Руководство по настройке и работе с модулем интеграции Suprema 2

ACFA-Интеллект

Обновлено 20/06/2025

Содержание

1 Введение в Руководство по настройке и работе с модулем интеграции Suprema 2

На странице:

1.1 Назначение документа

Документ *Руководство по настройке и работе с модулем интеграции Suprema 2* является справочно-информационным пособием и предназначен для специалистов по настройке и операторов модуля *Suprema 2*. Данный модуль входит в состав системы контроля и управления доступом, реализованной на основе программного комплекса *ACFA-Интеллект*.

В данном Руководстве представлены следующие материалы:

1. общие сведения о модуле интеграции *Suprema 2*;
2. настройка модуля интеграции *Suprema 2*;
3. работа с модулем интеграции *Suprema 2*.

1.2 Общие сведения о модуле интеграции *Suprema 2*

Модуль интеграции *Suprema 2* является компонентом *СКУД*, реализованной на базе программного комплекса *ACFA-Интеллект* и предназначен для обеспечение взаимодействия *СКУД Suprema 2* с ПК *ACFA-Интеллект* (мониторинг, управление).

Примечание.

Подробные сведения о СКУД *Suprema 2* приведены в официальной справочной документации по данной системе (производитель Suprema Inc.).

Перед настройкой модуля интеграции *Suprema 2* необходимо выполнить следующие действия:

1. Установить аппаратные средства *СКУД Suprema 2* на охраняемый объект.
2. Подключить оборудование *Suprema 2* к Серверу.
3. Установить программное обеспечение *BioStar 2* на Сервер (ПО доступно на официальном сайте производителя);
4. Настроить подключение *СКУД Suprema 2* к Серверу *BioStar 2* (настройка утилиты *BioStar 2* приведена в официальной документации).

2 Поддерживаемое оборудование и лицензирование модуля Suprema 2

Производитель	Suprema 17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Republic of Korea www.supremainc.com
Тип интеграции	SDK
Подключение оборудования	Ethernet

Поддерживаемое оборудование

Оборудование	Назначение
BSA2-OEPW	Биометрический терминал (считыватель)
FaceStation 2	Биометрический терминал (считыватель)
BioStation 2	Биометрический терминал (считыватель)
BioStation 3	Биометрический терминал (считыватель)
BioEntry W	Биометрический терминал (считыватель)
CoreStation	Контроллер
BioEntry P2	Биометрическое устройство (считыватель)
XPass 2	Считыватель
FaceStation F2 всех исполнений	Биометрический терминал (считыватель) с возможностью получения температуры от Suprema Thermal Camera
X-Station 2 всех исполнений	Терминал (считыватель) с возможностью работать с QR-кодами
XPass S2	Считыватель

Примечание

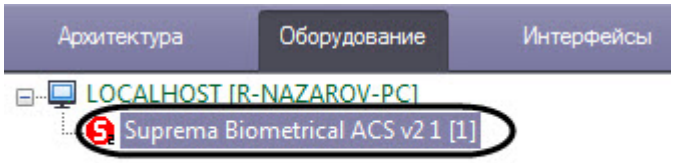
Поддерживаются все устройства, поддерживаемые SDK v.2. В таблице указаны те, работа с которыми была проверена отделом контроля качества ITV.

Защита модуля
За считыватель.

3 Настройка модуля интеграции Suprema 2

3.1 Активация модуля интеграции Suprema 2

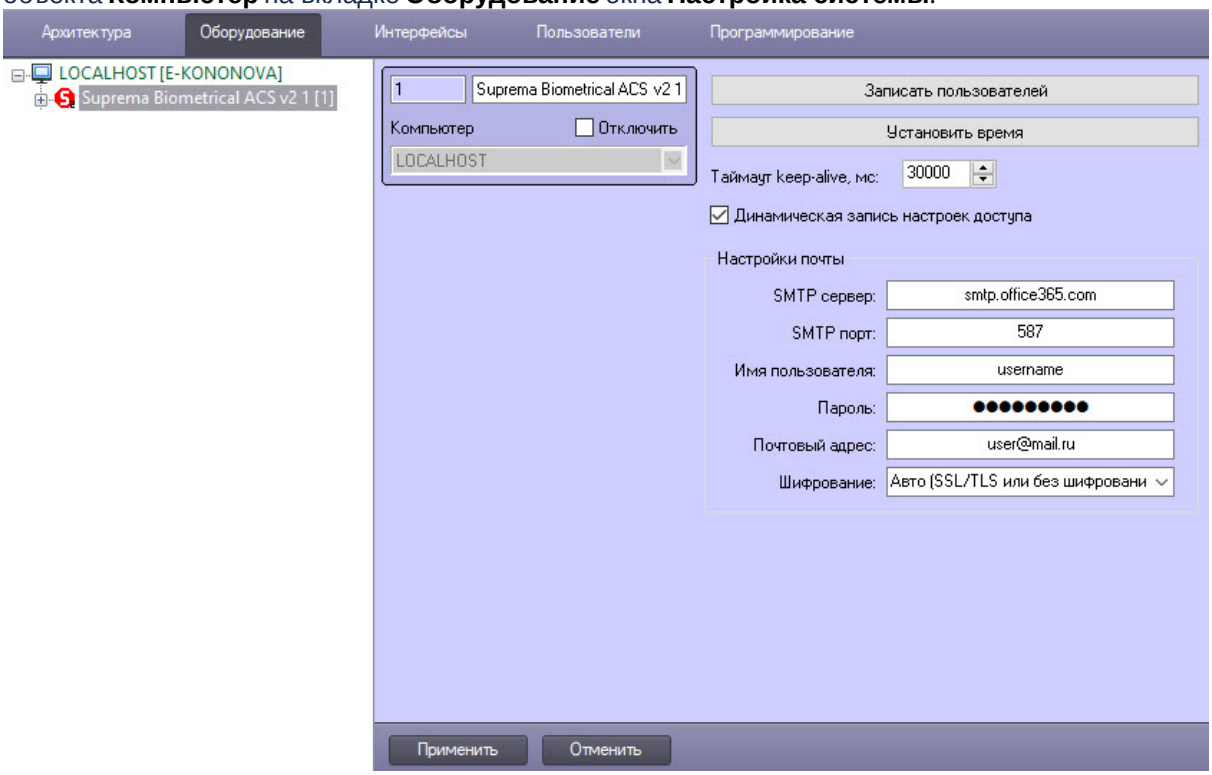
Для активации модуля интеграции *Suprema 2* необходимо на базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Suprema Biometrical ACS v2**.



3.2 Настройка головного объекта Suprema 2

Для настройки головного объекта *Suprema 2*:

1. Перейти на панель настроек объекта **Suprema Biometrical ACS v2**, который создается на базе объекта **Компьютер** на вкладке **Оборудование** окна **Настройка системы**.



2. Для записи пользователей во все контроллеры нажать кнопку **Записать пользователей**.
3. Для синхронизации времени всех контроллеров со временем компьютера нажать кнопку **Установить время**.
4. Таймаут установить в поле **Таймаут keep-alive, мс**. Значение по умолчанию – **30000** мс.
5. Для динамической записи настроек доступа пользователей установить флажок **Динамическая запись настроек доступа**.

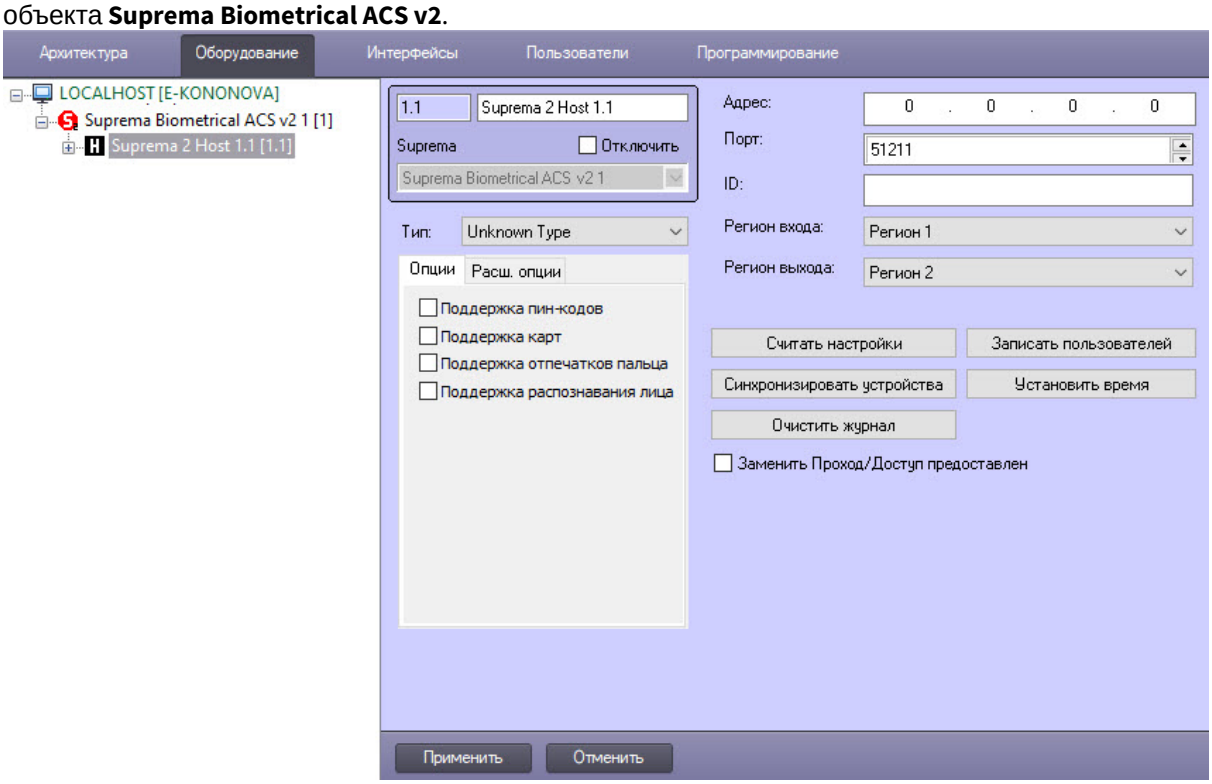
6. Для отправки QR-кодов по электронной почте:
   a. В поле **SMTP сервер** указать адрес SMTP-Сервера исходящей почты.
   b. В поле **SMTP порт** указать номер порта, используемого сервером исходящей почты.
   c. В поле **Имя пользователя** указать имя учетной записи, используемой для отправки сообщений на сервере исходящей почты.
   d. В поле **Пароль** указать пароль учетной записи на сервере исходящей почты.
   e. В поле **Почтовый адрес** указать адрес электронной почты, с которого будут отправляться сообщения.
   f. Из раскрывающегося списка **Шифрование** выбрать тип используемого шифрования: **Нет**, **Авто (SSL/TLS или без шифрования)** (используется по умолчанию), **SSL или TLS**, **STARTTLS**.
   Если отправка QR-кодов не требуется, этот шаг можно пропустить.
7. Нажать кнопку **Применить** для сохранения изменений.

