Руководство по настройке и работе с модулем интеграции Virdi

ACFA Интеллект

Last update 09/29/2022

Table of Contents

1 Введение в Руководство по настройке и работе с модулем интеграции Virdi 4
1.1 Назначение документа 4
1.2 Общие сведения о модуле интеграции «Virdi» 4
2 Поддерживаемое оборудование и лицензирование модуля Virdi 5
3 Настройка модуля интеграции Virdi 7
3.1 Настройка подключения СКУД Virdi 7
3.2 Настройка контроллера Virdi 7
3.2.1 Конфигурирование контроллера Virdi 7
Настройка соединения контроллера Virdi 8
Системные настройки контроллера Virdi 9
Управление конфигурацией контроллера Virdi 11
Настройка подключения к Web-серверу контроллера Virdi 11
3.2.2 Настройка входа Virdi 12
3.2.3 Настройка выхода Virdi 13
3.2.4 Настройка двери Virdi 14
3.2.5 Настройка зоны Virdi 15
3.2.6 Настройка раздела Virdi 17
3.2.7 Настройка считывателя Virdi 18
3.3 Настройка терминала Virdi 20
3.3.1 Настройка соединения терминала Virdi 20
3.3.2 Системные настройки терминала Virdi 21
3.3.3 Настройка разделов терминала Virdi 23
3.3.4 Управление конфигурацией терминала Virdi 24
3.3.5 Настройка аутентификации 25
4 Работа с модулем интеграции Virdi 27
4.1 Общие сведения о работе с модулем интеграции Virdi 27
4.2 Управление терминалом Virdi 27
4.3 Управление разделом Virdi 28
4.4 Управление дверью Virdi 29
4.5 Управление контроллером, считывателем и зоной Virdi 30

4.6 Добавление биометрических параметров Virdi 31
4.6.1 Добавление шаблона лица Virdi 31
4.6.2 Добавление шаблонов отпечатков пальцев Virdi 33
4.7 Работа с параметрами пользователя Virdi 40

1 Введение в Руководство по настройке и работе с модулем интеграции Virdi

На странице:

- Назначение документа
- Общие сведения о модуле интеграции «Virdi»

1.1 Назначение документа

Документ *Руководство по настройке и работе с модулем Virdi* является справочно-информационным пособием и предназначен для специалистов по настройке модуля *Virdi.*

В данном Руководстве представлены следующие материалы:

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

1.2 Общие сведения о модуле интеграции «Virdi»

Модуль *Virdi* является компонентом СКУД, реализованной на базе ПК *ACFA-Интеллект*, и предназначен для выполнения следующих функций:

1. конфигурирование аппаратных средств *Virdi*;
2. обеспечение взаимодействия аппаратных средств *Virdi* с ПК *ACFA-Интеллект*.

> **Примечание.**
>
> Подробные сведения о СКУД *Virdi* приведены в официальной справочной документации по данной системе (производитель Union Community Co. Ltd).

Перед настройкой модуля *Virdi* необходимо выполнить следующие действия:

1. установить аппаратные средства *Virdi* на охраняемый объект (см. справочную документацию по *Virdi*);
2. подключить аппаратные средства *Virdi* к Серверу ПК *Интеллект* (см. справочную документацию по *Virdi*).

2 Поддерживаемое оборудование и лицензирование модуля Virdi

Производитель	Union Community Co. Ltd 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea E-mail: sales@virditech.com Сайт: https://www.virditech.com
Тип интеграции	SDK
Подключение оборудования	Ethernet

Поддерживаемое оборудование

Оборудование	Назначение	Характеристика
MCP-040	Контроллер	• Зональный интерфейс: 8 зон (каждый порт двойного назначения) • Максимальное количество расписаний: 1024 • Максимальное количество пользователей: 50000 • Сеть: 10/100M Ethernet • Максимальное количество дверей: 4 • Интерфейс звонка: контролируемый порт звонка / сирены (1 порт) • Количество событий: 51200 • Порт связи: порт считывателя RS485 / входные порты Wiegand • Программируемые входы / Программируемые выходы
Терминалы серии AC	Терминал	AC-7000 AC-5100 AC-2200 AC-2100 AC-2000 AC-1100 AC-6000 Подробные сведения приведены в официальной справочной документации производителя соответствующего терминала (производитель Union Community Co. Ltd).

Оборудование	Назначение	Характеристика
Терминалы серии UBio-X	Терминал	UBio-X Pro Lite UBio-X Iris UBio-X Slim UBio-X Face UBio-X Pro2 UBio-X Pro Подробные сведения приведены в официальной справочной документации производителя соответствующего терминала (производитель Union Community Co. Ltd).
FOH02	Контрольный считыватель	Отпечатки пальцев Карты: RF: 125KHz proximity card SC: 13. 56 MHz smart card

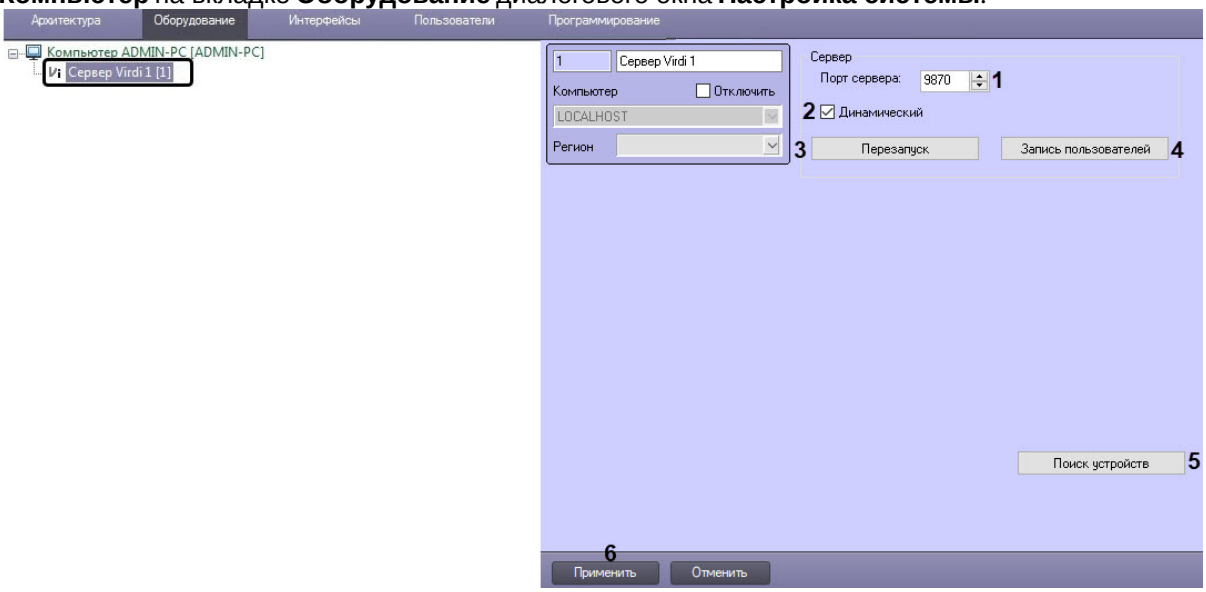
Защита модуля
За 1 контроллер/терминал.

3 Настройка модуля интеграции Virdi

3.1 Настройка подключения СКУД Virdi

Настройка подключения СКУД *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Сервер Virdi**, который создается на базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы**.



2. В поле **Порт сервера** (**1**) ввести порт Сервера ПК *ACFA-Интеллект*, к которому подключена СКУД *Virdi*.
3. Установить флажок **Динамический** (**2**), если требуется, чтобы изменения по сотрудникам, управлению доступом или временным зонам автоматически отправлялись в соответствующие контроллеры и терминалы, для которых вносятся изменения.
4. Нажать кнопку **Перезапуск** (**3**), если необходимо переподключиться ко всем контролерам и терминалам.
5. Нажать кнопку **Запись пользователей** (**4**), если необходимо записать пользователей во все контроллеры и терминалам.
6. Нажать кнопку **Поиск устройств** (**5**), чтобы найти все подключенные к Серверу устройства и построить соответствующее конфигурации дерево объектов.
7. Нажать кнопку **Применить** (**6**) для сохранения внесенных изменений.

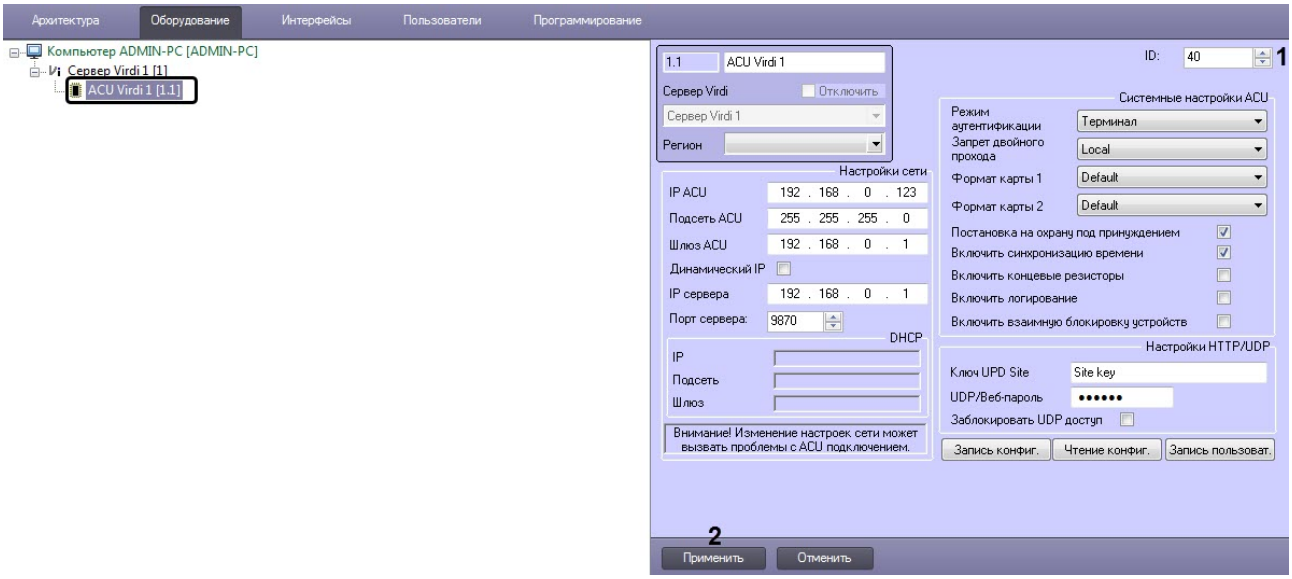
Настройка подключения СКУД *Virdi* завершена.

3.2 Настройка контроллера Virdi

3.2.1 Конфигурирование контроллера Virdi

Конфигурирование контроллера *Virdi* осуществляется на панели настройки объекта **ACU Virdi**, который создается на базе объекта **Сервер Virdi**.

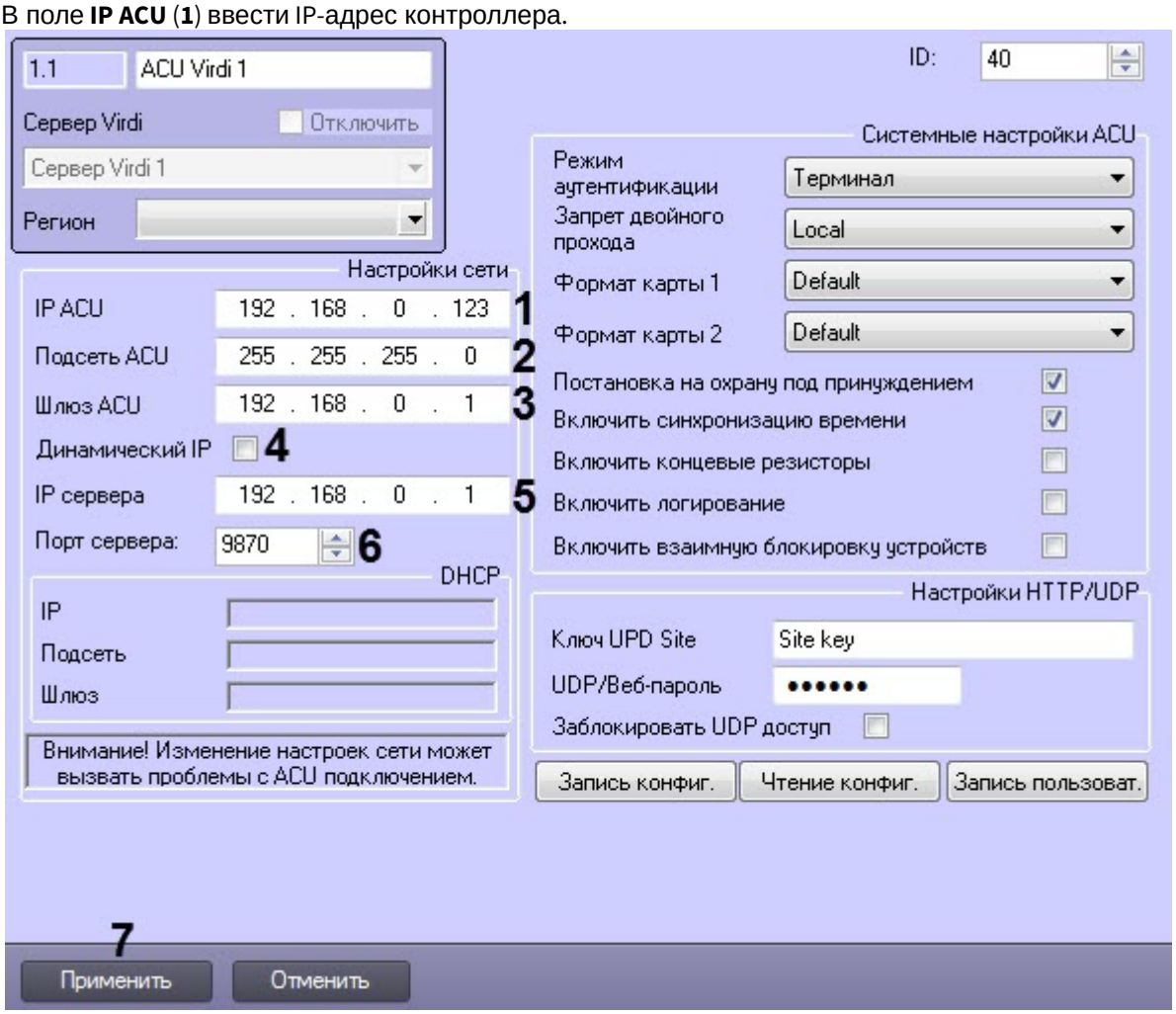
После создания объекта **ACU Virdi** необходимо в поле **ID** (**1**) указать идентификатор данного контроллера и нажать кнопку **Применить** (**2**).



