AXIS Camera Station Pro Secure Entry

Руководство пользователя

О программе

Secure Entry является компонентом AXIS Camera Station Pro. Используйте его для добавления устройств и управления расписаниями. Подробнее об этом можно узнать в *Руководстве пользователя AXIS Camera Station Pro*.

Настройте контроль доступа

Если вы добавили в свою систему дверной сетевой контроллер Axis, оборудование контроля доступа можно настроить в AXIS Camera Station версии 6.x или более поздней версии.

Полное описание рабочего процесса настройки дверного сетевого контроллера Axis в AXIS Camera Station Pro Secure Entry см. в разделе *Настройка сетевого дверного контроллера Axis*.

Примечание

Прежде чем приступать к настройке, обязательно выполните следующее:

- Обновите AXIS OS контроллера через меню **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)**.
- Установите дату и время для контроллера в разделе **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.
- Активируйте протокол HTTPS на контроллере в разделе **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.

Рабочий процесс настройки контроля доступа

1. Чтобы изменить существующий предустановленный профиль идентификации или создать новый профиль идентификации, см. *Профили идентификации, on page 20*.
2. Чтобы использовать пользовательскую настройку для форматов карт и длины PIN-кода, см. *Форматы карт и ПИН-коды, on page 22*.
3. Добавьте дверь и примените профиль идентификации к двери. См. *Добавление двери, on page 5*.
4. Настройте дверь.
   - *Добавление дверного монитора, on page 12*
   - *Добавить вход чрезвычайной ситуации, on page 13*
   - *Добавление считывающего устройства, on page 14*
   - *Добавление REX-устройства, on page 16*
5. Добавьте зону и добавьте двери в зону. См. *Добавление зоны, on page 17*.

Совместимость программного обеспечения устройств для дверных контроллеров

Внимание

При обновлении AXIS OS на дверном контроллере следует помнить следующее:

- **Поддерживаемые версии AXIS OS:** Поддерживаемые версии AXIS OS, перечисленные ниже применимы только при обновлении с изначально рекомендованной версии AXIS Camera Station Pro и если в системе имеется дверь. Если система не соответствует этим условиям, необходимо обновить ее до версии AXIS OS, рекомендованной на сайте для конкретной версии AXIS Camera Station Pro.
- **Минимальная поддерживаемая версия AXIS OS:** Самая старая версия AXIS OS, установленная в системе, определяет минимально поддерживаемую версию AXIS OS, но не более чем на две версии ниже текущей. Предположим, вы используете AXIS Camera Station Pro версии 6.5 и обновили все устройства до рекомендуемой версии AXIS OS 12.0.86.2. Тогда версия AXIS OS 12.0.86.2 становится минимально поддерживаемой версией для вашей системы в дальнейшем.
- **Обновление до версии AXIS OS, превышающей рекомендованную:** Предположим, вы обновили AXIS OS до версии , превышающей рекомендованную для конкретной версии AXIS Camera Station Pro. При этом вы всегда можете понизить версию обратно до рекомендованной версии AXIS OS, если она находится в пределах поддержки , установленной для версии AXIS Camera Station Pro.
- **Рекомендации по AXIS OS на будущее:** Для обеспечения стабильности и полной совместимости системы всегда следуйте рекомендациям для версии AXIS OS в соответствии с версией AXIS Camera Station Pro.

В таблице ниже приведены минимальные и рекомендуемые версии AXIS OS для каждой версии AXIS Camera Station Pro:

Версия AXIS Camera Station	Минимальная версия AXIS OS	Рекомендуемая версия AXIS OS
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

В таблице ниже приведены минимальные и рекомендуемые версии AXIS OS для каждой версии AXIS Camera Station 5:

Версия AXIS Camera Station	Рекомендуемая версия AXIS OS
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Двери и зоны

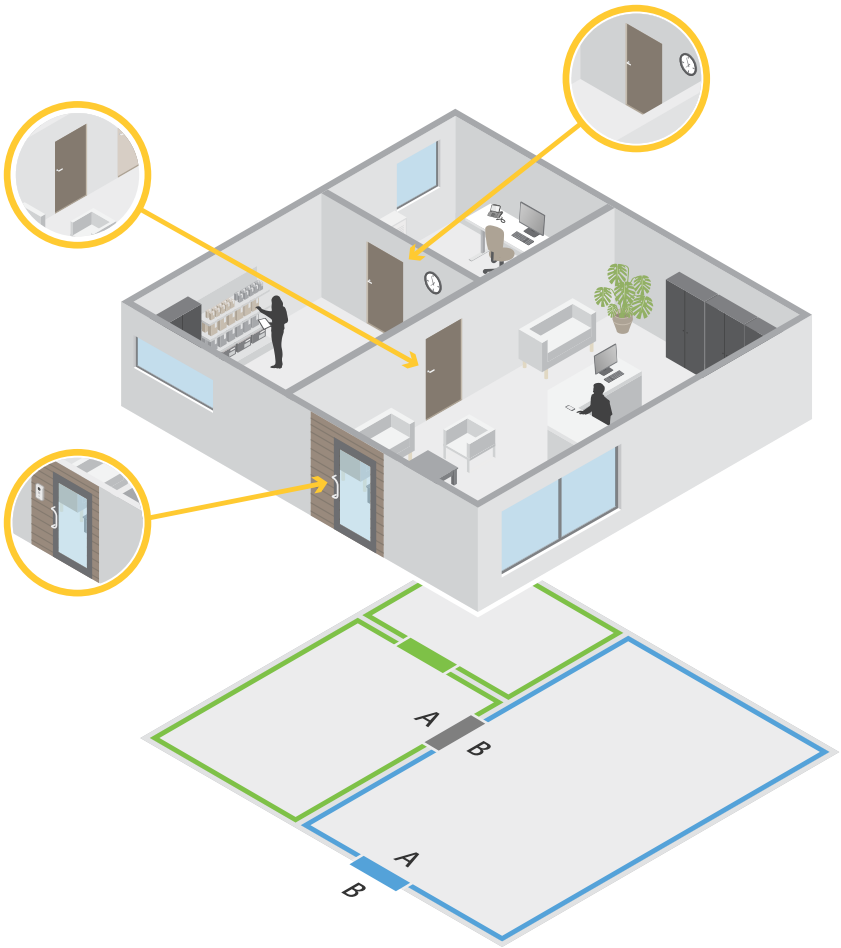
Перейдите в раздел **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**, чтобы получить обзор и настроить двери и зоны.

Схема контактов	Посмотреть схему контактов контроллера, связанную с дверью. Если схему контактов нужно распечатать, нажмите **Print (Печать)**.
Профиль идентификации	Изменить профиль идентификации для дверей.
Защищенный канал	Включение или выключение защищенного канала OSDP Secure Channel для конкретного считывателя.

Двери	
Название	Имя двери.
Дверной контроллер	Дверной контроллер, к которому подключена дверь.
Сторона A	Зона, в которой находится сторона A двери.
Сторона B	Зона, в которой находится сторона B двери.
Профиль идентификации	Профиль идентификации, применяемый к двери.
Форматы карт и ПИН-коды	Показывает тип формата карты или длину PIN-кода.
Статус	Состояние двери. • **Online (Онлайн):** Дверь находится в режиме онлайн и работает корректно. • **Reader offline (Считыватель в автономном режиме):** считыватель в конфигурации двери находится в автономном режиме. • **Reader error (Ошибка считывателя):** Считыватель в конфигурации двери не поддерживает защищенный канал, или защищенный канал выключен для считывателя.

Зоны	
Название	Имя зоны.
Количество дверей	Количество дверей, включенных в зону.

Пример конфигурации дверей и зон



- Имеется две зоны: зеленая и синяя.
- Имеется три двери: зеленая, синяя и коричневая.
- Зеленая дверь — это внутренняя дверь в зеленой зоне.
- Синяя дверь — это дверь по периметру, относящаяся только к синей зоне.
- Коричневая дверь — это дверь по периметру, принадлежащая зеленой и синей зонам.

Добавление двери

Примечание

- Для дверного контроллера можно настроить одну дверь с двумя замками либо же две двери с одним замком в каждой.
- Если дверной контроллер не имеет дверей, и вы используете новую версию AXIS Camera Station Pro Secure Entry со старой прошивкой на дверном контроллере, система не позволит вам добавить дверь. Однако система разрешает добавлять новые двери на системные контроллеры со старой прошивкой при наличии уже существующей двери.

Создание новой конфигурации двери для добавления двери:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите + **Add door (Добавить дверь)** и выберите дверь в раскрывающемся списке.

Типы дверей	
Дверной датчик	Обычная дверь с контролем состояния двери, поддерживающая замки и считывающие устройства. Требуется дверной контроллер.
Беспроводная сеть	Дверь, которую можно настроить с беспроводными замками и коммуникационными хабами ASSA ABLOY Aperio®. Подробнее см. в разделе *Добавление беспроводной блокировки, on page 10*.
Контролируемая дверь	Дверь, которая может сообщать, открыта она или закрыта. Подробнее см. в разделе *Добавление двери с мониторингом, on page 13*.
Выделенная дверь	Дверь, которую можно добавить как резервное устройство в системе без необходимости выбора оборудования.
Этаж	Тип двери для управления лифтом с аутентификацией доступа с помощью считывающего устройства. Для получения дополнительной информации см. раздел .

3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери. Контроллер отображается серым цветом, когда вы не можете добавить другую дверь, когда он находится в режиме офлайн либо если HTTPS не активен.
4. Нажмите **Next (Далее)**, чтобы перейти к странице конфигурации двери.
5. Выберите порт реле из раскрывающегося меню **Primary lock (Главная блокировка)**.
6. Чтобы настроить два замка двери, выберите порт реле из раскрывающегося меню **Secondary lock (Вторичная блокировка)**.
7. Выберите профиль идентификации. См. *Профили идентификации, on page 20*.
8. Настройте параметры двери. См. *Настройки двери, on page 7*.
9. *Добавление дверного монитора, on page 12*
10. *Добавить вход чрезвычайной ситуации, on page 13*
11. *Добавление считывающего устройства, on page 14*
12. *Добавление REX-устройства, on page 16*
13. Настройка уровня безопасности. См. *Уровень безопасности двери, on page 8*.
14. Нажмите **Сохранить**.

