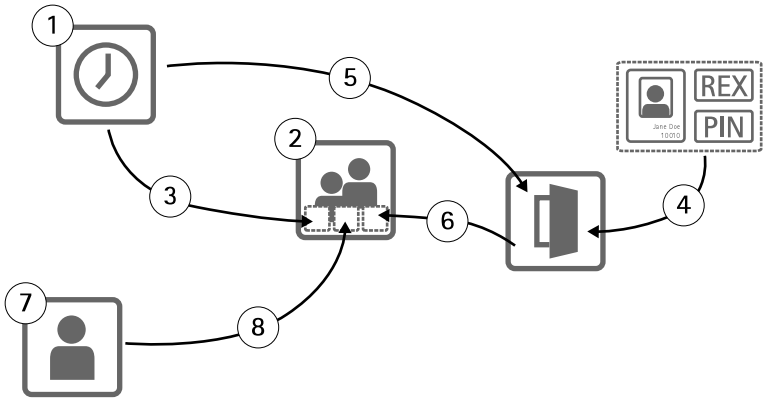
Чтобы добавить пользователей в группы и применить расписания доступа и двери, перетащите элементы в соответствующее место назначения в списках **Groups (Группы)** и **Doors (Двери)**.

Примечание.

Сообщения, требующие определенных действий, выделены красным цветом.

Выбор последовательности операций

Структура управления доступом является гибкой, что позволяет разработать последовательность операций, которая будет удовлетворять вашим потребностям. Ниже представлен пример последовательности операций.



1. Создание расписаний доступа. См. *стр. 35*.
2. Создание групп. См. *стр. 37*.
3. Применение расписаний доступа к группам.
4. Добавление типов идентификации для дверей или этажей. См. *стр. 38* и *стр. 39*.
5. Применение расписаний доступа к каждому типу идентификации.
6. Применение дверей или этажей к группам.

7. Создание пользователей. См. *стр. 44*.
8. Добавление пользователей к группам.

Примеры применения данной последовательности операций см. в разделе *Примеры комбинирования расписаний доступа на стр. 46*.

Создание и изменение расписаний доступа

Расписания доступа служат для определения общих правил того, когда доступ к дверям предоставляется, а когда — не предоставляется. Они также используются для определения правил того, когда группам предоставляется доступ к дверям, а когда — не предоставляется. Дополнительные сведения см. в разделе *Типы расписаний доступа на стр. 35*.

Создание нового расписания доступа:

1. Перейдите в раздел **Access Management (Управление доступом)**.
2. На вкладке **Access Schedules (Расписания доступа)** щелкните **Add new schedule (Добавить новое расписание)**.
3. В диалоговом окне **Add access schedule (Добавить расписание доступа)** введите имя расписания.
4. Для создания расписания доступа на регулярной основе выберите **Addition Schedule (Включающее расписание)**.

   Для создания исключающего расписания выберите **Subtraction Schedule (Исключающее расписание)**.

   Дополнительные сведения см. в разделе *Типы расписаний доступа на стр. 35*.
5. Нажмите кнопку **Save (Сохранить)**.

Чтобы раскрыть какой-либо элемент в списке **Access Schedules (Расписания доступа)**, щелкните  . Включающие расписания показаны зеленым шрифтом, а исключающие расписания — темно-красным.

Чтобы увидеть календарь для расписания доступа щелкните значок  .

Чтобы изменить название или элемент расписания доступа, щелкните значок  и внесите нужные изменения. Затем нажмите кнопку **Save (Сохранить)**.

Чтобы удалить расписание доступа, щелкните  .

Примечание.

Для дверного контроллера предусмотрено несколько готовых расписаний доступа, которые чаще всего применяются. Их можно использовать в качестве примера или изменить так, как нужно. Однако готовое расписание доступа **Always (Всегда)** нельзя изменить или удалить.

Типы расписаний доступа

Существуют два типа расписаний доступа:

- **Включающее расписание** — расписание доступа на регулярной основе, определяющее, когда возможен доступ к дверям. К типичным включающим расписаниям относятся часы работы офиса, часы работы предприятия, нерабочее время или ночное время.
- **Исключающее расписание** — исключения в расписании нормального доступа. Как правило, они используются для ограничения доступа в определенный период времени в рамках обычного включающего расписания. Например, исключающие расписания могут использоваться для запрета доступа пользователей в здание в неприсутственные дни, которые официально установлены как выходные дни.

Оба типа расписаний доступа можно использовать на двух уровнях:

- **Расписания по типу идентификации** — определяют, когда и как считыватели предоставляют пользователям доступ к двери. Каждый тип идентификации должен быть подключен к расписанию доступа, которое сообщает

системе, когда предоставить доступ пользователю с данным конкретным типом идентификации. Для каждого типа идентификации можно добавить несколько включающих и исключающих расписаний. Сведения о типах идентификации см. в разделе *стр. 39*.

- **Групповые расписания** — определяют, когда, но не как, членам группы предоставляется доступ к двери. Каждая группа должна быть подключена к одному или нескольким расписаниям доступа, которые сообщают системе, когда предоставить доступ к двери членам этой группы. Для каждой группы можно добавить несколько включающих и исключающих расписаний. Сведения о группах см. в разделе *стр. 37*.

Групповые расписания могут ограничивать права доступа на вход, но не могут расширять права доступа на вход или выход сверх того, что разрешено расписанием по типу идентификации. Другими словами, если расписание по типу идентификации ограничивает доступ на вход или выход в определенное время, то групповое расписание не может заменить расписание по типу идентификации. Однако если групповое расписание содержит больше ограничений доступа, чем расписание по типу идентификации, то групповое расписание заменяет расписание по типу идентификации.

Расписания по типу идентификации и групповые расписания можно по-разному комбинировать между собой для получения различных результатов. Примеры комбинирования расписаний доступа см. в разделе *стр. 46*.

Добавление элементов расписания

Как включающие, так и исключающие расписания могут включать одноразовые (одиночные) события или периодические события.

Для добавления элемента расписания в расписание доступа:

1. Раскройте расписание доступа в списке **Access Schedules (Расписания доступа)**.
2. Выберите пункт **Add schedule item (Добавить элемент расписания)**.
3. Введите название элемента расписания.
4. Выберите тип: **One time (Один раз)** или **Recurrence (Периодичность)**.
5. Укажите продолжительность в полях времени. См. *Параметры времени: на стр. 36*.
6. Для периодических событий задайте следующие параметры: **Recurrence pattern (Тип периодичности)** и **Range of recurrence (Диапазон периодичности)**. См. *Параметры типа периодичности на стр. 36* и *Параметры диапазона периодичности на стр. 37*.
7. Нажмите кнопку **Save (Сохранить)**.

Параметры времени:

Для времени доступны следующие параметры:

- **All day (Весь день)** — выберите для событий, которые длятся 24 часа в сутки. Затем укажите желаемую дату начала в разделе **Start (Начало)**.
- **Start (Начало)** — щелкните по полю времени для указания нужного времени. При необходимости щелкните по полю даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.
- **End (Конец)** — щелкните по полю времени для указания нужного времени. При необходимости щелкните по полю даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.

Параметры типа периодичности

Для типа периодичности доступны следующие параметры:

- **Yearly (Ежегодно)** — выберите для повтора раз в год.
- **Weekly (Еженедельно)** — выберите для повтора раз в неделю.

- Повтор каждую неделю в следующие дни недели: **Monday (Понедельник)**, **Tuesday (Вторник)**, **Wednesday (Среда)**, **Thursday (Четверг)**, **Friday (Пятница)**, **Saturday (Суббота)** и **Sunday (Воскресенье)** — выберите дни повтора.

Параметры диапазона периодичности

Для диапазона периодичности доступны следующие параметры:

- **First occurrence (Первое вхождение)** — щелкните по полю даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.
- **No end date (Нет конечной даты)** — выберите, чтобы вхождение повторялось до бесконечности.
- **End by (Дата завершения)** — щелкните по полю даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.

Создание и изменение групп

Группы позволяют эффективно управлять сразу всеми пользователями и их правами доступа. Группа состоит из учетных данных, по которым система распознает, из каких пользователей состоит группа, а также определяет, когда и как членам группы был предоставлен доступ к дверям.

Каждый пользователь должен принадлежать к одной или нескольким группам. Для добавления пользователя в группу следует перетащить пользователя в нужную группу в списке **Groups (Группы)**. Дополнительные сведения см. в разделе *Создание и изменение пользователей на стр. 44*.

Создание новой группы:

1. Перейдите в раздел **Access Management (Управление доступом)**.
2. На вкладке **Groups (Группы)** щелкните элемент **Add new group (Добавить новую группу)**.
3. В диалоговом окне **Add Group (Добавить группу)** введите учетные данные группы. См. *Учетные данные группы на стр. 37*.
4. Нажмите кнопку **Save (Сохранить)**.

Чтобы развернуть элемент списка **Groups (Группы)** и посмотреть, кто входит в состав группы, какие у членов группы права и расписание доступа к дверям, нажмите значок  .

Чтобы изменить имя группы или срок действия прав доступа, щелкните значок  и внесите необходимые изменения. Затем нажмите кнопку **Save (Сохранить)**.

Для проверки сведений о том, когда и как члены группы могут иметь доступ к определенным дверям, щелкните значок  .

Чтобы удалить группу или членов группы, а также двери или расписания из группы, щелкните  .

Учетные данные группы

Учетные данные группы содержат следующую информацию:

- **Name (Имя)** (обязательное поле)
- **Valid from (Действительно с)** и **Valid until (Действительно по)** — укажите даты, определяющие срок действия учетных данных группы. Щелкните поле даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.
- **Whitelist (Белый список)** — пользователи из группы «Белый список» в любое время могут открыть дверь, даже в случае неполадок в сети или отключения питания. Поскольку пользователи из этой группы всегда имеют доступ к дверям, к этой группе не применяются расписания и не устанавливаются значения «Действительно до» и «Действительно с». Такой параметр как "Long access time" (Длительное время доступа) не поддерживается, если

дверь открывает пользователь, входящий в группу «Белый список». В эту группу можно добавить только двери с беспроводными замками, которые поддерживают функцию «Белый список».

