ACFA Intellect

Руководство по настройке и работе с модулем Виртуальный сервер доступа

Last update 14/08/2019

Содержание

1 Введение в Руководство по настройке и работе с модулем Виртуальный сервер доступа....3
1.1 Назначение документа....3
1.2 Общие сведения о программном модуле «Виртуальный сервер доступа»....3
2 Лицензирование модуля Виртуальный сервер доступа....4
3 Настройка программного модуля Виртуальный сервер доступа....5
3.1 Настройка виртуальной точки прохода при распознавании номеров автомобилей....5
3.2 Настройка виртуальной точки прохода при распознавании лиц....6
3.3 Организация двухфакторной верификации....8
3.3.1 Общие сведения о двухфакторной верификации....8
3.3.2 Настройка двухфакторной верификации....9
4 Работа программного модуля Виртуальный сервер доступа....13

1 Введение в Руководство по настройке и работе с модулем Виртуальный сервер доступа

На странице:

- Назначение документа
- Общие сведения о программном модуле «Виртуальный сервер доступа»

1.1 Назначение документа

Документ *Руководство по настройке и работе с модулем «Виртуальный сервер доступа»* является справочно-информационным пособием и предназначен для специалистов по настройке программных комплексов *Auto-Интеллект* и *Face-Интеллект*. В данном Руководстве представлены следующие материалы:

1. Общие сведения о модуле *Виртуальный сервер доступа*.
2. Настройка модуля *Виртуальный сервер доступа*.
3. Работа модуля *Виртуальный сервер доступа*.

1.2 Общие сведения о программном модуле «Виртуальный сервер доступа»

Программный модуль *Виртуальный сервер доступа* является частью программного комплекса *ACFA-Интеллект* и служит для создания виртуальных точек прохода (без оборудования СКУД) на базе распознавания лиц и номеров автомобилей и объединенной работы программных комплексов *Auto-Интеллект* и *Face-Интеллект* с программным модулем *Учет рабочего времени*.

Также программный модуль «Виртуальный сервер доступа» позволяет в системах СКУД осуществлять двухфакторную верификацию в режиме Карта + Лицо и выполнять различные действия в системе (например, открывать или закрывать шлагбаум) с помощью скриптов или макрокоманд по событиям **Проход** или **Запрет прохода** (см. Программный комплекс Интеллект. Руководство по программированию).

2 Лицензирование модуля Виртуальный сервер доступа

Данный модуль не лицензируется.

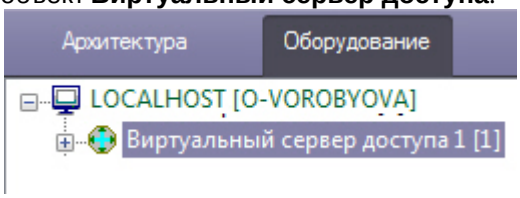
3 Настройка программного модуля Виртуальный сервер доступа

3.1 Настройка виртуальной точки прохода при распознавании номеров автомобилей

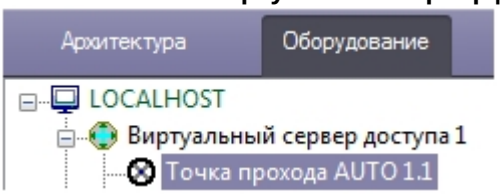
Организация виртуальной точки прохода при распознавании номеров автомобилей позволяет фиксировать проход (событие ACCESS_IN) при распознавании номера, который есть в базе данных (в настройках пользователя, задаваемых в программном модуле *Служба пропускного режима*).

Для организации виртуальной точки прохода при распознавании номеров автомобилей необходимо выполнить следующие действия:

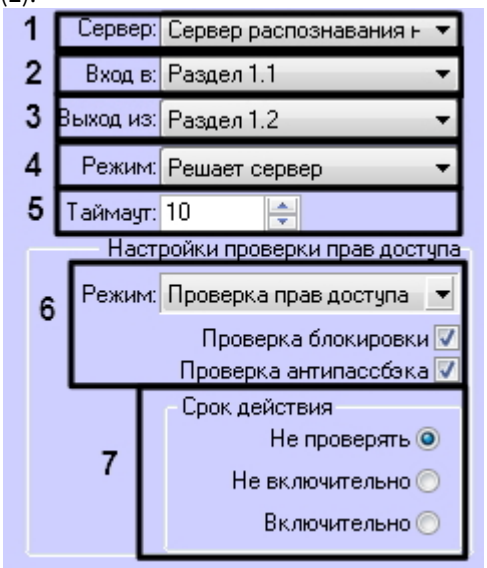
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода AUTO**.