Настройка головного объекта *Suprema 2* завершена.

3.3 Настройка контроллера Suprema 2

Для настройки контроллера *Suprema 2*:

1. Перейти на панель настройки объекта **Suprema 2 Host**, который создается на базе объекта **Suprema Biometrical ACS v2**.



2. В поле **Адрес** указать IP-адрес контроллера *Suprema 2*.
3. В поле **Порт** указать порт подключения контроллера *Suprema 2*.
4. В поле **ID** указать ID контроллера, подключенного по Ethernet.
5. Из раскрывающегося списка **Регион входа** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения входа.
6. Из раскрывающегося списка **Регион выхода** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения выхода.

> **Примечание**
>
> Поля **Регион входа** и **Регион выхода** должны быть обязательно заполнены, если используется входящая в *Бюро пропусков* подсистема *Учет рабочего времени*. В противном случае эти поля следует оставить пустыми.

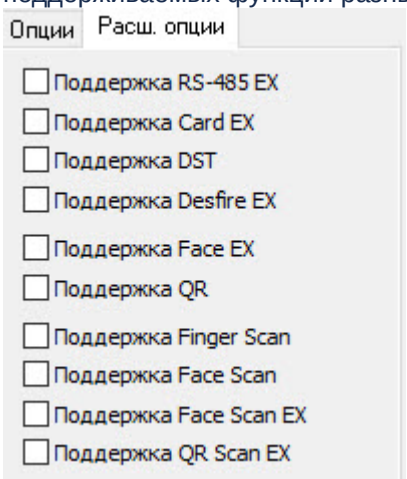
7. Нажать кнопку **Считывание настроек** для считывания текущих настроек контроллера, при этом также автоматически определяется его **Тип**. В зависимости от определенного типа контроллера меняются особенности его работы. Например, для контроллеров типа Xpass S2 меняется алгоритм работы модуля для вычитки событий и записи пользователей, т.к. при обычном алгоритме события приходят с задержкой и долго идет запись пользователей.

   > **Внимание!**
   >
   > Менять вручную настройку **Тип** не рекомендуется.

8. Нажать кнопку **Синхронизировать устройства** для автоматического создания в ПК *ACFA-Интеллект* дерева устройств, подключенных к контроллеру.
9. Нажать кнопку **Очистить журнал** для очистки журнала событий контроллера.
10. Нажать кнопку **Записать пользователей** для записи пользователей в контроллер.
11. Нажать кнопку **Установить время** для синхронизации времени контроллера с временем компьютера.
12. Настроить отправку события при успешном доступе: **Заменить проход/Доступ предоставлен**. Флажок снят – генерируется событие **Проход**, в противном случае – событие **Доступ предоставлен**.

    > **Примечание**
    >
    > Настройка необходима для работы подсистемы *Учет рабочего времени* модуля *Бюро пропусков* при наличии одного терминала доступа.

13. При считывании настроек (шаг 7) автоматически выставляются флажки на вкладке **Опции** с базовыми функциями устройства и вкладке **Расш. опции** с расширенными функциями устройства. Данные вкладки не редактируются и отображают функциональные особенности конкретного типа контроллера *Suprema 2*. Для каждого типа контроллера *Suprema 2* набор поддерживаемых функций разный. Вкладка **Расш. опции** имеет вид:



14. Нажать кнопку **Применить** для сохранения изменений.

Настройка контроллера *Suprema 2* завершена.

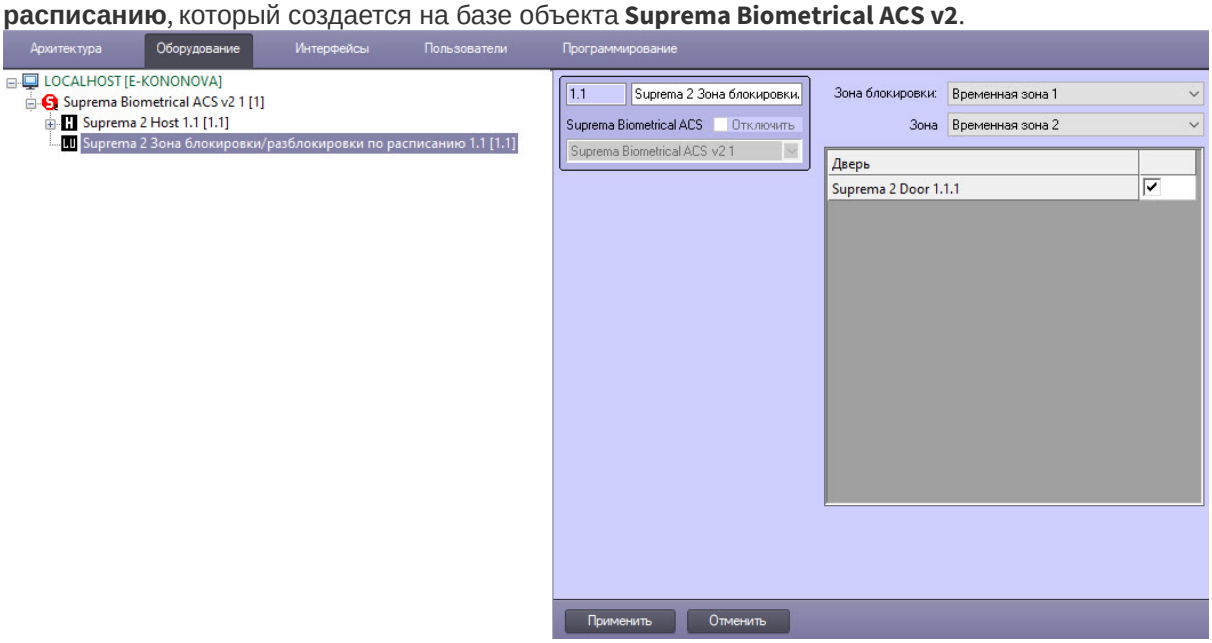
3.4 Настройка зон блокировки/разблокировки по расписанию модуля Suprema 2

На странице:

3.4.1 Настройка зон блокировки/разблокировки по расписанию

Для настройки зон блокировки/разблокировки по расписанию:

1. Перейти на панель настройки объекта **Suprema 2 Зона блокировки/разблокировки по расписанию**, который создается на базе объекта **Suprema Biometrical ACS v2**.