Настройка соединения контроллера Virdi

Настройка соединения контроллера *Virdi* осуществляется следующим образом:

1. В поле **IP ACU** (**1**) ввести IP-адрес контроллера.



2. В поле **Подсеть ACU** (**2**) ввести маску подсети контроллера.
3. В поле **Шлюз ACU** (**3**) ввести шлюз контроллера.
4. Установить флажок **Динамический IP** (**4**), если контроллер работает в сети с DHCP протоколом.
5. В поле **IP сервера** (**5**) ввести IP-адрес Сервера ПК *ACFA-Интеллект*.
6. В поле **Порт сервера** (**6**) ввести порт Сервера ПК *ACFA-Интеллект*.
7. Нажать кнопку **Применить** (**7**) для применения настроек.

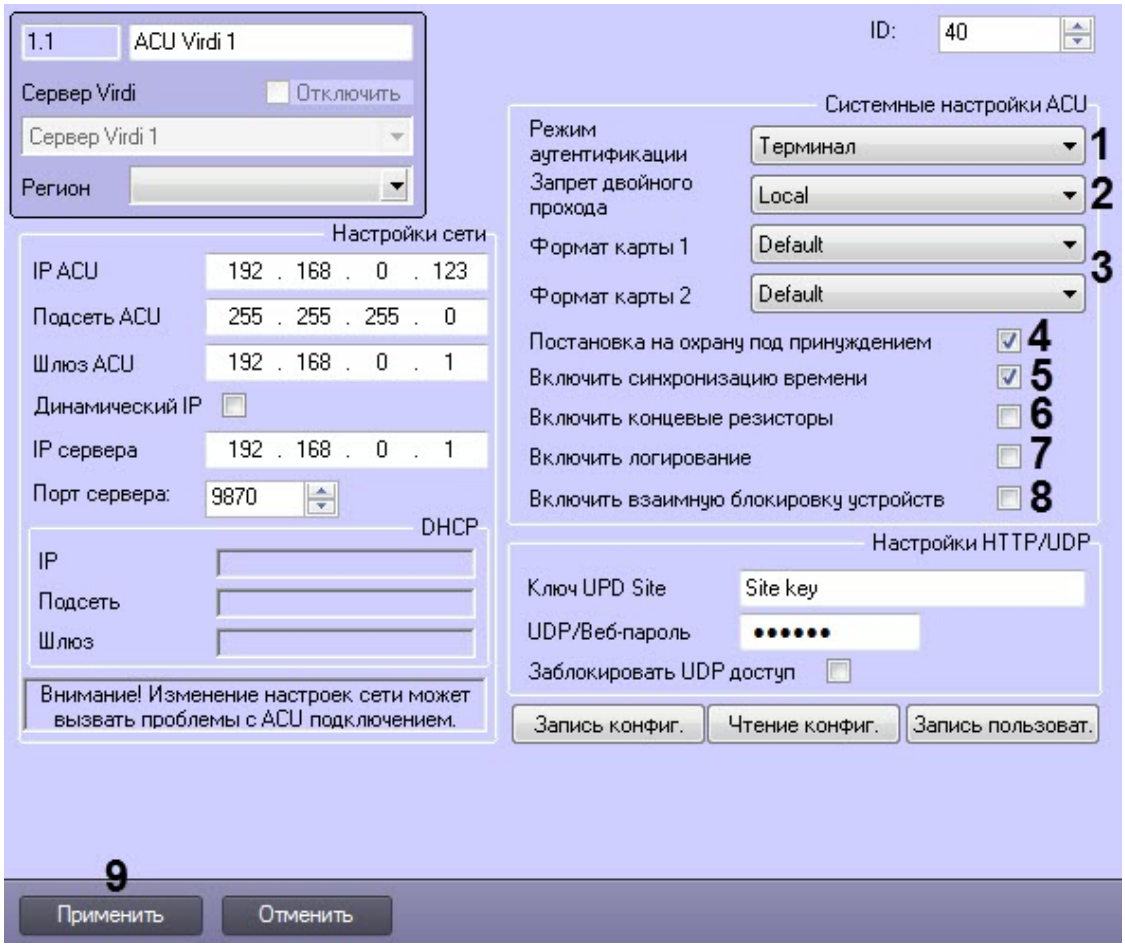
Настройка соединения контроллера *Virdi* завершена.

Системные настройки контроллера Virdi

Системные настройки контроллера *Virdi* осуществляются следующим образом:

1. Из раскрывающегося списка **Режим аутентификации** (**1**) выбрать режим аутентификации и работы контроллера:
   - **Сервер/Терминал** - принятие решений осуществляется Сервером, а если он недоступен, то контроллером.
   - **Терминал/Сервер** - принятие решений осуществляется контроллером, а если он недоступен, то Сервером.
   - **Сервер** - принятие решений осуществляется Сервером.
   - **Терминал** - принятие решений осуществляется контроллером.
   - **Режим оффлайн** - автономный режим контроллера.

> **Примечание**
>
> В автономном режиме контроллера управление с Сервера ПК *ACFA-Интеллект* недоступно.



2. Из раскрывающегося списка **Запрет двойного прохода** (**2**) выбрать режим контроля двойного прохода:
   - **Local** - контроль осуществляется контроллером.
   - **Server** - контроль осуществляется Сервером.
3. Из раскрывающихся списков **Формат карты 1** и **Формат карты 2** (**3**) выбрать формат представления данных карт доступа:
   - **Default** - стандартный.
   - **Hexademical** - шестнадцатеричный.
   - **Decimal** - десятичный.
   - **3:5 Decimal** - 3 или 5 десятичных цифр.
4. Установить флажок **Постановка на охрану под принуждением** (**4**), если необходимо разрешить принудительную постановку зоны на охрану, даже если в зоне есть открытые двери.
5. Установить флажок **Включить синхронизацию времени** (**5**), если необходимо включить синхронизацию времени Сервера и контроллера.
6. Установить флажок **Включить концевые резисторы** (**6**), если необходимо включить оконечные резисторы.
7. Установить флажок **Включить логирование** (**7**), если необходимо включить логирование всех событий при нажатии кнопок EXIT.

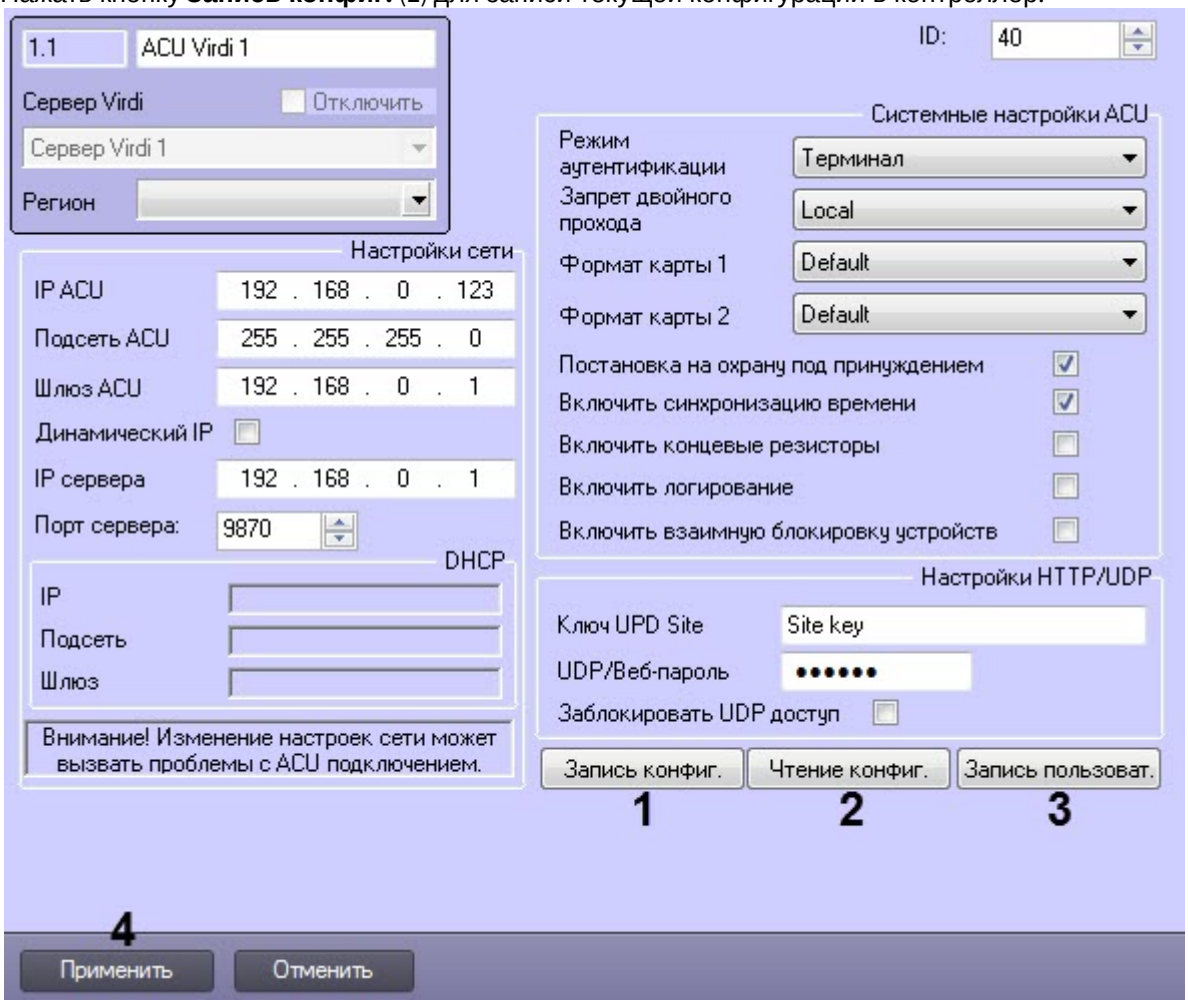
8. Установить флажок **Включить взаимную блокировку устройств** (**8**), если необходимо активировать спаренную блокировку всех дверей.
9. Нажать кнопку **Применить** (**9**) для применения настроек.

Системные настройки контроллера *Virdi* завершены.

Управление конфигурацией контроллера Virdi

Управление конфигурацией контроллера *Virdi* осуществляется следующим образом:

1. Нажать кнопку **Запись конфиг.** (**1**) для записи текущей конфигурации в контроллер.