3. Выполнить настройку точки прохода:
   a. Выбрать сервер распознавания номеров, на базе которого необходимо организовать точку прохода (**1**).



   b. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (**2**).
   c. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (**3**).
   d. Из раскрывающегося списка **Режим** выбрать режим предоставления доступа: автоматически (в том числе при помощи скрипта, контролирующего датчики двери) или по подтверждению от оператора путем нажатия на кнопку в **Диспетчере событий**. См. Работа с программным модулем Диспетчер событий (**4**).
   e. В поле **Таймаут** установить временной интервал ожидания подтверждения доступа в секундах (**5**).

> **Примечание**
>
> В течение выбранного таймаута все прочие запросы от сервера распознавания номеров игнорируются.

f. Если необходимо принимать решение о предоставлении доступа только на основании распознавания номеров установить режим **Только распознавание** (**4**). Если необходимо осуществлять проверку уровня доступа пользователя, которому принадлежит автомобиль, и временных зон этого уровня доступа, а также выполнять дополнительные проверки, выбрать режим **Проверка прав доступа** и установить флажки напротив тех проверок, которые необходимо осуществлять.
Проверка блокировки – если пользователь заблокирован, доступ предоставлен не будет.
Проверка антипассбэка – контроль двойного прохода через точку доступа.

> **Примечание.**
>
> Проверка уровня доступа и его временных зон будет осуществляться при режиме **Проверка прав доступа** всегда.

g. В разделе **Срок действия** установить переключатель в положение, соответствующее настройке проверки срока действия карты, указанного в интерфейсном модуле *Служба пропускного режима* (**5**).
Не проверять – если проверка срока действия карты не требуется.
Не включительно – не включать в проверку дату истечения срока действия карты.
Включительно – включать в проверку дату истечения срока действия карты.

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

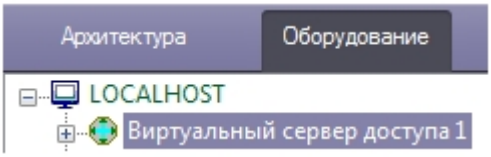
Организация виртуальной точки прохода при распознавании номеров автомобилей завершена.

3.2 Настройка виртуальной точки прохода при распознавании лиц

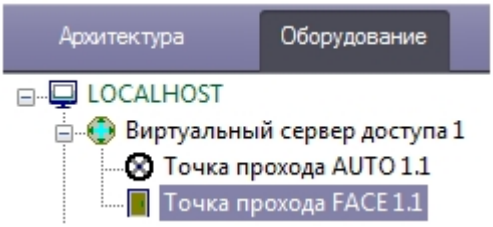
Организация виртуальной точки прохода при распознавании лиц позволяет фиксировать проход (событие ACCESS_IN) при распознавании лица, которое есть в базе данных (см. Программный комплекс Face-Интеллект. Руководство администратора).

Для организации виртуальной точки прохода при распознавании лиц необходимо выполнить следующие действия:

1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.

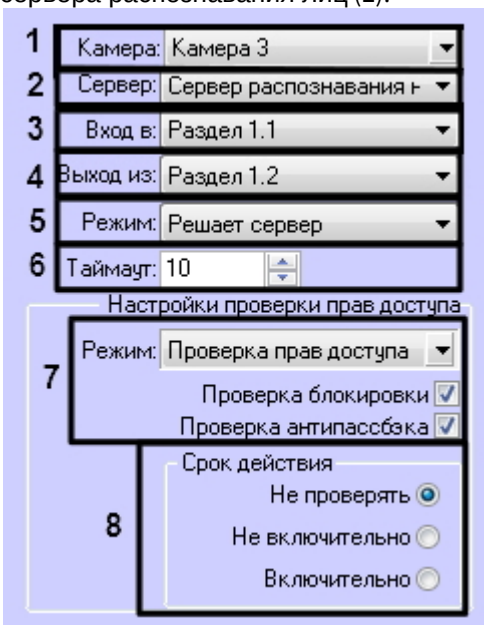


2. На базе объекта **Виртуальный сервер доступа** создать объект **Точка прохода FACE**.