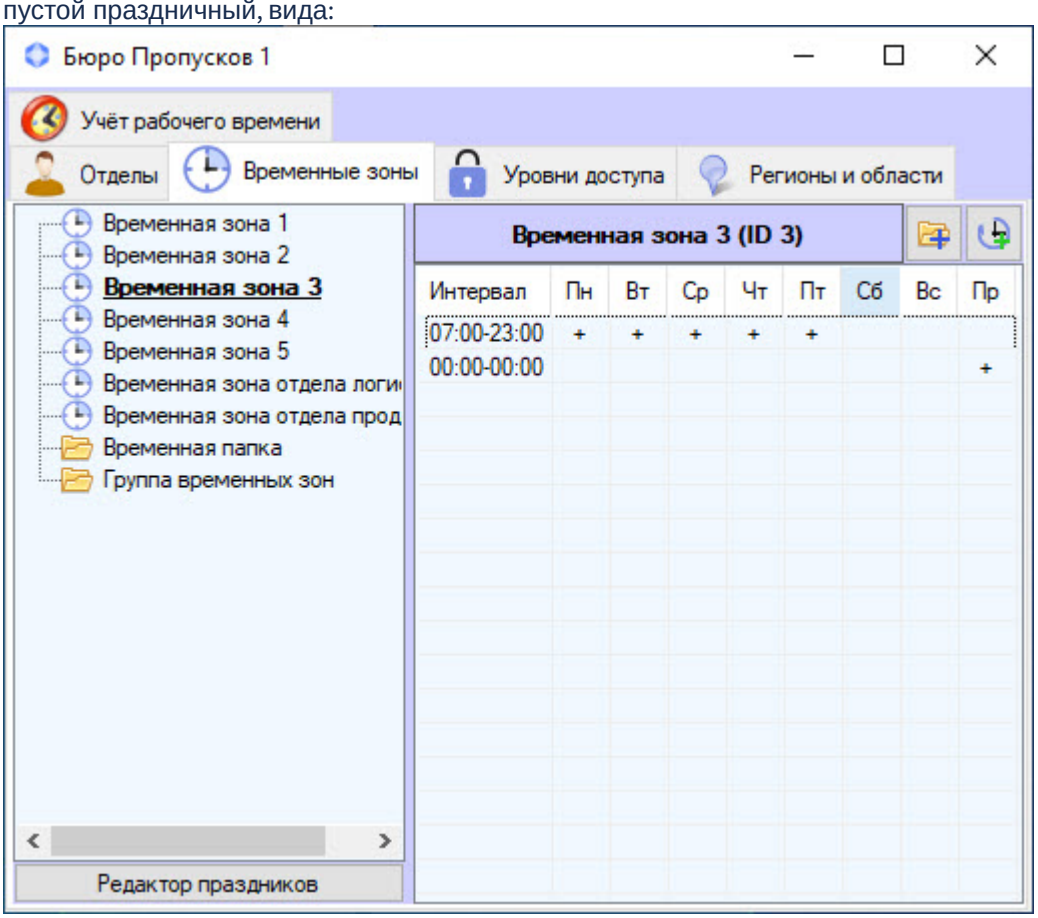
2. Из раскрывающегося списка **Зона блокировки** выбрать временную зону блокировки указанных дверей по расписанию.
3. Из раскрывающегося списка **Зона** выбрать временную зону разблокировки указанных дверей по расписанию.
4. Выбрать двери для блокировки/разблокировки по расписанию, установив соответствующие флажки.
5. Для сохранения изменений нажать кнопку **Применить**.
6. Перейти на панель настройки объекта **Suprema 2 Host**.
7. Нажать кнопку **Записать пользователей** для записи пользователей в контроллер (подробнее см. на странице Настройка контроллера Suprema 2).

Зоны блокировки/разблокировки по расписанию настроены.

3.4.2 Особенности добавления праздничных дней для ВЗ разблокировки дверей

Для добавления во временную зону разблокировки дверей праздничных дней требуется:

1. Создать временную зону (ВЗ) с 2 интервалами, первый из которых основной рабочий. а второй пустой праздничный, вида:



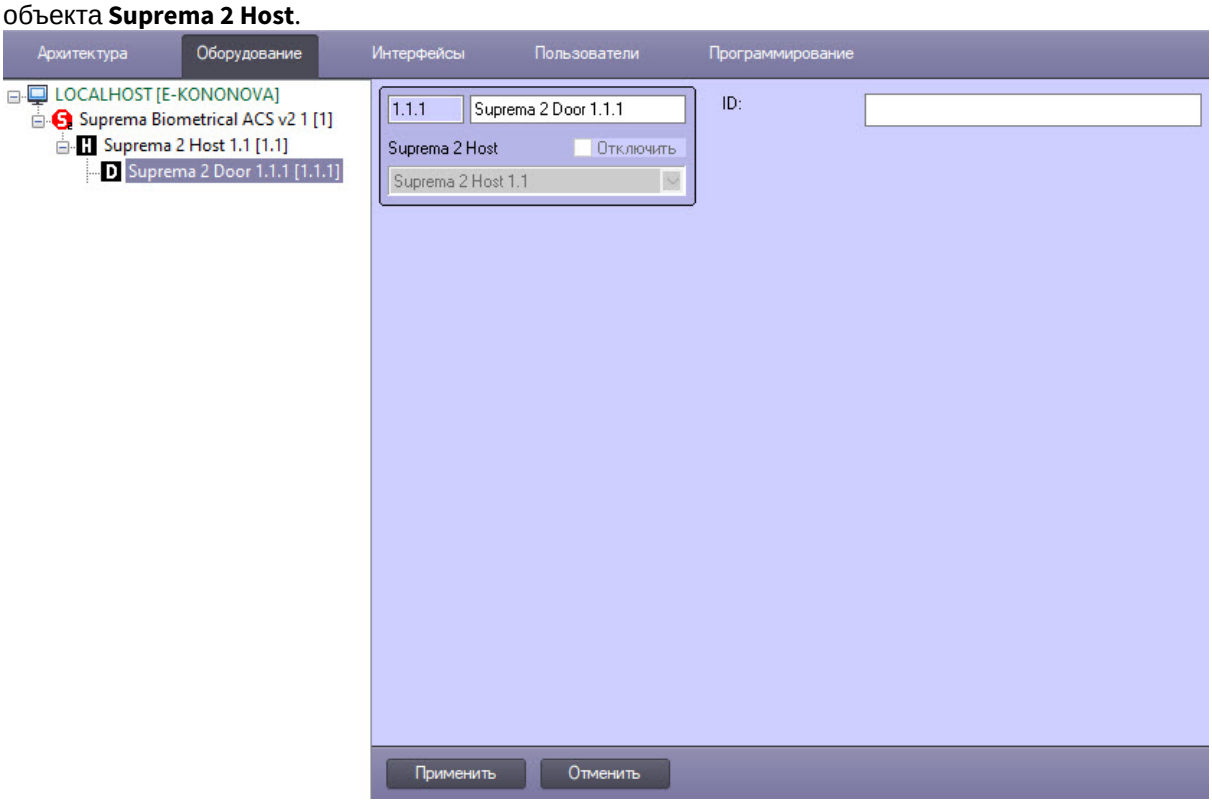
2. Добавить созданную ВЗ как зону разблокировки (параметр **Зона**) на панели настройки объекта **Suprema 2 Зона блокировки/разблокировки по расписанию**, зону блокировки при этом оставить пустой.
   При такой настройке дверь не будет разблокирована в этот день при условии, что этот день был определен как праздничный в системе.

Праздничный день добавлен во временную зону разблокировки дверей.

3.5 Настройка точки доступа Suprema 2

Для настройки точки доступа *Suprema 2*:

1. Перейти на панель настройки объекта **Suprema 2 Door**, который создается на базе объекта **Suprema 2 Host**.



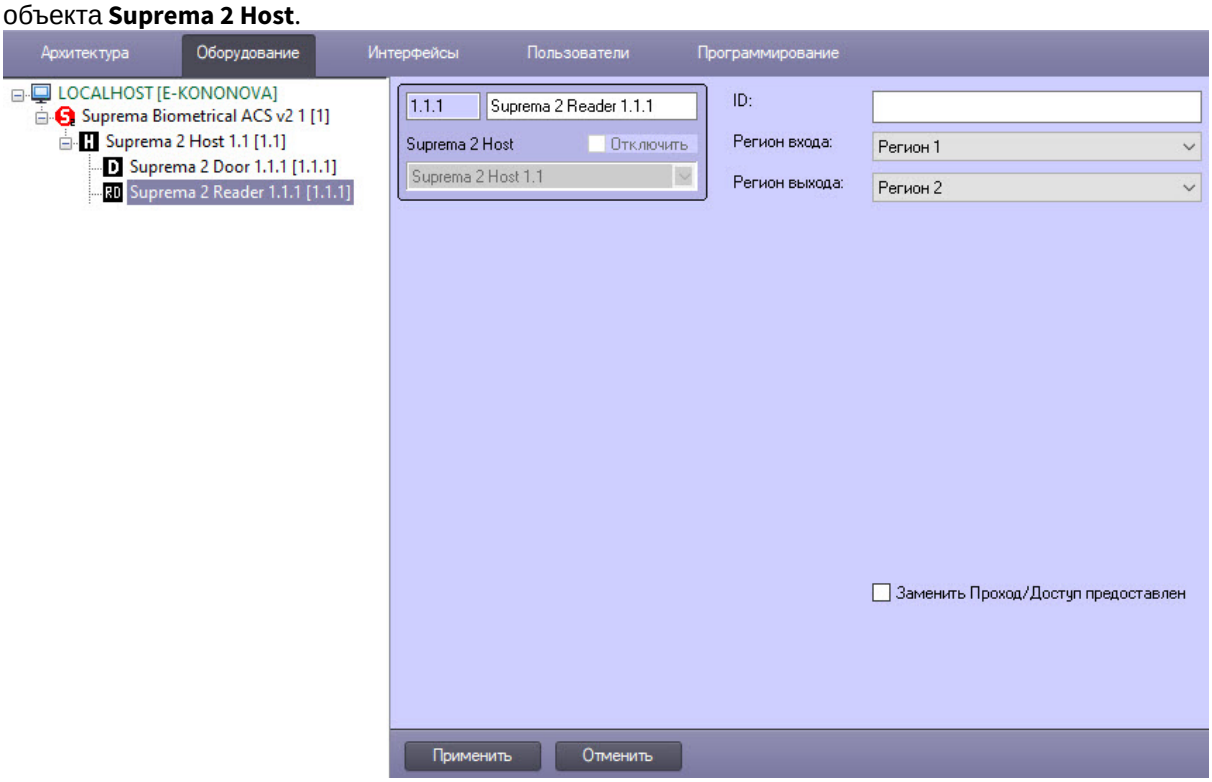
2. В поле **ID** указать идентификационный номер точки доступа.
3. Для сохранения изменений нажать кнопку **Применить**.