Чтобы добавить дверь, скопируйте существующую конфигурации двери:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите + **Add door (Добавить дверь)**.

3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери.
4. Нажмите **Next** ("Далее").
5. Выберите существующую конфигурацию двери из раскрывающегося меню **Copy configuration (Копировать конфигурацию)**. Отображаются подключенные двери, и контроллер становится серым, если он был настроен с двумя дверями или одной дверью с двумя замками.
6. Если необходимо, измените параметры.
7. Нажмите **Сохранить**.

Чтобы изменить параметры двери:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Doors (Конфигурация > Контроль доступа > Двери и зоны > Двери)**.
2. Выберите дверь в списке.
3. Нажмите кнопку **Edit (Изменить)**.
4. Измените значения параметров и нажмите **Save (Сохранить)**.

Чтобы удалить дверь:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Doors (Конфигурация > Контроль доступа > Двери и зоны > Двери)**.
2. Выберите дверь в списке.
3. Выберите пункт **Remove (Удалить)**.
4. Нажмите **Да**.

Добавление и настройка дверей и зон

Настройки двери

1. Перейдите к пункту **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Выберите дверь, которую требуется изменить.
3. Нажмите кнопку **Edit (Изменить)**.

Время доступа (с)	Задайте время (количество секунд), в течение которого дверь должна оставаться отпертой после предоставления доступа. Дверь будет оставаться отпертой, пока она не будет открыта или пока не истечет заданное время. Дверь блокируется при закрытии, даже если время доступа еще не истекло.
Open-too-long time (sec) (Время «открыта слишком долго» (с))	Действует, только если настроен дверной монитор. Установите количество секунд, в течение которых дверь остается отпертой. Если дверь открыта по истечении установленного времени, это вызывает

	сигнал тревоги, соответствующий событию «Открыта слишком долго». Задайте правило действия, чтобы определить, какое действие будет запускаться событием «Открыта слишком долго».
Длительное время доступа (сек)	Задайте время (количество секунд), в течение которого дверь должна оставаться отпертой после предоставления доступа. Длительное время доступа применяется вместо заданной длительности доступа для владельцев карт, для которых включен этот параметр.
Long open-too-long time (sec) (Длительное время «открыта слишком долго» (с))	Действует, только если настроен дверной монитор. Установите количество секунд, в течение которых дверь остается отпертой. Если дверь открыта по истечении установленного времени, это вызывает сигнал тревоги, соответствующий событию «Открыта слишком долго». Длительное время до подачи сигнала тревоги «Открыта слишком долго» применяется вместо заданного времени «открыта слишком долго» для владельцев карт, если активирована настройка **Длительное время доступа**.
Время задержки повторного запирания (мс)	Настройте время в миллисекундах, в течение которого дверь остается незапертой после ее открытия или закрытия.
Повторная блокировка	• **После открытия:** Действует, только если добавлен дверной монитор. • **After closing (После закрытия):** Действует, только если добавлен дверной монитор.
Дверь открыта силой	Выберите, будет ли система подавать сигнал тревоги, если дверь была открыта силой.
Дверь открыта слишком долго	Выберите, будет ли система подавать сигнал тревоги, если дверь оставалась открытой слишком долго.

Уровень безопасности двери

К двери можно добавить следующую функцию безопасности:

Правило двух человек – Правило двух человек требует введения учетных данных двумя людьми для получения доступа.

Двойной свайп – Двойное проведение карты позволяет владельцу карты изменить текущее состояние двери. Например, с помощью этой функции можно заблокировать или разблокировать дверь вне установленного расписания, что удобнее, чем вручную менять статус двери в системе. Двойной свайп не влияет на существующее расписание. Например, если расписание предусматривает блокировку двери при закрытии, и сотрудник уходит на обеденный перерыв, дверь все равно будет заблокирована согласно расписанию.

Можно настроить уровень безопасности при добавлении новой двери или для уже существующей двери.

Для добавления **правила двух человек** к существующей двери:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.

2. Выберите дверь, для которой нужно настроить уровень безопасности.
3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Включение **правила двух человек**.
6. Нажмите **Применить**.

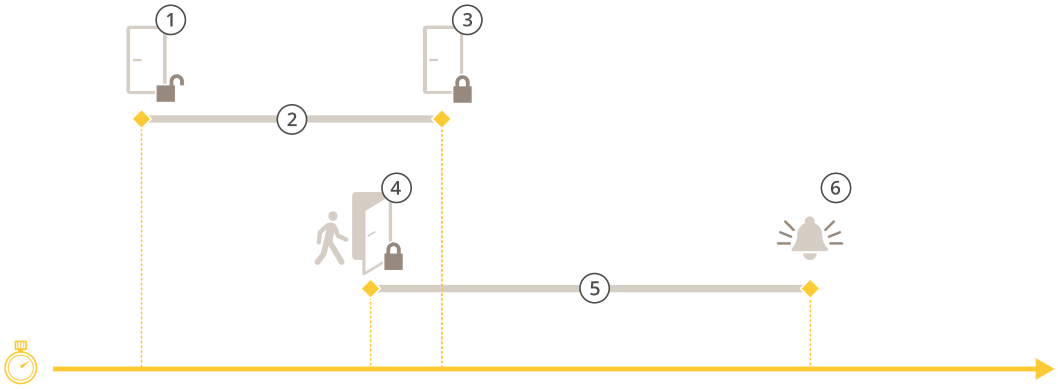
Правило двух человек	
Сторона A и **сторона B**	Выберите, с какой стороны двери будет использоваться правило.
Расписания	Выберите время, в которое будет действовать правило.
Время тайм-аута (в секундах)	Тайм-аут — это максимально допустимое время между считываниями карт или вводом других действительных учетных данных.

Для добавления **двойного свайпа** к существующей двери:

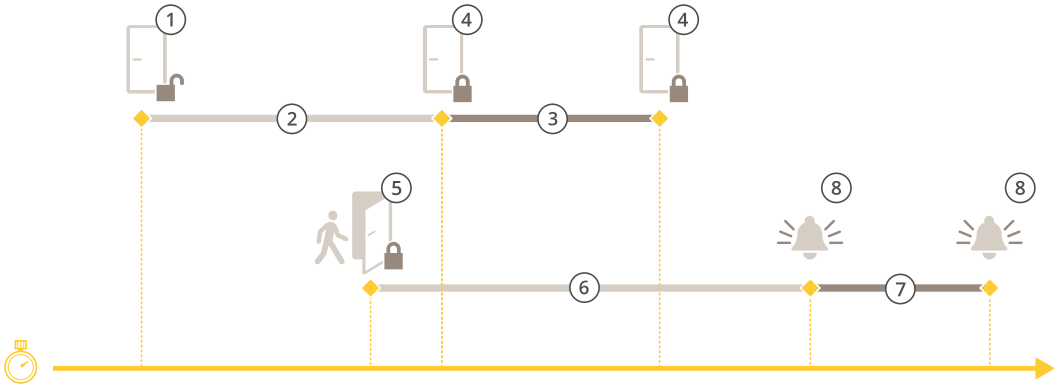
1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите дверь, для которой нужно настроить уровень безопасности.
3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Для включения функции **двойного свайпа**.
6. Нажмите **Применить**.
7. Для применения **двойного свайпа** к владельцу карты.
   7.1. Откройте вкладку **Access Management (Управление доступом)**.
   7.2. Нажмите ⋮ рядом с владельцем карты для редактирования и выберите **Edit (Изменить)**.
   7.3. Нажмите **More (Дополнительно)**.
   7.4. Выберите **Allow double-swipe (Разрешить двойной свайп)**.
   7.5. Нажмите **Применить**.

Двойной свайп	
Время тайм-аута (в секундах)	Тайм-аут — это максимально допустимое время между считываниями карт или вводом других действительных учетных данных.

Параметры времени



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 *Время до подачи сигнала тревоги «Открыта слишком долго»*
6 *Сигнал тревоги «Открыта слишком долго» выключается*



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

Добавление беспроводной блокировки

AXIS Camera Station Pro Secure Entry поддерживает ASSA ABLOY Aperio® беспроводные блокировки и концентраторы. Беспроводная блокировка подключается к системе через концентратор Aperio, подсоединенный к разъему RS485 дверного контроллера. Для одного дверного контроллера можно подключить до 16 беспроводных блокировок.

Примечание

- Для выполнения настройки требуется, чтобы на дверном контроллере Axis была установлена AXIS OS версии 11.6.16.1 или более поздней.
- Для выполнения настройки требуется, чтобы для AXIS Door Controller Extension имелась действительная лицензия.
- Необходимо синхронизировать время на дверном контроллере Axis и на сервере AXIS Camera Station Pro Secure Entry.
- Прежде чем начать работу, необходимо выполнить сопряжение блокировок Aperio с концентратором Aperio, используя прикладное средство с поддержкой технологии ASSA ABLOY.
- Если беспроводные блокировки находятся в автономном режиме, они не будут следовать расписанию отпирания.

1. Выполните доступ к дверному контроллеру.
   1.1. Откройте меню **Конфигурация > Устройства > Другие устройства**.
   1.2. Откройте веб-интерфейс дверного контроллера, подключенного к концентратору Aperio.
2. Включите AXIS Door Controller Extension.
   2.1. В веб-интерфейсе контроллера двери перейдите в раздел **Apps (Приложения)**.
   2.2. Откройте контекстное меню AXIS Door Controller Extension .
   2.3. Щелкните **Activate license with a key (Активировать лицензию ключом)** и выберите нужную лицензию.
   2.4. Включите **AXIS Door Controller Extension**.
3. Подключите беспроводную блокировку к дверному контроллеру через концентратор.
   3.1. В веб-интерфейсе дверного контроллера выберите **Access control > Wireless locks (Контроль доступа > Беспроводные блокировки)**.
   3.2. Нажмите **Connect communication hub (Подключить концентратор)**.
   3.3. Введите имя концентратора и нажмите **OK**.
   3.4. Нажмите **Connect wireless lock (Подключить беспроводную блокировку)**.
   3.5. Выберите адрес и возможности добавляемой блокировки замка и нажмите кнопку **Save (Сохранить)**.
4. Добавьте и настройте дверь с беспроводной блокировкой.
   4.1. В AXIS Camera Station Pro Secure Entry перейдите к пункту **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
   4.2. Нажмите **Add door (Добавить дверь)**.
   4.3. Выберите дверной контроллер, подключенный к концентратору Aperio, выберите **Wireless door (Дверь с беспроводным управлением)** в качестве значения **Door type (Тип двери)**.
   4.4. Нажмите **Next** (“Далее“).
   4.5. Выберите **Wireless lock (Беспроводная блокировка)**.
   4.6. Определите стороны двери A и B и добавьте нужные датчики. Дополнительные сведения см. в разделе *Двери и зоны, on page 4*.