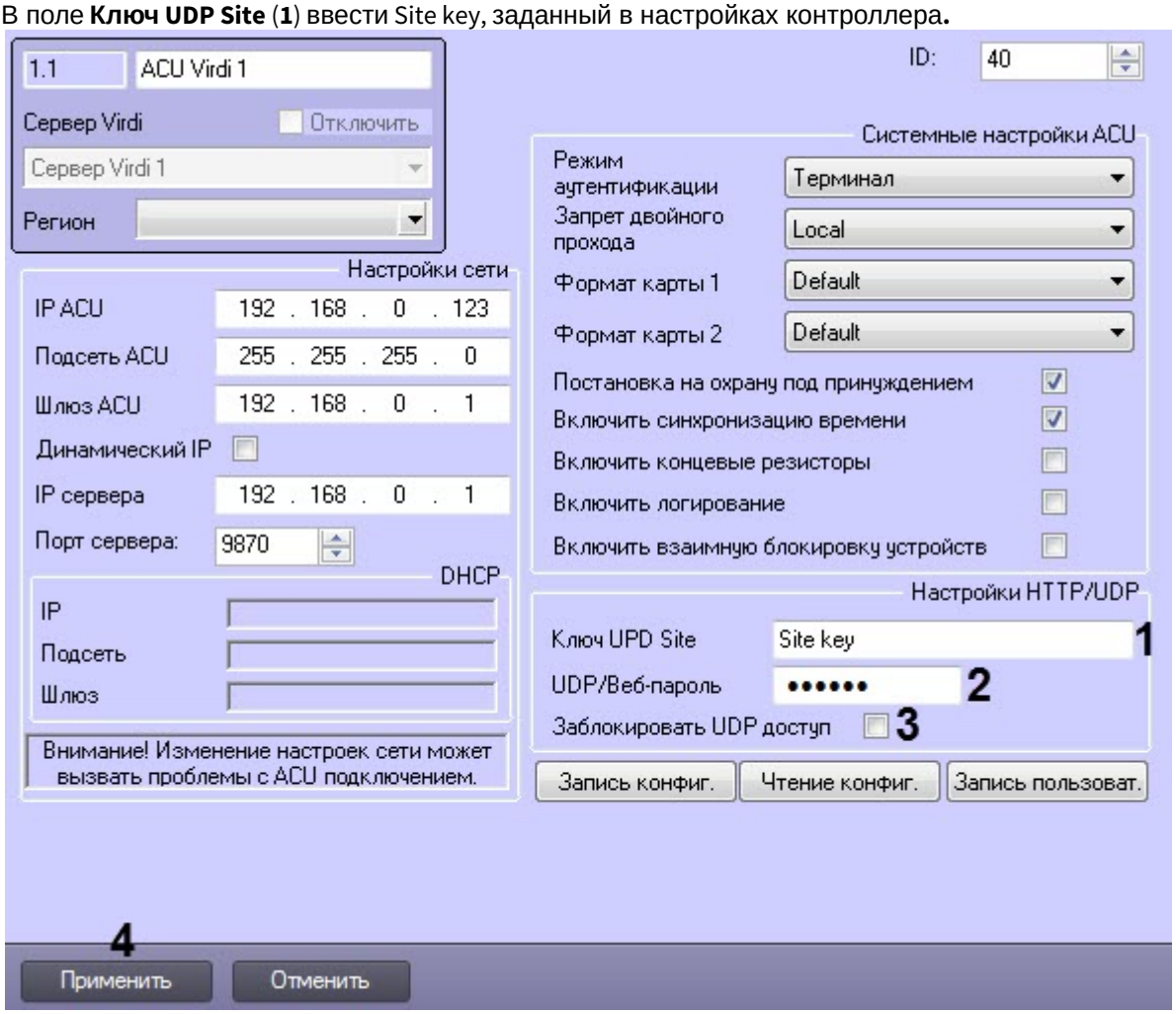
2. Нажать кнопку **Чтение конфиг.** (**2**) для считывания конфигурации контроллера.
3. Нажать кнопку **Запись конфиг.** (**3**) для пересылки пользователей в контроллер.
4. Нажать кнопку **Применить** (**4**) для применения настроек.

Управление конфигурацией контроллера *Virdi* завершено.

Настройка подключения к Web-серверу контроллера Virdi

Настройка подключения к Web-серверу контроллера *Virdi* осуществляется следующим образом:

1. В поле **Ключ UDP Site** (**1**) ввести Site key, заданный в настройках контроллера**.**



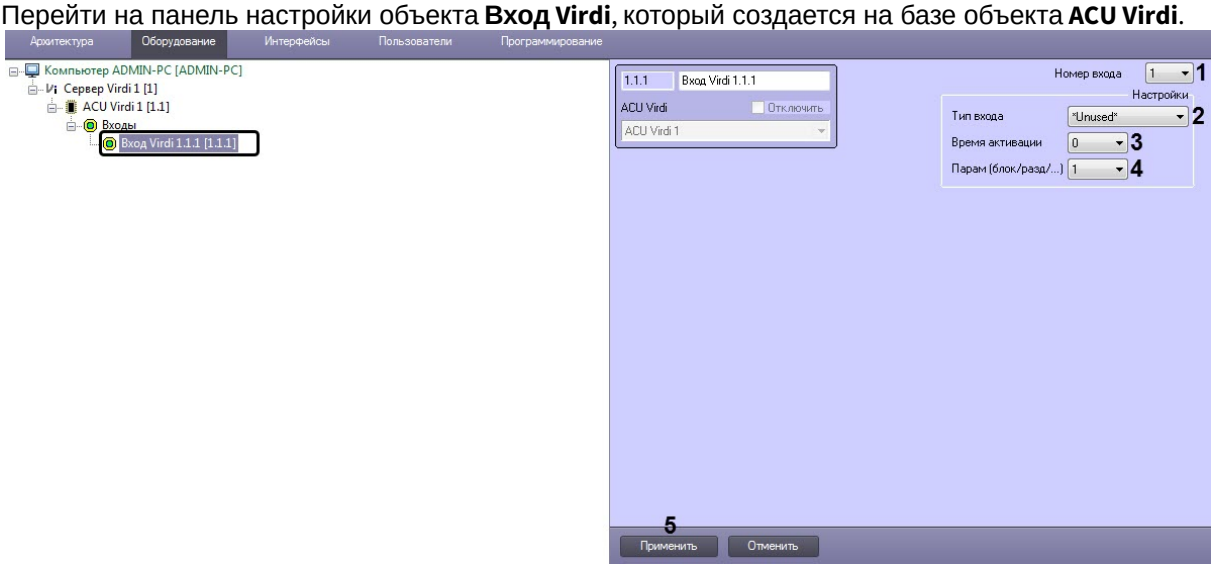
2. В поле **UDP/Веб-пароль** (**2**) ввести веб-пароль контроллера.
3. Установить флажок **Заблокировать UDP доступ** (**3**), если необходимо отключить возможность настройки контроллера через Web-интерфейс.
4. Нажать кнопку **Применить** (**4**) для применения настроек.

Настройка подключения к Web-серверу контроллера контроллера *Virdi* завершена.

3.2.2 Настройка входа Virdi

Настройка входа *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Вход Virdi**, который создается на базе объекта **ACU Virdi**.



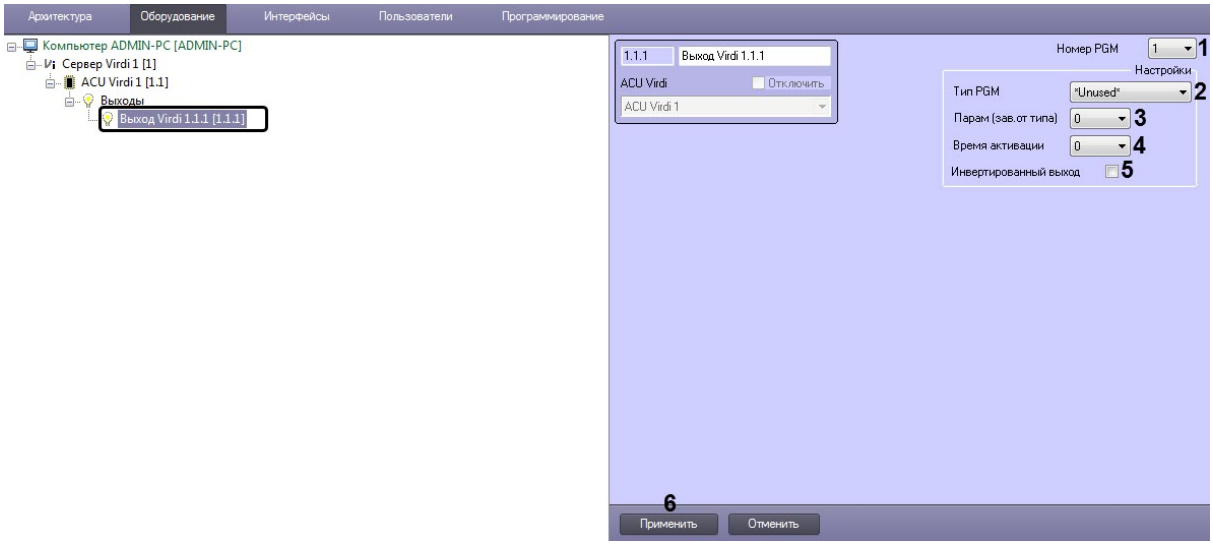
2. Из раскрывающегося списка **Номер входа** (**1**) выбрать номер входа: от **1** до **4**.
3. Из раскрывающегося списка **Тип входа** (**2**) выбрать тип входа:
   - **Unused** - не используется.
   - **Egress (NC)** - вход с нормально-замкнутыми контактами.
   - **Egress (NO)** - вход с нормально-разомкнутыми контактами.
   - **Fire (NC)** - пожарный вход с нормально-замкнутыми контактами.
   - **Fire (NO)** - пожарный вход с нормально-разомкнутыми контактами.
   - **Security (NC)** - охранный вход с нормально-замкнутыми контактами.
   - **Security (NO)** - охранный вход с нормально-разомкнутыми контактами.
4. Из раскрывающегося списка **Время активации** (**3**) выбрать время в секундах, на которое будет открыта дверь при срабатывании входа **Egress (NC)** и **Egress (NO)**: от **0** до **255**.
5. Из раскрывающегося списка **Парам (блок/разд/...)** (**4**):
   - Если выбран тип входа **Egress (NC)** и **Egress (NO)**, то выбрать номер двери, которая будет открыта при активации данного входа: от **1** до **4**.
   - Если выбран тип входа **Fire (NC)** и **Fire (NO)**, то выбрать номер раздела, в котором сработает пожарная сигнализация при активации данного входа: от **1** до **4**.
   - Если выбран тип входа **Security (NC)** и **Security (NO)**, то выбрать номер раздела, который будет поставлен/снят с охраны при активации данного входа: от **1** до **4**.
6. Нажать кнопку **Применить** (**5**) для применения настроек.

Настройка входа *Virdi* завершена.

3.2.3 Настройка выхода Virdi

Настройка выхода *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Выход Virdi**, который создается на базе объекта **ACU Virdi**.



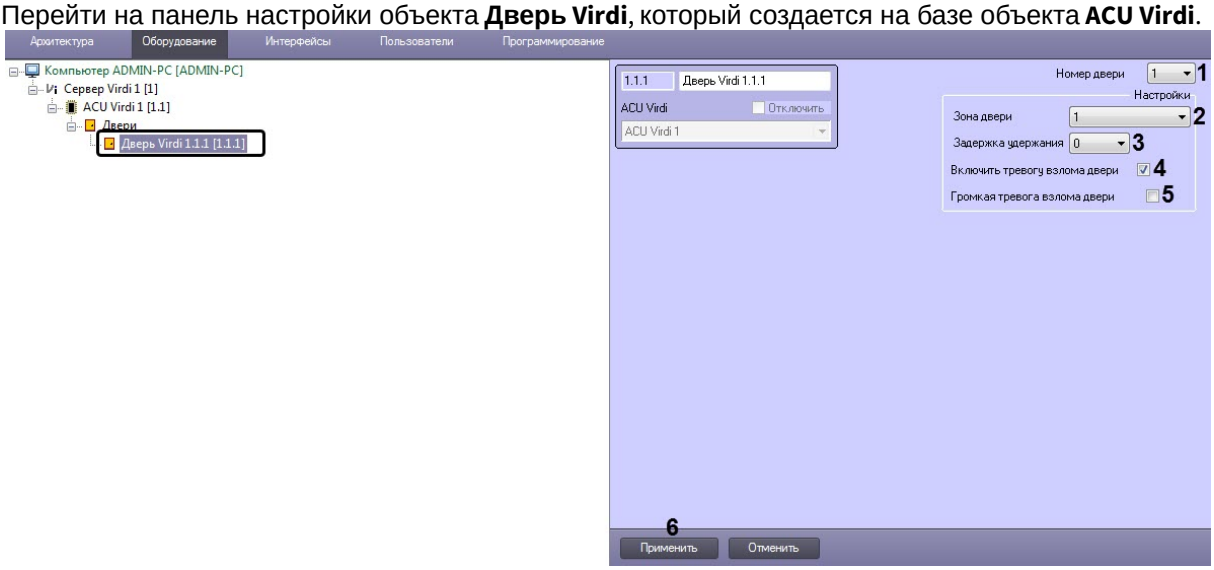
2. Из раскрывающегося списка **Номер PGM** (**1**) выбрать номер выхода от **1** до **8**.
3. Из раскрывающегося списка **Тип PGM** (**2**) выбрать тип выхода:
   - **Unused** - не используется.
   - **Matching success** - срабатывает после успешной авторизации какого-либо пользователя.
   - **Matching failed** - срабатывает после неуспешной авторизации какого-либо пользователя.
   - **Scheduled output** - срабатывает по назначенному расписанию.
   - **Alarm output** - срабатывает, когда происходит тревога.
   - **System troubles** - срабатывает, когда в системе происходит какая-либо проблема, например проблема с аккумулятором, проблема со считывателем и т.д.
   - **Arm/disarm status** - срабатывает при постановке/снятии региона с охраны.
   - **Fire alarm** - срабатывает, когда происходит пожарная тревога.
   - **Silent alarm** - срабатывает, когда происходит тихая тревога.
   - **Open too long** - срабатывает, когда дверь открыта слишком долго.
   - **Door forced** - срабатывает при принудительном удержании двери.
4. Из раскрывающегося списка **Парам (зав. от типа)** (**3**):
   a. если выбран тип выхода **Matching success** и **Matching failed**, выбрать номер двери, которая будет открыта при срабатывании соответствующего выхода: от **1** до **4**.
   b. если выбран тип выхода **Alarm output, Fire alarm** или **Silent alarm**, выбрать номер раздела, в котором сработает тревога при срабатывании соответствующего выхода: от **1** до **4**.
   c. если выбран тип выхода **Scheduled output**, выбрать номер расписания, согласно которому сработает соответствующий выход: от **0** до **255**.
5. Из раскрывающегося списка **Activation time** (**4**) выбрать время в секундах, на которое будет активирован выход: от **0** до **255**.
6. Установить флажок **Инвертированный выход** (**5**), если необходимо инвертировать выход.
7. Нажать кнопку **Применить** (**6**) для применения настроек.