Примечание.

- Чтобы можно было сохранить группу, необходимо ввести название группы в поле **Name (Имя)**.
- Если пользователь добавлен в группу «Белый список», к нему нельзя применить параметры «Действительно до» и «Действительно с».
- Синхронизация учетных данных группы «Белый список» с данными беспроводного замка занимает некоторое время и мешает выполнению обычных процедур открывания двери. Не следует добавлять или удалять из системы большое количество учетных данных в часы пиковой нагрузки. Когда синхронизация обновленных учетных данных с замком будет выполнена, в журнале событий появится запись `SyncOngoing: false` для данного замка.

Управление дверями

Управление общими правилами для каждой двери осуществляется на вкладке **Doors (Двери)**. Управление правилами включают в себя добавление типов идентификации, определяющих, каким образом пользователям будет предоставляться доступ к двери, а также расписания доступа, определяющие время действия каждого типа идентификации. Дополнительные сведения см. в разделах *Типы идентификации на стр. 39* и *Создание и изменение расписаний доступа на стр. 35*.

Управлять дверью можно только после того, как вы добавите ее в систему контроля доступа, что происходит после завершения настройки оборудования, см. раздел *Настройка оборудования на стр. 14*.

Управление дверью:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Doors (Двери)**.
2. В списке **Doors (Двери)** щелкните значок ▶ рядом с дверью, настройки которой надо изменить.
3. Перетащите эту дверь хотя бы в одну группу. Если список **Groups (Группы)** пуст, создайте новую группу. См. *Создание и изменение групп на стр. 37*.
4. Щелкните элемент **Add identification type (Добавить тип идентификации)** и выберите, какие учетные данные должны представить пользователи для считывателя, чтобы им был дан доступ к двери. См. *Типы идентификации на стр. 39*.

   Для каждой двери необходимо добавить хотя бы один тип идентификации.
5. Чтобы добавить несколько типов идентификации, повторите предыдущий шаг.

   Если добавлены оба типа идентификации — **Card number only (Только номер карты)** и **PIN only (Только PIN)**, то для доступа к двери пользователи могут либо провести карту перед считывателем, либо ввести свой PIN-код. Однако если добавлен только один тип идентификации — **Card number and PIN (Номер карты и PIN)**, то для доступа к двери пользователи должны провести карту перед считывателем и ввести свой PIN-код.
6. Для определения времени действия учетных данных перетащите расписание на каждый тип идентификации.

Для того чтобы вручную разблокировать, заблокировать или предоставить временный доступ к двери, выберите соответствующее действие по управлению дверями в ручном режиме. См. *Применение действий с дверями в ручном режиме на стр. 40*.

Примечание.

Элементы управления для ручной разблокировки, блокировки или предоставления временного доступа к двери недоступны для дверей с беспроводным управлением и беспроводных устройств.

Чтобы открыть какой-либо элемент в списке **Doors (Двери)**, щелкните ▶.

Чтобы изменить имя двери или считывателя, щелкните ✎ и внесите нужные изменения. Затем нажмите кнопку **Save (Сохранить)**.

Для проверки сочетаний считывателя, типа идентификации и расписания доступа щелкните значок  .

Для проверки функций замков, подключенных к дверям, используйте элементы управления, предназначенные для проверки. См. *Проверка дверного оборудования на стр. 22*.

Для удаления типов идентификации или расписаний доступа щелкните значок  .

Типы идентификации

Типы идентификации представляют собой портативные устройства хранения учетных данных или определенный объем записанной информации, либо это могут быть различные сочетания этих двух подходов, которые определяют, каким образом пользователям будет предоставляться доступ к двери. Широкое распространение получили следующие способы идентификации: использование данных, носителями которых служат специальные устройства, пригодные для считывателя (карточки или специальные брелоки); присвоение персональных идентификационных номеров (PIN-кодов); применение устройств, обрабатывающих запросы на выход (REX-устройства).

Для получения дополнительных сведений об учетных данных см. раздел *Учетные данные пользователя на стр. 44*.

Существуют следующие типы идентификации:

- **Facility code only (Только по коду объекта)** — пользователь может открыть дверь с помощью карточки с кодом данного объекта или другого устройства, которое пригодно для считывателя.
- **Card number only (Только по номеру карты)** — пользователь может открыть дверь только с помощью карточки или другого устройства, которое пригодно для считывателя. Номер карты — это уникальный номер, который обычно напечатан на самой карте. Чтобы узнать где расположен номер карты, ознакомьтесь с информацией, предоставляемой производителем карт. Номер карты также может быть получен системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**.
- **Card raw only (Только несформированные данные карты)** — пользователь может получить доступ к двери только с помощью карточки или другого устройства, которое пригодно для считывателя. Нужная информация хранится на карте в виде несформированных данных. Несформированные данные карты также могут быть получены системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**. Используйте этот тип идентификации только тогда, когда не удается обнаружить номер карты.
- **PIN only (Только по PIN-коду)** — пользователь может открыть дверь только после ввода четырехзначного персонального идентификационного номера (PIN-кода).
- **Facility code and PIN (По коду объекта и PIN-коду)** — чтобы открыть дверь, пользователю необходима не только карточка с кодом объекта (или другое устройство, которое пригодно для считывателя), но и PIN-код. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).
- **Card number and PIN (По номеру карты и PIN-коду)** — чтобы открыть дверь, пользователю необходима не только карточка (или другое устройство, которое пригодно для считывателя), но и PIN-код. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).
- **Card raw and PIN (Номер карты и PIN)** — для доступа к двери пользователю необходима как карточка (или другое устройство, которое пригодно для считывателя), так и PIN. Используйте этот тип идентификации только тогда, когда не удается обнаружить номер карты. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).
- **REX** — пользователь может открыть дверь путем активации REX-устройства (устройства, которое обрабатывает запросы на выход) с помощью кнопки, датчика или толкающего рычага.
- **License plate only (Только по номерному знаку автомобиля)** — пользователь может открыть дверь только по номерному знаку транспортного средства.
- **HID Mobile Access (С помощью приложения HID Mobile Access)** — пользователь может открыть дверь с помощью мобильного телефона с установленным приложением HID Mobile Access.

Добавление состояний запланированной разблокировки

Чтобы замок двери автоматически оставался открытым на протяжении указанного времени, можно добавить двери состояние **Scheduled unlock (Запланированная разблокировка)** и применить к нему расписание доступа.

Например, чтобы замок двери оставался открытым в рабочее время:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Doors (Двери)**.
2. Щелкните по значку рядом с элементом списка **Doors (Двери)**, который вы хотите изменить.
3. Нажмите кнопку **Add scheduled unlock (Добавить запланированную разблокировку)**.
4. Выберите состояние разблокировки в пункте **Unlock state (Разблокированное состояние)** (**unlocked (разблокировано)** или **unlock both locks (оба замка разблокированы)** в зависимости от количества замков, установленных на двери: один или два).
5. Нажмите кнопку **OK**.
6. Примените предустановленное расписание доступа **Office hours (Рабочее время)** к состоянию **Scheduled unlock (Запланированная разблокировка)**.

Чтобы проверить время, в течение которого дверь будет разблокирована, нажмите значок .

Чтобы удалить состояние запланированной разблокировки или расписание доступа, нажмите значок .

Применение действий с дверями в ручном режиме

На вкладке **Doors (Двери)** можно разблокировать или заблокировать двери, а также предоставить временный доступ к двери, если использовать элемент **Manual door actions (Действия с дверями в ручном режиме)**. Какие именно действия с дверями в ручном режиме доступны для конкретной двери, зависит от настроек для этой двери.

Применение действий с дверями в ручном режиме:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Doors (Двери)**.
2. В списке **Doors (Двери)** щелкните значок рядом с дверью, настройки которой надо контролировать.
3. Выберите нужное действие с дверью. См. *Действия с дверями в ручном режиме на стр. 40*.

Примечание.

Чтобы применить действия с дверями в ручном режиме, необходимо открыть страницу Access Management (Управление доступом) через тот дверной контроллер, к которому подключена конкретная дверь. Если открыть страницу Access Management (Управление доступом) через дверной контроллер для другой двери, то вместо меню действий с дверями в ручном режиме откроется ссылка на страницу Overview (Обзор) для того дверного контроллера, к которому подключена конкретная дверь. Щелкните эту ссылку, перейдите на страницу **Access Management (Управление доступом)** и выберите вкладку **Doors (Двери)**.

Действия с дверями в ручном режиме

Предусмотрены следующие действия с дверями, которые можно выполнить в ручном режиме:

- **Get door status (Получить статус двери)** — проверка текущего состояния дверного монитора, дверных сигналов и замков.
- **Access (Доступ)** — предоставление пользователям доступа к двери. При этом действует заданное время доступа. См. *Настройка замков и дверных мониторов на стр. 16*.
- Кнопка **Unlock (Разблокировать)** (один замок) или кнопка **Unlock both locks (Разблокировать оба замка)** (два замка) — разблокировка двери. Дверь остается разблокированной до тех пор, пока не будет нажата кнопка **Lock**

(Блокировать) или **Lock both locks (Блокировать оба замка)**; при этом активируется состояние двери согласно расписанию или происходит перезагрузка дверного контроллера.

- Кнопка **Lock (Блокировать)** (один замок) или кнопка **Lock both locks (Блокировать оба замка)** (два замка) — блокировка двери.
- Кнопка **Unlock second lock and lock primary (Разблокировать дополнительный замок и заблокировать главный замок)** — этот параметр доступен только в том случае, если для двери выполнена настройка дополнительного замка. Происходит разблокировка двери. Дополнительный замок остается разблокированным до тех пор, пока не будет нажата кнопка **Double lock (Двойная блокировка)** или не будет активировано состояние двери согласно расписанию.

Управление этажами

После установки в вашу систему сетевого релейного модуля ввода-вывода AXIS 9188 Network I/O Relay Module управление этажами можно осуществлять аналогично тому, как происходит управление дверями.

Примечание.