Настройка точки доступа *Suprema 2* завершена.

3.6 Настройка считывателя Suprema 2

Для настройки считывателя *Suprema 2*:

1. Перейти на панель настройки объекта **Suprema 2 Reader**, который создается на базе объекта **Suprema 2 Host**.



2. В поле **ID** указать идентификационный номер считывателя.
3. Из раскрывающегося списка **Регион входа** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения входа.
4. Из раскрывающегося списка **Регион выхода** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения выхода.

> **Примечание**
>
> Поля **Регион входа** и **Регион выхода** должны быть обязательно заполнены, если используется входящая в *Бюро пропусков* подсистема *Учет рабочего времени*. В противном случае эти поля следует оставить пустыми.

5. Настроить отправку события при успешном доступе: **Заменить проход/Доступ предоставлен**. Флажок снят – генерируется событие **Проход**, в противном случае – событие **Доступ предоставлен**.
6. Нажать кнопку **Применить** для сохранения изменений.

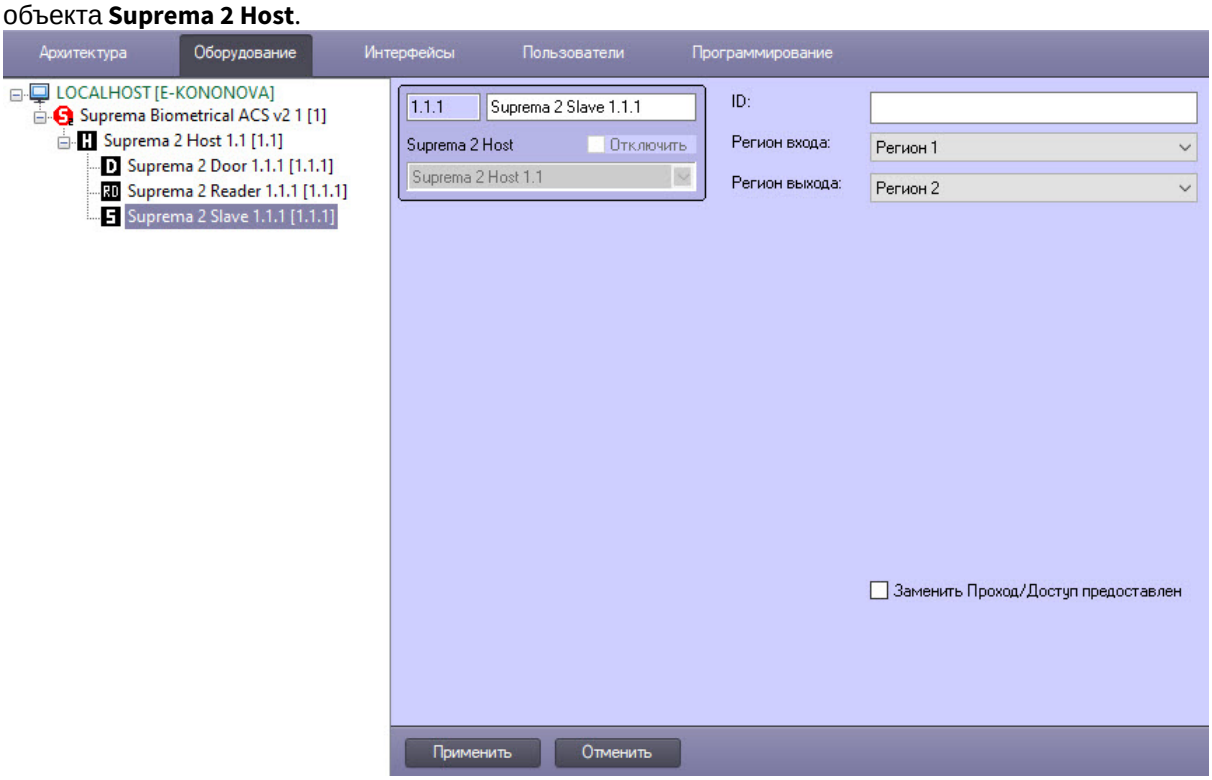
Настройка считывателя *Suprema 2* завершена.

3.7 Настройка зависимого контроллера Suprema 2

К контроллеру *Suprema 2* могут подключаться один или несколько контроллеров, образующие Master-Slave режим, в котором зависимый контроллер выступает в роли считывателя, а решение о предоставлении доступа принимает Master контроллер (подробнее см. в официальной справочной документации по данной системе (производитель Suprema Inc.)).

Настройка зависимого контроллера *Suprema 2* происходит так:

1. Перейти на панель настройки объекта **Suprema 2 Slave**, который создается на базе объекта **Suprema 2 Host**.



2. В поле **ID** указать идентификационный номер контроллера.
3. Из раскрывающегося списка **Регион входа** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения входа.
4. Из раскрывающегося списка **Регион выхода** выбрать Раздел, соответствующий территории, на которой окажется пользователь после совершения выхода.

> **Примечание**
>
> Поля **Регион входа** и **Регион выхода** должны быть обязательно заполнены, если используется входящая в *Бюро пропусков* подсистема *Учет рабочего времени*. В противном случае эти поля следует оставить пустыми.

5. Настроить отправку события при успешном доступе: **Заменить проход/Доступ предоставлен**. Флажок снят – генерируется событие **Проход**, в противном случае – событие **Доступ предоставлен**.
6. Нажать кнопку **Применить** для сохранения изменений.

Настройка зависимого контроллера *Suprema 2* завершена.

3.8 Особенности настройки пользователей интеграции Suprema 2

> **Внимание!**
>
> При создании уровня доступа в модуле *Бюро пропусков* необходимо в качестве точки доступа выбирать объекты **Suprema 2 Door** соответствующих контроллеров, к которым должен быть

доступ (см. Работа с уровнями доступа в Бюро пропусков). Если в качестве точки доступа выбрать объекты **Suprema 2 Host**, то такой УД работать не будет.

Настройка дополнительных параметров пользователя происходит в модуле *Бюро пропусков* (подробнее см. Руководство по настройке и работе с модулем Бюро пропусков). Для этого в режиме редактирования пользователя определить следующие дополнительные параметры:

1. **Suprema 2 Card Auth Mode** – определяет логику поведения системы:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Only Card** – пользователь может получить доступ только по карте;
   - **Card And Fingerprint** – пользователь может получить доступ, если сначала предъявит карту, а затем отпечаток пальца;
   - **Card And Pin** – пользователь может получить доступ, если сначала он предъявит карту, а затем введет ПИН-код;
   - **Fingerprint Or Pin After Card** – пользователь может получить доступ, если предъявит отпечаток пальца или введет ПИН-код после предъявления карты;
   - **Card And Fingerprint And Pin** – пользователь может получить доступ, если предъявит карту, затем отпечаток пальца и введет ПИН-код, и только в данной последовательности действий;
   - **Cannot Use** – пользователь всегда получает доступ, предоставив карту.

Suprema 2 Card Auth Mode	☐	Default
Suprema 2 Ex Card Auth Mode	☐	Default
Suprema 2 Ex Face Auth Mode	☐	Default
Suprema 2 Ex Finger Auth Mode	☐	Default
Suprema 2 Ex Id Auth Mode	☐	Default
Suprema 2 Faces	☐	0
Suprema 2 Finger Auth Mode	☐	Default
Suprema 2 Id Auth Mode	☐	Default
Suprema 2 Operator Level	☐	None
Suprema 2 QR Code	☐	
Suprema(2) Fingerprints	☐	0
Suprema(2) Security Level	☐	Default

2. **Suprema 2 Ex Card Auth Mode** – определяет логику авторизации с помощью карты доступа:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Card** – пользователь может получить доступ по карте;
   - **Card → Face** – пользователь может получить доступ, если сначала предъявит карту, а затем пройдет проверку лица на соответствие сохраненной фотографии;
   - **Card → Fingerprint** – пользователь может получить доступ, если сначала предъявит карту, а затем – отпечаток пальца;
   - **Card → Pin** – пользователь может получить доступ, если сначала предъявит карту, а затем введет ПИН-код;
   - **Card → Face or Fingerprint** – пользователь может получить доступ, если сначала предъявит карту, а затем пройдет проверку лица на соответствие сохраненной фотографии или предъявит отпечаток пальца;
   - **Card → Face or Pin** – пользователь может получить доступ, если сначала предъявит карту, а затем пройдет проверку лица на соответствие сохраненной фотографии или введет ПИН-код;
   - **Card → Fingerprint or Pin** – пользователь может получить доступ, если сначала предъявит карту, а затем предъявит отпечаток пальца или введет ПИН-код;
   - **Card → Face or Fingerprint or Pin** – пользователь может получить доступ, если сначала предъявит карту, а затем пройдет проверку лица на соответствие сохраненной фотографии, или предъявит отпечаток пальца, или введет ПИН-код;

- **Card → FaceFingerprint** – пользователь может получить доступ, если сначала предъявит карту, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого предъявит отпечаток пальца;
- **Card → Face → Pin** – пользователь может получить доступ, если сначала предъявит карту, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого введет ПИН-код;
- **Card → Fingerprint → Face** – пользователь может получить доступ, если сначала предъявит карту, затем предъявит отпечаток пальца, а после этого пройдет проверку лица на соответствие сохраненной фотографии;
- **Card → Fingerprint → Pin** – пользователь может получить доступ, если сначала предъявит карту, затем предъявит отпечаток пальца, а после этого введет ПИН-код;
- **Card → Face or Fingerprint → Pin** – пользователь может получить доступ, если сначала предъявит карту, затем пройдет проверку лица на соответствие сохраненной фотографии или предъявит отпечаток пальца, а после этого введет ПИН-код;
- **Card → Face → Fingerprint or Pin** – пользователь может получить доступ, если сначала предъявит карту, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого предъявит отпечаток пальца или введет ПИН-код;
- **Cannot Use** – пользователь всегда получает доступ, предоставив карту.

