

AXIS Camera Station Pro Secure Entry

О программе

Secure Entry является компонентом AXIS Camera Station Pro. Используйте его для добавления устройств и управления расписаниями. Дополнительные сведения приведены 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 версию AXIS OS контроллера в 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. Инструкции по редактированию предварительно заданных профилей идентификации или созданию нового профиля см. в *Профили идентификации, on page 23*.
2. Чтобы использовать пользовательскую настройку для форматов карт и длины PIN-кода, см. *Форматы карт и ПИН-коды, on page 26*.
3. Добавьте дверь и примените профиль идентификации к двери. См. *Добавьте дверь, on page 8*.
4. Настройте дверь:
 - *Add a door position sensor (Добавление датчика положения двери), on page 14*
 - *Add an emergency sensor (Добавление датчика аварийной ситуации), on page 16*
 - *Добавление считывающего устройства, on page 17*
 - *Добавление REX-устройства, on page 19*
5. Добавьте зону и добавьте двери в зону. См. *Добавление зоны, on page 21*.

Совместимость программного обеспечения устройств для дверных контроллеров

Внимание

При обновлении AXIS OS на дверном контроллере учитывайте следующее:

- **Поддерживаемые версии AXIS OS:** перечисленные ниже поддерживаемые версии AXIS OS применяются только при обновлении с исходной рекомендуемой версии AXIS Camera Station Pro Secure Entry и при наличии в системе настроенной двери. Если система не соответствует этим условиям, необходимо обновить ее до рекомендуемой версии AXIS OS для конкретной версии AXIS Camera Station Pro Secure Entry.
- **Минимальная поддерживаемая версия AXIS OS:** самая старая установленная в системе версия AXIS OS определяет минимальную поддерживаемую версию AXIS OS с ограничением в две предыдущие версии. Предположим, вы используете версию AXIS Camera Station Pro Secure Entry 6.5 и обновляете все устройства до рекомендуемой версии AXIS OS 12.0.86.2. После этого версия AXIS OS 12.0.86.2 становится минимальной поддерживаемой версией системы в дальнейшем.
- **Обновление до версии AXIS OS выше рекомендуемой:** предположим, вы обновили систему до версии AXIS OS, более новой, чем рекомендуемая для определенной версии AXIS Camera Station Pro Secure Entry. После этого вы всегда можете без проблем выполнить откат до рекомендуемой версии AXIS OS, если она находится в пределах ограничений поддержки, установленных для версии AXIS Camera Station Pro Secure Entry.
- **Будущие рекомендации по AXIS OS:** всегда используйте рекомендуемую версию AXIS OS для

соответствующей версии AXIS Camera Station Pro Secure Entry, чтобы обеспечить стабильность системы и полную совместимость.

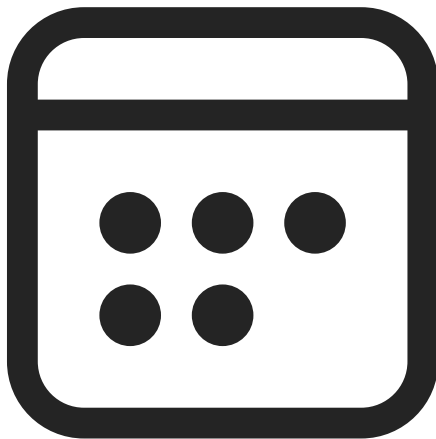
- **Изменение ветки:** для перехода с ветки 10.12.xx на ветку 11.0.xx или более позднюю требуется восстановление заводских настроек.

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 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Двери и зоны

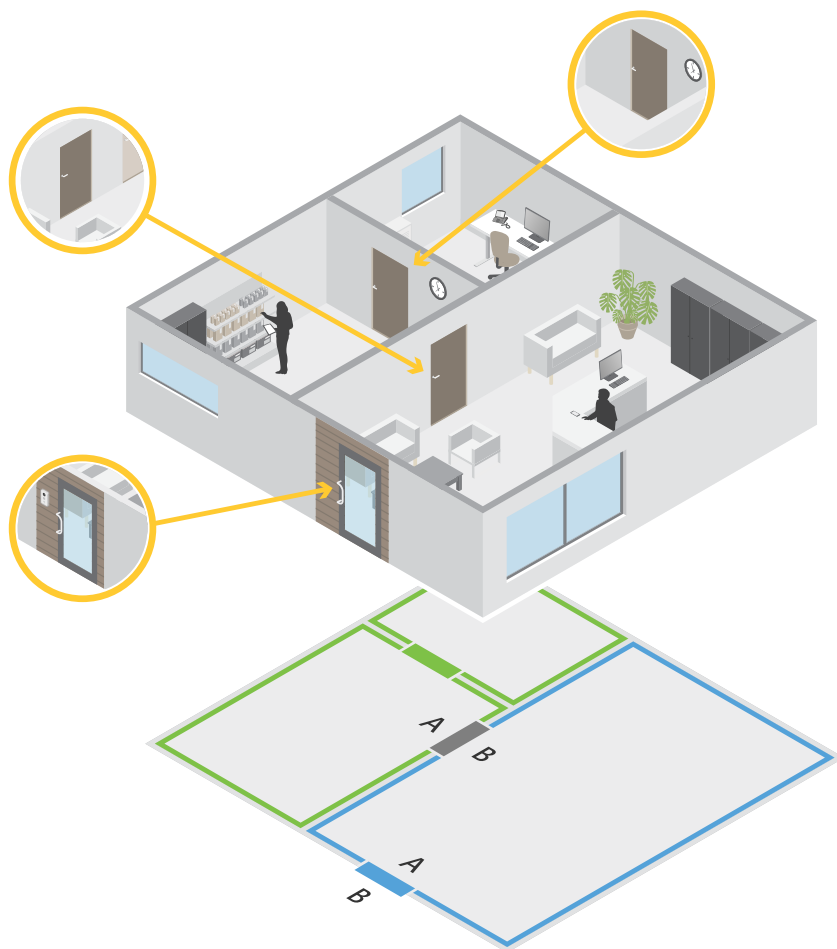
Перейдите в раздел **Configuration > Access control > Doors and zones** (Конфигурация > Контроль доступа > Двери и зоны > Зоны), чтобы получить обзор и настроить двери и зоны.

 Действия в ручном режиме	Задайте состояние двери вручную. Выберите один из следующих вариантов): Reset (Сбросить) (соблюдение правил системы), Grant access (Предоставить доступ), (разблокировка двери на 7 секунд), Unlock (Разблокировать), (оставить дверь незапертой), Lock (Заблокировать), (оставить дверь запертой) или Lockdown (Блокировка), (вход и выход запрещены).
 Расписания отпираания	Задайте расписание для автоматического отпираания дверей в определенное время. В остальное время двери остаются запертыми. Чтобы первый человек вручную открывал дверь перед активацией графика, включите функцию First person in (Первый входящий человек).
 Профиль идентификации	Изменить профиль идентификации для дверей.
 Схема контактов	Посмотреть схему контактов контроллера, связанную с дверью. Чтобы распечатать таблицу PIN-кодов, нажмите Print (Печать).
 Защищенный канал	Включение или выключение защищенного канала OSDP Secure Channel для конкретного считывателя.