При использовании контроллеров A1001 в режиме кластера с включенными глобальными событиями, убедитесь, что вы используете уникальные описательные имена для каждого этажа. Например, *"Elevator A, Floor 1" (Лифт A, этаж 1)*.

Примечание.

Для каждого сетевого дверного контроллера A1001 Network Door Controller можно настроить не более двух модулей AXIS 9188 Network I/O Relay Module.

Управление общими правилами для каждого этажа осуществляется на вкладке **Floors (Этажи)**. Управление правилами включают в себя добавление типов идентификации, определяющих, каким образом пользователям будет предоставляться доступ на этаж, а также расписания доступа, определяющие время действия каждого типа идентификации. Дополнительные сведения см. в разделах *Типы идентификации для доступа на этажи на стр. 42* и *Создание и изменение расписаний доступа на стр. 35*.

Управлять этажом можно только после того, как вы добавите его в систему контроля доступа, что происходит после завершения настройки оборудования, см. раздел *Настройка оборудования на стр. 14*.

Управление этажом:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Floors (Этажи)**.
2. В списке **Floors (Этажи)** щелкните значок ▶ рядом с этажом, настройки которого надо изменить.
3. Перетащите этот этаж хотя бы в одну группу. Если список **Groups (Группы)** пуст, создайте новую группу. См. *Создание и изменение групп на стр. 37*.
4. Щелкните элемент **Add identification type (Добавить тип идентификации)** и выберите, какие учетные данные должны представить пользователи для считывателя, чтобы им был предоставлен доступ на этаж. См. *Типы идентификации для доступа на этажи на стр. 42*.

   Для каждого этажа необходимо добавить хотя бы один тип идентификации.
5. Чтобы добавить несколько типов идентификации, повторите предыдущий шаг.

   Если добавлены оба типа идентификации — **Card number only (Только номер карты)** и **PIN only (Только PIN)**, то для доступа к двери пользователи могут либо провести карту перед считывателем, либо ввести свой PIN-код. Однако если добавлен только один тип идентификации — **Card number and PIN (Номер карты и PIN)**, то для доступа к двери пользователи должны провести карту перед считывателем и ввести свой PIN-код.
6. Для определения времени действия учетных данных перетащите расписание на каждый тип идентификации.

Для того чтобы вручную разблокировать, заблокировать или предоставить временный доступ на этажи, выберите соответствующее действие по управлению дверями в ручном режиме. См. *Применение действий с этажами в ручном режиме на стр. 43*.

Примечание.

Элементы управления для ручной разблокировки, блокировки или предоставления временного доступа на этаж недоступны для дверей с беспроводным управлением и/или беспроводных устройств.

Чтобы открыть какой-либо элемент в списке **Floors (Этажи)**, щелкните значок .

Чтобы изменить имя этажа или считывателя, щелкните значок и внесите нужные изменения. Затем нажмите кнопку **Save (Сохранить)**.

Для проверки сочетаний считывателя, типа идентификации и расписания доступа щелкните значок .

Для проверки функций замков, подключенных к этажам, используйте элементы управления, предназначенные для проверки. См. *Проверка этажного оборудования на стр. 22*.

Для удаления типов идентификации или расписаний доступа щелкните значок .

Типы идентификации для доступа на этажи

Для разных способов идентификации применяются портативные устройства хранения учетных данных или определенная информация, которую необходимо запомнить, либо это могут быть различные сочетания этих двух подходов, которые определяют, каким образом пользователям будет предоставляться доступ на этаж. Широкое распространение получили следующие способы идентификации: использование данных, носителями которых служат специальные устройства, пригодные для считывателя (карточки или специальные брелоки); присвоение персональных идентификационных номеров (PIN-кодов); применение устройств, обрабатывающих запросы на выход (REX-устройства).

Для получения дополнительных сведений об учетных данных см. раздел *Учетные данные пользователя на стр. 44*.

Существуют следующие типы идентификации:

- **Facility code only (Только по коду объекта)** — пользователь может открыть дверь на этаж с помощью карточки с кодом данного объекта или другого устройства, которое пригодно для считывателя.
- **Card number only (Только по номеру карты)** — пользователь может получить доступ на этаж только с помощью карточки или другого устройства, которое пригодно для считывателя. Номер карты — это уникальный номер, который обычно напечатан на самой карте. Чтобы узнать где расположен номер карты, ознакомьтесь с информацией, предоставляемой производителем карт. Номер карты также может быть получен системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**.
- **Card raw only (Только несформированные данные карты)** — пользователь может получить доступ на этаж только с помощью карточки или другого устройства, которое пригодно для считывателя. Нужная информация хранится на карте в виде несформированных данных. Несформированные данные карты также могут быть получены системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**. Используйте этот тип идентификации только тогда, когда не удается обнаружить номер карты.
- **PIN only (Только по PIN-коду)** — пользователь может получить доступ на этаж только после ввода четырехзначного персонального идентификационного номера (PIN-кода).
- **Facility code and PIN (По коду объекта и PIN-коду)** — чтобы попасть на этаж, пользователю необходима не только карточка с кодом объекта (или другое устройство, которое пригодно для считывателя), но и PIN-код. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).
- **Card number and PIN (По номеру карты и PIN-коду)** — для доступа на этаж пользователю необходима не только карточка (или другое устройство, которое пригодно для считывателя), но и PIN-код. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).
- **Card raw and PIN (По несформированным данным карты и PIN-коду)** — для доступа на этаж пользователю необходима не только карточка (или другое устройство, которое пригодно для считывателя), но и PIN-код. Используйте этот тип идентификации только тогда, когда не удается обнаружить номер карты. При этом пользователь должен представить свои учетные данные в определенном порядке (сначала карточка, потом PIN-код).

- **REX** — для доступа на этаж пользователю необходимо активировать устройство, обрабатывающее запросы на выход (REX-устройство): это может быть кнопка, датчик или толкающий рычаг.

Добавление состояний запланированной разблокировки

Чтобы доступ на этаж автоматически оставался открытым для всех в определенный период времени, можно добавить для этажа состояние **Scheduled unlock (Запланированная разблокировка)** и применить к нему расписание доступа.

Например, чтобы этаж был открыт для всех в рабочее время:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Floors (Этажи)**.
2. Щелкните значок ▶ рядом с элементом списка **Floor (Этажи)**, который нужно изменить.
3. Нажмите кнопку **Add scheduled unlock (Добавить запланированную разблокировку)**.
4. Выберите **Unlock state (Разблокированное состояние)** (**unlocked (разблокировано)** или **unlock both locks (разблокировать оба замка)** в зависимости от того, один или два замка надо открыть для входа на этаж).
5. Нажмите кнопку **OK**.
6. Примените предустановленное расписание доступа **Office hours (Рабочее время)** к состоянию **Scheduled unlock (Запланированная разблокировка)**.

Для проверки времени доступа на этаж нажмите значок  .

Чтобы удалить состояние запланированной разблокировки или расписание доступа, нажмите значок ⊖ .

Применение действий с этажами в ручном режиме

Для этажей могут быть установлены разные уровни доступа — доступ на этаж может быть ограничен или открыт для всех. Перейдя на вкладку **Floors (Этажи)**, можно предоставить временный доступ с помощью элемента **Manual floor actions (Действия с этажами в ручном режиме)**. В зависимости от заданных настроек для конкретного этажа будут доступны те или иные действия в ручном режиме.

Применение действий с этажами в ручном режиме:

1. В меню **Access Management (Управление доступом)** перейдите на вкладку **Floors (Этажи)**.
2. В списке **Floors (Этажи)** щелкните значок ▶ рядом с этажом, настройки которого надо контролировать.
3. Выберите нужное действие с этажом. См. *Действия по управлению этажами, выполняемые в ручном режиме на стр. 43*.

Примечание.

Чтобы применить действия с этажами в ручном режиме, необходимо открыть страницу Access Management (Управление доступом) через тот контроллер этажа, к которому подключена конкретная дверь. Если открыть страницу Access Management (Управление доступом) через другой контроллер этажа, то вместо меню действий с этажами в ручном режиме откроется ссылка на страницу Overview (Обзор) для того контроллера этажа, к которому подключен конкретный этаж. Щелкните эту ссылку, перейдите на страницу **Access Management (Управление доступом)** и выберите вкладку **Floors (Этажи)**.

Действия по управлению этажами, выполняемые в ручном режиме

Предусмотрены следующие действия по управлению этажами, которые можно выполнить в ручном режиме:

- **Get floor status (Получить состояние этажа)** — проверка текущего состояния реле, подключенного к этажу.
- **Access (Доступ)** — предоставление пользователям доступа на этаж. При этом действует заданное время доступа. См. *Настройка замков и дверных мониторов на стр. 16*.

- **Unlock (Разблокировать)** — этаж становится полностью доступным для всех, пока не будет нажата кнопка **Lock (Блокировать)** или не будет активировано состояние этажа по расписанию или не будет перезапущен дверной контроллер.
- **Lock (Блокировать)** — этаж становится недоступным для всех, пока не будет нажата кнопка **Unlock (Разблокировать)** или не будет активировано состояние этажа по расписанию или не будет перезапущен дверной контроллер.

Создание и изменение пользователей

У каждого человека должен быть уникальный профиль пользователя, чтобы ему был предоставлен доступ к дверям в системе контроля доступа. Профиль пользователя — это учетные данные, по которым система опознает пользователя, а также определяет, когда и как ему предоставляется доступ к дверям.

Каждый пользователь должен принадлежать к одной или нескольким группам, что обеспечивает эффективное управление пользовательскими правами доступа. Дополнительные сведения см. в разделе *Создание и изменение групп*.

Для создания нового профиля пользователя:

1. Перейдите в раздел **Access Management (Управление доступом)**.
2. Перейдите на вкладку **Users (Пользователи)** и выберите элемент **Add new user (Добавить нового пользователя)**.
3. В диалоговом окне **Add User (Добавить пользователя)** введите учетные данные пользователя. См. *Учетные данные пользователя на стр. 44*.
4. Нажмите кнопку **Save (Сохранить)**.
5. Перетащите пользователя в одну или несколько групп в списке **Groups (Группы)**. Если список **Groups (Группы)** пуст, создайте новую группу. См. *Создание и изменение групп на стр. 37*.