3. Выполнить настройку точки прохода:

a. Выбрать камеру, которой осуществляется распознавание лиц. Камера должна работать в составе сервера распознавания лиц (**1**).



b. Выбрать сервер распознавания лиц, на базе которого необходимо организовать точку прохода (**2**).
c. Из раскрывающегося списка **Вход в** выбрать объект **Раздел** соответствующий территории, в которую осуществляется вход (**3**).
d. Из раскрывающегося списка **Выход из** выбрать объект **Раздел** соответствующий территории, из которой осуществляется выход (**4**).
e. Из раскрывающегося списка **Режим** выбрать режим предоставления доступа: автоматически (в том числе при помощи скрипта, контролирующего датчики двери) или по подтверждению от оператора путем нажатия на кнопку в **Диспетчере событий**. См. Работа с программным модулем Диспетчер событий (**4**).
f. В поле **Таймаут** установить временной интервал ожидания подтверждения доступа в секундах (**5**).

> **Примечание**
>
> В течение выбранного таймаута все прочие запросы от сервера распознавания лиц игнорируются.

g. Если необходимо принимать решение о предоставлении доступа только на основании распознавания лиц, установить режим **Только распознавание** (**5**). Если необходимо осуществлять проверку уровня доступа пользователя, чье лицо оказалось распознано, и временных зон этого уровня доступа, а также выполнять дополнительные проверки, выбрать режим **Проверка прав доступа** и установить флажки напротив тех проверок, которые необходимо осуществлять.
h. **Проверка блокировки** – если пользователь заблокирован, доступ предоставлен не будет.
Проверка антипассбэка – контроль двойного прохода через точку доступа.

> **Примечание.**
>
> Проверка уровня доступа и его временных зон будет осуществляться при режиме **Проверка прав доступа** всегда.

i. В разделе **Срок действия** установить переключатель в положение, соответствующее настройке проверки срока действия карты, указанного в интерфейсном модуле *Служба пропускного режима* (**6**).
Не проверять – если проверка срока действия карты не требуется.
Не включительно – не включать в проверку дату истечения срока действия карты.
Включительно – включать в проверку дату истечения срока действия карты.

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

Организация виртуальной точки прохода при распознавании лиц завершена.