Двери	
Название	Имя двери.
Тип	Тип конфигурации двери.

Устройство	Устройство, подключенное к двери.
IP-адрес	IP-адрес дверного контроллера, подключенного к двери.
Сторона А	Зона, в которой находится сторона А двери.
Сторона В	Зона, в которой находится сторона В двери.
Профиль идентификации	Профиль идентификации, применяемый к двери.
Батарея	Состояние батареи дверного контроллера.
Статус	Состояние двери. • Online (В сети): дверь находится в сети и работает исправно. • Reader offline (Считывающее устройство не в сети): Считывающее устройство в конфигурации двери не в сети. • Reader error (Ошибка считывающего устройства): считыватель не поддерживает защищенный канал или эта функция отключена для считывающего устройства. • Old firmware (Старая версия встроенного ПО): на устройстве установлена устаревшая версия встроенного ПО. Для оптимальной производительности и безопасности обновите встроенное ПО.
Зоны	
Название	Имя зоны.
Количество дверей	Количество дверей, включенных в зону.
Уровень безопасности	Уровень безопасности для данной зоны.

Пример конфигурации дверей и зон



- Имеются две зоны: зеленая зона и синяя зона.
- Имеются три двери: зеленая дверь, синяя дверь и коричневая дверь.
- 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.

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 разблокированной до выполнения сброса.

Блокировка – 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.
3. Нажмите на любое действие в ручном режиме.

Двери

Добавьте дверь

Примечание

- Для дверного контроллера можно настроить одну дверь с двумя замками либо же две двери с одним замком в каждой. Мультиконтроллеры поддерживают дополнительные конфигурации замков.

Чтобы добавить дверь:

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

Типы дверей	
Дверной датчик	Обычная дверь с контролем состояния двери, поддерживающая замки и считывающие устройства. Требуется дверной контроллер.
Этаж	Тип двери для управления лифтом, обеспечивающий аутентификацию доступа к этажам лифта с использованием считывающих устройств для идентификационных карт. Подробнее см. в разделе <i>Добавить этаж</i> ^{BETA} , on page 9.
Контролируемая дверь	Дверь, которая может сообщать, открыта она или закрыта. Подробнее см. в разделе <i>Добавление двери с мониторингом</i> , on page 10.
Беспроводная сеть	Дверь, которую можно настроить с беспроводными замками и коммуникационными хабами ASSA ABLOY Aperio®. Подробнее см. в разделе <i>Добавление беспроводной блокировки</i> , on page 10.
Выделенная дверь	Заполнитель двери, который можно добавить в систему без выбора аппаратного обеспечения.

3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери. Контроллер отображается неактивным, если добавить еще одну дверь невозможно, контроллер находится вне сети или HTTPS не включен.
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 23.
8. Настройте дверь, добавив датчики или считыватели в разделах **Sensors (Датчики)**, **Side A (Сторона A)** и **Side B (Сторона B)**.

9. Настройте параметры конкретной двери. См. *Настройки двери, on page 12*.
10. Нажмите **Save (Сохранить)**.

Копирование конфигурации двери:

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



Добавление и настройка дверей и зон

Добавить этаж ^{BETA}

Этаж — это тип двери, который используется для управления доступом к этажам лифта. При добавлении этажа вы создаете ресурс лифта, который группирует все этажи для этого лифта. Каждый этаж использует считывающее устройство для карт внутри кабины лифта для аутентификации пользователей перед предоставлением доступа к этому этажу.

Прежде чем начать, потребуется выполнить:

- Поддерживаемый сетевой дверной контроллер, добавленный в систему, например *AXIS A1610*, *AXIS A1710-B* или *AXIS A1810-B*.
- Модуль расширения ввода-вывода для дополнительных реле. Мы рекомендуем модель *AXIS A9920*.

Примечание

Эта функция находится на этапе бета-тестирования и в настоящее время поддерживает до 64 этажей и только считывающие устройства для карт.

Чтобы настроить этаж:

1. Перейдите в **Configuration > Access control > Doors and zones** (Конфигурация > Контроль доступа > Двери и зоны).
2. Нажмите **+ Add (Добавить)** и выберите **Floor (Этаж) ^{BETA}**.
3. Введите имя для этажа.
4. Выберите ваш контроллер.
5. Во вкладке **Elevator (Лифт)** выберите существующий лифт и нажмите **Create new elevator (Создать новый лифт)**, чтобы добавить новый, а затем введите имя.

6. В разделе **Side A (Сторона А)** выберите **Card reader (Считывающее устройство для карт)** и конфигурируйте считывающее устройство. **Side B (Сторона Б)** не подлежит конфигурации по соображениям безопасности.
7. Нажмите **Save and add new (Сохранить и добавить новый)**, чтобы добавить дополнительные этажи к тому же лифту. Конфигурация лифта и считывающего устройства остается неизменной для следующего этажа. Этот параметр доступен только при наличии реле в контроллере.
8. Нажмите **Save (Сохранить)** после добавления этажа. Этажи отображаются в формате «название лифта — название этажа», например: «West Side — Floor 1» (Западная сторона, этаж 1)

Примечание

- Считывающие устройства, используемые на нескольких этажах, можно редактировать только на первом этаже, на котором они были добавлены.
- Лифты автоматически удаляются, когда удаляются все связанные с ними этажи.

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**.

Добавление беспроводной блокировки

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



Для просмотра видео откройте веб-версию данного документа.

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.
 - Время на дверном контроллере Axis и сервере AXIS Camera Station Pro Secure Entry должно быть синхронизировано.
 - Прежде чем начать работу, необходимо выполнить сопряжение блокировок Aperio с концентратором Aperio, используя прикладное средство с поддержкой технологии ASSA ABLOY.
 - К каждому разъему RS485 можно подключить только один сетевой концентратор Aperio. Подключение нескольких устройств по одной линии не поддерживается.
 - В автономном режиме беспроводные замки не выполняют расписания разблокировки.
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 **ОК**.
 - 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. В разделе **Doors (Двери)** нажмите  **Add (Добавить)**.
 - 4.3. В качестве **Door type (Тип двери)** выберите **Wireless door (Беспроводная дверь)** и дверной контроллер, подключенный к коммуникационному концентратору Aperio.
 - 4.4. Нажмите **Next (Далее)**.
 - 4.5. Выберите **Wireless lock (Беспроводная блокировка)**.

- 4.6. Определите стороны двери А и В и добавьте нужные датчики. Дополнительную информацию вы найдете по адресу *Двери и зоны, on page 4*.
- 4.7. Нажмите **Save (Сохранить)**.

После подключения беспроводного замка в обзоре дверей отображаются уровень заряда его аккумулятора и состояние.

Уровень заряда аккумулятора	Действие
Хорошо	Нет
Низкая	Замок работает нормально, однако аккумулятор следует заменить до того, как его уровень заряда достигнет критического значения.
Критические ошибки	Замените аккумулятор. Блокировка, возможно, работает неправильно.