3. **Suprema 2 Ex Face Auth Mode** определяет логику авторизации с помощью проверки лица на соответствие сохраненной фотографии:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Face** – пользователь может получить доступ, если пройдет проверку лица на соответствие сохраненной фотографии;
   - **Face → Fingerprint** – пользователь может получить доступ, если сначала пройдет проверку лица на соответствие сохраненной фотографии, а затем предъявит отпечаток пальца;
   - **Face → Pin**– пользователь может получить доступ, если сначала пройдет проверку лица на соответствие сохраненной фотографии, а затем введет ПИН-код;
   - **Face → Fingerprint or Pin** – пользователь может получить доступ, если сначала пройдет проверку лица на соответствие сохраненной фотографии, а затем предъявит отпечаток пальца или введет ПИН-код;
   - **Face → Fingerprint → Pin** – пользователь может получить доступ, если сначала пройдет проверку лица на соответствие сохраненной фотографии, затем предъявит отпечаток пальца, а после этого введет ПИН-код;
   - **Cannot Use** – пользователь всегда получает доступ, если пройдет проверку лица на соответствие сохраненной фотографии.
4. **Suprema 2 Ex Finger Auth Mode** определяет логику авторизации с помощью отпечатка пальца:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Fingerprint** – пользователь может получить доступ с помощью отпечатка пальца;
   - **Fingerprint → Face** – пользователь может получить доступ, если сначала предъявит отпечаток пальца, а затем пройдет проверку лица на соответствие сохраненной фотографии;
   - **Fingerprint → Pin** – пользователь может получить доступ, если сначала предъявит отпечаток пальца, а затем введет ПИН-код;
   - **Fingerprint → Face or Pin** – пользователь может получить доступ, если сначала предъявит отпечаток пальца, а затем пройдет проверку лица на соответствие сохраненной фотографии или введет ПИН-код;
   - **Fingerprint → Face → Pin** – пользователь может получить доступ, если сначала предъявит отпечаток пальца, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого введет ПИН-код;
   - **Cannot Use** – пользователь всегда получает доступ, предъявив отпечаток пальца.
5. **Suprema 2 Ex Id Auth Mode** определяет логику поведения авторизации с помощью уникального идентификатора пользователя (id):
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;

- **Id → Face** – пользователь может получить доступ, если сначала введет свой id, а затем пройдет проверку лица на соответствие сохраненной фотографии;
- **Id → Fingerprint** – пользователь может получить доступ, если сначала введет свой id, а затем предъявит отпечаток пальца;
- **Id → Pin**– пользователь может получить доступ, если сначала введет свой id, а затем введет ПИН-код;
- **Id → Face or Fingerprint** – пользователь может получить доступ, если сначала введет свой id, а затем пройдет проверку лица на соответствие сохраненной фотографии или предъявит отпечаток пальца;
- **Id → Face or Pin** – пользователь может получить доступ, если сначала введет свой id, а затем пройдет проверку лица на соответствие сохраненной фотографии или введет ПИН-код;
- **Id → Fingerprint or Pin** – пользователь может получить доступ, если сначала введет свой id, а затем предъявит отпечаток пальца или введет ПИН-код;
- **Id → Face or Fingerprint or Pin** – пользователь может получить доступ, если сначала введет свой id, а затем пройдет проверку лица на соответствие сохраненной фотографии, или предъявит отпечаток пальца, или введет ПИН-код;
- **Id → Face → Fingerprint** – пользователь может получить доступ, если сначала введет свой id, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого предъявит отпечаток пальца;
- **Id → Face → Pin** – пользователь может получить доступ, если сначала введет свой id, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого введет ПИН-код;
- **Id → Fingerprint → Face** – пользователь может получить доступ, если сначала введет свой id, затем предъявит отпечаток пальца, а после этого пройдет проверку лица на соответствие сохраненной фотографии;
- **Id → Fingerprint → Pin** – пользователь может получить доступ, если сначала введет свой id, затем предъявит отпечаток пальца, а после этого введет ПИН-код;
- **Id → Face or Fingerprint → Pin** – пользователь может получить доступ, если сначала введет свой id, затем пройдет проверку лица на соответствие сохраненной фотографии или предъявит отпечаток пальца, а после этого введет ПИН-код;
- **Id → Face → Fingerprint or Pin** – пользователь может получить доступ, если сначала введет свой id, затем пройдет проверку лица на соответствие сохраненной фотографии, а после этого предъявит отпечаток пальца или введет ПИН-код;
- **Id → Fingerprint → Face or Pin** – пользователь может получить доступ, если сначала введет свой id, затем предъявит отпечаток пальца, а после этого пройдет проверку лица на соответствие сохраненной фотографии или введет ПИН-код;
- **Cannot Use** – пользователь всегда получает доступ, введя свой id.

6. **Suprema 2 Faces** отображает количество векторов лиц, назначенных текущему пользователю.
7. **Suprema 2 Finger Auth Mode** определяет логику авторизации с помощью отпечатка пальца:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Only Fingerprint** – пользователь может получить доступ только с помощью отпечатка пальца;
   - **Fingerprint And Pin** – пользователь может получить доступ, если предъявит отпечаток пальца и затем введет ПИН-код;
   - **Cannot Use** – пользователь всегда получает доступ, предъявив отпечаток пальца.
8. **Suprema 2 Id Auth Mode** определяет логику авторизации с помощью id:
   - **Default** – используется поведение по умолчанию, заданное в настройках устройства;
   - **Fingerprint After Id** – пользователь может получить доступ, если сначала введет свой id, а затем предъявит отпечаток пальца;
   - **Pin After Id** – пользователь может получить доступ, если сначала введет свой id, а затем ПИН-код;

- **Fingerprint Or Pin After Id** – пользователь может получить доступ, если сначала введет свой id, а затем предъявит отпечаток пальца или введет ПИН-код;
- **Fingerprint And Pin After Id** – пользователь может получить доступ, если сначала введет свой id, а затем предъявит отпечаток пальца и введет ПИН-код;
- **Cannot use** – пользователь всегда получает доступ, введя свой id.

9. **Suprema 2 Operator Level** определяет доступ к настройкам контроллера с его клавиатуры:
   - **None** – значение по умолчанию. Пользователь не имеет доступа к настройкам;
   - **Admin** – пользователь имеет полный доступ к настройкам;
   - **System settings** – пользователь имеет доступ к настройкам системы, но не имеет доступа к настройкам пользователя;
   - **User information** – пользователь может видеть только информацию пользователя, но не может ничего изменить.

   > **Примечание**
   >
   > Доступ к настройкам контроллера можно получить, нажав кнопку Esc на клавиатуре контроллера, после этого устройство потребует предъявить отпечаток пальца, карту или id.

   > **Внимание!**
   >
   > Как минимум один пользователь должен иметь уровень администратора, иначе эта функция будет отключена.

10. **Suprema QR Code** содержит значение присвоенного пользователю QR-кода.
11. **Suprema Bypass Card** – при предъявлении этой карты будет предоставлен доступ и сгенерировано событие тревоги. Эта карта может быть использована пользователем, находящимся под принуждением.
12. **Suprema (2) Fingerprints** отображает количество отпечатков пальцев, назначенных текущему пользователю.
13. **Suprema (2) Security level** определяет уровень качества отпечатков пальцев. Для корректной настройки необходимо обратиться к официальной справочной документации по данной системе.

Настройка дополнительных параметров пользователей интеграции *Suprema 2* завершена.

4 Работа с модулем интеграции Suprema 2

4.1 Общие сведения о работе с модулем Suprema 2

Для работы с модулем интеграции *Suprema 2* используются следующие интерфейсные объекты:

1. **Карта**;
2. **Протокол событий**.

Сведения по настройке данных интерфейсных объектов приведены в документе Программный комплекс Интеллект: Руководство Администратора.

