

VisionLabs LUNA Access

Руководство пользователя

2.18.0

Содержание

1	Глоссарий	9
2	Введение	11
3	Системные требования при работе с Access UI	12
4	Поддерживаемые компоненты и версии	13
4.1	Поддерживаемые компоненты	13
4.2	Поддерживаемые версии сервисов	14
4.3	Поддерживаемые версий устройств	15
4.4	Поддерживаемые версий контроллеров и преобразователей	16
5	Работа с Access UI	18
5.1	Язык UI	18
5.2	Роли в Access	18
5.3	Добавление учетной записи	19
5.4	Авторизация в Access	19
5.5	Выход из учетной записи Access	22
5.6	Разделы Access	23
5.6.1	Создание компонента	24
5.6.2	Общая информация о компоненте	27
5.6.3	Группировка компонентов	29
5.6.4	Изменение компонента	30
5.6.5	Перезапуск компонента	33
5.6.6	Удаление компонента	33
6	Логирование	37
6.1	Фильтрация логов	38
7	Функции Access	43
7.1	Импортировать настройки	43
7.2	Экспортировать настройки	45
7.3	Сбросить настройки	46
7.4	Переменные ФИО	47
7.5	Прочие функции	47
7.5.1	Документация	47
8	Сервисы	48
8.1	Арапс	48
8.1.1	Функционал сервиса Арапс	48

8.1.2	Настройка параметров для подключения к СКУД APACS	48
8.2	Bastion	50
8.2.1	Функционал сервиса Bastion	50
8.2.2	Настройка параметров для подключения к СКУД Бастион	51
8.3	Bolid	52
8.3.1	Настройка параметров для подключения к СКУД Болид	52
8.4	CbsAkbars	54
8.4.1	Настройка параметров для подключения к CbsAkbars	54
8.5	CbsAlpha	55
8.5.1	Настройка параметров для подключения к CbsAlpha	56
8.6	CbsAlphaListSynchronisation	58
8.6.1	Настройка параметров CbsAlphaListSynchronisation	58
8.7	CbsMts	59
8.7.1	Настройка параметров для подключения к CbsMts	59
8.8	CbsVtb	60
8.8.1	Настройка параметров для подключения к CbsVtb	61
8.9	CryptoPro	63
8.9.1	Настройка параметров для подключения к CryptoPro	63
8.10	EyelsProxy	64
8.10.1	Настройка параметров для подключения к EyelsProxy	64
8.11	Gate	65
8.11.1	Настройка параметров для подключения к Gate	65
8.12	Luna	66
8.12.1	Настройка параметров для подключения к Luna	66
8.13	LunaAceConverter	68
8.13.1	Настройка параметров для подключения к LUNA ACE	68
8.13.2	Настройка LUNA ACE	69
8.14	LunaCars	69
8.14.1	Настройка параметров для подключения к LunaCars	70
8.15	LunaStreams	72
8.15.1	Настройка параметров для подключения к LunaStreams	72
8.16	Parsec	73
8.16.1	Возможности Parsec	73
8.16.2	Настройка параметров для подключения к Parsec	73
8.17	PercoWeb	75
8.17.1	Функции PercoWeb	75
8.17.2	Настройка параметров для подключения к СКУД PERCo-Web	75
8.18	PersonStorageActualization	77
8.18.1	Настройка параметров PersonStorageActualization	77

8.19	Rusguard	77
8.19.1	Функционал Rusguard	77
8.19.2	Настройка параметров для подключения к Rusguard	78
8.20	Salto	79
8.20.1	Настройка параметров для подключения к СКУД SALTO	79
8.21	Sigur	80
8.21.1	Функции Sigur	81
8.21.2	Настройка параметров для подключения к СКУД Sigur	81
8.22	SigurThroughDatabase	82
8.22.1	Варианты интеграции с LP5	83
8.22.2	Настройка параметров для подключения к SigurThroughDatabase	84
8.23	Strazh	85
8.23.1	Настройка параметров для подключения к СКУД STRAZH	85
8.24	Ubs	86
8.24.1	Настройка параметров Ubs	86
9	СКУД APACS	88
9.1	Поддерживаемые варианты интеграции СКУД APACS	88
9.2	Стандартная интеграция с использованием Apacs	89
9.3	Гостевой проход при двухфакторной аутентификации	92
9.4	Создание пользователя в RabbitMQ	92
9.5	Методы взаимодействия с Apacs	93
9.6	Диаграммы процессов взаимодействия с Apacs	94
9.6.1	Подключение сервиса Apacs	94
9.6.2	Обработка событий Apacs при 1 факторе	96
9.6.3	Обработка событий Apacs при 2 факторах	97
9.7	FAQ Apacs	98
10	СКУД Бастион	99
10.1	Поддерживаемые варианты интеграции СКУД Бастион	99
10.2	Стандартная интеграция с использованием СКУД Бастион	100
10.3	Настройка ПО СКУД Бастион 3	102
10.4	Настройка двухфакторной точки доступа Бастион	106
10.5	Методы взаимодействия с Бастион	109
10.6	Диаграммы процессов взаимодействия с Бастион	110
10.6.1	Подключение сервиса Бастион и репликация сотрудников	110
10.6.2	Обработка событий Бастион при 2 факторах	112
11	СКУД Болид	114
11.1	Поддерживаемые варианты интеграции СКУД Болид	114

11.2	Стандартная интеграция с использованием Болид	116
11.3	Настройка СКУД Болид	117
11.3.1	Подготовительные действия с ПО «Орион Про»	117
11.3.2	Добавление сотрудника в Орион Про	118
11.3.3	Добавление устройств в Орион Про	120
11.3.4	Настройка приложения «МОДУЛЬ ИНТЕГРАЦИИ ОРИОН ПРО»	123
11.4	Методы взаимодействия с Болид	124
11.5	Диаграммы процессов взаимодействия с Болид	125
11.5.1	Подключение сервиса Болид	125
11.5.2	Обработка событий Болид при 1 факторе	127
11.5.3	Обработка событий Болид при 2 факторах	128
11.6	Болид FAQ	129
12	СКУД Gate	130
12.1	Поддерживаемые варианты интеграции СКУД Gate	130
13	СКУД Parsec	132
13.1	Поддерживаемые варианты интеграции СКУД Parsec	132
13.2	Стандартная интеграция с использованием Parsec	134
13.3	Настройка ПО СКУД Parsec	135
13.3.1	Настройка групп доступа в СКУД Parsec	138
13.3.2	Добавление сотрудников в СКУД Parsec	139
13.4	Методы взаимодействия с Parsec	141
13.5	Диаграммы процессов взаимодействия с Parsec	141
13.5.1	Подключение сервиса Parsec	141
13.5.2	Обработка событий Parsec при 2 факторах	143
14	СКУД PERCo-Web	145
14.1	Поддерживаемые варианты интеграции СКУД PERCo-Web	145
14.2	Стандартная интеграция с использованием PERCo-Web	146
14.3	Методы взаимодействия с PERCo-Web	147
14.4	Диаграммы процессов взаимодействия с PERCo-Web	148
14.4.1	Подключение сервиса PERCo-Web	148
14.4.2	Обработка событий PERCo-Web при 1 факторе	150
15	СКУД RusGuard	152
15.1	Поддерживаемые варианты интеграции СКУД RusGuard	152
15.2	Стандартная интеграция с использованием RusGuard	154
15.3	Методы взаимодействия с RusGuard	155
15.4	Диаграммы процессов взаимодействия с RusGuard	156
15.4.1	Диаграмма взаимодействия RusGuard с Access	156

15.4.2	Диаграмма взаимодействия Access с биометрической системой	158
16	СКУД SALTO	160
16.1	Поддерживаемые варианты интеграции СКУД SALTO	160
16.2	Стандартная интеграция с использованием Salto	161
16.3	Уровни доступа СКУД SALTO	162
16.4	Методы взаимодействия с Salto	162
16.5	Диаграмма процессов взаимодействия с SALTO	163
17	СКУД Sigur	166
17.1	Поддерживаемые варианты интеграции СКУД Sigur	166
17.1.1	Варианты интеграции с LP5	166
17.1.2	Варианты интеграции с КБС	167
17.1.3	Варианты интеграции с LUNA CARS	168
17.2	Стандартные интеграции с использованием СКУД Sigur	168
17.3	Настройка ПО СКУД Sigur	171
17.3.1	Настройка точек доступа в Sigur	175
17.3.2	Настройка режимов доступа в ПО СКУД Sigur	177
17.4	Методы взаимодействия с Sigur	180
17.5	Диаграмма процессов взаимодействия с Sigur	180
17.6	Sigur FAQ	183
18	СКУД STRAZH	185
18.1	Поддерживаемые варианты интеграции СКУД STRAZH	185
18.2	Стандартная интеграция с использованием СКУД STRAZH	186
18.3	Настройка ПО СКУД STRAZH для двухфакторной авторизации	190
18.4	Методы взаимодействия с STRAZH	190
18.5	Диаграммы процессов взаимодействия с STRAZH	191
18.5.1	Подключение сервиса Strazh	191
18.5.2	Модификация сотрудников в СКУД STRAZH	193
18.5.3	Обработка событий STRAZH при 1 факторе	195
18.5.4	Обработка событий STRAZH при 2 факторах	195
19	Интеграции без СКУД	197
20	Контроллеры	198
20.1	ApacsController	198
20.1.1	Настройка параметров для подключения к контроллеру Apacs	198
20.2	GateController	199
20.2.1	Преобразователем GateEthernetWiegand	199
20.2.2	Настройка параметров для подключения к контроллеру Gate	199

20.3	LaurentController	201
20.3.1	Настройка параметров для подключения к контроллеру Laurent	201
20.4	PercoController	202
20.4.1	Настройка параметров для подключения к контроллеру PERCo	202
20.5	PusrController	204
20.5.1	Настройка параметров для подключения к контроллеру Pusr	204
20.6	SaltoController	205
20.6.1	Настройка параметров для подключения к контроллеру Salto	205
20.7	StrazhController	206
20.7.1	Настройка параметров для подключения к контроллеру Strazh	206
21	Устройства	209
21.1	Beward	209
21.1.1	Настройка параметров для подключения к Beward	209
21.2	BioSmart	212
21.2.1	Настройка параметров для подключения к BioSmart Quasar	212
21.3	Dahua	213
21.3.1	Настройка параметров для подключения к камере Dahua	214
21.4	DahuaThermo	215
21.4.1	Настройка параметров для подключения к тепловизору DahuaThermo	216
21.5	Fortuna315	217
21.5.1	Настройка параметров для подключения к Fortuna315	217
21.6	GrgFaster	219
21.6.1	Настройка параметров для подключения к GrgFaster	219
21.7	HikvisionCamera	221
21.7.1	Настройка параметров для подключения к HikvisionCamera	221
21.8	HikvisionCameraThermo	223
21.8.1	Настройка параметров для подключения к HikvisionCameraThermo	223
21.9	HikvisionRecognitionOnBoard	225
21.9.1	Настройка параметров для подключения к HikvisionRecognitionOnBoard	226
21.10	HikvisionTerminalThermo	228
21.10.1	Настройка параметров для подключения к HikvisionTerminalThermo	228
21.11	LunaFast2NextGen	233
21.11.1	Настройка параметров для подключения к LunaFast2NextGen	233
21.12	LunaFast4A1	235
21.12.1	Настройка параметров для подключения к LunaFast4A1	235
21.13	Panda	240
21.13.1	Настройка параметров для подключения к Panda	240
21.14	R20Face	242
21.14.1	Настройка параметров для подключения к R20Face	242

21.15 UniUbi	245
21.15.1 Настройка параметров для подключения к UniUbi	245
21.16 VKVision02	248
21.16.1 Настройка параметров для подключения к VKVision02	248
22 Пайплайны	250
22.1 Apacs2FA	250
22.2 CreateBastionEvent	252
22.3 Custom2FA	253
22.4 LunaEventListener	255
22.5 MatchByPhoto	255
22.6 MatchByPhotoInCbsAlpha	256
22.7 MatchInformerWebHook	257
22.8 MatchInformerWebSocket	259
22.9 SendCardToR20Face	260
22.10 SendCarsToLaurent	260
22.11 SendCarsToSigur	261
22.12 SendThermalEventToLuna	262
22.13 SendToBars	263
22.14 SendToController	264
22.15 SendToDevice	265
22.16 SendToGrgFaster	266
22.17 SendToLuna	267
22.18 SendToParsec	268
22.19 SendToSalto	269
22.20 SendToSigur	270
22.21 Strazh2FA	271

1. Глоссарий

Термин	Определение
Liveness	Программный способ, позволяющий подтвердить витальность (живучесть, жизненность) человека по одному или нескольким изображениям с целью предотвращения спуфинг-атак
LUNA ACE	Биометрический терминал контроля и управления доступом VisionLabs LUNA ACE. Предназначен для организации контроля доступа и учета рабочего времени по биометрическим данным. Детальную информацию см. в документации из комплекта поставки устройства.
LUNA PLATFORM (LP)	Автоматизированная система распознавания лиц компании VisionLabs, предназначенная для сбора, анализа, хранения и сопоставления биометрических данных, получаемых из изображений лиц. Более детальную информацию см. в документации из комплекта поставки системы.
LUNA CARS	Система, предназначенная для детектирования, трекинга, определения атрибутов транспортных средств и распознавания автомобильных номеров. Более детальную информацию см. в документации из комплекта поставки системы.
База данных (БД)	Совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных
Идентификация	Процедура определения субъекта биометрических данных путем сравнения биометрических признаков, полученных от субъекта биометрических данных, со всеми эталонными биометрическими признаками (контрольными шаблонами), хранящимися в биометрической базе данных.
Программное обеспечение (ПО)	Программа или множество программ, используемых для управления компьютером
Система контроля управления доступом (СКУД)	Совокупность программно-аппаратных технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещения определенного объекта. Например, турникеты на входе в банки/офисные здания
Система распознавания лиц	В контексте документа — продукты VisionLabs. Например, VisionLabs LUNA PLATFORM 5 (LP5)

Термин	Определение
Событие	Неизменяемый объект, который содержит информацию об одном лице. Событие генерируется с помощью внешней системы
Биометрическая система (БС)	Система, предназначенная для биометрического распознавания индивидов, основанного на их поведенческих и биологических характеристиках
Коммерческая биометрическая система (КБС)	Организация, аккредитованная МинЦифры для работы с биометрией согласно ФЗ-572, ПП РФ № 810, в результате этого имеющая право хранить у себя Векторы ЕБС и производить аутентификацию по биометрии с их использованием, а также оказывать услуги аутентификации третьим лицам (организациям)
Simple Object Access Protocol (SOAP)	Web протокол для обеспечения взаимодействия между сервисами, реализованный на языке WSDL.
Universally unique identifier (UUID)	Универсальный уникальный идентификатор. Название объектов (списки, события, камеры и т. д.), которые системы генерируют самостоятельно в качестве уникального названия.
Web Services Description Language (WSDL)	Язык описания веб-сервисов и доступа к ним, основанный на языке XML.

2. Введение

Документ описывает назначение и функции интерфейса пользователя сервиса **VisionLabs LUNA Access** версии 2.18.0 (далее — Access), а также содержит аппаратные и программные требования к ПО.

Access представляет собой совокупность программных технических средств контроля и средств управления, позволяет реализовать совместную работу продуктов VisionLabs и различных систем контроля и управления доступом.

Access решает следующие задачи:

- добавление устройств передачи видеосигнала, с кадрами которых будут работать LP или КБС;
- добавление вспомогательных устройств для считывания данных магнитных карт-пропуска или получения данных о температуре человека;
- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в LP;
- получение событий идентификации от LP и КБС с последующей отправкой в СКУД;
- логирование событий о попытке прохода неидентифицированного человека через турникет.

Интеграции с использованием Access, LUNA CARS/LP/КБС и внешних устройств позволяют решать следующие задачи:

- контроль доступа;
- повышение удобства прохода и пропускной способности контрольно-пропускных пунктов;
- контроль времени пребывания сотрудников, посетителей, автомобилей на охраняемой территории;
- защита от попыток несанкционированного доступа с помощью технологии Liveness.

Количество подключенных камер, терминалов и турникетов может быть любым и зависит от требований к разворачиваемой системе, но ограничено лицензией на продукты VisionLabs и возможностью СКУД.

В зависимости от выбранного решения контроль доступа для аутентификации людей может применяться с помощью распознавания лиц или магнитной карты-пропуска.

3. Системные требования при работе с Access UI

Требования к аппаратному обеспечению рабочей станции (Таблица 1).

Таблица 1. Требования к аппаратному обеспечению

Ресурс	Минимум	Рекомендовано
Процессор (CPU)	64-битный процессор Intel или AMD, с 2 ядрами с тактовой частотой 2,0 ГГц	Intel Core i3, 4 поколения и выше / AMD Ryzen 3 и выше
Оперативная память (RAM)	2 ГБ	4 ГБ и выше
Разрешение монитора	1600x1200 px	1920x1080 и выше

Рекомендации к программному обеспечению (Таблица 2).

Таблица 2. Рекомендации к программному обеспечению

Ресурс	Рекомендовано
Веб-браузер	Google Chrome (версия 117.0 и выше);
	Microsoft Edge (версия 117.0 и выше);
	Mozilla Firefox (версия 117.0 и выше);
	Safari.
Интернет-соединение	Наличие стабильного интернет-соединения со скоростью передачи данных от пользователя не ниже 1 Мбит/с.

4. Поддерживаемые компоненты и версии

4.1. Поддерживаемые компоненты

Access позволяет добавлять в интеграции следующие компоненты (Таблица 3):

Таблица 3. Поддерживаемые компоненты

Тип	Поддерживается	Примечания
ПО VisionLabs	LUNA PLATFORM 5 (LP5)	5.10 или новее
	LUNA CARS	Installer v.2.10.1 и новее. Обращение происходит к LUNA CARS Analytics
	FaceStream	5.1.6 и новее
СКУД	APACS, Sigur, Бастион, Bolid, Parsec, PercoWeb, Strazh, RusGuard, Gate, Salto и Барс-Х	Подключение к СКУД Барс-Х происходит с помощью пайплайна без сервиса.
Устройств	VisionLabs Терминал: LUNA ACE, LUNA Fast 4A1, LUNA Fast 8A1, LunaFast2NextGen	Терминал 8A1 подключается через настройки устройства 4A1.
	Beward	Терминалы: TFR80-210T1Q, TFR80-210
	BioSmart	Терминал: Quasar
	Dahua	Камера: Camera
		Тепловизор: Thermo
	Fortuna	Тепловизор: F315
	GrgFaster	Терминал: SV-M082f-C2
	Hikvision	Камера: DS-2CD3126G2-IS
		Терминалы-тепловизоры: DS-K1TA70MI-T, DS-K1T671TM-3XF, DS-K5671-3XF/ZU
		Терминалы: DS-K1T341AMF, DS-K1T341AM, DS-K1T680D-E1
	Sunell (Panda)	Тепловизор: SN-T5/13, SN-F22-13
	Uni-Ubi	Терминал-тепловизор: Uface 8-C temp, Uface 8T - temp
	Hi-Tech Security	Терминал: VK-Vision-02

Тип	Поддерживается	Примечания
	R20Face	Терминал: R20-Face-T8

4.2. Поддерживаемые версии сервисов

Access поддерживает следующие сервисы и версии прошивок (Таблица 4):

Таблица 4. Поддерживаемые внешние сервисы

Название в Access	Оригинальное название	Версия
Apacs	APACS 3000	8.3.1.0 update 18
Bastion	Elsys Бастион-2 / 3	2.1.11.2337 и новее
Bolid	Bolid-Орион Про	1.20.3 (build 11940)
	Модуль интеграции Орион Про	1.4, 1.5.1
CbsMts	КБС МТС	-
CbsAlpha	КБС Альфа	-
CbsVtb	КБС ВТБ	-
CbsAkbars	КБС Ак Барс	-
LunaStreams	VisionLabs FaceStream	от 5.1.6 и новее
Gate	Gate	1.22.95
Luna	VisionLabs LUNA PLATFORM	5.10 и новее
LunaAceConverter	LUNA ACE	1.2.23
LunaCars	VisionLabs LUNA CARS	
	LUNA CARS Installer	v.2.10.1 и новее
	LUNA CARS API	v.4.0.15 и новее
	LUNA CARS Stream	v.3.0.20 и новее
	LUNA CARS Analytics backend	v.4.0.8 и новее
	LUNA CARS Analytics frontend	v.2.0.61 и новее
Parsec	Parsec (ParsecNet3)	3.11.629 39 и новее
PercoWeb	PERCo-Web 2.0	4.30
Rusguard	RusGuard	3.3.1
Salto	Salto	6.6.3.0

Название в Access	Оригинальное название	Версия
		Package 6.6.3.94
		Service 4.23.3.595
Sigur	СКУД Сигур	1.6.3.18.s и новее
SigurThroughDatabase	СКУД Сигур	1.6.3.18.s и новее
Strazh	Rubezh Strazh	1.2.211201.648
CryptoPro	cryptopro-service	1.4.1 и новее

4.3. Поддерживаемые версии устройств

Access поддерживает следующие устройства и версии прошивок (Таблица 5):

Таблица 5. Поддерживаемые устройства

Устройство	Модель	Версия
Beward	TFR80-210T1Q, TFR80-210	1.2.13.0, 2.1.6.0
BioSmart	BioSmart Quasar	2.3.0.46
DahuaThermo	-	2.631.0000000.31.T
Fortuna315	-	Камера: V4.02.00, Тепловизор: 2.20.0.0.R26130.alpha8, Аппаратные версии: V1.0, Версии алгоритма: smart2.0.0-06-2020.06.17.16:06:42
GrgFaster	SV-M082f-C2	Версии прошивки: 1.004.30.3bb324.R, Аппаратные версии: 1.0.0
HikvisionCamera	DS-2CD3126G2-IS	V5.5.134 build 200430
HikvisionCameraTherm	DS-2TD2617B-3/PA	V5.5.26 build 200317
HikvisionRecognition OnBoard	DS-K1T341AMF, DS-K1T341AM, DS-K1T680D-E1	V3.2.30 build 220210
HikvisionTerminalThern	DS-K1TA70MI-T, DS-K1T671TM-3XF, DS-K5671-3XF/ZU	V3.2.32 build 210525

Устройство	Модель	Версия
LunaFast4A1	DS-K1T680D-E1, DS-K1T341AMF, DS-K1T341CMF, DS-K1T341AM, VL LUNA FAST 4A1, VL LUNA FAST 8A1, 671, DS-K1T671M, ACT-T1341M, DS-K1T680DF-E1, DS-K5671-ZU	V3.2.30 build 210415, V3.2.30 build 210525, V3.2.30 build 210526, V3.2.30 build 210812, V3.2.30 build 211025, V3.2.30 build 220607, V3.2.30 build 220803, V3.2.30 build 221027, V3.2.33 build 210816, V3.2.35 build 220415, V3.2.35 build 220817, V3.3.40 build 250106
Panda	SN-T5/13, SN-F22-13	v3.6.0825.1004.1.0.23.0.0, v3.6.0840.1004.1.45.1.0.2
R20Face	R20-Face-T8	GD-V31.6222, GD-V32.7267
UniUbi	Uface 8-C temp, Uface 8T - temp, R20-Face-T8	GD-V30.7219, GD-V32.7247, GD-V32.7267
VKVision02	VANCOR VK VISION 02	v2156

4.4. Поддерживаемые версии контроллеров и преобразователей

Access поддерживает следующие контроллеры, преобразователи и их версии прошивок (Таблица 6):

Таблица 6. Поддерживаемые контроллеры и преобразователи

Модель	Версия
Контроллеры	
Gate 8000 Ethernet	8216/003 (4.06)
Strazh STR20-IP	1.2.211201.648
Strazh Rubezh STR20-IP	0.21.1
Strazh Rubezh STR1-AP	0.33.2
SigurController E900U	37
Болид C2000-Ethernet	2.60
Болид C2000-2	2.20, 2.50

Модель	Версия
RusGuard ACS-103-CE	6.20
RusGuard ACS-102-CE V2.0	7.46
Parsec NC-8000	3.8
Parsec NC-60-K	1.4
Bastion Elsys MB-NET	2.13
Bastion Elsys MB-light	2.74
Bastion Elsys NG-800	4.11
PercoController CTL14	2.2.37
PercoController CT/L04.2	3.0.0.78; 3.0.0.79; 3.0.0.81
Laurent-2	L213
UCM-2A	6103
AAM-LAN-8W	Только с APACS.
APOLLO AAN-100/AAN-32S/AAN-32N	Только с APACS.
Преобразователи	
Gate Ethernet/Wiegand	04.06, 1.3.2003
S4A Wiegand to TCP/IP	6005

5. Работа с Access UI

5.1. Язык UI

Access поддерживает работу на двух языках:

- Русский;
- Английский.

Для смены языка необходимо нажать на кнопку **rus|eng** на главной панели (Рисунок 1).

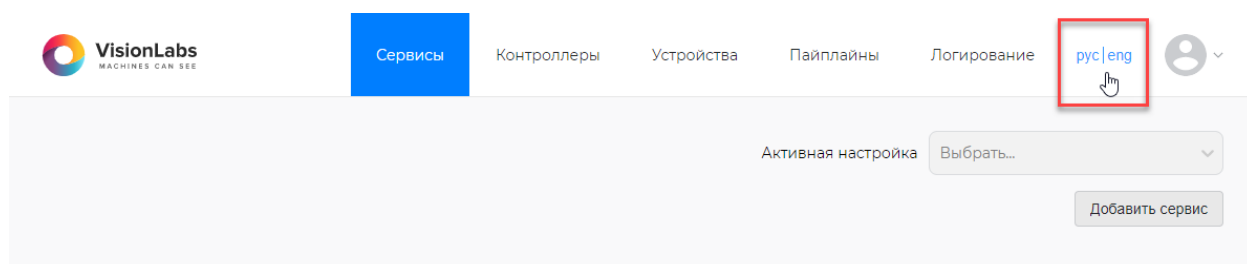


Рис. 1: Перевод интерфейса

Страница автоматически перезагрузится и отобразит англоязычный интерфейс (Рисунок 2)

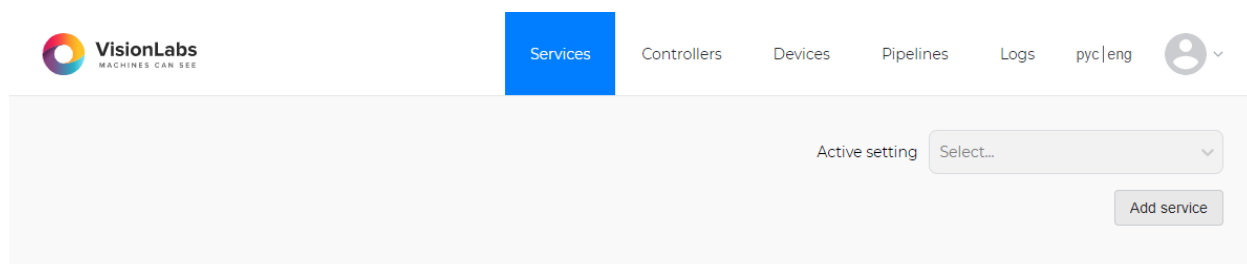


Рис. 2: Английский интерфейс

Для возврата к русскому интерфейсу нажмите на кнопку **rus|eng** еще раз.

5.2. Роли в Access

В Access доступна одна роль — «администратор». Описание прав «администратора» представлено в Таблице (Таблица 7).

Таблица 7. Перечень доступных разделов и прав

Роль	Разделы	Права
Администратор	Сервисы	Добавление/редактирование/удаление сервисов;

Роль	Разделы	Права
	Контроллеры	Добавление/редактирование/удаление контроллеров;
	Устройства	Добавление/редактирование/удаление устройств;
	Пайплайны	Добавление/редактирование/удаление пайплайнов;
	Логирование	Просмотр логов; Экспорт логов.

5.3. Добавление учетной записи

Все учетные записи пользователей создает администратор Access.

Описание процесса создания пользователей см. в Руководстве администратора.

5.4. Авторизация в Access

Доступ пользователя к Access осуществляется посредством входа в веб-браузере на сайт.

Необходимо открыть веб-браузер и перейти на сервер, где был установлен Access. Пример адреса: `http://<ip_address>:9092/services`.

Ссылку для входа в веб-интерфейс Access необходимо запросить у администратора.

При первичном входе в Access запускается страница Сервисы (Рисунок 3).

Не авторизованным пользователям не доступен просмотр и создание компонентов и логов.

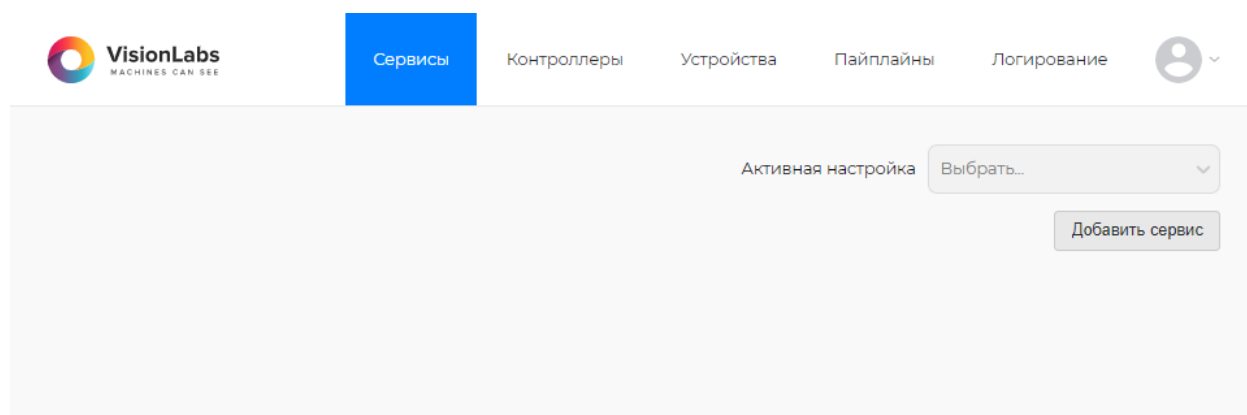


Рис. 3: Общий вид интерфейса Access в веб-браузере

Для авторизации в Access необходимо нажать на стрелку ▼ справа от аватара пользователя и нажать на кнопку «Вход» (Рисунок 4).

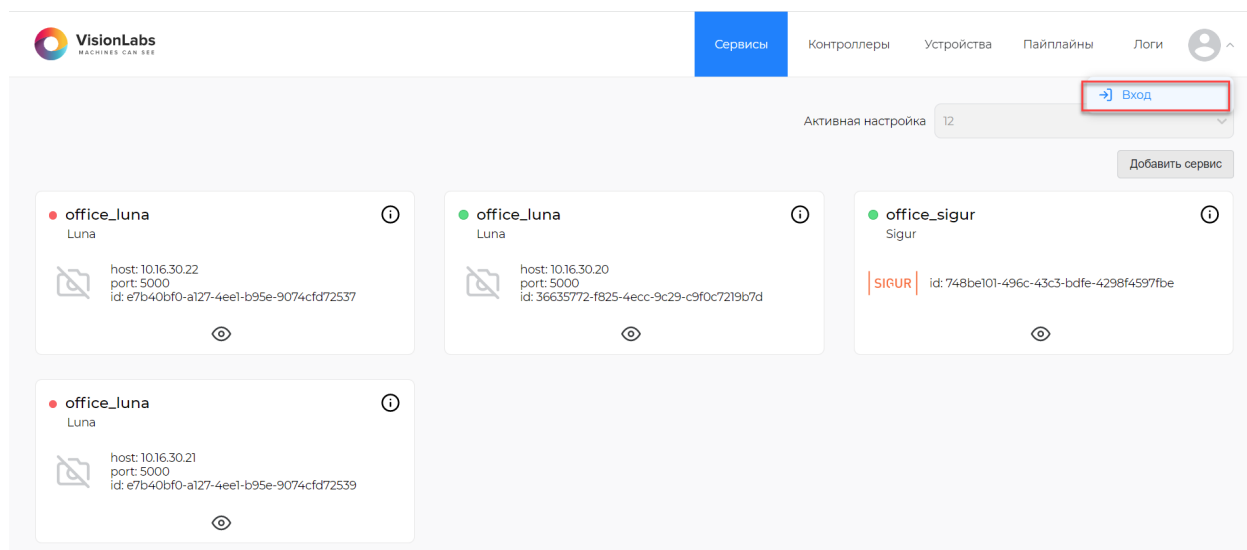


Рис. 4: Вход в учетную запись пользователя

Откроется форма авторизации (Рисунок 5).

Для авторизации в Access необходимо ввести учетные данные (логин и пароль) в соответствующие поля и нажать кнопку «Войти».




Рис. 5: Форма авторизации

Логин и пароль запрашиваются у администратора Access.

При входе в Access пользователь попадает на страницу «Сервисы» (Рисунок 6), где ему доступна возможность настройки и добавления компонентов Access.

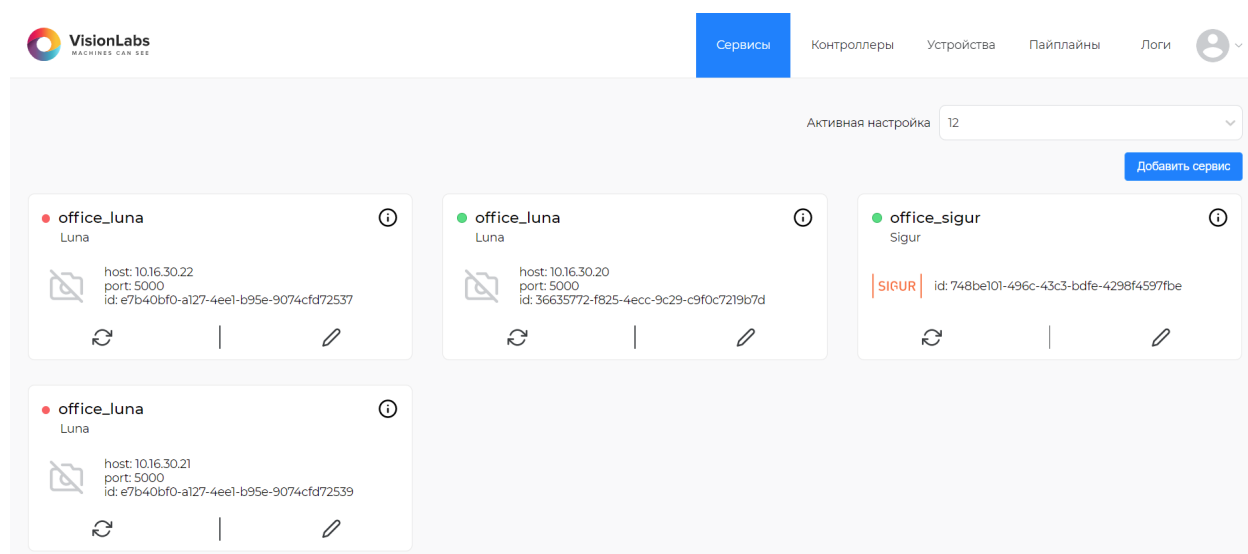



Рис. 6: Экран страницы при авторизации пользователя в Access

5.5. Выход из учетной записи Access

Для выхода из учетной записи необходимо нажать на стрелку  справа от аватара пользователя и нажать на кнопку «Выход» (Рисунок 7).

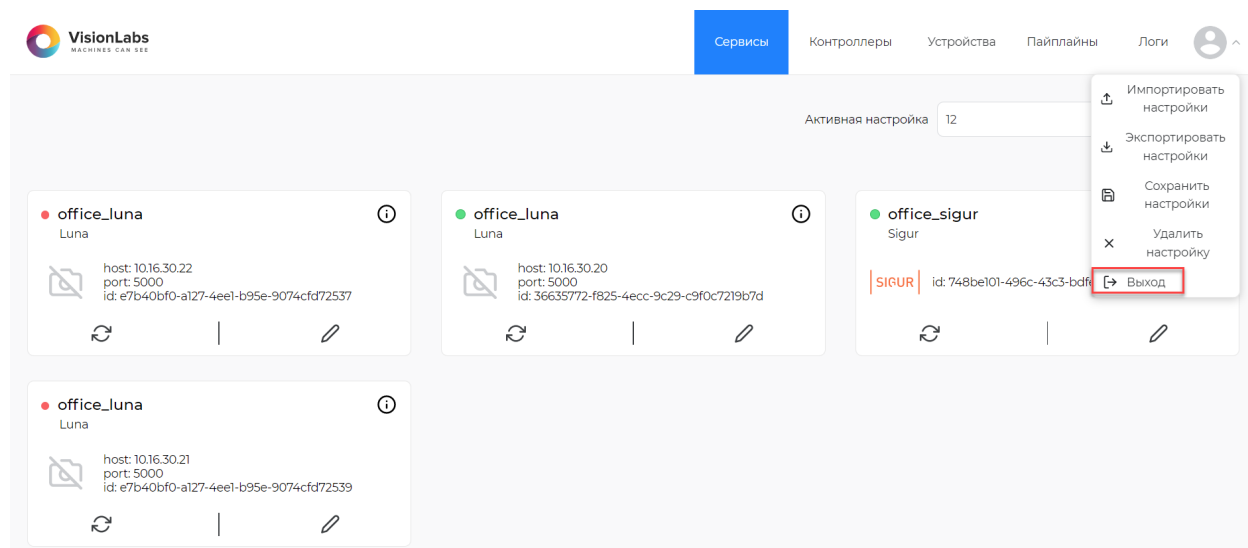


Рис. 7: Выход из учетной записи пользователя

После нажатия на кнопку «Выход» пользователь потеряет возможность взаимодействия с компонентами Access.

5.6. Разделы Access

Пользовательский интерфейс Access содержит 5 разделов в основном меню и 4 функции в выпадающем меню (Рисунок 8).

Основное меню состоит из разделов:

- [Сервисы](#) — просмотр и создание сервисов;
- [Контроллеры](#) — просмотр и создание контроллеров;
- [Устройства](#) — просмотр и создание устройств;
- [Пайплайны](#) — просмотр и создание пайплайнов;
- [Логирование](#) — просмотр логов.

Выпадающее меню состоит из функций:

- [Импортировать настройки](#) — функция, с помощью которой можно импортировать настройки;
- [Экспортировать настройки](#) — функция, которая позволяет экспортировать настройки;
- [Сбросить настройки](#) — сбросить все настройки;
- [Документация](#) — переход на онлайн документацию.

Чтобы развернуть выпадающее меню, необходимо нажать на стрелку ▾ справа от аватара пользователя.

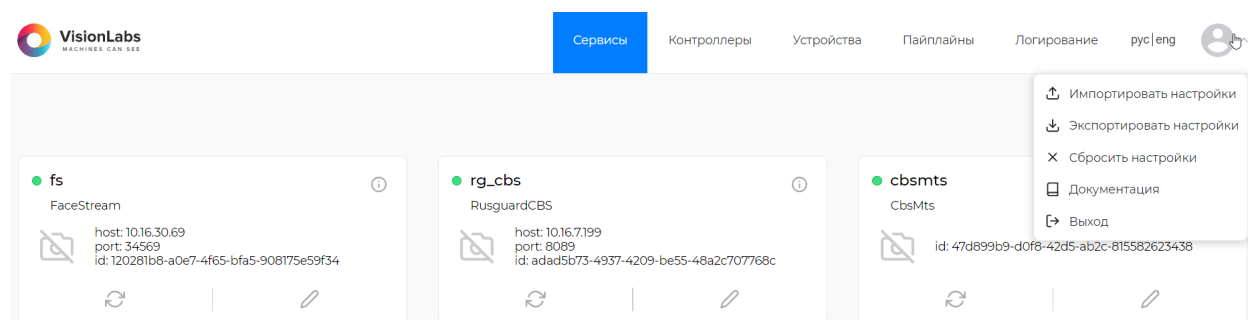


Рис. 8: Разделы меню, доступные пользователю

Компоненты одного типа (Сервисы, Контроллеры, Устройства или Пайплайны) должны иметь уникальные имена (параметр name).

Взаимодействие с компонентами Access происходит по общему алгоритму:

- [создание](#) компонентов
- [получение информации](#) о компоненте
- [группировка](#) компонентов (доступно только для контроллеров и устройств)
- [редактирование](#) компонента
- [перезапуск](#) компонента
- [удаление](#) компонента

5.6.1. Создание компонента

Для создания компонента необходимо выполнить следующие действия:

1. В правом верхнем углу нажать на кнопку «Добавить» компонент (Рисунок 9).

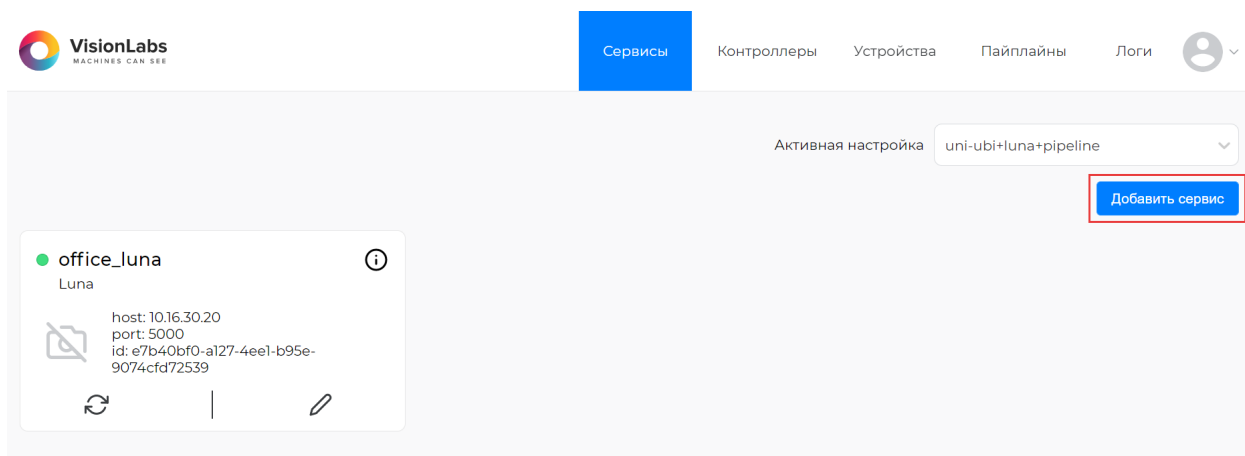


Рис. 9: Создание компонента

2. Откроется форма для создания компонента, в которой необходимо выбрать тип компонента (Рисунок 10).

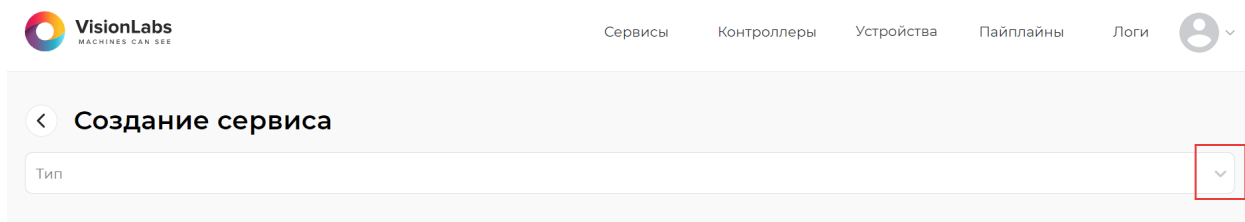
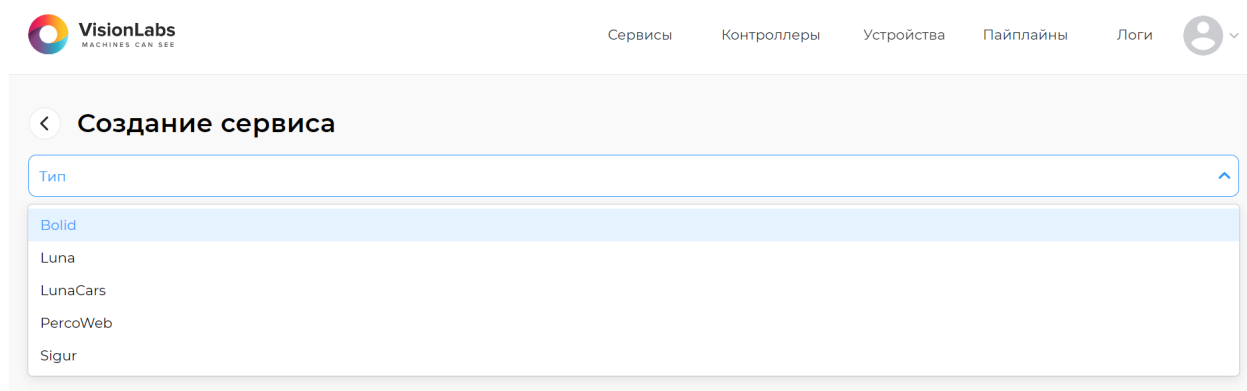


Рис. 10: Форма создания компонента

3. Разверните выпадающее меню, нажав на стрелку ▼ справа, и выберите необходимый тип компонента (Рисунок 11).

**Рис. 11:** Выбор типа компонента

4. Откроется форма для заполнения настроек компонента, в которую необходимо добавить необходимые параметры (Рисунок 12).

Для получения описания параметров компонента необходимо перейти в соответствующий раздел.

Рис. 12: Форма для заполнения настроек компонента

Для получения информации о настраиваемых параметрах нажмите на кнопку «Документация» в правом верхнем углу (Рисунок 13).

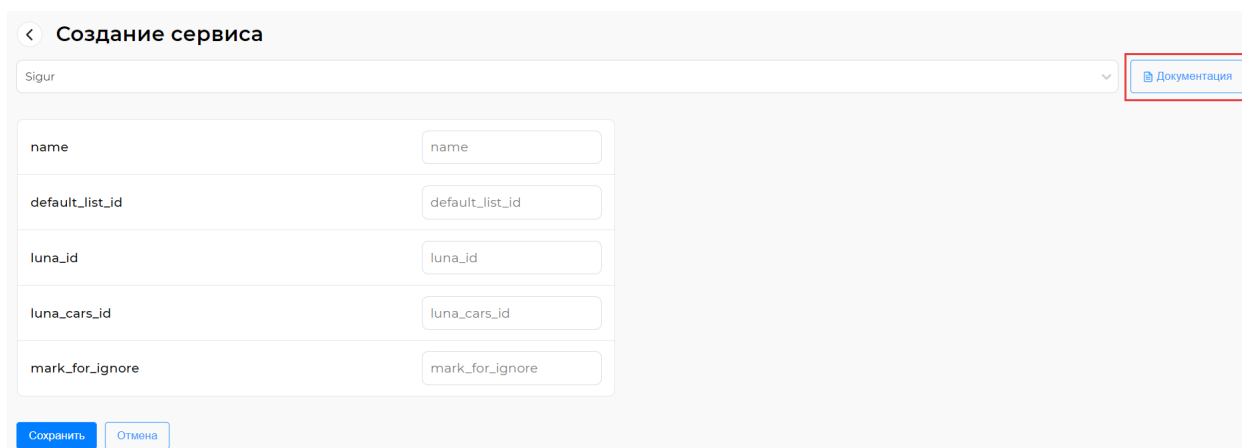


Рис. 13: Документация для создаваемого компонента

Во всплывающем окне отобразится информация с описанием необходимых параметров для создания компонента (Рисунок 14).

Sigur

Поддерживает версию СКУД Sigur 1.1.1.9s. Данный сервис предназначен для взаимодействия со СКУД Sigur. Сам СКУД синхронизирует сотрудников с нашим списком в Luna5 и слушает события на основе которых решает открывать или не открывать турникет. Данные события генерируются в VL Access пайплайном SendToSigur.

При создании нового сервиса используются следующие настройки:

- * name: str - имя сервиса,
- * default_list_id: str - Идентификатор списка Luna5, с которым Sigur будет синхронизировать сотрудников,
- * luna_id: str - Идентификатор сервиса Luna5.
- * mark_for_ignore: str - При синхронизации, если в теле имени сотрудника встречается данная комбинация,
- то он игнорируется

Рис. 14: Всплывающее окно с необходимыми параметрами компонента

5. После заполнения параметров компонента нажмите на кнопку «Сохранить» в левом нижнем углу (Рисунок 15).