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

Настройки двери

Чтобы изменить параметры 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)**.
4. В разделе **Door settings (Настройки двери)** измените любые параметры и нажмите **Save (Сохранить)**.

Время доступа (с)	Задайте время в секундах, в течение которого дверь остается незапертой после предоставления доступа. Дверь снова запирается при закрытии, даже если заданное время еще не истекло.
Open-too-long time (sec) (Время «открыта слишком долго» (с))	Действительно только при настроенном датчике состояния двери. Задайте время в секундах, в течение которого дверь может оставаться открытой. Если по истечении заданного времени дверь остается открытой, срабатывает тревога о слишком длительном открытии двери. Настройте правило действия, определяющее реакцию системы на это событие.
Длительное время доступа (сек)	Задайте время в секундах, в течение которого дверь остается незапертой после предоставления доступа держателям карт, для которых включен этот параметр. Этот параметр имеет приоритет над стандартным временем доступа.
Long open-too-long time (sec) (Длительное время «открыта слишком долго» (с))	Действительно только при настроенном датчике состояния двери. Задайте время в секундах, в течение которого дверь может оставаться

	открытой для держателей карт, для которых включен Long access time (Увеличенное время доступа) . Переопределяет стандартное время слишком длительного открытия двери.
Время задержки повторного запираения (мс)	Задайте время в миллисекундах, в течение которого дверь остается незапертой после ее открытия или закрытия.
Повторная блокировка	• After opening (После открытия): действительно только при добавленном датчике состояния двери. • After closing (После закрытия): действительно только при добавленном датчике состояния двери.
Дверь открыта силой	Выберите, должна ли система формировать системную тревогу при принудительном открытии двери. Требуется датчик положения двери (DPS).
Дверь открыта слишком долго	Выберите, должна ли система формировать системную тревогу, если дверь остается открытой слишком долго.

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. Нажмите  **Remove (Удалить)** и подтвердите.

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 прикладывание карты позволяет держателю карты изменить текущее состояние двери. Например, с его помощью можно запереть или разблокировать дверь вне установленного расписания, что удобнее разблокировки двери через систему. Двойное прикладывание карты не влияет на существующее расписание. Например, если по расписанию дверь должна запирается в конце рабочего дня, а сотрудник выходит на обеденный перерыв, дверь все равно заперется согласно расписанию.

Уровень безопасности можно настроить при добавлении новой двери или применить его к 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 А и сторона В	Выберите, с какой стороны двери будет использоваться правило.
Расписания	Выберите время, в которое будет действовать правило.
Время тайм-аута (в секундах)	Тайм-аут — максимально допустимый интервал между прикладываниями карты или другими действительными предъявлениями 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 — максимально допустимый интервал между прикладываниями карты или другими действительными предъявлениями учетных данных.

Add a door position sensor (Добавление датчика положения двери)

Датчик положения двери — это переключатель, отслеживающий физическое состояние двери. К двери можно добавить датчик положения двери и настроить способ его подключения.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 8*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Door position sensor (Датчик положения двери)**.
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 устранениядребезга)**.

7. Чтобы при разрыве соединения между контроллером двери и датчиком положения двери срабатывало событие, включите **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 15*.

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.

Контролируемые входы

Контролируемые входы могут инициировать событие при разрыве соединения с дверным контроллером.

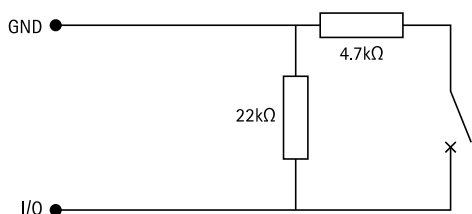
- Соединение между дверным контроллером и дверным монитором. См. *Add a door position sensor (Добавление датчика положения двери), on page 14*.
- Соединение между дверным контроллером и считывающим устройством, которое использует протоколы Wiegand. См. *Добавление считывающего устройства, on page 17*.
- Соединение между дверным контроллером и устройством REX. См. *Добавление REX-устройства, on page 19*.

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 K Ω parallel resistor and a 4.7 K Ω 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)**.

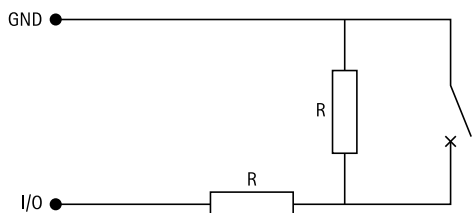
Параллельное соединение

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.



Add an emergency sensor (Добавление датчика аварийной ситуации)

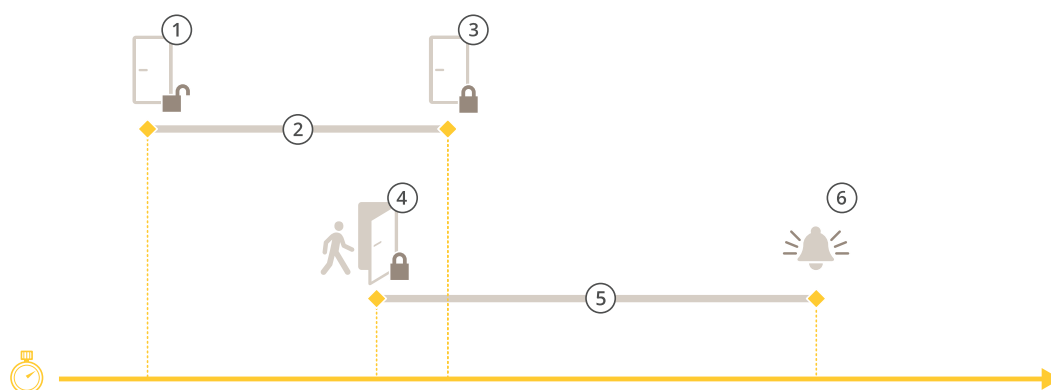
Вы можете добавить и настроить аварийный вход для инициирования действия, которое блокирует или разблокирует дверь. Можно также настроить способ подключения цепи.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 8*.
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 устранениядребезга (мс))**.
6. Выберите **Emergency action (Действие при чрезвычайной ситуации)**, которое должно запускаться при поступлении на дверь сигнала чрезвычайной ситуации.