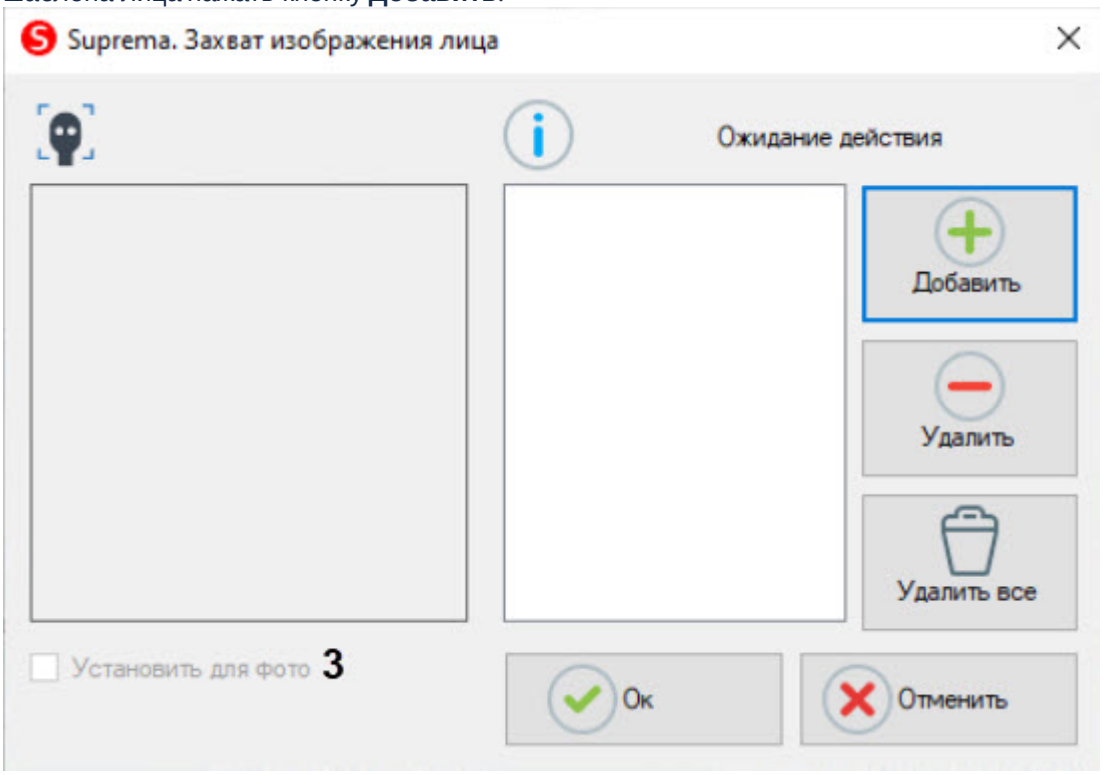
Работа с данными интерфейсными объектами подробно описана в документе Программный комплекс Интеллект: Руководство Оператора.

4.2 Добавление биометрических параметров Suprema 2

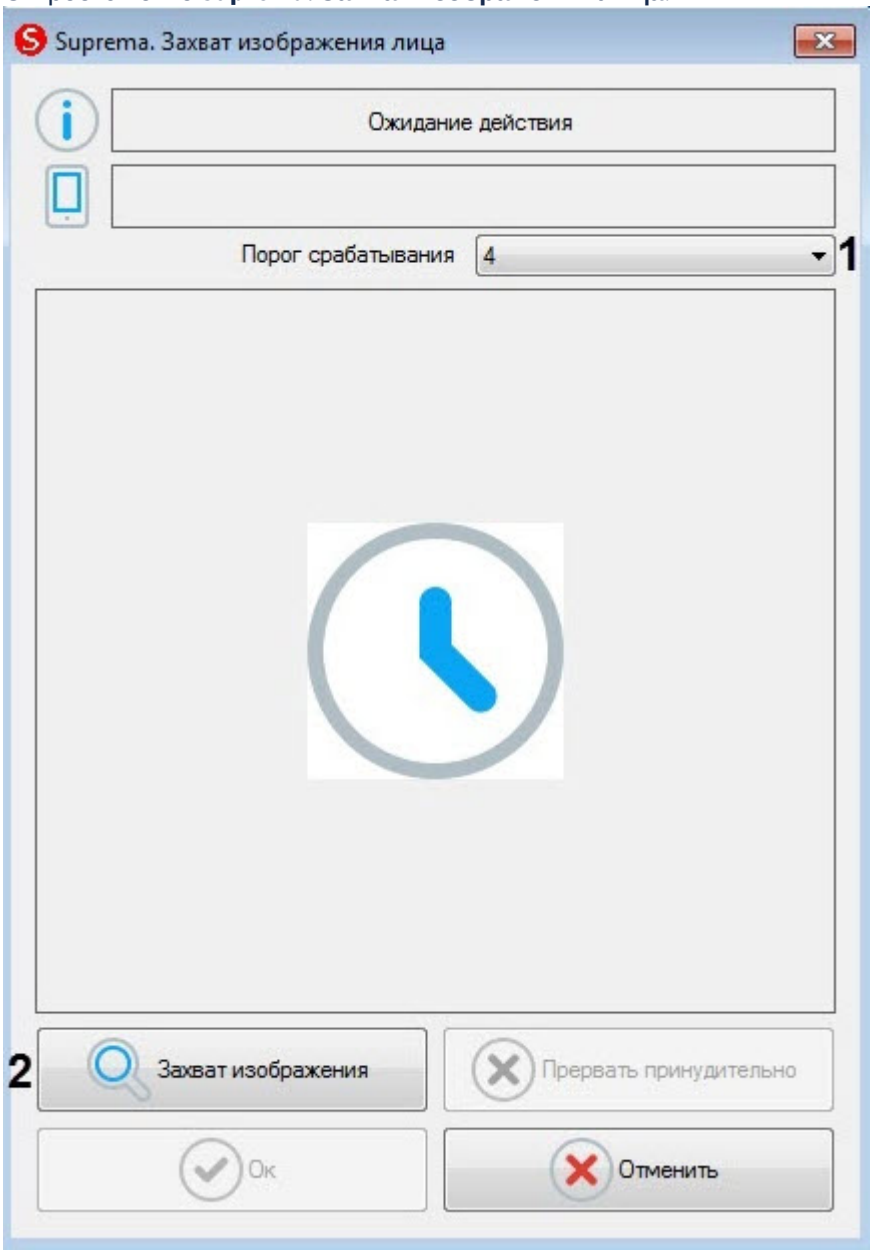
4.2.1 Добавление шаблона лица Suprema 2

Для добавления шаблона лица *Suprema 2* в модуле *Бюро Пропусков* необходимо выполнить следующие действия:

1. Перейти к добавлению биометрических данных в окне **Бюро пропусков** (см. Добавление биометрических параметров).
2. Выбрать расширение **(Редактирование лиц) Suprema 2 Host**, которое соответствует контроллеру с подключенным к нему биометрическим считывателем лица, либо терминалу.
3. Откроется диалоговое окно **Suprema. Захват изображения лица**. Для добавления нового шаблона лица нажать кнопку **Добавить**.



Откроется окно **Suprema. Захват изображения лица**.



4. В раскрывающемся списке **Порог срабатывания** (**1**) выбрать чувствительность захвата изображения лица: от **0** (низкая) до **8** (максимальная).
5. Для начала захвата лица нажать кнопку **Захват изображения** (**2**) и далее следовать указаниям, отображаемым в верхней части окна **Suprema. Захват изображения лица**. В случае успешного захвата лица отобразится полученная фотография, шаблон которой будет сохранен.

> **Внимание!**
>
> Произвольные фотографии (из файлов, с камер) в терминалы пересылаться не могут. Если терминалов много, то захват лица можно сделать с любого из них, далее это изображение будет пересылаться в другие терминалы с другими атрибутами доступа.

6. Установить флажок **Установить для фото** (**3**) для назначения захваченного терминалом лица в качестве фотографии пользователя.

7. Нажать кнопку **Ок** для завершения добавления шаблона лица, кнопку **Отменить** для отмены операции.
8. Для удаления шаблона лица необходимо выбрать его в списке шаблонов и нажать кнопку **Удалить**.

> **Примечание**
>
> Для удаления всех шаблонов лиц нажать кнопку **Удалить все**.

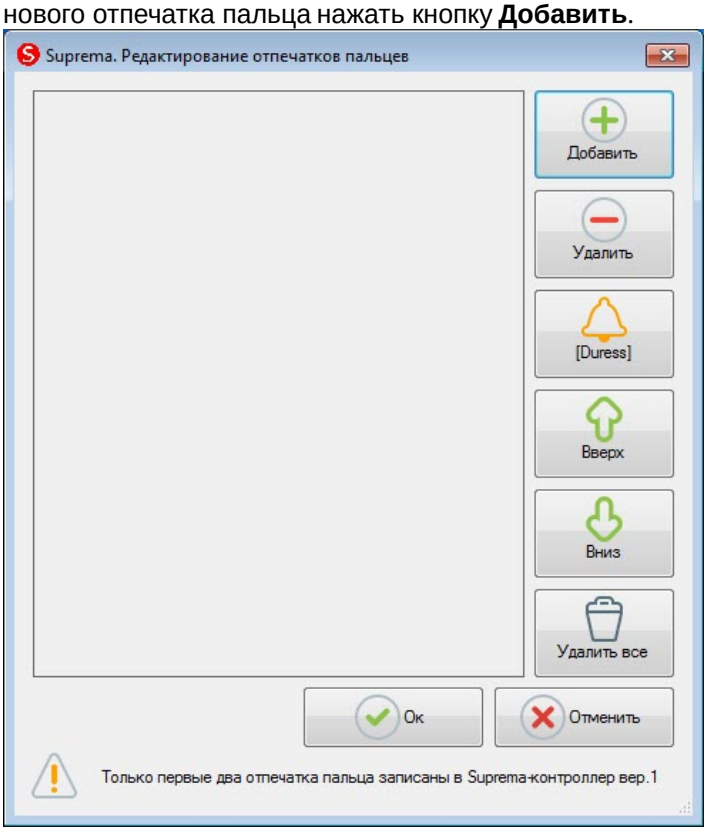
9. Нажать кнопку **Ок** для сохранения шаблона лица.

Добавление шаблона лица *Suprema 2* в модуле *Бюро Пропусков* завершено.