Создание сервиса

Sigur

name: sigur

default_list_id: d725f7c5-63dd-4c00-b6fi

luna_id: 7ba9dee2-2f82-433d-8fd1

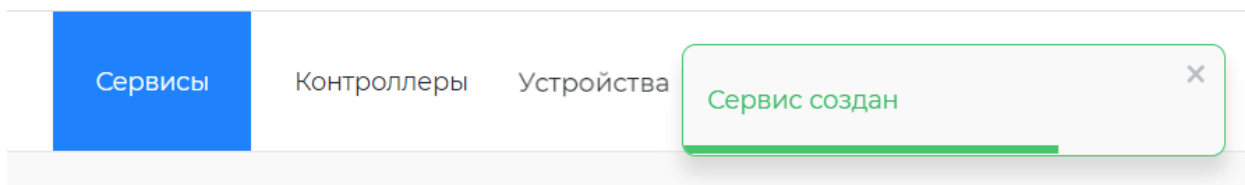
luna_cars_id: 417e1433-cac9-4fbl-b598-

mark_for_ignore: mark_for_ignore

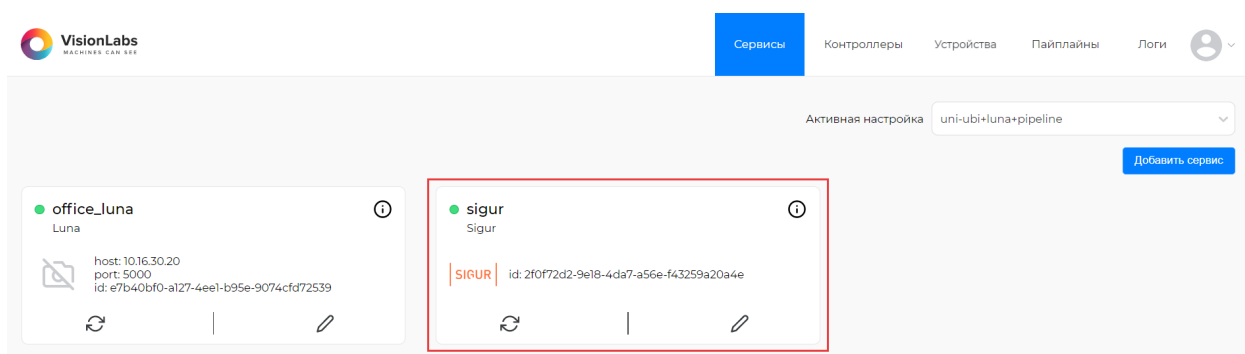
Сохранить Отмена

Рис. 15: Сохранение при создании компонента

В верхнем левом углу экрана отобразится сообщение «Компонент создан» (Рисунок 16).

**Рис. 16:** Подтверждение добавления компонента

При успешном добавлении компонент отобразится в списке в соответствующем разделе (Рисунок 17).

**Рис. 17:** Отображение нового компонента

5.6.2. Общая информация о компоненте

Компоненты отображаются на странице общего вида раздела.

Основная информация о компоненте расположена в блоке с описанием (Рисунок 18).

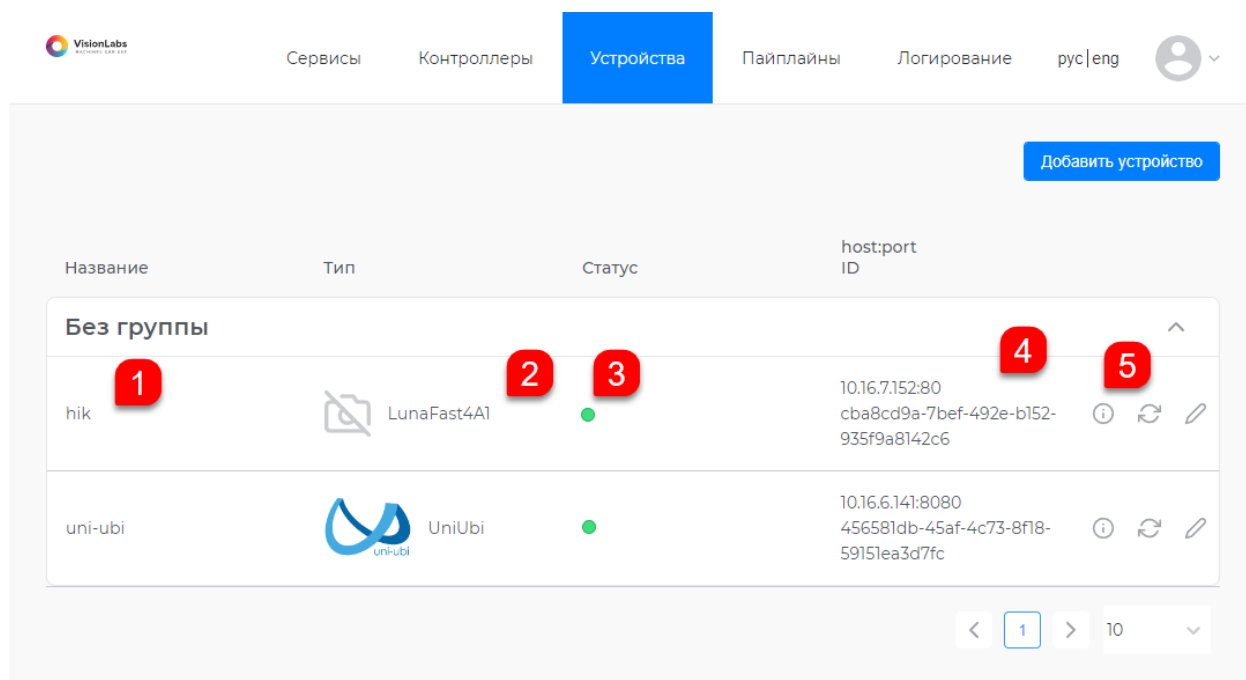


Рис. 18: Основные параметры

- 1 — имя;
- 2 — тип;
- 3 — статус;
- 4 — основная информация;
- 5 — дополнительная информация о параметрах.

Для получения дополнительной информации о параметрах необходимо навести курсор на ⓘ, информация отобразится во всплывающей подсказке (Рисунок 19).

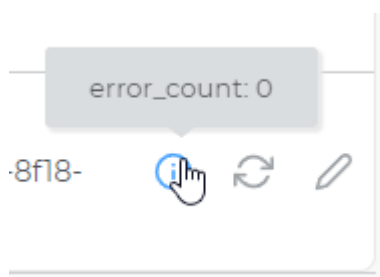


Рис. 19: Дополнительная информация о параметрах

5.6.3. Группировка компонентов

При создании устройства или контролеру доступно создание/выбор группы.

По умолчанию присваивается группа «Без группы».

Группировка позволяет визуально отделить компонент по признакам, которые интересуют пользователя: по расположению, типу, производителю и прочее.

Для создания группы в окне редактирования параметров устройства необходимо:

1. нажать на поле ввода группы
2. задать имя группы
3. нажать Создать (Рисунок 20)
4. сохранить изменения

Не рекомендуется вводить более 30 символов.

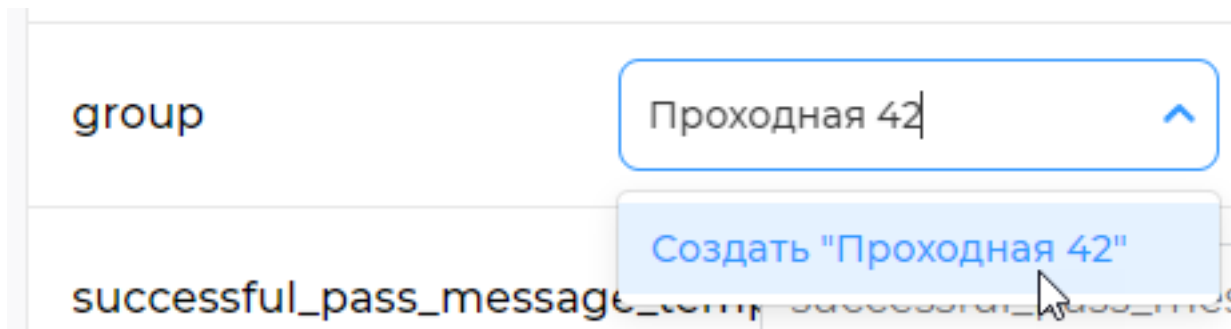


Рис. 20: Создание группы

Компонент помещен в группу (Рисунок 21).

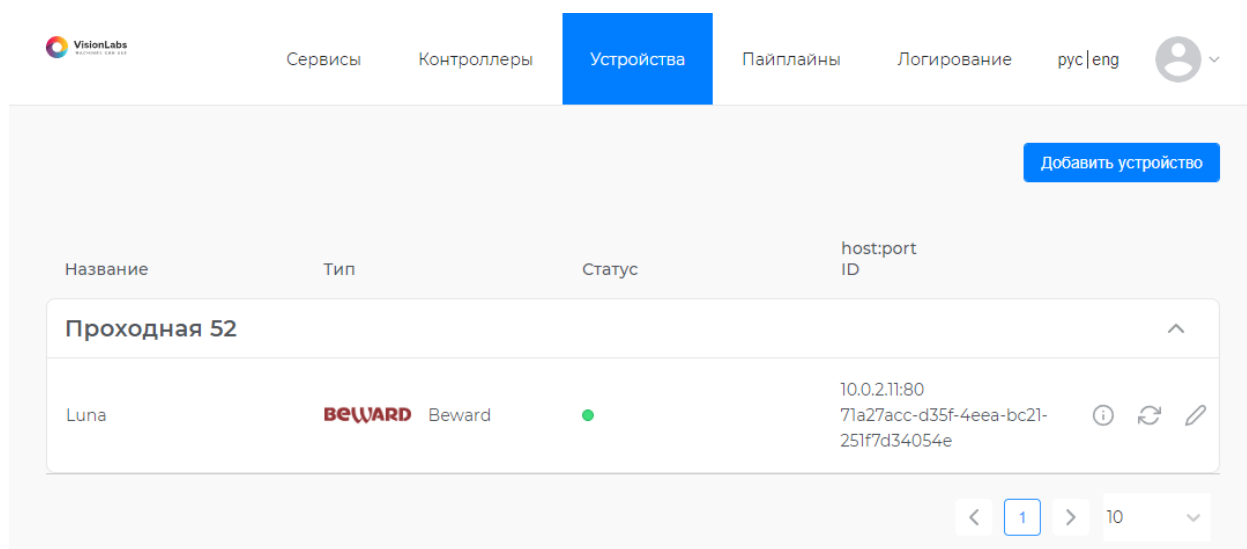


Рис. 21: Группа компонент

Для добавления компонента в существующую группу необходимо:

1. перейти к редактированию компонента
2. в выпадающем списке group выбрать интересующую группу (Рисунок 22)
3. сохранить изменения устройства.

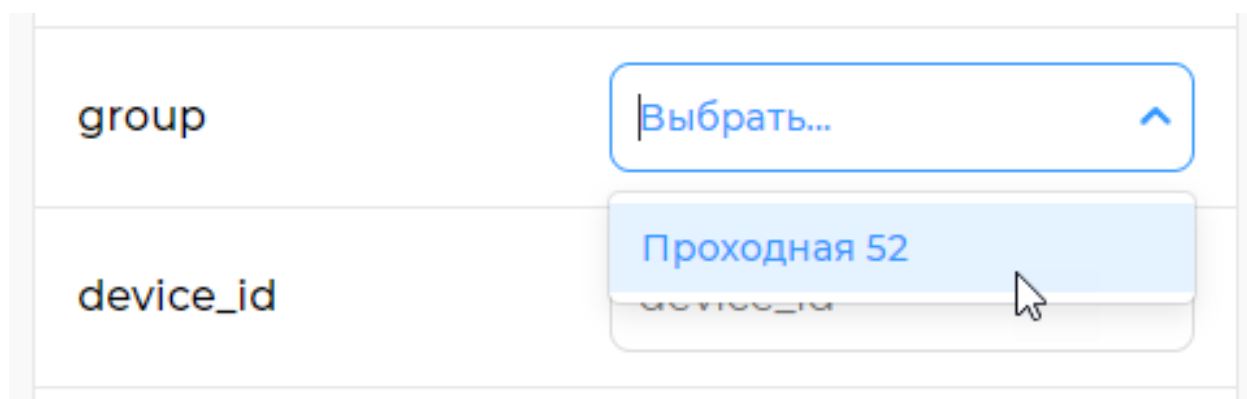



Рис. 22: Добавление в группу

5.6.4. Изменение компонента

Для изменения параметров компонента необходимо:

1. Нажать кнопку  для выбранного компонента (Рисунок 23).

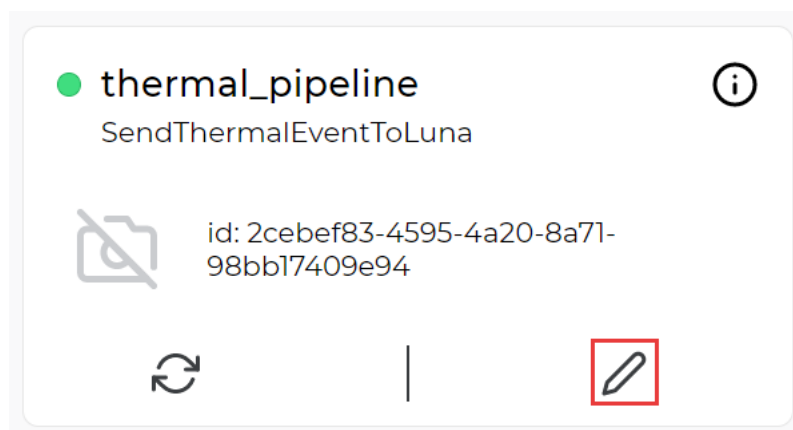


Рис. 23: Редактирование компонента

2. Откроется форма для редактирования компонента, в которую необходимо внести изменения (Рисунок 24).

Для получения описания параметров компонента необходимо перейти в соответствующий раздел.

3. Нажать на кнопку «Сохранить».

<

Редактирование пайплайна

SendThermalEventToLuna

ID	2cebef83-4595-4a20-8a7
name	thermal_pipeline
luna_id	e7b40bf0-a127-4ee1-b95e
handler_id	f5eb389e-6f07-42f9-8813
default_list_id	6c20808c-5366-416c-adc
black_list_id	6ffcb761-8c6c-4084-8084
to_high_temperature	38
to_low_temperature	36
min_similarity	0,01

Сохранить

Удалить

Отмена

Рис. 24: Форма редактирования

После успешного редактирования в верхнем левом углу экрана отобразится сообщение «Компонент обновлен» (Рисунок 25).

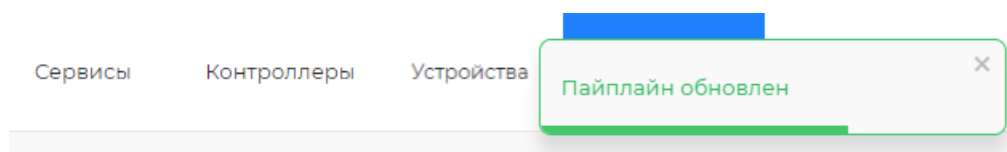


Рис. 25: Подтверждение обновления

5.6.5. Перезапуск компонента


Для перезапуска компонента необходимо нажать кнопку  (Рисунок 26).



Рис. 26: Перезапуск компонент

После успешного перезапуска в верхнем левом углу экрана отобразится сообщение «Компонент перезапущен» (Рисунок 27).

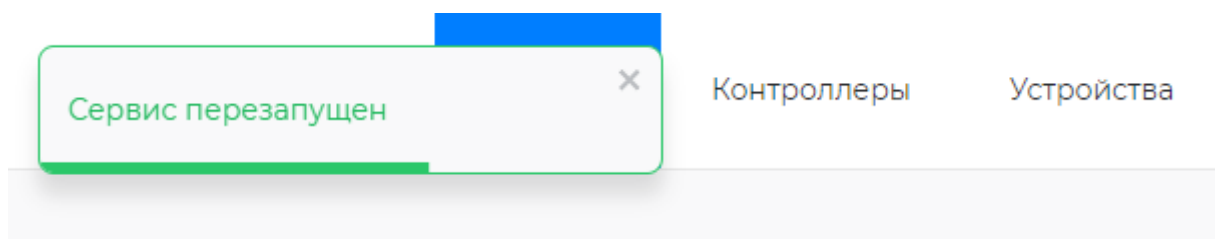


Рис. 27: Подтверждение перезапуска

5.6.6. Удаление компонента

Для удаления компонента необходимо выполнить следующие действия:

1. Нажать кнопку  (Рисунок 28).

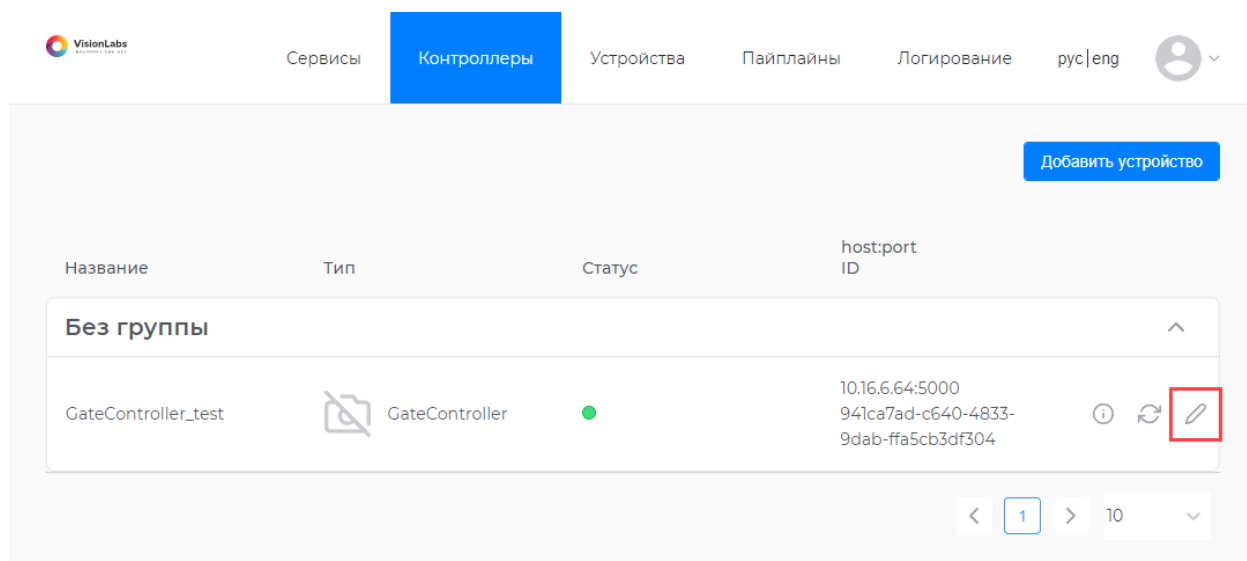


Рис. 28: Удаление компонента

2. Откроется форма для редактирования компонента, в которой необходимо нажать на кнопку «Удалить» в левом нижнем углу (Рисунок 29).

<

Редактирование контроллера

LaurentController

ID	b5f92a58-edd3-4d0d-b0c
name	Laurent
host	10.16.7.33
port	80
scenario_id	30bf70e1-848a-4235-a554
relay	3
delay_time	5

Сохранить

Удалить

Отмена

Рис. 29: Удаление компонента

После успешного удаления компонента в верхнем левом углу экрана отобразится сообщение «Контроллер удален» (Рисунок 30).

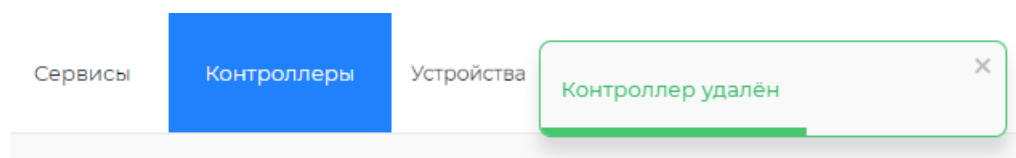


Рис. 30: Подтверждение удаления компонента

При успешном удалении компонент пропадет из списка.

При удалении сервиса удаляются его дочерние компоненты.

Дочерними компонентами выступают соответствующие контроллеры:

- сервис Apacs — ApacsController;
- сервис PercoWEB — PercoController;
- сервис Salto — SaltoController;
- сервис Strazh — StrazhController.

6. Логирование

Раздел «Логирование» предназначен для отображения системных логов и поиска логов в истории (Рисунок 31).

Получение и отображение новых логов выполняется с минимальными задержками в режиме, приближенном к реальному времени.

Access хранит логи за последние 7 дней во внутренней БД, после этого логи удаляются.

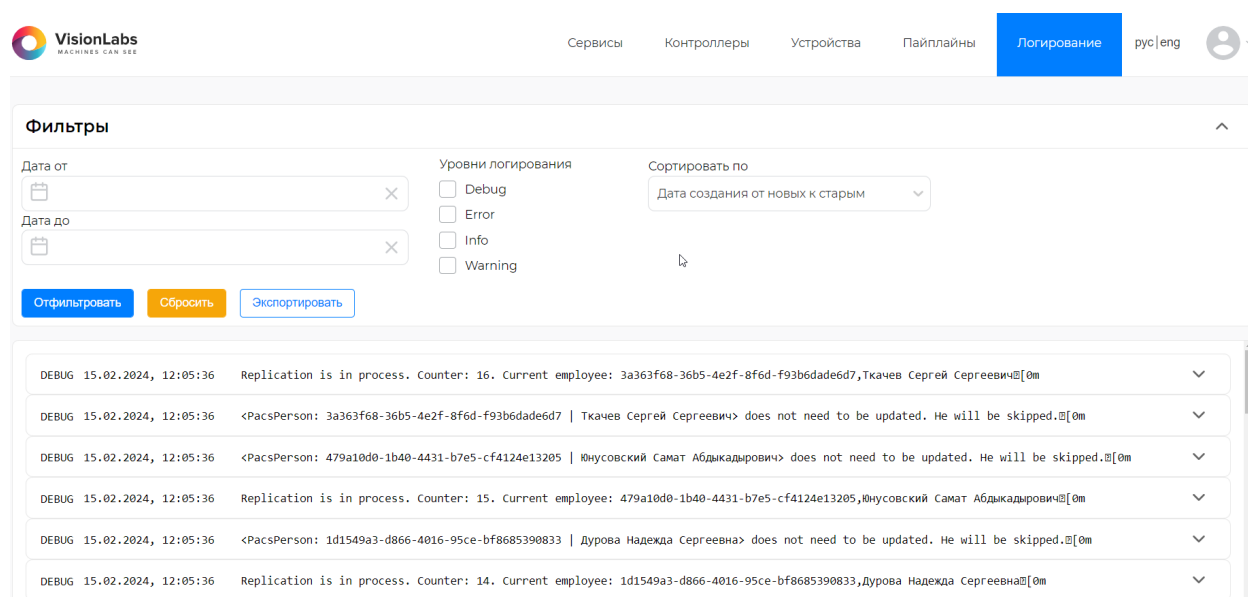


Рис. 31: Раздел «Логирование»

Для того, чтобы развернуть подробную информацию о целевом логе следует нажать на стрелку ▼ справа от необходимого лога (Рисунок 32).

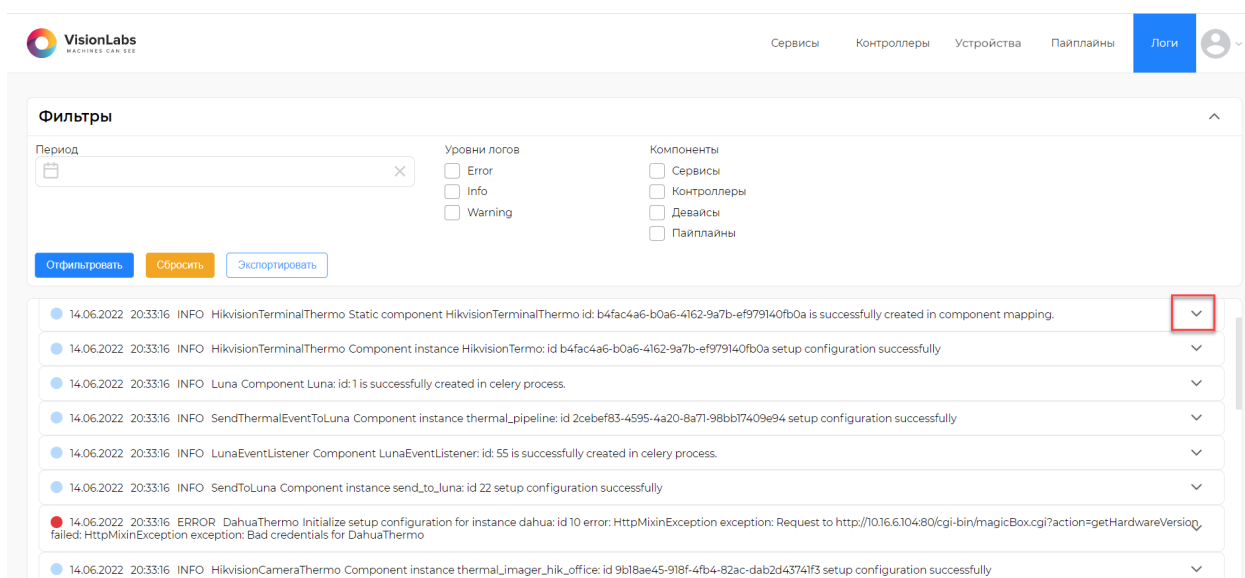


Рис. 32: Подробная информация о логах

Откроется целевой лог с подробной информацией (Рисунок 33).

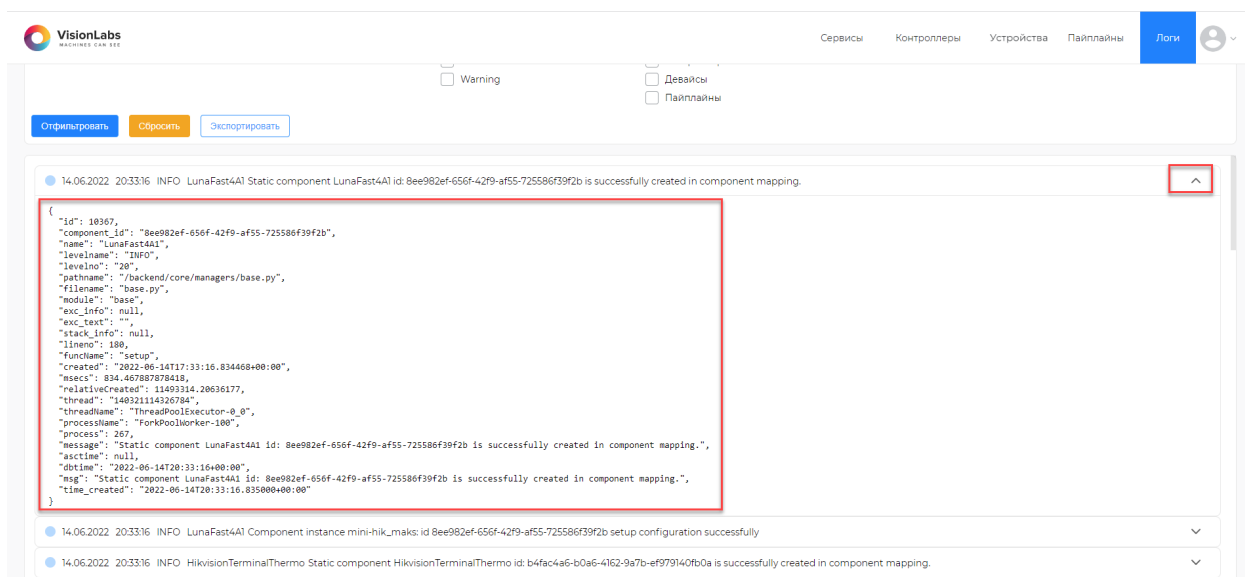
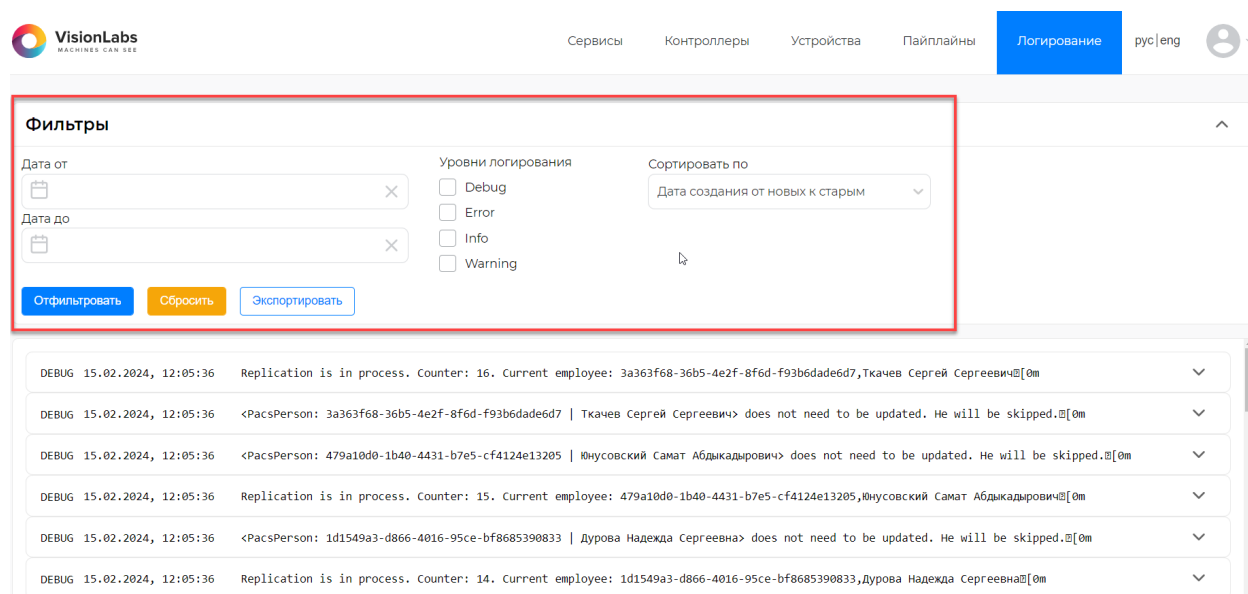


Рис. 33: Подробная информация о логах

6.1. Фильтрация логов

Раздел «Логирование» позволяет отфильтровать последние логи, чтобы ограничить отображение логов на экране (Рисунок 34).

С помощью фильтров пользователь может быстро найти необходимый лог.

**Рис. 34:** Фильтры в разделе «Логирование»

Фильтры, доступные пользователю на экране раздела «Логирование»:

- «Дата» — выбор периода фиксации логов;
- «Уровни логирования» — выбор уровня логов («Debug», «Error», «Info», «Warning»);
- «Сортировать» — выбор варианта сортировки логов («От старых к новым», «От новых к старым»).

Пользователю необходимо поставить галочку у необходимого(-ых) фильтра(-ов), и нажать кнопку «Отфильтровать» в левом нижнем углу, чтобы установленные настройки применились (Рисунок 35).

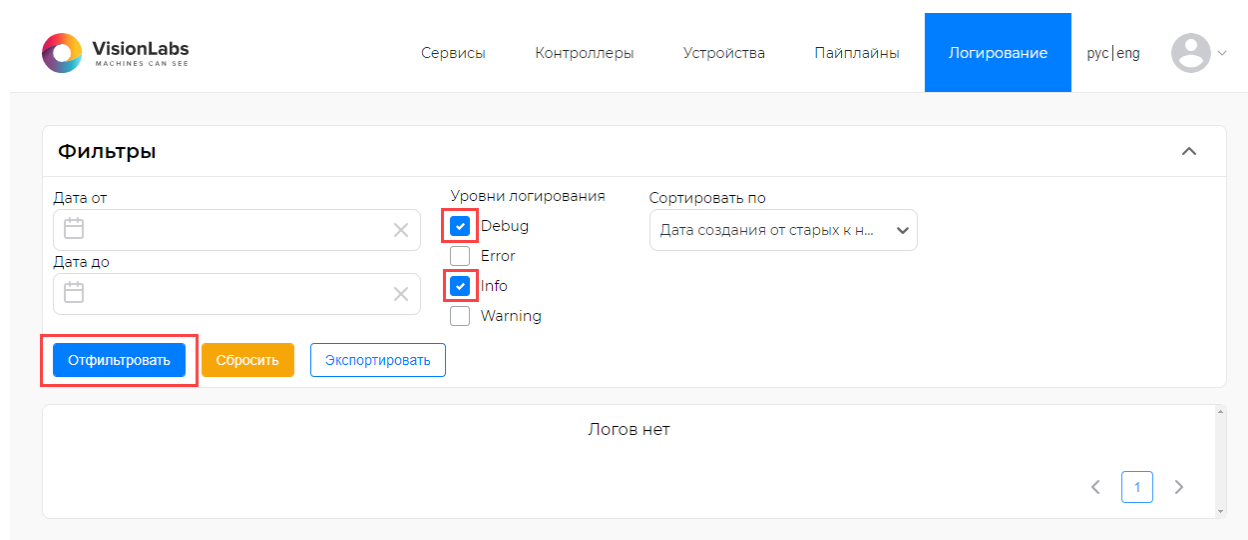


Рис. 35: Выбор фильтров

При успешном применении фильтров должна отобразиться информация с логами с учетом выбранных фильтров (Рисунок 36).

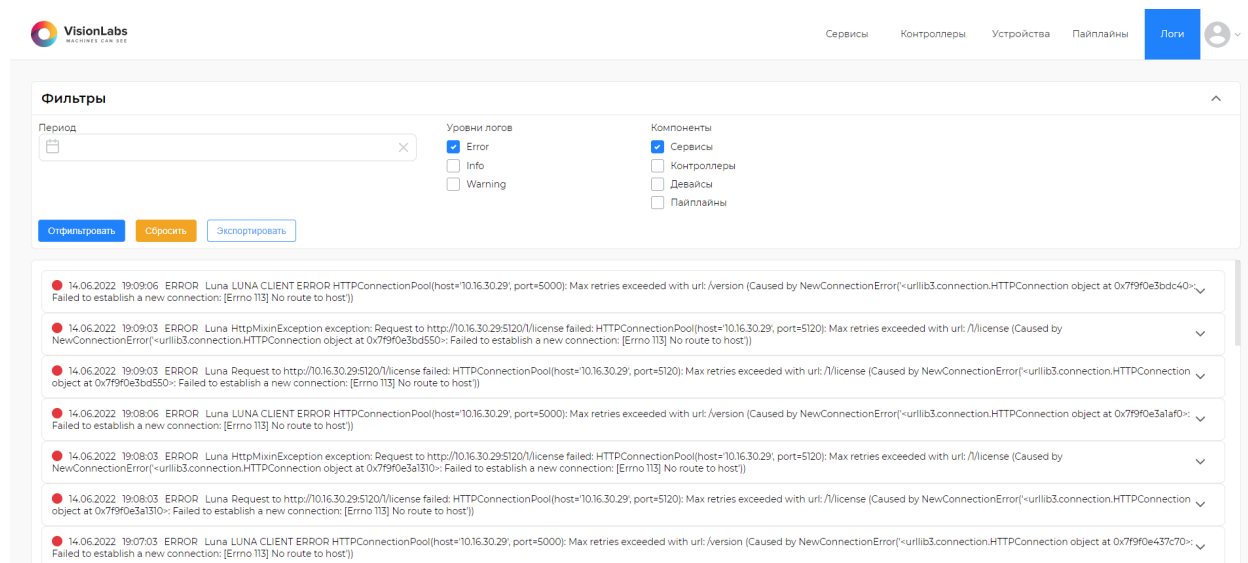


Рис. 36: Отображение логов после фильтрации

Для сброса установленных фильтров необходимо нажать кнопку «Сбросить» (Рисунок 37).

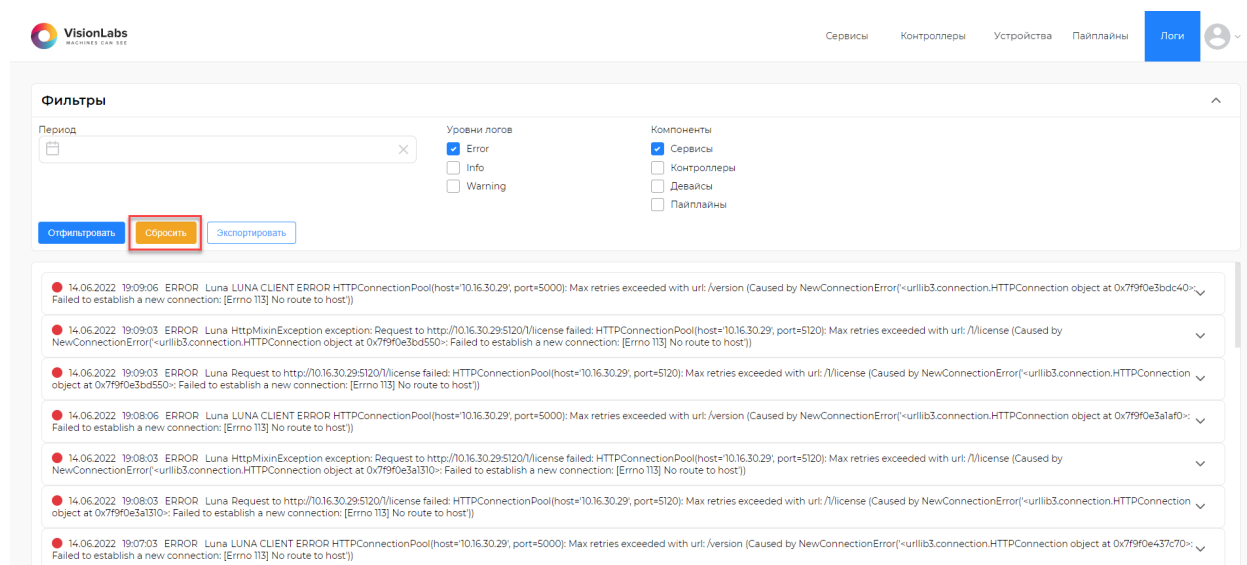


Рис. 37: Сброс настроек фильтра

При необходимости можно экспортировать отфильтрованные логи. Для этого необходимо нажать кнопку «Экспортировать» (Рисунок 38). Логи сохраняются на локальный компьютер в формате txt.

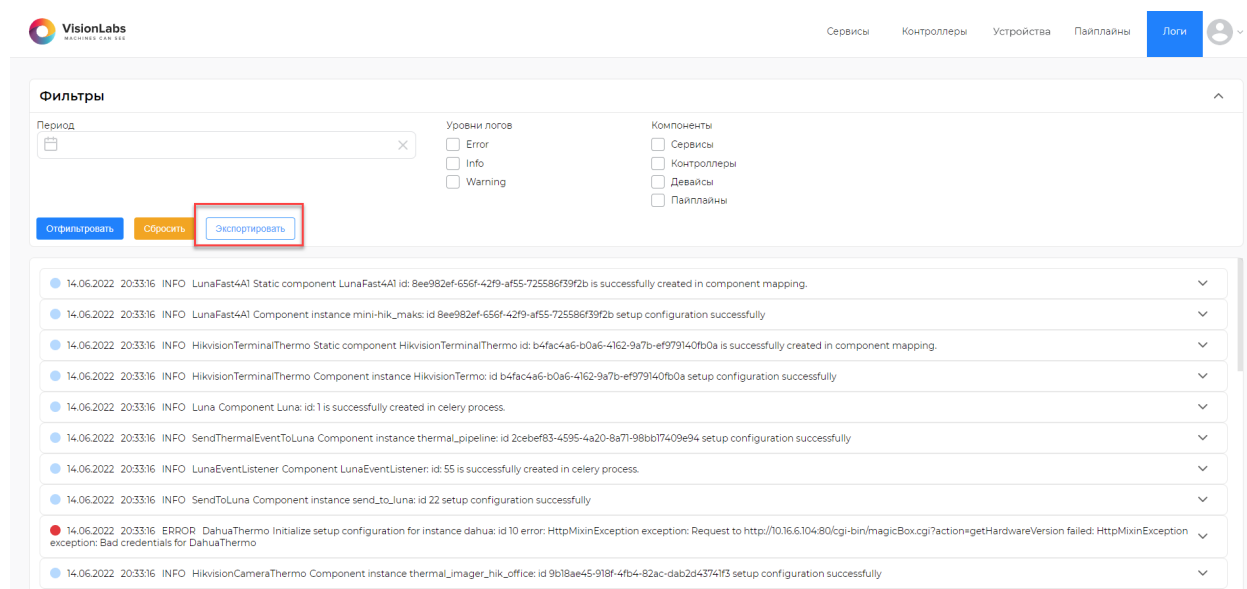


Рис. 38: Экспорт логов

Чтобы свернуть блок «Фильтры», необходимо нажать на стрелку ▼ в правом верхнем углу (Рисунок 39).

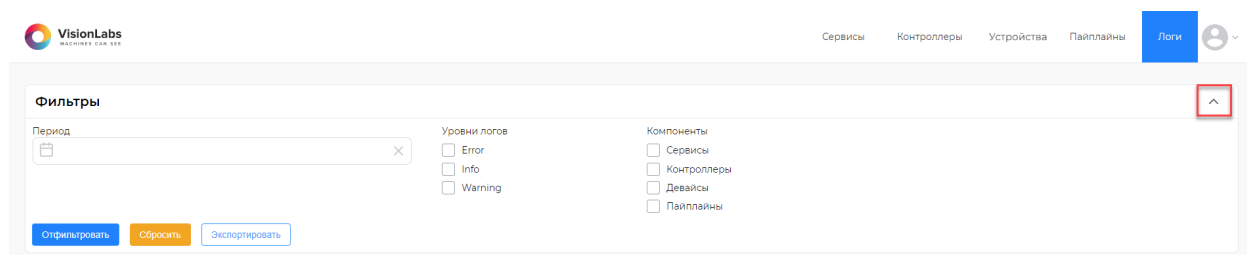


Рис. 39: Скрытие фильтров

7. Функции Access

7.1. Импортировать настройки

Функция «Импортировать настройки» предназначена для импорта настроек с локального компьютера в Access.

Для импорта настроек выполните следующие действия:

1. В правом верхнем углу нажать на стрелку ▼ справа от аватара пользователя, чтобы развернуть выпадающее меню (Рисунок 40).

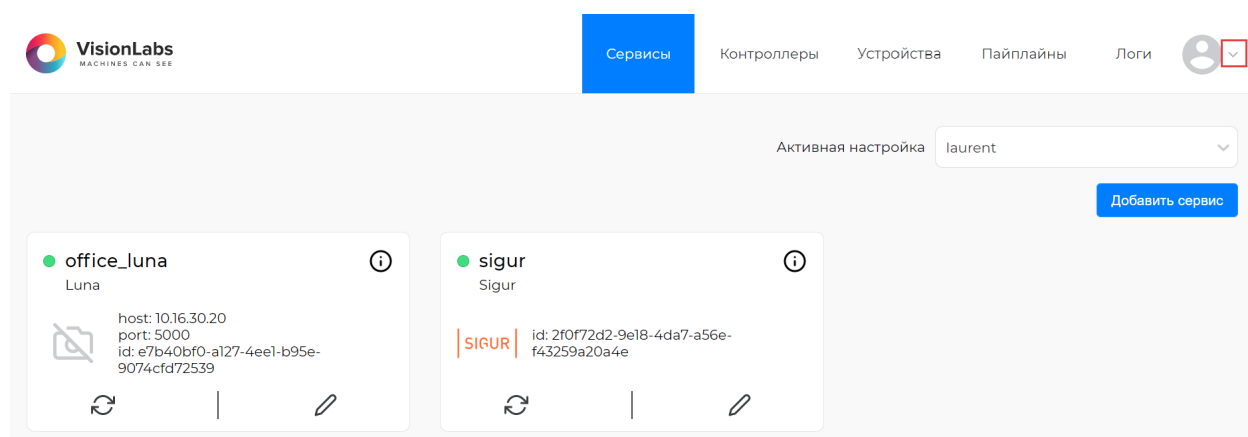


Рис. 40: Переход к функции «Импортировать настройки»

2. В выпадающем меню выбрать функцию «Импортировать настройки» (Рисунок 41).

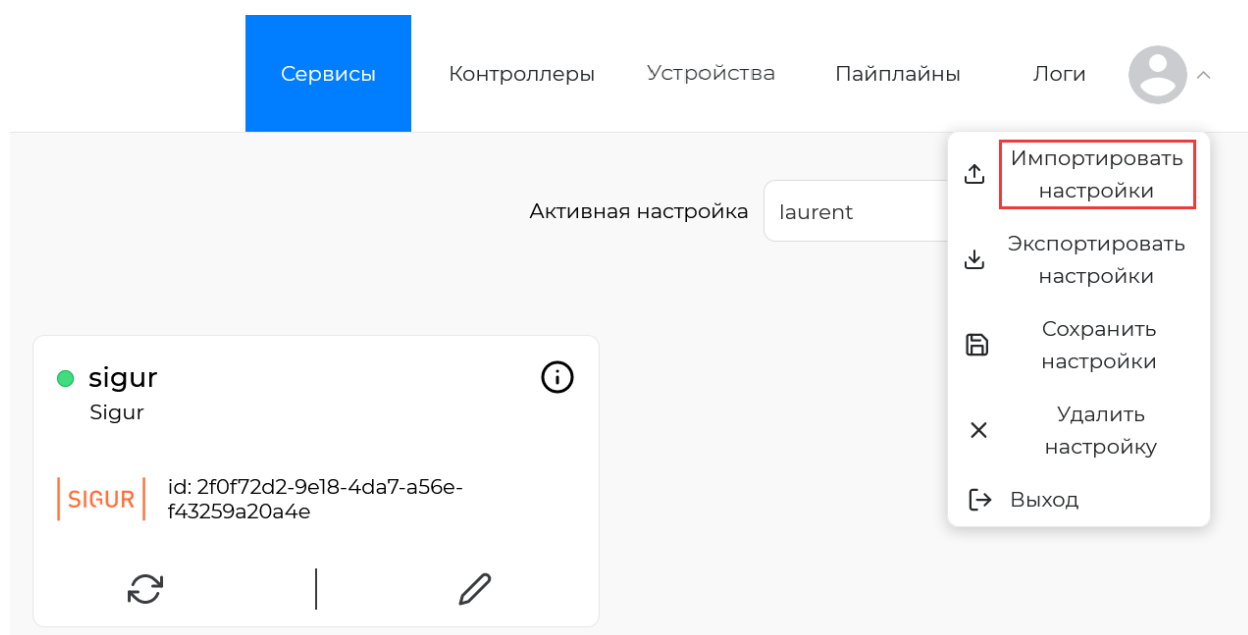




Рис. 41: Функция «Импортировать настройки»

3. Откроется форма для экспорта файла, нажмите на  , чтобы выбрать файл в формате json (Рисунок 42).

Файл настройки





Добавить

Рис. 42: Выбор файла настроек

4. В поле «Название настройки» перенесется название импортируемого файла, при необходимости укажите имя загружаемой настройки (Рисунок 43).

Файл настройки

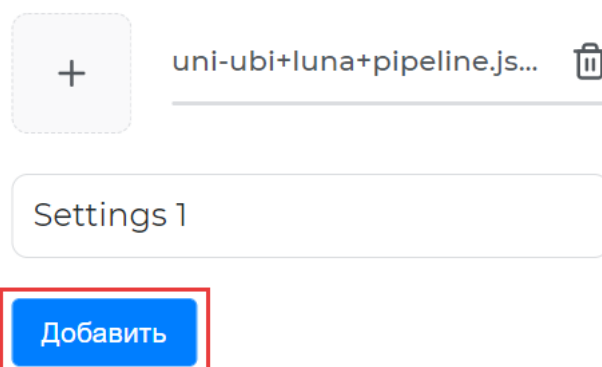
 

Добавить

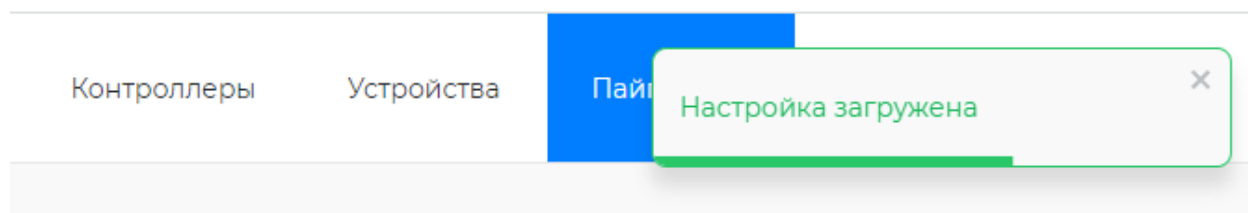
Рис. 43: Поле «Название настройки»

5. Нажмите на кнопку «Добавить» (Рисунок 44).