4.7. Нажмите **Сохранить**.

Подключив беспроводную блокировку, можно посмотреть уровень заряда аккумулятора и его состояние в обзоре дверей.

Уровень заряда аккумулятора	Действие
Хорошо	Нет
Низкая	Блокировка работает как положено, но следует заменить аккумулятор до того, как уровень его заряда станет критическим.
Критические ошибки	Замените аккумулятор. Блокировка, возможно, работает неправильно.

Состояние замка	Действие
Дистанционное обучение	Нет
Заклинивание замка	Устраните любые механические проблемы с замком.

Добавление дверного монитора

Дверной монитор — это датчик положения двери, который контролирует физическое состояние двери. Можно добавить дверной монитор к двери и настроить способ его подключения.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 5*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Door monitor sensor (Датчик дверного монитора)**.
4. Выберите порт ввода-вывода, к которому вы хотите подключить дверной монитор.
5. В разделе **Door open if (Дверь открыта, если)** выберите способ подключения цепей дверного монитора.
6. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (Время устранения дребезга)**.
7. Чтобы при прерывании соединения между дверным контроллером и дверным монитором инициировалось событие, включите параметр **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 19*.

Дверь открыта, если	
Цепь разомкнута	Цепь дверного монитора является нормально замкнутой. Дверной монитор отправляет сигнал открытия двери при размыкании цепи. Когда цепь замкнута, дверной монитор отправляет сигнал, означающий, что дверь закрыта.
Цепь замкнута	Цепь дверного монитора является нормально разомкнутой. Дверной монитор отправляет сигнал открытия двери при замыкании цепи. Дверной монитор отправляет сигнал закрытия двери при размыкании цепи.

Добавление двери с мониторингом

Дверь с мониторингом – это тип двери, который позволяет отслеживать ее состояние (открыта или закрыта). Например, такую функцию можно использовать для противопожарной двери, на которой замок не нужен, однако требуется контроль положения двери.

Дверь с мониторингом отличается от обычной двери с дверным монитором. Обычная дверь с дверным монитором поддерживает замки и устройства считывания и при этом требует наличия дверного контроллера. Дверь с мониторингом поддерживает один датчик положения, но требует только сетевого модуля ввода-вывода, подключенного к дверному контроллеру. К одному сетевому модулю ввода-вывода можно подключить до пяти датчиков положения двери.

Примечание

Для двери с мониторингом требуется сетевой модуль ввода-вывода AXIS A9210 с последней версией прошивки, включая приложение AXIS Monitoring Door ACAP.

Настройка двери с мониторингом:

1. Установите AXIS A9210 и обновите его до последней версии AXIS OS.
2. Установите датчики положения двери.
3. В AXIS Camera Station Pro выберите **Configuration** > **Access control** > **Doors and zones** (Конфигурация > Управление доступом > Двери и зоны).
4. Нажмите **Add door (Добавить дверь)**.
5. Введите имя.
6. В разделе **Type (Тип)** выберите **Monitoring door (Дверь с мониторингом)**.
7. В разделе **Device (Устройство)** выберите ваш сетевой модуль ввода-вывода.
8. Нажмите **Next** ("Далее").
9. В разделе **Sensors (Датчики)** нажмите **+ Add (Добавить)** и выберите **Door position sensor (Датчик положения двери)**.
10. Выберите порт ввода-вывода, к которому подключен датчик положения двери.
11. Нажмите **Добавить**.

Добавить вход чрезвычайной ситуации

Вы можете добавить и настроить аварийный вход для инициирования действия, которое блокирует или разблокирует дверь. Можно также настроить способ подключения цепи.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 5*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Emergency input (Вход чрезвычайной ситуации)**.
4. В разделе **Emergency state (Чрезвычайная ситуация)** выберите способ подключения цепи.
5. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (ms) (Время устранения дребезга (мс))**.
6. Выберите **Emergency action (Действие при чрезвычайной ситуации)**, которое должно запускаться при поступлении на дверь сигнала чрезвычайной ситуации.

Аварийное состояние	
Цепь разомкнута	Ко входу чрезвычайной ситуации подключена нормально замкнутая цепь. Сигнал чрезвычайной ситуации отправляется на вход чрезвычайной ситуации, когда цепь размыкается.
Цепь замкнута	Ко входу чрезвычайной ситуации подключена нормально разомкнутая цепь. Сигнал чрезвычайной ситуации отправляется на вход чрезвычайной ситуации, когда цепь замыкается.

Аварийное действие	
Отпереть дверь	Дверь отпирается при получении сигнала чрезвычайной ситуации.
Запереть дверь	Дверь запирается при получении сигнала чрезвычайной ситуации.

Добавление считывающего устройства

Можно настроить дверной контроллер на использование двух проводных считывающих устройств. Вы можете добавить считывающее устройство только с одной стороны или с обеих сторон двери.

Если к считывающему устройству применена пользовательская настройка для форматов карт или длины PIN-кода, это наглядно отображается в столбце **Card Formats (Форматы карт)** в разделе **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны)**. См. *Двери и зоны, on page 4*.

Примечание

- Также к одному контроллеру можно подключить до 16 Bluetooth-считывателей. Подробнее см. в разделе *Добавление считывающего Bluetooth-устройства, on page 15*.
- Если вы используете систему сетевой видеосвязи Axis в качестве IP-считывателя, система использует конфигурацию PIN-кода, заданную на веб-странице устройства.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 5*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **Card reader (Устройство для считывания карт)**.
4. Выберите **Reader type (Тип считывающего устройства)**.
5. Использование пользовательской настройки длины PIN-кода для данного считывателя.
   5.1. Нажмите **Дополнительно**.
   5.2. Включите параметр **Custom PIN length (Пользовательская длина PIN-кода)**.
   5.3. Задайте параметры **Min PIN length (Минимальная длина PIN-кода)**, **Max PIN length (Максимальная длина PIN-кода)** и **End of PIN character (Последний знак PIN-кода)**.
6. Использование пользовательского формата карты для данного считывателя.
   6.1. Нажмите **Дополнительно**.
   6.2. Включите параметр **Custom card formats (Пользовательские форматы карт)**.
   6.3. Выберите требуемые форматы карт для считывающего устройства. Если формат карты с такой же битовой длиной уже используется, необходимо сначала деактивировать этот формат. Значок предупреждения отображается в клиенте, когда настройка формата карты отличается от настройки, заданной в конфигурации системы.
7. Нажмите **Добавить**.

8. Для добавления считывающего устройства на другой стороне двери еще раз повторите эту процедуру.

Для получения информации о настройке считывателя штрих-кодов AXIS см. раздел *Настройка считывателя штрих-кодов AXIS*.

Тип считывателя карт	
OSDP RS485, полудуплекс	Для считывателей RS485 выберите **OSDP RS485 half duplex (OSDP RS485, полудуплекс** и порт считывателя.
Wiegand	В случае считывателей, использующих протоколы Wiegand, выберите **Wiegand** и порт считывателя.
Считыватель IP-адресов	В случае IP-считывателей выберите **IP reader (IP-считыватель)** и выберите устройство из раскрывающегося меню. Сведения о требованиях и поддерживаемых устройствах см. в разделе *Считыватель IP-адресов, on page 16*.

Wiegand	
Контрольный индикатор	Выберите **Single wire (Однопроводной)** или **Dual wire (R/G) (Двухпроводной (кр/зел))**. Считыватели с управлением двумя светодиодами используют разные провода для красного и зеленого цветов.
Оповещение о несанкционированном доступе	Выберите активное состояние входа сигнала несанкционированного доступа (взлома) для считывателя. • **Open circuit (Разомкнутая цепь)**: Считывающее устройство отправляет на дверь сигнал несанкционированного доступа (взлома), когда цепь разомкнута. • **Closed circuit (Замкнутая цепь)**: Считывающее устройство отправляет на дверь сигнал несанкционированного доступа (взлома), когда цепь замкнута.
Время устранения дребезга для обнаружения несанкционированных действий	Чтобы изменения в состоянии входа сигнала несанкционированного доступа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Tamper debounce time (Время устранения дребезга для обнаружения несанкционированных действий)**.
Контролируемый вход	Включите параметры, чтобы при прерывании соединения между дверным контроллером и считывающим устройством инициировалось событие. См. *Контролируемые входы, on page 19*.

Добавление считывающего Bluetooth-устройства

Вы можете использовать AXIS A4612 Network Bluetooth Reader для расширения лимита проводных дверей в контроллерах доступа Axis. Контроллер может управлять до 16 такими считывателями, каждому из которых может быть назначена своя дверь. Каждый считыватель способен управлять замком двери, кнопкой выхода (REX) и датчиком положения двери (DPS).

Добавление и использование этих считывающих устройств не требует дополнительной лицензии.

Чтобы добавить AXIS A4612 Network Bluetooth Reader к двери:

1. Убедитесь, что AXIS A4612 сопряжен с контроллером двери. См. *Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth, on page 34*.
2. Перейдите на страницу конфигурации двери. См. раздел *Добавление двери, on page 5*.
3. Для одной стороны двери нажмите **Add (Добавить)**, затем **Card reader (Устройство для считывания карт)**.
4. Выберите **IP-считыватель**, затем выберите сопряженный AXIS A4612 из выпадающего списка. Если это считывающее устройство будет использоваться для сопряжения учетных данных, отметьте его как предназначенное для сопряжения. Нажмите **Добавить**.
5. На вкладке **Overview (Обзор)** измените профиль идентификации. Вы можете выбрать профили **Tap in app (Касание в приложении)** или **Touch reader (Касание считывателя)**, если AXIS A4612 установлен только с одной стороны двери, а с другой используется кнопка выхода (REX).