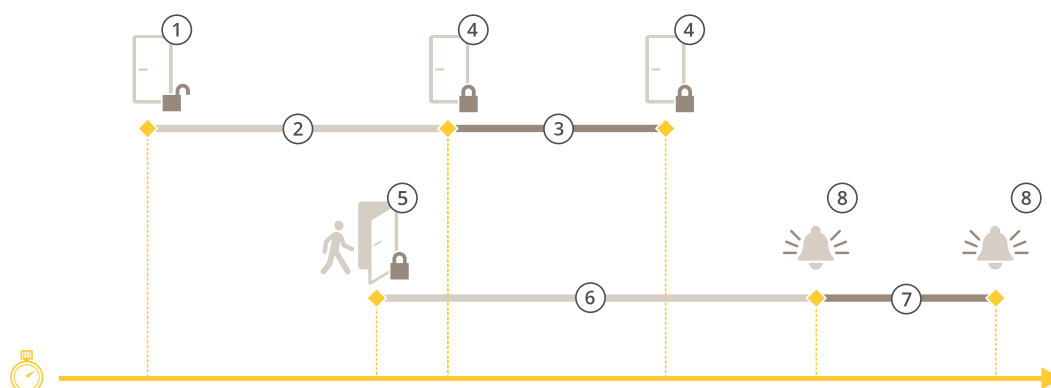
Аварийное состояние	
Цепь разомкнута	Ко входу чрезвычайной ситуации подключена нормально замкнутая цепь. Сигнал чрезвычайной ситуации отправляется на вход чрезвычайной ситуации, когда цепь размыкается.
Цепь замкнута	Ко входу чрезвычайной ситуации подключена нормально разомкнутая цепь. Сигнал чрезвычайной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

Параметры времени



- 1 Доступ предоставлен — замок отпирается
- 2 Время доступа
- 3 No action taken - lock stays locked (Действие не выполняется — замок остается запертым)
- 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 No action taken - lock stays locked (Действие не выполняется — замок остается запертым)
- 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 считывающего устройства

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

Если применить к считывателю пользовательскую настройку форматов карт или длины PIN-кода, она отображается в **Card formats (Форматы карт)** в разделе **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**. См. *Двери и зоны, on page 4*.

Примечание

- К дверному контроллеру можно добавить до 16 считывающих устройств Bluetooth. Дополнительные сведения см. в разделе *Добавление считывающего Bluetooth-устройства, on page 20*.
 - Если в качестве IP-считывателя используется сетевое переговорное устройство Axis, система использует конфигурацию PIN-кода, заданную на веб-странице устройства.
1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 8*.
 2. Для одной стороны двери нажмите **Add (Добавить)**.
 3. Выберите **Card reader (Устройство для считывания карт)**.
 4. Выберите **Reader type (Тип считывающего устройства)**.
 5. Для использования пользовательской длины PIN-кода для этого 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. Если настройка формата карты отличается от настроек, заданных в системе, в клиенте отображается значок предупреждения.
 7. Нажмите **Добавить**.
 8. Чтобы добавить считывающее устройство с другой стороны двери, повторите эту процедуру.

Сведения об установке AXIS Barcode Reader см. в *Установка считывателя штрих-кодов AXIS, on page 25*.

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. Сетевые переговорные устройства Axis можно использовать в качестве IP-считывающих устройств.

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 состояние цепи, при котором активируется вход контроля вскрытия считывающего устройства.

	• 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 устранениядребезга 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 устранениядребезга для обнаружения несанкционированных действий) .
Контролируемый вход	Включите параметры, чтобы при прерывании соединения между дверным контроллером и считывающим устройством инициировалось событие. См. <i>Контролируемые входы, on page 15</i> .

Добавление REX-устройства

С одной или обеих сторон двери можно добавить устройство запроса на выход (REX). В качестве REX-устройства может использоваться пассивный ИК-датчик, REX-кнопка или толкающий рычаг.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 8*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите REX-устройство.
4. Выберите порт ввода-вывода, к которому необходимо подключить устройство REX. Если доступен только один порт, он выбирается 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 устранениядребезга (мс))**.
8. Чтобы при разрыве соединения между дверным контроллером и устройством REX срабатывало событие, включите **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 15*.

Действие	
Отпереть дверь	Выберите, чтобы отпереть дверь при приеме сигнала REX.
Нет	Выберите этот параметр, чтобы не выполнять никаких действий при получении дверью сигнала REX.

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 IP-считывателя

В качестве считывателя можно использовать сетевой интерком Axis или другое IP-устройство. Перед назначением устройства на дверь нужно добавить его в AXIS Camera Station Pro.

Примечание

Перед началом работы убедитесь, что IP-считыватель включен и подключен к той же сети, что и AXIS Camera Station Pro.

1. Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Add devices (Добавить устройства)**.
2. Выберите IP-считыватель из списка обнаруженных устройств и нажмите **Add (Добавить)**.
3. При появлении запроса введите учетные данные устройства.

После добавления устройства его можно назначить на дверь. См. *Добавление считывающего устройства, on page 17*.

Добавление считывающего Bluetooth-устройства

С помощью сетевого Bluetooth-считывающего устройства AXIS A4612 можно расширить возможности проводного подключения дверных контроллеров Axis. К одному дверному контроллеру можно подключить до 16 таких считывающих устройств. Каждый считыватель способен управлять замком двери, кнопкой выхода (REX) и датчиком положения двери (DPS).

Для добавления и использования этих считывающих устройств дополнительные лицензии не требуются.

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 20*.
2. Перейдите на страницу конфигурации двери. См. раздел *Добавьте дверь, on page 8*.
3. С одной стороны двери нажмите  **Add (Добавить)**, затем **Card reader (Считыватель карт)**.
4. Выберите **IP-считыватель**, затем выберите сопряженный AXIS A4612 из выпадающего списка. Если это считывающее устройство используется для сопряжения учетных данных, установите для него признак использования 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).

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 Secure Entry.
 - 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)** со стороны двери, где расположен Bluetooth-считыватель.
 - 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 23*.
6. Добавьте мобильный пропуск для владельца карты. См. *Добавить учетные данные, on page 35*.
7. Выполните сопряжение мобильного пропуска со считывающим устройством:
 - 7.1. Поднесите мобильный телефон держателя карты к Bluetooth-считывателю с включенным режимом сопряжения.
 - 7.2. Следуйте инструкциям из электронного письма, отправленного владельцу карты.

Зоны

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 периметра)**: держатели карт входят в зону или выходят из нее через эту дверь.
- **Internal door (Внутренняя дверь)**: внутренняя дверь в пределах зоны.

Примечание

Дверь по периметру может принадлежать двум зонам. Внутренняя дверь может принадлежать только одной зоне. Обзор см. в разделе *Пример конфигурации дверей и зон, on page 7*.

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. По умолчанию для двери периметра сторона А является стороной входа в зону. Чтобы изменить сторону, выберите **Leave (Выход)** в раскрывающемся меню.
8. Для удаления двери из зоны выберите нужную дверь и нажмите **Remove (Удалить)**.
9. Нажмите **Save (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 использованием тех же реквизитов для входа, которые были введены другими людьми, выполнившими вход в зону до них. Перед повторным использованием учетных данных человек должен выйти из области.

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.

Уровень безопасности можно настроить при добавлении новой зоны или применить его к существующей зоне. 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 необходимые функции безопасности для зоны.
6. Нажмите Применить.

Запрет на повторный проход	
Log violation only (Soft) (Только нарушение в журнале (мягкое))	Выберите этот параметр, чтобы разрешить второму человеку войти с использованием тех же учетных данных, что и первый человек. Данный вариант приводит только к подаче сигнала тревоги в системе.
Deny access (Hard) (Запрет доступа (строгий))	Выберите этот параметр, чтобы запретить второму человеку входить с использованием тех же учетных данных, 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, чтобы отключить тайм-аут. В этом случае защита от повторного прохода действует до тех пор, пока пользователь не покинет 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.

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.

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).

Доступные профили идентификации:

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.

PIN-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 является зарегистрированным товарным знаком Denso Wave Incorporated в Японии и других странах.