Файл настройки

**Рис. 44:** Добавление файла настройки

После успешного импорта настройки в верхнем левом углу экрана отобразится сообщение «Настройка загружена» (Рисунок 45).

**Рис. 45:** Подтверждение загрузки настройки

Если настройка создана и импортирована корректно, то компоненты, которые содержатся в данной настройке отобразятся в соответствующих разделах «Сервисы», «Контроллеры», «Устройства» и «Пайплайны».

7.2. Экспортировать настройки

Функция «Экспортировать настройки» предназначена для экспорта настроек на локальный компьютер из Access.

Чтобы выполнить экспорт настроек, необходимо выполнить следующие действия:

1. В правом верхнем углу нажать на стрелку ▼ справа от аватара пользователя, чтобы развернуть выпадающее меню (Рисунок 46).

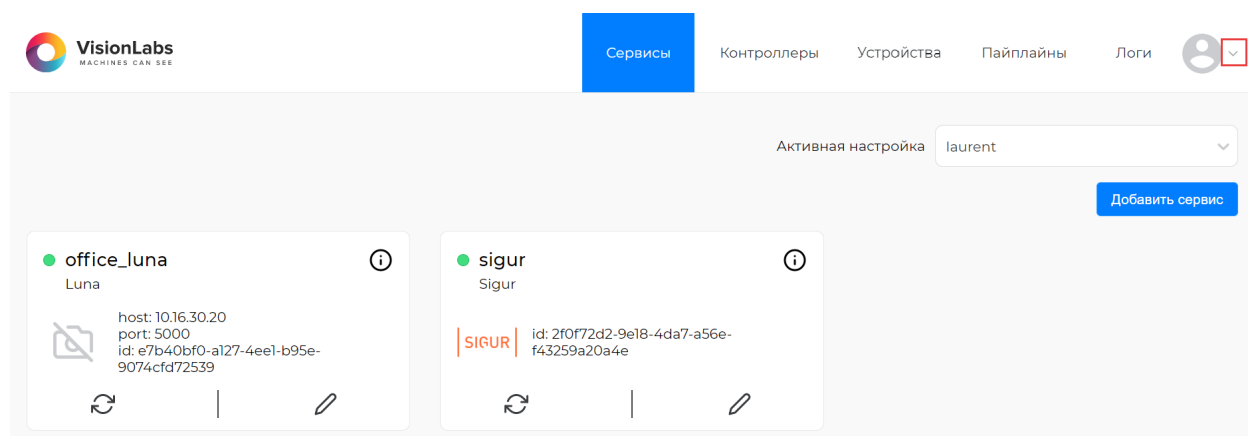


Рис. 46: Переход к функции «Экспортировать настройки»

- В выпадающем меню выбрать функцию «Экспортировать настройки» (Рисунок 47).

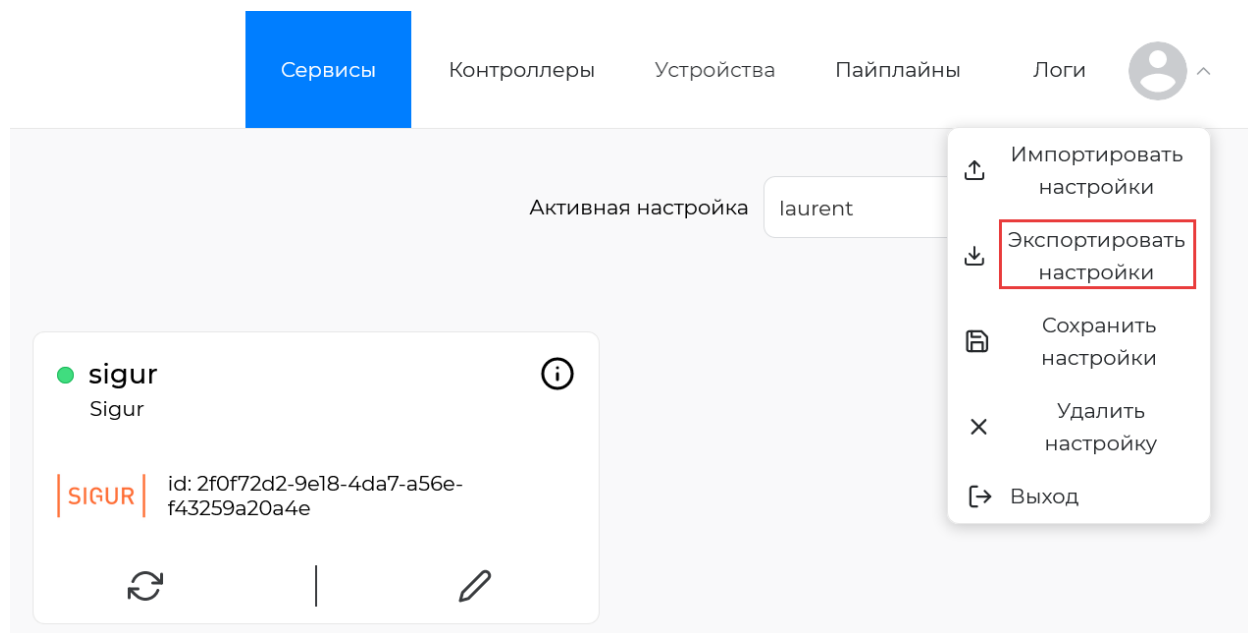


Рис. 47: Функция «Экспортировать настройки»

Файл с настройками будет загружен на локальный компьютер в формате json с параметрами всех компонентов, которые содержатся в данной настройке.

7.3. Сбросить настройки

Функция «Сбросить настройки» удаляет все компоненты и связанные с ними данные в разделах «Сервисы», «Контроллеры», «Устройства» и «Пайплайны».

7.4. Переменные ФИО

Поле для ввода `successful_pass_message_template` позволяет выводить ФИО распознанных лиц:

Если ФИО имеет более 30 символов, то имя будет сокращено до Фамилия И.О.

- `{fullname}` - ФИО лица из поля «Информация» (`user_data`). Иванов Петр Сергеевич;
- `{lastname}` - Фамилия лица. Это первое слово из поля «Информация». Иванов;
- `{firstname}` - Имя лица. Это второе слово из поля «Информация». Петр;
- `{middlename}` - Отчество лица. Это третье слово из поля «Информация». Сергеевич;
- `{short_lastname}` - Первая буква фамилии с точкой на конце. И.;
- `{short_firstname}` - Первая буква имени с точкой на конце. П.;
- `{short_middlename}` - Первая буква отчества с точкой на конце. С. .

Для вывода сообщения на экране терминала необходимо указать желаемые варианты ФИО в поле `successful_pass_message_template` в настройках устройств (Таблица 8).

Таблица 8. Пример использования переменных ФИО

Запись в настройках	Вывод на терминале
Добро пожаловать, {fullname}!	Добро пожаловать, Иванов Петр Сергеевич!
Добро пожаловать, {firstname} {middlename}!	Добро пожаловать, Петр Сергеевич!

7.5. Прочие функции

7.5.1. Документация

Кнопка «Документация» предназначена для перехода на HTML документацию Access.

8. Сервисы

Сервисы в Access необходимы для выбора параметров для подключения к внешним системам.

Все поля настройки являются обязательными, если не указывается обратное.

8.1. Апас

Сервис предназначен для взаимодействия со СКУД **APACS 3000**.

8.1.1. Функционал сервиса Апас

Основные функции:

- добавление контроллеров, с которыми будет работать биометрическая система;
- получение регулярных обновлений персон и контроллеров из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в локальном хранилище персон;
- получение событий идентификаций;
- отправка запроса в ПО СКУД о событиях идентификаций;
- интеграция с LP5;
- интеграция с КБС: Альфа;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.1.2. Настройка параметров для подключения к СКУД APACS

Настройки сервиса и возможные значения (Таблица 9):

Таблица 9. Настройка сервиса APACS

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
bio_system_id	Выпадающий список для выбора биометрической системы (LP5 или КБС) в Access.	-	-
host	IP адрес или доменное имя сервера с установленным ПО APACS	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт на котором развернут APACS	-	7010
max_workers	Количество параллельных потоков для репликации лиц	>0	10
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа используемой сети.	On - https	Off
		Off - http	
login	Логин пользователя ПО СКУД. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в ПО СКУД APACS	-
password	Пароль пользователя созданный в ПО СКУД APACS.	Поддерживается ввод латиницы, цифр и символов.	-
feature_profile	Ключ профиля, принадлежащий мастер ключу системы. Данные ключа располагаются в ПО СКУД APACS: «Справка» → «О программе»	-	-
rabbitmq_login	Имя пользователя из RabbitMQ от Apacs	Поддерживается ввод латиницы и цифр	-
rabbitmq_password	Пароль пользователя из RabbitMQ от Apacs	Поддерживается ввод латиницы и цифр	-

Параметр	Описание	Возможные значения	Значение по умолчанию
card_format_source	Тип формата карт, для выгрузки кодов организаций и их смещений. Подробнее см. ниже	-	-
enable_controller_creation	Включение репликации контроллеров ApacsController	On - репликация включена Off - репликация отключена	On
card_priority_number	Маркер приоритета для карт. Все карты с таким же номером приоритета будут более приоритетными	Числовые значения больше или равные 0	-
kyc_field_number	Номер дополнительного поля в карточках сотрудников, где прописаны внутренние id сотрудников (KYC)	1-20	-

Мастер ключ можно найти в любом клиентском приложении Apacs в разделе «Справка» → «О программе».

Тип формата карт (card_format_source) можно найти в любом клиентском приложении Apacs во вкладке «Консоль» → раздел «Корень системы» → раздел «Сервер оборудования» → выберите сетевой драйвер → выберите контроллер → раздел «Группа: Формат карт» → выберите любой формат карты → вкладка «Общие» → поле «Тип объекта».

8.2. Bastion

Сервис предназначен для взаимодействия со [СКУД Bastion 2 и 3](#).

8.2.1. Функционал сервиса Bastion

Основные функции:

- получение информации о точках доступа;
- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в локальном хранилище персон;
- получение событий идентификаций;
- отправка запроса в ПО СКУД о событиях идентификаций;
- интеграция с КБС МТС и LP 5;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.2.2. Настройка параметров для подключения к СКУД Бастион

Настройки сервиса и возможные значения (Таблица 10):

Таблица 10. Настройка сервиса Bastion

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выпадающий список для выбора идентификатора биометрической системы (LP5 или КБС) в Access.	-	-
host	IP адрес или доменное имя сервера с установленным ПО Bastion	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт Onvif сервиса Bastion 2. Для сервиса Bastion 3 используется порт 8089	-	10112
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https	Off

Параметр	Описание	Возможные значения	Значение по умолчанию
		Off - http	
username	Логин пользователя Onvif сервиса Bastion	Пользователь созданный в Bastion	-
password	Пароль пользователя Onvif сервиса Bastion	Пароль пользователя	-
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
bastion_version	Выпадающий список для выбора версии СКУД Бастион	2 или 3	2

8.3. Bolid

Сервис предназначен для взаимодействия со СКУД [Болид](#).

8.3.1. Настройка параметров для подключения к СКУД Болид

Настройки сервиса и возможные значения (Таблица 11):

Таблица 11. Настройка сервиса Bolid

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
bio_system_id	Выпадающий список для выбора биометрической системы (LP5 или КБС) в Access.	-	-
host	IP адрес или доменное имя сервера с установленным ПО Bolid	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт сервиса Bolid	-	8090
max_workers	Количество обработчиков репликации данных из биометрической системы в Бolid. Количество задается исходя от нагрузки на биометрическую систему	>0	10
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https	Off
		Off - http	
login	Логин пользователя Бolid. Задается в ПО Бolid: АБД → Пароли → Тип пароля — «Удаленное управление»	Пользователь созданный в Бolid. Поддерживается ввод латиницы, цифр и символов.	-
password	Пароль пользователя Бolid. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-

Параметр	Описание	Возможные значения	Значение по умолчанию
token_ttl_sec	Время для обновления токена доступа в секундах. Найти значение в файле ProgramData\BolidIntegrServ\settings.ini поле TokenLifeTime	Не рекомендуется менять параметр.	300

8.4. CbsAkbars

Используется для получения идентификатора дескриптора в КБС Акбарс по фотографии.

8.4.1. Настройка параметров для подключения к CbsAkbars

Настройки сервиса и возможные значения (Таблица 12):

Таблица 12. Настройка сервиса CbsAkbars

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя КБС	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к КБС	-	5000

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
token	Токен VisionLabs для доступа к КБС.	-	-
match_class	Опциональное поле для выбора одного или нескольких классов матчинга. Список классов задается перечислением значений через запятую.	-	fz115_class
		fz115_class	
		import_high_class	
		import_low_class	
		selfreg_class	
		selfreg_wopass_class	

8.5. CbsAlpha

Используется для получения идентификатора дескриптора в КБС Альфа по КУС. Проверяет наличие персоны по КУС в списке CbsAlpha с идентификатором указанным в параметре cbs_list_id, и создает персону если КУС не найден.

Поиск персон по КУС производится по значению, указанному в дополнительном поле 20 карточки сотрудника СКУД АРАС. Номер этого поля определяется параметром kyc_field_number в сервисе Aracs.

Данные KYC заполняются в поле `external_id` (Внешний ID) в LUNA CLEMENTINE 2.0.

Поддерживается работа только с LUNA PLATFORM 5.10 и новее.

8.5.1. Настройка параметров для подключения к CbsAlpha

Настройки сервиса и возможные значения (Таблица 13):

Таблица 13. Настройка сервиса CbsAlpha

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя КБС	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к КБС	-	5000
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
username	Логин пользователя LP5	-	-
password	Пароль пользователя LP5	-	-
account_id	UUID пользователя LP5	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
handler_id	UUID обработчика для работы с событиями прохода, созданный в LP5.	UUID обработчика	-
default_list_id	UUID идентификатора списка LP5, с которым будут синхронизированы сотрудники	Идентификатор списка, созданный в LP5.	-
face_detection_threshold	Минимальный порог при распознавании лиц	0...1	0.5
event_receiving_mode	Режим для получения событий от LP5 (от версии 5.53.0). Опциональное поле	None - не прослушивать события	websocket
		websocket - протокол с использованием постоянного соединения	
		webhook - обратные вызовы по протоколу HTTP. Клиент - Luna Platform, сервер - Luna Access	
vl_access_host	IP адрес сервера, на котором установлен Access. Обязательное поле при подключении через webhook	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access. Обязательное поле при подключении через webhook	-	9091

Параметр	Описание	Возможные значения	Значение по умолчанию
vl_access_basic_username	Логин для взаимодействия с Access. Обязательное поле при подключении через webhook	-	-
vl_access_basic_password	Пароль для взаимодействия с Access. Обязательное поле при подключении через webhook	-	-
max_greatest_side_size	Во время репликации, уменьшить большую сторону фотографии до указанного размера, сохраняя пропорции (Пустое значение - не уменьшать фотографии)	0...1920	-
cbs_list_id	Идентификатор списка лиц ЕБС	-	-

8.6. CbsAlphaListSynchronisation

Сервис предназначен для синхронизации двух списков в CbsAlpha. Сервис отслеживает изменения в cbs list и сопоставляет с лицами из luna list. В случае, если находятся дубликаты лиц, то удаление дубликата производится из luna list.

8.6.1. Настройка параметров CbsAlphaListSynchronisation

Настройки сервиса и возможные значения (Таблица 14):

Таблица 14. Настройка сервиса CbsAlpha

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
pac_id	Уникальный идентификатор сервиса в Access	Выпадающий список для выбора сервиса	-
synchronisation_interval_hours	Периодичность запуска синхронизации списков luna list и cbs list в часах	>0	-

8.7. CbsMts

Используется для получения идентификатора дескриптора в КБС МТС по фотографии.

8.7.1. Настройка параметров для подключения к CbsMts

Настройки сервиса и возможные значения (Таблица 15):

Таблица 15. Настройка сервиса CbsMts

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя в КБС	IP адрес в виде X.X.X.X. или site.domain.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
port	Порт для подключения к КБС. Поле может быть пустым	-	55580
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
urn	Путь до каталога лиц в КБС	-	/cbs/persons
token	Токен VisionLabs для доступа к КБС МТС	-	-
timeout	Время в секундах таймаута при неудачной попытке соединения с сервисом. Необходимо увеличивать время, если имеется большая задержка между серверами.	Время выбирается исходя из задержки в сети, для поддержания работоспособности.	10
cert_name	Имя сертификата для подключения к КБС. Директория хранения сертификатов '/tls/'	-	-

8.8. CbsVtb

Используется для получения идентификатора дескриптора в КБС ВТБ по фотографии.

8.8.1. Настройка параметров для подключения к CbsVtb

Настройки сервиса и возможные значения (Таблица 16):

Таблица 16. Настройка сервиса CbsVtb

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
auth_host	IP адрес или доменное имя сервера для получения токена авторизации КБС ВТБ. Запрашивается у представителя VisionLabs	IP адрес в виде X.X.X.X. или site.domain.	-
auth_port	Порт сервера для получения токена авторизации КБС ВТБ. Запрашивается у представителя VisionLabs	-	-
auth_enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
Off – неактивно			

Параметр	Описание	Возможные значения	Значение по умолчанию
auth_client_id	Идентификатор клиента для получения токена КБС ВТБ. Запрашивается у представителя VisionLabs	-	-
auth_client_secret	Секретный ключ клиента для получения токена. Запрашивается у представителя VisionLabs	-	-
host	IP адрес или доменное имя КБС ВТБ	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к КБС ВТБ	-	5000
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
user_session_id	Идентификатор пользовательской сессии для отправки фото на матчинг	-	-
ibm_client_id	Идентификатор ibm_client для отправки фото на матчинг. Запрашивается у представителя VisionLabs	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
system	Системный параметр КБС ВТБ. Запрашивается у представителя VisionLabs	-	-
channel	Системный параметр КБС ВТБ. Запрашивается у представителя VisionLabs	-	-
process_code	Системный параметр КБС ВТБ. Запрашивается у представителя VisionLabs	-	-
signer_service_id	Выпадающий список для выбора сервиса CryptoPro	Добавленный сервис CryptoPro	-

8.9. CryptoPro

Используется для подписи или расшифровки запросов на идентификацию в биометрическую систему.

Основные функции:

- выбор сертификата для подписи;
- выбор типа создаваемой подписи;
- создание совмещенной подписи (содержит в себе подписываемый контент и подпись);
- создание открепленной подписи (только подпись);
- проверка подписи.

8.9.1. Настройка параметров для подключения к CryptoPro

Настройки сервиса и возможные значения (Таблица 17):

Таблица 17. Настройка сервиса CryptoPro

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя сервиса	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к сервису	-	-
api_key	Токен доступа к сервису	-	-
cert_serial_number	Серийный номер целевого сертификата (получить список установленных сертификатов можно через API: http://host:port/docs)	-	-
cert_pin	PIN-код целевого сертификата	-	-
signature_type	Тип создаваемой подписи	PKCS7 CADES_BES	-

8.10. EyelsProxy

Сервис-прокси, обеспечивающий передачу данных между клиентом и контроллером: принимает запрос от клиента, отправляет его контроллеру, получает ответ и возвращает его обратно клиенту.

8.10.1. Настройка параметров для подключения к EyelsProxy

Настройки сервиса и возможные значения (Таблица 18):

Таблица 18. Настройка сервиса EyelsProxy

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя контроллера Eyels	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к контроллеру Eyels	-	-

8.11. Gate

Сервис предназначен для взаимодействия со СКУД Gate.

8.11.1. Настройка параметров для подключения к Gate

Настройки сервиса и возможные значения (Таблица 19):

Таблица 19. Настройка сервиса Gate

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
luna_id	Выпадающий список для выбора идентификатора сервиса Luna		-

8.12. Luna

Сервис для работы с LP5. Сервис предназначен для обмена данными с LP5 с последующей передачей во внешние системы и устройства.

Поддерживаемые версии: 5.10 и выше.

8.12.1. Настройка параметров для подключения к Luna

Настройки сервиса и возможные значения (Таблица 20):

Таблица 20. Настройка сервиса Luna

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя сервера с установленной LP5	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт сервера, на котором развернута LP5	-	5000
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа используемой сети.	On - https Off - http	Off
username	Логин пользователя LP5. Заполняется, если не указан account_id	-	-
password	Пароль пользователя LP5. Заполняется, если не указан account_id	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
account_id	UUID пользователя LP5. Если задан, поля username и password не требуются	-	-
handler_id	UUID обработчика для работы с событиями прохода, созданный в LP5.	UUID обработчика	-
default_list_id	UUID идентификатора списка LP5, с которым будут синхронизированы сотрудники	Идентификатор списка, созданный в LP5.	-
face_detection_threshold	Минимальный порог при распознавании лиц	0...1	0.5
event_receiving_mode	Режим для получения событий от LP5 (от версии 5.53.0). Опциональное поле	None - не прослушивать события	websocket
		websocket - протокол с использованием постоянного соединения	
		webhook - обратные вызовы по протоколу HTTP. Клиент - Luna Platform, сервер - Luna Access	
vl_access_host	IP адрес сервера, на котором установлен Access. Обязательное поле при подключении через webhook	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access. Обязательное поле при подключении через webhook	-	9091

Параметр	Описание	Возможные значения	Значение по умолчанию
vl_access_basic_username	Логин для взаимодействия с Access. Обязательное поле при подключении через webhook	-	-
vl_access_basic_password	Пароль для взаимодействия с Access. Обязательное поле при подключении через webhook	-	-
max_greatest_side_size	Во время репликации, уменьшить большую сторону фотографии до указанного размера, сохраняя пропорции (Пустое значение - не уменьшать фотографии)	0...1920	-

8.13. LunaAceConverter

Сервис для отправки данных полученных от устройств LUNA ACE в LP5. Полученный запрос от устройства, перенаправляется в LP5, затем генерируется ответ для устройства на основе полученного ответа от LP5.

- Поддерживается версия LUNA ACE 1.2.23

8.13.1. Настройка параметров для подключения к LUNA ACE

Настройки сервиса и возможные значения (Таблица 21):

Таблица 21. Настройка сервиса LUNA ACE

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
luna_id	Выпадающий список для выбора идентификатора сервиса Luna в Access.	-	-

8.13.2. Настройка LUNA ACE

1. Подключитесь к устройству по SSH.
2. Откройте файл: `vi /opt/luna_ace/ace_device.conf`.
3. В параметре `luna_platform_address` указать URL сервиса LunaAceConverter.

Для получения URL сервиса необходимо перейти в созданный сервис LunaAceConverter в Access и скопировать полный путь из строки поиска браузера:

```
http://<ip_address>:9092/service/<UUID>
```

4. Перейдите в директорию: `cd /opt/luna_ace/services/ace_device`
5. Перезапустите устройство: `restart`

8.14. LunaCars

Сервис для программно-аппаратной интеграции, необходимый для связи LUNA CARS и преграждающих устройств – шлагбаумов, откатных ворот и так далее, для контроля доступа ТС.

Сервис интеграции с LUNA CARS. Поддерживаемые модули LUNA CARS:

- LUNA CARS API: v.4.0.15;
- LUNA CARS Stream: v.3.0.20;
- LUNA CARS Analytics: v.4.0.8.

Access подключается к LUNA CARS Analytics backend.

События в очереди имеют тип `CarDetectionEvent`.

8.14.1. Настройка параметров для подключения к LunaCars

Настройки сервиса и возможные значения (Таблица 22):

Таблица 22. Настройка сервиса LunaCars

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя сервера с установленным LUNA CARS Analytics.	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт сервера, на котором развернут LUNA CARS Analytics backend.	-	8080
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https Off - http	Off
api_port	Порт сервера, на котором развернут LUNA CARS API	-	8100
login	Логин администратора LUNA CARS Analytics. Поддерживается ввод латиницы, цифр и символов.	-	admin@test.ru
password	Пароль администратора LUNA CARS Analytics. Поддерживается ввод латиницы, цифр и символов.	-	admin

Параметр	Описание	Возможные значения	Значение по умолчанию
event_expiry_time	Через сколько секунд события можно пропустить как устаревшие, необходимо уменьшать время до ~15 секунд, если поток ТС постоянный.	>10	60
min_license_plate_accuracy	Минимальная точность распознавания государственного номерного знака. При котором будет производиться идентификация ГРЗ.	Значение формируется на этапе проектирования и корректируется на этапе тестирования. 0,00..1,00 0,00 – идентифицировать все ГРЗ. 1,00 – идентифицировать ГРЗ только в лучшем качестве.	0,6
event_memory_time	Время в секундах, за которое сервис не создает повторное событие на это же ТС, необходимо увеличивать значение, если ТС долго стоит в зоне распознавания в очереди на въезд и по схожим причинам.	60...180	90
timeout	Время таймаута при неудачной попытке соединения с сервисом. Необходимо увеличивать время, если имеется большая задержка между серверами.	Время выбирается исходя из задержки в сети, для поддержания работоспособности.	-

8.15. LunaStreams

Сервис для работы с LunaStreams.

LunaStreams это сервис FaceStream.

Сервис предназначен для:

- получения списка имен потоков из LunaStreams для последующей передачи в СКУД.
- формирования события детекции на основе кадра из LunaStreams для последующей отправки на матчнинг в любые поддерживаемые биометрические системы, в т.ч. Luna, CbsMts, CbsAlpha, CbsVtb, CbsAkbars.

Поддерживаемые версии:

- FaceStream 5.1.6 и новее;
- LunaStreams 0.2.1 и новее.

8.15.1. Настройка параметров для подключения к LunaStreams

Настройки сервиса и возможные значения (Таблица 23):

Таблица 23. Настройка сервиса LunaStreams

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя сервера с установленным LunaStreams	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт сервера, на котором развернут LunaStreams	-	5160
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https	Off

Параметр	Описание	Возможные значения	Значение по умолчанию
handle_event_interval	Интервал задержки между получением детекции от одного источника.	Off - http 1...10	3

8.16. Parsec

Сервис предназначен для взаимодействия со СКУД [Parsec](#) для обеспечения прохода распознанных лиц через турникет/дверь с магнитным замком.

8.16.1. Возможности Parsec

Основные возможности:

- получение информации о точках доступа;
- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/редактирование/удаление данных в локальном хранилище персон;
- получение событий идентификаций;
- отправка запроса в ПО СКУД о событиях идентификаций;
- интеграция с КБС МТС и LP 5;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.16.2. Настройка параметров для подключения к Parsec

Настройки сервиса и возможные значения (Таблица 24):

Таблица 24. Настройка сервиса Parsec

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выпадающий список для выбора имени биометрической системы (LP5 или КБС) в Access.	-	-
host	IP адрес или доменное имя сервера с установленным Parsec	IP адрес в виде X.X.X.X. или site.domain	-
port	Порт сервера, на котором развернут Parsec	-	-
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https Off - http	Off
username	Логин пользователя Parsec.	-	-
integration_key	Ключ интеграции Parsec. Используется в качестве пароля для подключения к сервису.	-	-
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091

8.17. PercoWeb

Сервис предназначен для взаимодействия со СКУД [PERCo-Web](#).

8.17.1. Функции PercoWeb

Основные функции:

- добавление контроллеров, с которыми будет работать LP5;
- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в LP5;
- получение событий идентификаций;
- отправка запроса в ПО СКУД о событиях идентификаций;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.17.2. Настройка параметров для подключения к СКУД PERCo-Web

Настройки сервиса и возможные значения (Таблица 25):

Таблица 25. Настройка сервиса PercoWeb

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Идентификатор биометрической системы	-	-
host	IP адрес или доменное имя сервера с установленным PERCo-Web	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт сервера, на котором развернут PERCo-Web	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа используемой сети.	On - https Off - http	Off
login	Логин пользователя PERCo-Web. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в PERCo-Web	-
password	Пароль пользователя PERCo-Web. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
token_ttl_min	Срок действия токена безопасности в минутах. Значение должно совпадать с ПО PERCo-Web, расположение Менеджера PERCo-Web → Настройки → Дополнительные настройки → Время жизни сессии. (по умолчанию 1 день).	-	1440
max_workers	Максимальное количество потоков, которые можно использовать для репликации лиц.	>0	10

8.18. PersonStorageActualization

Сервис периодически актуализирует данные в хранилище персон (PersonStorage). Удаляет персону из хранилища персон, если она не была найдена в биометрической системе.

PersonStorage хранит в себе информацию о сотрудниках в СКУД и их descriptor_id из биометрической системы.

8.18.1. Настройка параметров PersonStorageActualization

Настройки сервиса и возможные значения (Таблица 26):

Таблица 26. Настройка сервиса PersonStorageActualization

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
pac_id	Уникальный идентификатор сервиса в Access	Выпадающий список для выбора сервиса	-
actualization_interval_hours	Периодичность актуализации персон в часах	>0	1

8.19. Rusguard

Сервис предназначен для взаимодействия со СКУД [RusGuard](#).

8.19.1. Функционал Rusguard

Основные функции:

- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в локальном хранилище персон;
- получение событий идентификаций;

- отправка запроса в ПО СКУД о событиях идентификаций;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет;
- возможна интеграция с КБС.

8.19.2. Настройка параметров для подключения к Rusguard

Настройки сервиса и возможные значения (Таблица 27):

Таблица 27. Настройка сервиса Rusguard

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Идентификатор биометрической системы	-	-
host	IP адрес или доменное имя сервера с установленным Rusguard	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт сервера, на котором развернут Rusguard	-	8089
max_workers	Максимальное количество потоков, которые можно использовать для репликации лиц.	>0	10
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа используемой сети.	On - https	Off
		Off - http	

Параметр	Описание	Возможные значения	Значение по умолчанию
target_photo_number	Номер фотографии в СКУД, которая используется для репликации.	1..3	1
target_card_type_id	Идентификатор реплицируемого типа карты. Если поле пустое, реплицируется любая карта сотрудника. Доступные идентификаторы типов карт, отображаются в блоке Info.	-	-
replicate_session_interval_sec	Периодичность синхронизации БД СКУД и хранилища Access, в секундах. Необходимо указывать минимально допустимое время синхронизации, так как Access не получает уведомлений от внешних системы о добавлении/удалении сотрудника.	>0	5

8.20. Salto

Сервис предназначен для взаимодействия со СКУД [SALTO](#).

8.20.1. Настройка параметров для подключения к СКУД SALTO

Для добавления сервиса необходимо создать его со следующими настройками (Таблица 28):

Таблица 28. Настройка сервиса Salto

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Идентификатор биометрической системы	-	-
host	IP адрес или доменное имя Salto.	-	-
port	Порт сервера, на котором развернут Salto.	-	8100
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа сети в решении.	On - https Off - http	Off
login	Логин пользователя Salto. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в Salto	-
password	Пароль пользователя Salto. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
max_workers	Максимальное количество потоков, которые можно использовать для репликации лиц.	>0	10

8.21. Sigur

Сервис предназначен для взаимодействия со СКУД [Sigur](#).

8.21.1. Функции Sigur

Основные функции:

- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в LP5;
- получение событий идентификаций;
- интеграции с КБС: МТС, ВТБ, Ак Барс;
- интеграция с LUNA CARS;
- отправка запроса в ПО СКУД о событиях идентификаций.
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.21.2. Настройка параметров для подключения к СКУД Sigur

Для добавления сервиса необходимо создать его со следующими настройками (Таблица 29):

Таблица 29. Настройка сервиса Sigur

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выпадающий список для выбора идентификатора биометрической системы (LP5 или КБС) в Access.	-	-
host	IP адрес или доменное имя Sigur.	IPv4 или site.domain	-
luna_cars_id	Идентификатор сервиса LunaCars в Access.	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
mark_for_ignore	При синхронизации с Sigur, если в теле запроса сотрудника встречается данная комбинация, то запрос игнорируется. Опция необходима для разнесения различных копий Sigur в одной системе.	Любое строковое значение	-
ignore_replication_field_name	Название дополнительного поля, отвечающего за игнорирование при репликации. Поле должно иметь логический тип, и отвечать на вопрос: Игнорировать сотрудника при репликации? (Да/Нет)	Любое строковое значение	-
additional_person_field	Название дополнительного поля из карточки сотрудника, где записан идентификатор дескриптора	Любое строковое значение	-

8.22. SigurThroughDatabase

Сервис обеспечивает интеграцию со СКУД Sigur через прямое подключение к его базе данных.

Access синхронизирует данные сотрудников из базы данных Sigur, учитывая только тех пользователей, у которых заведена карта доступа.

При успешной идентификации сотрудника в биометрической системе Luna, Access отправляет номер его карты на промежуточные контроллеры GateController или PusrController, физически подключенные к СКУД Sigur. Эти контроллеры передают команды на открытие/закрытие прохода.

Интеграция осуществляется напрямую с БД Sigur, без использования API

Sigur не инициирует соединение с Access — данные передаются только в одну сторону (от Access к Sigur через контроллеры)

Функционал SigurThroughDatabase

Основные функции:

- получение регулярных обновлений из БД ПО СКУД;
- отправка запросов на добавление/изменение данных в LP5;
- получение событий идентификаций;
- отправка запроса в ПО СКУД о событиях идентификаций;
- логирование событий о попытке прохода неидентифицированного сотрудника через турникет.

8.22.1. Варианты интеграции с LP5

В каждой интеграции с LP5 (Таблица 30) используется сервис [Luna](#).

Таблица 30. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
SigurThroughDatabase + PusrController / GateController	Beward	MatchByPhoto + SendToDevice + SendToController
	BioSmart	MatchByPhoto + SendToDevice + SendToController
	Dahua	MatchByPhoto + SendToController
	Dahua Thermo	MatchByPhoto + SendToController
	Fortuna315	MatchByPhoto + SendToController
	HikvisionCamera	MatchByPhoto + SendToController
	HikvisionCamera Thermo	MatchByPhoto + SendToController
	HikvisionTerminal Thermo	MatchByPhoto + SendToDevice + SendToController
	LunaFast4A1	MatchByPhoto + Custom2FA
	Panda	MatchByPhoto + SendToController
	UniUbi	MatchByPhoto + SendToDevice + SendToController
	VKVision02	LunaStreams + MatchByPhoto + SendToDevice + SendToController

Сервис	Устройство	Пайплайн
	R20Face	MatchByPhoto + SendToDevice + SendCardToR20Face

8.22.2. Настройка параметров для подключения к SigurThroughDatabase

При создании нового сервиса используются следующие настройки (Таблица 31):

Таблица 31. Настройка сервиса SigurThroughDatabase

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Идентификатор биометрической системы	-	-
host	IP адрес или доменное имя базы данных Sigur.	IP адрес в виде X.X.X.X. или site.domain.	
port	Порт базы данных Sigur.	-	3305
max_workers	Максимальное количество потоков, которые можно использовать для репликации лиц.	>0	10
db_username	Имя пользователя, с помощью которого происходит подключение к базе данных Sigur.	-	-
db_password	Пароль пользователя базы данных Sigur.	-	-

8.23. Strazh

Сервис предназначен для взаимодействия со СКУД [STRAZH](#).

- Поддерживает интеграции с КБС МТС.

8.23.1. Настройка параметров для подключения к СКУД STRAZH

Для добавления сервиса необходимо создать его со следующими настройками (Таблица 32):

Таблица 32. Настройка сервиса Strazh

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов	-
bio_system_id	Идентификатор биометрической системы	-	-
host	IP адрес или доменное имя сервера с установленным Strazh.	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт сервера, на котором развернут Strazh	-	443
max_workers	Максимальное количество потоков, которые можно использовать для репликации лиц.	>0	10
login	Логин пользователя Strazh. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в Strazh.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
password	Пароль пользователя Strazh. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
enable_ssl	Метод шифрования данных при передаче по сети. Зависит от типа используемой сети.	On - https Off - http	On
additional_person_field	Имя дополнительного поля персоны из СКУД, где будет записан идентификатор дескриптора.	-	-

8.24. Ubs

Сервис получает и обрабатывает сообщения от Kafka Московского регионального сегмента ЕБС, конечным результатом обработки является создание события идентификации.

8.24.1. Настройка параметров Ubs

Настройки сервиса и возможные значения (Таблица 33):

Таблица 33. Настройка сервиса Ubs

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
pacs_id	Уникальный идентификатор сервиса в Access	Выпадающий список для выбора сервиса	-
kafka_servers	Список IP-адресов или URL разделенных запятой, для подключения к Kafka ЕБС	-	
kafka_topic	Топик Kafka для прослушивания	-	
project_id	Идентификатор проекта в ЕБС	-	
event_expiry_time	Время актуальности события в секундах	60	

9. СКУД APACS

Программные интеграции ПО СКУД APACS с биометрическими системами реализованы для обеспечения прохода распознанных лиц через турникет/дверь с магнитным замком.

- Поддерживаемая версия СКУД APACS 8.3.1.0.

Поддерживается подключение контроллеров AAM LAN 8W и AAN.

Поддерживается возможность запуска нескольких экземпляров Luna Access в интеграции с одним СКУД APACS.

9.1. Поддерживаемые варианты интеграции СКУД APACS

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 34) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 34. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Apacs + ApacsController	LunaFast4A1	(SendToLuna + Apacs2FA) / (MatchByPhoto + SendToDevice + SendToController)
Apacs	GrgFaster	MatchByPhoto + SendToGrgFaster

В каждой интеграции с КБС (Таблица 35) используется сервис КБС.

Таблица 35. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsAlpha + Apacs + ApacsController	Beward	MatchByPhotoInCbsAlpha + SendToController + SendToDevice
	Dahua	MatchByPhotoInCbsAlpha + SendToController
	HikvisionCamera	MatchByPhotoInCbsAlpha + SendToController
	LunaFast4A1	MatchByPhotoInCbsAlpha + SendToController + SendToDevice
	UniUbi	MatchByPhotoInCbsAlpha + SendToController + SendToDevice
	R20Face	MatchByPhotoInCbsAlpha + SendCardToR20Face + SendToDevice
	HikvisionCamera	MatchByPhotoInCbsAlpha + SendToController

9.2. Стандартная интеграция с использованием Apacs

Интеграция 1ф (Рисунок 48) и (Таблица 36).

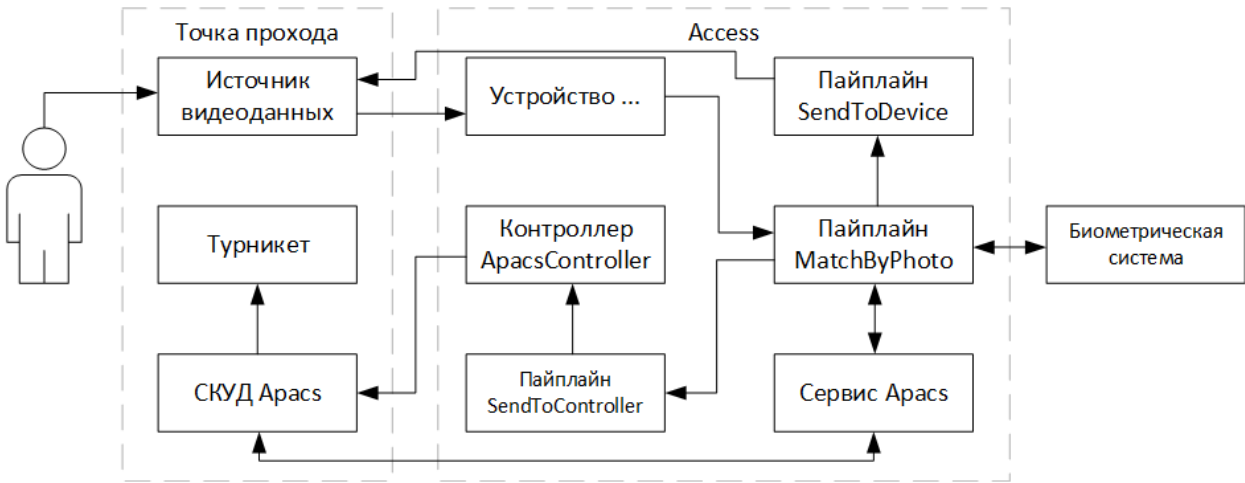


Рис. 48: Схема компонентов при 1ф интеграции с Apacs

Таблица 36. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.

Компонент	Описание
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream. Биометрический терминал позволяет создать обратную связь для демонстрации человеку информации о проходе.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Может быть либо Luna , либо сервис поддерживаемой КБС).
Сервис Араcs	Компонент Access для выполнения репликации/синхронизации сотрудников из СКУД и прослушивания событий СКУД.
Пайплайн SendToController	Компонент Access для отправки номера карты и ФИО в АраcsController с после матчинга человека и подтверждения номера карты в Access.
Контроллер АраcsController	Компонент Access для отправки в СКУД номера карты. При использовании контролера gate или rusr необходимо использовать соответствующий компонент. При использовании биометрического терминала, отправляет в него ФИО сотрудника для отображения на экране.
СКУД Араcs	Центральное ПО для работы с Араcs. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Турникет	Преграждающее устройство для разграничения доступов

Интеграция 2ф (Рисунок 49) и (Таблица 37).

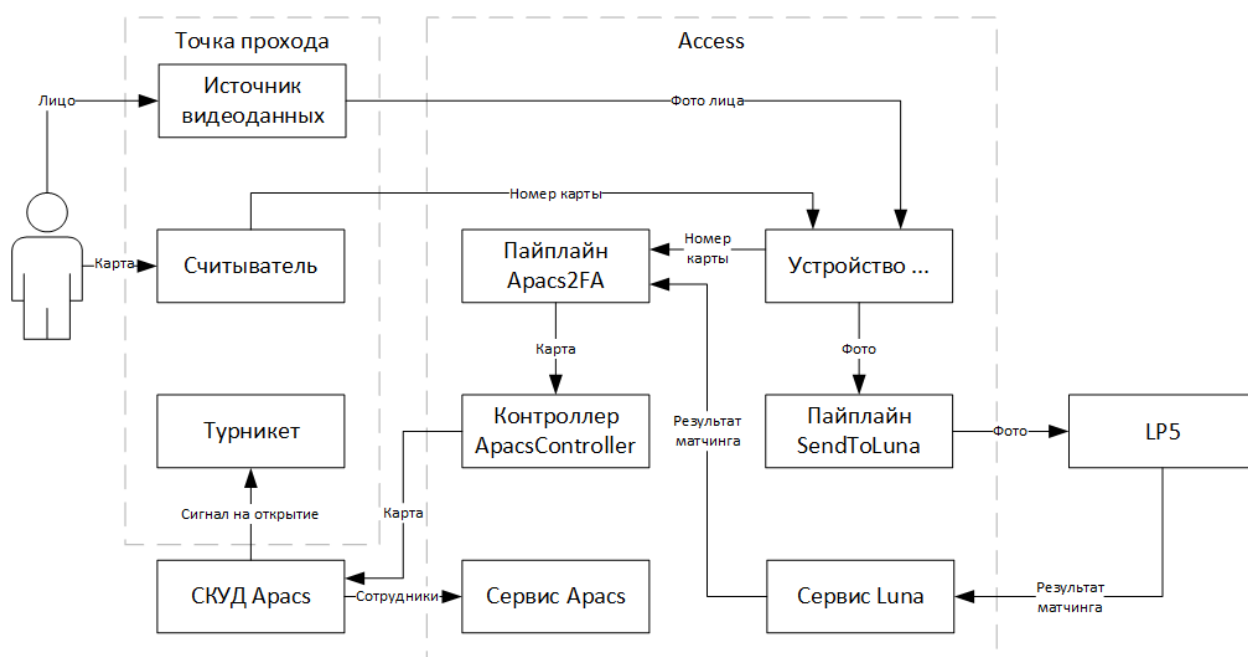


Рис. 49: Схема компонентов при 2ф интеграции с Apacs

Таблица 37. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Считыватель	Устройство для приема данных карты доступа.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Пайплайн SendToLuna	Компонент Access для отправки фото в LP5.
Сервис Luna	Компонент Access , который прослушивает события матчинга от LP5.

Компонент	Описание
LP5	Биометрическая система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных.
Пайплайн Apacs2FA	Компонент Access , который принимает событие с номером карты и событие матчинга человека. Сравнивает полученный номер от устройства с номером, соответствующем лицу и при их совпадении передает номер карты в ApacsController.
Контроллер ApacsController	Компонент Access для отправки в СКУД номера карты. При использовании контролера gate или push необходимо использовать соответствующий компонент.
Сервис Apacs	Компонент Access для выполнения репликации/синхронизации сотрудников из СКУД и прослушивания событий СКУД.
СКУД Apacs	Центральное ПО для работы с Apacs. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Турникет	Преграждающее устройство для разграничения доступов

9.3. Гостевой проход при двухфакторной аутентификации

При необходимости прохода гостя при активной двухфакторной аутентификации и отсутствии возможности получения фото гостя, необходимо выполнить следующие шаги:

1. Добавьте персону в СКУД без фотографии с ФИО и номером карты.
2. Включите опцию `use_cards_without_face` в настройках пайплайна [Apacs2FA](#).

9.4. Создание пользователя в RabbitMQ

Для создания пользователя в RabbitMQ с правами только на чтение и запись конкретной очереди, выполните следующие шаги:

Доступно на сервере, где развернут Apacs.

1. Откройте командную строку Windows.
2. Перейдите в директорию исполняемых файлов для RabbitMQ:

```
cd "c:\Program Files\RabbitMQ Server\rabbitmq_server-*.*.*\sbin"
```

Вместо символа * подставьте значение версии RabbitMQ Server.

3. Добавьте пользователя в RabbitMQ:

```
rabbitmqctl add_user <login> <password>
```

Вместо <login> и <password> подставьте свои значения. Подробнее см. на [официальном сайте](#).

4. Добавьте пользователю права:

```
rabbitmqctl set_permissions -p / <login> "^apc.webapi.vl-access-2" "^apc.webapi.vl-access-2" "^apc.webapi.vl-access-2"
```

Вместо <login> подставьте своё значение. Подробнее см. на [официальном сайте](#).

Данные права дают возможность создать exchange для СКУД Арас, чтобы записывать в очередь события об изменении пользователя. Также эти права дают возможность читать из этой очереди события для дальнейшей синхронизаций пользователей для Access.

9.5. Методы взаимодействия с Арас

Начало эндпоинта для всех запросов (Таблица 38): /v1/webapi/v3.

Таблица 38. Используемые методы СКУД АРАС

Задача	Метод	Описание
Авторизоваться	POST /session/login/	Авторизация Access в СКУД. Авторизация происходит при добавлении сервиса и до выхода из системы
Выйти из системы	POST /session/logout/	Отправляется при перезапуске или удалении компонента Арас
Получить инфо о СКУД	GET /webapi/ping/	Проверка доступности СКУД раз в минуту.
Создать запрос	POST /query/	Создать запрос (получение данных сотрудника, номер карты и так далее) и получить ID запроса (query_id)
Получить результат запроса	POST /query/{query_id}/500/	Запрос на получение результата (500 - число объектов), с ID объектов (object_id).
Получить данные по ID	POST /object/id/{object_id}/	Получение данных сотрудника

Задача	Метод	Описание
Отправить карту AAM	POST /object/execCmd/{object_id} /cmdEmulateCardByNumber,	Отправить карту на AAM/AAN контроллер
Отправить карту Apollo	POST /object/execCmd/{object_id} /cmdSendCard/	Отправить карту на Apollo контроллер

9.6. Диаграммы процессов взаимодействия с Арас

9.6.1. Подключение сервиса Арас

Диаграмма процесса (Рисунок 50).