Чтобы развернуть элемент списка **Users (Пользователи)** и просмотреть учетные данные пользователя, выберите  .

Чтобы найти определенного пользователя, введите фильтр в поле фильтрации пользователей. Для точного совпадения введите текст в кавычках. Например, "John" или "potter, virginia".

Чтобы изменить учетные данные пользователя, выберите значок  и внесите необходимые изменения. Затем нажмите кнопку **Save (Сохранить)**.

Чтобы удалить, пользователя, нажмите значок  .

Важно!

Если пользователь был создан в приложении AXIS Visitor Manager, его нельзя изменить или удалить в приложении AXIS Entry Manager. Дополнительные сведения о приложении AXIS Visitor Manager и службе считывания QR-кода см. в разделе *AXIS Visitor Access на стр. 26*.

Учетные данные пользователя

Учетные данные пользователя содержат следующую информацию:

- **First name (Имя)** (обязательное поле)
- **Last Name (Фамилия)**
- **Valid from (Действительно с)** и **Valid until (Действительно по)** — укажите даты, определяющие срок действия учетных данных этого пользователя. Щелкните поле даты для выбора нужного месяца, дня и года. Можно также непосредственно ввести дату в это поле.
- **Suspend credential (Приостановить действие учетных данных)** — служит для приостановки действия учетных данных. Если действие учетных данных приостановлено, пользователь не может открыть ни одну из дверей в системе с помощью этих учетных данных. Чтобы вновь предоставить пользователю доступ к дверям, снимите данный флажок. Предполагается, что приостановка носит временный характер. Если надо закрыть пользователю доступ на постоянной основе, то лучше удалить профиль этого пользователя.

- **PIN** (необходим, если не используется номер карты или несформированные данные карты) — введите персональный идентификационный номер (PIN-код), состоящий из четырех цифр, который был выбран пользователем или назначен для него.
- **Facility code (Код объекта)** — введите код для проверки системы контроля доступа на объекте. Если указан предустановленный код объекта, то это поле заполняется автоматически, см. *Предустановленный код объекта на стр. 25*
- **Card number (Номер карты)** (необходим, если не используется PIN-код или несформированные данные карты) — введите номер карты. Чтобы узнать где расположен номер карты, ознакомьтесь с информацией, предоставляемой производителем карт. Номер карты также может быть получен системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**.
- **Card raw (Несформированные данные карты)** (требуется, если не указаны PIN или номер карты) — введите несформированные данные карты. Эти данные могут быть получены системой. Проведите карточку перед подключенным к системе считывателем, выберите в списке этот считыватель и нажмите кнопку **Retrieve (Получить)**. Используйте этот тип идентификации только тогда, когда не удается обнаружить номер карты.
- **Long access time (Длительное время доступа)** — установите этот флажок, чтобы изменить существующий интервал времени доступа и обеспечить длительное время доступа для пользователя (в течение которого дверь открыта), см. раздел *О дверном мониторе и параметрах времени на стр. 16*
- **License plate (Номерной знак автомобиля)** (этот вид учетных данных не доступен при установке дверного контроллера по умолчанию) — при активации этих учетных данных с помощью программных решений от партнеров, укажите номерной знак для автомобиля пользователя.
  Этот вид учетных данных можно использовать только вместе с программным решением от партнеров Axis и при наличии камеры с ПО для распознавания номерных знаков. Для получения более подробной информации обратитесь к партнеру Axis или к местному торговому представителю Axis.
- **HID Mobile Access (С помощью приложения HID Mobile Access)** — пользователь может открыть дверь с помощью мобильного телефона с установленным приложением HID Mobile Access.

Примечание.

Кнопка **Retrieve (Получить)** доступна только после завершения настройки оборудования при условии, что к контроллеру подсоединен хотя бы один считыватель.

Импортирование пользователей

Пользователей можно добавлять в систему путем импортирования текстового файла в формате CSV. Импортирование пользователей рекомендуется в том случае, когда сразу надо добавить много пользователей.

Прежде чем импортировать пользователей, необходимо создать и сохранить файл (*.csv или *.txt) в правильном формате CSV. Отделяйте значения друг от друга запятыми без пробелов, при этом каждый пользователь должен отделяться от других символом конца строки.

Пример

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

Импортирование пользователей:

1. Выберите в меню **Setup > Import Users (Настройка > Импортирование пользователей)**.
2. Найдите и выберите файл *.csv или *.txt, который содержит список пользователей.
3. Выберите для каждого столбца нужный вариант учетных данных.
4. Чтобы импортировать пользователей в систему, нажмите кнопку **Import users (Импортировать пользователей)**.
5. Убедитесь в том, что для каждого столбца выбран правильный тип учетных данных.
6. Если данные в столбцах указаны правильно, нажмите кнопку **Start importing users (Начать импортирование пользователей)**. Если данные в столбцах указаны неправильно, нажмите кнопку **Cancel (Отмена)** и начните сначала.

7. После завершения импортирования нажмите кнопку **OK**.

Для учетных данных можно использовать следующие параметры:

- **First name (Имя)**
- **Last Name (Фамилия)**
- **PIN code (PIN-код)**
- **Card number (Номер карты)**
- **License plate (Номерной знак а/м)**
- **HID Mobile Access**
- **Unassigned (Не назначенный)** — эти данные не будут импортироваться. Выберите этот вариант, если надо пропустить определенный столбец.

Для получения дополнительных сведений об учетных данных см. раздел *Создание и изменение пользователей*.

Экспортирование пользователей

На странице Export представлен список всех пользователей в системе в формате CSV. Этот список можно использовать для экспортирования пользователей в другую систему.

Экспортирование списка пользователей:

1. Откройте простой текстовый редактор и создайте новый документ.
2. Выберите в меню **Setup > Export Users (Настройка > Экспортирование пользователей)**.
3. Выберите все значения на странице и скопируйте их.
4. Вставьте скопированные значения в текстовый документ.
5. Сохраните этот документ в виде файла в формате *.csv или *.txt.

Примеры комбинирования расписаний доступа

Расписания по типу идентификации и групповые расписания можно по-разному комбинировать между собой для получения различных результатов. Примеры ниже относятся к последовательности операций, описанной в разделе *стр. 34*.

Пример

Для создания комбинации расписаний, которая

- предоставляет охранникам доступ к двери в любое время
  - при использовании карты в дневную смену (с понедельника по пятницу, с 6:00 до 16:00) и
  - при использовании карты и PIN-кода до и после дневной смены, и которая
- предоставляет персоналу дневной смены доступ к той же двери
  - при использовании карты только во время дневной смены:

1. Создайте **Addition schedule (Включающее расписание)** под названием **Day shift hours (Дневная смена)**. См. *стр. 35*.
2. Создайте **Schedule item (Элемент расписания)** дневной смены, который повторяется с понедельника по пятницу, 06:00–16:00.
3. Создайте две группы. **Group (Группа)** под названием **Guards (Охрана)** и **Group (Группа)** под названием **Day shift personnel (Персонал дневной смены)**. См. *стр. 37*.

4. Перетащите предустановленное расписание доступа **Always (Всегда)** в группу **Guards (Охрана)**.
5. Перетащите расписание доступа **Day shift hours (Дневная смена)** в группу **Day shift personnel (Персонал дневной смены)**.
6. Добавьте следующие типы идентификации к дверному считывателю: **Card number and PIN (Номер карты и PIN)** и **Card number only (Только номер карты)**.
7. Перетащите предустановленное расписание доступа **Always (Всегда)** к типу идентификации **Card number and PIN (Номер карты и PIN)**.
8. Перетащите расписание доступа **Day shift hours (Дневная смена)** к типу идентификации **Card number only (Только номер карты)**.
9. Перетащите дверь в обе группы. Затем добавьте пользователей в группы по необходимости. См. *стр. 44*.

Пример

Для создания комбинации расписаний, которая

- предоставляет охранникам доступ к двери в любое время
  - при использовании карты в дневную смену (с понедельника по пятницу, с 6:00 до 16:00) и
  - при использовании карты и PIN-кода до и после дневной смены, и которая
- предоставляет персоналу дневной смены доступ к той же двери каждый день с 6:00 до 16:00,
  - при использовании карты во время дневной смены и
  - при использовании карты и PIN-кода в ночную смену и в выходные:

1. Создайте **Addition schedule (Включающее расписание)** под названием **Day shift hours (Дневная смена)**. См. *стр. 35*.
2. Создайте **Schedule item (Элемент расписания)** дневной смены, который повторяется с понедельника по пятницу, 06:00–16:00.
3. Создайте **Subtraction schedule (Исключающее расписание)** под названием **Nights & weekends (Ночная смена и выходные)**.
4. Создайте **Schedule item (Элемент расписания)** ночной смены и выходных, который повторяется с воскресенья по субботу, 16:00–06:00.
5. Перетащите предустановленное расписание доступа **Always (Всегда)** и расписание доступа **Nights & weekends (Ночная смена и выходные)** в группу **Day shift personnel (Персонал дневной смены)**.
6. Создайте две группы. **Group (Группа)** под названием **Guards (Охрана)** и **Group (Группа)** под названием **Day shift personnel (Персонал дневной смены)**. См. *стр. 37*.
7. Перетащите предустановленное расписание доступа **Always (Всегда)** в группу **Guards (Охрана)** и группу **Day shift personnel (Персонал дневной смены)**.
8. Перетащите расписание доступа **Nights & weekends (Ночная смена и выходные)** в группу **Day shift personnel (Персонал дневной смены)**.
9. Добавьте следующие типы идентификации к дверному считывателю: **Card number and PIN (Номер карты и PIN)** и **Card number only (Только номер карты)**.
10. Перетащите предустановленное расписание доступа **Always (Всегда)** к типу идентификации **Card number and PIN (Номер карты и PIN)**.
11. Перетащите расписание доступа **Day shift hours (Дневная смена)** к типу идентификации **Card number only (Только номер карты)**.
12. Перетащите дверь в обе группы. Затем добавьте пользователей в группы по необходимости. См. *стр. 44*.