Создание профиля идентификации

1. Перейдите к пункту **Configuration > Access control > Identification profiles** (Конфигурация > Контроль доступа > Профили идентификации).
2. Нажмите **+ Create identification profile** (Создать профиль учетных данных).
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. Для стороны А нажмите **+ Add** (Добавить), выберите тип идентификации и расписание.
 - Чтобы требовать от держателей карт использование более чем одного типа идентификации, выберите несколько типов в одной строке.
 - Чтобы разрешить владельцам карт использовать любой из типов, снова нажмите **+ Add** (Добавить) и добавьте еще одну строку.
6. Для стороны В нажмите **+ Add** (Добавить), выберите тип идентификации и расписание.
7. Нажмите кнопку **ОК**.



Настройка профилей идентификации

Редактирование профиля 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 **ОК**.

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.

Удаление профиля 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 **ОК**.

Сброс 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 .

Считыватель штрих-кодов AXIS

Считыватель штрих-кодов **AXIS Barcode Reader** — это приложение, которое можно установить на камерах Axis. Дверной контроллер Axis использует внешний ключ аутентификации периферийных устройств для предоставления доступа и аутентификации **AXIS Barcode Reader** и **AXIS License Plate Verifier**. Полный порядок настройки **AXIS License Plate Verifier** в **AXIS Camera Station Pro** см. в разделе

Установка считывателя штрих-кодов AXIS

1. Загрузите файл установки приложения с веб-сайта axis.com.
2. Перейдите на веб-страницу вашего переговорного устройства или камеры Axis.
3. Установите приложение.
4. Активируйте лицензию.
5. Запустите приложение.
6. Мы рекомендуем изменить следующую настройку камеры для повышения точности QR.
 - 6.1. Перейдите к настройкам камеры.
 - 6.2. В разделе **Image > Exposure** (Изображение > Экспозиция) переместите ползунок **Blur-noise trade-off** (Оптимум между размытием и шумом) в среднее положение.

Настройка считывателя штрих-кодов AXIS

1. Чтобы изменить профиль идентификации QR-кода перейдите к пункту **Configuration > Access control > Identification profiles** (Конфигурация > Контроль доступа > Профили идентификации) и нажмите . См. *Профили идентификации*.
2. Добавьте дверь. См. раздел *Add a door* (Добавление двери).
3. Выберите **QR** в качестве профиля идентификации для данной двери. См. *Настройка параметров двери*.

4. Добавьте считыватель штрих-кодов. См. *Добавление считывающего устройства*.
 - 4.1. Для одной стороны двери нажмите **Add reader** (Добавить считыватель).
 - 4.2. Выберите **AXIS Barcode Reader** (Считыватель штрих-кодов AXIS) в раскрывающемся списке **Reader type** (Тип считывающего устройства). Введите имя и нажмите кнопку **OK**.

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. Включите **AXIS Camera Station Secure Entry**.
 - 2.4. Нажмите **Add** (Добавить), введите IP-адрес дверного контроллера и вставьте ключ для проверки подлинности.
 - 2.5. Выберите считывающее устройство, выполняющее считывание штрих-кодов из раскрывающегося меню двери.

Форматы карт и ПИН-коды

Формат карты определяет способ интерпретации считывателем данных с карты. Доступны предварительно заданные форматы карт, которые можно использовать или редактировать, а также можно создавать пользовательские форматы карт.

Перейдите к пункту **Configuration > Access Control > Card formats and PIN** (Конфигурация > Контроль доступа > Форматы карт и ПИН-коды). На странице есть две вкладки:

Конфигурация PIN-кода – Задайте длину PIN-кода и последний символ PIN-кода.

Форматы карт – Просматривайте, создавайте, редактируйте, удаляйте и активируйте форматы карт.

Форматы карт

В таблице перечислены все доступные форматы карт со следующей информацией:

Используется	Активен ли формат. Одновременно может быть активен только один формат для каждой длины в битах.
Наименование формата карты	Название формата карты.
Длина в битах	Длина формата карты в битах.
Источник	Является ли формат System default (Системный по умолчанию) или Custom (Пользовательский), созданным вами.

Добавление формата карты

1. Перейдите в Configuration (Конфигурация) > Access control (Контроль доступа) > Card formats and PIN (Форматы карт и PIN-код).
2. Нажмите **+** Add (Добавить).
3. Введите имя и длину в битах от 1 до 256.
4. Если порядок следования битов в данных, получаемых от считывателя карт, нужно менять на обратный, выберите пункт **Invert bit order** (Инвертировать порядок битов).
5. 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.
6. Включите **Card number** (Номер карты), **Facility code** (Код объекта) или оба параметра. В формате карты должен быть активен хотя бы один из них.
7. Задайте диапазон битов данных для поля данных. Диапазон должен находиться в пределах заданной длины в битах.
8. Выберите выходной формат данных для поля данных.
 - Десятичный: Десятичная система счисления. В ней используются цифры 0–9.
 - Шестнадцатеричный: Шестнадцатеричная система счисления. В ней используются 16 символов: цифр от 0 до 9 и букв от a до f.
9. Выберите порядок следования битов.
 - Прямой порядок байтов: Первый бит является наименьшим, то есть младшим значащим битом.
 - Обратный порядок байтов: Первый бит является наибольшим, то есть старшим значащим битом.
10. Нажмите кнопку ОК.

Примечание

- Нельзя одновременно активировать два формата карт с одинаковой длиной в битах. Например, если вы определили два 32-битных формата карт, активным может быть только один из них. 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.
- Предварительно заданные форматы карт можно редактировать, но нельзя удалять. Чтобы отменить изменения в предварительно заданном формате, выберите значок сброса, чтобы восстановить настройки по умолчанию. Созданные вами форматы карт можно удалять.



Настройка форматов карт

Редактирование формата 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 .

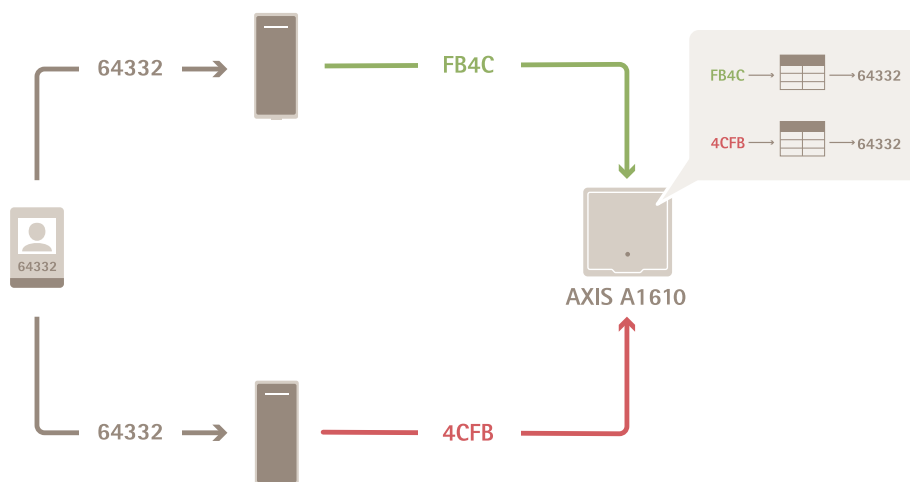
3. Если вы редактируете предопределенный формат карты, вы можете редактировать только Инвертирование порядка битов и Инвертирование порядка байтов.
4. Нажмите кнопку ОК.