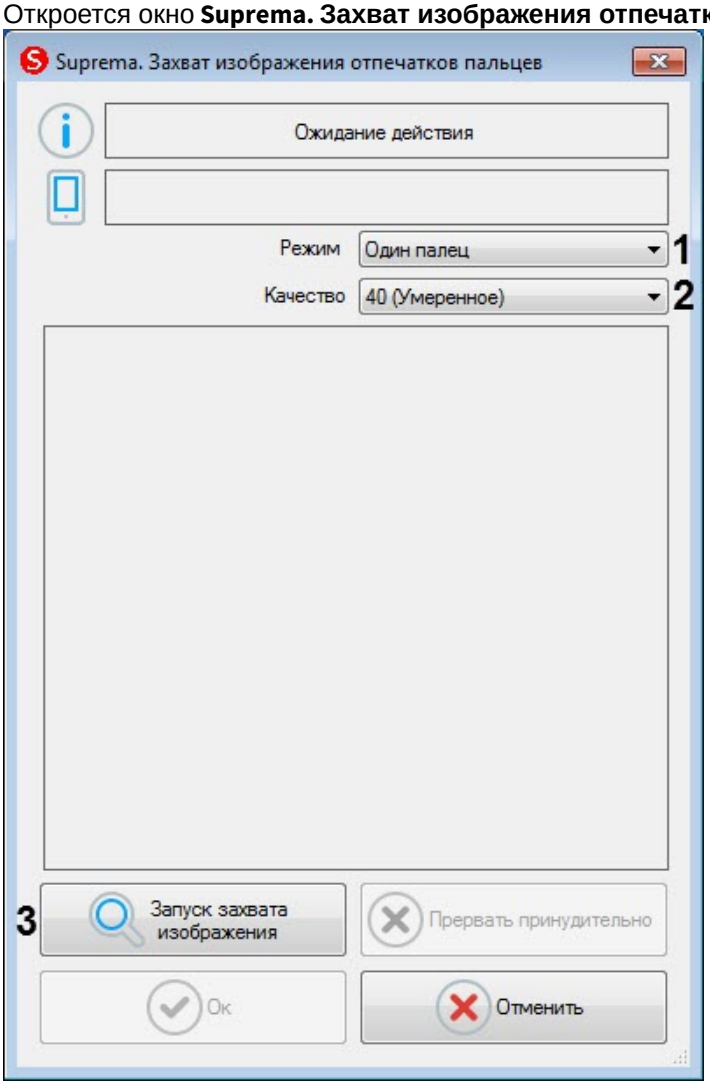
4.2.2 Добавление шаблонов отпечатков пальцев Suprema 2

Для добавления шаблонов отпечатков пальцев *Suprema 2* в модуле *Бюро Пропусков* необходимо выполнить следующие действия:

1. Перейти к добавлению биометрических данных в окне **Бюро пропусков** (см. Добавление биометрических параметров).
2. Выбрать расширение **(Редактирование отпечатков пальцев) Suprema 2 Host**, которое соответствует контроллеру с подключенным к нему биометрическим считывателем отпечатков пальцев.
3. Откроется диалоговое окно **Suprema. Редактирование отпечатков пальцев**. Для добавления нового отпечатка пальца нажать кнопку **Добавить**.



Откроется окно **Suprema. Захват изображения отпечатков пальцев**.

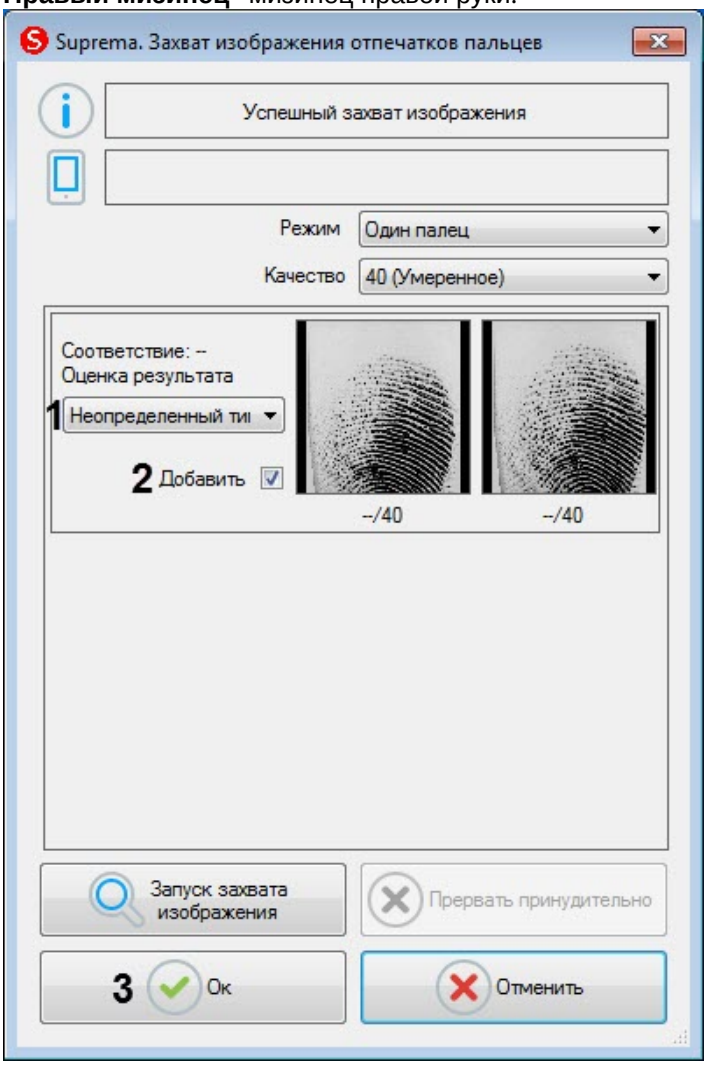


4. В раскрывающемся списке **Режим** (**1**) выбрать режим захвата отпечатков: **Один палец**. Остальные режимы захвата для данного контрольного считывателя недоступны.
5. В раскрывающемся списке **Качество** (**2**) выбрать качество захвата отпечатков:
   - **20 (Слабое)** - низкое качество.
   - **40 (Умеренное)** - среднее качество (по умолчанию).
   - **60 (Сильное)** - высокое качество.
   - **80 (Самое сильное)** - наивысшее качество.
6. Для начала захвата отпечатков нажать кнопку **Запуск захвата изображения** (**3**) и далее следовать указаниям, отображаемым в верхней части окна **Suprema. Захват изображения отпечатков пальцев**.

   > **Примечание**
   >
   > Для захвата отпечатков необходимо каждый палец или группу пальцев приложить к считывателю по 2 раза с задержкой в 5 секунд после нажатия кнопки **Запуск захвата изображения** и после первого захвата.

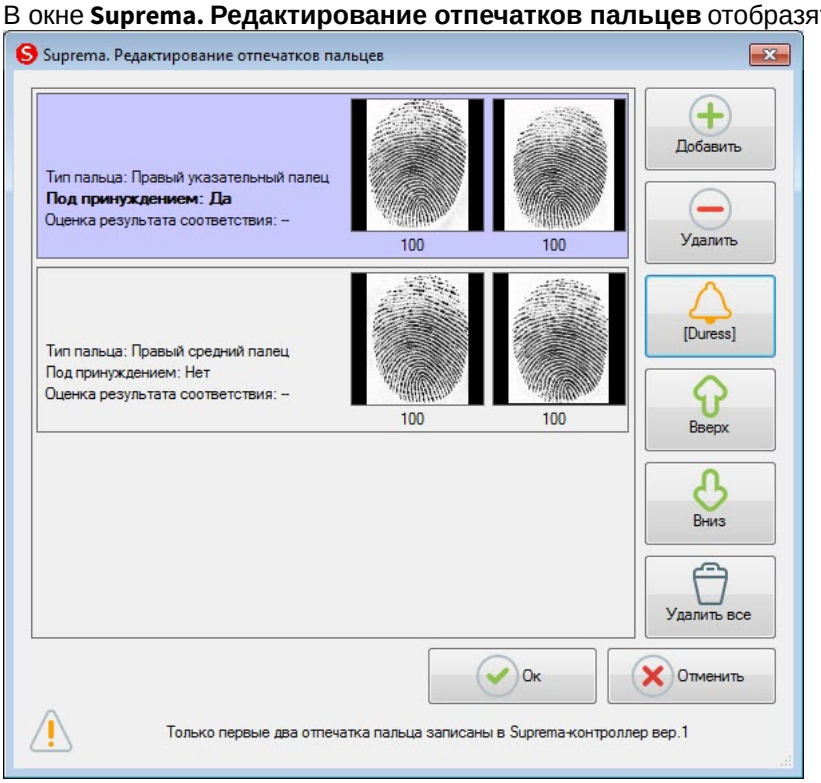
7. После завершения захвата отпечатков пальцев необходимо в раскрывающемся списке (**1**) для каждого отпечатка выбрать тип отсканированного пальца:
   - **Неопределенный тип** - неопределенный.

- **Левый большой палец** - большой палец левой руки.
- **Левый указательный палец** - указательный палец левой руки.
- **Левый средний палец** - средний палец левой руки.
- **Левый безымянный палец** - безымянный палец левой руки.
- **Левый мизинец** - мизинец левой руки.
- **Правый большой палец** - большой палец правой руки.
- **Правый указательный палец** - указательный палец правой руки.
- **Правый средний палец** - средний палец правой руки.
- **Правый безымянный палец** - безымянный палец правой руки.
- **Правый мизинец** - мизинец правой руки.



8. Снять флажок **Добавить** (**2**), если данный отпечаток не нужно добавлять пользователю.
9. Нажать кнопку **Ок** (**3**) для сохранения результата захвата отпечатков.