Считыватель IP-адресов

В AXIS Camera Station Secure Entry в качестве IP-считывателя можно использовать сетевой домофон Axis.

Примечание

- Для этого требуется AXIS Camera Station 5.38 или более поздней версии и сетевой дверной контроллер AXIS со встроенным ПО версии 10.6.0.2 или более поздней версии.
- Для использования домофона в качестве IP-считывателя никакой его специальной настройки не требуется.

Поддерживаемые устройства:

- Сетевой видеодомофон AXIS A8207-VE Network Video Door Station со встроенным ПО версии 10.5.1 или более поздней версии
- Сетевой видеодомофон AXIS A8207-VE Mk II Network Video Door Station со встроенным ПО версии 10.5.1 или более поздней версии
- AXIS I8116-E Network Video Intercom

Добавление REX-устройства

Вы можете по своему усмотрению добавить REX-устройство только с одной стороны двери или с обеих сторон. В качестве REX-устройства может использоваться пассивный ИК-датчик, REX-кнопка или толкающий рычаг.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 5*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **REX-устройство**.
4. Выберите порт ввода-вывода, к которому вы хотите подключить REX-устройство. Если доступен только один порт, он будет выбран автоматически.
5. В пункте **Action (Действие)** выберите действие, которое будет запускаться при приеме сигнала REX дверью.
6. В разделе **REX active (REX активен)** выберите способ подключения цепей дверного монитора.
7. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (ms) (Время устранения дребезга (мс))**.
8. Чтобы при прерывании соединения между дверным контроллером и REX-устройством инициировалось событие, включите параметр **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 19*.

Действие	
Отпереть дверь	Выберите, чтобы отпереть дверь при приеме сигнала REX.
Нет	Выберите этот вариант, если при поступлении сигнала REX на дверь не должно выполняться никаких действий.

REX активен	
Цепь разомкнута	Выберите этот вариант в случае нормально замкнутой цепи REX. Устройство REX отправляет сигнал, когда цепь размыкается.
Цепь замкнута	Выберите этот вариант в случае нормально разомкнутой цепи REX. Устройство REX отправляет сигнал, когда цепь замыкается.

Добавление зоны

Зона — это конкретная физическая зона с группой дверей. Можно создавать зоны и добавлять в зоны двери. Различают двери двух типов:

- **Perimeter door (Дверь по периметру).** Владельцы карт входят в зону через эту дверь и покидают зону через нее же.
- **Internal door (Внутренняя дверь).** Внутренняя дверь внутри зоны.

Примечание

Дверь по периметру может принадлежать двум зонам. Внутренняя дверь может принадлежать только одной зоне.

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Нажмите **Add zone (Добавить зону)**.
3. Введите имя зоны.
4. Нажмите **Add door (Добавить дверь)**.
5. Выберите двери для добавления в зону и нажмите **Add (Добавить)**.
6. По умолчанию дверь настраивается как дверь по периметру. Чтобы изменить тип двери, выберите **Internal door (Внутренняя дверь)** в раскрывающемся меню.
7. Для двери по периметру по умолчанию устанавливается, что для входа в зону используется сторона двери A. Чтобы изменить сторону, выберите **Leave (Выход)** в раскрывающемся меню.
8. Для удаления двери из зоны выберите нужную дверь и нажмите **Remove (Удалить)**.
9. Нажмите **Сохранить**.

Чтобы изменить параметры зоны:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Выберите зону из списка.
3. Нажмите кнопку **Edit (Изменить)**.
4. Измените значения параметров и нажмите **Save (Сохранить)**.

Чтобы удалить зону:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Выберите зону из списка.
3. Выберите пункт **Remove (Удалить)**.
4. Нажмите **Да**.

Уровень безопасности зон

К зоне можно добавить следующую функцию безопасности:

Запрет на повторный проход – Предотвращает проход людей с использование тех же реквизитов для входа, которые были введены другими людьми, выполнившими вход в зону до них. Человек должен будет сначала выйти из зоны, прежде чем он сможет снова использовать свои учетные данные.

Примечание

- При наличии запрета на повторный проход мы рекомендуем использовать датчики положения дверей на всех дверях в зоне, чтобы убедиться, что пользователь открыл дверь, воспользовавшись своей картой.
- Если контроллер двери переходит в автономный режим, функция запрета на повторный проход продолжает работать при условии, что все двери в зоне относятся к одному и тому же контроллеру. Однако, если двери в зоне принадлежат разным контроллерам, перешедшим в автономный режим, функция запрета на повторный проход перестает работать.

Можно настроить уровень безопасности при добавлении новой зоны или для уже существующей зоны. Чтобы добавить уровень безопасности к существующей зоне, выполните следующие действия:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите зону, для которой нужно настроить уровень безопасности.
3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Включите функции безопасности, которые требуется добавить для двери.
6. Нажмите **Применить**.

Запрет на повторный проход	
Log violation only (Soft) (Только нарушение в журнале (мягкое))	Используйте этот параметр, если требуется разрешить второму человеку войти через дверь, используя те же реквизиты для входа, что и первый человек. Данный вариант приводит только к подаче сигнала тревоги в системе.

Deny access (Hard) (Запрет доступа (строгий))	Используйте это параметр, если требуется запретить второму пользователю вход через данную дверь, если он использует те же реквизиты для входа, что и первый человек. Данный вариант также приводит к подаче сигнала тревоги в системе.
Время тайм-аута (в секундах)	Время до тех пор, пока система не позволит пользователю повторно войти в систему. Введите 0, если тайм-аут использовать не требуется. Это означает, что для зоны установлен запрет на повторный проход до тех пор, пока пользователь не покинет данную зону. Используйте значение тайм-аута, равное **0**, с параметром **Deny access (Hard) (Запрет доступа (строгий))**, только когда все двери в зоне имеют считывающие устройства с обеих сторон.

Контролируемые входы

Контролируемые входы могут вызывать событие при нарушении соединения с дверным контроллером.

- Соединение между дверным контроллером и дверным монитором. См. *Добавление дверного монитора, on page 12*.
- Соединение между дверным контроллером и считывающим устройством, которое использует протоколы Wiegand. См. *Добавление считывающего устройства, on page 14*.
- Соединение между дверным контроллером и устройством REX. См. *Добавление REX-устройства, on page 16*.

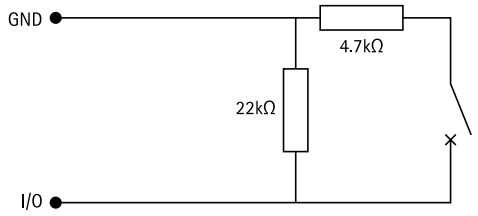
Для использования контролируемых входов:

1. Установите резисторы на концах линии как можно ближе к периферийному устройству в соответствии со схемой подключения.
2. Перейдите на страницу конфигурации считывающего устройства, дверного монитора или REX-устройства и включите параметр **Supervised input (Контролируемый вход)**.
3. Если вы следовали схеме параллельного соединения, выберите **Parallel first connection with a 22 КОм parallel resistor and a 4.7 КОм serial resistor (Параллельное соединение с параллельным резистором 22 кОм и последовательным резистором 4,7 кОм)**.
4. Если вы следовали схеме последовательного подключения, выберите **Serial first connection (Последовательное соединение)** и укажите значение резистора, выбрав его в раскрывающемся меню **Resistor values (Значения резистора)**.

Схемы подключения

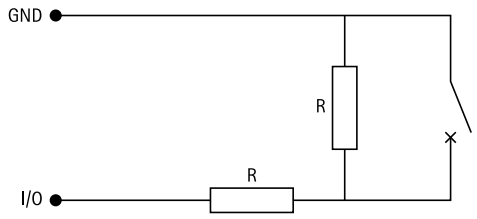
Параллельное соединение

Значение резистора должно быть 4,7 кОм и 22 кОм.



Сначала последовательное соединение

Значение резистора должно быть одинаковым и находиться в диапазоне 1-10 КОм.



Действия в ручном режиме

Вы можете вручную выполнять следующие действия с дверями и зонами:

Сброс – Возвращает к настроенным системным правилам.

Предоставить доступ – Разблокировка двери или зоны на 7 секунд, а затем повторная блокировка.

Отпереть – Дверь остается незапертой до тех пор, пока вы не выполните сброс.

Зафиксировать – Обеспечивает блокировку двери до тех пор, пока система не предоставит доступ владельцу карты.

Блокировать – Никто не войдет и не выйдет, пока вы не сбросите или не разблокируете систему.

Чтобы выполнить действие вручную:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите дверь или зону, для которой необходимо выполнить действие в ручном режиме.
3. Нажмите на любое действие в ручном режиме.

Профили идентификации

Профиль идентификации представляет собой комбинацию типов идентификации и расписаний. Вы можете применить профиль идентификации к одной или нескольким дверям, чтобы установить, как и когда владелец карты может получить доступ к двери.

Типы идентификации — это носители информации об учетных данных, необходимой для доступа к двери. Распространенные типы идентификации — это токены, персональные идентификационные номера (PIN-коды), отпечатки пальцев, определение структуры лица, а также устройства, обрабатывающие запросы на выход (REX-устройства). Тип идентификации может содержать один или несколько типов информации.

Поддерживаемые типы идентификации: Карта, PIN-код, REX, статический QR-код и динамический QR-код.

Примечание

Вы должны использовать динамический QR-код и PIN-код совместно.

Чтобы создать, изменить или удалить профили идентификации, перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.

На выбор доступны пять профилей идентификации по умолчанию, которые можно при необходимости изменить или использовать без каких-либо изменений.

Карта – Для открытия двери владелец карты должен провести карту перед считывателем.

Карта и PIN-код – Для открытия двери владелец карты должен провести карту перед считывателем и ввести PIN-код.

ПИН; PIN-код; ПИН-код – Для открытия двери владелец карты должен ввести PIN-код.

Карта или PIN-код – Для открытия двери владелец карты должен провести карту перед считывателем или ввести PIN-код.

QR-код – Чтобы получить доступ к двери, владельцы карты должны продемонстрировать камере код QR Code®. Профиль идентификации QR-кода можно использовать как для статических, так и для динамических QR-кодов.

Номерной знак а/м – Владелец карты должен подъехать к камере на автомобиле с одобренным номерным знаком.