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).

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.

64332 = 1111 1011 0100 1100 $\longrightarrow$ 0011 0010 1101 1111 = 13023

$\longrightarrow$ Read from left Read from right $\longleftarrow$

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.

$$64\ 332 = \begin{matrix} 1111 & 1011 & 0100 & 1100 \\ \text{F} & \text{B} & 4 & \text{C} \end{matrix} \longrightarrow \begin{matrix} 0100 & 1100 & 1111 & 1011 \\ 4 & \text{C} & \text{F} & \text{B} \end{matrix} = 19707$$

Стандартный 26-битный формат карты Wiegand



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

PIN-код

Задайте минимальную и максимальную длину PIN-кода. Если для минимальной и максимальной длины заданы разные значения, укажите завершающий символ PIN-кода, обозначающий окончание ввода PIN-кода.

1. Перейдите в Configuration (Конфигурация) > Access Control (Контроль доступа) > Card formats and PIN (Форматы карт и PIN-код) > PIN configuration (Настройка PIN-кода).
2. Введите Min PIN length (Минимальная длина PIN-кода) и Max PIN length (Максимальная длина PIN-кода).
3. При необходимости введите End of PIN character (Завершающий символ PIN-кода).
4. Нажмите кнопку OK.

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 основной ключ шифрования используется для создания ключа защищенного канала OSDP. 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*.

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. По умолчанию это порт 55767. Сведения о настройке пользовательских портов см. в разделе *General server settings (Общие настройки сервера)*.
- Подключение вспомогательного сервера к основному серверу приводит к замене его ключа считывающего устройства, что делает все существующие учетные данные Bluetooth недействительными. Чтобы избежать этого, создавайте учетные данные Bluetooth на основном сервере, а не на вспомогательном.

Последовательность операций

1. Настройте сервер в качестве подсервера и создайте файл конфигурации. См. *Создание файла конфигурации на подсервере, on page 30*.
2. Настройте сервер в качестве основного сервера и импортируйте файл конфигурации для подсерверов. См. *Импорт файла конфигурации на основной сервер, on page 30*.
3. Настройте глобального владельца карты и группы владельцев карт на основном сервере. См. *Добавление владельца карты, on page 33* и *Добавление группы, on page 38*.
4. Просмотр и наблюдение за глобальными владельцами карт и группами владельцев карт с подсервера. См. *Контроль доступа, on page 33*.

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. Дополнительную информацию 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 31*.

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 35*.

Внимание

Если отключить пользователя в Active Directory, AXIS Camera Station Pro безвозвратно удаляет держателя карты и все связанные с ним данные, включая историю. Это действие нельзя отменить. Чтобы заблокировать доступ держателя карты без потери его данных, приостановите его учетную запись в AXIS Camera Station Pro вместо отключения пользователя в Active Directory.

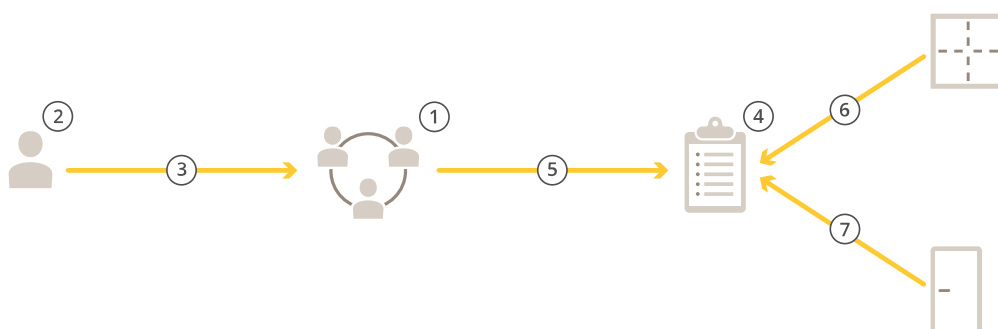
Контроль доступа

Используйте вкладку **Access management (Управление доступом)** для настройки и управления держателями карт, группами и правилами доступа в системе.

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

Рабочий процесс управления доступом

Структура системы управления доступом является гибкой, поэтому можно разработать рабочий процесс в соответствии с вашими потребностями. Пример рабочего процесса:



1. *Добавление группы, on page 38.*
2. *Добавление владельца карты, on page 33.*
3. *Добавьте владельцев карт в группы.*
4. *Добавление правила доступа, on page 38.*
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 держателя карты, указав учетные данные, идентифицирующие человека, а также определив, когда и каким образом ему разрешен доступ через двери.

Пользователей из базы данных Active Directory также можно сопоставить с держателями карт. См. *Настройки Active Directory^{BETA}, on page 31.*

1. Откройте вкладку  **Access management (Управление доступом)**.
2. Перейдите в **Cardholder management (Управление держателями карт) > Cardholders (Держатели карт)** и нажмите **+ Add (Добавить)**.
3. Введите имя и фамилию владельца карты. При необходимости можно добавить дополнительные сведения о владельце карты.
 - В поле **Email (Электронная почта)** введите адрес электронной почты владельца карты.
 - В поле **Groups (Группы)** выберите группы, в которые вы хотите добавить владельца карты.
 - В поле **Access rules (Правила доступа)** выберите правила доступа, которые будут применяться ко владельцу карты.

4. Чтобы добавить фотографию, нажмите **Cardholder picture** (Фотография владельца карты) и выберите подходящий вариант:
 - **Upload** (Загрузить файл), чтобы добавить изображение со своего устройства.
 - **Capture** (Сделать снимок), чтобы сделать снимок с помощью камеры.

Примечание

Поддерживаемые форматы изображения: JPG, PNG или GIF. Размер изображений автоматически изменяется до максимального значения 700×700 пикселей, затем файлы конвертируются в формат JPG.

5. Нажмите на кнопку **Advanced** (Расширенные настройки), чтобы настроить дополнительные параметры.
6. Добавьте учетные данные владельца карты. См. *Добавить учетные данные, on page 35*.
7. Нажмите **Save** (Сохранить).
8. Чтобы распечатать пропуски, выберите одного или нескольких держателей карт и нажмите **Print Badge**^{BETA} (Печать пропуска ^{BETA}). Дополнительную информацию см. в разделе *Печать бейджа ^{BETA}, on page 44*.

Вы можете найти владельца карты по имени или фамилии, используя строку поиска. Чтобы фильтровать список по источнику, нажмите **Filter** (Фильтр) выберите **Local** (Локально), **Global** (Глобально), **AD** или **Center** (Центр).