Настройка сигналов тревоги и событий

Происходящие в системе события — например, когда пользователь подносит карту к считывателю или активируется REX-устройство — заносятся в журнал событий. Можно настроить заносимые в журнал события так, чтобы они инициировали сигналы тревоги, которые будут заноситься в журнал сигналов тревоги.

- Просмотр журнала событий. См. *стр. 48*.
- Экспорт журнала событий. См. *стр. 48*.
- Просмотр журнала сигналов тревоги. См. *стр. 49*.
- Настройка журнала событий и журнала сигналов тревоги. См. *стр. 49*.

Сигналы тревоги также можно настроить, чтобы они инициировали какие-либо действия, например отправку уведомлений по электронной почте. Дополнительные сведения см. в разделе *Как настроить правила действия на стр. 50*.

Просмотр журнала событий

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

Если активированы глобальные события, то можно открыть журнал событий из любого дверного контроллера в системе. Для получения дополнительных сведений о глобальных событиях см. раздел *Настройка журнала событий и журнала сигналов тревоги на стр. 49*.

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. 48*.

Для администратора некоторые события могут представлять больший интерес, чем прочие. Поэтому можно выбрать, какие события и для каких контроллеров должны заноситься в журнал событий. Дополнительные сведения см. в разделе *Параметры журнала событий на стр. 49*.

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.
- Source (Источник) — фильтр для событий, связанных с выбранным контроллером. Доступно только в кластере контроллеров при условии активации глобальных событий.
- Date and time (Дата и время) — фильтрация событий в журнале для заданного диапазона дат и времени.

Экспорт журнала событий

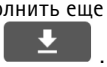
Чтобы экспортировать занесенные в журнал события, выберите **Event Log (Журнал событий)**.

1. Нажмите значок  .
2. Выберите формат экспорта во всплывающем меню, чтобы начать экспорт.

Примечание.

Формат CSV поддерживается во всех браузерах, формат XLSX поддерживается в Chrome™ и Internet Explorer®.

Примечание.

После завершения экспорта значок кнопки экспорта меняется с  на  . Чтобы выполнить еще одну операцию экспорта, обновите веб-страницу. При этом значок кнопки экспорта меняется обратно на  .

Просмотр журнала сигналов тревоги

Для просмотра сработавших сигналов тревоги откройте **Alarm Log (Журнал сигналов тревоги)**. Если активированы глобальные события, то можно открыть журнал сигналов тревоги из любого дверного контроллера в системе. Для получения дополнительных сведений о глобальных событиях см. раздел *Настройка журнала событий и журнала сигналов тревоги на стр. 49*.

Чтобы развернуть запись в журнале сигналов тревоги и просмотреть подробные сведения, например, идентификатор двери и состояние, щелкните значок  .

Чтобы удалить сигнал тревоги из списка после проверки причины тревоги, нажмите кнопку **Acknowledge (Подтвердить)**. Для удаления всех сигналов тревоги нажмите кнопку **Acknowledge all alarms (Подтвердить все сигналы тревоги)**.

Для администратора может потребоваться, чтобы некоторые события инициировали сигналы тревоги. Поэтому можно выбрать, какие события и для каких контроллеров будут инициировать сигналы тревоги. Дополнительные сведения см. в разделе *Параметры журнала сигналов тревоги на стр. 50*.

Настройка журнала событий и журнала сигналов тревоги

Страница настройки журнала событий и журнала сигналов тревоги позволяет определить события, которые должны заноситься в журнал и запускать сигнал тревоги.

Чтобы все подключенные контроллеры имели данные о событиях и сигналах тревоги, выберите **Global events (Глобальные события)**. После активации параметра "Глобальные события" достаточно открыть всего одну страницу Event Log (Журнал событий) и одну страницу Alarm Log (Журнал сигналов тревоги), чтобы одновременно управлять событиями и сигналами тревоги применительно ко всем дверным контроллерам в системе. Параметр "Глобальные события" включен по умолчанию.

Если отключить параметр "Глобальные события", то надо будет открывать одну страницу Event Log (Журнал событий) и одну страницу Alarm Log (Журнал сигналов тревоги) для каждого дверного контроллера и управлять событиями и сигналами тревоги в индивидуальном порядке.

Важно!

При каждом включении или отключении параметра "Глобальные события" происходит очистка журнала событий. Это означает, что все события до текущего момента удаляются и ведение журнала событий начинается заново.

Сигналы тревоги также можно настроить, чтобы они инициировали какие-либо действия, например отправку уведомлений по электронной почте. Дополнительные сведения см. в разделе *Как настроить правила действия на стр. 50*.

Параметры журнала событий

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

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 для всех дверных контроллеров. Данное событие будет зарегистрировано для всех контроллеров и будет занесено в журнал событий.
- **Log for selected sources (Заносить в журнал для выбранных источников)** — активировано ведение журнала событий для выбранных дверных контроллеров. Данное событие будет зарегистрировано для всех выбранных контроллеров и будет занесено в журнал событий. Выберите данный параметр для тех событий, которым в журнале сигналов тревоги будет сопоставлен либо параметр **No alarms (Нет сигналов тревоги)**, либо **Log alarm for selected controllers (Заносить в журнал сигналы тревоги для выбранных контроллеров)**.

  В списке **Configure event logging (Настроить ведение журнала событий)** нажмите кнопку **Select controllers (Выбрать контроллеры)** для того журнала событий, который вы хотите активировать. Откроется диалоговое окно **Device Specific Event Logging (Ведение журнала событий в зависимости от устройства)**. Для варианта **Log event (Занести событие в журнал)** выберите контроллеры, для которых должно быть активировано ведение журнала сигналов тревоги, и нажмите кнопку **Save (Сохранить)**.

Параметры журнала сигналов тревоги

Чтобы задать события, которые должны запускать сигнал тревоги, перейдите в меню **Setup > Configure Event and Alarm Logs (Настройка > Настройка журнала событий и журнала сигналов тревоги)**.

Предусмотрены следующие варианты инициирования сигналов тревоги и занесения их в журнал:

- **No alarms (Нет сигналов тревоги)** — ведение журнала сигналов тревоги отключено. Данное событие не будет инициировать никаких сигналов тревоги и не будет включено в журнал сигналов тревоги.
- **Log alarm for all sources (Заносить в журнал сигналы тревоги для всех источников)** — активировано ведение журнала сигналов тревоги для всех дверных контроллеров. Данное событие будет инициировать сигнал тревоги и будет включено в журнал сигналов тревоги.
- **Log alarm for selected sources (Заносить в журнал сигналы тревоги для выбранных источников)** — активировано ведение журнала сигналов тревоги для выбранных дверных контроллеров. Данное событие будет инициировать сигнал тревоги и будет включено в журнал сигналов тревоги.

  В списке **Configure alarm logging (Настроить ведение журнала сигналов тревоги)** нажмите кнопку **Select sources (Выбрать источники)** под тем элементом журнала сигналов тревоги, который вы хотите активировать. Откроется диалоговое окно **Device Specific Alarm Triggering (Инициирование сигнала тревоги в зависимости от устройства)**. Для варианта **Trigger alarm (Инициировать сигнал тревоги)** выберите дверные контроллеры, для которых должно быть активировано ведение журнала сигналов тревоги, и нажмите кнопку **Save (Сохранить)**.

Как настроить правила действия

Страницы Event (Событие) позволяют настроить устройство Axis так, чтобы при возникновении разных событий выполнялись те или иные действия. Например, устройство может отправить уведомление по электронной почте или активировать выходной порт при запуске сигнала тревоги. 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. в разделах *Триггеры на стр. 51* и *Действия на стр. 54*.

В примере описано, как настроить правило действия, состоящее в отправке уведомления при срабатывании любого сигнала тревоги.

1. Настройте сигналы тревоги. См. *Настройка журнала событий и журнала сигналов тревоги на стр. 49*.
2. Перейдите в меню **Setup > Additional Controller Configuration > Events > Action Rules (Настройка > Настройка дополнительного контроллера > События > Правила действия)** и нажмите кнопку **Add (Добавить)**.
3. Выберите пункт **Enable rule (Активировать правило)** и введите описательное имя для этого правила.
4. Выберите **Event Logger (Ведение журнала событий)** из раскрывающегося списка **Trigger (Инициирующее событие)**.

5. В качестве альтернативного варианта можно выбрать **Schedule (Расписание)** и **Additional conditions (Дополнительные условия)**. См. раздел ниже.
6. В меню **Действия** выберите **Отправить уведомление** в раскрывающемся списка **Тип**.
7. Выберите получателя электронной почты в раскрывающемся списке. См. *Как добавить получателей на стр. 54*.

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.

Триггеры

Предусмотрены следующие **триггеры** и **события**, инициирующие выполнение правил действия:

- **Точка доступа**
  - **Access Point Enabled (Точка доступа активирована)** — правило действия инициируется, если настроено устройство в точке доступа (например, считыватель или REX-устройство); это может быть состояние при завершении настройки оборудования или при добавлении типа идентификации.
- **Конфигурация**

- **Access Point Changed (Точка доступа изменена)** — правило действия инициируется, если настройка устройства в точке доступа (например, считывателя или REX-устройства) изменена; это может быть при настройке оборудования или при изменении типа идентификации, чтобы изменить способ, посредством которого можно открыть дверь.
- **Access Point Removed (Точка доступа удалена)** — правило действия инициируется, если выполнен сброс настроек оборудования для устройства в точке доступа (например считывателя или REX-устройства).
- **Area Changed (Область изменена)** — не поддерживается данной версией инструментального средства AXIS Entry Manager. Это необходимо настроить в клиенте — например, в системе управления доступом через прикладной программный интерфейс VAPIX®, который поддерживает эту функцию, с использованием устройств, способных обеспечить необходимые сигналы. При изменении области доступа активируется правило действия.
- **Area Removed (Область удалена)** — не поддерживается данной версией инструментального средства AXIS Entry Manager. Это необходимо настроить в клиенте — например, в системе управления доступом через прикладной программный интерфейс VAPIX®, который поддерживает эту функцию, с использованием устройств, способных обеспечить необходимые сигналы. При удалении из системы области доступа активируется правило действия.
- **Door Changed (Параметры двери изменены)** — правило действия активируется при изменении параметров настройки двери — например, если изменено имя двери или если дверь добавлена в систему. В частности, это можно использовать для отправки уведомления, если выполняется установка и настройка двери.
- **Door Removed (Дверь удалена)** — правило действия активируется при удалении двери из системы. В частности, это можно использовать для отправки уведомления, если дверь удалена из системы.