Настройка выхода *Virdi* завершена.

3.2.4 Настройка двери Virdi

Настройка двери *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Дверь Virdi**, который создается на базе объекта **ACU Virdi**.



2. Из раскрывающегося списка **Номер двери** (**1**) выбрать номер входа: от **1** до **4**.
3. Из раскрывающегося списка **Зона двери** (**2**) выбрать зону, к которой будет относиться данная дверь:
   - ***Unassigned*** - не назначено.
   - от **1** до **8**.
4. Из раскрывающегося списка **Задержка удержания** (**3**) выбрать время в секундах, по истечении которого открытая дверь будет считаться удерживаемой: от **0** до **255**.

> **Примечание**
>
> - Общее время до появления тревоги удержания двери считается следующим образом: время **Open time** (см. Настройка считывателя Virdi) + время **Door held delay**.
> - Для получения данной тревоги тип зоны, к которой относится данная дверь, должен быть **Exit1**, **Exit2**, **Instant** или **Interior**.

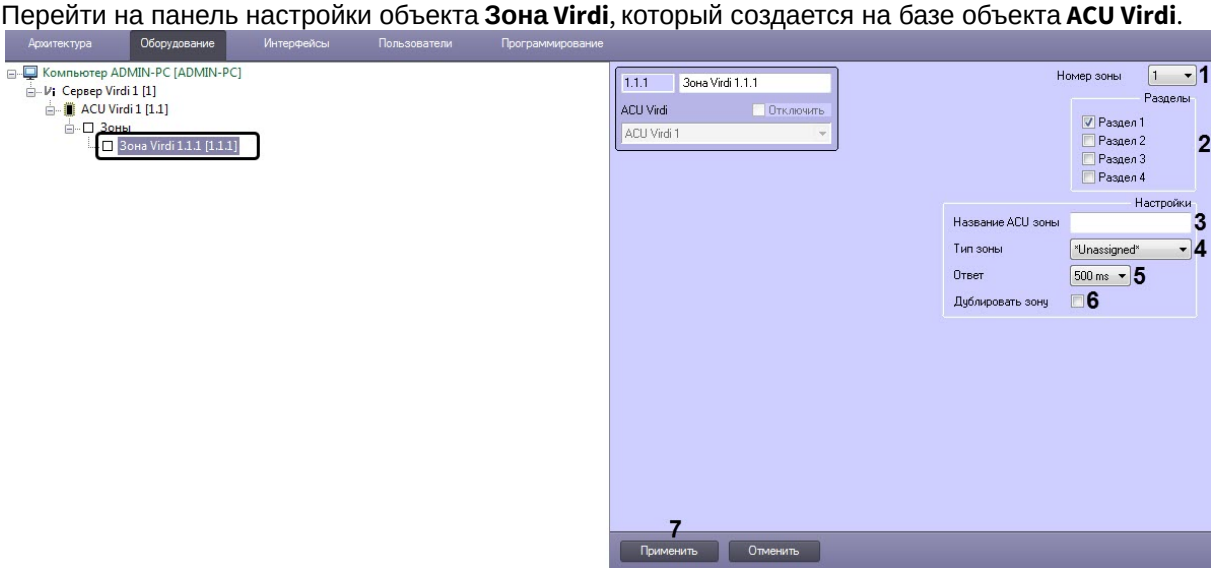
5. Установить флажок **Включить тревогу взлома двери** (**4**), если необходимо отслеживать удержание двери.
6. Установить флажок **Громкая тревога взлома двери** (**5**), если необходимо при удержании двери генерировать визуальную и звуковую тревогу на считывателе данной двери.
7. Нажать кнопку **Применить** (**6**) для применения настроек.

Настройка двери *Virdi* завершена.

3.2.5 Настройка зоны Virdi

Настройка зоны *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Зона Virdi**, который создается на базе объекта **ACU Virdi**.



2. Из раскрывающегося списка **Номер зоны** (**1**) выбрать номер зоны: от **1** до **8**.
3. Установить флажки напротив соответствующих разделов (**2**), которые необходимо включить в данную зону.
4. В поле **Название ACU зоны** (**3**) ввести произвольное имя данной зоны (не более 10 символов).
5. Из раскрывающегося списка **Тип зоны** (**4**) выбрать тип зоны:
   - ***Unused*** - не используется.
   - **Exit1** - данный тип зоны имеет временную задержку на вход и выход, которая задается на панели настройки раздела *Virdi* в параметрах **Entry delay 1** и **Exit delay 1** соответственно (см. Настройка раздела Virdi).
   - **Exit2** - данный тип зоны имеет временную задержку на вход и выход, которая задается на панели настройки раздела *Virdi* в параметрах **Entry delay 2** и **Exit delay 2** соответственно (см. Настройка раздела Virdi).
   - **Instant** - данный тип зоны используется при мониторинге периметра зоны. Данный тип зоны не имеет временной задержки и подаст сигнал тревоги сразу, если раздел зоны поставлен на охрану и зона будет открыта.
   - **Interior** - данный тип зоны используется при мониторинге внутренней области зоны и имеет временную задержку на вход и выход, которая задается на панели настройки раздела *Virdi* в параметрах **Entry delay** и **Exit delay** соответственно. Если раздел поставлен на охрану и нет задержки на вход или выход, то данная зона немедленно подаст сигнал тревоги.
   - **24H Emergency** - данный тип зоны всегда активен, независимо от того, поставлен ли раздел на охрану или нет. Данный тип зоны предназначен для сигнализации и мониторинга.
   - **24H Silent panic** - данный тип зоны всегда активен, независимо от того, поставлен ли раздел на охрану или нет. Данный тип зоны предназначен только для мониторинга.
   - **Fire** - данный тип зоны отслеживает появление пожарной тревоги и неисправности. Пожарная тревога возникает, если зона пожара замкнута, а неисправность - если пожарная зона отключена.
   - **Arm/Disarm** - внешняя кнопка или сигнал могут ставить/снимать контроллер с охраны, когда данная зона открыта или закрыта.
   - ***Unassigned*** - не назначено.
6. Из раскрывающегося списка **Ответ** (**5**) выбрать время отклика изменения состояния зоны в секундах. Если зона открыта/закрыта в течение данного времени, то произойдет изменение состояния зоны: **500 ms** или **100 ms**.

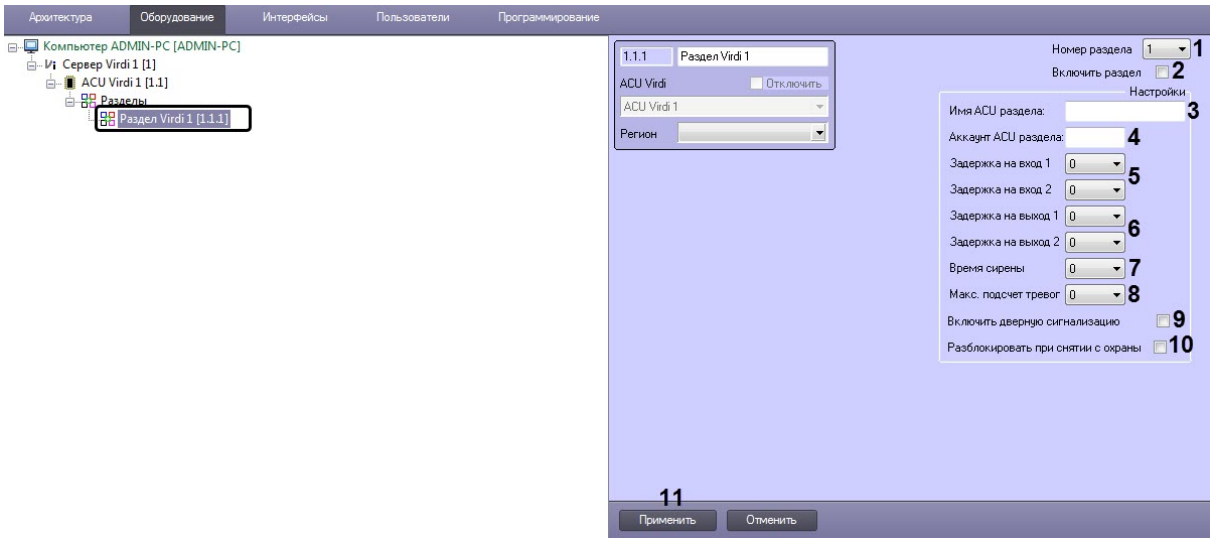
7. Установить флажок **Дублировать зону** (**6**), если требуется больше, чем 4 аппаратных входа для зон.
8. Нажать кнопку **Применить** (**7**) для применения настроек.

Настройка зоны *Virdi* завершена.

3.2.6 Настройка раздела Virdi

Настройка раздела *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Раздел Virdi**, который создается на базе объекта **ACU Virdi**.



2. Из раскрывающегося списка **Номер раздела** (**1**) выбрать номер раздела: от **1** до **4**.
3. Установить флажок **Включить раздел** (**2**), чтобы активировать данный раздел.
4. В поле **Имя ACU раздела** (**3**) ввести название раздела (максимум 16 символов).
5. В поле **Аккаунт ACU раздела** (**4**) ввести номер учетной записи раздела в виде 4-х шестнадцатеричных цифр. По умолчанию номер учетной записи совпадает с идентификатором контроллера.
6. Из раскрывающихся списков **Задержка на вход 1 и Задержка на вход 2** (**5**) выбрать в секундах временную задержку на вход: от **0** до **255**.
7. Из раскрывающихся списков **Задержка на выход 1 и Задержка на выход 2** (**6**) выбрать в секундах временную задержку на выход: от **0** до **255**.

> **Примечание**
>
> - **Задержка на вход 1** и **Задержка на выход 1** действует на все зоны типа **EXIT1**.
> - **Задержка на вход 2** и **Задержка на выход 2** действует на все зоны типа **EXIT2**.

8. Из раскрывающегося списка **Время сирены** (**7**) выбрать в секундах время действия сигнала сирены при возникновении в разделе тревоги: от **0** до **255**.
9. Из раскрывающегося списка **Макс. подсчет тревог** (**8**) выбрать максимальное количество повторений сигнала сирены при возникновении в разделе тревоги: от **0** до **255**.
10. Установить флажок **Включить дверную сигнализацию** (**9**), если необходимо, чтобы считыватель издавал 2 коротких звуковых сигнала при открытии зоны типа **EXIT1**, **EXIT2** или **INSTANT** и назначенных им разделов. Это можно использовать в качестве индикатора открытия двери, но не в качестве индикатора тревоги.

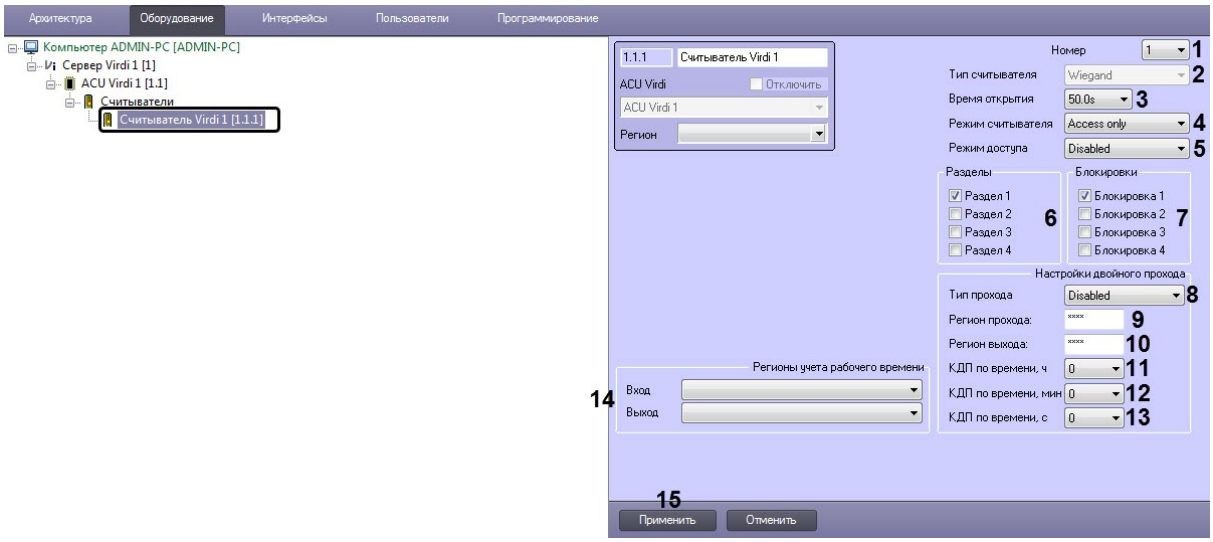
11. Установить флажок **Разблокировать при снятии с охраны** (**10**), если необходимо, чтобы двери, принадлежащие данному разделу, автоматически разблокировывались при снятии раздела с охраны. Двери будут открыты до повторной постановки раздела на охрану.
12. Нажать кнопку **Применить** (**11**) для применения настроек.