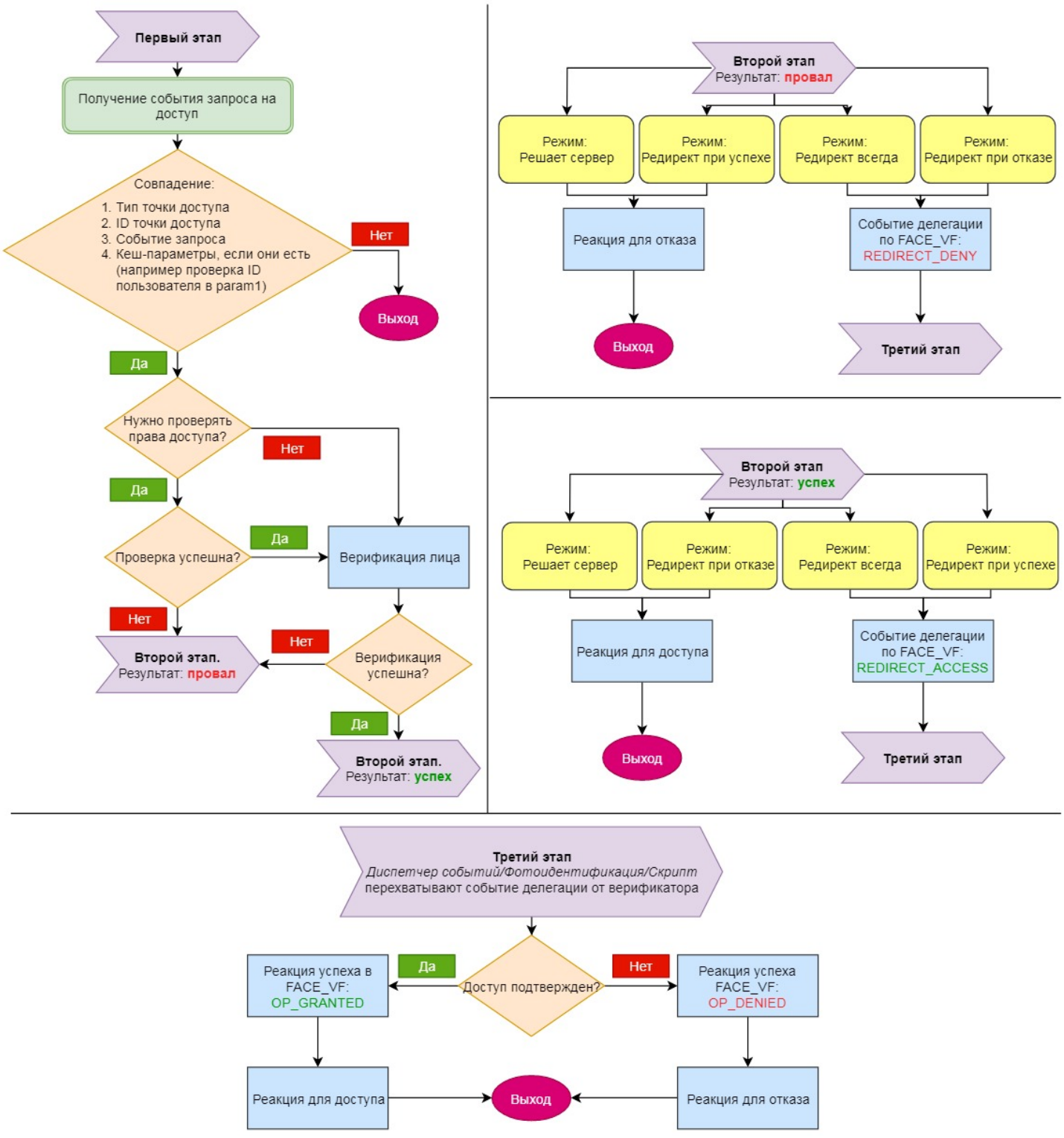
3.3 Организация двухфакторной верификации

3.3.1 Общие сведения о двухфакторной верификации

Двухфакторная верификация позволяет в системах СКУД предоставлять доступ только после совместной удачной проверки Карты доступа пользователя и Лица данного пользователя.

> **Внимание!**
>
> В данном режиме первой всегда должна прикладываться карта доступа пользователя и только затем происходить верификация лица.

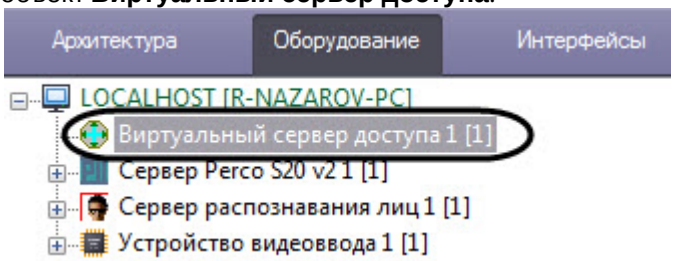
Двухфакторная верификация происходит в несколько этапов. Блок схема работы двухфакторной верификации представлена ниже.