10. В окне **Suprema. Редактирование отпечатков пальцев** отобразятся захваченные отпечатки.



11. Для удаления одного отпечатка пальца необходимо выбрать соответствующий отпечаток и нажать кнопку **Удалить**.

> **Примечание**
>
> Чтобы удалить все отпечатки пальце необходимо нажать кнопку **Удалить все**.

12. Чтобы сделать отпечаток "Под принуждением" необходимо выбрать соответствующий отпечаток и нажать кнопку **[Duress]**.

> **Примечание**
>
> В результате при считывании данного отпечатка пальца будет генерироваться тихая тревога.

13. Для перемещения отпечатков пальцев вверх или вниз по списку необходимо выбрать соответствующий отпечаток и нажать кнопку **Вверх** или **Вниз**.
14. Для завершения ввода отпечатков пальцев нажать кнопку **Ок**.

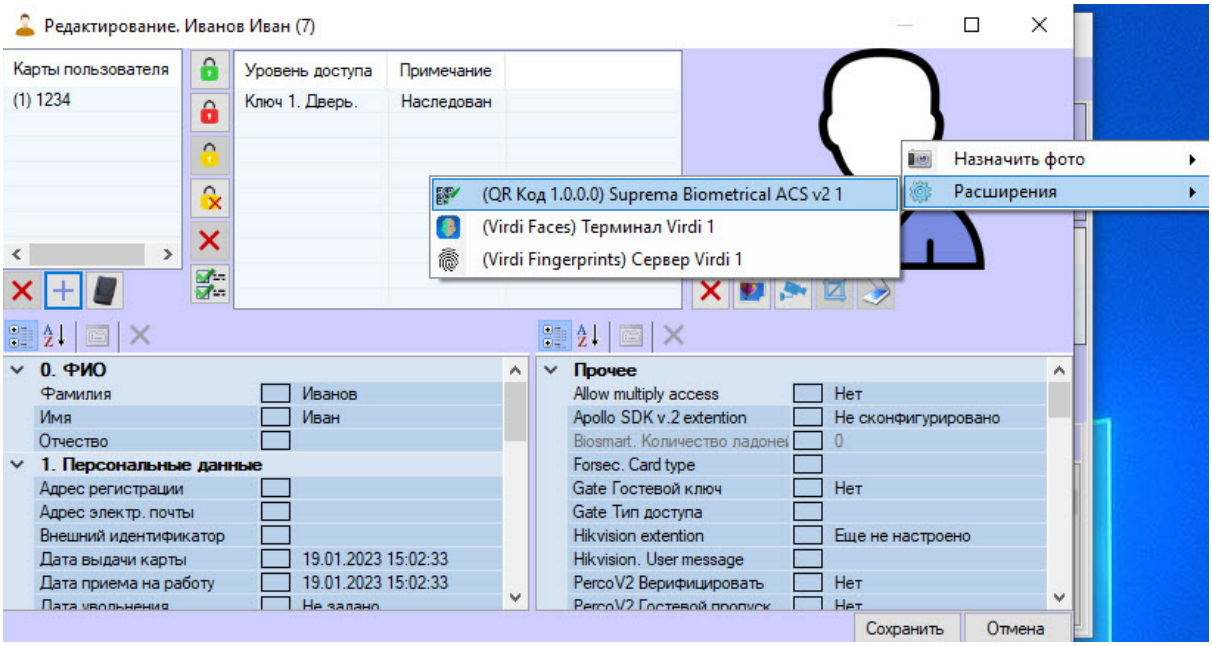
Добавление шаблонов отпечатков пальцев *Suprema 2* в модуле *Бюро Пропусков* завершено.

4.3 Работа с QR-кодами

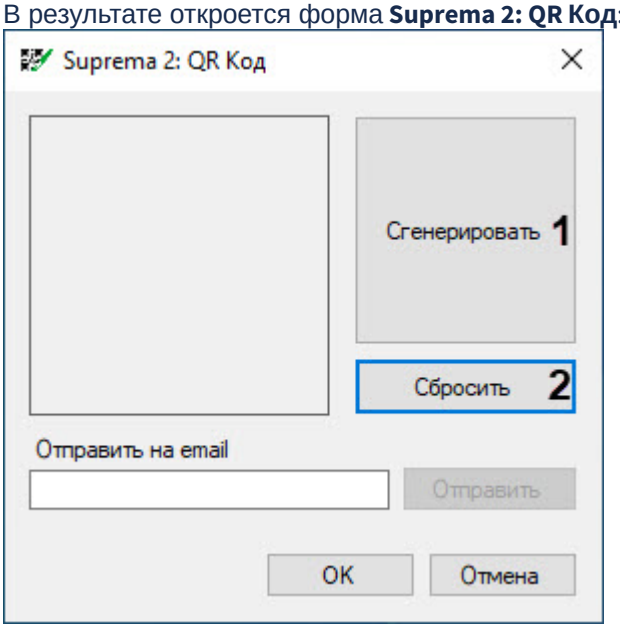
При подключении терминала X-Station 2 можно работать с QR-кодами: сгенерировать код, отправить его по указанному адресу электронной почты, а также использовать для прохода через терминал, для этого:

1. Добавить головной объект **Suprema Biometrical ACS v2** в качестве контрольного считывателя (см. Настройка контрольных считывателей в Бюро пропусков).

2. Выбрать считыватель **(QR Код 1.0.0) Suprema Biometrical ACS v2** из доступных кнопок **Расширения** (подробнее см. Добавление биометрических параметров).

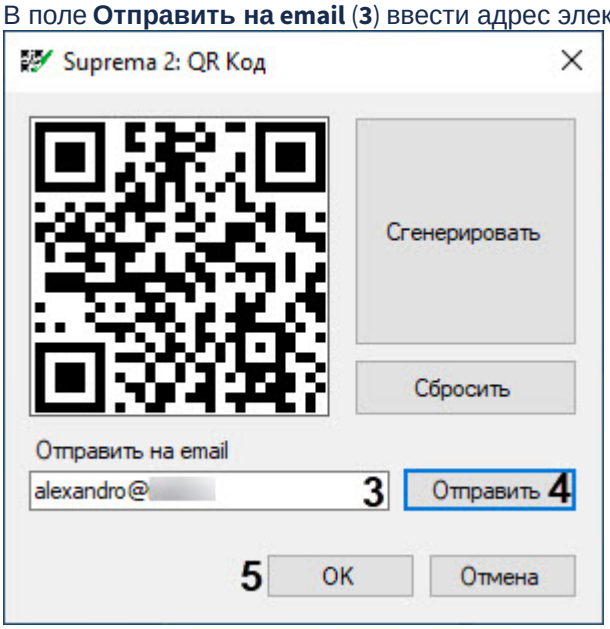


В результате откроется форма **Suprema 2: QR Код**:



3. Чтобы сгенерировать QR-код, в открывшейся форме нажать кнопку **Сгенерировать**(**1**), для отмены действия нажать кнопку **Сбросить** (**2**).

4. В поле **Отправить на email** (**3**) ввести адрес электронной почты для отправки QR-кода.



5. Нажать кнопку **Отправить** (**4**), чтобы отправить сгенерированный QR-код по указанному на предыдущем шаге адресу.
6. Для сохранения изменений и возврата к форме редактирования пользователя нажать кнопку **OK** (**5**).
7. Для сохранения QR-кода в *Бюро пропусков* в форме редактирования пользователя нажать кнопку **Сохранить**.
   QR-код будет сохранен в *Бюро пропусков* и может использоваться пользователем для прохода через терминал.

4.4 Управление контроллером Suprema 2

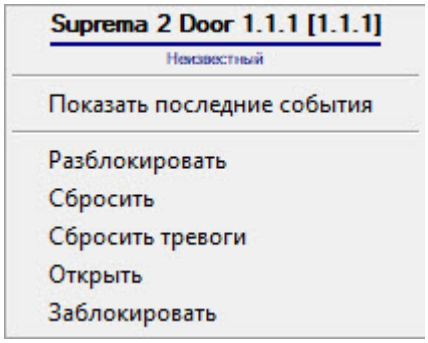
Управление контроллером *Suprema 2* в интерактивном окне **Карта** не осуществляется.

Возможны следующие состояния контроллера *Suprema 2*:

	Подключен
	Подключен, но рассинхронизирован
	Отключен

4.5 Управление дверью Suprema 2

Управление дверью *Suprema 2* осуществляется в интерактивном окне **Карта** с использованием функционального меню объекта **Suprema 2 Door**.



Команды для управления дверью *Suprema 2* описаны в таблице:

Команда функционального меню	**Выполняемая функция**
Разблокировать	Разблокировать
Сбросить	Перевести в дежурный режим
Сбросить тревоги	Сбросить тревоги с помощью оператора
Открыть	Открыть
Заблокировать	Заблокировать

Возможны следующие состояния двери *Suprema 2*:

	Заблокировано
	Разблокировано
	Нет связи
	Закрыто

SUPREMA_2_DOOR 1.1.1[1.1.1] 	Открыто
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Удержание в открытом состоянии
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Тревога удержания в открытом состоянии
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Тревога принудительного удержания в открытом состоянии
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Заблокировано по расписанию
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Заблокировано оператором
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Экстренное блокирование
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Разблокировано по расписанию
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Разблокировано оператором

SUPREMA_2_DOOR 1.1.1[1.1.1] 	Экстренное разблокирование
SUPREMA_2_DOOR 1.1.1[1.1.1] 	Тревога двойного прохода