Активация в приложении – Владелец карты должен активировать учетные данные в мобильном приложении AXIS Camera Station, находясь в зоне действия считывающего устройства Bluetooth.

Сенсорное считывающее устройство – Владелец карты должны прикоснуться к Bluetooth-считывателю, имея при себе мобильный телефон с цифровым пропуском.

QR Code — охраняемый товарный знак Denso Wave Incorporated в Японии и других странах.

Чтобы создать профиль идентификации:

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Нажмите **Create identification profile (Создать профиль идентификации)**.
3. Введите имя профиля идентификации.
4. Выберите **Include facility code for card validation (Включить код объекта для проверки карты)**, чтобы использовать код объекта в качестве одного из полей проверки учетных данных. Это поле доступно, только если вы активировали параметр **Facility code (Код объекта)** в разделе **Access management > Settings (Управление доступом > Настройки)**.
5. Настройте профиль идентификации для одной стороны двери.
6. Повторите предыдущие действия для другой стороны двери.
7. Нажмите кнопку **OK**.

Чтобы внести изменения в профиль идентификации:

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Выберите профиль идентификации и нажмите значок .
3. Чтобы изменить имя профиля идентификации, введите новое имя.
4. Внесите требуемые изменения для данной стороны двери.
5. Чтобы изменить профиль идентификации для другой стороны двери, повторите предыдущие действия.
6. Нажмите кнопку **OK**.

Чтобы удалить профиль идентификации:

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Выберите профиль идентификации и нажмите значок .
3. Если этот профиль идентификации применен к двери, выберите для двери другой профиль идентификации.
4. Нажмите кнопку **OK**.

Изменить профиль идентификации	
×	Чтобы удалить тип идентификации и соответствующее расписание.

Тип идентификации	Чтобы изменить тип идентификации, выберите один или несколько типов из раскрывающегося меню **Identification type (Тип идентификации)**.
Расписание	Чтобы изменить расписание, выберите одно или несколько расписаний из раскрывающегося меню **Schedule (Расписание)**.
+ **Добавить**	Чтобы добавить тип идентификации и соответствующее расписание, нажмите **Add (Добавить)** и задайте типы идентификации и расписания.

Настройка профилей идентификации

Форматы карт и ПИН-коды

Формат карты определяет, как данные хранятся в карте. Он представляет собой таблицу перевода для установления соответствия между входящими данными и проверенными данными в системе. Каждому формату карты соответствует свой набор правил, определяющий, как организовано хранение информации на карте. Задавая формат карты, вы сообщаете системе, как интерпретировать информацию, которую контроллер получает от считывателя карт.

На выбор доступно несколько предварительно определенных широко применяемых форматов карт. При необходимости в них можно внести нужные изменения либо можно их использовать без каких-либо изменений. Можно также создать пользовательские форматы карт.

Перейдите в раздел **(Конфигурация > Контроль доступа > Форматы карт и PIN-коды)** для создания, редактирования или активации форматов карт. Можно также настроить PIN-код.

Пользовательские форматы карт могут содержать следующие поля данных, используемые для проверки учетных данных.

Номер карты – Подмножество двоичных данных учетных данных, кодируемых в виде десятичных или шестнадцатеричных чисел. Номер карты служит для идентификации конкретной карты или владельца карты.

Код объекта – Подмножество двоичных данных учетных данных, кодируемых в виде десятичных или шестнадцатеричных чисел. Код объекта служит для идентификации конкретного конечного заказчика или объекта.

Чтобы создать формат карты:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Щелкните **Add card format (Добавить формат карты)**.
3. Введите имя формата карты.
4. В поле **Bit length (Длина в битах)** введите количество битов от 1 до 256.
5. Если порядок следования битов в данных, получаемых от считывателя карт, нужно менять на обратный, выберите пункт **Invert bit order (Инвертировать порядок битов)**.

6. Если порядок следования байтов данных, получаемых от считывателя карт, нужно менять на обратный, выберите пункт **Invert byte order (Инвертировать порядок байтов)**. Этот параметр доступен, только если указанная битовая длина кратна восьми.
7. Выберите и настройте поля данных, которые должны быть активны в формате карты. В формате карты должно быть активно поле **Card number (Номер карты)** или **Facility code (Код объекта)**.
8. Нажмите кнопку **OK**.
9. Чтобы активировать формат карты, установите флажок перед его именем.

Примечание

- Нельзя одновременно активировать два формата карт с одинаковой длиной в битах. Например, если вы определили два 32-битных формата карт, только один из них может быть активным. Деактивируйте один формат карты, чтобы активировать другой.
- Вы можете активировать и деактивировать форматы карт, только если для данного дверного контроллера был настроен хотя бы один считыватель.

ⓘ	Чтобы увидеть пример выходных данных после инвертирования порядка битов, нажмите значок ⓘ.
Фокусное расстояние	Задайте диапазон битов данных для поля данных. Диапазон должен быть в пределах заданного вами значения параметра **Bit length (Длина в битах)**.
Выходной формат	Выберите выходной формат данных для поля данных. **Десятичный**: Эта система также широко известна как десятичная система счисления, состоит из цифр 0–9. **Шестнадцатеричная система**: (или позиционная система счисления с основанием 16) использует 16 уникальных символов, а именно цифры 0-9 и буквы a-f.
Битовый порядок поддиапазона	Выберите порядок следования битов. **Прямой порядок байтов**: Первый бит является наименьшим (наименее значимым). **Обратный порядок байтов**: Первый бит является наибольшим (наиболее значимым).

Чтобы внести изменения в формат карты:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Выберите формат карты и нажмите значок ✎.
3. Если вы редактируете предопределенный формат карты, вы можете редактировать только **Инвертирование порядка битов** и **Инвертирование порядка байтов**.
4. Нажмите кнопку **OK**.

Можно удалить только пользовательские форматы карт. Чтобы удалить пользовательский формат карты:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Выберите пользовательский формат карты, нажмите значок 🗑 и **Yes (Да)**.

Для сброса предустановленного формата карты:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Для сброса формата карты к схеме полей по умолчанию нажмите значок .

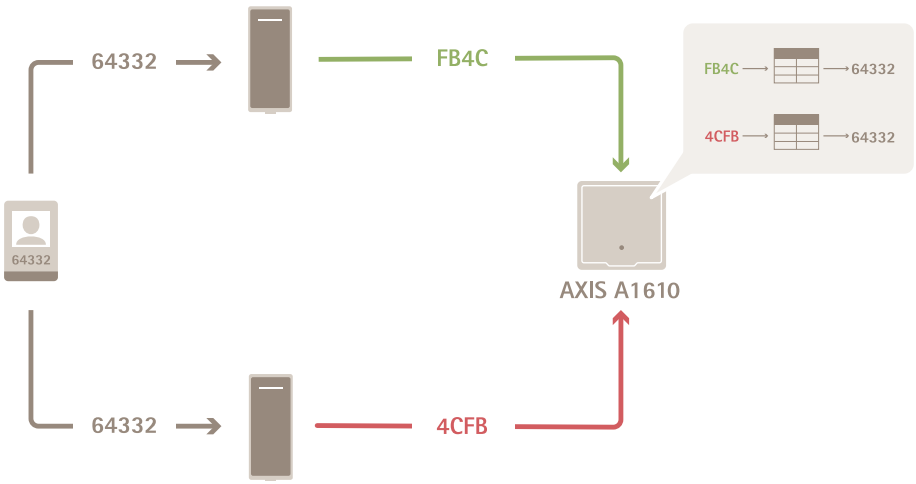
Чтобы настроить длину PIN-кода:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. В разделе **PIN configuration (Конфигурация PIN-кода)** нажмите значок .
3. Задайте параметры **Min PIN length (Минимальная длина PIN-кода)**, **Max PIN length (Максимальная длина PIN-кода)** и **End of PIN character (Последний знак PIN-кода)**.
4. Нажмите кнопку **OK**.

Настройка форматов карт

Настройка параметров форматов карт

Общее представление



- Номер карты в десятичном формате: `64332`.
- Одно считывающее устройство преобразует номер карты в шестнадцатеричное число `FB4C`. Другое считывающее устройство преобразует его в шестнадцатеричное число `4CFB`.
- Сетевой дверной контроллер AXIS A1610 Network Door Controller принимает число `FB4C` и преобразует его в десятичное число `64332` в соответствии с настройками формата карт, которые применяются к считывающему устройству.

- Сетевой дверной контроллер AXIS A1610 Network Door Controller принимает число `4CFB`, инвертирует порядок байтов, получая число `FB4C`, и преобразует его в десятичное число `64332` в соответствии с настройками формата карт, которые применяются к считывающему устройству.

Инвертировать порядок битов

После инвертирования порядка следования битов данные карты, полученные от считывающего устройства, читаются справа налево бит за битом.

Инвертировать порядок байтов

Группа из восьми битов составляет один байт. После инвертирования порядка следования байтов данные карты, полученные от считывающего устройства, читаются справа налево байт за байтом.

Стандартный 26-битный формат карты Wiegand

1 *Ведущий бит контроля четности*
2 *Код объекта*
3 *Номер карты*
4 *Конечный бит контроля четности*

Зашифрованная связь

Защищенный канал OSDP

AXIS Camera Station Secure Entry поддерживает передачу данных по защищенному каналу по протоколу OSDP (OSDP Secure Channel), что обеспечивает возможность шифрования данных, которыми контроллер обменивается со считывателями Axis.

Чтобы включить OSDP Secure Channel для всей системы:

1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
2. Введите основной ключ шифрования и нажмите **OK**.
3. Включите параметр **OSDP Secure Channel (Защищенный канал OSDP Secure Channel)**. Этот параметр доступен только после ввода основного ключа шифрования:
4. По умолчанию ключ защищенного канала OSDP Secure Channel генерируется с использованием основного ключа шифрования. Чтобы вручную задать ключ для OSDP Secure Channel:
   4.1. В разделе **OSDP Secure Channel (Защищенный канал OSDP Secure Channel)** нажмите значок .

4.2. Снимите флажок **Use main encryption key to generate OSDP Secure Channel key (Использовать основной ключ шифрования для формирования ключа для OSDP Secure Channel)**.

4.3. Введите ключ для OSDP Secure Channel и нажмите **OK**.