• **Дверь**

- **Battery Alarm (Сигнал тревоги, связанный с батареей)** — правило действия активируется, если батарея беспроводного устройства управления дверью имеет низкий заряд или разряжена.
- **Door Alarm (Сигнал тревоги, связанный с дверью)** — правило действия активируется, если согласно дверному монитору дверь была открыта силой, дверь слишком долго находится в открытом положении или дверь имеет какую-либо неисправность. В частности, это можно использовать для отправки уведомления, если кто-то пытается силой открыть дверь и войти.
- **Door Double-Lock Monitor (Монитор двойной блокировки двери)** — правило действия активируется только тогда, когда состояние дополнительной (второй) блокировки меняется либо на "заблокировано", либо на "разблокировано".
- **Door Lock Monitor (Монитор блокировки двери)** — правило действия активируется тогда, когда состояние стандартной блокировки меняется либо на "заблокировано", либо на "разблокировано". Например, активируется состояние неисправности, если дверной монитор обнаруживает, что дверь открыта несмотря на то, что замок заблокирован.
- **Door Mode (Режим двери)** — правило действия активируется при изменении состояния двери — например, если был предоставлен доступ к двери или она была заблокирована, либо если дверь находится в запертом режиме. Более подробные описания этих режимов можно найти в интерактивном справочном руководстве.
- **Door Monitor (Дверной монитор)** — правило действия активируется при изменении состояния дверного монитора. В частности, это можно использовать для отправки уведомления, если дверной монитор указывает, что дверь открыта или закрыта.
- **Door Tamper (Злоумышленные действия, связанные с дверью)** — правило действия активируется, если дверной монитор обнаруживает, что подключение нарушено — например, кто-то перерезал провода, идущие к дверному монитору. Для использования этого триггера необходимо выбрать параметр **Enable supervised inputs (Активировать контролируемые входы)**, а также должны быть установлены резисторы на концах линии для входных портов соответствующих дверных разъемов. Дополнительные сведения см. в разделе *Как использовать контролируемые входы на стр. 19*.
- **Door Warning (Предупреждение, связанное с дверью)** — правило действия активируется до того, как раздастся сигнал тревоги, соответствующий событию «Открыта слишком долго». В частности, это можно использовать для подачи предупреждающего сигнала о том, что дверной контроллер вскоре инициирует

реальный сигнал тревоги, соответствующий событию «Открыта слишком долго», если дверь не будет закрыта до истечения времени, заданного для указанного события. Для получения дополнительных сведений о событии «Открыта слишком долго» см. раздел *Настройка замков и дверных мониторов на стр. 16*.

- **Lock Jammed (Блокировка зажата)** — правило действия активируется в том случае, если созданы физические препятствия для работы беспроводного устройства блокировки двери.

- **Event Logger (Система регистрации событий)** — отслеживает все события, происходящие в дверном контроллере — например, считывание данных с карты или открывание двери пользователем. Если активирован параметр **Global events (Глобальные события)**, то система регистрации событий отслеживает все события, происходящие в каждом контроллере системы. Настройка сигналов тревоги и событий, инициирующих правило действия, выполняется в меню **Setup > Configure Event and Alarm Logs (Настройка > Настройка журнала событий и журнала сигналов тревоги)**. Система регистрации событий находится в общем пользовании и может содержать до 30 000 событий. При достижении предела новые события заносятся в журнал вместо наиболее старых событий по правилу простой очередности. Это означает, что первое событие будет перезаписано в первую очередь.

  - **Alarm (Сигнал тревоги)** — правило действия активируется, если был инициирован один из заданных сигналов тревоги. Системный администратор может в настройках задать, какие события являются более важными, чем другие, и определить, должно ли конкретное событие инициировать сигнал тревоги или нет.

  - **Dropped Alarms (Пропущенные сигналы тревоги)** — правило действия активируется, если новые записи сигналов тревоги не могут быть внесены в журнал сигналов тревоги. Например, если одновременно генерируется так много сигналов тревоги, что система регистрации событий не в состоянии все их отследить. Если какой-то сигнал пропущен, то оператору может быть отправлено уведомление.

  - **Dropped Events (Пропущенные события)** — правило действия активируется, если новые записи событий не могут быть внесены в журналы событий. Например, если одновременно происходит так много событий, что система регистрации событий не в состоянии все их отследить. Если какое-то событие пропущено, то оператору может быть отправлено уведомление.

- **Оборудование**

  - **Network (Сеть)** — правило действия активируется при потере сетевого подключения. Выберите **Yes (Да)** для активации правила действия при потере сетевого подключения. Выберите **No (Нет)** для активации правила действия, когда сетевое подключение будет восстановлено. Выберите **IPv4/v6 address removed (IPv4/v6-адрес удален)** или **New IPv4/v6 (Новый IPv4/v6-адрес)** для запуска действия при изменении IP-адреса.

  - **Peer Connection (Подключение к соседним узлам)** — правило действия активируется, если устройство Axis установило связь с другим дверным контроллером, если потеряно сетевое подключение между устройствами или если не удалось установить связь между дверными контроллерами. В частности, это можно использовать для отправки уведомления о том, что потеряно сетевое подключение дверного контроллера.

- **Входной сигнал**

  - **Digital Input Port (Входной порт для цифровых сигналов)** — правило действия активируется, когда порт ввода-вывода получает сигнал от подключенного устройства. См. *Порты ввода-вывода на стр. 67*.

  - **Manual Trigger (Ручной триггер)** — правило действия активируется при активации ручного триггера. Это можно использовать в клиенте, например, в системе управления доступом через прикладной программный интерфейс VAPIX®, для того чтобы вручную активировать или останавливать правило действия.

  - **Virtual Inputs (Виртуальные входные сигналы)** — правило действия активируется, если меняется состояние одного из виртуальных входных сигналов. Это можно использовать в клиенте, например, в системе управления доступом через прикладной программный интерфейс VAPIX®, для того чтобы инициировать те или иные действия. В частности, виртуальные входные сигналы можно связать с кнопками пользовательского интерфейса системы управления.

- **Расписание**

  - **Interval (Интервал)** — правило активируется в момент начала действия расписания и остается активным до окончания действия расписания.

- **Pulse (Импульс)** — правило действия активируется, когда происходит однократное событие. То есть событие, которое происходит в определенный момент времени и не имеет длительности.

- **Система**

  - **System Ready (Система готова)** — правило действия активируется, когда система находится в состоянии готовности. В частности, устройство Axis может распознавать состояние системы и отправлять уведомление после завершения загрузки системы.

    Выберите **Yes (Да)** для активации правила действия, когда устройство находится в состоянии готовности. Следует отметить, что правило действия будет работать только в том случае, если запущены все необходимые службы, например, система обработки событий.

- **Время**

  - **Recurrence (Повторение)** — правило действия активируется путем отслеживания созданных вами повторяющихся событий. Этот триггер можно использовать для активации повторяющихся событий, например отправки уведомлений каждый час. Выберите шаблон повторяющегося события или создайте новый шаблон. Дополнительные сведения о задании шаблона повторяющихся событий см. в разделе *Как настроить периодичность на стр. 56*.

  - **Use Schedule (Использовать расписание)** — правило действия активируется согласно выбранному расписанию. См. *Создание расписаний на стр. 55*.

Действия

Можно настроить несколько действий:

- **Output Port (Выходной порт)** — активация порта ввода-вывода для управления внешним устройством.
- **Send Notification (Отправить уведомление)** — отправка уведомляющего сообщения получателю.
- **Status LED (Индикатор состояния)** — можно настроить индикатор состояния так, чтобы он мигал, пока выполняется правило действия, или в течение заданного интервала времени в секундах. Индикатор состояния можно использовать во время установки и настройки для визуальной проверки правильности работы триггера с заданными параметрами — например, триггера, соответствующего событию для двери "Открыта слишком долго". Чтобы задать цвет мигающего индикатора состояния, выберите в раскрывающемся списке **LED Color (Цвет индикатора)**.

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 *Типы получателей на стр. 54*.

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**.

Типы получателей

Можно использовать следующие типы получателей:

HTTP

HTTPS

Email (Электронная почта)

TCP

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. 59*.

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.

Отчеты

Страница Reports (Отчеты) позволяет просматривать, печатать и экспортировать отчеты, которые содержат разные сведения о системе. Дополнительные сведения о доступных видах отчетов см. в разделе *Типы отчетов на стр. 57*.

Просмотр, печать и экспорт отчетов

Чтобы открыть страницу отчетов, выберите элемент **Reports (Отчеты)**.

Для просмотра отчета нажмите кнопку **View and print (Просмотр и печать)**.

Для печати отчета:

1. Нажмите кнопку **View and print (Просмотр и печать)**.
2. Выберите столбцы, которые будут включены в отчет. По умолчанию выбраны все столбцы.
3. Если хотите сузить данные, используемые для отчета, введите фильтр в соответствующее поле фильтра. Например, можно отфильтровать пользователей по группам, к которым они принадлежат; двери по их расписаниям; а группы по дверям, к которым у них есть доступ.

   Для точного совпадения введите текст фильтра в кавычках. Например, "John".
4. Для сортировки элементов отчета в другом порядке нажмите значок ▲▼ в соответствующем столбце. Для смены обычного и обратного порядка сортировки используйте кнопки сортировки.

   ▲ Отображает элементы в обычном порядке (по возрастанию).

   ▼ Отображает элементы в обратном порядке (по убыванию).
5. Нажмите кнопку **Print selected columns (Печать выбранных столбцов)**.

Для экспорта отчета нажмите кнопку **Export CSV file (Экспорт CSV-файла)**.