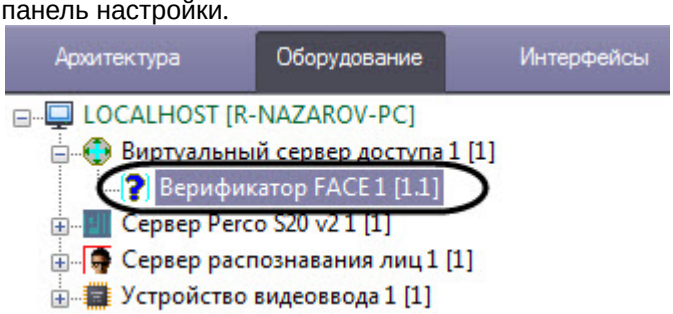
3.3.2 Настройка двухфакторной верификации

Для настройки двухфакторной верификации необходимо выполнить следующие действия:

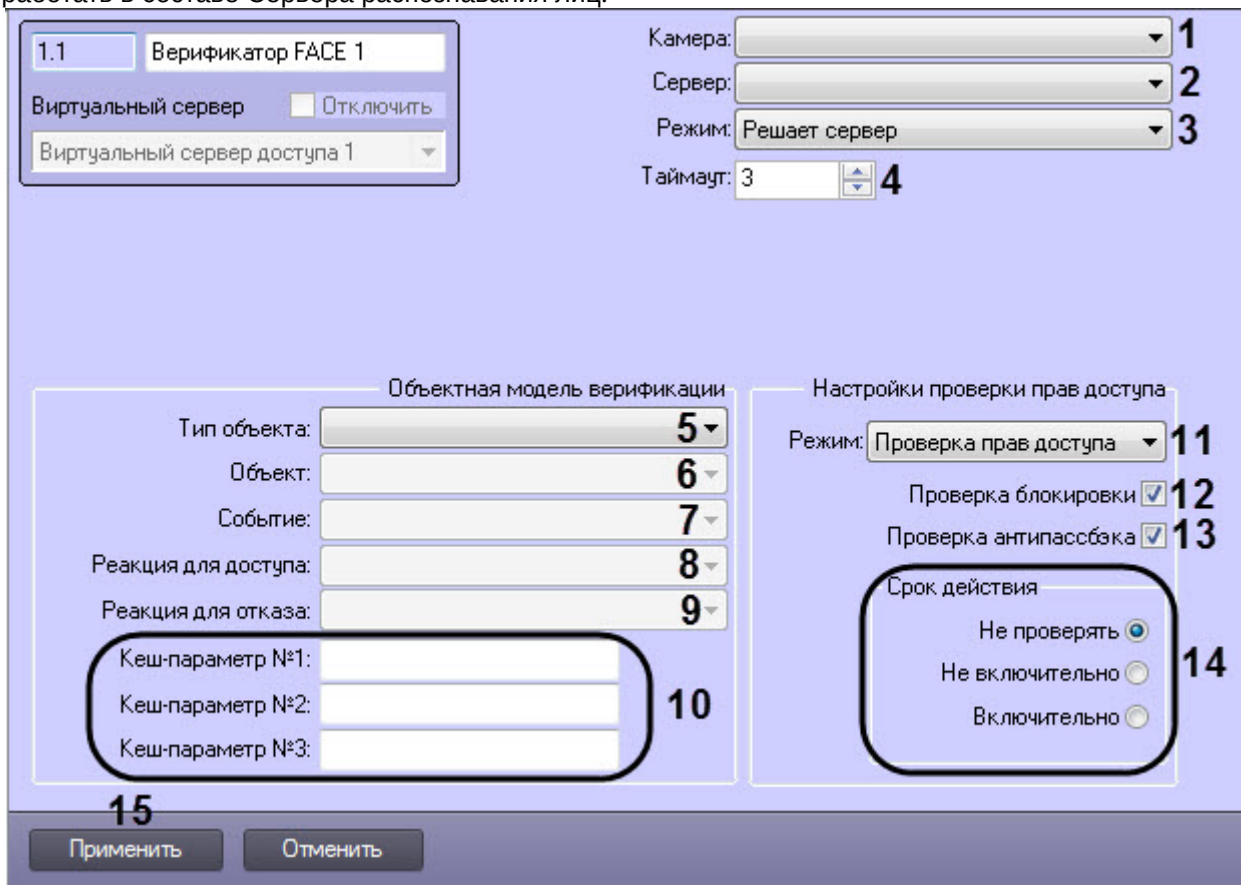
1. На базе объекта **Компьютер** на вкладке **Оборудование** диалогового окна **Настройка системы** создать объект **Виртуальный сервер доступа**.



2. На базе объекта **Виртуальный сервер доступа** создать объект **Верификатор FACE** и перейти на его панель настройки.