Сведения о том, как включить или отключить функцию OSDP Secure Channel для конкретного считывателя, см. в разделе *Двери и зоны*.

Считыватель штрих-кодов AXIS

Считыватель штрих-кодов AXIS Barcode Reader — это приложение, которое можно установить на камерах Axis. Дверной контроллер Axis может проверять подлинность считывателя штрих-кодов AXIS, используя ключ проверки подлинности для предоставления доступа. Для получения информации о последовательности операций по настройке считывателя штрих-кодов AXIS см. раздел *Настройка считывателя штрих-кодов Axis*.

Чтобы создать подключение между дверным контроллером и считывателем штрих-кодов AXIS, выполните следующие действия:

1. В AXIS Camera Station Pro Secure Entry:
   1.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   1.2. В разделе **External Peripheral Authentication Key (Ключ проверки подлинности внешнего периферийного оборудования)** нажмите **Show authentication key (Показать ключ проверки подлинности)** и **Copy key (Копировать ключ)**.
2. В веб-интерфейсе устройства, где работает считыватель штрихкодов AXIS Barcode Reader, выполните следующие действия:
   2.1. Откройте приложение AXIS Barcode Reader.
   2.2. Если сертификат сервера не настроен в AXIS Camera Station Pro Secure Entry, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.
   2.3. Если сертификат сервера не настроен в AXIS Camera Station Pro Secure Entry, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.
   2.4. Включите **AXIS Camera Station Secure Entry**.
   2.5. Нажмите **Add (Добавить)**, введите IP-адрес дверного контроллера и вставьте ключ для проверки подлинности.
   2.6. Выберите считывающее устройство, выполняющее считывание штрих-кодов из раскрывающегося меню двери.

Создать подключение с дверным контроллером

1. В AXIS Camera Station Pro Secure Entry:
   1.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   1.2. В разделе **External Peripheral Authentication Key (Ключ проверки подлинности внешнего периферийного оборудования)** нажмите **Show authentication key (Показать ключ проверки подлинности)** и **Copy key (Копировать ключ)**.
2. В веб-интерфейсе устройства, где работает считыватель штрихкодов AXIS Barcode Reader, выполните следующие действия:
   2.1. Откройте приложение AXIS Barcode Reader.
   2.2. Если сертификат сервера не настроен в AXIS Camera Station Pro Secure Entry, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.

2.3. Если сертификат сервера не настроен в AXIS Camera Station Pro Secure Entry, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.

2.4. Включите **AXIS Camera Station Secure Entry**.

2.5. Нажмите **Add (Добавить)**, введите IP-адрес дверного контроллера и вставьте ключ для проверки подлинности.

2.6. Выберите считывающее устройство, выполняющее считывание штрих-кодов из раскрывающегося меню двери.

Мультисерверная БЕТА-ВЕРСИЯ

В мультисерверной системе можно использовать глобальных владельцев карт и группы владельцев карт на основном сервере также и на подключенных подсерверах.

Примечание

- Одна система может поддерживать до 64 подсерверов.
- Для этого требуется AXIS Camera Station 5.47 или более поздней версии.
- Для этого основной сервер и подсерверы должны быть расположены в одной сети.
- На основном сервере и на подсерверах необходимо настроить брандмауэр Windows таким образом, чтобы он разрешал входящие TCP-соединения на порт Secure Entry. Порт по умолчанию — 55767. Сведения о настройке конфигурации портов см. в разделе .

Последовательность операций

1. Настройте сервер в качестве подсервера и создайте файл конфигурации. См. *Создание файла конфигурации на подсервере, on page 27*.
2. Настройте сервер в качестве основного сервера и импортируйте файл конфигурации для подсерверов. См. *Импорт файла конфигурации на основной сервер, on page 27*.
3. Настройте глобального владельца карты и группы владельцев карт на основном сервере. См. *Добавление владельца карты, on page 30* и *Добавление группы, on page 35*.
4. Просмотр и наблюдение за глобальными владельцами карт и группами владельцев карт с подсервера. См. .

Создание файла конфигурации на подсервере

1. На подсервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Sub server (Подсервер)**.
3. Нажмите **Generate (Сформировать)**. Создается файл конфигурации в формате .json.
4. Нажмите **Download (Скачать)** и выберите путь для сохранения файла.

Импорт файла конфигурации на основной сервер

1. На основном сервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Main server (Основной сервер)**.
3. Нажмите + **Add (Добавить)** и перейдите к файлу конфигурации, созданному на подсервере.
4. Введите имя сервера, IP-адрес и номер порта для подсервера.
5. Нажмите **Import (Импорт)** для добавления подсервера.
6. Состояние подсервера отображается как `Connected`.

Отзыв подсервера

Отозвать подсервер можно только до того, как файл конфигурации будет импортирован на основной сервер.

1. На основном сервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Sub server (Подсервер)** и выберите **Revoke server (Отозвать сервер)**.
   Теперь можно настроить этот сервер в качестве основного сервера или в качестве подсервера.

Удаление подсервера

После импорта файла конфигурации подсервера он подключается к основному серверу.

Для удаления подсервера:

1. С основного сервера:
   1.1. Перейдите к пункту **Access management > Dashboard (Управление доступом > Панель управления)**.
   1.2. Измените глобальных владельцев карт и группы на локальных владельцев карт и группы.
   1.3. Перейдите в раздел **Configuration > Access control > Multi server (Конфигурация > Контроль доступа > Мультисерверная система)**.
   1.4. Нажмите **Main server (Основной сервер)** для вывода на отображение списка подсерверов.
   1.5. Выберите подсервер и нажмите **Delete (Удалить)**.
2. С подсервера:
   – Перейдите в раздел **Configuration > Access control > Multi server (Конфигурация > Контроль доступа > Мультисерверная система)**.
   – Нажмите **Sub server (Подсервер)** и выберите **Revoke server (Отозвать сервер)**.

Настройки Active Directory[БЕТА]

Примечание

Для доступа к AXIS Camera Station Pro Secure Entry используются учетные записи Microsoft Windows, а также пользователи и группы Active Directory. Процедура добавления пользователей в Windows может отличаться в зависимости от используемой версии. Более подробные сведения см. на сайте *support.microsoft.com*. Если вы используете домен Active Directory, обратитесь к администратору сети.

При первом открытии страницы настроек Active Directory можно выполнить импорт пользователей Microsoft Active Directory владельцам карт в AXIS Camera Station Pro Secure Entry. См. *Импорт пользователей Active Directory, on page 28*.

После начальной настройки на странице параметров Active Directory появятся следующие параметры.

- Создание групп владельцев карт и управление ими на основе групп в Active Directory.
- Настройка запланированной синхронизации между Active Directory и системой управления доступом.
- Выполнение синхронизации вручную для обновления всех владельцев карт, импортированных из Active Directory.
- Управление сопоставлением данных между данными пользователя из Active Directory и свойствами держателя карты.

Импорт пользователей Active Directory

Для импортирования пользователей Active Directory владельцам карт в AXIS Camera Station Pro Secure Entry:

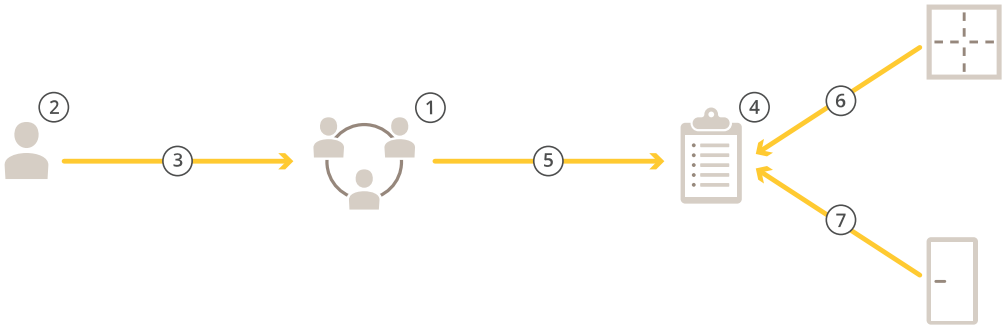
1. Перейдите в меню **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Active Directory settings (Настройки Active Directory)**[БЕТА].
2. Щелкните **Set up import (Настроить импорт)**.
3. Для выполнения этих трех действий следуйте инструкциям на экране.
   3.1. Выберите пользователя из Active Directory для использования его в качестве шаблона для сопоставления данных.
   3.2. Сопоставьте данные пользователя из базы данных Active Directory со свойствами владельца карты.
   3.3. Создайте новую группу владельцев карт в системе управления доступом и выберите, какие группы Active Directory требуется импортировать.

Изменение импортированных данных пользователей невозможно, однако вы можете добавить учетные данные для импортированного владельца карты, см. раздел *Добавить учетные данные, on page 31*.

Настройка управления доступом

Рабочий процесс управления доступом

Структура управления доступом является гибкой, что позволяет разработать рабочий процесс, отвечающий вашим потребностям. Пример рабочего процесса представлен ниже.



1. Добавьте группы. См. *Добавление группы, on page 35*.
2. Добавьте владельцев карт. См. *Добавление владельца карты, on page 30*.
3. Добавьте владельцев карт в группы.
4. Добавьте правила доступа. См. *Добавление правила доступа, on page 36*.
5. Примените группы к правилам доступа.
6. Примените зоны к правилам доступа.
7. Примените двери к правилам доступа.

Добавление владельца карты

Владелец карты — это человек с уникальным идентификатором, зарегистрированным в системе. Настройте владельца карты с учетными данными, которые идентифицируют человека, а также когда и как предоставить ему доступ к дверям.

Можно также сопоставить пользователей в базе данных Active Directory в качестве владельцев карт. См. раздел *Настройки Active Directory[БЕТА], on page 28*.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)** > **Cardholders (Владельцы карт)** и нажмите **+ Add (Добавить +)**.
3. Введите имя и фамилию владельца карты и нажмите **Next (Далее)**.
4. При желании нажмите **Advanced (Дополнительно)** и выберите необходимые параметры.
5. Добавьте учетные данные владельца карты. См. *Добавить учетные данные, on page 31*
6. Нажмите **Сохранить**.
7. Добавьте владельца карты в группу.
   7.1. В разделе **Groups (Группы)** выберите группу, в которую вы хотите добавить владельца карты, и нажмите **Edit (Изменить)**.
   7.2. Нажмите **+ Add (Добавить +)** и выберите владельца карты, которого вы хотите добавить в группу. Можно выбрать несколько владельцев карт.
   7.3. Нажмите **Добавить**.
   7.4. Нажмите **Сохранить**.