Отчет, включающий в себя все возможные столбцы и элементы, соответствующие типу отчета, экспортируется в виде CSV-файла, в котором значения разделены запятыми. Если не указано иное, то экспортированный файл (*.csv) сохраняется в папке загрузок по умолчанию. Папку загрузок можно выбрать в пользовательских настройках браузера.

Примечание.

В отчетах отображаются только пользователи, у которых есть учетные данные.

Типы отчетов

Доступны следующие типы отчетов:

- Расписания доступа. Дополнительные сведения о типах и настройках расписания доступа см. в разделах *стр. 35* и *стр. 36*.
- Группы. Для получения дополнительных сведений об учетных данных групп см. раздел *стр. 37*.
- Двери. Дополнительные сведения о дверях и типах идентификации см. в разделах *стр. 38* и *стр. 39*.
- Пользователи. Для получения дополнительных сведений об учетных данных пользователей см. раздел *стр. 44*.
- Дверные контроллеры. Дополнительные сведения о подключенных контроллерах и типах их идентификации см. в разделе *стр. 30*. Для получения дополнительных сведений о параметрах времени дверных мониторов см. *стр. 18*

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. 59*.

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. 59*.

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. *Дата и время на стр. 60*.

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.

Дата и время

В устройстве Axis дата и время задаются в меню **Setup > Additional Controller Configuration > System Options > Date & Time (Настройка > Дополнительная настройка контроллера > Параметры системы > Дата и время)**.

Current Server Time (Текущее время сервера) – отображается текущая дата и время (в 24-часовом формате).

Чтобы изменить дату и время, выберите **Time mode (Режим задания времени)** среди параметров **New Server Time (Новое время сервера)**:

- **Synchronize with computer time (Синхронизировать с временем компьютера)** – установка времени по часам компьютера. Данный способ служит для однократной установки даты и времени и не предполагает автоматическое обновление.

- **Synchronize with NTP Server (Синхронизировать с NTP-сервером)** – дата и время сообщаются NTP-сервером. При таком выборе дата и время будут постоянно обновляться. Для получения сведений о настройках NTP-сервера см. раздел *Настройка NTP на стр. 63*.

  Если для NTP-сервера используется имя хоста, то необходимо настроить DNS-сервер. См. *Настройка DNS на стр. 63*.

- **Set manually (Установить вручную)** – этот вариант позволяет вручную задать дату и время.

При использовании NTP-сервера выберите **Time zone (Часовая зона)** из раскрывающегося списка. При необходимости установите флажок **Automatically adjust for daylight saving time changes (Автоматически учитывать локальные изменения времени для более эффективного использования дневного периода)**.

Сеть

Основные настройки TCP/IP

Устройство Axis поддерживает IP, версия 4 (IPv4).

Используя IPv4, устройство Axis может получить следующие варианты адреса:

- **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. 69*.

ARP/Ping

Чтобы назначить устройству IP-адрес, можно использовать команды ARP или Ping. Указания о том, как это сделать, см. в разделе *Назначение IP-адреса с помощью ARP/Ping на стр. 61*.

Сервис ARP/Ping по умолчанию включен, но он автоматически отключается через 2 минуты после запуска устройства или сразу после задания IP-адреса. Для повторного назначения IP-адреса с помощью ARP/Ping, необходимо перезапустить устройство, чтобы включить ARP/Ping еще на две минуты.

Чтобы отключить службу, выберите в меню **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Настройка > Настройка дополнительного контроллера > Параметры системы > Сеть > TCP/IP > Основные)** и снимите флажок **Enable ARP/Ping setting of IP address (Включить ARP/Ping для IP-адреса)**.

Проверку связи с устройством все равно можно проводить при отключенном сервисе.

Назначение IP-адреса с помощью ARP/Ping

Устройству можно назначить IP-адрес с помощью команды ARP или Ping. Команду необходимо ввести в течение 2 минут после подключения питания.

1. Получите свободный статический IP-адрес в том же сегменте сети, где находится компьютер.
2. Найдите серийный номер (S/N) на этикетке устройства.

3. Откройте командную строку и введите следующие команды:

   Синтаксическая структура для Linux/Unix

   ```
   arp -s <IP-адрес> <серийный номер> temp
   ping -s 408 <IP-адрес>
   ```

   Пример для Linux/Unix

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Синтаксическая структура для Windows (для ввода команд может потребоваться вход в систему с учетной записью администратора)

   ```
   arp -s <IP-адрес> <серийный номер>
   ping -l 408 -t <IP-адрес>
   ```

   Пример для Windows (для ввода команд может потребоваться вход в систему с учетной записью администратора)

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. Перезапустите устройство путем отключения и повторного подключения сетевого разъема.
5. После получения от устройства ответа `Reply from 192.168.0.125:...` или аналогичного закройте командную строку.
6. Откройте браузер и введите в адресной строке `http://<IP-адрес>`.

Сведения о других способах назначения IP-адреса см. в документе *How to assign an IP address and access your device (Как назначить IP-адрес и получить доступ к устройству)* на странице *www.axis.com/support*.

Примечание.

- Чтобы открыть командную строку в Windows, откройте меню **Start (Пуск)** и выполните поиск по слову `cmd`.
- Чтобы использовать команду ARP в Windows 8/Windows 7/Windows Vista, щелкните правой кнопкой мыши значок командной строки и выберите **Run as administrator (Запуск от имени администратора)**.
- Чтобы открыть командную строку в Mac OS X, откройте **Terminal utility (Терминал)** из меню **Application > Utilities (Приложение > Утилиты)**.

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. 4*) 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. 58*.

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.

Параметры системы

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. 58*. 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. 69*.

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)**.

Параметры системы

Порты и устройства

Порты ввода-вывода

Дополнительный разъем устройства Axis имеет два настраиваемых порта ввода-вывода для подключения внешних устройств. Дополнительные сведения о подключении внешних устройств см. в руководстве по установке на странице *www.axis.com/techsup*.

Параметры портов ввода-вывода настраиваются в меню **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Настройка > Дополнительная настройка 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 их **нормальных состояний** можно задать 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. 69*.

Сведения об обновлении встроенного ПО см. в разделе *Как обновить встроенное ПО на стр. 70*.

Резервное копирование данных приложения

Чтобы создать резервную копию данных приложения, перейдите к пункту **Setup > Create a backup (Настройка > Создание резервной копии)**. Создаваемая резервная копия включает следующие данные: пользователи, учетные данные, группы и расписания. При создании резервной копии файл с данными сохраняется локально на компьютере.

Важно!

Если данные приложения включают учетные данные для получения доступа с использованием смартфона (HID Mobile Access), создать резервную копию таких данных невозможно.

Чтобы восстановить данные приложения с помощью ранее созданного файла резервной копии, перейдите в меню **Setup > Upload a backup (Настройка > Загрузка резервной копии)**. Перед загрузкой файла резервной копии необходимо выполнить сброс устройства к заводским установкам. Указания о том, как это сделать, см. в разделе *Сброс к заводским установкам на стр. 69*.

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. 70*.

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. 69*.

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.

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. 4* .
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)**.

Устранение неполадок

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.

Автономные дверные контроллеры:

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.

Дверные контроллеры в системе:

Для обновления всех дверных контроллеров в системе можно использовать AXIS Device Manager или AXIS Camera Station. Дополнительные сведения см. на сайте *www.axis.com*.

Важно!

- Не следует выполнять последовательное обновление.

Примечание.

- Все контроллеры в системе всегда должны иметь одинаковую версию встроенного ПО.
- Следует одновременно обновлять все контроллеры в системе, выбирая для этого вариант «Параллельно» в приложении AXIS Device Manager или AXIS Camera Station.

Процедура аварийного восстановления

Если в процессе обновления произойдет отключение питания или нарушение сетевого подключения, то обновление завершится с ошибкой, и устройство может перестать отвечать. Красный мигающий индикатор состояния означает ошибку при обновлении. Для восстановления устройства следуйте указаниям ниже. Найдите серийный номер устройства, который указан на его этикетке.

1. Если используете **UNIX/Linux**, введите в командную строку следующее:

   ```
   arp -s <IP-адрес> <серийный номер> temp
   ping -l 408 <IP-адрес>
   ```

   При использовании **Windows** введите в командную строку следующее (для ввода команд может потребоваться вход в систему с учетной записью администратора):

   ```
   arp -s <IP-адрес> <серийный номер>
   ping -l 408 -t <IP-адрес>
   ```

2. Если устройство не ответит в течение 30 секунд, перезапустите его и дождитесь ответа. Нажмите клавиши CTRL+C для остановки функции Ping.
3. Откройте браузер и введите IP-адрес устройства. На открывшейся странице нажмите кнопку **Browse (Обзор)** и выберите файл обновления, который следует использовать. Затем нажмите кнопку **Load (Загрузить)**, чтобы заново начать процесс обновления.
4. После завершения обновления (1–10 минут) устройство автоматически перезагрузится, и индикатор состояния будет непрерывно гореть зеленым светом.
5. Переустановите устройство в соответствии с инструкциями в руководстве по установке.

Если процедура аварийного восстановления не поможет восстановить работоспособность устройства, свяжитесь со службой поддержки Axis по адресу *www.axis.com/support*.

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.

Устранение неполадок

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.	При включенном протоколе HTTPS убедитесь, что при попытке входа используется должный протокол (HTTP или HTTPS). Возможно, придется вручную ввести `http` или `https` в адресное поле браузера. Если утерян пароль для пользователя root, необходимо произвести сброс параметров устройства к заводским установкам по умолчанию. См. *Сброс к заводским установкам на стр. 69*.
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. *Дата и время на стр. 60*.

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. 64*. 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)**.

Индикатор состояния и индикатор сети часто мигают красным цветом

Сбой оборудования	Свяжитесь с торговым представителем компании Axis.

Устройство не запускается

Устройство не запускается	Если устройство не запускается, выньте и вновь вставьте кабель питания в инжектор при подключенном сетевом кабеле.

Характеристики

Разъемы

Сведения о расположении разъемов см. в разделе .