Настройка раздела *Virdi* завершена.

3.2.7 Настройка считывателя Virdi

Настройка считывателя *Virdi* осуществляется следующим образом:

1. Перейти на панель настройки объекта **Считыватель Virdi**, который создается на базе объекта **ACU Virdi**.



2. Из раскрывающегося списка **Номер** (**1**) выбрать номер считывателя: от **1** до **12**.

> **Примечание**
>
> В раскрывающемся списке **Тип считывателя** (**2**) указан тип считывателя. Изменить данное значение нельзя.

3. Из раскрывающегося списка **Время открытия** (**3**) выбрать время в секундах, на которое будет открыта дверь после успешной аутентификации пользователя: от **1s** до **255s**.
4. Из раскрывающегося списка **Режим считывателя** (**4**) выбрать режим предоставления доступа:
   - **Access only** - после успешной аутентификации пользователя, назначенная считывателю дверь будет открыта на заданное в параметре **Open time** время.
   - **Access + Security** - после успешной аутентификации пользователя, назначенная считывателю дверь будет открыта на заданное в параметре **Opentime** время. Если на контроллере нажата клавиша F1, то после успешной аутентификации пользователя, назначенный считывателю и пользователю раздел, будет автоматически поставлен на охрану. Если раздел уже поставлен на охрану, то данный раздел автоматически будет снят с охраны, а дверь будет разблокирована.

> **Примечание**

Если режим предоставления доступа установлен как **Access + Security**, то аутентификация пользователей будет происходить в режиме **Offline mode**, независимо от установленного режима работы аутентификации контроллера (см. Системные настройки контроллера Virdi).

5. Из раскрывающегося списка **Режим доступа** (**5**) выбрать режим доступа:
   - **Disabled** - отключен.
   - **Enter** - вход
   - **Exit** - выход.
   - **Out** - из территории.
   - **In** - на территорию.
6. Установить флажки напротив соответствующих разделов (**6**), к которым будет относиться данный считыватель.
7. Установить флажки напротив соответствующих дверей (**7**), к которым будет относится данный считыватель.
8. Из раскрывающегося списка **Тип прохода** (**8**) выбрать режим контроля двойного прохода:
   - **Disabled** - отключен.
   - **Hard Passback** (строгий) - запрет повторного входа в зону доступа вплоть до выхода из зоны.
   - **Soft Passback** (мягкий) - повторный доступ не запрещается, но в случае нарушения формируются соответствующее событие.
   - **Timed Passback** (временной) - в течение заданного времени после прохода используется строгий режим, после истечения данного времени - мягкий.

   > **Примечание**
   >
   > **Timed Passback** недоступен, если контроль двойного прохода осуществляется Сервером (см. Системные настройки контроллера Virdi).

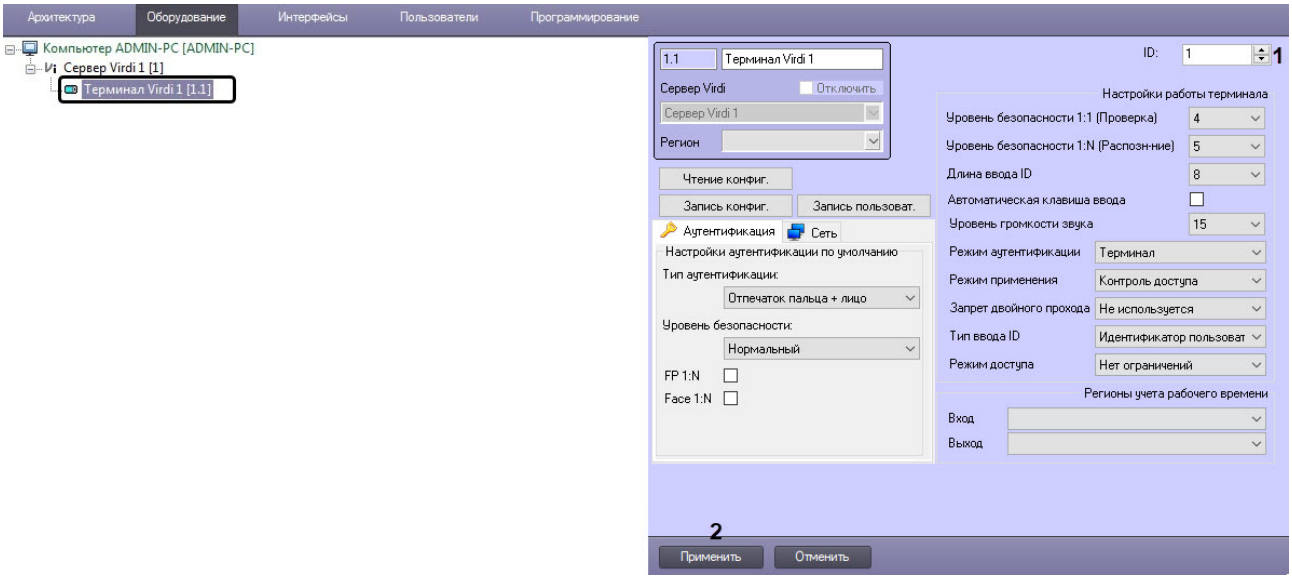
9. В поле **Регион прохода** (**9**) ввести произвольное название региона на вход (максимум 4 символа). В зависимости от выбранного режима контроля двойного прохода, пользователю будет запрещено или разрешено входить в указанный регион повторно (необходимо, чтобы данное название региона было указано хотя бы у 2-х считывателей).
10. В поле **Регион выхода** (**10**) ввести произвольное название региона на выход (максимум 4 символа). В зависимости от выбранного режима контроля двойного прохода, пользователю будет запрещено или разрешено выходить из указанного региона повторно (необходимо, чтобы данное название региона было указано хотя бы у 2-х считывателей).
11. Если выбран режим проверки двойного прохода **Timed Passback**, то из раскрывающегося списка **КДП по времени, ч** (**11**) выбрать время в часах, в течении которого будет использоваться строгий режим.
12. Если выбран режим проверки двойного прохода **Timed Passback**, то из раскрывающегося списка **КДП по времени, мин** (**12**) выбрать время в минутах, в течении которого будет использоваться строгий режим.
13. Если выбран режим проверки двойного прохода **Timed Passback**, то из раскрывающегося списка **КДП по времени, с** (**13**) выбрать время в секундах, в течении которого будет использоваться строгий режим.
14. Из раскрывающихся списков **Entrance** и **Exit** (**14**) выбрать разделы, расположенные со стороны входа и выхода через дверь соответственно.
15. Нажать кнопку **Применить** (**15**) для применения настроек.

Настройка считывателя *Virdi* завершена.

3.3 Настройка терминала Virdi

Настройка терминала *Virdi* осуществляется на панели настройки объекта **Терминал Virdi**, который созд ается на базе объекта **Сервер Virdi**.

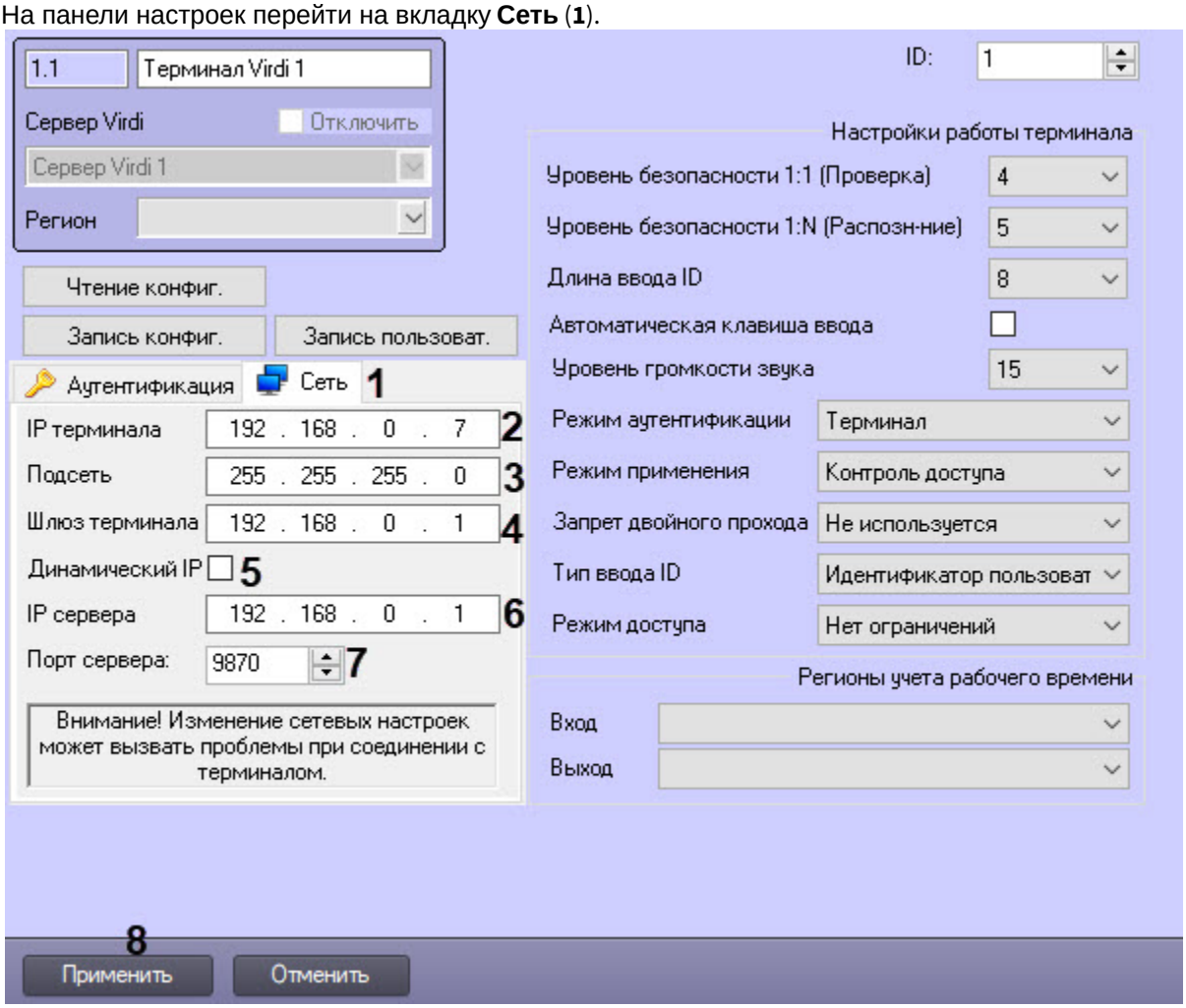
После создания объекта **Терминал Virdi** необходимо в поле **ID** (**1**) указать идентификатор данного терминала и нажать кнопку **Применить** (**2**).



3.3.1 Настройка соединения терминала Virdi

Настройка соединения терминала *Virdi* осуществляется следующим образом:

1. На панели настроек перейти на вкладку **Сеть** (**1**).



2. В поле **IP терминала** (**2**) ввести IP-адрес терминала.
3. В поле **Подсеть** (**3**) ввести маску подсети терминала.
4. В поле **Шлюз терминала** (**4**) ввести шлюз терминала.
5. Установить флажок **Динамический IP** (**5**), если терминал работает в сети с DHCP протоколом.
6. В поле **IP сервера** (**6**) ввести IP-адрес Сервера ПК *ACFA-Интеллект*.
7. В поле **Порт сервера** (**7**) ввести порт Сервера ПК *ACFA-Интеллект*.
8. Нажать кнопку **Применить** (**8**) для применения настроек.