Расширенный набор	
Длительное время доступа	Выберите, чтобы предоставить владельцу карты длительное время доступа и длительное время до подачи сигнала тревоги «Открыта слишком долго» при наличии установленного дверного монитора.
Приостановить владельца карты	Выберите, чтобы приостановить владельца карты.
Разрешить двойной свайп	Выберите, чтобы разрешить владельцу карты переопределять текущее состояние двери. В качестве примера, с его помощью можно отпереть дверь вне обычного графика.
Исключение из блокировки	Выберите если требуется, чтобы владелец карты имел доступ во время блокировки.
Снять запрет на проход в обратном направлении	Выберите, чтобы снять для владельца карты запрет на повторный проход. Запрет прохода в обратном направлении предотвращает повторное использование реквизитов для входа другими людьми. Первый человек должен сначала выйти из области, только после этого его реквизиты для входа могут быть использованы снова.
Глобальный владелец карты	Выберите для активации просмотра и мониторинга владельца карты на подсерверах. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 27*.

Добавление владельцев карт и групп

Добавить учетные данные

Владельцу карты можно назначить следующие типы учетных данных:

- ПИН; PIN-код; ПИН-код
- Карта
- Номерной знак а/м
- QR-код
- Мобильный телефон

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **Mobile credential (Данные о мобильном телефоне)**.
2. Введите имя для учетных данных.
3. Установите даты начала и окончания действия учетных данных.

4. Выберите опцию **Send the mobile credential to the cardholder after saving (Отправить цифровой пропуск владельцу карты после сохранения)**. Владелец карты получит сообщение электронной почты с инструкциями по активации.
5. Нажмите **Добавить**.

Пример см. в разделе *Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth, on page 34*.

Чтобы добавить данные номерного знака владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **License plate (Номерной знак)**.
2. Введите название для учетных данных, описывающее транспортное средство.
3. Введите номерной знак автомобиля для транспортного средства.
4. Установите даты начала и окончания действия учетных данных.
5. Нажмите **Добавить**.

Пример см. в разделе *Использование номерного знака автомобиля в качестве учетных данных, on page 33*.

Чтобы добавить PIN-код для владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **PIN-код**.
2. Введите PIN-код.
3. Чтобы использовать PIN-код под принуждением для активации скрытого сигнала тревоги, включите параметр **Duress PIN (PIN-код под принуждением)** и введите PIN-код под принуждением.
4. Нажмите **Добавить**.

Заданный PIN-код действителен всегда. Кроме того, можно настроить так называемый «PIN-код под принуждением», который позволяет открыть дверь, но при этом активирует скрытый сигнал тревоги в системе.

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **PIN-код**.
2. Чтобы вручную ввести данные карты, введите имя карты, номер карты и длину в битах.

Примечание

Длина в битах настраивается, только если вы создаете формат карты с определенной битовой длиной, которой нет в системе.

3. Чтобы автоматически получить данные последней использованной карты:
   3.1. Выберите дверь в раскрывающемся меню **Select reader (Выбрать считыватель)**.
   3.2. Проведите карту через считыватель, подключенный к этой двери.
   3.3. Нажмите **Get last swiped card data from the door's reader(s) (Получить последние считанные данные карты с дверного считывающего устройства)**.

Примечание

Чтобы получить данные с карты, можно использовать считывающее USB-устройство 2N для настольных компьютеров. Более подробную информацию см. в разделе *Настройка считывающего USB-устройства 2N для настольных компьютеров*.

4. Введите код объекта. Это поле доступно, только если вы активировали параметр **Facility code (Код объекта)** в разделе **Access management > Settings (Управление доступом > Настройки)**.
5. Установите даты начала и окончания действия учетных данных.
6. Нажмите **Добавить**.

Чтобы добавить данные QR-кода владельца карты:

Примечание

Использование QR-кода в качестве учетных данных требует, чтобы время на системном контроллере совпадало со временем на камере, на которой работает AXIS Barcode Reader. Рекомендуется использовать один и тот же источник времени для обоих устройств для выполнения идеальной синхронизации времени.

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **QR-код**.
2. Введите имя для учетных данных.
3. Параметр **Dynamic QR (Динамический QR-код)** по умолчанию включен. Динамический QR-код необходимо использовать вместе с PIN-кодом.
4. Установите даты начала и окончания действия учетных данных.
5. Для автоматической отправки QR-кода по электронной почте после сохранения владельца карты, выберите **Send QR code to cardholder when credential is saved (Отправить QR-код владельцу карты при сохранении учетных данных)**.
6. Нажмите **Добавить**.

Дата окончания срока действия	
Действует с	Установите дату и время, когда учетные данные будут действительны.
Действует до	Выберите вариант из раскрывающегося меню.

Действует до	
Нет даты окончания	Срок действия учетных данных никогда не истечет.
Дата	Установите конкретную дату и время истечения срока действия учетных данных.
С момента первого использования	Выберите срок истечения действия учетных данных с момента их первого использования. Выберите количество дней, месяцев или лет или количество раз после первого использования.
С момента последнего использования	Выберите срок истечения действия учетных данных с момента их последнего использования. Выберите количество дней, месяцев или лет после последнего использования.

Использование номерного знака автомобиля в качестве учетных данных

В этом примере показано, как предоставить доступ, используя номерной знак автомобиля в качестве учетных данных, с помощью дверного контроллера и камеры с AXIS License Plate Verifier.

1. Добавьте дверной контроллер и камеру к AXIS Camera Station Pro Secure Entry. См.
2. Задайте дату и время для новых устройств с помощью параметра **Synchronize with computer time (Синхронизировать с временем компьютера)**. См. .
3. Обновите прошивку на новых устройствах до последней доступной версии. См. .
4. Добавьте новую дверь, подключенную к вашему дверному контроллеру. См. *Добавление двери, on page 5*.
   4.1. Добавьте считывающее устройство на **сторону A**. См. *Добавление считывающего устройства, on page 14*.

4.2. В разделе **Door settings (Настройка параметров двери)** выберите **AXIS License Plate Verifier** в качестве значения **Reader type (Тип считывающего устройства)** и введите имя для считывающего устройства.

4.3. Дополнительно можно также добавить считывающее устройство или устройство, обрабатывающее запросы на выход, на **сторону B**.

4.4. Нажмите кнопку **OK**.

5. Установите на камеру AXIS License Plate Verifier и выполните активацию. См. руководство пользователя *AXIS License Plate Verifier*.
6. Запустите AXIS License Plate Verifier.
7. Настройте AXIS License Plate Verifier.
   7.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   7.2. В разделе **External Peripheral Authentication Key (Ключ проверки подлинности внешнего периферийного оборудования)** нажмите **Show authentication key (Показать ключ проверки подлинности)** и **Copy key (Копировать ключ)**.
   7.3. Откройте AXIS License Plate Verifier из веб-интерфейса камеры.
   7.4. Не выполняйте настройку.
   7.5. Выберите в меню **Settings (Настройки)**.
   7.6. В разделе **Access control (Контроль доступа)** выберите **Secure Entry** в качестве значения **Type (Тип)**.
   7.7. В поле **IP address (IP-адрес)** введите IP-адрес дверного контроллера.
   7.8. В поле **Authentication key (Ключ проверки подлинности)** вставьте скопированный вами ранее ключ проверки подлинности.
   7.9. Нажмите **Подключить**.
   7.10. В разделе **Door controller name (Имя дверного контроллера)** выберите нужный дверной контроллер.
   7.11. В разделе **Reader name (Имя считывающего устройства)** выберите добавленное вами ранее считывающее устройство.
   7.12. Включите интеграцию.
8. Добавьте владельца карты, которому хотите предоставить доступ. См. *Добавление владельца карты, on page 30*
9. Добавление данных номерного знака для нового владельца карты. См. *Добавить учетные данные, on page 31*
10. Добавление правила доступа. См. *Добавление правила доступа, on page 36*.
    10.1. Добавление расписания.
    10.2. Добавьте владельца карты, которому вы хотите предоставить доступ к номерному знаку.
    10.3. Добавьте дверь со считывающим устройством AXIS License Plate Verifier.

Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth

В этом примере показано, как добавить в систему считывающее устройство Bluetooth AXIS A4612, чтобы владельцы карт могли открывать двери с помощью приложения AXIS Mobile Credential.

1. Установите считывающее устройство Bluetooth и подключите его к дверному контроллеру.
2. Добавьте считывающее устройство Bluetooth в веб-интерфейс дверного контроллера.
   2.1. Войдите в интерфейс дверного контроллера и перейдите в раздел **Peripherals (Периферийные устройства)** > **Readers (Считывающие устройства)**.
   2.2. Нажмите **Add reader (Добавить считывающее устройство)**.

2.3. Введите необходимые данные в диалоговом окне **Add Bluetooth reader (Добавить считывающее устройство Bluetooth)**.

2.4. Нажмите **Добавить**.

3. Добавьте считывающее устройство Bluetooth к двери в AXIS Camera Station Pro.

3.1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.

3.2. Выберите дверь, к которой нужно добавить считывающее устройство Bluetooth, и нажмите **Edit (Редактировать)**.

3.3. Нажмите **+ Add (Добавить)** на той стороне двери, где установлено считывающее устройство Bluetooth.

3.4. Выберите **Card reader (Устройство для считывания карт)**.

3.5. В разделе **Add IP reader (Добавить IP-считыватель)** выберите **IP-считыватель**.

3.6. В разделе **Select IP reader (Выбрать IP-считыватель)** выберите считывающее устройство Bluetooth.

3.7. Нажмите **Добавить**.

4. Выберите считывающее устройство Bluetooth для сопряжения. Это нужно сделать как минимум для одного считывающего устройства Bluetooth в вашей системе.

4.1. Выберите только что добавленное считывающее устройство Bluetooth.

4.2. Нажмите кнопку **Edit** (Изменить).