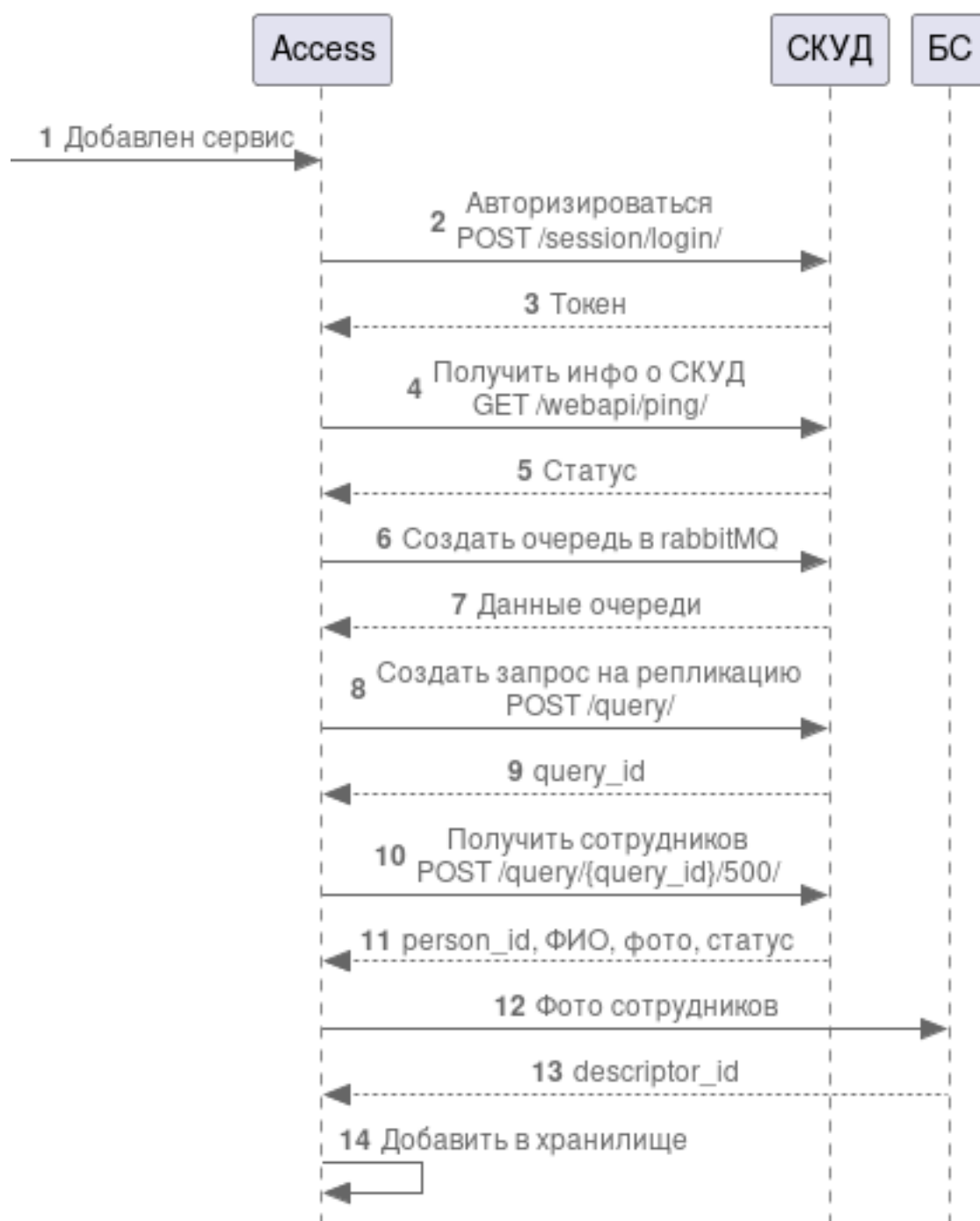


Рис. 50: Диаграмма процессов при подключении SKUD

1. Пользователь добавил в Access сервис Аракс.
2. Access отправляет запрос на авторизацию в SKUD.
3. SKUD возвращает токен для авторизации. Токен имеет время жизни, по истечению которого Access повторно выполняет авторизацию.

4. Access отправляет запрос на получение информации о СКУД.
5. СКУД возвращает информацию. Access использует только версию СКУД для проверки совместимости и информации пользователя в UI.
6. Access отправляет запрос на создание очереди в rabbitMQ для просмотра событий сотрудников.
7. СКУД возвращает ID очереди.
8. Access создает запрос на репликацию сотрудников из СКУД.
9. СКУД возвращает query_id.
10. Access отправляет запрос на получение результатов по запросу репликации.
11. СКУД возвращает person_id, ФИО, статус, фото, дата и время последнего изменения.
12. Access отправляет запрос с фото сотрудников к БС на извлечение descriptor_id (face_id).
13. БС возвращает descriptor_id.
14. Access сохраняет информацию по каждому сотруднику в локальное хранилище.

9.6.2. Обработка событий Арас при 1 факторе

Диаграмма процесса (Рисунок 51).

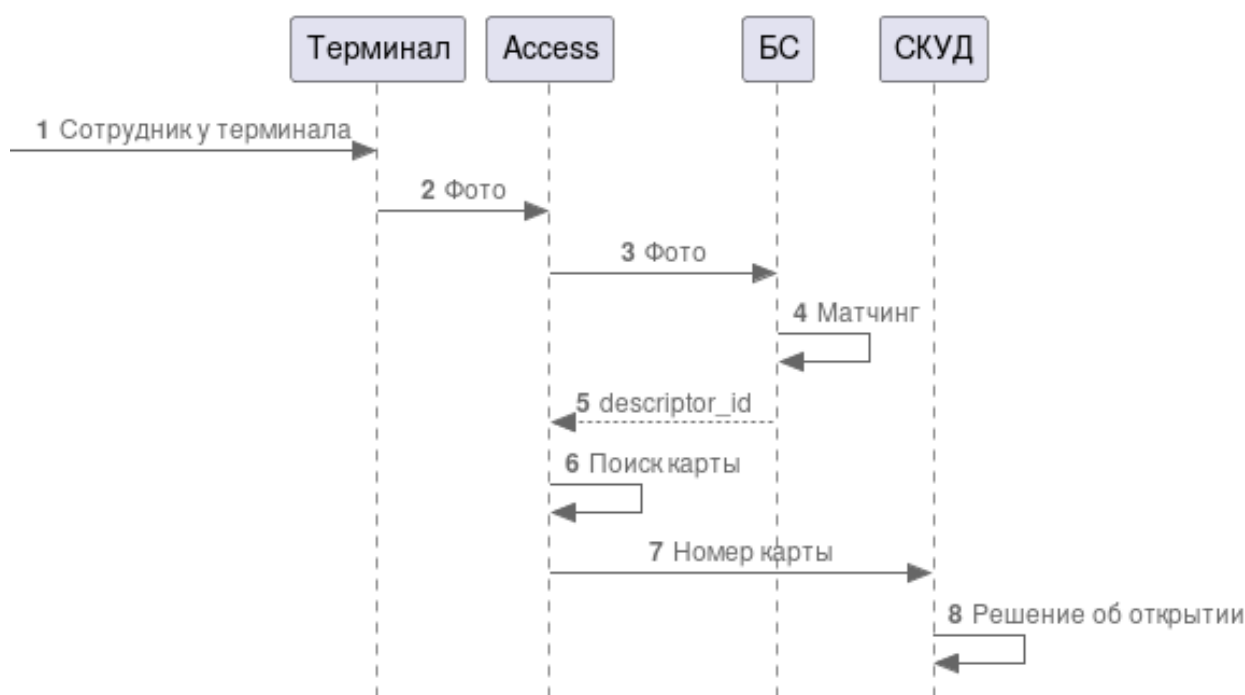


Рис. 51: Диаграмма процессов при 1 факторе

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access результат матчинга.
6. Access сравнивает номер карты лица и номер карты, полученный от сотрудника.
7. Access отправляет в СКУД номер карты.
8. СКУД принимает решение о пропуске человека.

9.6.3. Обработка событий Арас при 2 факторах

Диаграмма процесса (Рисунок 52).

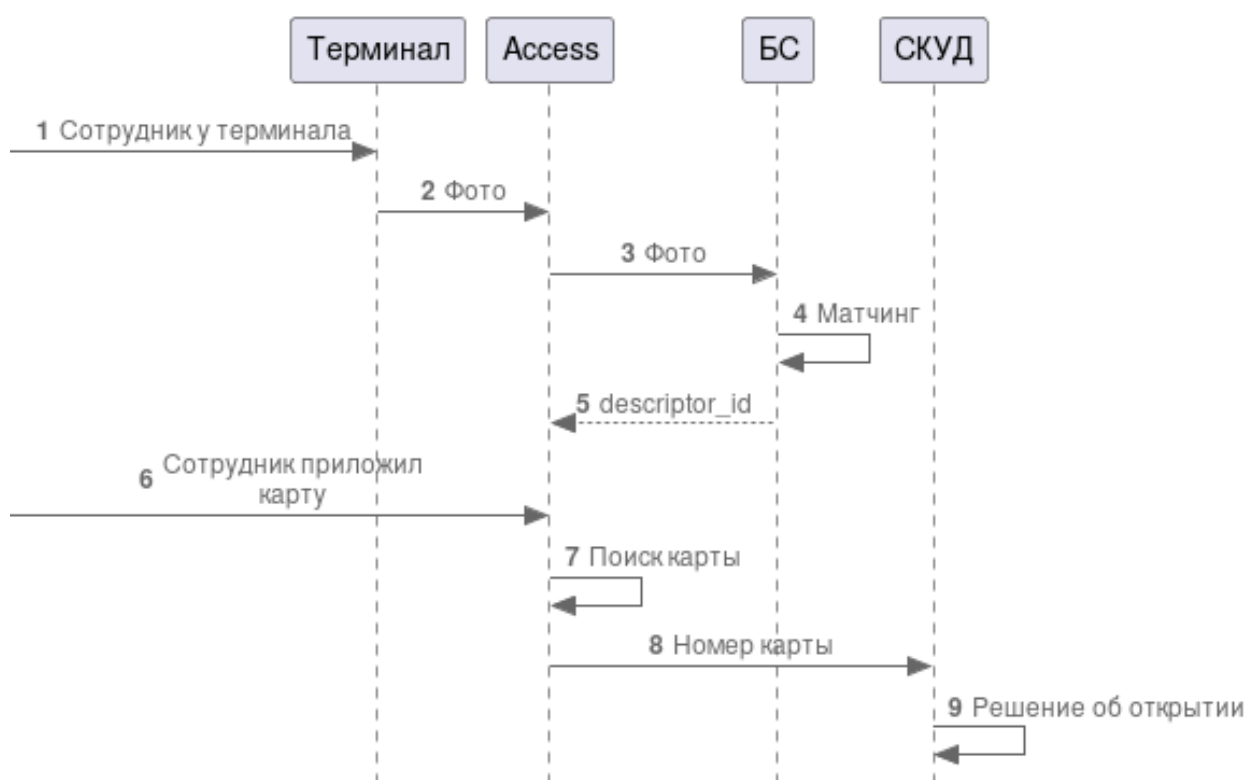


Рис. 52: Диаграмма процессов при 2 факторах

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.

4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access результат матчинга.
6. Сотрудник прикладывает карту (подпроцесс использования карты не зависит от обработки фото, но, как правило, сначала приходит фото).
7. Access сравнивает номер карты лица и номер карты, полученный от сотрудника.
8. Access отправляет в СКУД номер карты.
9. СКУД принимает решение о пропуске человека.

9.7. FAQ Apacs

1. Что такое Facility_code (код организации)?

Номера карт в APACS имеют смещение + номер карты. При считывании карты, Access получает «код организации + номер карты».

В APACS имеется таблица соответствий смещений и их кодов организаций. При помощи таблицы соответствий можно преобразовать номер карты в «код организации + номер карты в смещении + номер карты», чтобы сопоставить с данными карт сотрудников в APACS.

2. Человек не реплицировался, что делать?

Если при репликации в логе появляется ошибка репликации сотрудника или его нет в списке LP5 (можно увидеть через LUNA CLEMENTINE), хотя есть в СКУД, то нужно в СКУД перейти в данные сотрудника > Доступы, отключить Активность и сохранить изменения. Далее включить Активность и сохранить изменения.

10. СКУД Бастион

СКУД синхронизирует сотрудников с локальным хранилищем персон и слушает события, на основе которых решает открывать или не открывать турникет. Данные события генерируются в Access пайплайном `CreateBastionEvent`.

- Поддерживаемая версия СКУД Бастион: 2.1.11.2337, 2.1.13.2347, 2025.1, 0.23.3-17064.

В интеграции с **Бастион 2** необходимо использовать пайплайны, вызывающие отображение текста на терминале (рекомендуется `SendToDevice`, либо `LunaEventListener` при работе с Luna).

В интеграции с **Бастион 3** отдельные пайплайны для отображения текста не требуются - эту функцию выполняет `CreateBastionEvent`.

При подключении устройств необходимо указывать имена точек доступа, автоматически сгенерированные сервисом на основе точек прохода в СКУД. Указываются в Info сервиса. Они генерируются в формате «имя точки доступа - идентификатор». Например: «турникет_выход - 907efa78-cb2f-4f46-b374-785c7f9901a5».

Полученные имена точек доступа необходимо указывать в:

- При использовании внутренних устройств Access (HikvisionTerminal, Panda ...), указать в поле «name»
- При использовании LunaStream, указать в поле «source»

10.1. Поддерживаемые варианты интеграции СКУД Бастион

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 39) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 39. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Bastion	Beward	CreateBastionEvent + MatchByPhoto + SendToDevice
	BioSmart	CreateBastionEvent + MatchByPhoto + SendToDevice
	Dahua	CreateBastionEvent + MatchByPhoto
	Dahua Thermo	CreateBastionEvent + MatchByPhoto
	Fortuna315	CreateBastionEvent + MatchByPhoto
	HikvisionCamera	CreateBastionEvent + MatchByPhoto
	HikvisionCamera Thermo	CreateBastionEvent + MatchByPhoto
	HikvisionTerminal Thermo	CreateBastionEvent + MatchByPhoto + SendToDevice
	LunaFast4A1	CreateBastionEvent + MatchByPhoto + SendToDevice
	Panda	CreateBastionEvent + MatchByPhoto
	UniUbi	CreateBastionEvent + MatchByPhoto + SendToDevice
	VKVision02	CreateBastionEvent + MatchByPhoto + SendToDevice
	R20Face	CreateBastionEvent + MatchByPhoto + SendToDevice

В каждой интеграции с КБС (Таблица 40) используется сервис КБС.

Таблица 40. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsMts + Bastion	Beward	CreateBastionEvent + MatchByPhoto + SendToDevice
	Dahua	CreateBastionEvent + MatchByPhoto
	HikvisionCamera	CreateBastionEvent + MatchByPhoto
	LunaFast4A1	CreateBastionEvent + MatchByPhoto + SendToDevice
	UniUbi	CreateBastionEvent + MatchByPhoto + SendToDevice

10.2. Стандартная интеграция с использованием СКУД Бастион

Программные интеграции ПО СКУД Bastion с биометрическими системами реализованы для обеспечения прохода распознанных лиц через турникет/дверь с магнитным замком.

Схема интеграции Bastion для прохода распознанных лиц через турникет/дверь с магнитным замком. При интеграции с Bastion используются стандартные компоненты Access (Рисунок 53) и

(Таблица 41).

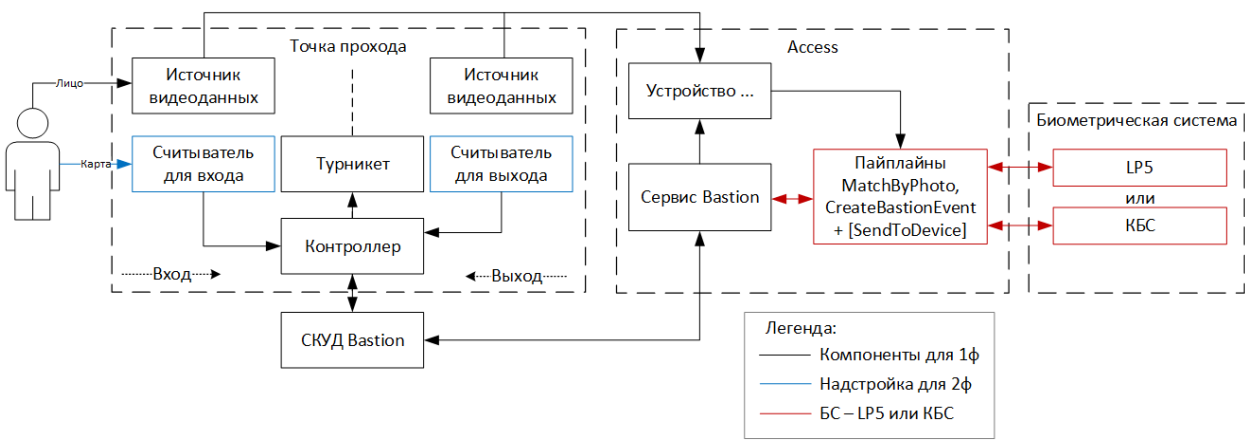


Рис. 53: Схема компонентов при интеграции с Bastion

Таблица 41. Описание интеграции

Компонент	Описание
1ф	
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключено более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Контроллер	Плата управления точкой прохода.
Турникет	Преграждающее устройство для разграничения доступов
СКУД Bastion	Центральное ПО для работы с Bastion. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Сервис Bastion	Компонент Access для обработки информации от СКУД.
Надстройка для 2ф	
Считыватель	Устройство для приема данных карты доступа.

Компонент	Описание
Работа с LP5 и КБС	
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС
Пайплайн CreateBastionEvent	Компонент Access для прослушивания очередей событий в Luna и генерации событий в Access
Пайплайн SendToDevice	Компонент Access для отправки сигнала на открытие реле в устройство и вывода текста на экран. Необходим только при интеграции СКУД Bastion 2

10.3. Настройка ПО СКУД Бастион 3

1. Откройте ПО СКУД Бастион-3 — Панель управления.
2. Перейдите в раздел Драйверы → Драйвер Face → Конфигуратор драйвера «Face» → Общие настройки (Рисунок 54).

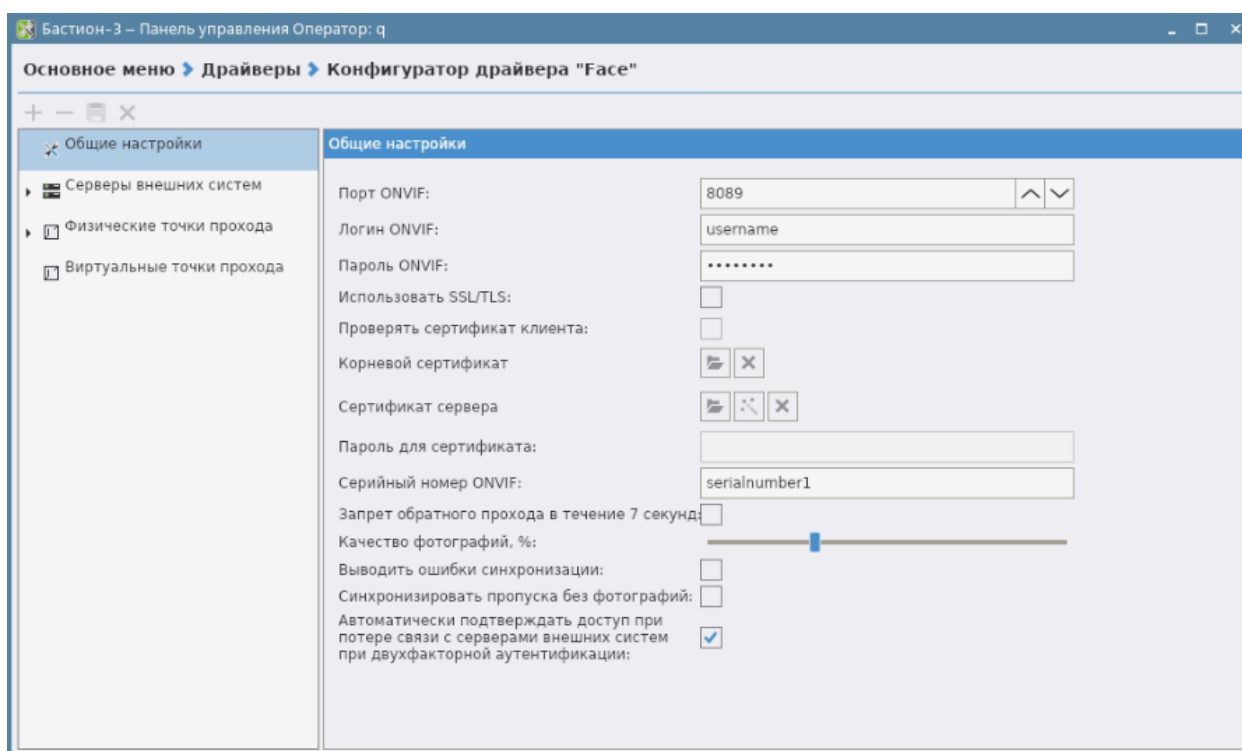


Рис. 54: Конфигурация драйвера Face

3. Установите порт, логин и пароль ONVIF.

4. Перейдите в раздел «Серверы внешних систем» и добавьте новый сервер, нажав «+».
5. В настройке нового сервера введите адрес Access в формате «host:port» в поля адреса «службы управления профилями персон» и «службы событий», установите логин и пароль обеих служб (Рисунок 55).

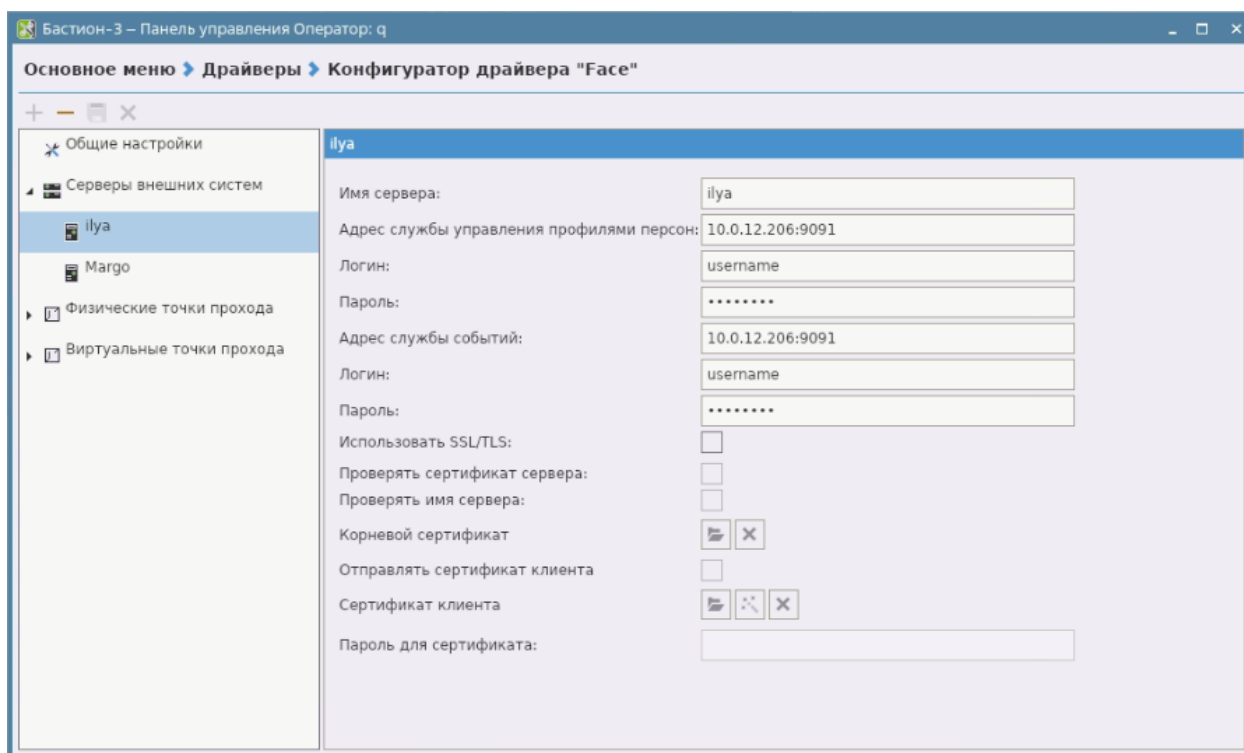


Рис. 55: Конфигурация сервера внешних систем

6. Перейдите в раздел «Физические точки прохода» и добавьте новую точку прохода, нажав «+».
7. Выберите точку прохода Дверь N R{N}.
8. В поле «Описание» введите название камеры, работающей с этой точкой прохода.

Описание точки прохода должно совпадать с именем устройства в Access.

9. Выберите режим работы «Доступ в режиме идентификации» (Рисунок 56).

При изменении режима у точки прохода в СКУД необходимо перезапустить сервис Bastion в Access и заново инициировать репликацию.

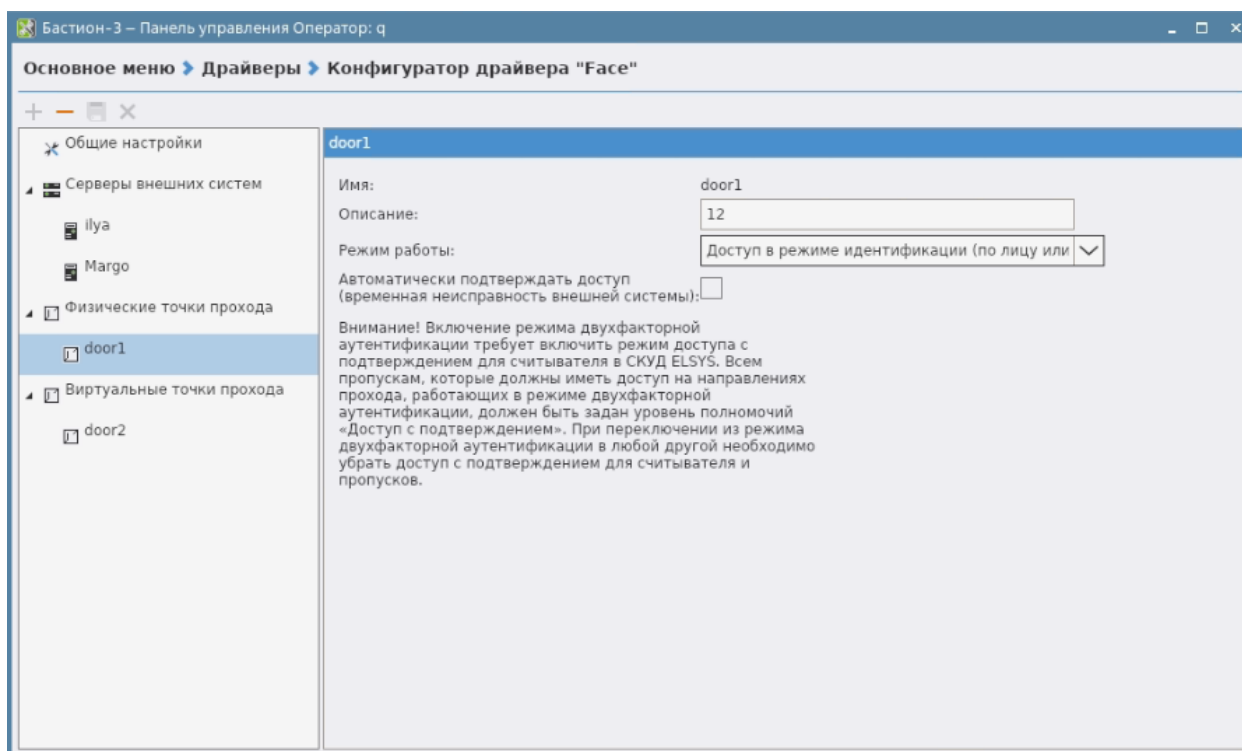


Рис. 56: Конфигурация точки прохода

10. Сохраните изменения, нажав иконку дискеты.
11. Настройте управление пропусками: Бастион 3 → Бюро пропусков.
12. Создайте новую заявку на пропуск. Перейдите в раздел Заявки → Нажмите «+» на панели инструментов (Рисунок 57).

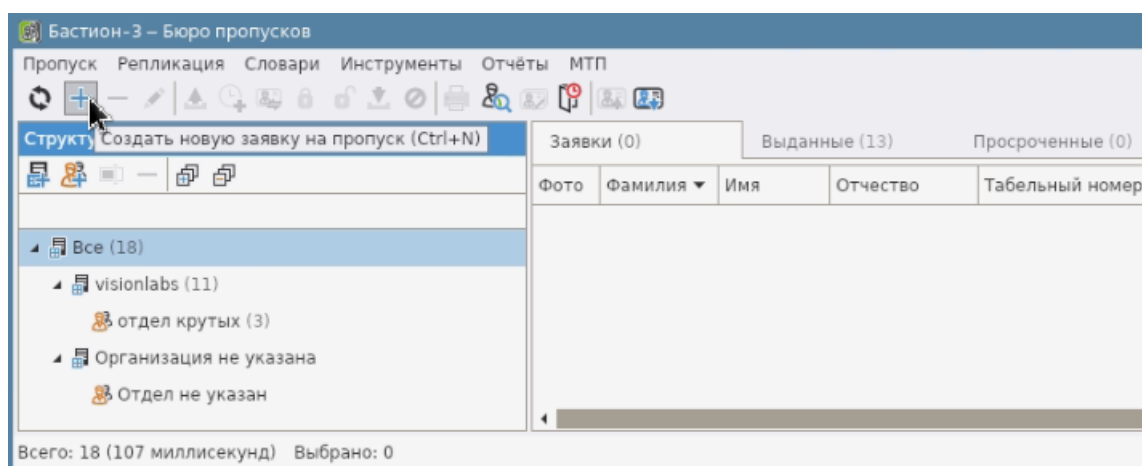


Рис. 57: Создание заявки на пропуск

13. Заполните необходимые поля и нажмите Ок (Рисунок 58).

Свойства пропуска

Персона | Пропуск | Уровень доступа | Профили | Реквизиты | Материальные пропуски ▾

Фамилия: Цискаридзе

Имя: Николай

Отчество: Николаевич

Организация: Все

Место работы: Все

Табельный номер:

Должность: <Не указано>

Комментарий:

Персона создана: 24.01.2025 11:31:19

OK Отмена

Рис. 58: Заполнение заявки на пропуск

14. Выдача пропусков. Перейдите в Заявки → Выберите целевую заявку → Нажмите «Выдать пропуск» на панели инструментов (Рисунок 59).

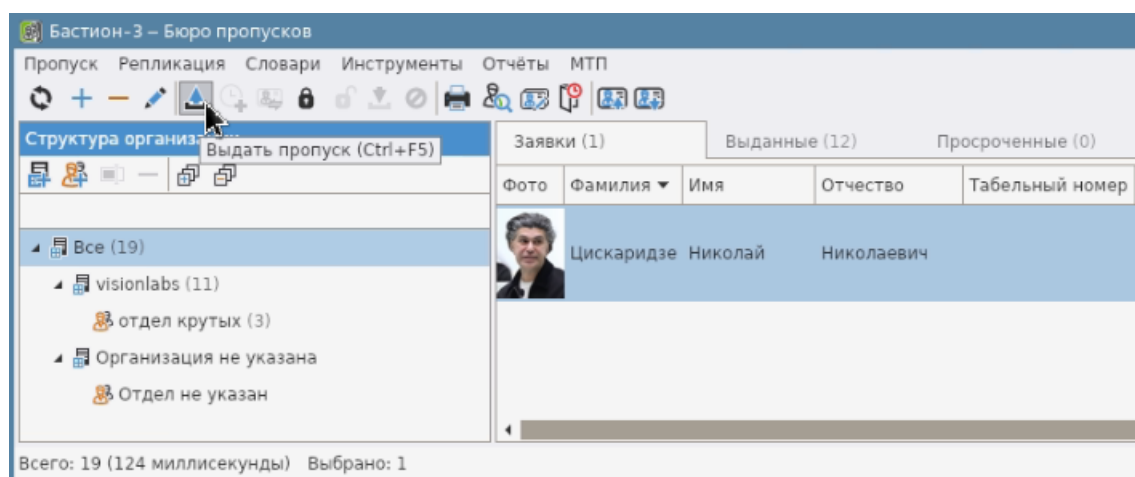


Рис. 59: Выдача пропусков

15. Отметьте пункт «Выдать новую карту доступа» → Сгенерировать случайный код → Выдать (Рисунок 60).

Рис. 60: Выдача пропусков

Выданные пропуска отображаются на вкладке «Выданные».

16. Редактирование пропуска. Перейдите на вкладку Выданные → Необходимый пропуск → Свойства пропуска.

10.4. Настройка двухфакторной точки доступа Бастион

1. Откройте ПО СКУД Бастион-3 — Панель управления.
2. Перейдите в раздел Драйверы → Драйвер Face → Конфигуратор драйвера «Face» → Физические точки прохода и выберите/добавьте точку прохода.
3. В поле «Описание» введите название камеры, работающей с этой точкой прохода.

Описание точки прохода должно совпадать с именем устройства в Access.

4. Выберите режим работы «Доступ в режиме двухфакторной аутентификации».

При изменении режима у точки прохода в СКУД необходимо перезапустить сервис Bastion в Access.

5. Сохраните изменения, нажав иконку дискеты (Рисунок 61).

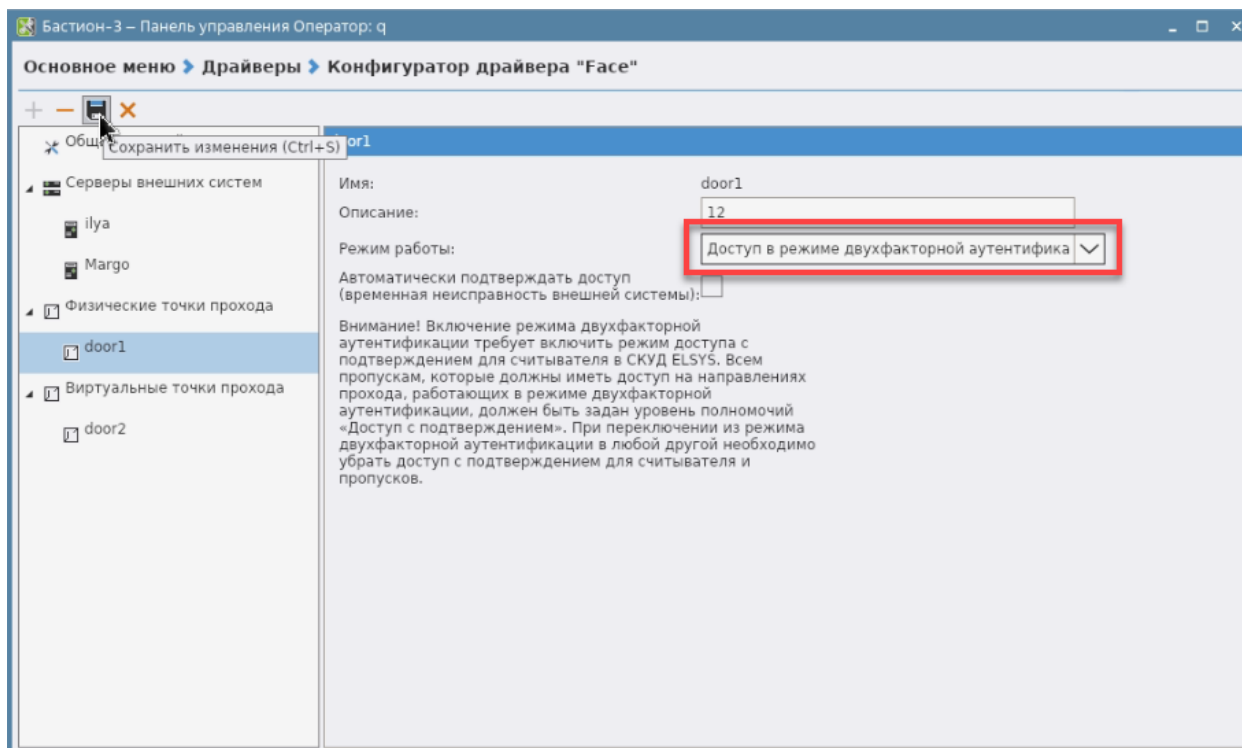


Рис. 61: Конфигурация точки прохода для 2fa

6. Откройте Панель управления и перейдите в раздел Драйверы → Профили настроек персонала (Рисунок 62).

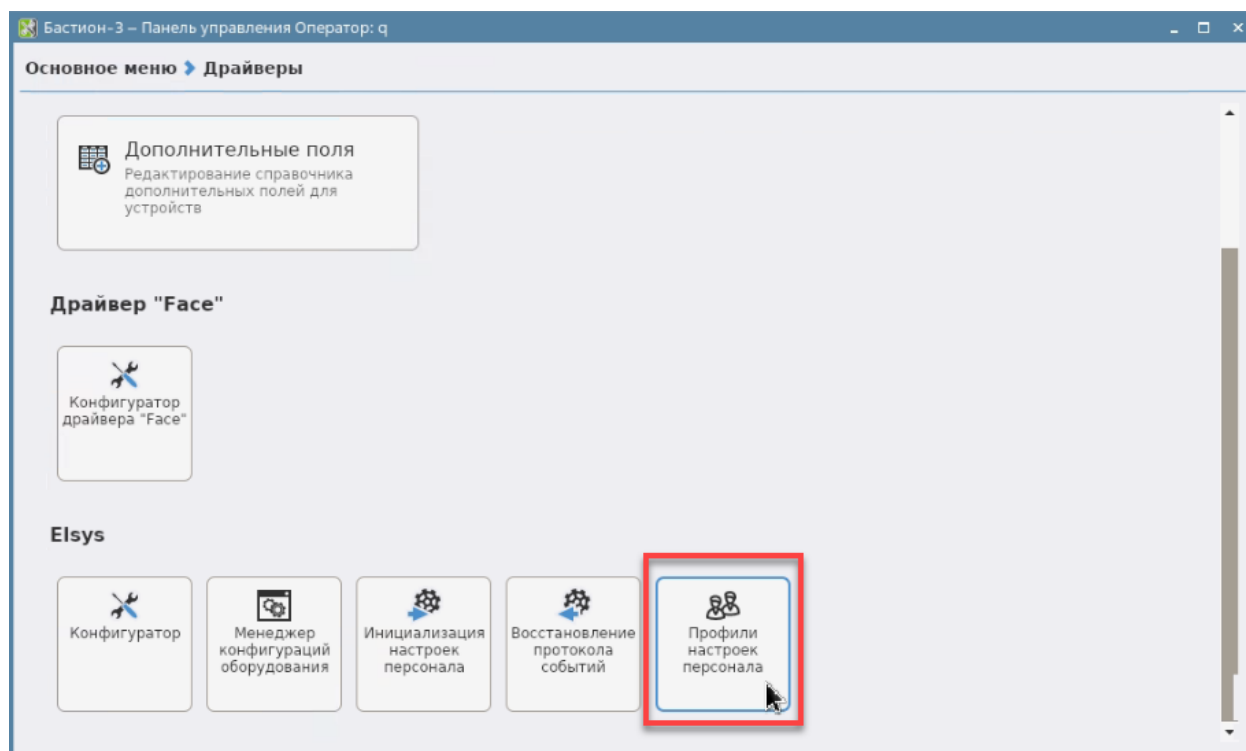


Рис. 62: Профили настроек персонала

7. Выберите профиль → Полномочия и включите функцию «Доступ с подтверждением».
8. Сохраните изменения, нажав иконку дискеты (Рисунок 63).

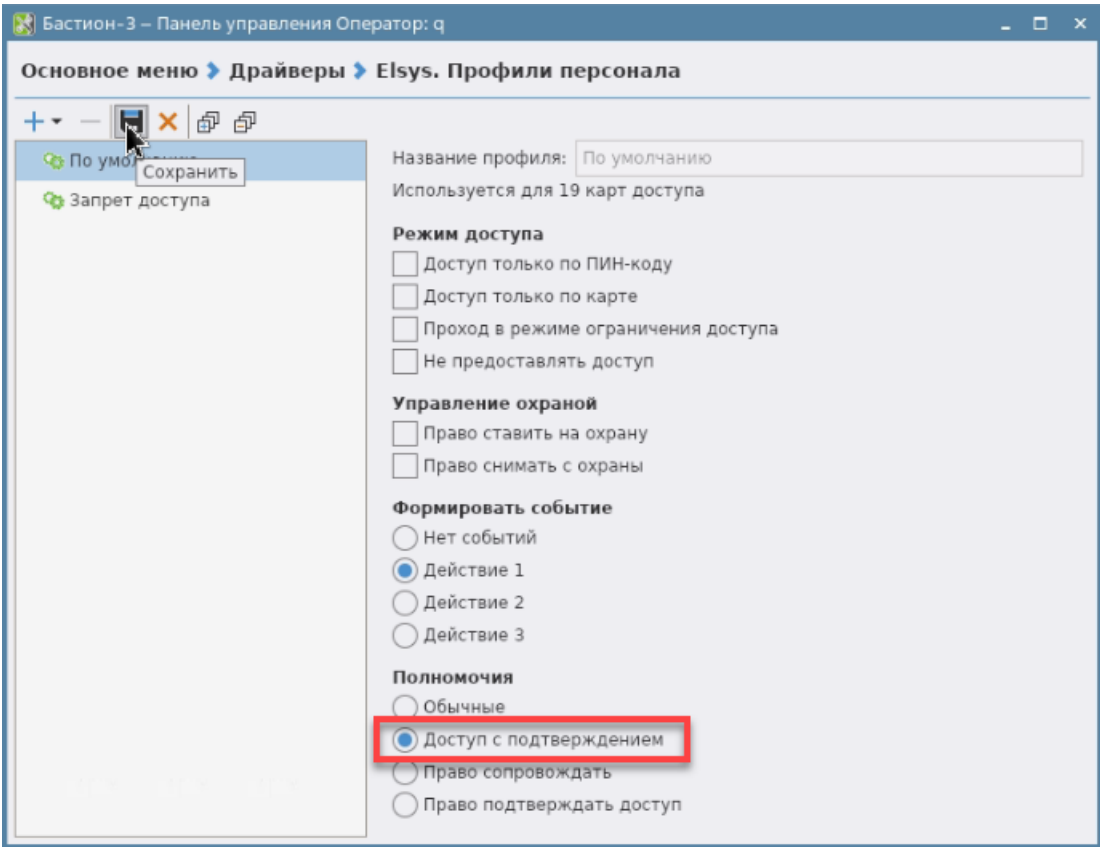


Рис. 63: Включение доступа с подтверждением

9. В UI Access перейдите на вкладку «Сервисы» и нажмите на кнопку рестарта компонента Bastion. В info компонента Bastion проверьте настройку «enabled_2fa» точки доступа, которую редактировали на предыдущем шаге.

10.5. Методы взаимодействия с Бастион

Access выступает в роли сервера и клиента (Таблица 42).

Отправка методов ONVIF в Access происходит на эндпоинт POST /vl-access/webhook/service/onvif/{component id}.

Таблица 42. Используемые методы СКУД Бастион

Задача	Метод	Описание
Получить точки доступа	POST /onvif/accesscontrol	Запрос к СКУД. Получение ID точек доступа (контроллеров) для ручного сопоставления камер/терминалов и точек доступа

Задача	Метод	Описание
Получить список сервисов ONVIF	POST /onvif/device_service	Получение списка component_id ONVIF сервисов Access для подключения
Создание пользователя	CreateCredential	Метод ONVIF
Обновление пользователя	ModifyCredential	Метод ONVIF
Удаление пользователя	DeleteCredential	Метод ONVIF
Создание подписки	CreatePullPoint Subscription	Метод ONVIF. Подписка на события.
Получить события детекции	PullMessages	Получения события детекции сотрудника. Запрос отправляется каждые 10 секунд и ожидает 10 секунд до появления кадра.

10.6. Диаграммы процессов взаимодействия с Бастион

10.6.1. Подключение сервиса Бастион и репликация сотрудников

Диаграмма процесса (Рисунок 64).

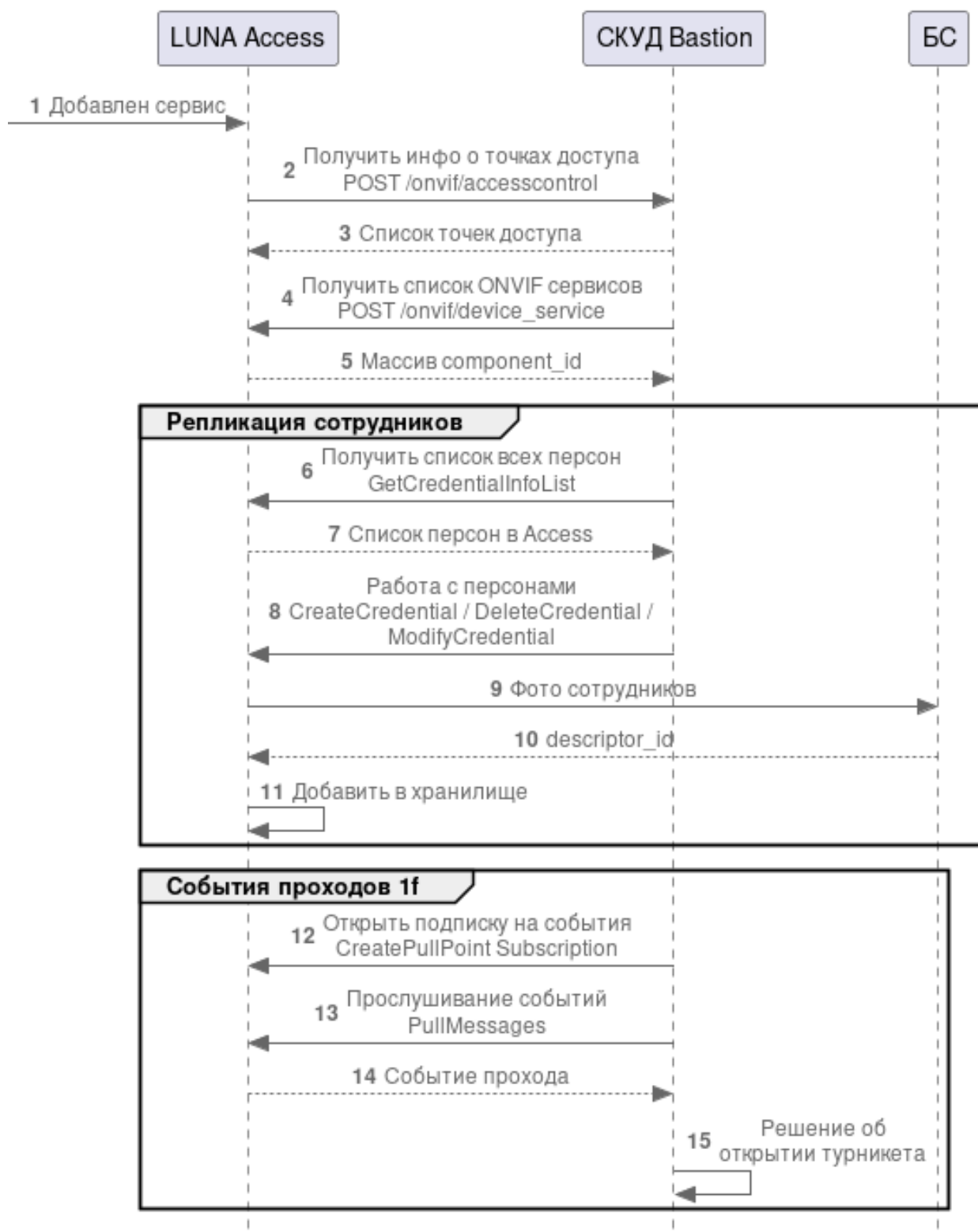


Рис. 64: Диаграмма процессов при подключения СКУД

Подключение сервиса

1. Пользователь добавил в Access сервис Bastion.
2. Access отправляет запрос в СКУД для получения точек прохода. Полученные точки прохода отображаются в поле info свойств сервиса. Запрос используется в качестве проверки доступности СКУД.
3. СКУД возвращает точки доступа.
4. СКУД отправляет запрос в Access для получения списка сервисов Access поддерживающих протокол ONVIF.
5. Access возвращает component_id ONVIF сервисов.

Репликация сотрудников

6. СКУД отправляет запрос в Access для получения списка всех персон.
7. Access возвращает список персон.
8. СКУД отправляет в Access запрос POST /vl-access/webhook/service/onvif/{component_id} CreateCredential (или DeleteCredential ModifyCredential) для работы с сотрудниками в хранилище Access.
9. Access отправляет запрос с фото сотрудников к БС на извлечение descriptor_id (face_id).
10. БС возвращает descriptor_id.
11. Access сохраняет информацию по каждому сотруднику в локальное хранилище.