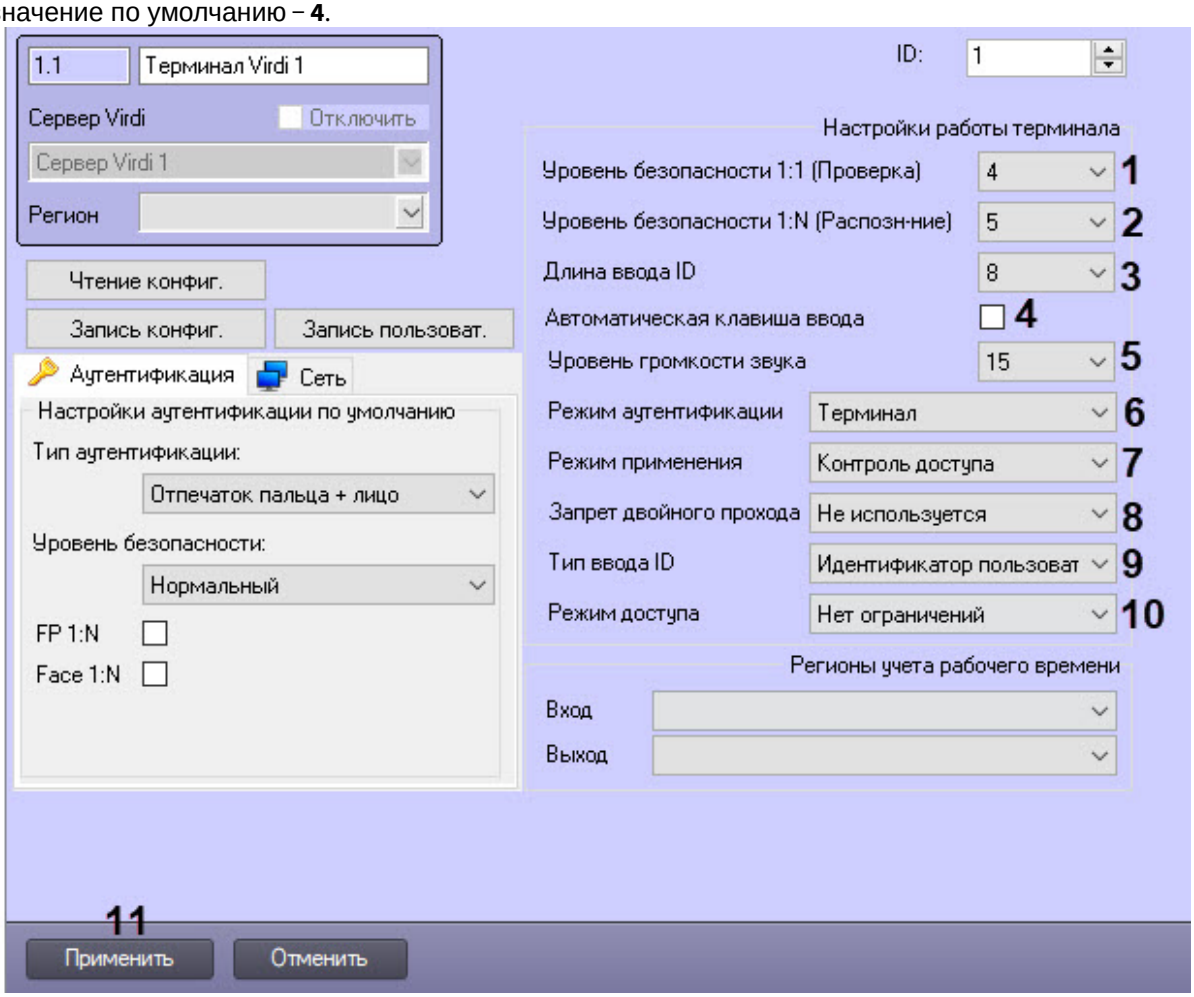
Настройка соединения терминала *Virdi* завершена.

3.3.2 Системные настройки терминала Virdi

Системные настройки терминала *Virdi* осуществляются следующим образом:

1. Из раскрывающегося списка **Уровень безопасности 1:1 (Проверка)** (**1**) выбрать уровень качества верификации, если используется только один тип аутентификации: от **1** до **9**,

значение по умолчанию – **4**.



2. Из раскрывающегося списка **Уровень безопасности 1:N (Распознавание)** (**2**) выбрать уровень качества идентификации, если используется несколько типов аутентификации: от **1** до **9**, значение по умолчанию – **5**.
3. Из раскрывающегося списка **Длина ввода ID** (**3**) выбрать длину идентификатора пользователя : от **4** до **8**.

> **Внимание!**
>
> Для работы в ПК *ACFA-Интеллект* необходимо выбрать значение **8**. Также в самом терминале **Длина ввода ID** должна быть установлена в значение **8**.

4. Установить флажок **Автоматическая клавиша ввода** (**4**), если необходимо разрешить автоматический ввод ключа с клавиатуры терминала (кнопки F1-F4).
5. Из раскрывающегося списка **Уровень громкости звука** (**5**) выбрать уровень громкости динамика терминала: от **0** до **20**.
6. Из раскрывающегося списка **Режим аутентификации** (**6**) выбрать режим аутентификации и работы терминала:
   - **Сервер/Терминал** - принятие решений осуществляется Сервером, а если он недоступен, то терминалом.
   - **Терминал/Сервер** - принятие решений осуществляется терминалом, а если он недоступен, то Сервером.
   - **Сервер** - принятие решений осуществляется Сервером.

- **Терминал** - принятие решений осуществляется терминалом.
- **Режим оффлайн** - автономный режим терминала.

> **Примечание**
>
> В автономном режиме терминала управление с Сервера ПК *ACFA-Интеллект* недоступно.

7. Из раскрывающегося списка **Режим применения** (**7**) выбрать режим работы терминала:
   - **Контроль доступа** - режим точки доступа.

   > **Внимание!**
   >
   > Для работы терминала с ПК *ACFA-Интеллект* необходимо выбрать режим работы **Контроль доступа**.

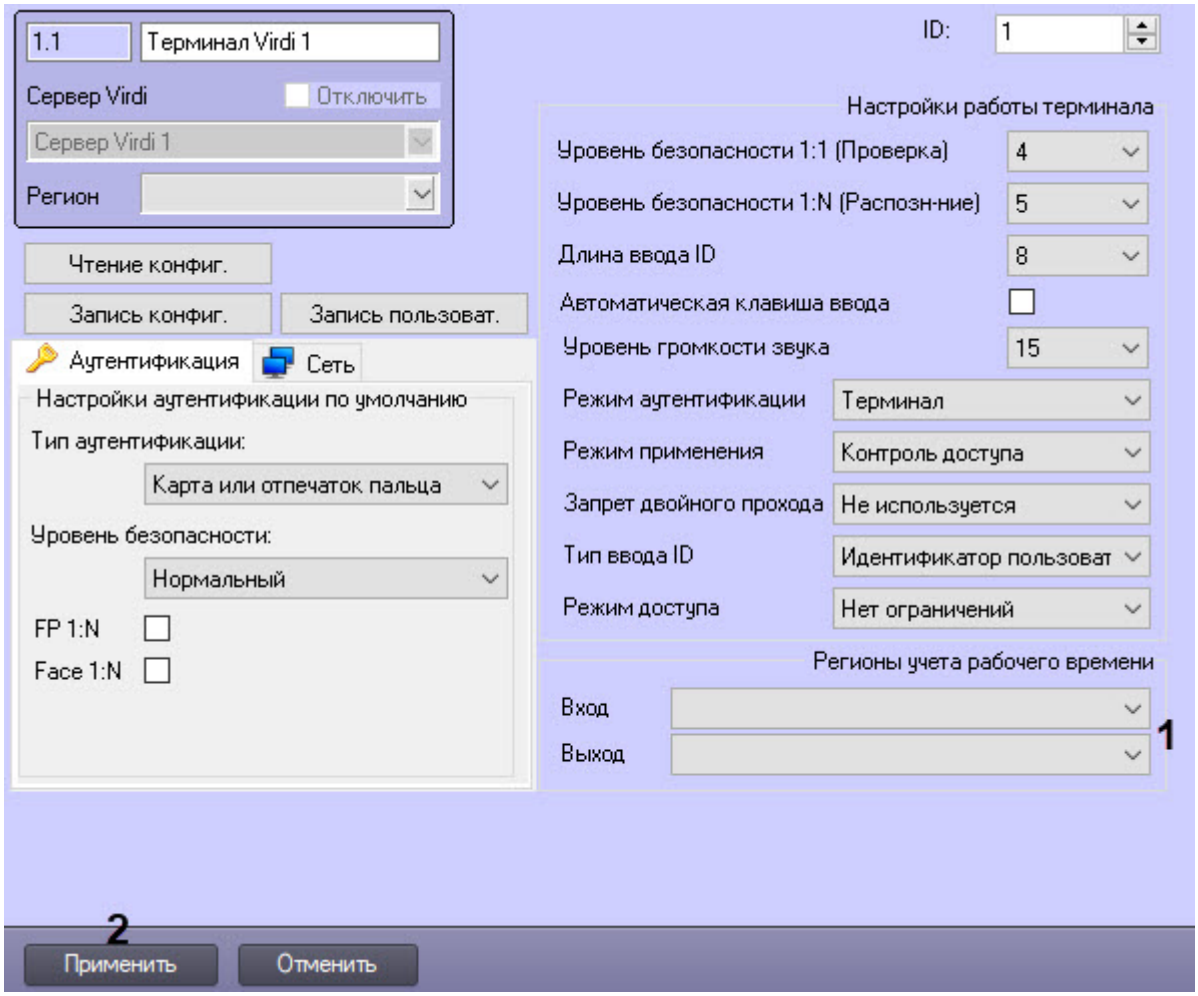
   - **Время/Появление на работе** - режим учета рабочего времени.
   - **Пьет воду...** - режим совместимости с алкотестерами.
8. Из раскрывающегося списка **Запрет двойного прохода** (**8**) выбрать режим поведения терминала при обнаружении двойного прохода:
   - **Не используется** - не используется.
   - **Пустить при потере связи** - разрешать проход, если связь с Сервером потеряна.
   - **Не пускать при потере связи** - запрещать проход, если связь с Сервером потеряна.
9. Из раскрывающегося списка **Тип ввода ID** (**9**) выбрать тип идентификаторов пользователей:
   - **Идентификатор пользователя** - собственные идентификаторы пользователей.
   - **Уникальный идентификатор** - заданные в терминале уникальные идентификаторы пользователей.
10. Из раскрывающегося списка **Режим доступа** (**10**) выбрать режим предоставления доступа терминалом, если на терминале отсутствует клавиатура для ввода цифр:
    - **Нет ограничений** - без ограничений.
    - **Только пальцы и пароли** - только отпечатки пальцев и пароль.
11. Нажать кнопку **Применить** (**11**) для применения настроек.

Системные настройки терминала *Virdi* завершены.

3.3.3 Настройка разделов терминала Virdi

Настройка разделов терминала *Virdi* осуществляется следующим образом:

1. Из раскрывающегося списка **Вход** и **Выход** (**1**) выбрать разделы, расположенные со стороны входа и выхода через дверь соответственно.



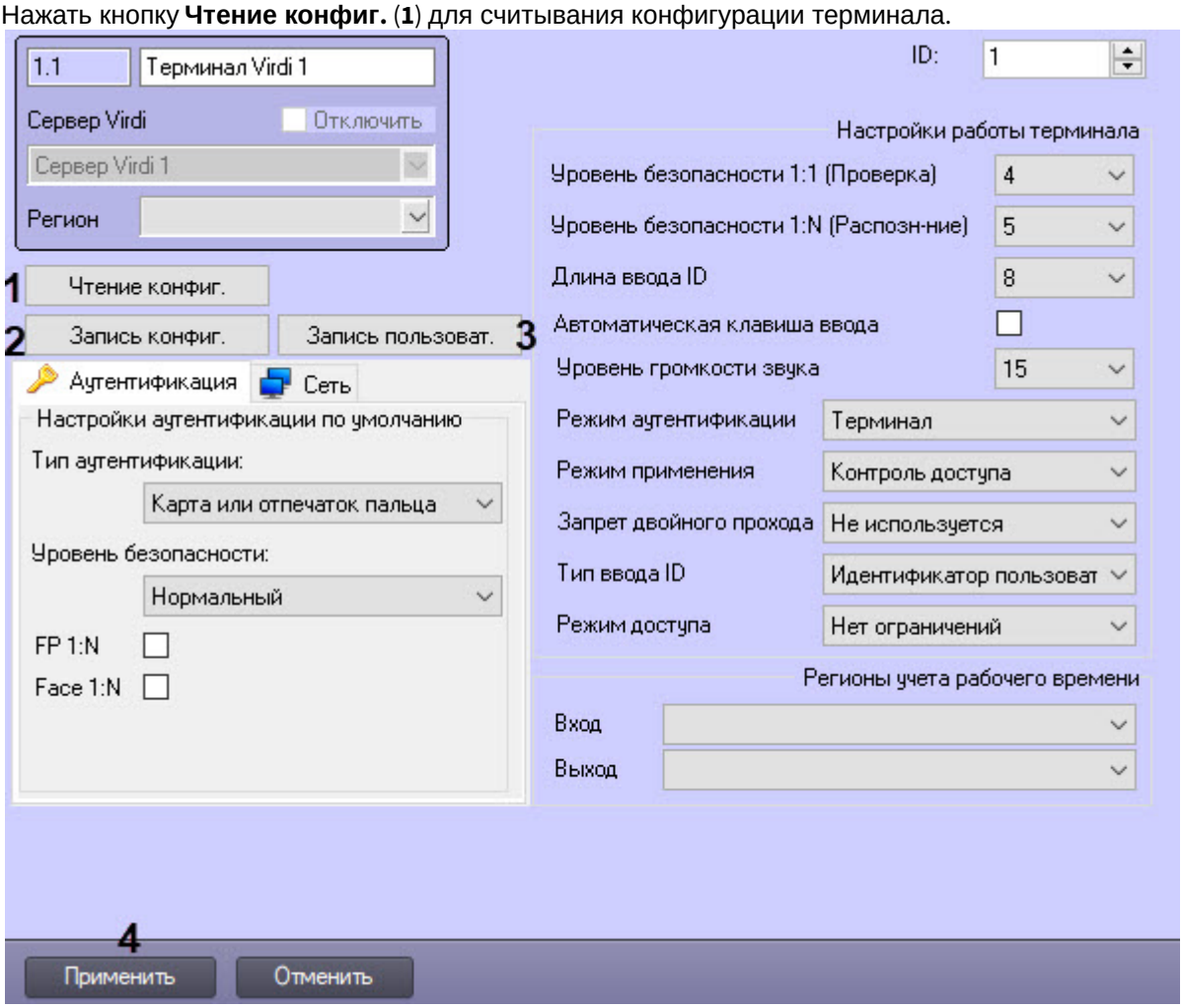
2. Нажать кнопку **Применить** (**2**) для применения настроек.