Расширенный набор	
Длительное время доступа	Выберите этот параметр, чтобы предоставить держателю карты увеличенное время доступа и увеличенное время допустимого открытия двери при наличии установленного датчика состояния двери.
Приостановить владельца карты	Выберите, чтобы приостановить владельца карты. Этот параметр временно отменяет все права доступа держателя карты.
Разрешить двойной свайп	Выберите, чтобы разрешить владельцу карты переопределять текущее состояние двери. Например, держатель карты может использовать этот параметр для разблокировки двери вне установленного расписания.
Исключение из блокировки	Выберите этот параметр, чтобы предоставить держателю карты доступ при блокировке.
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. <i>Мультисерверная ^{BETA}-версия, on page 30</i> .



Для просмотра видео откройте веб-версию данного документа.

Добавление владельцев карт и групп

Добавить учетные данные

Владельцу карты можно назначить следующие типы учетных данных:

- Учетные данные на основе QR-кода, *on page 35*
- PIN-код, *on page 36*
- Учетные данные карты, *on page 36*
- Учетные данные номерного знака, *on page 36*

Дата окончания срока действия	
Действует с	Задайте дату и время, начиная с которых учетные данные становятся действительными.
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 действия учетных данных после последнего использования. Выберите количество дней, месяцев или лет после последнего использования.

Учетные данные на основе QR-кода

Примечание

Для использования QR-кодов в качестве учетных данных необходимо синхронизировать время на системном контроллере и камере с AXIS Barcode Reader. Для синхронизации времени рекомендуется использовать один и тот же источник времени для обоих устройств.

Чтобы добавить данные QR-кода владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **QR-код**.
2. Введите имя для учетных данных.
3. Параметр **Динамический QR-код** включен по умолчанию. Его необходимо использовать вместе с учетными данными **PIN-код**.
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**.

PIN-код

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. При необходимости для активации скрытой тревоги с отдельным PIN-кодом включите **Duress PIN (PIN-код принуждения)** и задайте PIN-код принуждения.
4. Задайте даты **Valid from (Действует с)** and **Valid to (Действует до)** для учетных данных.
5. Нажмите **Добавить**.

Мобильный пропуск

Примечание

Держатель карты должен иметь адрес электронной почты для получения мобильных учетных данных.

Учетные данные карты

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить)** и выберите **Card (Карта)**.
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 еще 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 readers (Получить последние считанные данные карты с дверных считывающих устройств)**.

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**.

Учетные данные номерного знака

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**.

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. *Добавление устройств*.
2. Обновите прошивку на новых устройствах до последней доступной версии. См. *Обновление микропрограммы*.
3. Добавьте новую дверь, подключенную к вашему дверному контроллеру. См. *Добавьте дверь, on page 8*.
 - 3.1. Добавьте считывающее устройство на сторону А. См. *Добавление считывающего устройства, on page 17*.
 - 3.2. 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.
 - 3.3. Дополнительно можно также добавить считывающее устройство или устройство, обрабатывающее запросы на выход, на сторону В.
 - 3.4. Нажмите кнопку **OK**.
4. Установите на камеру AXIS License Plate Verifier и выполните активацию. См. руководство пользователя *AXIS License Plate Verifier*.
5. Запустите AXIS License Plate Verifier.
6. Настройте AXIS License Plate Verifier.
 - 6.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
 - 6.2. 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)**.
 - 6.3. Откройте AXIS License Plate Verifier из веб-интерфейса камеры.
 - 6.4. Пропустите мастер настройки.
 - 6.5. Выберите в меню **Settings (Настройки)**.
 - 6.6. В разделе **Access control (Контроль доступа)** выберите **Secure Entry** в качестве значения **Type (Тип)**.
 - 6.7. В поле **IP address (IP-адрес)** введите IP-адрес дверного контроллера.
 - 6.8. В поле **Authentication key (Ключ аутентификации)** вставьте скопированный ранее ключ аутентификации.
 - 6.9. Нажмите **Подключить**.
 - 6.10. В разделе **Door controller name (Имя дверного контроллера)** выберите нужный дверной контроллер.
 - 6.11. В разделе **Reader name (Имя считывающего устройства)** выберите добавленное вами ранее считывающее устройство.
 - 6.12. Включите интеграцию.
7. Добавьте держателя карты, которому необходимо предоставить доступ. См. *Добавление владельца карты, on page 33*
8. Добавление данных номерного знака для нового владельца карты. См. *Добавить учетные данные, on page 35*

9. Добавление правила доступа. См. *Добавление правила доступа, on page 38*.
 - 9.1. Добавление расписания.
 - 9.2. Добавьте держателя карты, которому необходимо предоставить доступ к номерным знакам.
 - 9.3. Добавьте дверь со считывающим устройством AXIS License Plate Verifier.

Добавление группы

Группы позволяют совместно управлять держателями карт и их правилами доступа.

1. Откройте вкладку  Access management (Управление доступом).
2. Перейдите в Cardholder management (Управление держателями карт) > Groups (Группы) и нажмите  Add (Добавить).
3. Введите название и, по желанию, инициалы для группы.
4. Выберите Global group (Глобальная группа), чтобы просматривать держателей карт на подчиненных серверах и отслеживать их состояние. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 30*.
5. Добавление в группу владельцев карт:
 - 5.1. Нажмите  Add (Добавить).
 - 5.2. Выберите владельцев карт, которых вы хотите добавить, и нажмите Add (Добавить).
6. Нажмите Save (Сохранить).
7. Чтобы распечатать пропуски для всех держателей карт в группе, выберите группу и нажмите Print Badge БЕТА (Печать пропуска БЕТА). Дополнительную информацию см. в разделе *Печать бейджа БЕТА, on page 44*.

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.

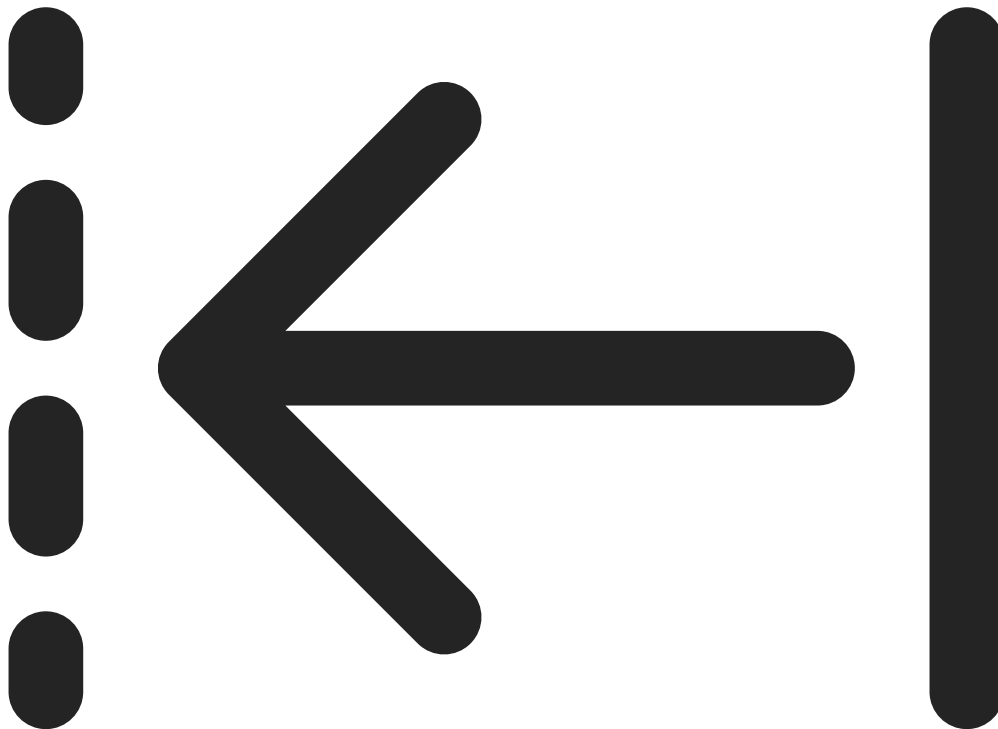
Двери и зоны – где применяется правило доступа.