Схемы подключения и сведения о схеме контактов оборудования, созданной в результате настройки оборудования, см. в разделах *Схемы подключения на стр. 78* и *Настройка оборудования на стр. 14*.

В следующем разделе приводятся технические характеристики разъемов.

Разъем данных считывателя

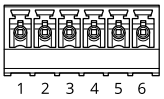
6-контактная клеммная колодка с поддержкой стандарта RS485 и протоколов Wiegand для связи со считывателем.

Порты RS485 поддерживают:

- Двухпроводной полудуплекс RS485
- Четырехпроводной полный дуплекс RS485

Порты Wiegand поддерживают:

- Двухпроводной Wiegand



Функция		Контакт	Примечания
RS485	A-	1	Для полного дуплекса RS485 Для полудуплекса RS485
	B+	2	
RS485	A-	3	Для полного дуплекса RS485 Для полудуплекса RS485
	B+	4	
Wiegand	D0 (данные 0)	5	Для Wiegand
	D1 (данные 1)	6	

Важно!

Порты RS485 имеют фиксированную скорость передачи данных 9600 бит/с.

Важно!

Рекомендуемая максимальная длина кабеля: 30 м.

Важно!

Выходные цепи, упоминаемые в данном разделе, соответствуют Классу 2 ограничения по мощности.

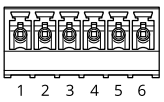
Разъем ввода-вывода считывателя

6-контактная клеммная колодка для подключения:

- Питания дополнительного оборудования (выход питания пост. тока).
- Цифрового входа.

- Цифрового выхода.
- 0 В пост. тока (-).

Контакт 3 на разъемах ввода-вывода считывателя можно контролировать. При нарушении соединения активируется событие. Чтобы использовать контролируемые входы, установите резисторы на концах линии. Для контролируемых входов используйте схему подключения. См. *стр. 78*.



Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1		0 В пост. тока
Выход питания пост. тока	2	Для питания дополнительного оборудования. Примечание. Этот контакт можно использовать только для подачи питания на внешние устройства.	12 В пост. тока Макс. нагрузка = 300 мА
Настраиваемый (вход или выход)	3–6	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 40 В пост. тока
		Цифровой выход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным). При подключении индуктивной нагрузки, например реле, параллельно нагрузке следует включить диод для защиты от переходных напряжений.	От 0 до макс. 40 В пост. тока, с открытым стоком, 100 мА.

Важно!

Рекомендуемая максимальная длина кабеля: 30 м.

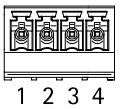
Важно!

Выходные цепи, упоминаемые в данном разделе, соответствуют Классу 2 ограничения по мощности.

Разъем дверного датчика

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

Можно контролировать все входные контакты дверных датчиков. При нарушении подключения раздается сигнал тревоги. Чтобы использовать контролируемые входы, установите резисторы на концах линии. Для контролируемых входов используйте схему подключения. См. *стр. 78*.



Характеристики

Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1, 3		0 В пост. тока
Вход	2, 4	Для обмена данными с дверным монитором. Цифровой вход — подсоедините к контакту 1 или 3, чтобы, соответственно, активировать или оставьте свободным (неподсоединенным), чтобы деактивировать. Примечание. Этот контакт может использоваться только для входа.	От 0 до макс. 40 В пост. тока

Важно!

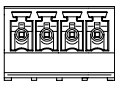
Рекомендуемая максимальная длина кабеля: 30 м.

Вспомогательный разъем

4-контактная настраиваемая клеммная колодка ввода-вывода для подключения:

- питания дополнительного оборудования (выход питания пост. тока),
- цифрового входа,
- Цифровой выход
- 0 В пост. тока (-)

Пример схемы подключения см. в разделе *Схемы подключения на стр. 78*.



Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1		0 В пост. тока
Выход питания пост. тока	2	Для питания дополнительного оборудования. Примечание. Этот контакт можно использовать только для подачи питания на внешние устройства.	3,3 В пост. тока Макс. нагрузка = 100 мА
Настраиваемый (вход или выход)	3–4	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 40 В пост. тока
		Цифровой выход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным). При подключении индуктивной нагрузки, например реле, параллельно нагрузке следует включить диод для защиты от переходных напряжений.	От 0 до макс. 40 В пост. тока, с открытым стоком, 100 мА.

Важно!

Рекомендуемая максимальная длина кабеля: 30 м.

Важно!

Выходные цепи, упоминаемые в данном разделе, соответствуют Классу 2 ограничения по мощности.

Характеристики

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.	10–28 В пост. тока, макс. 36 Вт Макс. нагрузка на выходах = 14 Вт

Сетевой разъем

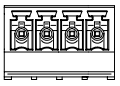
Разъем RJ45 Ethernet. Используйте кабели категории 5e или выше.

Функция	Технические характеристики
Питание и Ethernet	Power over Ethernet IEEE 802.3af/802.3at, тип 1, класс 3, 44–57 В пост. тока Макс. нагрузка на выходах = 7,5 Вт

Разъем питания замка

4-контактная клеммная колодка для питания одного или двух замков (выход питания пост. тока). Разъем замка также может использоваться для питания внешних устройств.

Подсоедините замки и устройства к контактам согласно схеме контактов оборудования, созданной в результате настройки оборудования.



Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1, 3		0 В пост. тока
0 В пост. тока, свободно, или 12 В пост. тока	2, 4	Для управления одним или двумя замками с напряжением 12 В. Используйте схему контактов оборудования. См. *Настройка оборудования на стр. 14*.	12 В пост. тока Макс. общая нагрузка = 500 мА

ПРИМЕЧАНИЕ.

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

Важно!

Выходные цепи, упоминаемые в данном разделе, соответствуют Классу 2 ограничения по мощности.

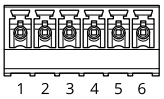
Характеристики

Разъем питания и реле

6-контактная клеммная колодка со встроенным реле для подключения:

- внешних устройств;
- питания дополнительного оборудования (выход питания пост. тока);
- 0 В пост. тока (-).

Подсоедините замки и устройства к контактам согласно схеме контактов оборудования, созданной в результате настройки оборудования.



Функция	Контакт	Примечания	Технические характеристики
0 В пост. тока (-)	1, 4		0 В пост. тока
Реле	2–3	Для подключения устройств реле. Используйте схему контактов оборудования. См. *Настройка оборудования на стр. 14*. Два контакта реле гальванически отделены от остальных цепей.	Макс. ток = 700 мА Макс. напряжение = +30 В пост. тока
12 В пост. тока	5	Для питания дополнительного оборудования. Примечание. Этот контакт можно использовать только для подачи питания на внешние устройства.	Макс. напряжение = +12 В пост. тока Макс. нагрузка = 500 мА
24 В пост. тока	6	Не используется	

ПРИМЕЧАНИЕ.

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

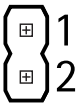
Важно!

Выходные цепи, упоминаемые в данном разделе, соответствуют Классу 2 ограничения по мощности.

Контактная головка, используемая для оповещения при несанкционированных действиях

Две 2-контактные головки для обхода:

- Оповещения при несанкционированных действиях на заднем плане (TB)
- Сигнал тревоги при несанкционированных действиях на переднем плане (TF)



Функция	Контакт	Примечания
Оповещение при несанкционированных действиях на заднем плане	1–2	Чтобы обойти подачу сигнала тревоги при несанкционированных действиях на переднем и заднем плане одновременно, установите перемычки между TB 1, TB 2 и TF 1, TF 2 соответственно. Обход оповещения при несанкционированных действиях означает, что система не будет определять попытки несанкционированных действий.
Оповещение при несанкционированных действиях на переднем плане	1–2	

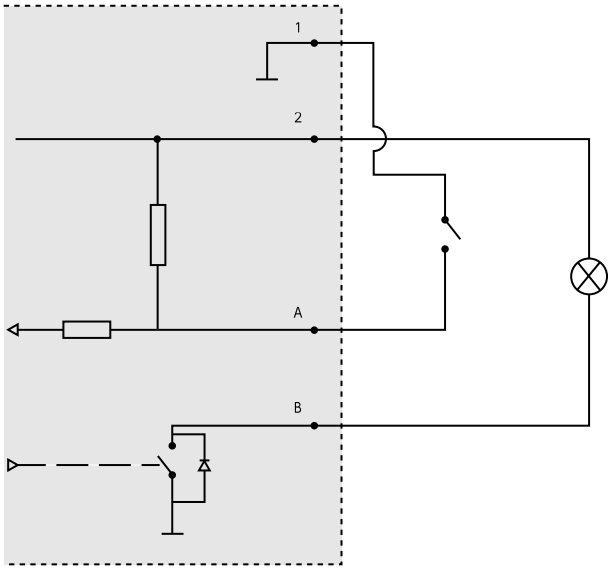
Примечание.

По умолчанию подключено оповещение при несанкционированных действиях как на переднем, так и на заднем плане. Триггер Casing Open (Корпус вскрыт) можно настроить таким образом, чтобы действие выполнялось при открытии крышки дверного контроллера или при снятии дверного контроллера со стены или с потолка. Сведения о настройке оповещения и событий см. в разделе *Настройка сигналов тревоги и событий на стр. 48*.

Схемы подключения

Подсоедините устройства согласно схеме контактов оборудования, созданной в результате настройки оборудования. Дополнительные сведения о настройке оборудования и схеме контактов оборудования см. в разделе *Настройка оборудования на стр. 14*.

Вспомогательный разъем

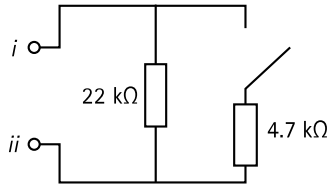


1 0 В пост. тока (-)
2 выход питания пост. тока: 3,3 D, макс. 100 мА
A Вход-выход настроен как вход.
B Вход-выход настроен как выход.

Контролируемые входы

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

Характеристики



i *Вход*

ii *0 В пост. тока (-)*

Примечание.

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

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.

Руководство пользователя
AXIS A1001 & AXIS Entry Manager

Версия M23.3
Дата: Май 2021
Артикул T10010336