Настройка разделов терминала *Virdi* завершена.

3.3.4 Управление конфигурацией терминала Virdi

Управление конфигурацией терминала *Virdi* осуществляется следующим образом:

1. Нажать кнопку **Чтение конфиг.** (**1**) для считывания конфигурации терминала.

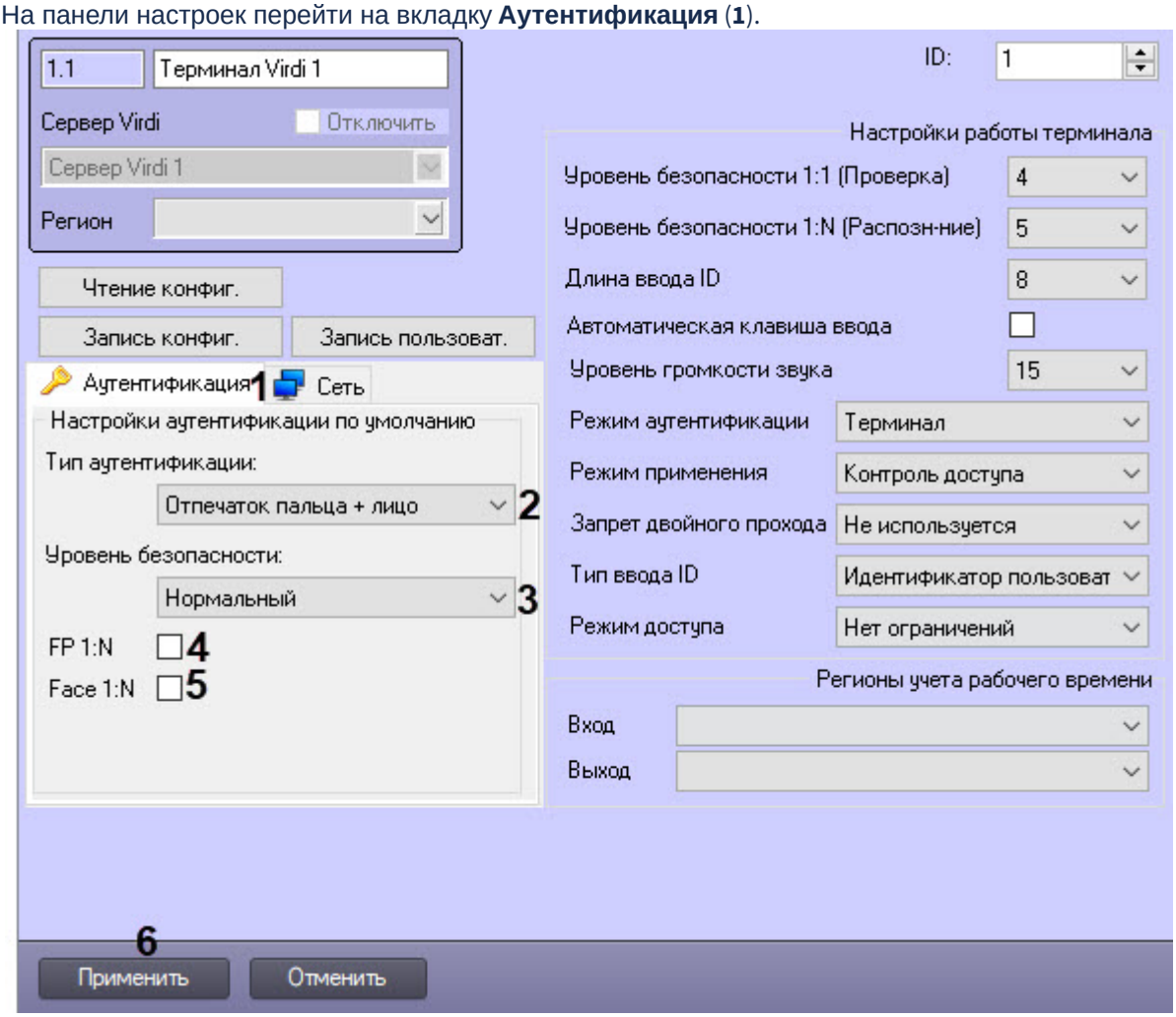


2. Нажать кнопку **Запись конфиг.** (**2**) для записи текущей конфигурации в терминал.
3. Нажать кнопку **Запись пользоват.** (**3**) для пересылки пользователей в терминал.
4. Нажать кнопку **Применить** (**4**) для применения настроек.

3.3.5 Настройка аутентификации

Настройка параметров аутентификации пользователя терминала *Virdi* осуществляется следующим образом:

1. На панели настроек перейти на вкладку **Аутентификация** (**1**).



2. В поле **Тип аутентификации** (**2**) из выпадающего списка выбрать тип аутентификации по умолчанию.
3. Выбрать из раскрывающегося списка **Уровень безопасности** (**3**) требуемый уровень качества аутентификации по умолчанию, от **Самый низкий** до **Самый высокий**.
4. Выставить флажок **FP 1:N** (**4**) для включения возможности аутентификации, когда первым подносится палец, который сверяется со всей базой отпечатков устройства. Проверка может пройти с задержкой в зависимости от количества отпечатков в базе отпечатков.
5. Выставить флажок **Face 1:N** (**5**) для включения возможности аутентификации, когда первым проверяется лицо, которое сверяется со всей базой лиц устройства. Проверка может пройти с задержкой в зависимости от количества лиц в базе лиц.
6. Для сохранения изменений нажать кнопку **Применить** (**6**).

4 Работа с модулем интеграции Virdi

4.1 Общие сведения о работе с модулем интеграции Virdi

Для работы с модулем интеграции *Virdi* 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 Управление терминалом Virdi

Управление терминалом *Virdi* осуществляется в интерактивном окне **Карта** с использованием функционального меню объекта **Терминал Virdi**.

Команды для управления терминалом *Virdi* описаны в таблице:

Команда функционального меню	Выполняемая функция
Заблокировать терминал	Блокирует терминал
Открыть дверь	Открывает дверь
Разблокировать терминал	Снимает блокировку терминала
Закрыть дверь	Закрывает дверь
Открыть дверь (в течении длительного времени)	Открывает дверь надолго

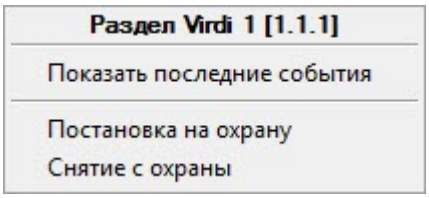
Возможны следующие состояния терминала *Virdi:*

	Корпус взломан

Терминал Virdi 1 [1.1] 	Потеря связи
Терминал Virdi 1 [1.1] 	Заблокирован
Терминал Virdi 1 [1.1] 	Закрыто
Терминал Virdi 1 [1.1] 	Взлом двери
Терминал Virdi 1 [1.1] 	Удержание двери
Терминал Virdi 1 [1.1] 	Открыто
Терминал Virdi 1 [1.1] 	На связи

4.3 Управление разделом Virdi

Управление разделом *Virdi* осуществляется в интерактивном окне **Карта** с использованием функционального меню объекта **Раздел Virdi**.



Команды для управления разделом *Virdi* описаны в таблице:

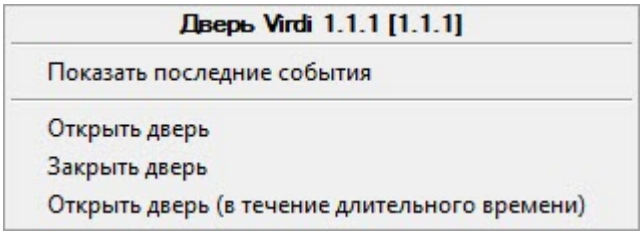
Команда функционального меню	Выполняемая функция
Поставка на охрану	Ставит раздел на охрану
Снятие с охраны	Снимает раздел с охраны

Возможны следующие состояния раздела *Virdi:*

	Снят с охраны
	На охране
	Тревога

4.4 Управление дверью Virdi

Управление дверью *Virdi* осуществляется в интерактивном окне **Карта** с использованием функционального меню объекта **Дверь Virdi**.



Команды для управления дверью *Virdi* описаны в таблице:

Команда функционального меню	Выполняемая функция
Открыть дверь	Открывает дверь
Закрыть дверь	Закрывает дверь
Открыть дверь (в течение длительного времени)	Открывает дверь до тех пор, пока не будет послана команда на закрытие двери

Возможны следующие состояния двери *Virdi:*

Дверь Virdi 1.1.1 [1.1.1] 	Закрыто
Дверь Virdi 1.1.1 [1.1.1] 	Открыто

4.5 Управление контроллером, считывателем и зоной Virdi

Управление контроллером, считывателем и зоной *Virdi* в интерактивном окне **Карта** не осуществляется.

Возможны следующие состояния контроллера *Virdi*:

ACU Virdi 1 [1.1] 	Потеря связи
ACU Virdi 1 [1.1] 	Корпус взломан
ACU Virdi 1 [1.1] 	На связи

Возможны следующие состояния считывателя *Virdi*:

Считыватель Virdi 1 [1.1.1] 	Норма
Считыватель Virdi 1 [1.1.1] 	Ошибка на линии RS485
Считыватель Virdi 1 [1.1.1] 	Статус неизвестен

Возможны следующие состояния зоны *Virdi*:

Зона Virdi 1.1.1 [1.1.1] 	Норма
Зона Virdi 1.1.1 [1.1.1] 	Зона открыта
Зона Virdi 1.1.1 [1.1.1] 	Неисправность

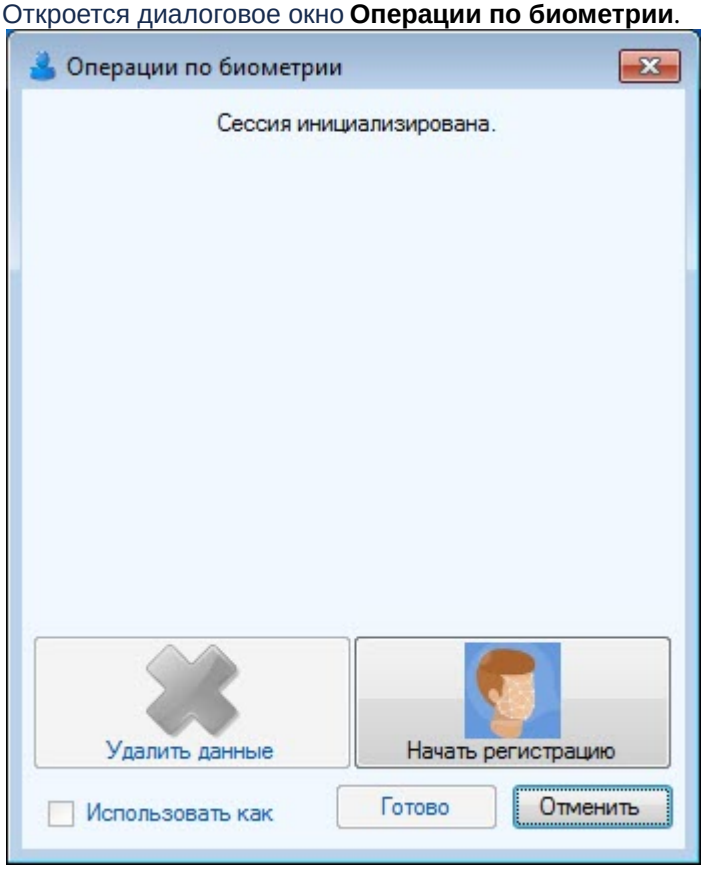
4.6 Добавление биометрических параметров Virdi

4.6.1 Добавление шаблона лица Virdi

Для добавления шаблона лица *Virdi* 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 **(Virdi Faces) <Название терминала Virdi>**, которое соответствует терминалу с биометрическим считывателем лица.

3. Откроется диалоговое окно **Операции по биометрии**.



4. Для добавления нового шаблона лица нажать кнопку **Начать регистрацию**. Далее необходимо следовать инструкциям на экране терминала. В случае успешного захвата лица отобразится

полученная фотография, шаблон которой будет сохранен.

5. Если необходимо использовать полученную фотографию в качестве фотографии пользователя, установить флажок **Использовать как фото человека** (см. Назначение пользователю фотографии).
6. Для удаления шаблона лица нажать кнопку **Удалить данные**.
7. Нажать кнопку **Готово** для сохранения шаблона лица.