События при 1 факторе

12. СКУД отправляет запрос в Access на открытие подписки на получение событий (лучшие кадры человека у терминала).
13. СКУД раз в 10 секунд отправляет запрос POST /vl-access/webhook/service/onvif/{component_id} PullMessages на ожидание события прохода.
14. Access возвращает событие прохода в СКУД.
15. СКУД принимает решение об открытии терминала.

10.6.2. Обработка событий Бастион при 2 факторах

Диаграмма процесса (Рисунок 65).

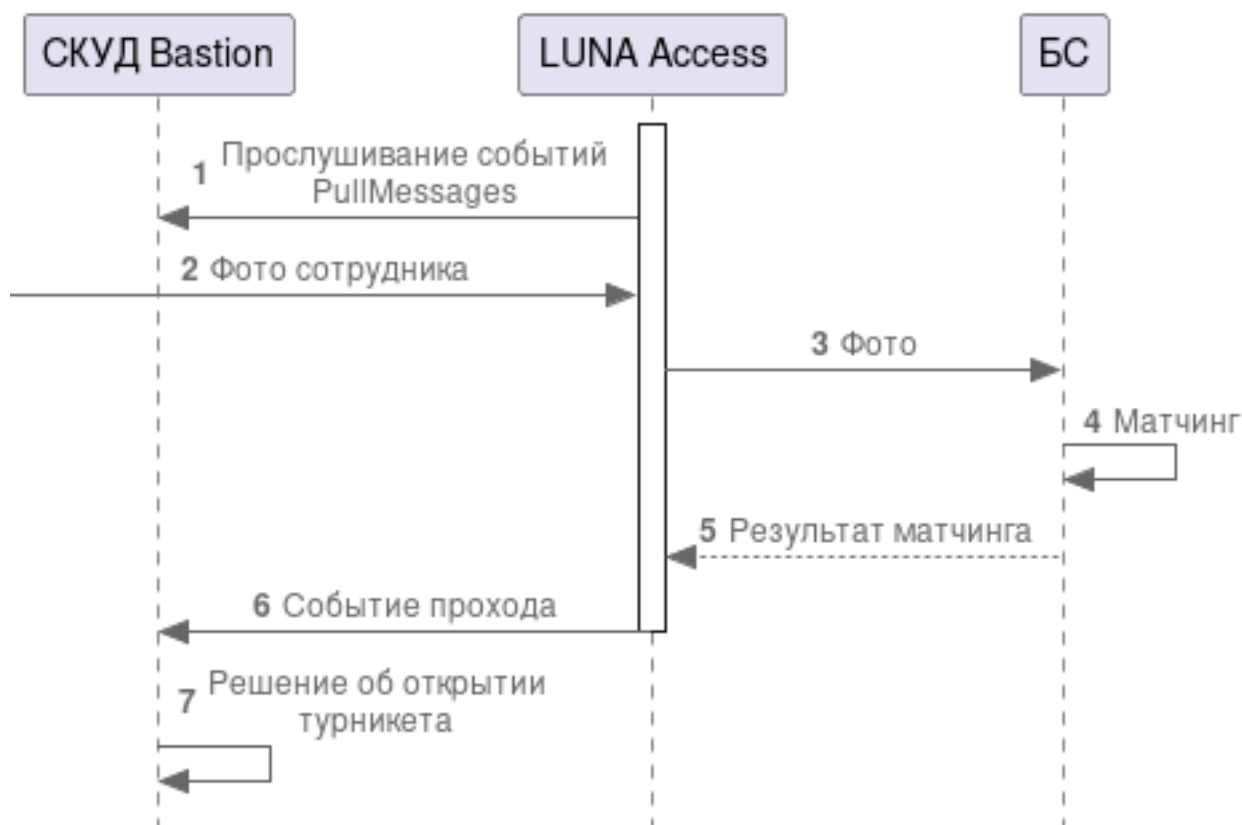


Рис. 65: Диаграмма процессов при 2 факторах

1. Access раз в 10 секунд отправляет запрос PullMessages в SKUD на ожидание события прохода.
2. В Access поступает лучший кадр сотрудника у терминала.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. BC производит сравнение фотографий с терминала и сохраненной в базе.
5. BC возвращает в Access решение о предоставлении доступа.
6. Access возвращает событие прохода в SKUD.
7. SKUD принимает решение об открытии терминала.

11. СКУД Болид

Программно-аппаратная интеграция, необходимая для связи LP5/КБС и ПО СКУД Болид для обеспечения управления связанным устройством (приборы серии С-2000 или иные совместимые с ПО Болид устройства).

Для работы должен быть установлен и запущен лицензионный модуль интеграции Орион ПРО. Версия Болид — 1.20.3. Версия модуля интеграции Орион Про — 1.4.

Информационное взаимодействие обеспечивается через пакет программного обеспечения автоматизированное рабочее место (АРМ) «Орион Про».

Модуль интеграции Орион ПРО лицензируется отдельно.

Модуль интеграции является SOAP web-сервисом, доступ к которому осуществляется по протоколам HTTP/HTTPS, описание веб-сервиса соответствует спецификации WSDL версии 2.0.

СКУД поддерживает работу на ОС Windows 7/8/8.1/10 (32 bit или 64 bit).

11.1. Поддерживаемые варианты интеграции СКУД Болид

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 43) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 43. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
1ф		
Bolid + GateController / PusrController	Beward	MatchByPhoto + SendToDevice + SendToController
	BioSmart	MatchByPhoto + SendToDevice + SendToController

Сервис	Устройство	Пайплайн
	Dahua	MatchByPhoto + SendToController
	Dahua Thermo	MatchByPhoto + SendToController
	Fortuna315	MatchByPhoto + SendToController
	HikvisionCamera	MatchByPhoto + SendToController
	HikvisionCamera Thermo	MatchByPhoto + SendToController
	HikvisionTerminal Thermo	MatchByPhoto + SendToDevice + SendToController
	LunaFast4A1	MatchByPhoto + Custom2FA
	Panda	MatchByPhoto + SendToController
	UniUbi	MatchByPhoto + SendToDevice + SendToController
	VKVision02	LunaStreams + MatchByPhoto + SendToDevice + SendToController
	R20Face	MatchByPhoto + SendToDevice + SendCardToR20Face
2ф		
Bolid + GateController / PusrController	LunaFast4A1	Custom2FA + MatchByPhoto + SendToDevice

В каждой интеграции с КБС (Таблица 44) используется сервис КБС.

Таблица 44. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsMts + Bolid + GateController / PusrController	Beward	MatchByPhoto + SendToController + SendToDevice
	Dahua	MatchByPhoto + SendToController
	HikvisionCamera	MatchByPhoto + SendToController
	LunaFast4A1	MatchByPhoto + SendToController + SendToDevice

Сервис	Устройство	Пайплайн
	UniUbi	MatchByPhoto + SendToController + SendToDevice
	R20Face	MatchByPhoto + SendCardToR20Face + SendToDevice

11.2. Стандартная интеграция с использованием Болид

При интеграции с Болид используются стандартные компоненты Access (Рисунок 66) и (Таблица 45).

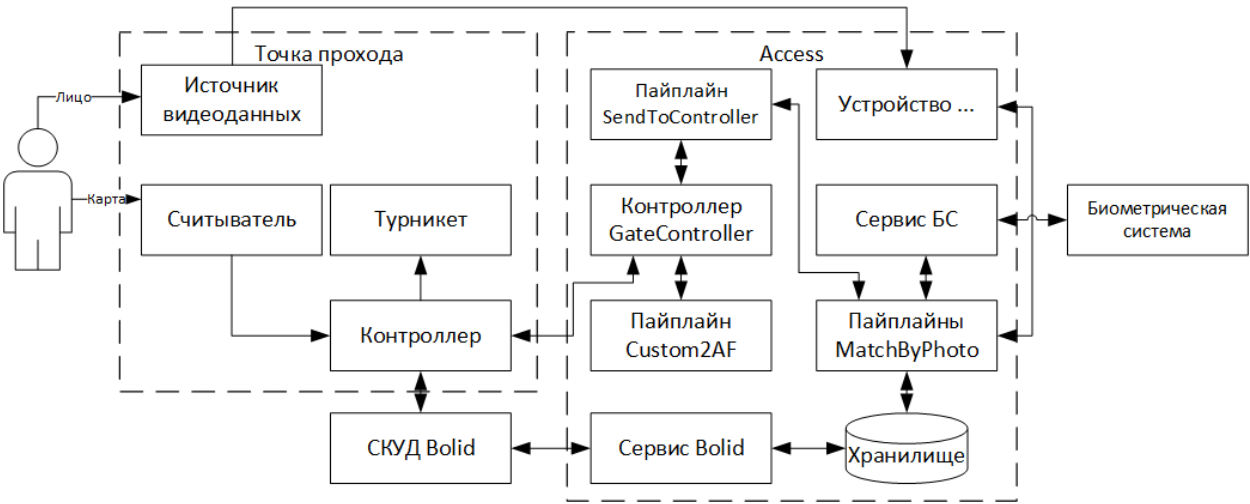


Рис. 66: Схема компонентов при интеграции с Bolid

При использовании 1ф интеграции (без карты) компоненты передачи номера карты в Access не требуется.

Таблица 45. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.

Компонент	Описание
Считыватель	Устройство для приема данных карты доступа.
Контроллер	Плата управления точкой прохода.
Турникет	Преграждающее устройство для разграничения доступов
СКУД Bolid	Центральное ПО для работы с Bolid. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Сервис Bolid	Компонент Access для обмена данными с СКУД
Сервис БС	Компонент Access для взаимодействия с БС: для LP5 это Luna , для КБС - соответствующий сервис КБС.
Контроллер GateController	Компонент Access для взаимодействия с контроллером СКУД.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Пайплайн Custom2FA	Компонент Access реализующий логику при работе в режиме 2ф.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с КБС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Пайплайн SendToController	Компонент Access для взаимодействия с КБС

11.3. Настройка СКУД Болид

11.3.1. Подготовительные действия с ПО «Орион Про»

Для запуска и настройки Bolid необходимо выполнить подготовительные действия с ПО «Орион Про»:

1. Запустите приложение Центральный сервер Орион Про.
2. Запустите приложение Оболочка системы (Orion Shell).
3. На панели Orion Shell необходимо запустить модуль АБД (Рисунок 67):

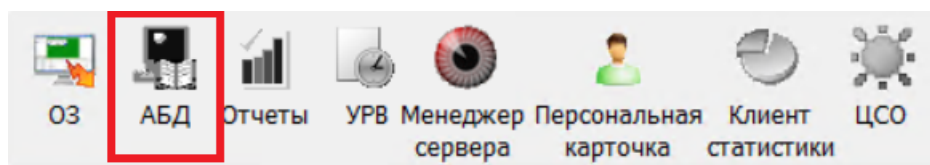


Рис. 67: Запуск АБД на панели Orion Shell

4. Запустите Модуль интеграции Орион Про.
5. Запустите на панели Orion Shell Оперативные задачи (ОЗ), если не запустились автоматически.

11.3.2. Добавление сотрудника в Орион Про

1. Добавить нового сотрудника. Заполнить необходимые поля (Рисунок 68) согласно правилам создания сотрудников на объекте:
2. Перейдите в раздел Сотрудники
3. Нажмите кнопку «добавить»
4. Заполните необходимые поля сотрудника

Выберите статус «Администратор», или другой отдел с сотрудниками, у которых есть полный доступ к системе.

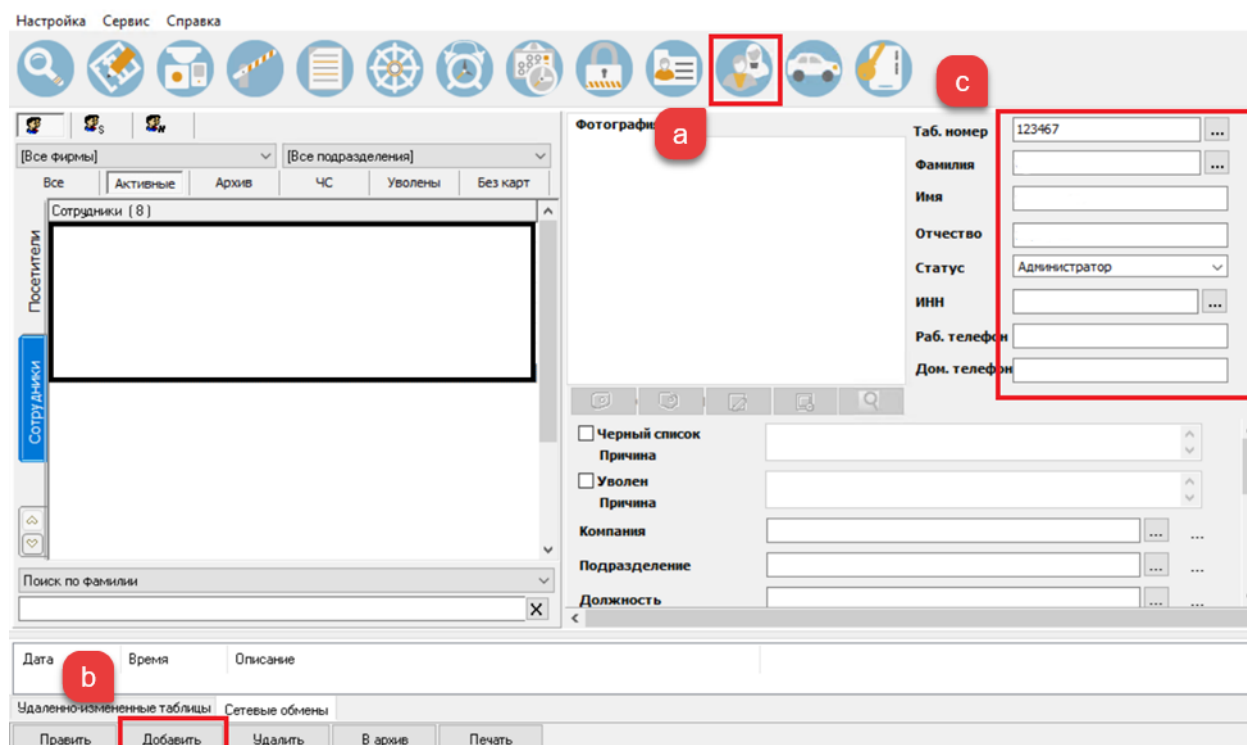


Рис. 68: Добавление нового сотрудника

5. Добавить новому пользователю уровень доступа «Максимум» и задать пароль (Рисунок 69).
6. Перейдите в раздел Доступ;
7. Нажмите Добавить;
8. Выберите нужного сотрудника, введите пароль
9. Выберите уровень доступа Максимум

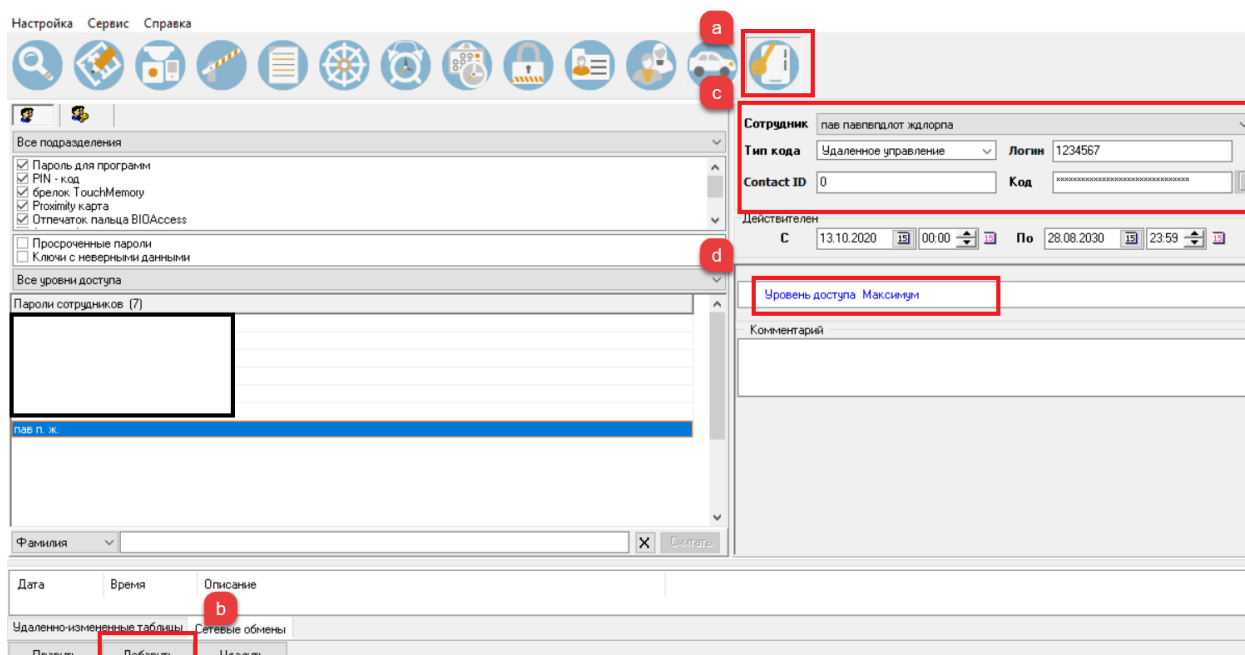


Рис. 69: Задание уровня доступа сотруднику

11.3.3. Добавление устройств в Орион Про

1. Добавить новый раздел (Рисунок 70):
2. выбрать вкладку «Структура системы»;
3. выбрать «разделы»;
4. выбрать все «Разделы»;
5. добавить новый раздел со стандартными параметрами и назвать его.

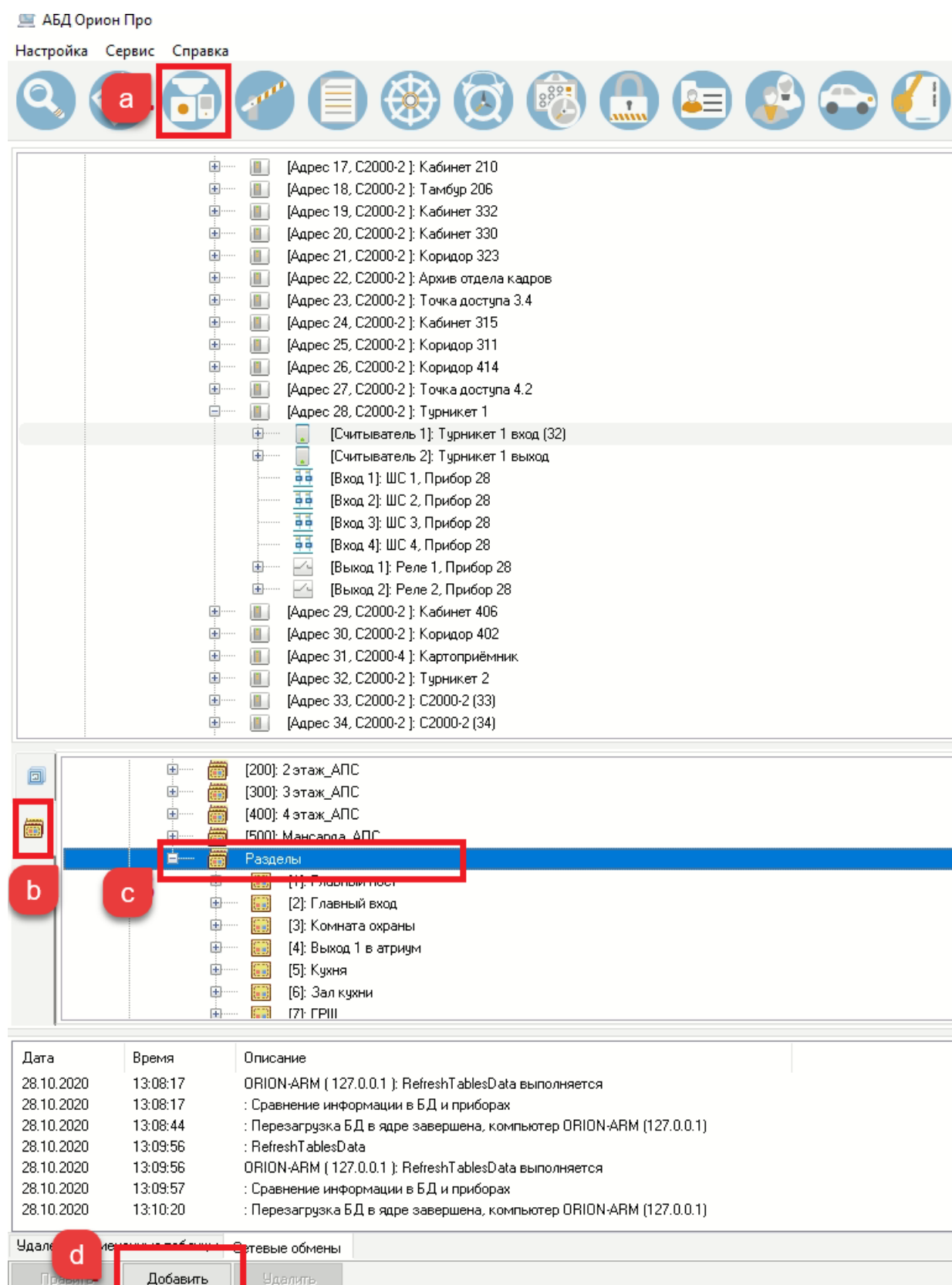


Рис. 70: Задание уровня доступа сотруднику

6. Привязать устройства к вновь созданному разделу (Рисунок 71):
7. Выберите раздел.
8. Нажмите кнопку «Добавить».

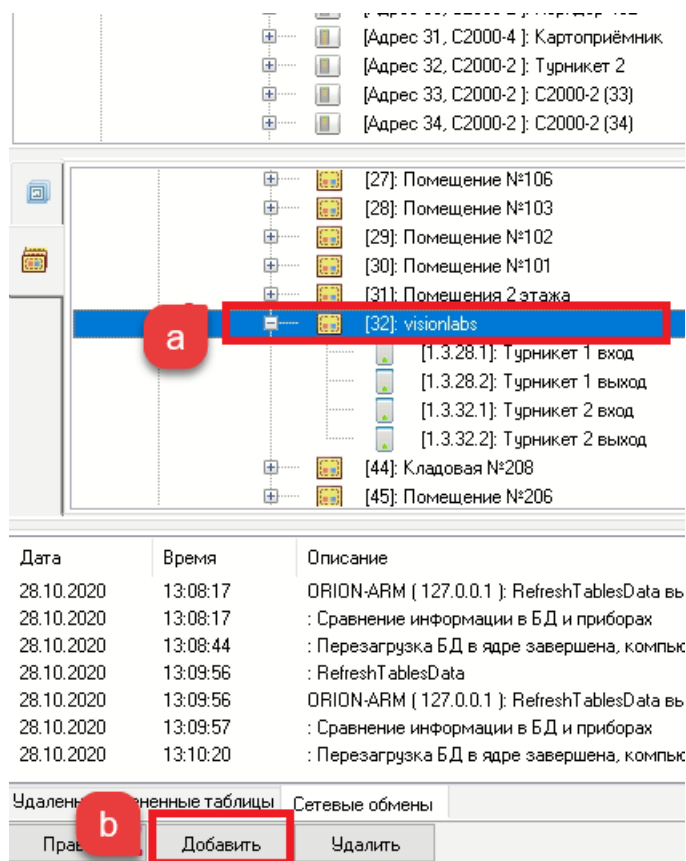


Рис. 71: Привязка устройств к разделу

9. Перейдите к списку устройств и выберите необходимые (Рисунок 72):
10. выделить его и нажмите кнопку [>>] для переноса в активное поле;
11. Подтвердите изменения нажав [OK];
12. Нажмите кнопку «Сохранить».

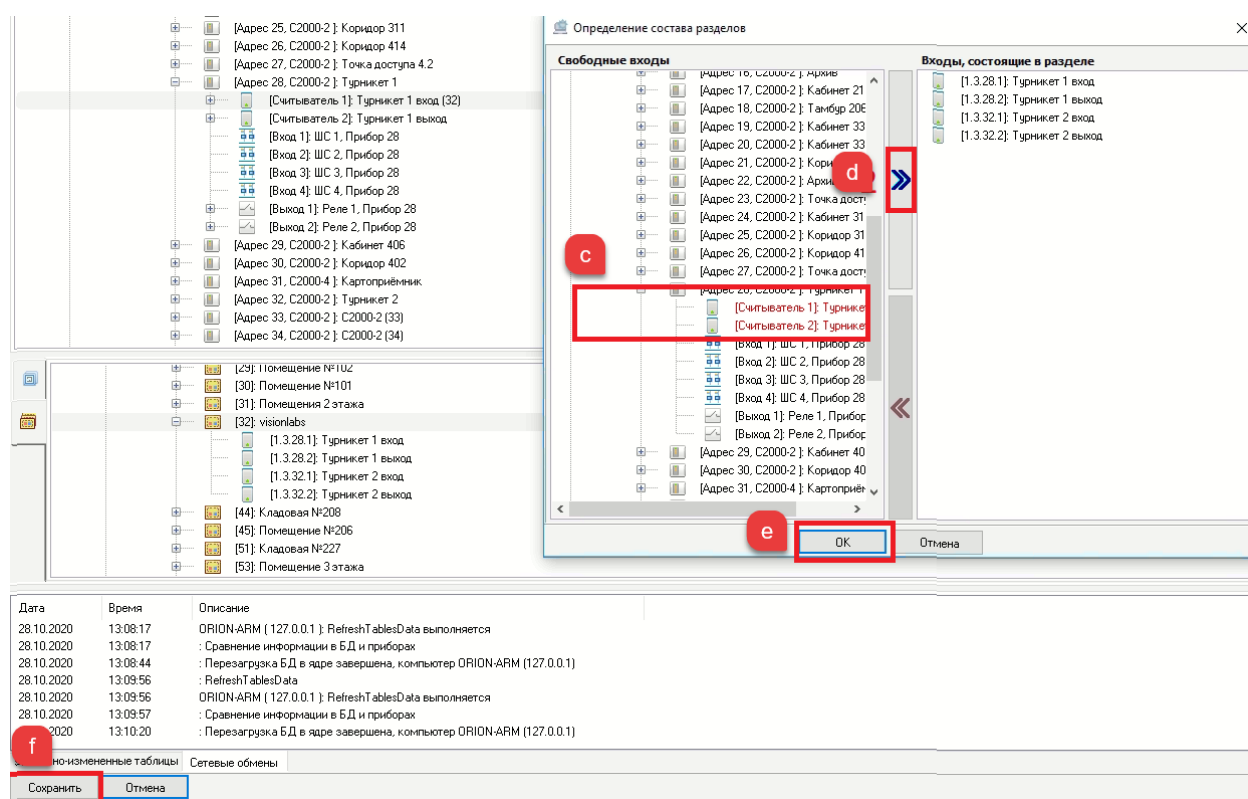


Рис. 72: Привязка устройств к разделу

- Отредактировать файл orion.ini в папке с установленным приложением Орион Про (расположен по умолчанию: C:\BOLID\ARM_ORION_PRO1_20_3), добавив в него параметры (при их отсутствии):

```
[Checkerdb]
Remarks=1
timechecker=5
Logon=1
RemoteCmd=1
CmdOn=1
[ChangeDB]
on=1
```

- Перезапустить все приложения Орион Про.

11.3.4. Настройка приложения «МОДУЛЬ ИНТЕГРАЦИИ ОРИОН ПРО»

Для настройки приложения «МОДУЛЬ ИНТЕГРАЦИИ ОРИОН ПРО» необходимо выполнить следующие действия:

1. Скачать официальный дистрибутив приложения «модуль интеграции Орион Про» по ссылке: https://bolid.ru/production/orion/po-orion/po-integration/mod_integr_orion_pro.html.
2. Запустить установку. После окончания установки запустить модуль, проверить настройки подключения к БД, если все верно, запустить модуль. Если все работает правильно необходимо закрыть модуль.
3. Установить модуль для запуска как службу, для этого необходимо выполнить в терминале команду от имени администратора в папке с установленным модулем (расположен по умолчанию: C:\BOLID\IntegrServ):

```
IntegrServ.exe /INSTALL
```

4. В панели управление системой необходимо найти установленную службу и запустить ее, нажав правую кнопку мыши и выбрав пункт «Запустить» (Рисунок 73).

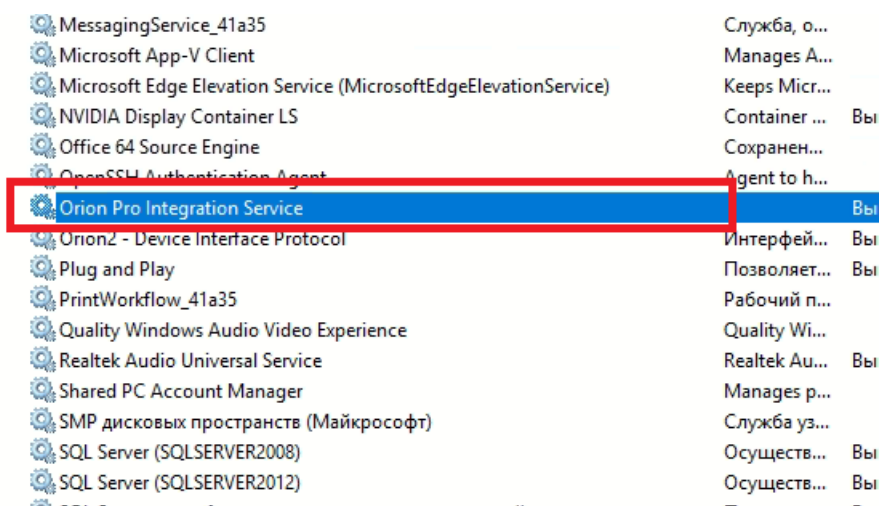


Рис. 73: Панель управления системой

11.4. Методы взаимодействия с Болид

Для обмена данными с СКУД используется API (Таблица 46).

Таблица 46. Используемые методы СКУД Болид

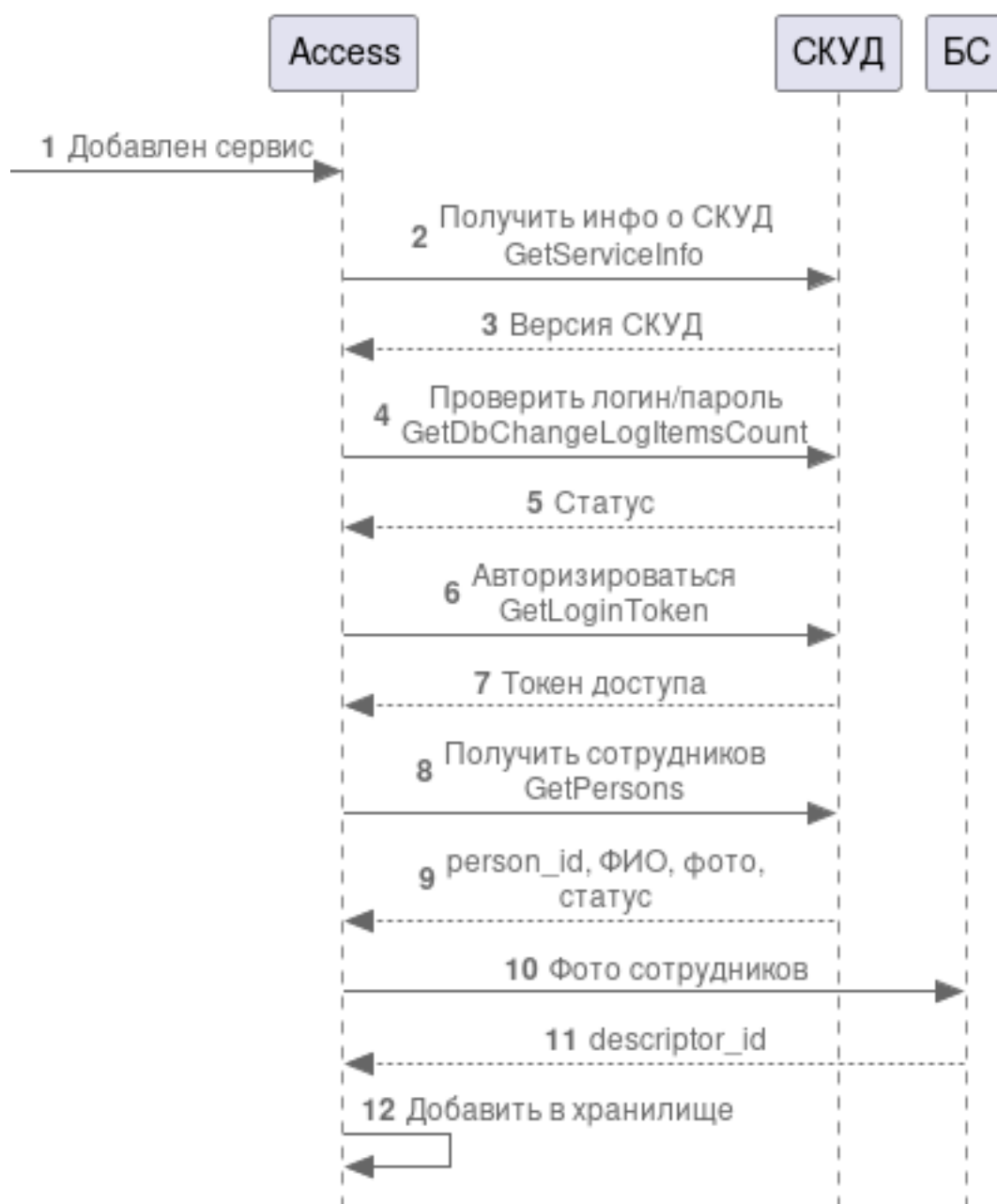
Задача	Операция	Описание
Получить инфо о СКУД	GetService Info	Получение версии СКУД для проверки совместимости и отображения в UI. Проверка доступности СКУД (каждую минуту).

Задача	Операция	Описание
Получить статус авторизации	GetDb ChangeLog ItemsCount	Получение статуса правильности ввода логина/пароля учетной записи в СКУД.
Авторизовать	GetLogin Token	Авторизация Access в СКУД. Авторизация происходит при добавлении сервиса и перед истечением токена (за 10 минут)
Продлить токен	Extend Token Expiration	При выполнении запросов проверяется время жизни токена. Запрос выполняется если срок жизни токена подходит к концу
Получить сотрудников	Get Persons	Репликация и синхронизация сотрудников (person_id, ФИО, статус, фото, дата и время последнего изменения) из СКУД в локальное хранилище. Происходит итерационно по 500 строк.
Получить информацию о сотруднике	Get PersonById	Получение данных сотрудника из СКУД (person_id, ФИО, статус, фото, дата и время последнего изменения)
Получить номер карты	Get Keys	Получение карт типа PROXIMITY по всем сотрудникам. Выбираются самые последние для каждого сотрудника
Получить события	GetDb Change LogItems Count	Получение событий сотрудников (добавление, изменение или удаление) каждые 5 секунд.

11.5. Диаграммы процессов взаимодействия с Болид

11.5.1. Подключение сервиса Болид

Диаграмма процесса (Рисунок 74).

**Рис. 74:** Диаграмма процессов при подключения SKUD

1. Пользователь добавил в Access сервис Bolid.
2. Access отправляет запрос на получение информации о SKUD.
3. SKUD возвращает информацию. Access проверяет доступность SKUD и использует версию SKUD для проверки совместимости и информации пользователя в UI.
4. Access отправляет запрос на корректность пары логин/пароль от учетной записи в SKUD.
5. SKUD возвращает статус активности учетной записи. Если запись активна, то работа продол-

жается.

6. Access отправляет запрос на авторизацию в СКУД.
7. СКУД возвращает токен для авторизации. Токен имеет время жизни, по истечению которого Access повторно выполняет авторизацию.
8. Access отправляет запрос на получение информации о сотрудниках для репликации данных в локальное хранилище.
9. СКУД возвращает person_id, ФИО, статус активности для однозначности, фото, дата и время последнего изменения.
10. Access отправляет запрос с фото сотрудников к БС на извлечение descriptor_id (face_id).
11. БС возвращает descriptor_id.
12. Access сохраняет информацию по каждому сотруднику в локальное хранилище.

11.5.2. Обработка событий Болид при 1 факторе

Диаграмма процесса (Рисунок 75).

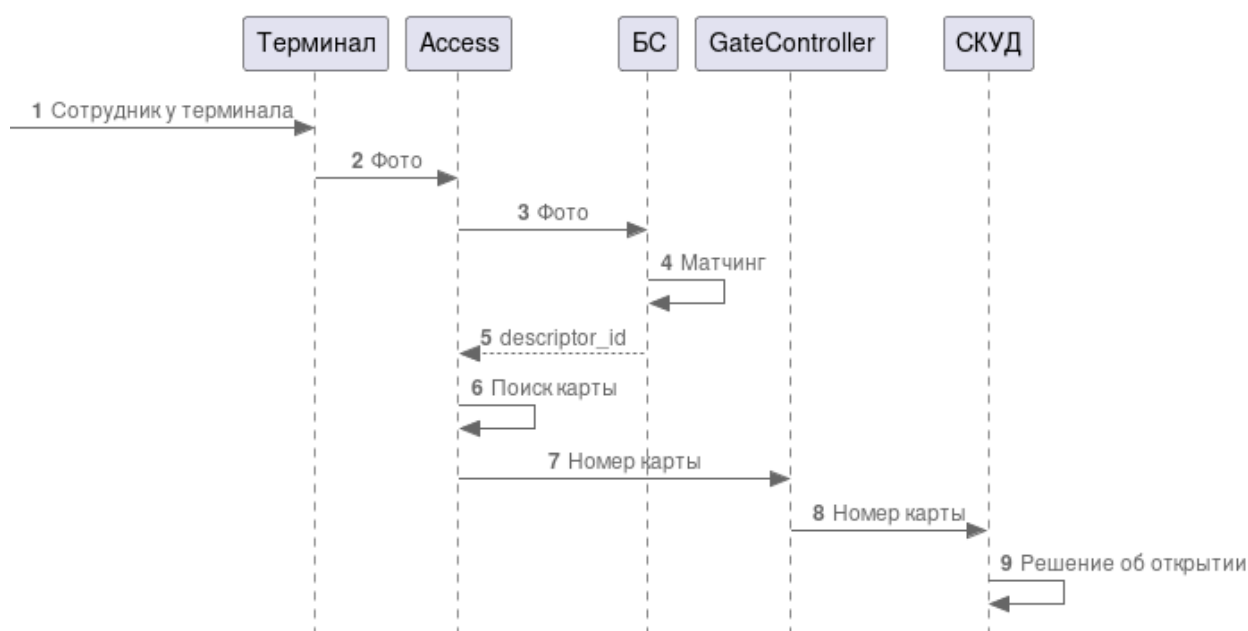


Рис. 75: Диаграмма процессов при 1 факторе

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему (БС) фото сотрудника.

4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access descriptor_id.
6. Access ищет номер карты сотрудника через соотнесение descriptor_id и person_id.
7. Access отправляет номер карты в GateController.
8. GateController передает номер карты в Gate Wiegand, который в свою очередь передает его контроллеру СКУД.
9. Контроллер СКУД принимает решение о пропуске сотрудника.

11.5.3. Обработка событий Болид при 2 факторах

Диаграмма процесса (Рисунок 76).

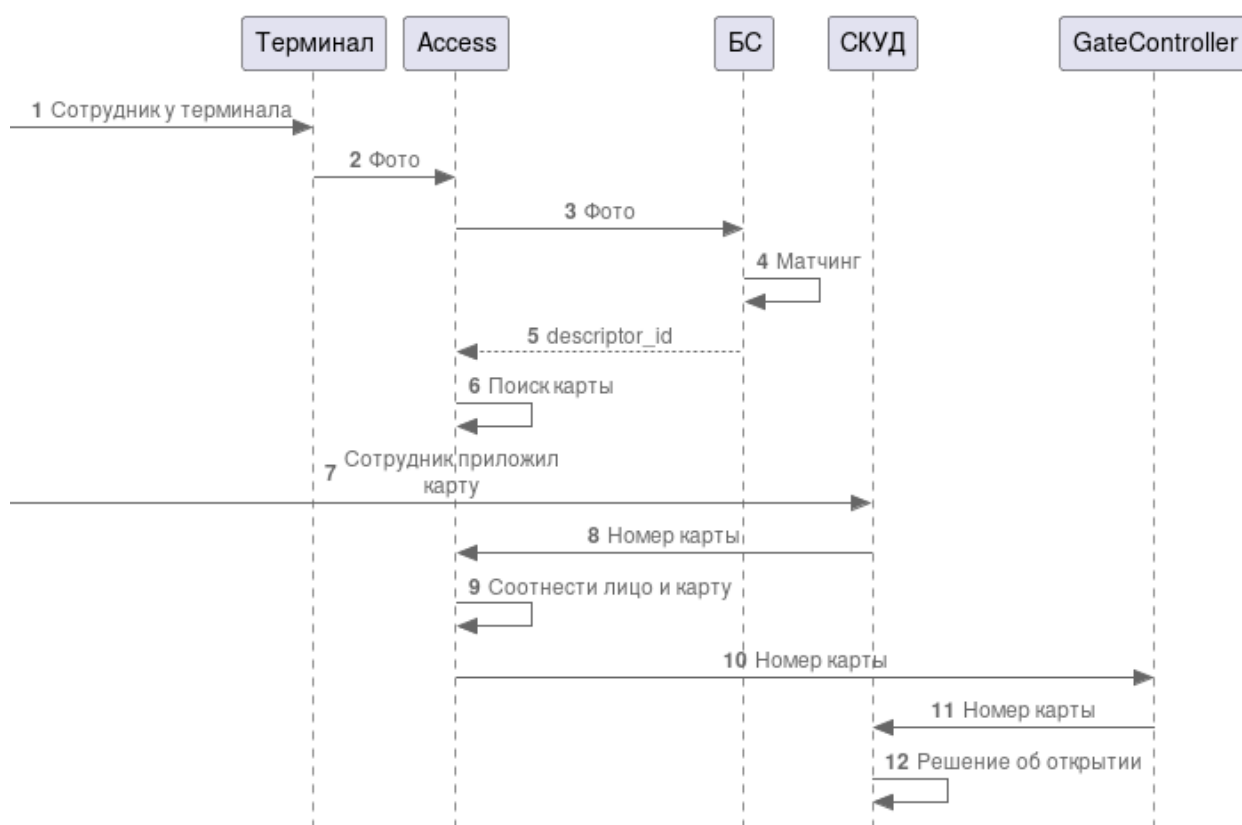


Рис. 76: Диаграмма процессов при 2 факторах

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.

4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access descriptor_id.
6. Access ищет номер карты сотрудника через соотнесение descriptor_id и person_id.
7. Сотрудник прикладывает карту (подпроцесс использования карты не зависит от обработки фото, но, как правило, сначала приходит фото).
8. СКУД отправляет в Access номер карты.
9. Access сравнивает номера карт полученных на шагах 6 и 8.
10. Access отправляет номер карты в GateController.
11. GateController отправляет номер карты в СКУД.
12. СКУД принимает решение об открытии.

11.6. Болид FAQ

1. Почему не могу добавить фото сотрудника размером более 100 кб?
 - В Орион Про может сбросится максимально допустимый размер фото до 100кб. Необходимо перейти в АДБ Орион Про Настройка > Настройки > Персонал > «Максимальный размер фотографий сотрудников, кБ» установить 10240 кБ (10 мБ) или больше.

12. СКУД Gate

Интеграционный модуль (sync.exe), запускаемый в директории Gate Server, определяет изменения в БД СКУД и отправляет изменения на ip:port указанные в файле настроек .env. Access принимает, обрабатывает запросы и вносит соответствующие изменения в список Luna.

Поддерживаемая версия СКУД: Gate Terminal 1.22.95, Gate Server 1.22.95

12.1. Поддерживаемые варианты интеграции СКУД Gate

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 47) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 47. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Gate + GateController / PusrController	Beward	LunaEventListener + SendThermalEventToLuna/SendToLuna
	BioSmart	LunaEventListener + SendToLuna
	Dahua	LunaEventListener + SendToLuna
	Dahua Thermo	LunaEventListener + SendThermalEventToLuna
	Fortuna315	LunaEventListener + SendThermalEventToLuna
	HikvisionCamera	LunaEventListener + SendToLuna
	HikvisionCamera Thermo	LunaEventListener + SendThermalEventToLuna
	HikvisionTerminal Thermo	LunaEventListener + SendThermalEventToLuna

Сервис	Устройство	Пайплайн
	LunaFast4A1	LunaEventListener + SendToLuna
	Panda	LunaEventListener + SendThermalEventToLuna
	UniUbi	LunaEventListener + SendThermalEventToLuna / SendToLuna
	VKVision02	LunaEventListener
	R20Face	LunaEventListener + SendToLuna

13. СКУД Parsec

Поддерживает версию СКУД ParsecNET 3: 3.11.629 39.

Сервис позволяет обрабатывать запросы от СКУД, такие как:

- передача списка сотрудников в локальное хранилище персон,
- добавление/редактирование/удаление сотрудников в локальном хранилище персон,
- получение событий детекции с устройств.

Сервис выполняет следующие запросы в СКУД:

- отправка url адресов ONVIF сервисов,
- получение идентификаторов точек доступа.

При запуске сервиса, сначала запрашиваются идентификаторы точек доступа и генерируются их имена.

СКУД опрашивает Access на наличие детектов, и формирует ответ, в котором содержится идентификатор сотрудника, а также идентификатор точки доступа.

По мере возникновения валидной детекции лица, сервис возвращает ответ в СКУД.

При подключении устройств необходимо указывать имена точек доступа, автоматически сгенерированные сервисом на основе точек прохода в СКУД. Указываются в Info сервиса. Они генерируются в формате «имя точки доступа - идентификатор». Например: «турникет_выход - 907efa78-cb2f-4f46-b374-785c7f9901a5».

Полученные имена точек доступа необходимо указывать в:

- При использовании внутренних устройств Access (HikvisionTerminal, Panda ...), указать в поле «name»
- При использовании LunaStream, указать в поле «source»

13.1. Поддерживаемые варианты интеграции СКУД Parsec

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 48) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 48. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Parsec	Beward	SendToParsec + MatchByPhoto + SendToDevice
	BioSmart	SendToParsec + MatchByPhoto + SendToDevice
	Dahua	SendToParsec + MatchByPhoto
	Dahua Thermo	SendToParsec + MatchByPhoto
	Fortuna315	SendToParsec + MatchByPhoto
	HikvisionCamera	SendToParsec + MatchByPhoto
	HikvisionCamera Thermo	SendToParsec + MatchByPhoto
	HikvisionTerminal Thermo	SendToParsec + MatchByPhoto + SendToDevice
	LunaFast4A1	SendToParsec + MatchByPhoto
	Panda	SendToParsec + MatchByPhoto
	UniUbi	SendToParsec + MatchByPhoto + SendToDevice
	VKVision02	SendToParsec + MatchByPhoto + SendToDevice
	R20Face	SendToParsec + MatchByPhoto + SendToDevice

В каждой интеграции с КБС (Таблица 49) используется сервис КБС.

Таблица 49. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsMts + Parsec	Beward	SendToParsec + MatchByPhoto + SendToDevice
	Dahua	SendToParsec + MatchByPhoto + SendToDevice
	HikvisionCamera	SendToParsec + MatchByPhoto + SendToDevice
	LunaFast4A1	SendToParsec + MatchByPhoto + SendToDevice
	UniUbi	SendToParsec + MatchByPhoto + SendToDevice

13.2. Стандартная интеграция с использованием Parsec

При интеграции с Parsec используются стандартные компоненты Access (Рисунок 77) и (Таблица 50).