3. Из раскрывающегося списка **Камера** (**1**) выбрать камеру, которая осуществляет захват лиц. Камера должна работать в составе Сервера распознавания лиц.



4. Из раскрывающегося списка **Сервер** (**2**) выбрать Сервер распознавания лиц.
5. Из раскрывающегося списка **Режим** (**3**) выбрать режим работы верификатора:
   - **Решает сервер** - в зависимости от результата проверки/верификации лица генерируется реакция для доступа или отказа.
   - **Редирект всегда** - вне зависимости от результата второго этапа верификатор перенаправляет своё решение на *Диспетчер событий/Фотоидентификацию/Скрипт* с помощью события делегации и

ожидает решение внешнего верификатора. В зависимости от результата генерируется реакция для доступа или отказа.
- **Редирект при отказе** - если первый этап успешен, то данный режим аналогичен режиму **Решает сервер**. Если первый этап провален, то осуществляется делегация внешнему верификатору.
- **Редирект при успехе** - если первый этап провален, то данный режим аналогичен режиму **Решает сервер**. Если первый этап успешен, то осуществляется делегация внешнему верификатору.

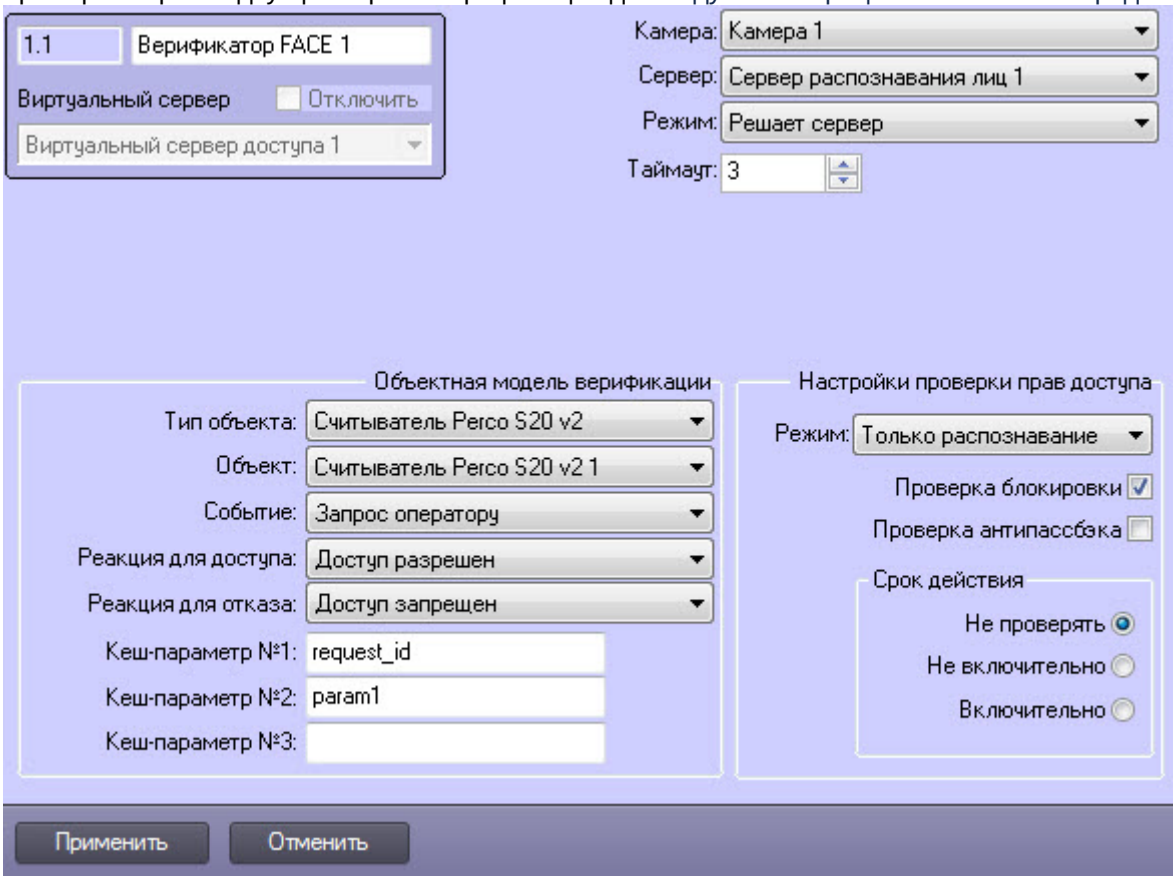
6. В поле **Таймаут** (**4**) задать время ожидания лица в камере Сервера распознавания лиц. Если лицо не появится перед камерой в течение данного времени, то верификация лица будет провалена.
7. Из раскрывающегося списка **Тип объекта** (**5**) выбрать тип объекта, который будет являться инициатором проверки лица. Как правило это точка доступа, считыватель и т.п.
8. Из раскрывающегося списка **Объект** (**6**) выбрать объект заданного выше типа.
9. Из раскрывающегося списка **Событие** (**7**) выбрать событие, по которому будет запущена проверка лица. Список доступных событий зависит от выбранного типа объекта.
10. Из раскрывающегося списка **Реакция для доступа** (**8**) выбрать команду, которая будет отправлена на объект-инициатор при успешной верификации лица. Список доступных команд зависит от выбранного типа объекта.
11. Из раскрывающегося списка **Реакция для отказа** (**9**) выбрать команду, которая будет отправлена на объект-инициатор при неуспешной проверке/верификации лица. Список доступных команд зависит от выбранного типа объекта.
12. При необходимости в полях **Кеш-параметры №1-N3** (**10**) задать параметры, которые индивидуальны для каждого программного модуля интеграции СКУД, с которым осуществляется работа.