4.3. В разделе **Edit bluetooth reader (Выбрать считывающее устройство bluetooth)** выберите **Use this reader for pairing (Использовать это считывающее устройство для сопряжения)**.

4.4. Нажмите **Применить**.

5. Выберите профиль идентификации **Tap in app (Активация в приложении)** или **Touch reader (Сенсорное считывающее устройство)**. Для получения дополнительных сведений см. *Профили идентификации, on page 20*.

6. Добавьте мобильный пропуск для владельца карты. См. *Добавить учетные данные, on page 31*.

7. Выполните сопряжение мобильного пропуска со считывающим устройством.

7.1. Поднесите мобильный телефон владельца карты к считывающему устройству Bluetooth, настроенному для сопряжения.

7.2. Следуйте инструкциям из электронного письма, отправленного владельцу карты.

Добавление группы

Группы позволяют эффективно управлять множеством владельцев карт и связанными с ними правилами доступа.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)** > **Groups (Группы)** и нажмите **+ Add (Добавить +)**.
3. Введите название и, по желанию, инициалы для группы.
4. Выберите **Global group (Глобальная группа)** для просмотра и отслеживания владельца группы на подсерверах. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 27*.
5. Добавление в группу владельцев карт:

5.1. Щелкните **+ Добавить**.

5.2. Выберите владельцев карт, которых вы хотите добавить, и нажмите **Add (Добавить)**.

6. Нажмите **Сохранить**.

Добавление правила доступа

Правило доступа определяет условия, которые должны быть выполнены для предоставления доступа.

Правило доступа состоит из следующих элементов:

Владельцы карт и группы владельцев карт – кому следует предоставлять доступ.

Двери и зоны – где применяется правило доступа.

Расписания – когда следует предоставлять доступ.

Чтобы добавить правило доступа:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)**.
3. В разделе **Access rules (Правила доступа)** нажмите **+ Add (Добавить +)**.
4. Введите имя правила доступа и нажмите **Next (Далее)**.
5. Настройка владельцев карт и групп:
   5.1. В разделе **Cardholders (Владельцы карт)** или **Groups (Группы)** нажмите **+ Add (Добавить +)**.
   5.2. Выберите владельцев карт или группы и нажмите **Add (Добавить)**.
6. Настройка дверей и зон:
   6.1. В разделе **Doors (Двери)** или **Zones (Зоны)** нажмите **+ Add (Добавить +)**.
   6.2. Выберите двери или зоны и нажмите **Добавить (Add)**.
7. Настройка расписаний:
   7.1. В разделе **Schedules (Расписания)** нажмите **+ Add (Добавить +)**.
   7.2. Выбрав одно или несколько расписаний, нажмите **Add (Добавить)**.
8. Нажмите **Сохранить**.

Правило доступа, в котором отсутствует один или более компонентов, описанных выше, является неполным. Просмотреть все неполные правила доступа можно на вкладке **Incomplete (Неполные)**.

Экспорт отчетов о конфигурации системы

Вы можете экспортировать отчеты, содержащие различные типы информации о системе. AXIS Camera Station Pro Secure Entry Экспорт отчета в виде файла со значениями, разделенными запятыми (CSV), и сохранение его в папке загрузки по умолчанию. Для экспорта отчета:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Reports (Отчеты)** > **System configuration (Конфигурация системы)**.
3. Выберите отчеты, которые вы хотите экспортировать, и нажмите **Download (Загрузить)**.

Подробный отчет о владельцах карты	Включает информацию о владельцах карт, об учетных данных, о проверке карт и о последней операции.
Отчет о доступе владельцев карты	Включает информацию о владельце карты, а также информацию о группах владельцев карт, о правилах доступа, дверях и зонах, с которыми связан владелец карты.
Отчет о доступе группы владельцев карты	Включает имя группы владельцев карт, а также информацию о владельцах карт, правилах доступа, дверях и зонах, с которыми связана группа владельцев карт.
Отчет о правилах доступа	Включает имя правила доступа, а также информацию о владельцах карт, группах владельцев карт, дверях и зонах, с которыми связано правило доступа.
Отчет о доступе к двери	Включает имя двери, а также информацию о владельцах карт, группах владельцев карт, правилах доступа и зонах, с которыми связана дверь.
Отчет о доступе к зоне	Включает имя зоны, а также информацию о владельцах карт, группах владельцев карт, правилах доступа и дверях, с которыми связана зона.

Создание отчетов о действиях владельцев карт

Отчет о присутствии содержит список владельцев карт в определенной зоне в данный момент времени.

В отчете о сборе указываются владельцы карт в определенной зоне. Это помогает определить, кто находится в безопасности во время чрезвычайных ситуаций. Помогает управляющим зданиями в определении местонахождения персонала и посетителей после эвакуации. Пункт сбора - это специально отведенное место, где персонал должен отметится во время чрезвычайных ситуаций. Это позволяет сформировать отчет о присутствующих на территории и тех, кто покинул объект. Система отмечает владельцев карт как отсутствующих до тех пор, пока они не зарегистрируются в пункте сбора или пока кто-нибудь вручную не отметит, что они в безопасности.

Как для отчетов о сборе, так и для отчетов о присутствии требуется определить зоны отслеживания владельцев карт.

Создать и запустить отчет о сборе или присутствии:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Reports (Отчеты)** > **Cardholder activity (Действия владельцев карт)**.
3. Нажмите **+ Add (Добавить +)** и выберите **Roll call / Mustering (Сбор/присутствие)**.
4. Назовите отчет
5. Выберите зоны для отчета.
6. Выберите группы для отчета.
7. Если вам нужен отчет о сборе, выберите **Mustering point (Пункт сбора)** и считыватель для пункта сбора.
8. Выберите временные рамки для отчета.
9. Нажмите **Сохранить**.

10. Выберите отчет и нажмите **Run (Выполнить)**.

Состояние отчета о присутствии	Описание
Присутствует	Владелец карты вошел в указанную зону и не вышел из нее до того, как вы запустили отчет.
Не присутствует	Владелец карты вышел из указанной зоны и не входил в нее до того, как вы запустили отчет.

Состояние отчета о сборе	Описание
В безопасности	Владелец карты провел своей картой по считывателю в пункте сбора.
Отсутствуют	Владелец карты не провел карту по считывателю в пункте сбора.

Настройка параметров управления доступом

Чтобы настроить поля данных владельцев карт, которые должны использоваться в панели управления, предназначенной для управления доступом:

1. На вкладке **Access management (Управление доступом)** нажмите **Settings (Настройки)** > **Custom cardholder fields (Пользовательские поля держателя карты)**.
2. Выберите **+ Add (Добавить +)** и введите имя. Можно добавить до 6 пользовательских полей.
3. Нажмите **Добавить**.

Чтобы разрешить использование кода объекта для проверки вашей системы контроля доступа:

1. На вкладке **Access management (Управление доступом)** нажмите **Settings (Настройки)** > **Facility code (Код объекта)**.
2. Выберите **Facility code on (Вкл. код объекта)**.

Примечание

Также необходимо выбрать **Include facility code for card validation (Включить код объекта для проверки карты)** при настройке профилей идентификации. См. *Профили идентификации, on page 20*.

Чтобы отредактировать шаблон электронного письма для отправки QR-кода или мобильных учетных данных:

1. На вкладке **Access management (Управление доступом)** нажмите **Настройки** > **Email templates (Шаблоны электронной почты)**.
2. Измените свой шаблон и нажмите **Update (Обновить)**.

Импорт и экспорт

Импорт владельцев карт

Данная функция позволяет импортировать сведения о владельцах карт, группах владельцев карт, учетные данные и фотографии владельцев карт из CSV-файла. Чтобы импортировать фотографии владельцев карт, убедитесь в том, что сервер имеет доступ к фотографиям.

Когда вы импортируете владельца карт, система управления доступом автоматически сохраняет конфигурацию системы, включая все конфигурации оборудования, и удаляет все ранее сохраненные.

Можно также сопоставить пользователей в базе данных Active Directory в качестве владельцев карт. См. раздел *Настройки Active Directory[БЕТА], on page 28*.

Варианты импорта	
Новинка	При выборе этого варианта добавляются новые владельцы карт, а существующие удаляются.
Обновить	При выборе этого варианта обновляются существующие владельцы карт и добавляются новые а владельцы карт.
Добавить	При выборе этого варианта сохраняются существующие владельцы карт и добавляются новые. Номера карт и идентификаторы владельцев карт уникальны, они могут быть использованы только один раз.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Import cardholders (Импорт владельцев карт)**.
3. Выберите **New (Новые)**, **Update (Обновить)** или **Add (Добавить)**.
4. Нажмите **Next** ("Далее").
5. Нажмите **Choose a file (Выбрать файл)** и перейдите к файлу CSV. Нажмите кнопку **Открыть**.
6. Введите разделитель столбцов, выберите уникальный идентификатор и нажмите **Next (Далее)**.
7. Назначьте каждому столбцу заголовок.
8. Нажмите **Импорт**.

Настройки импорта	
Первая строка является заголовком	Выберите в том случае, если CSV-файл содержит заголовок столбца.
Разделитель столбцов	Введите формат разделителя столбцов для файла CSV.
Уникальный идентификатор	Для идентификации владельца карты по умолчанию система использует **Cardholder ID (Идентификатор владельца карты).** Можно также использовать его имя и фамилию или адрес электронной почты. Уникальный идентификатор предотвращает импорт дубликатов личных записей.
Формат номера карты	По умолчанию выбран параметр **Allow both hexadecimal and number (Разрешить шестнадцатеричный и числовой форматы).**

экспорт владельцев карт

Эта команда экспортирует имеющиеся в системе данные владельцев карт в файл в формате CSV.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Export cardholders (Экспорт владельцев карт)**.
3. Выберите место расположения загрузки и нажмите **Save (Сохранить)**.

AXIS Camera Station Pro Secure Entry обновляет фотографии владельцев карт в папке `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` при изменении конфигурации.

Отмена импорта

Система автоматически сохраняет свою конфигурацию при импорте владельцев карт. Параметр **Undo import (Отмена импорта)** сбрасывает данные владельца карты и всю конфигурацию оборудования до состояния, которое было до импорта последнего владельца карты.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Undo import (Отмена импорта)**.
3. Нажмите **Да**.

T10231644_ru

2026-02 (M4.3)