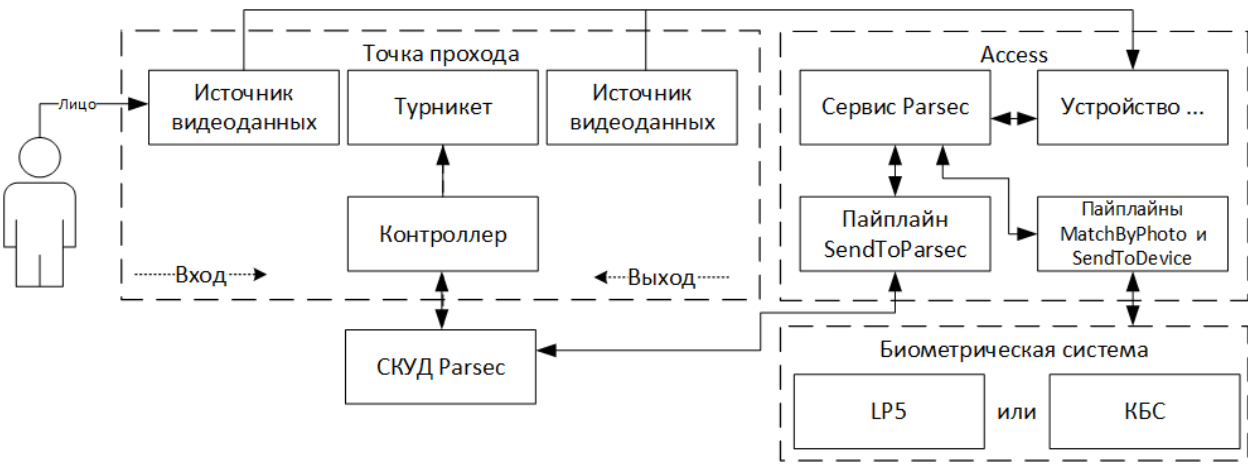


Рис. 77: Схема компонентов при интеграции с Parsec

Таблица 50. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Контроллер	Плата управления точкой прохода.
Турникет	Преграждающее устройство для разграничения доступов
СКУД Parsec	Центральное ПО для работы с Parsec. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Пайплайн SendToParsec	Компонент Access для обмена данными с СКУД
Сервис Parsec	Компонент Access для обработки информации от СКУД
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом (для вывода сообщений и фото на экран) необходимо дополнительно подключать пайплайн SendToDevice

Компонент	Описание
Пайплайн SendToController	Компонент Access для взаимодействия с КБС
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через LunaStream.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Может быть либо Luna , либо КБС МТС .

13.3. Настройка ПО СКУД Parsec

Для запуска и настройки ПО СКУД Parsec установите Parsec.NET и запустите программу «Администрирование» и проверьте настройки (Рисунок 78):

1. Убедиться, что запущен «Расширенный режим» (Файл→Расширенный режим).
2. Перейти в раздел «Редактор оборудования» и убедиться, что контроллеры подключены.

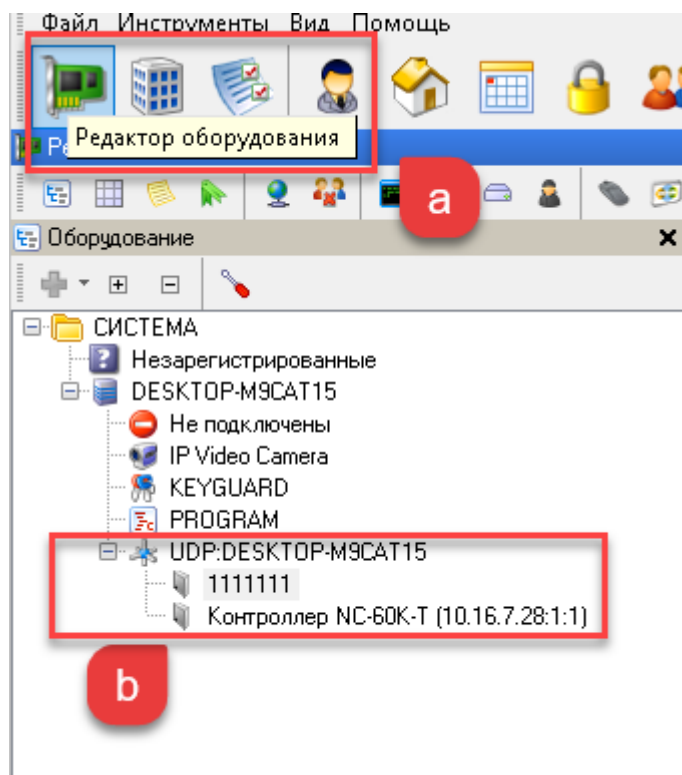


Рис. 78: Раздел «Редактор оборудования»

3. В каждом необходимом контроллере, установить следующие настройки во вкладке «Режимы прохода» (Рисунок 79).

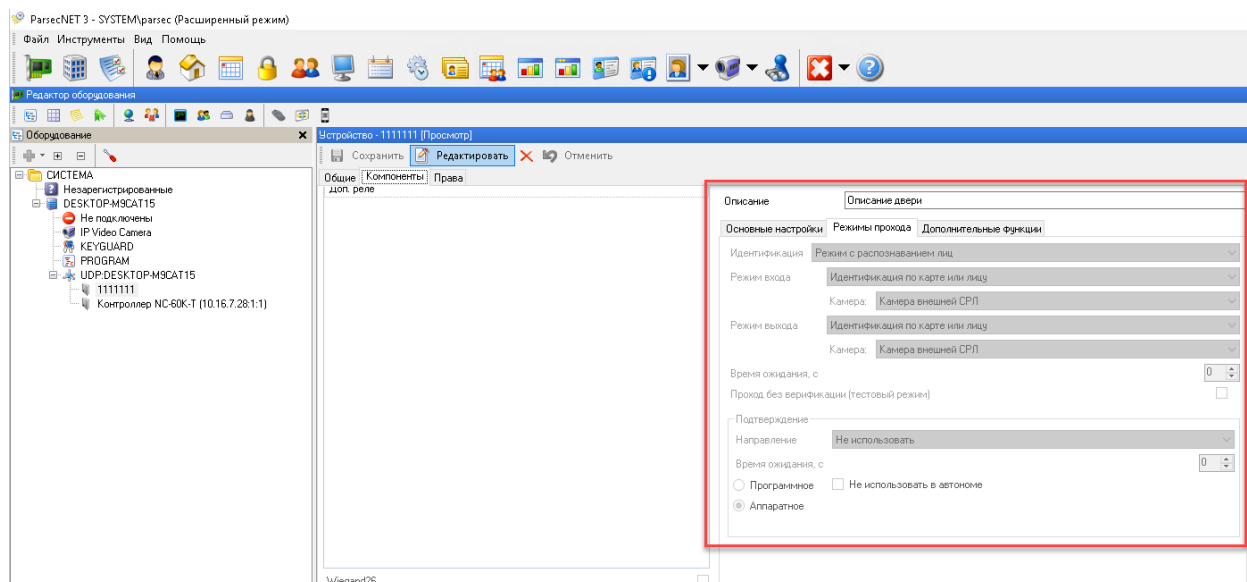


Рис. 79: Вкладка «Режимы прохода»

4. Перейти в раздел «Редактор системных настроек», затем открыть вкладку «Распознавание

лиц (Onvif)» (Рисунок 80).

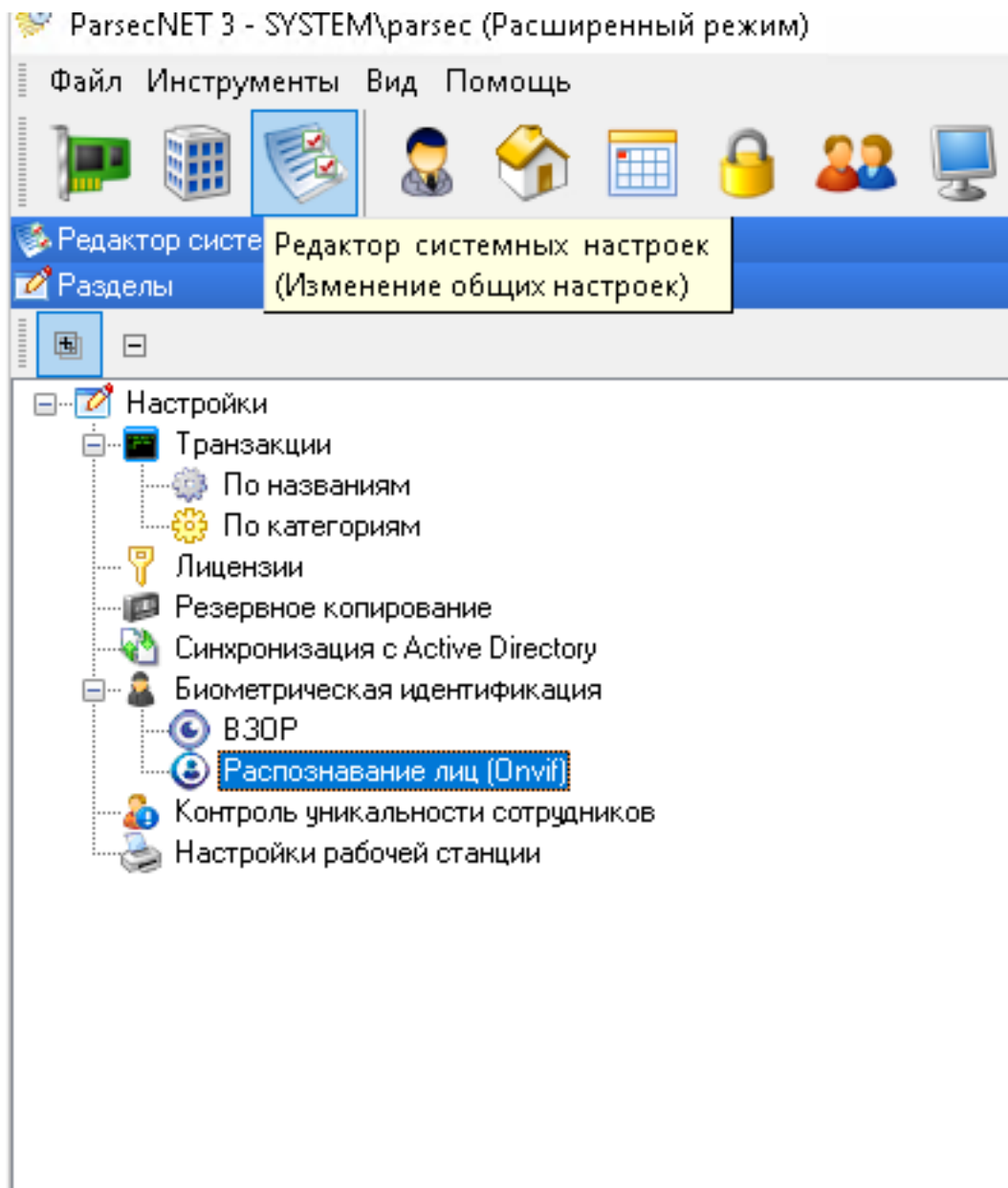


Рис. 80: Вкладка «Распознавание лиц (Onvif)»

5. В окне «Распознавание лиц (Onvif)» нажать кнопку изменить и убедиться, что пункт «Использовать СРЛ» включен, а «Тип СРЛ» установлен «Распознавание лиц Onvif».
6. В поля «IP Адрес» и «Порт» ввести данные сервера Access.
 IP адрес всех компонентов должен вести на сервер Access.
7. Кнопку «Проверка подключения» нажимать только после настройки Access, для этого требуется «Ключ интеграции».

8. После нажатия на кнопку «Проверка подключения», поля в блоке «Сервисы системы распознавания лиц» заполняются автоматически.
9. Нажать кнопку «Сохранить».
10. Реплицировать сотрудников в список Luna путем нажатия кнопки «Передача сотрудников и посетителей». Перед этим убедитесь что все сотрудники корректно добавлены в разделе «Редактор персонала» см. п. [«Добавление сотрудников в СКУД Parsec»](#)

Пример отображения сотрудника выгруженного из СКУД Parsec в список LUNA PLATFORM (Рисунок 81).





1 (Количество лиц: 275)				
<input type="checkbox"/>	Информация	Внешний ID	Дата создания	
<input type="checkbox"/>	 Говард Кутузович Лавкрафт	20704647-9782-43c1-84d1-7337778e9a3e	22.09.2023, 14:39:13	  

Рис. 81: Отображение сотрудника в LUNA PLATFORM

13.3.1. Настройка групп доступа в СКУД Parsec

1. Перейти в раздел «Редактор групп доступа».
2. Добавьте новую группу доступа.
3. Добавьте территорию доступа куда входят точки доступа (Рисунок 82).

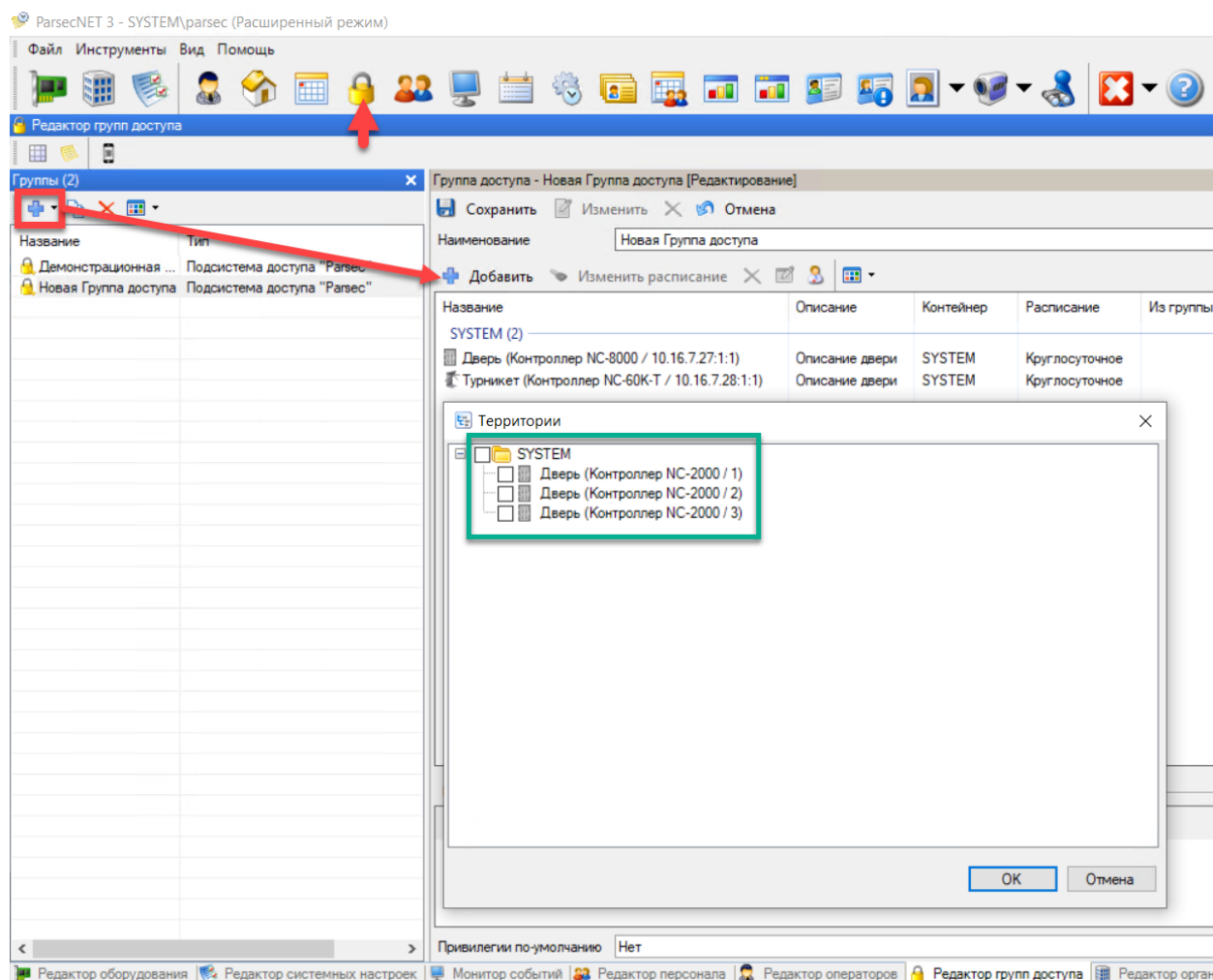


Рис. 82: Настройка групп доступа

4. Нажмите кнопку «Сохранить».

13.3.2. Добавление сотрудников в СКУД Parsec

Добавление сотрудников в СКУД Parsec необходимо для их последующей выгрузки в LUNA PLATFORM (Рисунок 83).

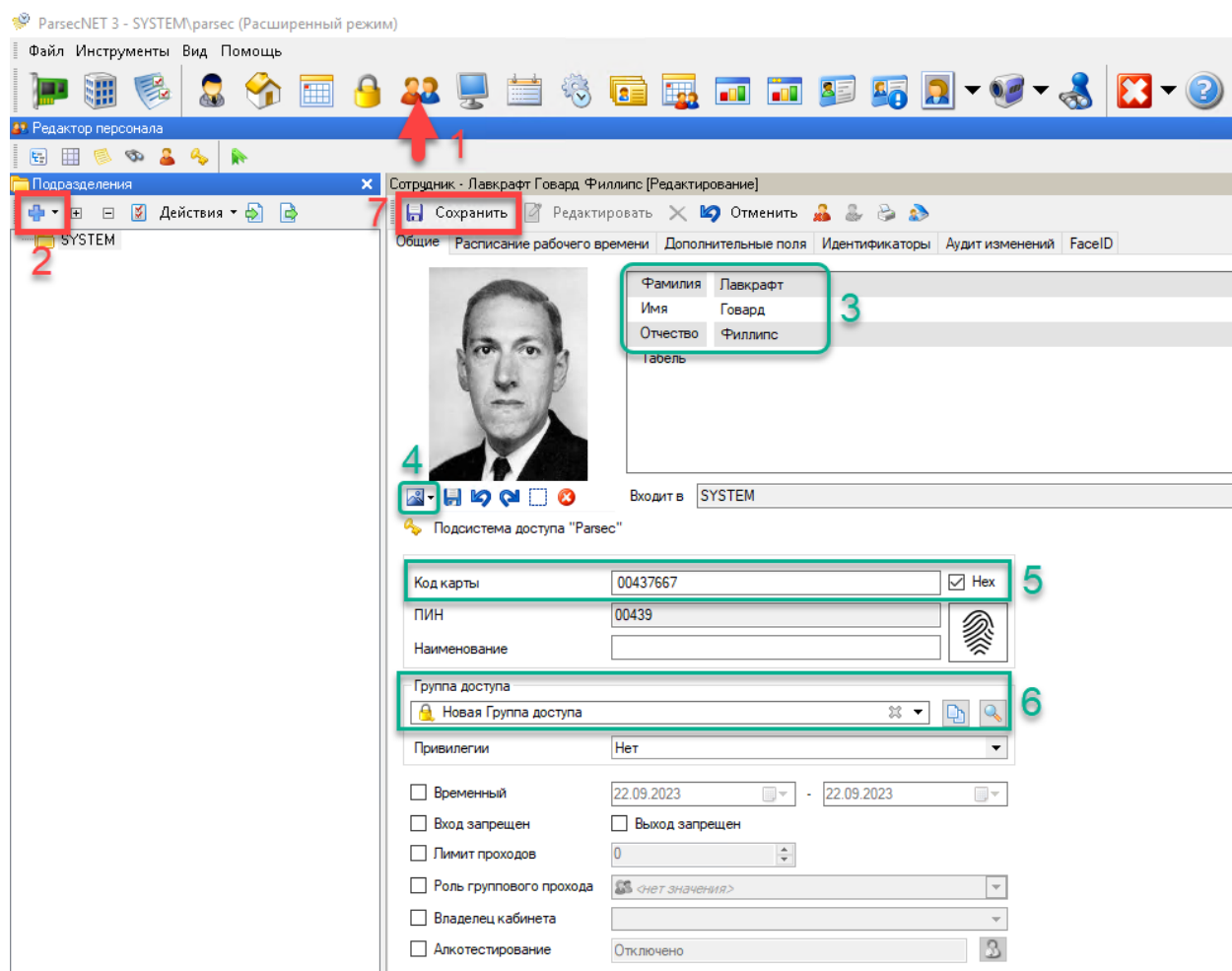


Рис. 83: Раздел «Редактирование персонала». Добавление нового сотрудника

1. Перейти в раздел «Редактор персонала».
2. Нажать кнопку добавления нового сотрудника.
3. Заполните поля «Фамилия» и «Имя».
4. Добавьте фото сотрудника.
5. Заполните поле «Код карты». При этом поле «ПИН» заполняется автоматически.

Если проход по картам не предусмотрен на объекте или у данного сотрудника нет карты — введите любое значение в поле «Код карты».

6. Выберите группу доступа сотрудника.
7. Нажмите кнопку «Сохранить».

При корректном добавлении сотрудников все новые или измененные данные будут добавлены в базу LUNA PLATFORM автоматически.

13.4. Методы взаимодействия с Parsec

Access выступает в роли сервера и клиента (Таблица 51).

Отправка методов ONVIF в Access происходит на эндпоинт POST /vl-access/webhook/service/onvif/{component_id}.

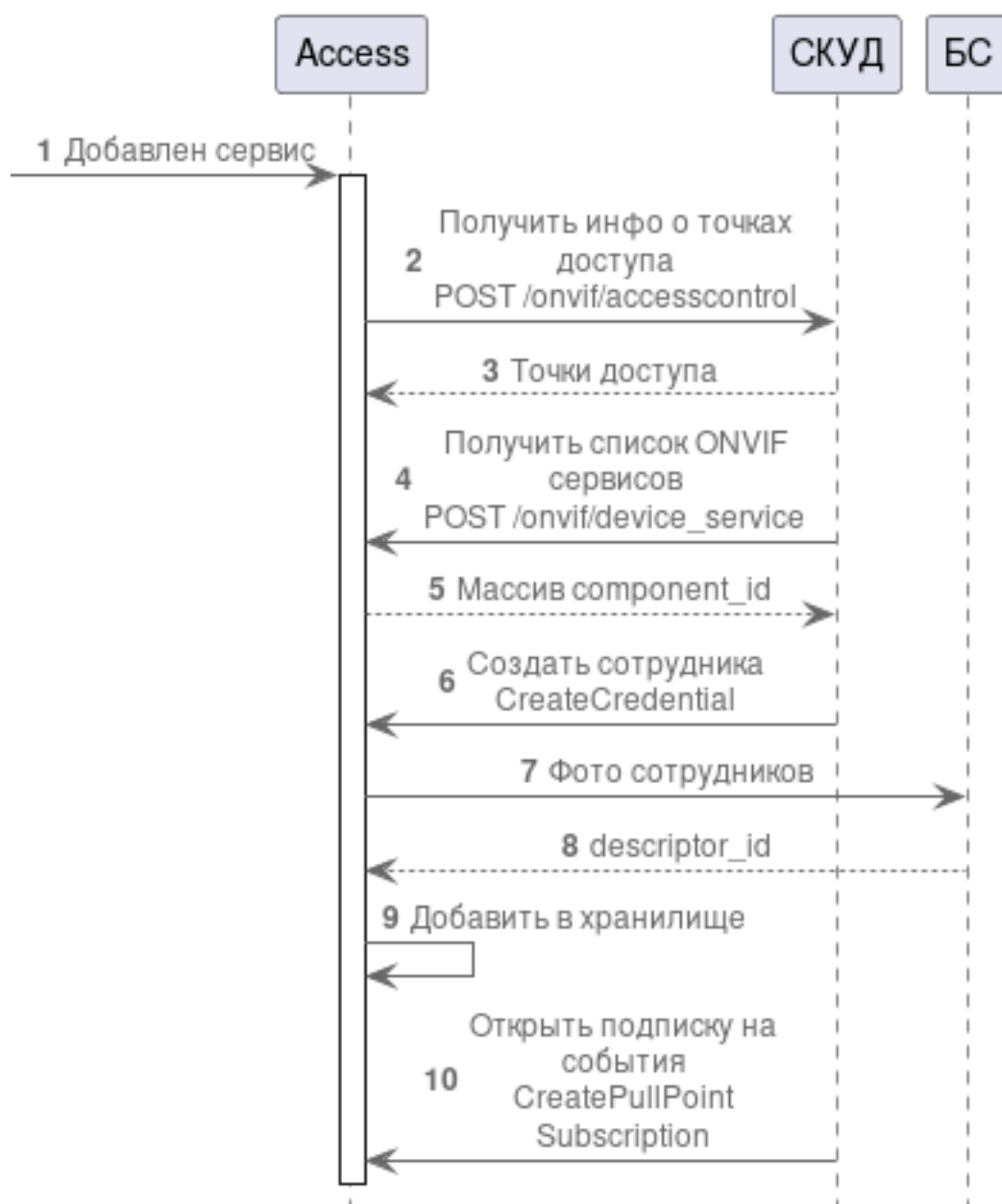
Таблица 51. Используемые методы СКУД Parsec

Задача	Метод	Описание
Получить точки доступа	POST /onvif/accesscontrol	Запрос к СКУД. Получение ID точек доступа (контроллеров) для ручного сопоставления камер/терминалов и точек доступа
Получить список сервисов ONVIF	POST /onvif/device_service	Получение списка component_id ONVIF сервисов Access для подключения
Создание пользователя	CreateCredential	Метод ONVIF
Обновление пользователя	ModifyCredential	Метод ONVIF
Удаление пользователя	DeleteCredential	Метод ONVIF
Создание подписки	CreatePullPoint Subscription	Метод ONVIF. Подписка на события.
Получить события детекции	PullMessages	Получения события детекции сотрудника. Запрос отправляется каждые 10 секунд и ожидает 10 секунд до появления кадра.

13.5. Диаграммы процессов взаимодействия с Parsec

13.5.1. Подключение сервиса Parsec

Диаграмма процесса (Рисунок 84).

**Рис. 84:** Диаграмма процессов при подключения СКУД

1. Пользователь добавил в Access сервис Parsec.
2. Access отправляет запрос в СКУД для получения точек доступов. Полученные точки доступа отображаются в поле info свойств сервиса. Запрос используется в качестве проверки доступности СКУД.
3. СКУД возвращает точки доступа.
4. СКУД отправляет запрос в Access для получения списка сервисов Access поддерживающих протокол ONVIF.

5. Access возвращает component_id ONVIF сервисов.
6. СКУД отправляет в Access запрос POST /vl-access/webhook/service/onvif/{component_id} CreateCredential для передачи сотрудников в хранилище Access.
7. Access отправляет запрос с фото сотрудников к БС на извлечение descriptor_id (face_id).
8. БС возвращает descriptor_id.
9. Access сохраняет информацию по каждому сотруднику в локальное хранилище.
10. СКУД отправляет запрос в Access на открытие подписки на получение событий (лучшие кадры человека у терминала).

13.5.2. Обработка событий Parsec при 2 факторах

Диаграмма процесса (Рисунок 85).

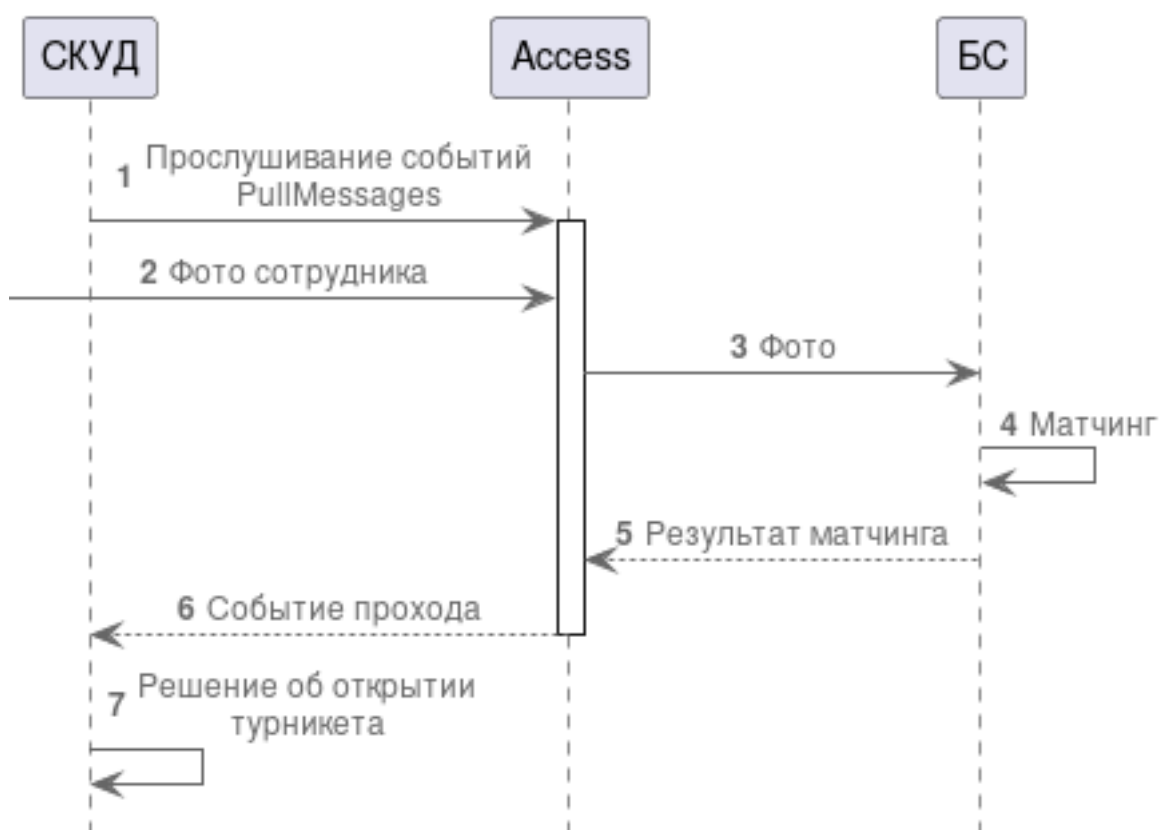


Рис. 85: Диаграмма процессов при 2 факторах

1. СКУД отправляет раз в 10 секунд запрос POST /vl-access/webhook/service/onvif/{component_id} PullMessages на ожидание в течении 10 секунд события прохода.
2. В Access поступает лучший кадр сотрудника у терминала.

3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографий с терминала и сохраненной в базе.
5. БС возвращает в Access решение о предоставлении доступа.
6. Access возвращает событие прохода вСКУД.
7. СКУД принимает решение об открытии терминала.

14. СКУД PERCo-Web

Программные интеграции ПО СКУД PERCo-Web с LP5 реализована для обеспечения прохода распознанных лиц через турникет/дверь с магнитным замком.

- Поддерживает версии PERCo-Web системы 2.0, номер сборки PERCo-Web 4.30.

Выполняет репликацию данных пользователей из СКУД PERCo-Web и генерирует контроллеры PercoController из полученного списка устройств для последующего выполнения запросов на вход или выход.

14.1. Поддерживаемые варианты интеграции СКУД PERCo-Web

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 52) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 52. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
PercoWeb + PercoController	Beward	MatchByPhoto + SendToController + SendToDevice
	BioSmart	MatchByPhoto + SendToController + SendToDevice
	Dahua	MatchByPhoto + SendToController
	HikvisionCamera	MatchByPhoto + SendToController
	LunaFast4A1	MatchByPhoto + SendToController + SendToDevice
	UniUbi	MatchByPhoto + SendToController + SendToDevice
	VKVision02	MatchByPhoto + SendToController + SendToDevice
	R20Face	MatchByPhoto + SendCardToR20Face / SendToController + SendToDevice

14.2. Стандартная интеграция с использованием PERCo-Web

Поддерживается только 1ф интеграция (Рисунок 86) и (Таблица 53).

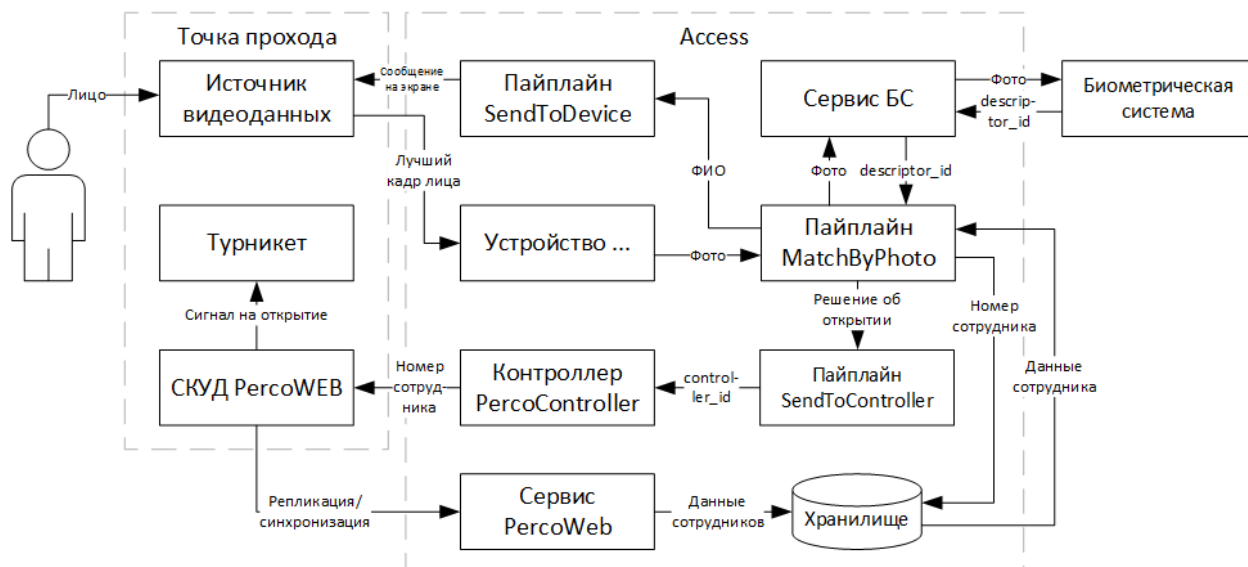


Рис. 86: Схема компонентов при 1ф интеграции с PERCo-Web

Таблица 53. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream. Биометрический терминал позволяет создать обратную связь для демонстрации человеку информации о проходе.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.

Компонент	Описание
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Сервис БС	Компонент Access для взаимодействия с БС: для LP5 это Luna, для КБС - соответствующий сервис КБС.
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Может быть либо LP5, либо поддерживаемая КБС.
Хранилище	БД в составе Access для хранения информации о сотрудниках.
Пайплайн SendToController	Компонент Access передает идентификатор сотрудника в PercoController после матчинга человека и подтверждения номера карты в Access.
Контроллер PercoController	Компонент Access для отправки в СКУД номера карты.
СКУД PercoWEB	Центральное ПО для работы с PercoWEB. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Турникет	Преграждающее устройство для разграничения доступов
Сервис PercoWEB	Компонент Access для выполнения репликации/синхронизации сотрудников из СКУД и прослушивания событий СКУД.

14.3. Методы взаимодействия с PERCo-Web

Начало эндпоинта для всех запросов (Таблица 54): /api.

Таблица 54. Используемые методы СКУД PERCo-Web

Задача	Метод	Описание
Авторизоваться	POST /system/auth	Авторизация Access в СКУД. Авторизация происходит при добавлении сервиса для получения токена. Время жизни токена - 840 секунд.
Проверка доступности	GET /system/language/	Проверка доступности СКУД. Выполняется раз в минуту
Получить контроллеры	GET /devices	Получить device_id контроллеров для создания в Access PercoController.

Задача	Метод	Описание
Получить информацию о контроллере	GET /devices/{device_активен. id}	Получить информацию о контроллере по его id, если он активен.
Синхронизация сотрудников	GET /users/staff/tab	Получить информацию о сотрудниках: наличие фото, статус активности, ФИО и person_id.
Получить фото сотрудников	GET /users/{user_ id}/image	Получить фото сотрудника
Получить события	GET /eventsystem	Запрос на получение событий изменения сотрудников. Запрос отправляется каждые 10 секунд.
Открыть турникет	POST /devices/{device_контроллере, id}/pass	Отправка запрос для открытия доступа человеку на том же контроллере, от которого пришло событие.

14.4. Диаграммы процессов взаимодействия с PERCo-Web

14.4.1. Подключение сервиса PERCo-Web

Диаграмма процесса (Рисунок 87).

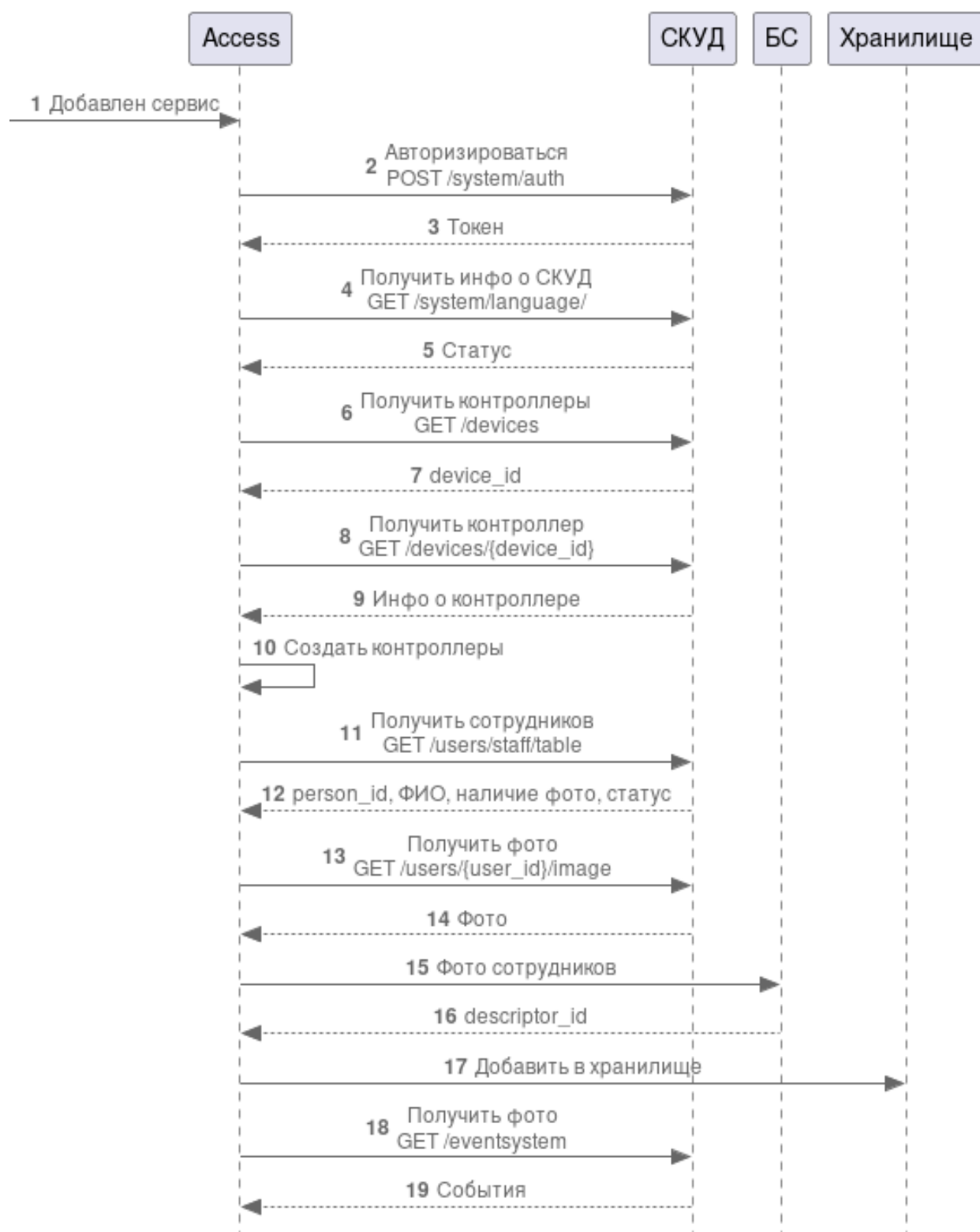
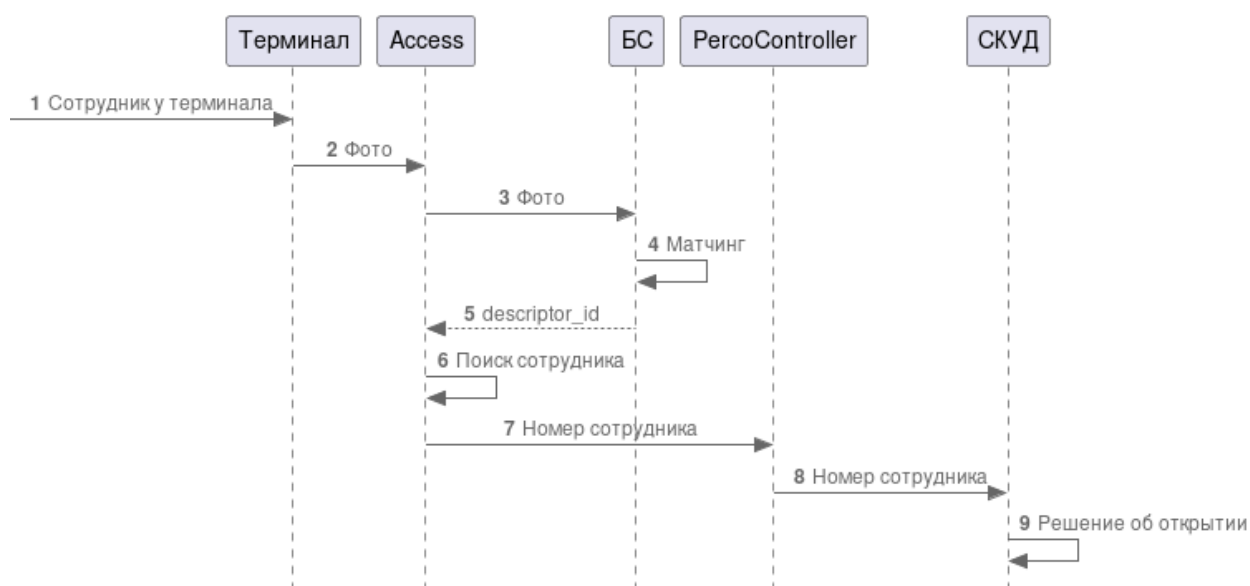


Рис. 87: Диаграмма процессов при подключения СКУД

1. Пользователь добавил в Access сервис PERCo-Web.
2. Access отправляет запрос на авторизацию в СКУД.
3. СКУД возвращает токен для авторизации. Токен имеет время жизни, по истечению которого Access повторно выполняет авторизацию.
4. Access отправляет запрос GET /system/language/ для определения активен ли сервис.
5. СКУД возвращает ответ.
6. Access отправляет запрос на получение списка активных контроллеров.
7. СКУД возвращает массив device_id.
8. Access отправляет запрос на получение информации о контроллере, для каждого полученного device_id.
9. СКУД возвращает данные контроллера.
10. Access создает PercoController по количеству полученных device_id.
11. Access отправляет запрос на репликацию сотрудников из СКУД.
12. СКУД возвращает данные сотрудников.
13. Access отправляет запрос на получение фото сотрудников, которые активны и имеют фото.
14. СКУД возвращает фото сотрудников.
15. Access отправляет запрос с фото сотрудников к БС на извлечение descriptor_id (face_id).
16. БС возвращает descriptor_id.
17. Access сохраняет в хранилище данные сотрудников.
18. Access отправляет запрос каждые 10 секунд для получения событий об изменении сотрудников для выполнения синхронизации.
19. СКУД возвращает события.

14.4.2. Обработка событий PERCo-Web при 1 факторе

Диаграмма процесса (Рисунок 88).

**Рис. 88:** Диаграмма процессов при 1 факторе

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access результат матчинга.
6. Access ищет номер сотрудника по полученному descriptor_id.
7. Access отправляет в СКУД номер сотрудника.
8. СКУД принимает решение о пропуске человека.

15. СКУД RusGuard

Программные интеграции ПО СКУД Rusguard с биометрическими системами реализованы для обеспечения прохода распознанных лиц через турникет.

Access реплицирует сотрудников из СКУДа в свою БД, запрашивая идентификатор дескриптора в КБС по фотографии сотрудника. Для актуализации данных сессия репликации по умолчанию перезапускается через 5 секунд после завершения (задается в настройках сервиса).

- Поддерживает версии: Система - 3.3.1, База данных - 3.3.1

15.1. Поддерживаемые варианты интеграции СКУД RusGuard

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью репликации - механизма первоначального переноса данных пользователей.

Настройку репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 55) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 55. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Rusguard + GateController / PusrController	Beward	MatchByPhoto + SendToController + SendToDevice
	BioSmart	MatchByPhoto + SendToController + SendToDevice
	Dahua	MatchByPhoto + SendToController
	Dahua Thermo	MatchByPhoto + SendToController
	Fortuna315	MatchByPhoto + SendToController
	HikvisionCamera	MatchByPhoto + SendToController
	HikvisionCamera Thermo	MatchByPhoto + SendToController
	HikvisionTerminal Thermo	MatchByPhoto + SendToController + SendToDevice

Сервис	Устройство	Пайплайн
	LunaFast4A1	MatchByPhoto + SendToController
	Panda	MatchByPhoto + SendToController
	UniUbi	MatchByPhoto + SendToController + SendToDevice
	VKVision02	MatchByPhoto + SendToController + SendToDevice
	R20Face	MatchByPhoto + SendToController + SendToDevice

В каждой интеграции с КБС (Таблица 56) используется сервис КБС.

Таблица 56. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsMts + Rusguard + LunaStreams	R20Face	MatchByPhoto + SendCardToR20Face + SendToDevice
	BioSmart	MatchByPhoto + GateController / PusrController + SendToDevice
	Dahua	MatchByPhoto + GateController / PusrController
	Dahua Thermo	MatchByPhoto + GateController / PusrController
	Fortuna315	MatchByPhoto + GateController / PusrController
	HikvisionCamera	MatchByPhoto + GateController / PusrController
	HikvisionCamera Thermo	MatchByPhoto + GateController / PusrController
	HikvisionTerminal Thermo	MatchByPhoto + GateController / PusrController + SendToDevice
	LunaFast4A1	MatchByPhoto + GateController / PusrController
	Panda	MatchByPhoto + GateController / PusrController
	UniUbi	MatchByPhoto + GateController / PusrController

Сервис	Устройство	Пайплайн
	VKVision02	MatchByPhoto + GateController / PusrController + SendToDevice
	R20Face	MatchByPhoto + GateController / PusrController + SendToDevice

15.2. Стандартная интеграция с использованием RusGuard

При интеграции с RusGuard используются стандартные компоненты Access (Рисунок 89) и (Таблица 57).

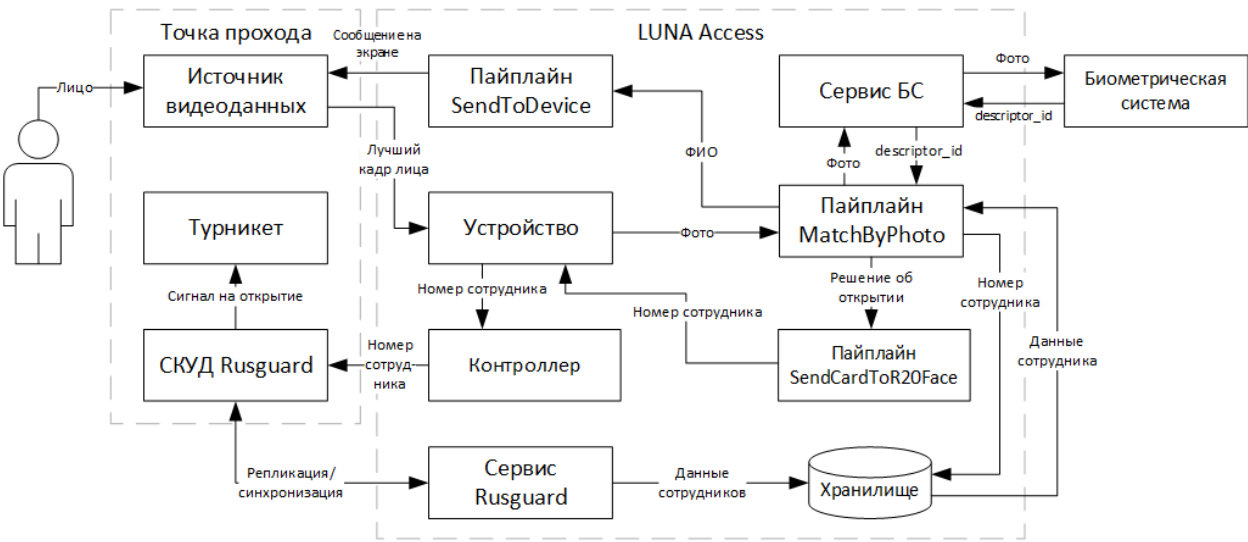


Рис. 89: Схема компонентов при интеграции с RusGuard

Таблица 57. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream (тогда необходим сервис LunaStreams).
Турникет	Преграждающее устройство для разграничения доступов.