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 (Держатели карт) или Groups (Группы) нажмите **+** Add (Добавить).

5.2. Выберите владельцев карт или группы и нажмите Add (Добавить).

5.3. Вы также можете перетащить запись владельца карты или группу прямо в поле правила доступа, чтобы применить правило к нужным пользователям. Правила доступа, на которые можно перетащить элементы, выделяются. Если вы перетаскиваете сразу нескольких владельцев карт или групп, будет показано количество перемещаемых объектов.

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 **Save (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

Можно экспортировать отчеты, содержащие различные типы информации о системе. AXIS Camera Station Pro Secure Entry экспортирует отчеты в виде CSV-файла с разделителями-запятыми и сохраняет их в папке загрузок 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 карт	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 карт	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 зданием находить

сотрудников и посетителей после эвакуации. Место сбора — назначенное считывающее устройство, на котором персонал отмечается в чрезвычайных ситуациях. Система формирует отчет о лицах, находящихся на территории и за ее пределами. 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 (Переключка / Сбор персонала).
4. Назовите отчет
5. Выберите зоны для отчета.
6. Выберите группы для отчета.
7. Если требуется отчет о сборе персонала, выберите Mustering point (Место сбора) и считывающее устройство.
8. Выберите временные рамки для отчета.
9. Нажмите Save (Сохранить).
10. Выберите отчет и нажмите Run (Выполнить).

Состояние отчета о присутствии	Описание
Присутствует	Держатель карты вошел в указанную зону и не вышел из нее до формирования отчета.
Не присутствует	Держатель карты вышел из указанной зоны и не вошел в нее снова до формирования отчета.

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.

Импорт и экспорт

Импорт владельцев карт

Этот параметр позволяет импортировать держателей карт, группы, учетные данные и фотографии из CSV-файла. Чтобы импортировать фотографии владельцев карт, убедитесь в том, что сервер имеет доступ к фотографиям.

При импорте держателей карт система управления доступом автоматически сохраняет конфигурацию системы, включая всю конфигурацию оборудования, и удаляет ранее сохраненную конфигурацию.

Пользователей из базы данных Active Directory также можно сопоставить с держателями карт. См. *Настройки Active Directory^{BETA}, on page 31.*

Варианты импорта	
Новинка	Удаляет существующих держателей карт и добавляет новых.
Обновить	Обновляет существующих держателей карт и добавляет новых.
Добавить	Сохраняет существующих держателей карт и добавляет новых. 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)**, найдите CSV-файл и нажмите **Open (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. Используйте этот параметр, чтобы предотвратить импорт дублирующих записей о сотрудниках.
Формат номера карты	Параметр Allow both hexadecimal and number (Разрешить шестнадцатеричные и числовые значения) по умолчанию включен.

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 (Отменить импорт)** восстанавливает данные держателей карт и всю конфигурацию оборудования в состояние, в котором они находились до последнего импорта.

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

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. Нажмите **+ 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

При настройке профилей идентификации также необходимо выбрать **Include facility code for card validation (Учитывать код объекта при проверке карты)**. См. *Профили идентификации, on page 23*.

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)**.

Шаблоны бейджей ^{BETA}

Вы можете настроить шаблоны бейджей с информацией о владельце карты, фотографиями, логотипами и индивидуальным брендингом. Для создания нового шаблона:

1. Перейдите в **Access management (Управление доступом) > Settings (Настройки) > Badge templates (Шаблоны бейджа) ^{BETA}**.
2. Нажмите **Create new template (Создать новый шаблон)**.
3. Введите название в поле **Template name (Название шаблона)**.
4. Выберите **Use as default template for printing (Использовать по умолчанию для печати)**, чтобы сделать этот шаблон шаблоном по умолчанию.
5. Настройте дизайн бейджа:
 - Выберите до пяти текстовых полей для отображения на лицевой стороне, включая любые настраиваемые поля, которые вы создали. При печати на бейдже будут отображаться только заполненные поля.
 - Выберите шрифт и цвет для текста.
 - Добавьте цвет фона или изображение.

- Загрузите логотип вашей организации.
 - Для обратной стороны добавьте либо цвет фона, либо изображение.
6. Нажмите **Save (Сохранить)**, чтобы сохранить изменения, или **Save as (Сохранить как)**, чтобы создать новый шаблон.

Примечание

После того, как шаблон был создан, его нельзя изменить, только переименовать.

Печать бейджа ^{BETA}

Вы можете печатать идентификационные бейджи для владельцев карт, используя настроенные шаблоны бейджей. Кодирование карт в настоящее время не поддерживается. Прежде чем начать, убедитесь в следующем:

- Убедитесь, что у владельца карты есть хотя бы одни учетные данные карты. Вы не можете печатать бейджи для владельцев карт без учетных данных.
- Необходим принтер с поддержкой размера карт CR80 и совместимых материалов для печати, например плотного картона.
- Настройте параметры печати в вашем браузере:
 1. Установите размер страницы на CR80 или пользовательский размер, соответствующий размерам вашей карты.
 2. Установите ориентацию на «Портрет».
 3. Отключите поля или установите для них минимальное значение.

Внимание

Функция Secure Entry (Безопасный вход) работает с принтерами, для которых доступны драйверы Windows. Работоспособность подтверждена для принтеров серии HID Fargo. Если вам нужен драйвер для принтера, обратитесь к поставщику принтера.

Для печати бейджей:

1. Перейдите в **Access management (Управление доступом) > Cardholder management (Управление владельцами карт) > Cardholders (Владельцы карт)**.
2. Выберите одного или несколько владельцев карт.
3. Нажмите **Print badge (Печатать бейдж) ^{BETA}**.
4. Нажмите **Select template (Выбрать шаблон)** и в раскрывающемся списке **Template (Шаблон)** выберите нужный шаблон пропуска.
5. Если у держателя карты несколько учетных данных карты, выберите один вариант в раскрывающемся списке **Card (Карта)**.
6. Нажмите кнопку **Print (Печать)**.

Примечание

Если ваш принтер не поддерживает двустороннюю печать, сначала распечатайте все страницы лицевой стороны, затем переверните стопку карт и загрузите их в лоток снова, чтобы распечатать оборотные страницы.

T10231644_ru

2026-07 (M8.5)

© 2025 – 2026 Axis Communications AB