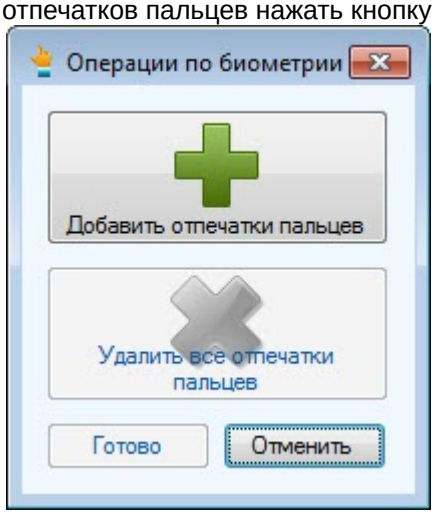
Добавление шаблона лица *Virdi* завершено.

4.6.2 Добавление шаблонов отпечатков пальцев Virdi

Для добавления шаблонов отпечатков пальцев *Virdi* 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 **(Virdi Fingerprints) <Название сервера Virdi/терминала>**, которое соответствует контроллеру с подключенным к нему биометрическим считывателем отпечатков пальцев, либо терминалу.

3. Откроется диалоговое окно **Операции по биометрии**. Для добавления нового шаблона отпечатков пальцев нажать кнопку **Добавить отпечатки пальцев**.



> **Примечание**
>
> Для удаления всех шаблонов необходимо нажать кнопку **Удалить все отпечатки пальцев**. Данная кнопка активна, если ранее уже были добавлены шаблоны отпечатков пальцев.

4. Откроется диалоговое окно **Virdi**. Для продолжения необходимо нажать кнопку **Next**.

5. Выбрать палец, для которого необходимо добавить шаблон.

6. Далее необходимо приложить палец к считывателю несколько раз.

7. В случае успешного захвата шаблон отпечатков пальца будет автоматически сохранен в контроллере/терминале.

8. Для добавления нового шаблона необходимо повторить процедуру, выбрав другой палец. Пальцы, для которых уже существует шаблон, выделяются зеленым цветом.

9. Нажать кнопку **Next** для завершения добавления шаблонов отпечатков пальцев.

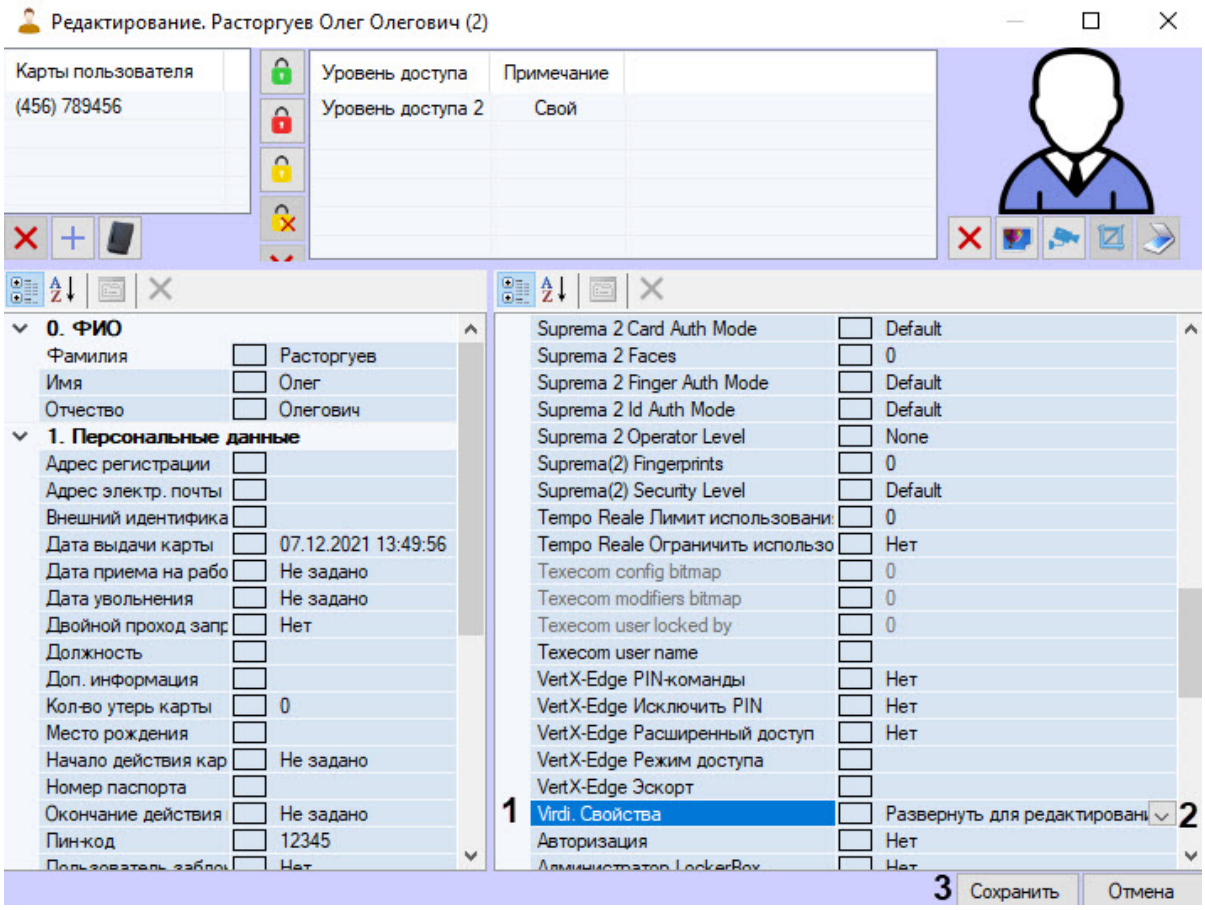
10. Нажать кнопку **Finish** для сохранения добавленных шаблонов отпечатков пальцев.

Добавление шаблонов отпечатков пальцев *Virdi* завершено.

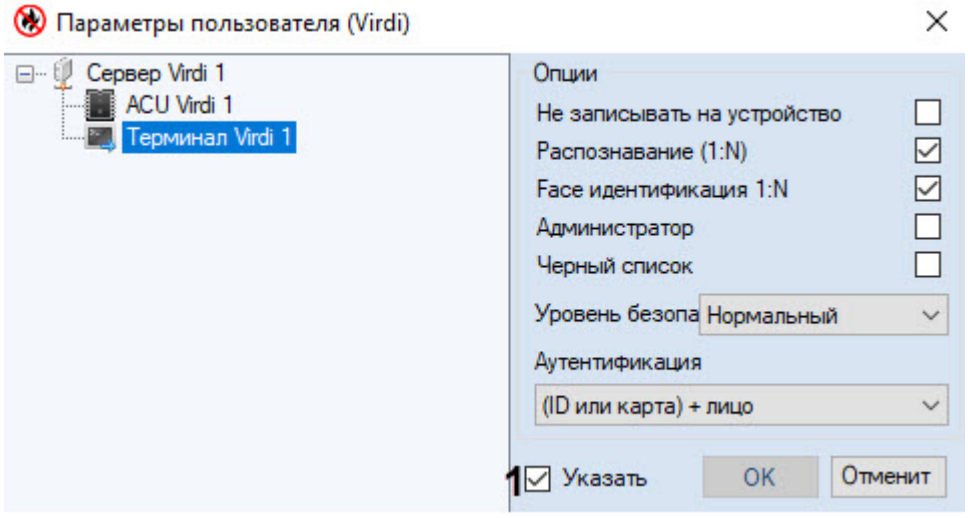
4.7 Работа с параметрами пользователя Virdi

Чтобы в ПК *ACFA-Интеллект* настроить параметры пользователя *Virdi*, следует выполнить следующие шаги:

1. В программном модуле *Бюро пропусков* открыть форму редактирования пользователя (подробнее см. Редактирование пользователя).
2. В открывшейся форме редактирования выбрать **Virdi. Свойства** (**1**) и далее нажать кнопку **Развернуть для редактирования** (**2**).



3. Будет открыта форма **Параметры пользователя (Virdi)**, в которой выбрать настраиваемый объект:

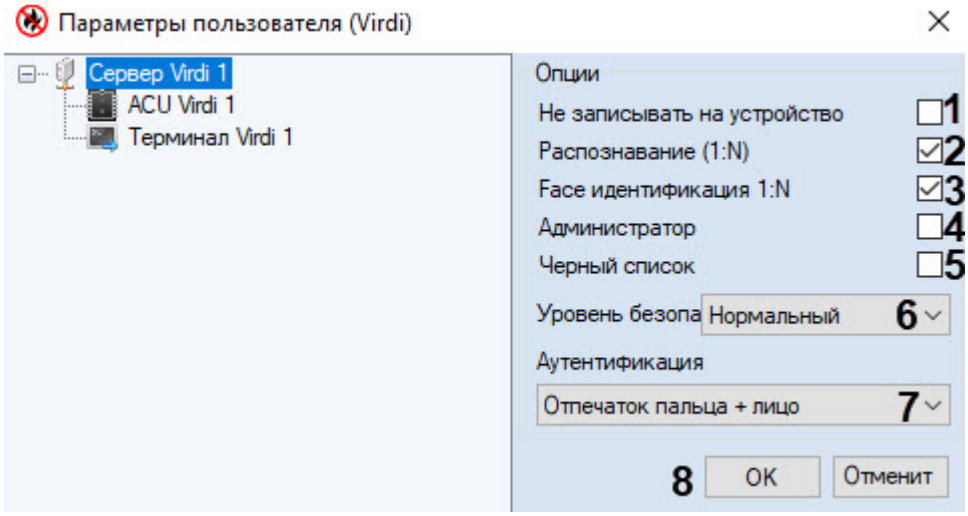


   a. **Сервер Virdi**;
   b. **ACU Virdi**;
   c. **Терминал Virdi**.

   Авторизация объекта **Сервер Virdi** включена по умолчанию. Чтобы включить авторизацию

объектов **ACU Virdi** и **Терминал Virdi**, следует выставить флажок **Указать** (**1**), после этого настройки этих объектов станут активными.

4. Чтобы не записывать пользователя на устройство, выставить флажок **Не записывать на устройство** (**1**). В этом случае в режиме **Terminal** для этого пользователя проход будет запрещен как для неизвестного пользователя (см. Системные настройки терминала Virdi).



5. Выставить флажок **Распознавание (1:N)** (**2**), чтобы включить возможность распознавания, в которой в зависимости от выбранного типа аутентификации (**7**) происходит сверка пользовательских биометрических данных с базой данных устройства. Проверка может занять продолжительное время в зависимости от количества данных в базе.
6. Выставить флажок **Face идентификация 1:N** (**3**), чтобы первым распознавалось лицо, и это лицо сверялось со всей базой лиц устройства. Проверка может занять продолжительное время в зависимости от количества лиц в базе.
7. Выставить флажок **Администратор** (**4**), чтобы заблокировать настройки на самом оборудовании и разрешить изменять настройки только пользователю с ролью администратора.
8. Выставить флажок **Черный список** (**5**), чтобы включить блокировку пользователя.
9. Выбрать из раскрывающегося списка **Уровень безопасности** (**6**) требуемый уровень качества проверки, от **Самый низкий** до **Самый высокий**. Значение по умолчанию – **Нормальный**.
10. Выбрать из раскрывающегося списка **Аутентификация** (**7**) тип аутентификации:
    - **Отпечаток пальца** – только отпечаток пальца.
    - **Отпечаток пальца внутри карты (*)** – отпечаток пальца, приложенный к карте.
    - **Пароль –** только пароль.
    - **Карта –** только карта.
    - **Карта или отпечаток пальца –** карта или отпечаток пальца.
    - **Карта + отпечаток пальца** – карта + отпечаток пальца.
    - **Карта или пароль –** карта или пароль.
    - **Карта + пароль** – карта + пароль.
    - **(ID или Карта) + отпечаток пальца –** идентификатор пользователя или карта + отпечаток пальца.
    - **(ID или Карта) + пароль –** идентификатор пользователя или карта + пароль.
    - **Отпечаток пальца + пароль –** отпечаток пальца + пароль.
    - **Пароль, если палец не распознан** – пароль, если аутентификация по отпечатку пальца не удалась.
    - **Карта + пароль + отпечаток пальца –** карта + пароль + отпечаток пальца.
    - **Лицо** – лицо.
    - **Лицо или пароль –** лицо или пароль.
    - **Карта или лицо –** карта или лицо.
    - **Отпечаток пальца или лицо –** отпечаток пальца или лицо.

- **Карта или отпечаток или лицо –** карта или отпечаток пальца или лицо.
- **Карта + лицо –** карта + лицо.
- **(ID или карта) + лицо** – идентификатор пользователя или карта + лицо.
- **Отпечаток пальца + лицо –** отпечаток пальца + лицо.
- **Лицо + пароль –** лицо + пароль.
- **Карта + отпечаток пальца + лицо –** карта + отпечаток пальца + лицо.
- **Карта + лицо + пароль –** карта + лицо + пароль.
- **Отпечаток пальца + лицо + пароль –** отпечаток пальца + лицо + пароль.
- **Карта + отпечаток + лицо + пароль –** карта + отпечаток пальца + лицо + пароль.

11. Для сохранения изменений нажать кнопку **ОК** (**8**).

> **Примечание**
>
> При заданных в *Бюро пропусков* настройках пользователя *Virdi* они будут иметь приоритет перед настройками терминала *Virdi*/сервера *Virdi*. Если настройки в **Бюро пропусков** не сконфигурированы, то решения принимает терминал *Virdi*/сервер *Virdi*.