Компонент	Описание
СКУД RusGuard	Центральное ПО для работы с RusGuard. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Сервис Rusguard	Компонент Access для отправки запросов и обработки данных от СКУД.
Устройство	Компонент Access для получения данных от источника видеоданных.
Контроллер	Плата управления точкой прохода.
Пайплайн SendCardToR20Face	Компонент Access для обмена данными с СКУД
Сервис БС	Компонент Access для взаимодействия с БС: для LP5 это Luna , для КБС - соответствующий сервис КБС.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Может быть либо Luna , либо поддерживаемая КБС.
Хранилище	БД в составе Access для хранения информации о сотрудниках.

15.3. Методы взаимодействия с RusGuard

Для обмена данными с СКУД используется API (Таблица 58).

Таблица 58. Используемые методы СКУД RusGuard

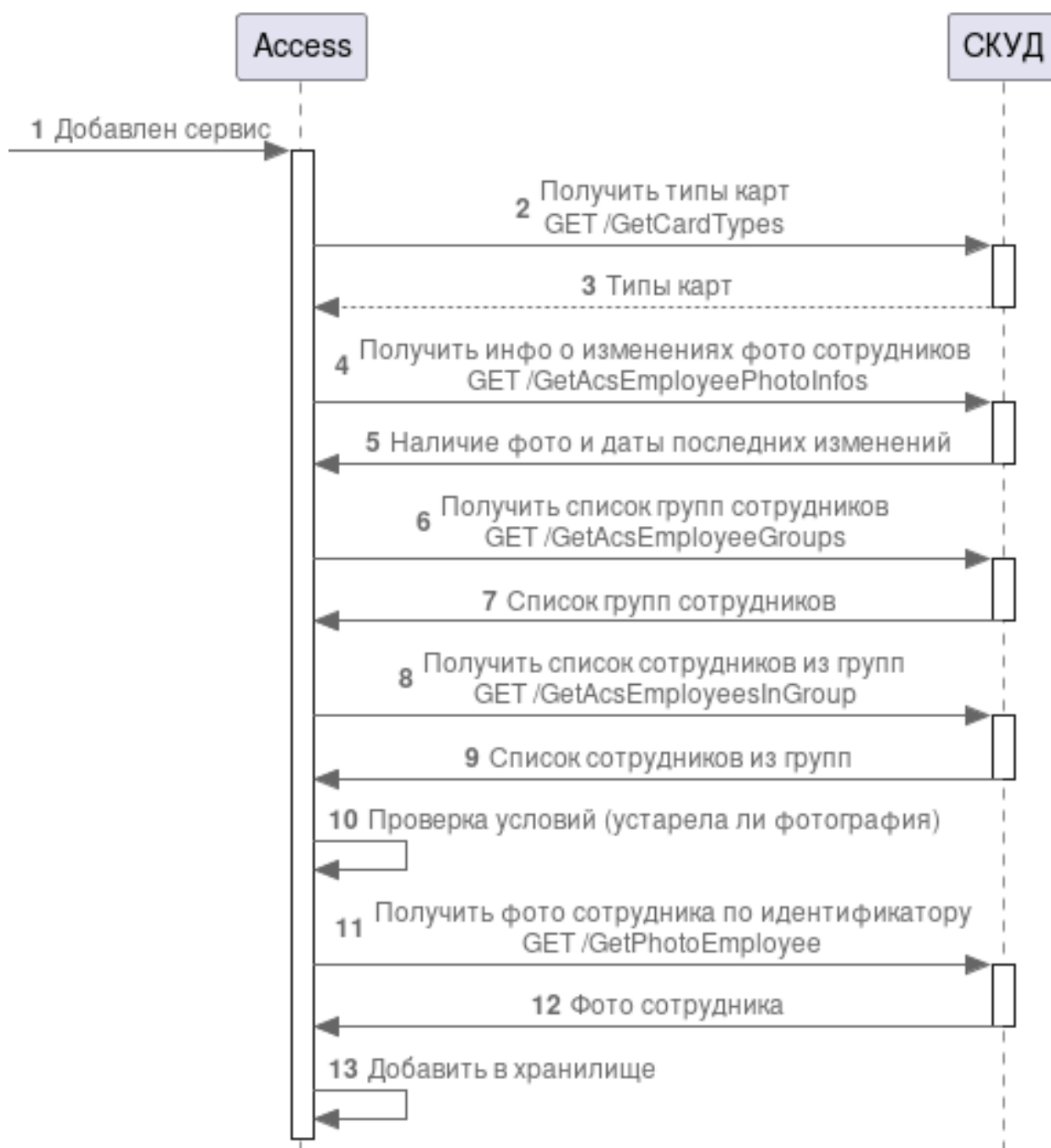
Задача	Метод	Описание
Получить типы карт	GET /GetCardTypes	Получить типы карт в СКУД. Используется для проверки соединения со СКУД
Получить инфо о фото сотрудников	GET /GetAcsEmployeePhotoInfos	Получить информацию о фотографиях сотрудников в СКУД
Получить список групп сотрудников	GET /GetAcsEmployeeGroups	Получить список групп сотрудников в СКУД

Задача	Метод	Описание
Получить список сотрудников из группы	GET /GetAcsEmployeesInGroup	Получить список сотрудников из группы в СКУД
Получить фото сотрудника по идентификатору	GET /GetPhotoEmployee?PersonGuidId=employee_id&photoNumber=photo_number	Получить фото сотрудника в формате base64 по его идентификатору

15.4. Диаграммы процессов взаимодействия с RusGuard

15.4.1. Диаграмма взаимодействия RusGuard с Access

Диаграмма процесса (Рисунок 90).

**Рис. 90:** Диаграмма взаимодействия RusGuard с Access

1. Пользователь добавил в Access сервис Rusguard.
2. Access отправляет запрос GET /GetCardTypes на получение типов карт в СКУД, для проверки соединения.
3. СКУД возвращает массив card_types.

4. Access отправляет запрос GET /GetAcsEmployeePhotoInfos на получения информации о наличии фото сотрудников и даты их последних изменений в СКУД.
5. СКУД возвращает массив photos.
6. Access отправляет запрос GET /GetAcsEmployeeGroups на получения списка групп сотрудников в СКУД.
7. СКУД возвращает массив с данными групп (идентификатор и имя группы).
8. Access отправляет запрос GET /GetAcsEmployeesInGroup на получение сотрудников из группы, для каждой группы из прошлого запроса.
9. СКУД возвращает массив с данными по каждому сотруднику.
10. Access выполняет проверку устарела ли фотография сотрудника
11. Access отправляет запрос GET /GetPhotoEmployee?PersonGuidId=employee_id&photoNumber=photo_number на получение фото по каждому сотруднику из прошлого запроса, где:
 - employee_id - идентификатор сотрудника
 - photo_number - номер фотографии в СКУД
12. СКУД возвращает ответ с фотографией сотрудника в формате base64 по каждому сотруднику.
13. Access сохраняет в хранилище данные сотрудников.

15.4.2. Диаграмма взаимодействия Access с биометрической системой

Диаграмма процесса (Рисунок 91).

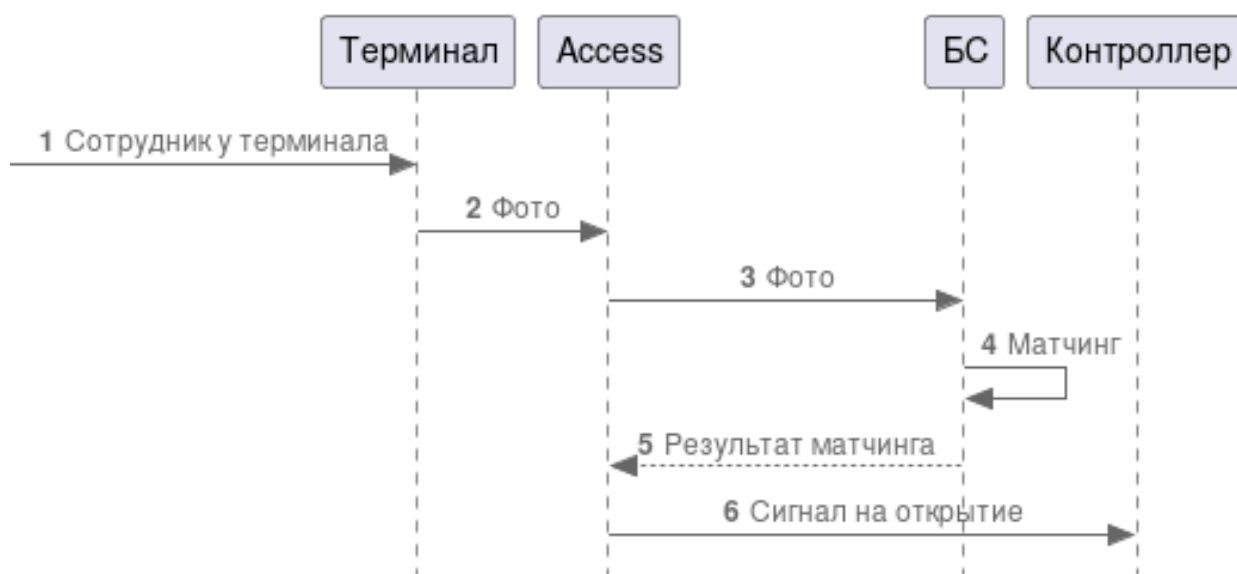


Рис. 91: Диаграмма взаимодействия Access с биометрической системой

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access решение о предоставлении доступа.
6. Access по полученному из БС дескриптору определяет номер карты доступа сотрудника и отправляет на контроллер сигнал на открытие точки доступа, указывая именно этот номер карты. На СКУД передаётся событие прохода

16. СКУД SALTO

СКУД синхронизирует сотрудников со списком в Luna и слушает события, на основе которых решает открывать или не открывать турникет. Данные события генерируются в Access пайплайном SendToSalto.

- Поддерживает версию СКУД SALTO: 6.6.3.0.

Выполняет репликацию данных пользователей из СКУД SALTO в указанный список Luna и генерирует контроллеры SaltoController из полученного списка дверей для последующего выполнения запросов на проход.

Настройку ПО СКУД SALTO см. в официальной документации.

16.1. Поддерживаемые варианты интеграции СКУД SALTO

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

В каждой интеграции с LP5 (Таблица 59) используется сервис [Luna](#).

Таблица 59. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Salto + SaltoController	Beward	MatchByPhoto + SendToSalto
	BioSmart	MatchByPhoto + SendToSalto
	Dahua	MatchByPhoto + SendToSalto
	HikvisionCamera	MatchByPhoto + SendToSalto
	LunaFast4A1	MatchByPhoto + SendToSalto
	UniUbi	MatchByPhoto + SendToSalto
	VKVision02	MatchByPhoto + SendToSalto
	R20Face	MatchByPhoto + SendToSalto

16.2. Стандартная интеграция с использованием Salto

Интеграция Salto (Рисунок 92) и (Таблица 60).

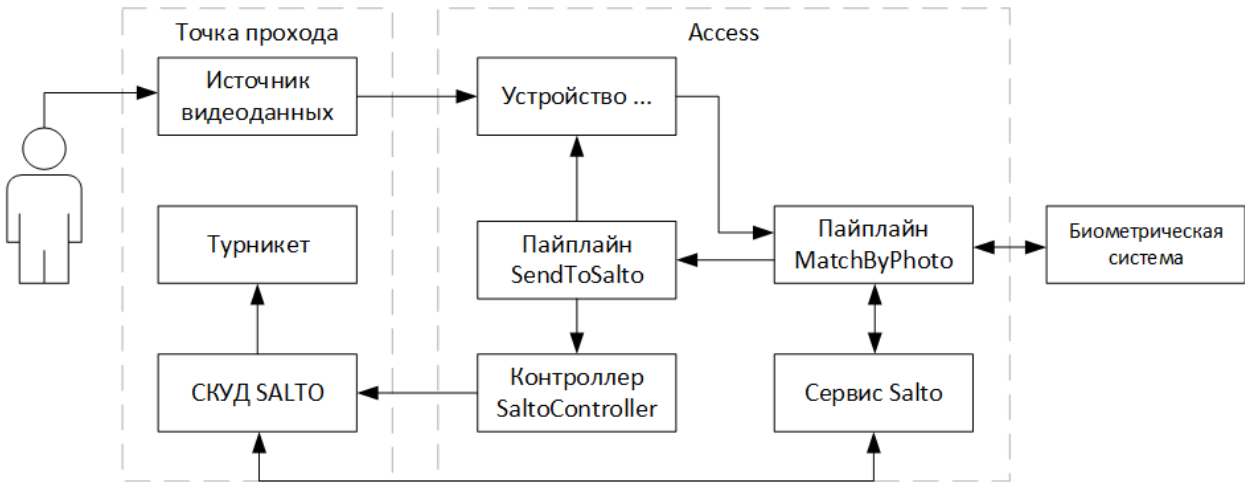


Рис. 92: Схема компонентов при 1ф интеграции с Salto

Таблица 60. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие). Биометрический терминал позволяет создать обратную связь для демонстрации человеку информации о проходе.
Турникет	Преграждающее устройство для разграничения доступов
СКУД SALTO	Центральное ПО для работы с Salto. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Контроллер SaltoController	Компонент Access для отправки в СКУД запроса на открытие двери определенной точки доступа.

Компонент	Описание
Пайплайн SendToSalto	Компонент Access для обмена данными с СКУД и передачи данных для отображения на экране устройства.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС.
Сервис Salto	Компонент Access для выполнения репликации/синхронизации сотрудников из СКУД и прослушивания событий СКУД.
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Поддерживается Luna.

16.3. Уровни доступа СКУД SALTO

В СКУД SALTO, интегрированной с LUNA Access, реализована гибкая система уровней доступа.

Уровни доступа могут назначаться как дверям, так и сотрудникам. Каждый сотрудник и каждая дверь могут иметь список идентификаторов уровней доступа.

Хранение информации:

- Уровни доступа дверей сохраняются в поле info соответствующих контроллеров в LUNA Access.
- Уровни доступа сотрудников хранятся в локальном хранилище персон.

Проверка доступа:

При попытке открытия двери LUNA Access сравнивает уровни доступа сотрудника и двери. Дверь откроется только в случае, если у сотрудника есть хотя бы один уровень доступа, совпадающий с одним из уровней, назначенных двери.

Особенности интеграции:

Запрос на открытие двери отправляется в СКУД SALTO в обезличенном виде. В событиях прохода СКУД не отображается кто именно прошёл по биометрии — событие фиксируется как открытие двери оператором СКУД.

16.4. Методы взаимодействия с Salto

Начало эндпоинта для всех запросов (Таблица 61), кроме авторизации: /grpc

Таблица 61. Используемые методы СКУД Salto

Задача	Метод	Описание
Эндпоинт авторизации	/oauth/connect/token	Запрос токена авторизации СКУД. Авторизация происходит при добавлении сервиса
Получить версию СКУД	POST /GetBootstrapConfiguration	Получить версию СКУД
Получить точки доступа СКУД	POST /GetDoorListStarting FromItem	Запрос на получение точек доступа СКУД
Получить список сотрудников в СКУД (репликация)	POST /GetUserListStarting FromItem	Запрос на получение списка всех сотрудников в СКУД
Получить список событий в СКУД (синхронизация)	POST /GetStatusOfGetSystem AuditorEventList	Запрос на получение списка последних событий в СКУД

16.5. Диаграмма процессов взаимодействия с SALTO

Диаграмма процесса (Рисунок 93).

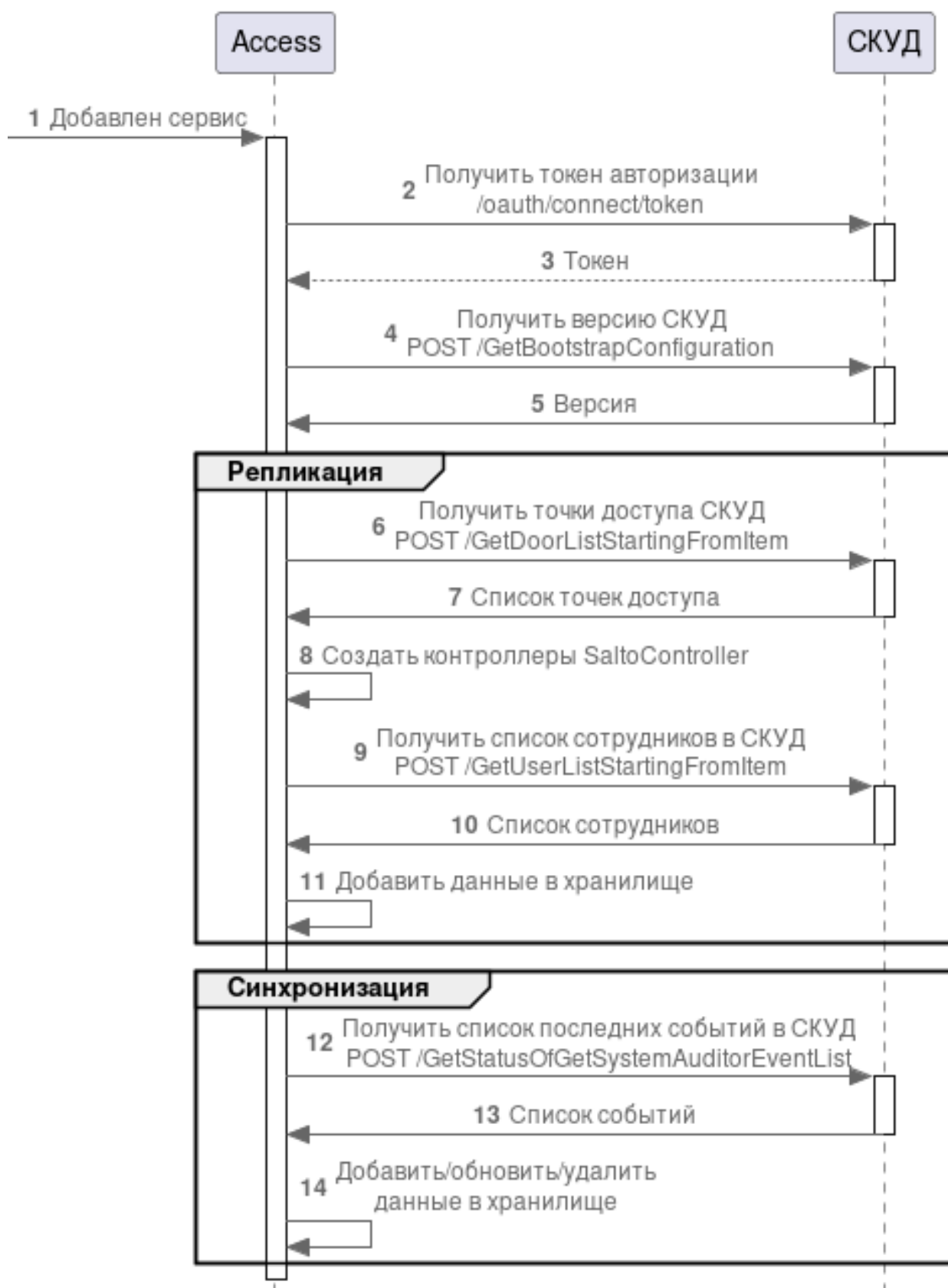


Рис. 93: Диаграмма взаимодействия SKUD SALTO с Access

1. Пользователь добавил в Access сервис Salto.
2. Access отправляет запрос на получение токена авторизации в СКУД.
3. СКУД возвращает токен для авторизации. Токен имеет время жизни, по истечению которого Access повторно выполняет авторизацию.
4. Access отправляет запрос на получение информации о СКУД.
5. СКУД возвращает информацию. Access использует только версию СКУД для проверки совместимости и вывода версии в UI.
6. Access отправляет запрос на получение точек доступа, созданных в СКУД.
7. СКУД возвращает ID точек доступа.
8. Access создает контроллеры SaltoController в соответствии с полученными ID.
9. Access отправляет запрос на получение списка сотрудников в СКУД.
10. СКУД возвращает список сотрудников.
11. Access сохраняет информацию по каждому сотруднику в локальное хранилище.
12. Access отправляет запрос каждые 10 секунд для получения событий об изменении сотрудников/дверей для выполнения синхронизации.
13. СКУД возвращает события.
14. Access добавляет/обновляет/удаляет информацию по каждому сотруднику в локальном хранилище.

17. СКУД Sigur

СКУД синхронизирует сотрудников со списком в Биометрической системе и слушает события, на основе которых решает открывать или не открывать турникет. Данные события генерируются в VL Access пайплайном SendToSigur. Используемый протокол: HTTP.

- Поддерживает версию СКУД Sigur: 1.6.3.18.s.

17.1. Поддерживаемые варианты интеграции СКУД Sigur

Программные интеграции с ПО СКУД Sigur реализованы для взаимодействия:

- с LP5 и КБС для прохода распознанных лиц через турникет/дверь с магнитным замком.
- с LUNA CARS для обеспечения контроля доступа транспортных средств при проезде через преграждающие устройства.

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

17.1.1. Варианты интеграции с LP5

В каждой интеграции с LP5 (Таблица 62) используется сервис [Luna](#).

Таблица 62. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
Sigur/ Sigur + LunaStreams	Beward	SendToSigur + MatchByPhoto + SendToDevice
	BioSmart	MatchByPhoto + SendToSigur + SendToDevice
	Dahua	MatchByPhoto + SendToSigur
	Dahua Thermo	MatchByPhoto + SendToSigur
	Fortuna315	MatchByPhoto + SendToSigur

Сервис	Устройство	Пайплайн
	HikvisionCamera	MatchByPhoto + SendToSigur
	HikvisionCamera Thermo	MatchByPhoto + SendToSigur
	HikvisionTerminal Thermo	MatchByPhoto + SendToSigur + SendToDevice
	LunaFast4A1	MatchByPhoto + SendToSigur
	Panda	MatchByPhoto + SendToSigur
	UniUbi	MatchByPhoto + SendToSigur + SendToDevice
	VKVision02	MatchByPhoto + SendToSigur + SendToDevice
	R20Face	MatchByPhoto + SendToSigur + SendToDevice

17.1.2. Варианты интеграции с КБС

В каждой интеграции с КБС (Таблица 63) используется сервис КБС.

Таблица 63. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
CbsMts + Sigur	Beward	MatchByPhoto + SendToDevice + SendToSigur
	Dahua	MatchByPhoto + SendToSigur
	HikvisionCamera	MatchByPhoto + SendToSigur
	LunaFast4A1	MatchByPhoto + SendToDevice + SendToSigur
CbsAkbars + Sigur	Beward	MatchByPhoto + SendToDevice + SendToSigur
	Dahua	MatchByPhoto + SendToSigur
	HikvisionCamera	MatchByPhoto + SendToSigur
	LunaFast4A1	MatchByPhoto + SendToDevice + SendToSigur
CbsVtb + Sigur	Beward	MatchByPhoto + SendToDevice + SendToSigur
CbsVtb + Sigur + [PersonStorage Actualization]	Dahua	MatchByPhoto + SendToSigur

Сервис	Устройство	Пайплайн
CbsVtb + Sigur + [CryptoPro]	HikvisionCamera	MatchByPhoto + SendToSigur
	LunaFast4A1	MatchByPhoto + SendToDevice + SendToSigur

Сервисы указанные в скобках, например [CryptoPro] - не являются обязательными и могут использоваться в интеграциях при необходимости.

17.1.3. Варианты интеграции с LUNA CARS

В каждой интеграции с СКУД ТС (Таблица 64) используется сервис [LunaCars](#).

СКУД ТС - Система контроля доступа на территорию автотранспорта с помощью шлагбаума.

LUNA CARS передает события детекций ТС в Access для дальнейшей обработки.

Подключение камер происходит через LUNA CARS.

Таблица 64. Варианты интеграции СКУД ТС

Дополнительный сервис	Пайплайн
Sigur	SendCarsToSigur
Sigur + LaurentController	SendCarsToLaurent

17.2. Стандартные интеграции с использованием СКУД Sigur

1. Схема интеграции Sigur для прохода распознанных лиц через турникет/дверь с магнитным замком. При интеграции с Sigur используются стандартные компоненты Access (Рисунок 94) и (Таблица 65).

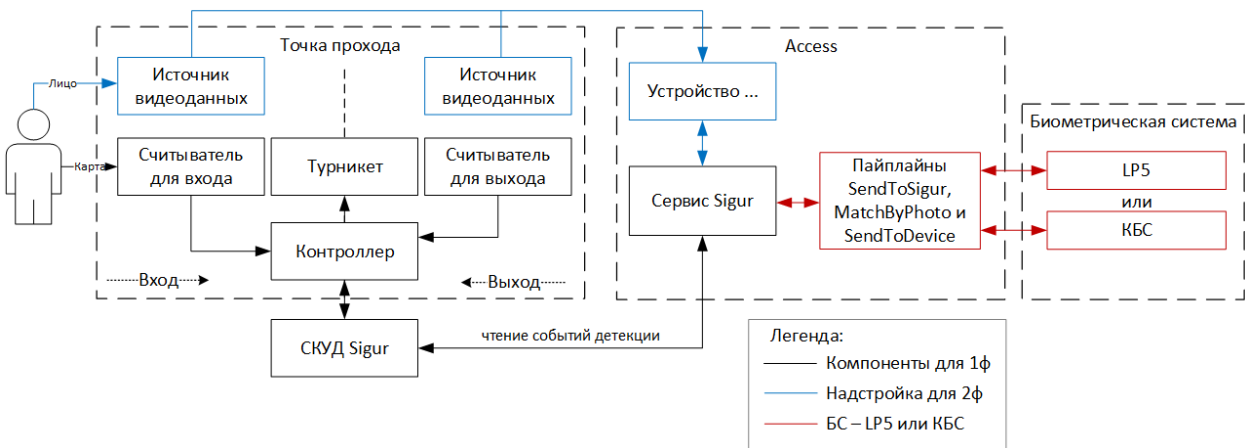


Рис. 94: Схема компонентов при интеграции с Sigur

Таблица 65. Описание интеграции

Компонент	Описание
1ф	
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключено более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Считыватель	Устройство для приема данных карты доступа.
Контроллер	Плата управления точкой прохода.
Турникет	Преграждающее устройство для разграничения доступов
СКУД Sigur	Центральное ПО для работы с Sigur. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Сервис Sigur	Компонент Access для обработки информации от СКУД.
Надстройка для 2ф	
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.

Работа с LP5 и КБС

Компонент	Описание
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС
Пайплайн SendToController	Компонент Access для взаимодействия с КБС
Пайплайн SendToDevice	Компонент Access для отправки сигнала на открытие реле в устройство и вывода текста на экран

2. Схема интеграции Sigur для обеспечения контроля доступа транспортных средств при проезде через преграждающие устройства. При интеграции с Sigur используются стандартные компоненты Access (Рисунок 95) и (Таблица 66).

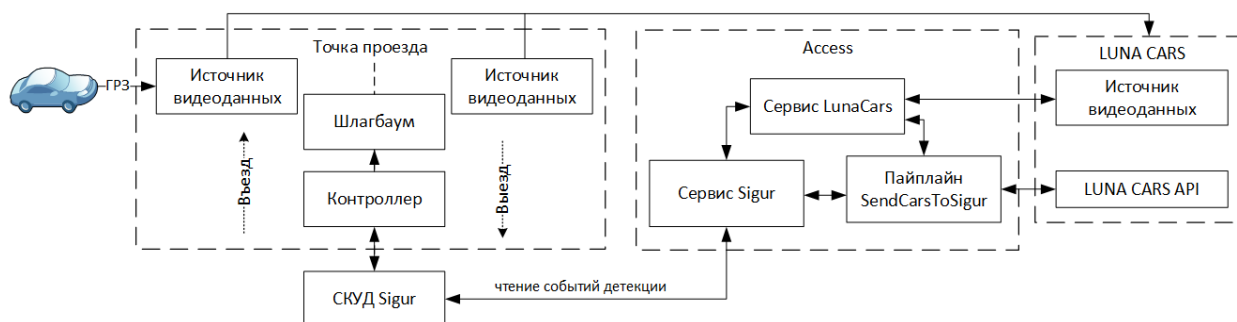


Рис. 95: Схема компонентов при интеграции с Sigur

Таблица 66. Описание интеграции

Компонент	Описание
Транспортное средство (ТС)	Автомобиль, желающий проехать через точку проезда.
Точка проезда	Набор компонентов, используемых для контроля доступа ТС. Точек прохода может быть подключено более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой источник видеоданных.
Контроллер	Плата управления точкой проезда.
Шлагбаум	Преграждающее устройство для разграничения доступов
СКУД Sigur	Центральное ПО для работы с Sigur. Хранит данные ТС и принимает решение о предоставлении доступа.

Компонент	Описание
Сервис Sigur	Компонент Access для обработки информации от СКУД.
Источник видеоданных	Устройство для извлечения кадра Государственного регистрационного знака ТС.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Работа с LUNA CARS	
Пайплайн SendCarsToSigur	Компонент Access для отправки событий из LUNA CARS в Sigur. Access подключается к LUNA CARS Analytics backend с помощью websocket
Сервис LunaCars	Компонент Access для программно-аппаратной интеграции, необходимый для связи LUNA CARS и преграждающих устройств

17.3. Настройка ПО СКУД Sigur

Для запуска и настройки ПО СКУД Sigur необходимо выполнить следующие действия:

1. Убедиться, что используется ПО СКУД Sigur версии 1.6.3.18.s или новее:
 - В меню программы управления Sigur выбрать пункт меню «Справка» → «О программе».
 - Сверить версию ПО с указанной на сайте www.sigur.com.
 - При необходимости обновить ПО до последней версии.
2. Настроить взаимодействие между модулем интеграции и сервером ПО СКУД «Sigur»:
 - В меню программы управления Sigur выбрать пункт меню «Файл» → «Настройки».
 - В диалоге «Редактирование настроек» перейти к пункту «Видеонаблюдение» (Рисунок 96).
 - Добавить сервер видеонаблюдения (Рисунок 97).

|s| Редактирование настроек

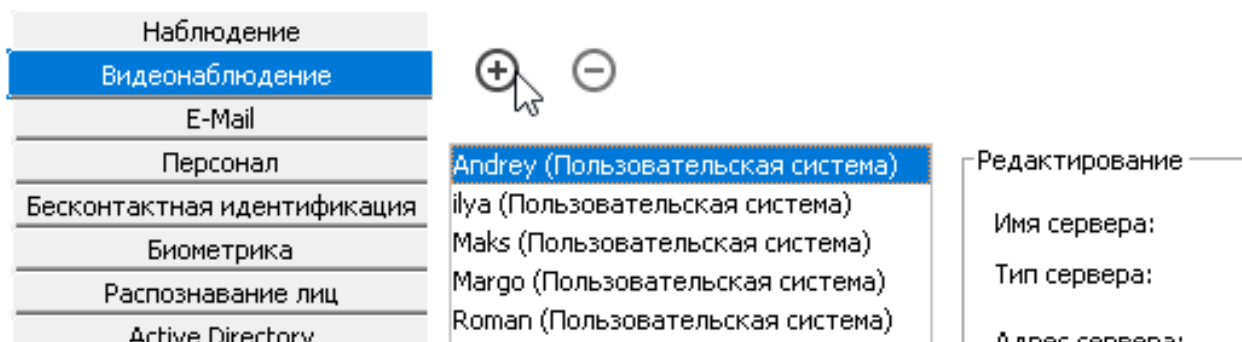


Рис. 96: Редактирование настроек Sigur

- Указать произвольное имя сервера.
- Тип сервера — «Пользовательская система».
- Нажать «Ок»;

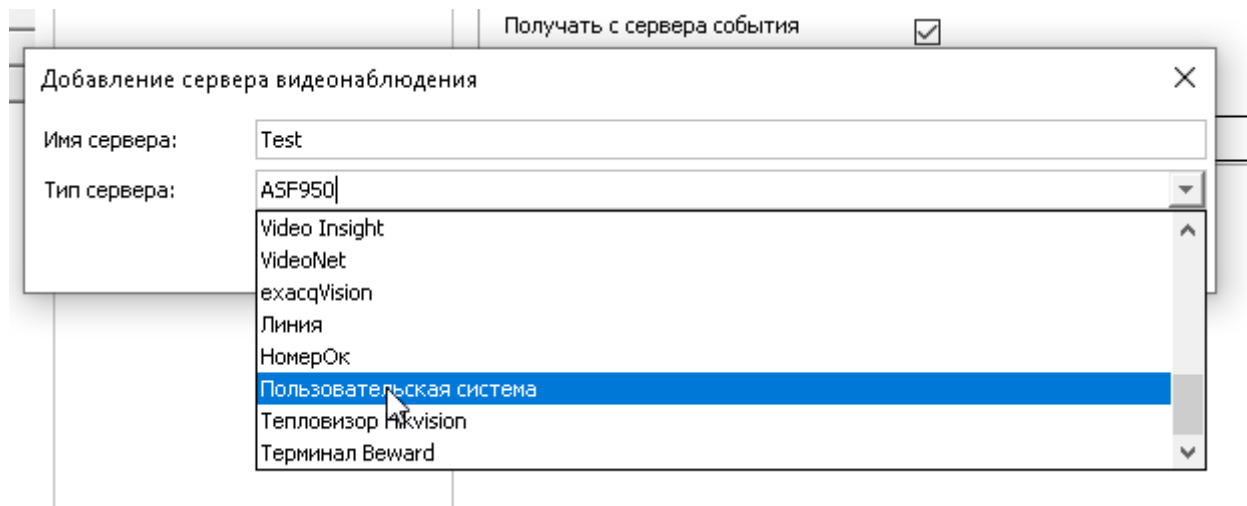


Рис. 97: Добавление сервера видеонаблюдения

3. Настроить параметры сервера (Рисунок 98):

Редактирование

Имя сервера:	<input type="text" value="Test"/>
Тип сервера:	<input type="text" value="Пользовательская система"/>
Адрес сервера:	<input type="text" value="10.0.10.161"/>
Порт сервера (HTTP):	<input type="text" value="9091"/>
Путь к сервису:	<input type="text" value="ebhook/service/sigur/f24bc9c5-fa32-4ac0-9728-07bc1178b4d9/"/>
Имя пользователя:	<input type="text"/>
Пароль пользователя:	<input type="password"/>
Аутентификация:	<input type="text" value="отключена"/>
Выгружать на сервер фотографии	<input checked="" type="checkbox"/>
Выгружать на сервер пропуска	<input type="checkbox"/>
Получать с сервера события	<input checked="" type="checkbox"/>
Выгружать на сервер доп. параметры	<input checked="" type="checkbox"/>
Доп. параметры для выгрузки	<input type="text" value="MDM_ID"/> <input type="button" value="Выбрать"/>

Рис. 98: Редактирование параметров сервера видеонаблюдения

- «Адрес сервера» и «Порт сервера (HTTP)» — используются при обращении к серверу со стороны СКУД по протоколу HTTP;
- «Адрес сервера» соответствует IP адресу машины, на которой запущен Access;
- «Порт сервера (HTTP)» — порт для интеграционного модуля (значение по умолчанию «9091», если порт уже используется — изменить);
- «Путь к сервису» задает общий префикс путей на сервере для всех запросов от СКУД. Данное значение следует взять из блока информации компонента Sigur в Access, значение поля webhook-url (Рисунок 99).

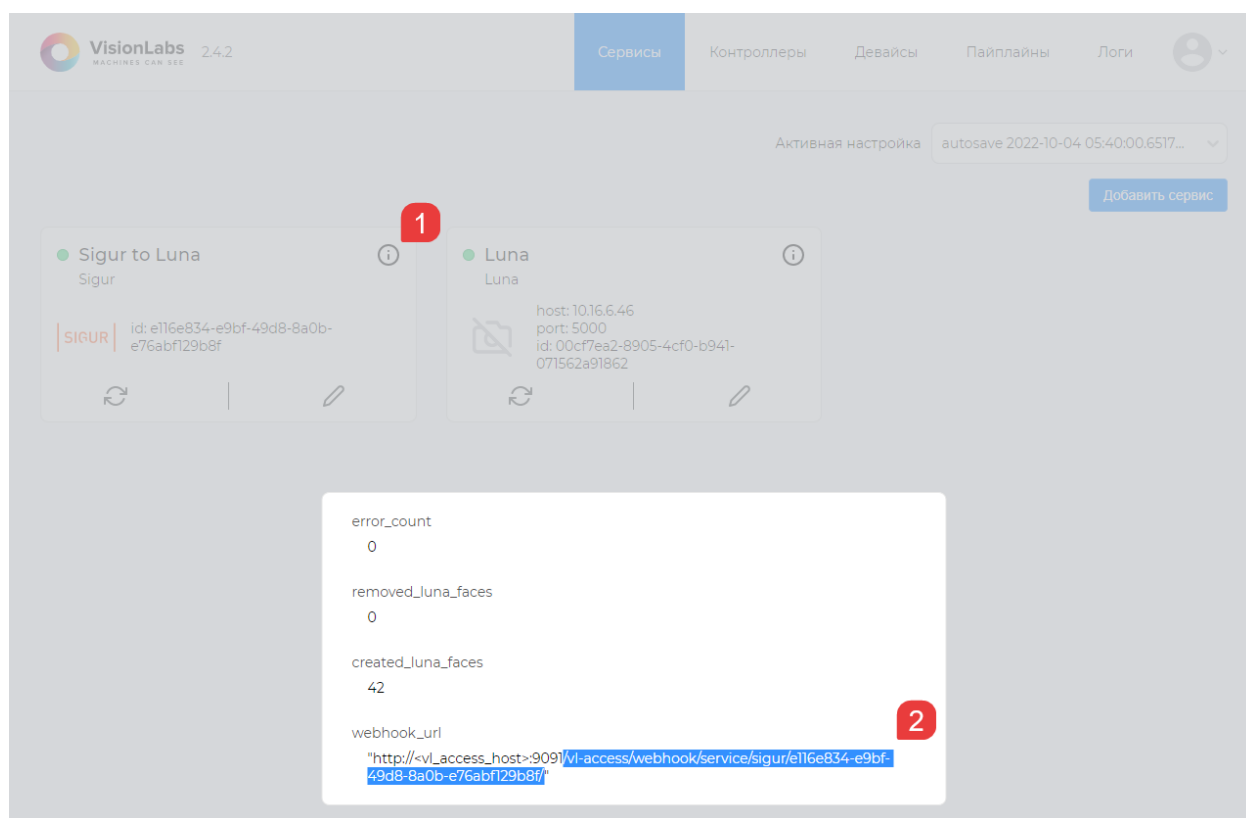


Рис. 99: Ссылка на Webhook

- Активировать флаг «Выгружать на серверов фотографии» при использовании сервиса Sigur, отключить при использовании сервиса SigurThroughDatabase.
 - Активировать флаг «Получать с сервера события».
4. Включить функцию распознавания лиц:
- В диалоге «Редактирование настроек» перейти к пункту «Распознавание лиц».
 - Установить галочку в пункте «Включить распознавание лиц» (Рисунок 100).

5

Редактирование настроек

×

Наблюдение	<input checked="" type="checkbox"/> Включить распознавание лиц ②	
1С:Предприятие		
Видеонаблюдение	Максимальная ширина кадра:	800 (*)
Печать пропусков	Максимальная высота кадра:	600 (*)
Платежная система	Минимальный размер лица в кадре (%):	5 (*)
SMS	Максимальный размер лица в кадре (%):	95 (*)
Telegram	Точность детектирования лица (%):	80 (*)
E-Mail	Точность распознавания лица (%):	80
Персонал		
Active Directory		
Оправдательные документы	Нужно негативных кадров подряд, чтобы "потерять" лицо:	5 (*)
Пропуска посетителей	Достаточно кадров подряд, в которых "не потеряно" лицо, для идентификации:	5 (*)
Архив	Достаточно миллисекунд подряд, в которых "не потеряно" лицо, для идентификации:	5000 (*)
Синхронизация данных	Алгоритм детектирования лица:	ALG1 - быстрый ▾ (*)
Dnevnik.ru	Алгоритм выделения антропометрических точек лица:	ALG1 - быстрый ▾ (*)
Распознавание документов	Алгоритм распознавания лица:	ALG1 - быстрый ▾ (*)
Биометрика		
Беспроводные замки		
Устройства хранения		
Mifare и BLE		
Зоны		
Повторные проходы		
Дополнительные параметры		
Распознавание лиц ①		
HTTP(WEB)		

(*) - относится только к встроенному распознаванию лиц Sigur.

Рис. 100: Включение функции распознавания лиц в настройках системы

17.3.1. Настройка точек доступа в Sigur

При возникновении ошибок перезапустите сервер ПО СКУД Sigur, чтобы он смог подключиться к интеграционному модулю.

Для настройки точек доступа в Sigur необходимо выполнить следующие действия:

1. В боковом меню программы управления Sigur выбрать пункт «Оборудование» (Рисунок 101).

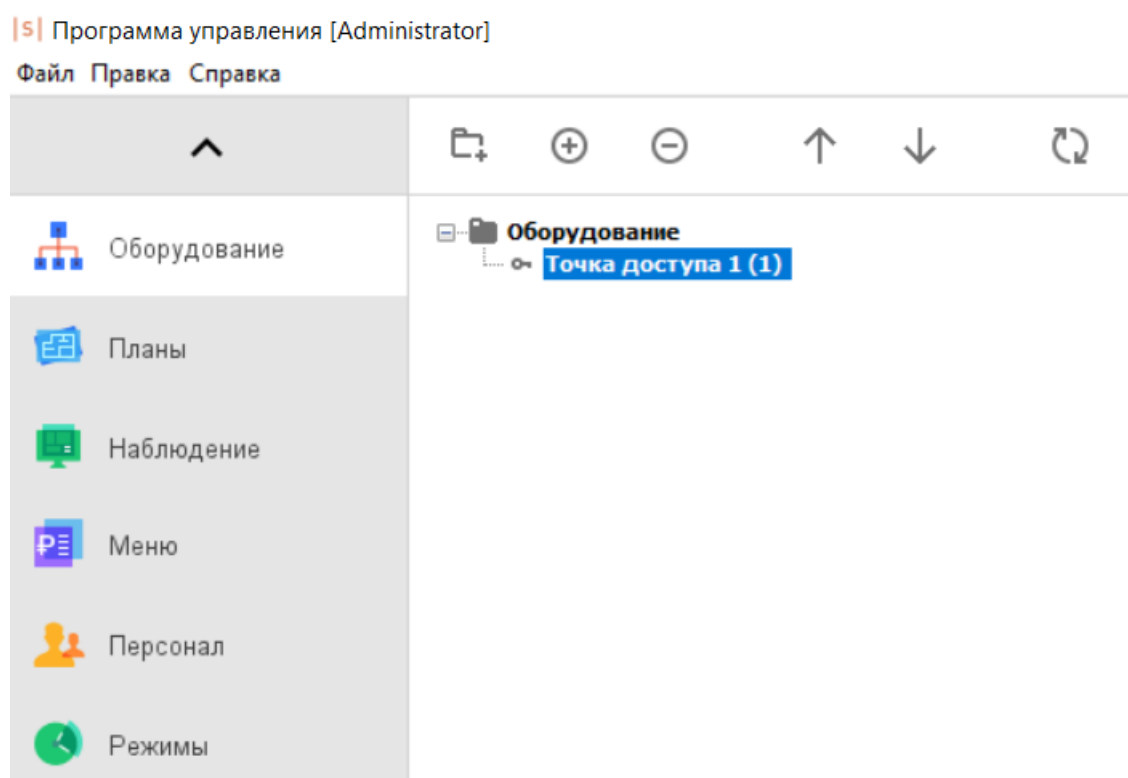


Рис. 101: Боковое меню программы управления Sigur

2. Выбрать требуемую точку доступа и настроить для неё параметры видеонаблюдения (Рисунок 102):

The screenshot shows a software configuration window. At the top, a status box displays 'Состояние: Есть связь. Нормальный режим.' Below this, the 'Настройки:' section has two tabs: 'Основные' and 'Видеонаблюдение'. The 'Видеонаблюдение' tab is active, showing settings for two cameras: 'Камера "на выход"' and 'Камера "на вход"'. The 'Камера "на выход"' settings are visible, including a system selection dropdown set to 'demo_luna (Пользовательская система)', a camera selection dropdown set to 'demo_hik', and an offset value of 5. There are three checkboxes: 'Распознавание автомобильных номеров' (unchecked), 'Разрешить верификацию по лицу' (checked), and 'Включить идентификацию по лицу' (checked). At the bottom of the settings panel are 'Применить' and 'Отменить' buttons. Below the settings panel are three buttons: 'автономная память', 'доступ', and 'настройки'.

Рис. 102: Настройка параметров оборудования видеонаблюдения

- «Система» — выбрать название созданной пользовательской системы;
- «Камера» — выбрать камеру. При нажатии на выпадающий список в нём должны отобразиться названия всех устройств, созданных в Access, это говорит о том, что интеграция работает исправно и Sigur удалось подключиться к Access. Выбрать устройство, которое используется для идентификации нужной точки доступа;
- Активировать флаги «Разрешить верификацию по лицу» и «Включить идентификацию по лицу»;
- Нажать кнопку «Применить».

После этого, должна начаться репликация сотрудников со стороны Sigur. Описание работы алгоритма репликации см. в разделе [Диаграмма взаимодействия СКУД Sigur с LUNA Access](#).

17.3.2. Настройка режимов доступа в ПО СКУД Sigur

В СКУД реализовано два режима идентификации в выбранном направлении:

- Режим 1ф - по факту распознавания лица объекта доступа
- Режим 2ф - по основному идентификационному признаку (карта) и по лицу объекта доступа

Для настройки ПО выполните следующие действия:

1. В программе управления Sigur в боковом меню «Оборудование» выберете необходимую точку доступа и перейдите в настройки видеонаблюдения (Рисунок 103):

Рис. 103: Настройка параметров оборудования видеонаблюдения

Для включения режима 1ф: активируйте флаг «Включить идентификацию по лицу».

Для включения режима 2ф: активируйте флаг «Разрешить верификацию по лицу».

2. Перейдите на вкладку «Режимы» и, создав новый или выбрав нужный из уже существующих, перейти на вкладку «Специальные правила» (Рисунок 104):

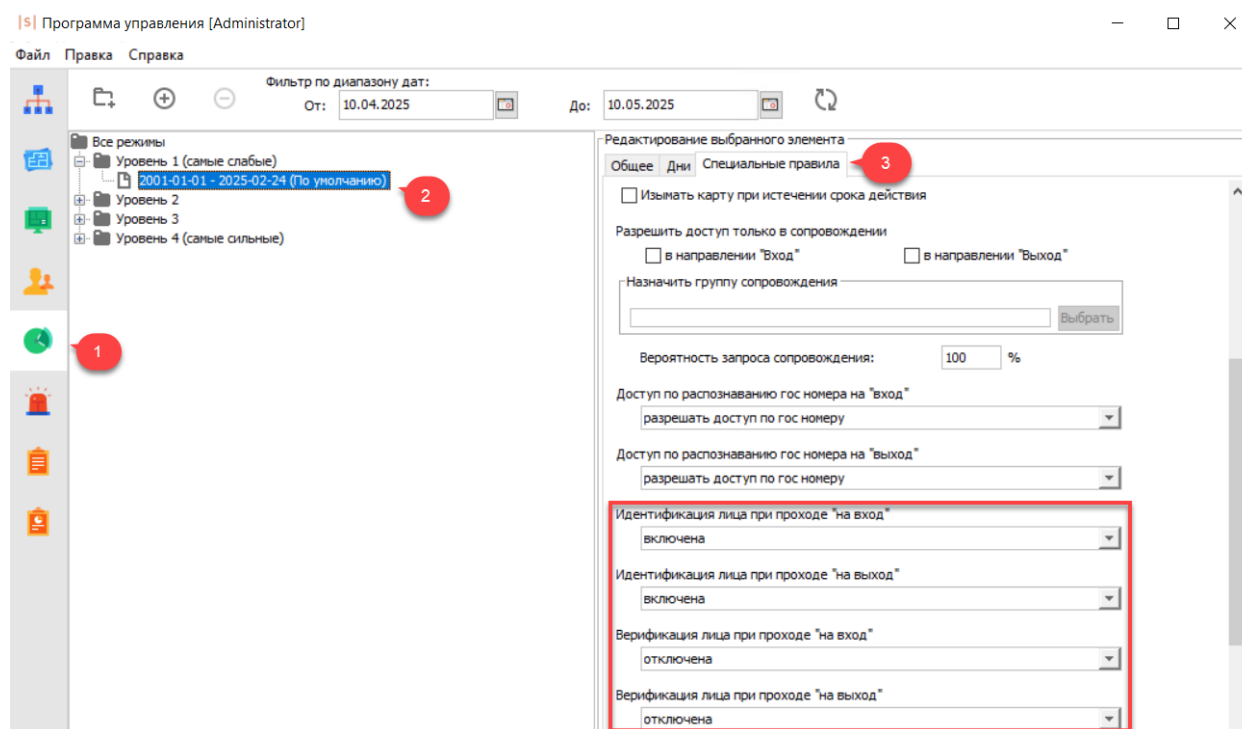


Рис. 104: Настройка специальных правил прохода

Для работы в режиме 1ф: Если в каком-либо из направлений должен осуществляться доступ только по факту распознавания лиц, то для параметров «Идентификация лица при проходе «на вход/выход» установите значение «Включена».