> **Примечание**
>
> Например, в модуле интеграции *PERCo-S-20 v.2* каждый запрос оператору сопровождается параметром **request_id**. Этот параметр необходимо обязательно возвращать при подтверждении доступа, иначе команда будет проигнорирована. Для СКУД *Noder* таким параметром является **param1**.

13. Из раскрывающегося списка **Режим** (**11**) выбрать режим проверки прав доступа:
    a. **Проверка прав доступа** - активирует проверку прав доступа пользователя по параметрам ниже. Только после проверки прав доступа, в случае успеха, будет осуществяться верификация по лицу.
    b. **Только распознавание** - пропускает проверку прав доступаи переходит сразу к верификации лица.
14. Установить флажок **Проверка блокировки** (**12**), если необходимо проверять заблокирован ли пользователь или нет.
15. Установить флажок **Проверка антипассбэка** (**13**), если необходимо осуществлять проверку контроля двойного прохода.
16. Выбрать способ проверки срока действия карты доступа пользователя (**14**):
    - **Не проверять** - проверка срока действия карты осуществляться не будет.
    - **Не включительно** - в день истечения срока действия карты пользователю будет отказано в доступе.
    - **Включительно** - в день истечения срока действия карты пользователю доступ будет разрешен.
17. Нажать кнопку **Применить** (**15**) для сохранения настроек.

> **Внимание!**
>
> Параметры с (**1**) по (**9**) являются обязательными. Если не указать хотя бы один из них, то все выбранные значения данных параметров будут сброшены по умолчанию даже после нажатия кнопки **Применить**.

Пример настройки двухфакторной верификации для модуля интеграции *PERCo-S-20 v.2* представлен ниже.



Настройка двухфакторной верификации завершена.

4 Работа программного модуля Виртуальный сервер доступа

Программный модуль *Виртуальный сервер доступа* позволяет выполнять следующие функции:

1. Объединять работу программных комплексов *Auto-* и *Face-Интеллект* с программным модулем *Учет рабочего времени*. При успешном распознавании номера или лица генерируется событие **Проход** (ACCESS_IN), что может служить, например, началом рабочего дня сотрудника.
2. Выполнять различные действия в системе (например, открывать или закрывать шлагбаум) с помощью скриптов или макрокоманд по событиям **Проход** или **Запрет прохода** (см. Программный комплекс Интеллект. Руководство по программированию).

Документация по программным комплексам *Auto-* и *Face-* и *Интеллект базовый,* а также по программному модулю *Учет рабочего времени* доступа здесь.