Для работы в режиме 2ф: Если в каком-либо из направлений должен осуществляться доступ по факту предъявления основного идентификатора сотрудника и факта распознавания его лица, то для параметров «Верификация лица при проходе «на вход/выход» установите одно из следующих значений:

- Мягкая — пропускать в любом случае. После идентификации по основному признаку (поднесение карты) система предоставляет допуск, если он возможен по иным критериям, даже если человек в кадре так и не появился. Такое разрешение доступа будет сопровождаться событием «Лицо не опознано».
- Жёсткая — пропускать только при совпадении. После идентификации по основному признаку (поднесение карты) система проверяет, узнавалось ли лицо данного человека в кадре в течение указанного в настройках времени до события, и если нет, ждёт появления человека в кадре в течение 5 секунд. Если человек в кадре так и не появился, доступ не предоставляется. На вкладке «Наблюдение» в ПО выводится событие: «Доступ запрещен. Лицо не опознано».
- Жёсткая групповая — пропускать только при совпадении с лицом из отдела. После идентификации по основному признаку (поднесение карты) система проверяет, узнавалось ли лицо

человека в кадре в течение указанного в настройках времени до события, и если нет, ждет появления человека в кадре в течение 5 секунд. Обнаруженное лицо проверяется на соответствие любому из лиц, находящихся в том же отделе, что и идентифицированный объект. Если человек в кадре так и не появился, доступ не предоставляется. На вкладке «Наблюдение» в ПО выводится событие: «Доступ запрещен. Лицо не опознано».

- Мягкая групповая — пропускать при несовпадении с лицом из отдела. После идентификации по основному признаку система предоставляет допуск, если он возможен по иным критериям, даже если лицо идентифицированного или любого другого субъекта того же отдела так и не появилось. Такое разрешение доступа будет сопровождаться событием «Лицо не опознано».

17.4. Методы взаимодействия с Sigur

Для обмена данными с СКУД используется API (Таблица 67).

Таблица 67. Используемые методы СКУД Sigur

Метод	Описание
GET /event	Получение событий детекции. Однонаправленное стрим соединение, в котором Access транслирует возникающие события детекций для СКУДа.
GET /getpersons	Получить список сотрудников из Access. На основе ответа этого запроса, СКУД принимает решение о дальнейшем добавлении/обновлении/удалении сотрудников в Access
POST /updateprson {id, name, photoVersion, photo}	Обновить данные сотрудника в Access
GET /removeperson {id}	Удалить данные сотрудника в Access
GET /getchannels	Получить список источников событий в Access, используется для конфигурации направлений прохода

17.5. Диаграмма процессов взаимодействия с Sigur

Access выступает в роли сервера, а Sigur в роли клиента. После настройки клиента, СКУД Sigur самостоятельно выполняет все запросы к Luna Access (Рисунок 105).

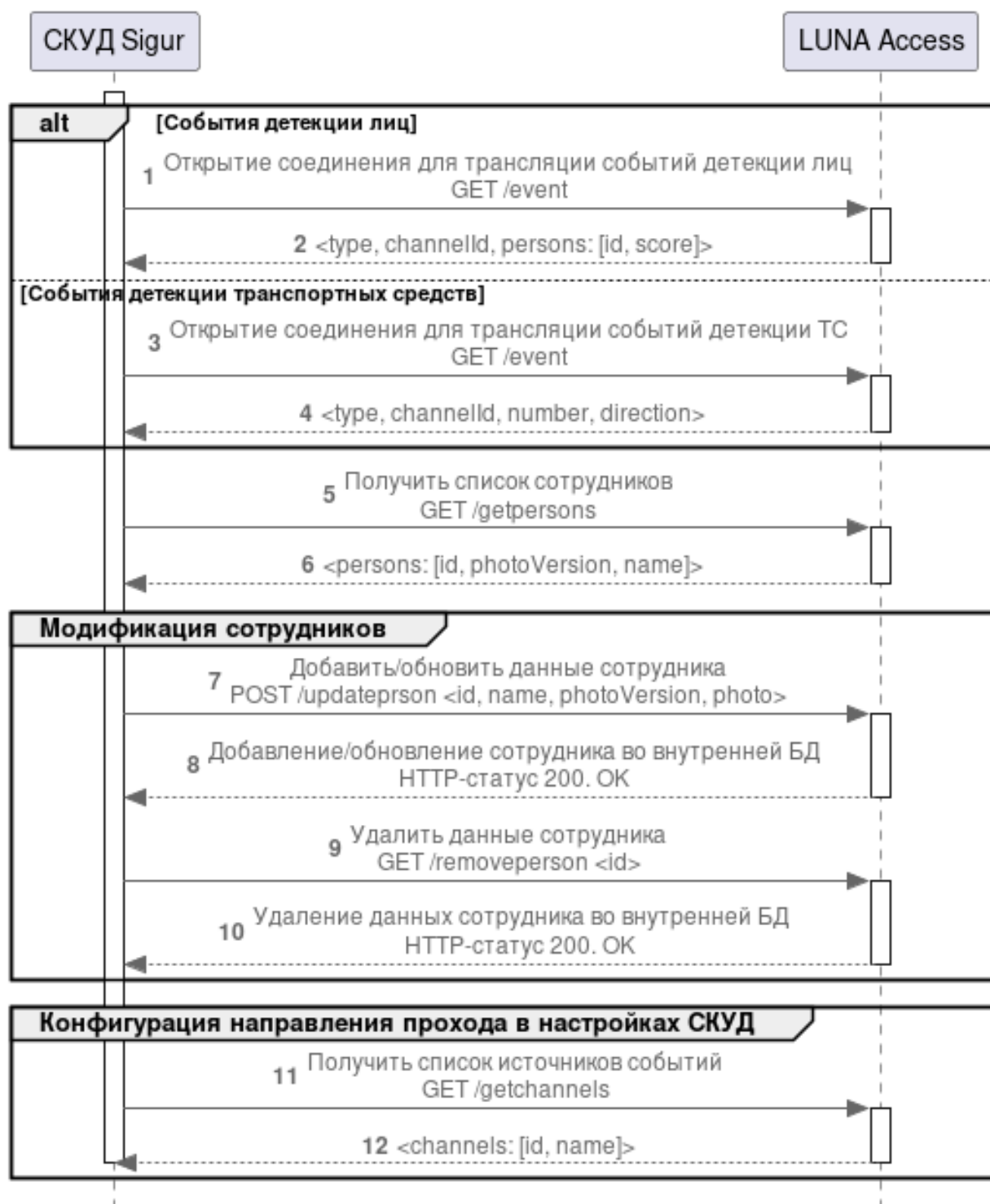


Рис. 105: Диаграмма взаимодействия СКУД Sigur с Access

События детекции лиц

1. СКУД Sigur инициирует GET-запрос: /event для получения событий детекции лиц от Access, со-

единение всегда остается открытым.

2. Access возвращает в соединение события по мере того как они возникают. Даже если событий нет, Access раз в 5 секунд присылает искусственное «Keep alive» событие, чтобы обе стороны соединения были уверены, что соединение все еще в порядке. Access возвращает json-объект события, с полями:

- type - Тип события;
- channelId - ID канала в Access;
- persons - Массив с результатами распознавания;
 - id - ID персоны;
 - score - Степень схожести как вещественное число от 0 до 1.

События детекции ТС

3. СКУД Sigur инициирует GET-запрос: /event для получения событий детекции ТС от Access, соединение всегда остается открытым (Access присылает новые события в СКУД по мере возникновения).
4. Access возвращает в соединение события по мере того как они возникают. Даже если событий нет, Access раз в 5 секунд присылает искусственное «Keep alive» событие, чтобы обе стороны соединения были уверены, что соединение все еще в порядке. Access возвращает json-объект события, с полями:

- type - Тип события;
- channelId - ID канала в Access;
- number - Строка распознанного Государственного регистрационного знака ТС;
- direction - Направление вертикального движения автомобиля в кадре. Не обязательное поле, может отсутствовать. Если присутствует, то может принимать значения «up» или «down».

Получение списка сотрудников

5. СКУД Sigur инициирует GET-запрос: /getpersons для синхронизации данных с Access. Запрос выполняется при старте сервера СКУД и при изменении каких либо синхронизируемых данных на стороне СКУД. В случае если запрос или последующие за ним запросы завершатся неудачно, СКУД будет пытаться раз в 5 секунд повторить запрос до тех пор пока синхронизация не пройдет без ошибок.
6. Access возвращает json-объект, с полями:
 - id - ID сотрудника;
 - photoVersion - Текущая «версия фотографии» сотрудника в Access, значением поля выступает время обновления фотографии в СКУД в формате timestamp (unix формат);
 - name - Имя сотрудника.

Модификация сотрудников

7. СКУД Sigur инициирует POST-запрос: /updateperson для добавления или обновления данных сотрудника в Access. В теле запроса передается json-объект с полями:

- `id` - ID сотрудника в СКУД, целое число от 1 до $2^{31}-1$;
 - `name` - Имя сотрудника;
 - `photoVersion` - Текущая «версия фотографии» сотрудника в Access, значением поля выступает время обновления фотографии в СКУД в формате timestamp (unix формат);
 - `photo` - Фотография в формате JPEG, закодированная в base64.
8. Access ищет в своей базе сотрудника с указанным `id`. Если такой есть, то его данные должны быть обновлены для приведения в соответствие с переданными. Если такого нет, то он должен быть создан. В случае успеха Access возвращает HTTP-статус 200. OK. При неудаче СКУД досрочно прервет синхронизацию данных, т. е. перестанет исполнять `updateperson` и `removeperson` запросы, новую попытку СКУД совершит через 5 секунд.
9. СКУД Sigur инициирует GET-запрос: `/removeperson` для удаления данных сотрудника в Access. В теле запроса передается json-объект с полем:
- `id` - ID удаляемого сотрудника.

Конфигурация направления прохода

10. Access ищет в своей базе сотрудника с указанным `id` и удаляет его данные. В случае успеха Access возвращает HTTP-статус 200. OK. При неудаче СКУД досрочно прервет синхронизацию данных, новую попытку СКУД совершит через 5 секунд.
11. СКУД Sigur инициирует GET-запрос: `/getchannels` для выявления каналов устройств видеонаблюдения созданных в Access. Запрос выполняется при выполнении пользователем в интерфейсе СКУД действий по конфигурированию связи каналов и точек прохода.
12. Access возвращает json-объект «channels», с полями:
- `id` - ID канала;
 - `name` - Название канала.

Связь каналов и точек прохода происходит в пользовательском интерфейсе СКУД.

17.6. Sigur FAQ

1. Почему пуст выпадающий список в поле **bio_system_id** при настройке параметров подключения сервиса Sigur?
 - Необходимо проверить наличие добавленного сервиса биометрической системы, он должен быть поддерживаемого типа. Поддерживаемые типы: [Luna](#), [CbsMts](#).
2. Почему пуст выпадающий список в поле **luna_cars_id** при настройке параметров подключения сервиса Sigur?
 - Необходимо проверить наличие добавленного сервиса [LunaCars](#).
3. Почему после настройки Sigur не началась синхронизация сотрудников?
 - Для того, чтобы данные синхронизировались должны быть выполнены следующие пункты:

- Включено распознавание в настройках ПО СКУД;
- Включено распознавание в оборудовании. В настройках точки доступа должна быть привязана камера и установлена галочка для необходимого режима (идентификация или верификация);
- У сотрудника должен быть доступ на эту точку доступа;
- У сотрудника должен быть режим доступа, в котором включён необходимый режим идентификации;
- Триггером запуска синхронизации сотрудников может являться любое редактирование любого сотрудника.

18. СКУД STRAZH

Выполняет репликацию данных пользователей из СКУД в указанный список Биометрической системы и генерирует контроллеры StrazhController из полученного списка устройств для последующего выполнения запросов на вход или выход.

- Поддерживает версию СКУД: 1.2.211201.648.

Интеграция поддерживает работу в режиме 1ф и 2ф.

18.1. Поддерживаемые варианты интеграции СКУД STRAZH

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

Перенос данных пользователей из СКУД в LP5 происходит с помощью двух механизмов:

- репликация - механизм первоначального переноса данных пользователей;
- синхронизация - механизм периодического переноса данных пользователей при изменении состава/данных пользователей.

Настройку синхронизации/репликации см. в настройках сервисов.

В каждой интеграции с LP5 (Таблица 68) используется сервис [Luna](#).

Если терминал не имеет средств вывода данных (например, экрана), пайплайн [SendToDevice](#) не требуется.

Таблица 68. Варианты интеграции с LP5

Сервис	Устройство	Пайплайн
1f		
Strazh + StrazhController	LunaFast4A1	MatchByPhoto + SendToDevice + SendToController
2f		
Strazh + StrazhController	Beward	Strazh2FA + MatchByPhoto
	BioSmart	Strazh2FA + MatchByPhoto
	Dahua	Strazh2FA + MatchByPhoto
	Dahua Thermo	Strazh2FA + MatchByPhoto
	Fortuna315	Strazh2FA + MatchByPhoto
	HikvisionCamera	Strazh2FA + MatchByPhoto

Сервис	Устройство	Пайплайн
	HikvisionCamera Thermo	Strazh2FA + MatchByPhoto
	HikvisionTerminal Thermo	Strazh2FA + MatchByPhoto
	LunaFast4A1	Strazh2FA + MatchByPhoto
	Panda	Strazh2FA + MatchByPhoto
	UniUbi	Strazh2FA + MatchByPhoto
	VKVision02	Strazh2FA + MatchByPhoto
	R20Face	Strazh2FA + MatchByPhoto

В каждой интеграции с КБС (Таблица 69) используется сервис КБС.

Таблица 69. Варианты интеграции с КБС

Сервис	Устройство	Пайплайн
1f		
CbsMts + Strazh + StrazhController	Beward	MatchByPhoto + SendToDevice + SendToController
2f		
CbsMts + Strazh + StrazhController	Beward	MatchByPhoto + Strazh2FA
	Dahua	MatchByPhoto + Strazh2FA
	HikvisionCamera	MatchByPhoto + Strazh2FA
	LunaFast4A1	MatchByPhoto + Strazh2FA
	UniUbi	MatchByPhoto + Strazh2FA

18.2. Стандартная интеграция с использованием СКУД STRAZH

При интеграции с STRAZH используются стандартные компоненты Access (Рисунок 106) и (Таблица 70).

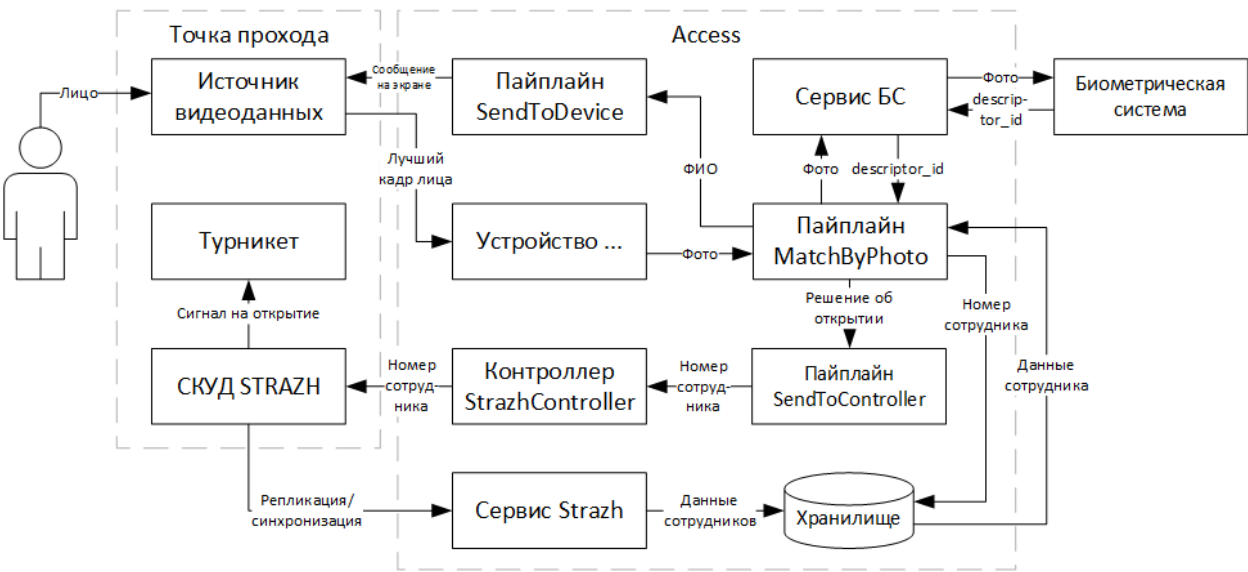


Рис. 106: Схема компонентов при 1ф интеграции

Таблица 70. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream. Биометрический терминал позволяет создать обратную связь для демонстрации человеку информации о проходе.
Контроллер	Плата управления точкой прохода.
Турникет	Преграждающее устройство для разграничения доступов
СКУД STRAZH	Центральное ПО для работы с Strazh. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Сервис Strazh	Компонент Access для обработки информации от СКУД

Компонент	Описание
Контроллер StrazhController	Компонент Access для взаимодействия с контроллером СКУД. Для каждого считывателя должен быть создан отдельный контроллер.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных. Может быть либо Luna, либо поддерживая КБС.
Пайплайн SendToController	Компонент Access для отправки номера карты и ФИО в StrazhController с после матчинга человека и подтверждения номера карты в Access.
Хранилище	Локальная система хранения связей между персонами СКУД и их биометрическими данными.

Интеграция 2ф (Рисунок 107) и (Таблица 71).

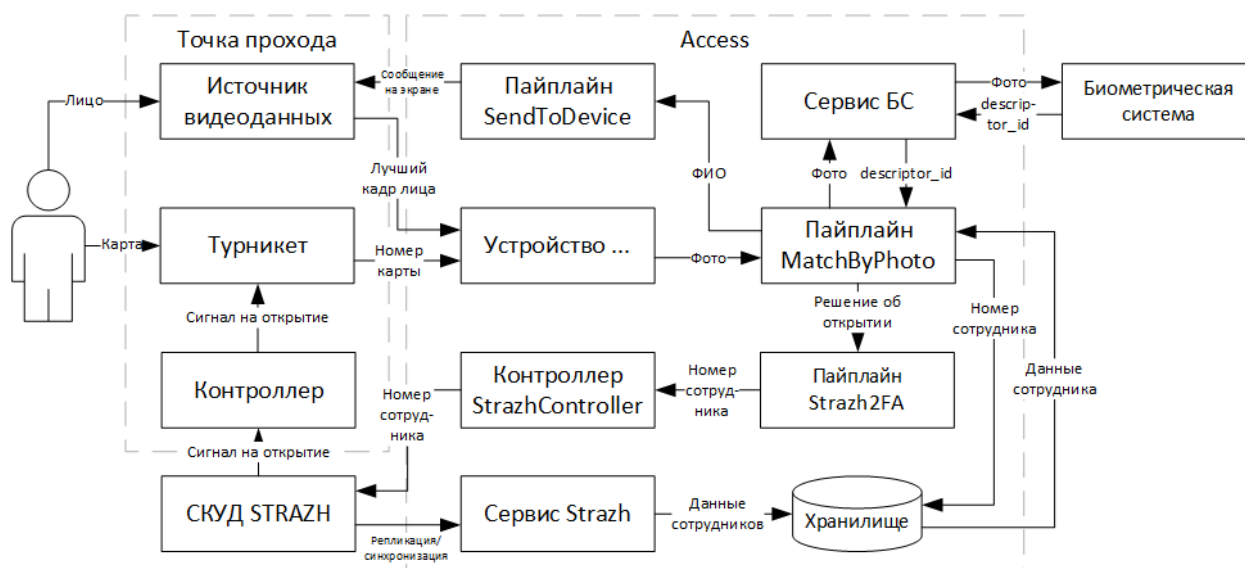


Рис. 107: Схема компонентов при 2ф интеграции

Таблица 71. Описание интеграции

Компонент	Описание
Человек	Персона, желающая пройти через точку прохода.
Точка прохода	Набор компонентов, используемых для контроля доступа человека. Точек прохода может быть подключена более одной, ограничивается лицензией на СКУД. Точка прохода может использовать как на вход, так и на выход. Для каждого направления используется свой считыватель и источник видеоданных.
Источник видеоданных	Устройство для извлечения кадра лица человека. Может быть как биометрический терминал (LUNA FAST 4A1 и другие), либо камера, подключенная через FaceStream. Биометрический терминал позволяет создать обратную связь для демонстрации человеку информации о проходе.
Контроллер	Плата управления точкой прохода.
Устройство ...	Компонент Access для получения данных от источника видеоданных. Выбирается исходя из используемого устройства.
Пайплайн MatchByPhoto	Компонент Access для взаимодействия с БС. При работе с биометрическим терминалом необходимо дополнительно подключать пайплайн SendToDevice
Сервис БС	Компонент Access для взаимодействия с Биометрической системой: для LP5 это Luna , для КБС - соответствующий сервис КБС.
Биометрическая система	Система сравнения эталонного фото персоны и лучшего кадра, полученного от источника видеоданных.
Сервис Strazh	Компонент Access для обработки информации от СКУД
Пайплайн Strazh2FA	Компонент Access для обмена данными с СКУД
Контроллер StrazhController	Компонент Access для взаимодействия с контроллером СКУД. Для каждого считывателя должен быть создан отдельный контроллер.
СКУД STRAZH	Центральное ПО для работы с Strazh. Хранит данные сотрудников и принимает решение о предоставлении доступа.
Турникет	Преграждающее устройство для разграничения доступов
Хранилище	Локальная система хранения связей между персонами СКУД и их биометрическими данными.

18.3. Настройка ПО СКУД STRAZH для двухфакторной авторизации

В СКУД реализованы уровни привилегий. Для работы 1ф и 2ф авторизации уровень привилегий точки прохода должен быть равен уровню сотрудника, иначе будет отказано в доступе.

При наличии у сотрудника уровня привилегии больше, чем у точки прохода, авторизация будет происходить только по 1ф (по карте).

Для настройки ПО выполните следующие действия:

1. Перейдите в Настройки СКД > Точки прохода > Создать новую (если не создана).
2. Введите необходимые данные точки прохода при необходимости.

На этом процесс настройки 1ф авторизации завершен, выполните шаги 3-5 если планируется 2ф.

3. Нажмите вкладку «Дополнительные параметры» и добавьте «Подтверждение похода внешней системой» с значением «Да».
4. Добавьте параметр «Максимальное время ожидания подтверждения прохода внешней системой».
5. Скорректируйте таймаут ожидания ответа внешней системы и решение по умолчанию, если система не успевает обработать запрос.

После этого при попытке пройти через эту точку с картой у которой уровень привилегий меньше уровня привилегий точки, через механизм SSE будет отправлено событие с type: `access_confirmation` и data в виде JSON объекта с полями `request` и `response`.

В `request` содержится запрос на поход, в `response` находится предварительное решение СКУД о возможности похода (т.е. решение после стандартных проверок профиля, расписания и т.д.).

Далее СКУД ожидает, что ему отправят решение о походе путем HTTP POST на `/access_confirmation` с указанием UUID запроса и решением пускать или нет.

Вне зависимости от решения СКУД в `response` внешняя система может пускать и не пускать.

18.4. Методы взаимодействия с STRAZH

Для обмена данными с СКУД используется API (Таблица 72).

Таблица 72. Используемые методы СКУД STRAZH

Задача	Метод	Описание
Авторизоваться	POST <code>/api/v1/login/</code>	Авторизация Access в СКУД. Авторизация происходит при добавлении сервиса и по истечению токена

Задача	Метод	Описание
Получить инфо о СКУД	GET /api/v1/info	Получение версии СКУД для проверки совместимости и отображения в UI.
Получить сотрудников	GET /api/v1/staff	Репликация и синхронизация сотрудников (person_id, ФИО, фото) из СКУД в локальное хранилище
Получить информацию о сотруднике	GET /api/v1/staff/{person_id}	Получение данных сотрудника из СКУД (ФИО, фото)
Получить фото сотрудника	GET /api/v1/images/{person_id}	Получение фото сотрудника из СКУД для отправки в биометрическую систему
Получить точки доступа	GET /api/v1/access_points	Получение ID точек доступа (контроллеров) для ручного сопоставления камер/терминалов и точек доступа
Открыть точку прохода	POST /api/v1/request_access	Отправка сигнала на проход в контроллер для предоставления доступа.
Подтвердить 2ой фактор	POST /api/v1/access_confirmation	Отправка в СКУД подтверждение о прохождении проверки по второму фактору (фото)
Открыть SSE соединение	GET /sse	Открыть SSE соединение для просмотра очереди событий (считывание, обновление данных сотрудников)

18.5. Диаграммы процессов взаимодействия с STRAZH

18.5.1. Подключение сервиса Strazh

Диаграмма процесса (Рисунок 108).

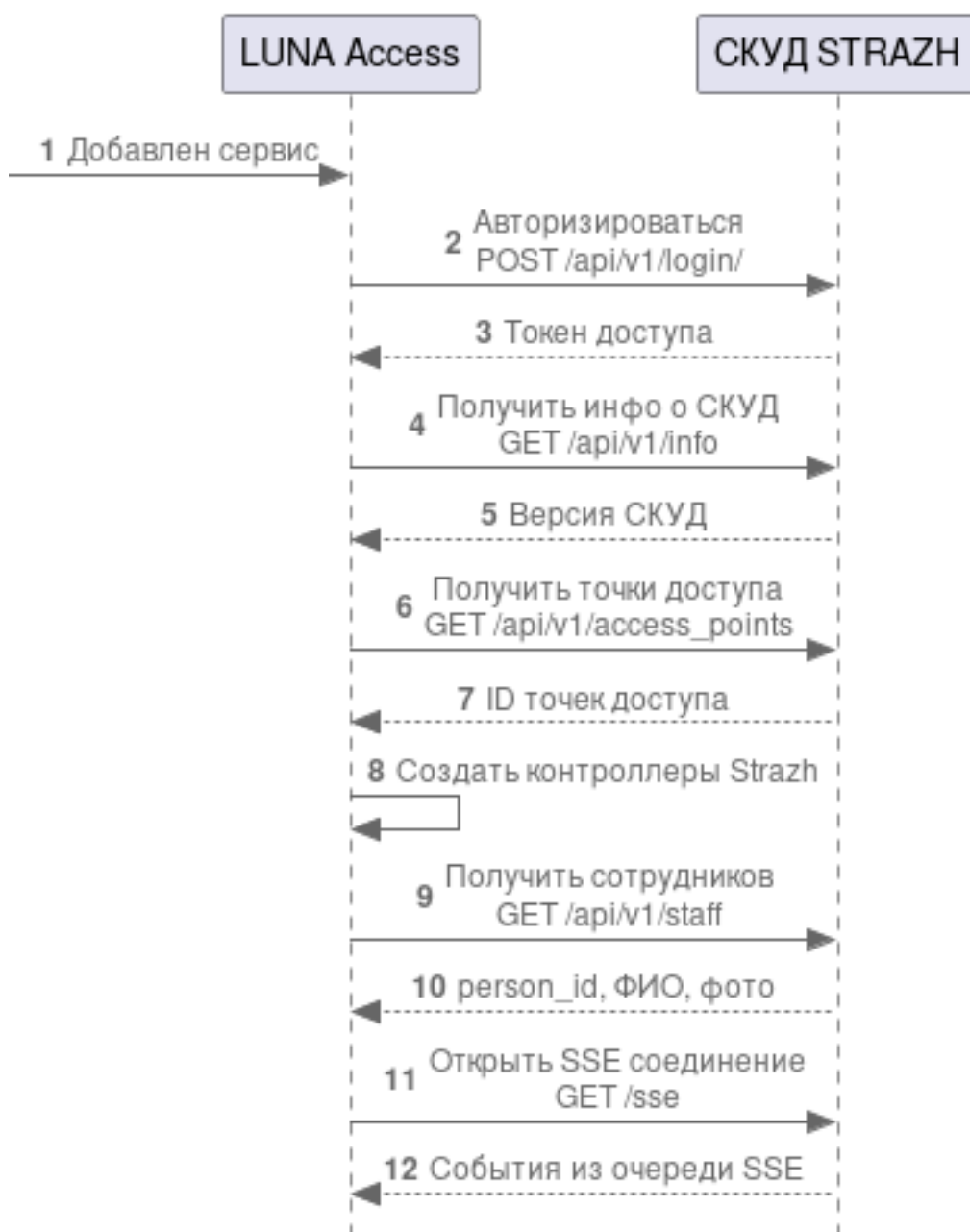


Рис. 108: Диаграмма процессов при подключения СКУД

1. Пользователь добавил в Access сервис Strazh.
2. Access отправляет запрос на авторизацию в СКУД.
3. СКУД возвращает токен для авторизации. Токен имеет время жизни, по истечению которого Access повторно выполняет авторизацию.
4. Access отправляет запрос на получение информации о СКУД.
5. СКУД возвращает информацию. Access использует только версию СКУД для проверки совме-

стимости и информации пользователя в UI.

6. Access запрашивает инфо о точках доступа (контроллерах), подключенных к СКУД.
7. СКУД возвращает ID точек прохода.
8. Access создает контроллеры StrazhController в соответствии с полученными ID.
9. Access отправляет запрос на получение информации о сотрудниках для репликации данных в локальное хранилище.
10. СКУД возвращает person_id, ФИО и фото.
11. Access отправляет запрос на открытие SSE соединения для просмотра списка событий (изменение в сотрудниках, проход).
12. СКУД открывает SSE соединение с Access.

18.5.2. Модификация сотрудников в СКУД STRAZH

Диаграмма процесса (Рисунок 109).

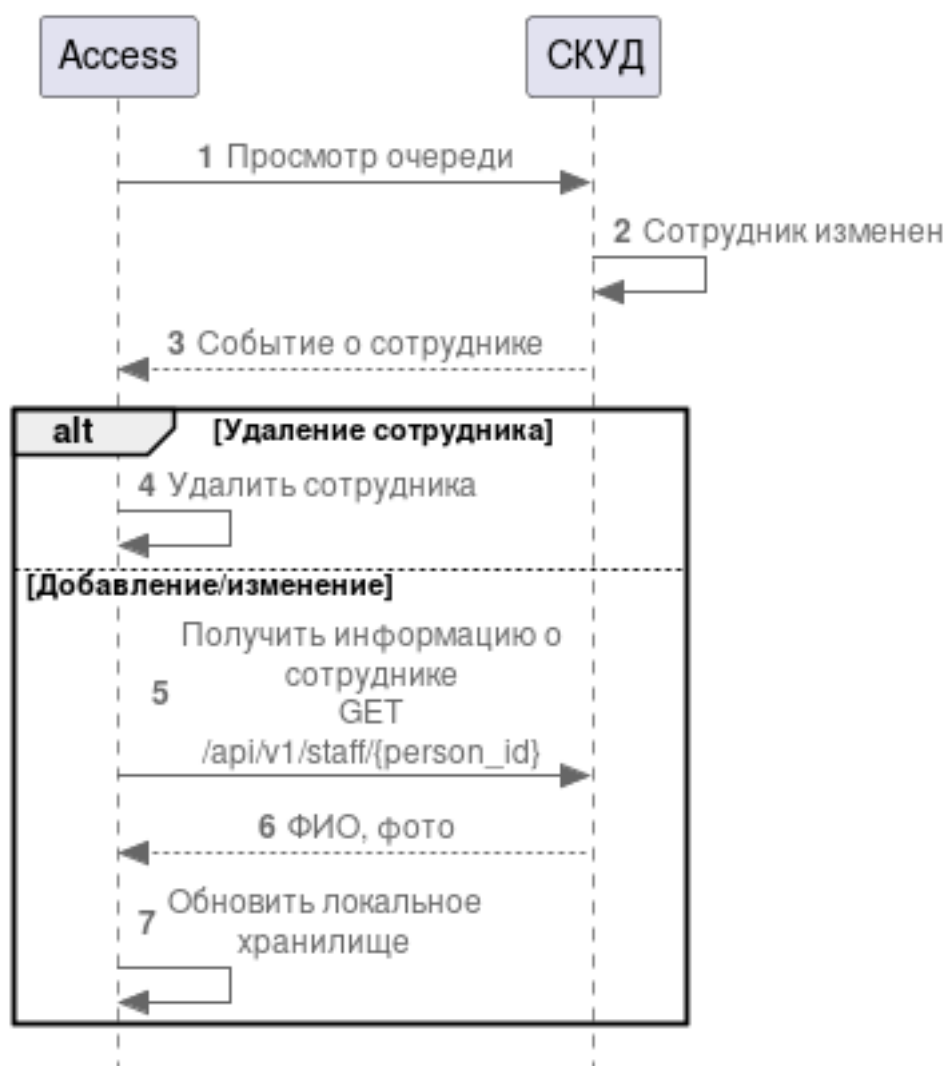


Рис. 109: Диаграмма процессов при изменении сотрудников в СКУД

1. Access просматривает очередь событий в СКУД по SSE соединению.
2. Сотрудник изменен в СКУД (добавлен, изменен или удален).
3. Access находит в очереди события с тегами CREATE, MODIFY_DATA или DELETE.
4. Access удаляет из локального хранилища сотрудника.
5. Access запрашивает данные по сотруднику по его person_id.
6. СКУД возвращает ФИО и фото сотрудника.
7. Access обновляет информацию о сотруднике в локальном хранилище.

18.5.3. Обработка событий STRAZH при 1 факторе

Диаграмма процесса (Рисунок 110).

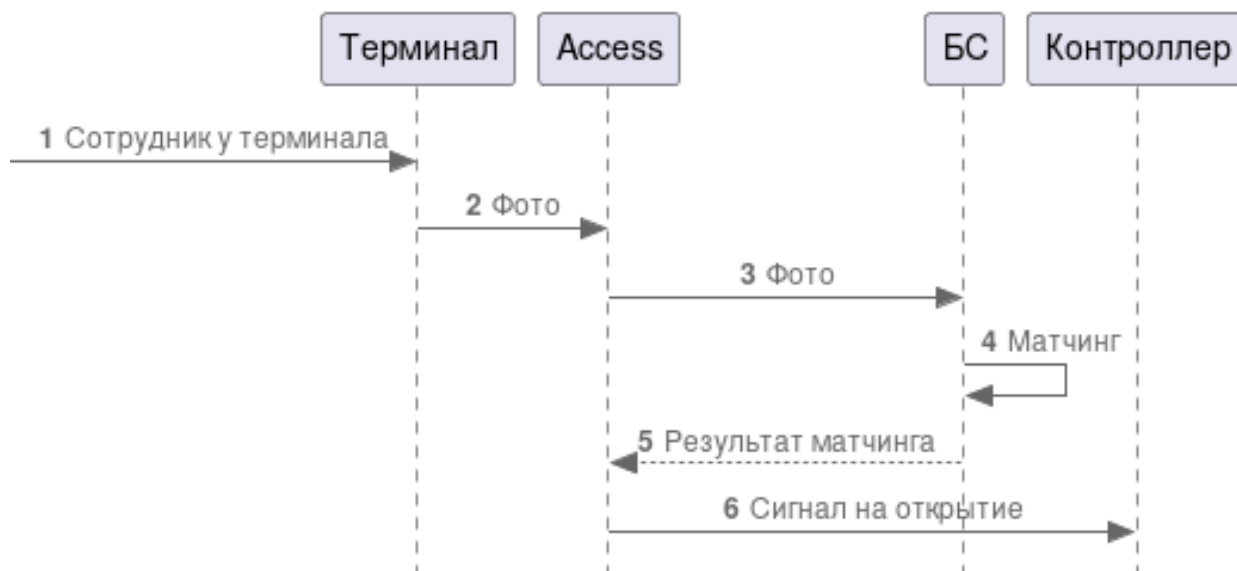
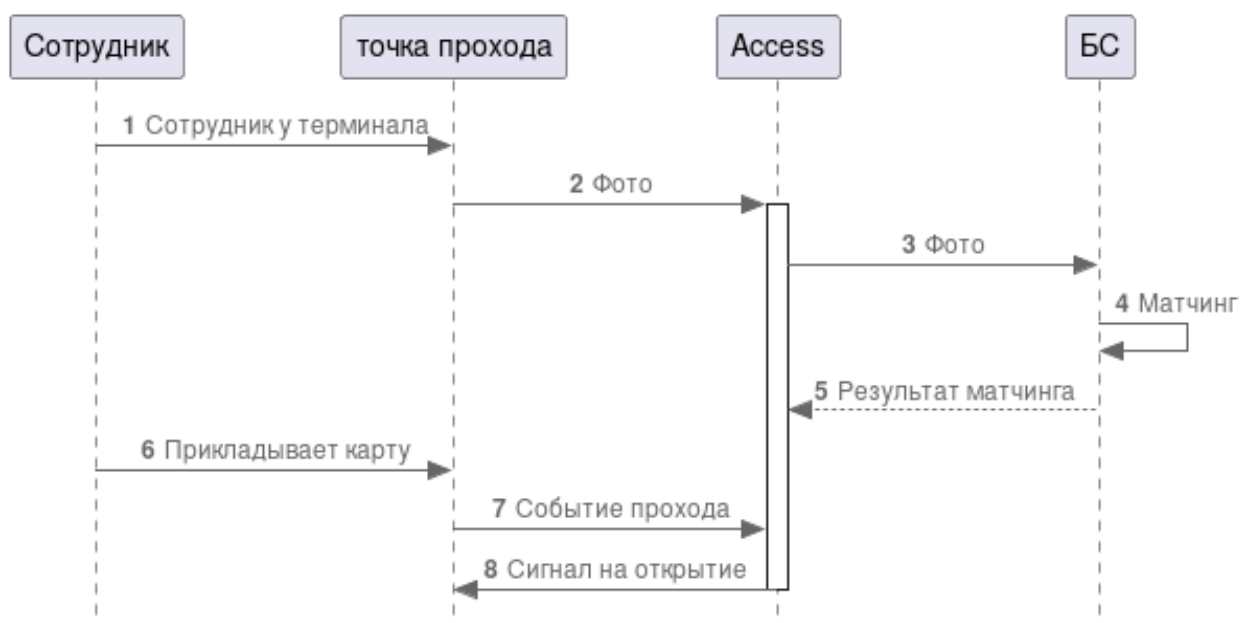


Рис. 110: Диаграмма процессов при 1 факторе

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access решение о предоставлении доступа.
6. Access отправляет на контроллер сигнал на открытие точки доступа.

18.5.4. Обработка событий STRAZH при 2 факторах

Диаграмма процесса (Рисунок 111).

**Рис. 111:** Диаграмма процессов при 2 факторах

1. Сотрудник у биометрического терминала на точке прохода.
2. Терминал отправляет в Access лучший кадр сотрудника.
3. Access отправляет в Биометрическую систему фото сотрудника.
4. БС производит сравнение фотографией с терминала и сохраненного в базе.
5. БС возвращает в Access решение о предоставлении доступа.
6. Сотрудник прикладывает карту (подпроцесс использования карты не зависит от обработки фото, но, как правило, сначала приходит фото).
7. Точка доступа отправляет информацию в Access по SSE о проходе (ID точки доступа, направление прохода и person_id).
8. Access агрегирует информацию о каждом факторе и отправляет на контроллер сигнал на открытие точки доступа.

19. Интеграции без СКУД

Устройство детекции лиц генерирует событие, Access передает событие в LP5 на распознавание, LP5 обрабатывает событие и возвращает результат в Access для дальнейшей обработки.

В каждой интеграции (Таблица 73) используется сервис [Luna](#).

Таблица 73. Варианты интеграции без СКУД

Сервис	Устройство	Пайплайн
Без СКУД	HikvisionRecognition OnBoard	SendToLuna
- (Барс-х)	LunaFast4A1	SendToBars + LunaEventListener + SendToLuna
LunaAceConverter	-	-

20. Контроллеры

Контроллеры необходимы для работы с контроллерами различных производителей для связи систем VisionLabs и устройств контроля доступа других производителей.

Все поля настройки являются обязательными, если не указывается обратное.

20.1. ApacsController

Контроллер Apacs генерируется автоматически при работе сервиса Apacs из полученных точек прохода. Поддерживается до четырех считывателей.

20.1.1. Настройка параметров для подключения к контроллеру Apacs

Настройки контроллера Apacs и возможные значения (Таблица 74):

Таблица 74. Настройки контроллера Apacs

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
apacs_id	Имя экземпляра Apacs в Access	-	-
external_controller_id	Уникальный идентификатор устройства, используемого в интеграции. Указывается в Access.	UUID устройства	-

Параметр	Описание	Возможные значения	Значение по умолчанию
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем более должна быть пауза.	1...10	5
(1-8)_source	Источника событий (камеры или терминала), привязанного к соответствующему считывателю	-	-

20.2. GateController

Контроллер GateController предназначен для работы с преобразователем GateEthernetWiegand, с помощью которого можно отправить номер карты Wiegand формата на контроллер. Для запуска необходимо указать IP, порт и имена компонентов на соответствующие выходы устройства, чтобы понимать, какое направление открыть при получении детекций с устройств.

20.2.1. Преобразователем GateEthernetWiegand

Преобразователь обеспечивает прием кодовой посылки по сети Ethernet от сервера распознавания, декодирование полученной посылки и выдачу кода идентификатора на требуемый Wiegand вход контроллера СКУД. Конфигурация преобразователя происходит с помощью специальной утилиты — программы, работающей под управлением операционной системы Windows. В программе задается начальный IP адрес устройства и другие параметры связи.

20.2.2. Настройка параметров для подключения к контроллеру Gate

Настройки контроллера Gate и возможные значения (Таблица 75):

Таблица 75. Настройки контроллера Gate

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем более должна быть пауза.	1...10	7
host	IP адрес или доменное имя устройства	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт устройства	-	5000
entry_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к двери (выход 0)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
exit_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к считывателю карт 1 (выход 1)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

20.3. LaurentController

Контроллер Laurent2 предназначен для контроля и управления доступом совместно с сервисом Luna Cars.

- Поддерживаемые устройства: Laurent2.
- Поддерживаемые версии прошивки: L212.

20.3.1. Настройка параметров для подключения к контроллеру Laurent

Настройки контроллера и возможные значения (Таблица 76):

Таблица 76. Настройки контроллера Laurent

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя устройства	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт устройства	-	-
password	Пароль к устройству	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
delay_time	Время в секундах, на которое реле открывается	1..10	-

20.4. PercoController

Контроллеры PERCo генерируется автоматически при работе сервиса PercoWeb из подключенных устройств при запуске сервиса. Для использования необходимо в ручном режиме внести entry_source и exit_source значения для каждого из создавшихся контроллеров.

20.4.1. Настройка параметров для подключения к контроллеру PERCo

Настройки контроллера и возможные значения (Таблица 77):

Таблица 77. Настройки контроллера PERCo

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем более должна быть пауза.	1...10	5
external_controller_id	Уникальный идентификатор устройства, используемого в интеграции. Указывается в Access.	UUID устройства	-
perco_web_id	Имя экземпляра сервиса PercoWEB в Access	-	-
description	Дополнительное поле для ввода описания точки прохода	Поддерживаются русские и латинские символы, не рекомендуется вводить более 50 символов.	-
entry_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к двери (выход 0)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
exit_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к считывателю карт 1 (выход 1)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

20.5. PusrController

Контроллер предназначен для работы с преобразователем WGNetConverter, с помощью которого можно отправить номер карты Wiegand формата на контролер.

- Поддерживаемые устройства: WG-TCP
- Поддерживаемые прошивки: V6005

Важно, чтобы преобразователь находился в режиме TCP Server. Для этого при первичной настройке необходимо в веб-интерфейсе в разделе Serial Port выбрать соответствующий Work Mode.

20.5.1. Настройка параметров для подключения к контроллеру Pusr

Настройки контроллера и возможные значения (Таблица 78):

Таблица 78. Настройки контроллера Pusr

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем более должна быть пауза.	1...10	5
host	IP адрес или доменное имя устройства	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт устройства	20108	

Параметр	Описание	Возможные значения	Значение по умолчанию
entry_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к двери (выход 0)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
exit_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к считывателю карт 1 (выход 1)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

20.6. SaltoController

Контроллер Salto генерируется автоматически при работе сервиса Salto из полученных точек прохода. Для использования и работы, после генерации, необходимо в ручном режиме внести entry_source значение для каждого из создавшихся контроллеров.

20.6.1. Настройка параметров для подключения к контроллеру Salto

Настройки контроллера и возможные значения (Таблица 79):

Таблица 79. Настройки контроллера Salto

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем боле должна быть пауза.	1...10	5
salto_id	Имя экземпляра Salto в Access	-	-
external_controller_id	Уникальный идентификатор устройства, используемого в интеграции. Указывается в Access.	UUID устройства	-
entry_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к двери (выход 0)	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

20.7. StrazhController

Контроллеры Strazh генерируется автоматически при работе сервиса Strazh из полученных устройств при запуске сервиса. Для использования необходимо в ручном режиме внести entry_source и exit_source значения для каждого из создавшихся контроллеров.

20.7.1. Настройка параметров для подключения к контроллеру Strazh

Настройки контроллера и возможные значения (Таблица 80):

Таблица 80. Настройки контроллера Strazh

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
retry_entry_sleep_interval	Интервала паузы между прохождением в секундах, чем больше поток людей, тем более должна быть пауза.	1...10	5
external_controller_id	Уникальный идентификатор устройства, используемого в интеграции. Указывается в Access.	UUID устройства	-
strazh_id	Имя экземпляра Strazh в Access	-	-
second_factor_expiry_time	Лимит времени в секундах на получение второго фактора при использовании двухфакторной аутентификации. Не рекомендуется устанавливать лимит более 10 секунд.	0...10	-

Параметр	Описание	Возможные значения	Значение по умолчанию
entry_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к считывателю карт А	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
exit_source	Выпадающий список для выбора устройства, ожидаемое в виде source события, привязанного к считывателю карт В	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

21. Устройства

Для выполнения программно-аппаратной интеграции LP5/КБС/LUNA CARS для контроля доступа необходимо использовать устройства – терминал, камеры и т. д.

Все поля настройки являются обязательными, если не указывается обратное.

21.1. Beward

Биометрический терминал с функциями измерения температуры, определения маски и встроенным реле.

- Поддерживаемые устройства: TFR80-210T1Q / TFR80-210.
- Поддерживаемые версии прошивки: 1.2.13.0 / 2.1.6.0.

21.1.1. Настройка параметров для подключения к Beward

Настройки устройства и возможные значения (Таблица 81):

Таблица 81. Настройки Beward

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	-
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Face is not identified
display_message_time_sec	Время отображения текста на экране в секундах. Работает только в сторону увеличения стандартного значения установленного в прошивке.	Целые числа больше нуля	-
host	IP адрес или доменное имя сервера с установленным Beward	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт сервера, на котором развернут Beward	-	80

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
login	Логин пользователя Beward. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в Beward	-
password	Пароль пользователя Beward. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
open_door_time	Время замыкания реле в миллисекундах	Время берется из инструкции к реле.	2000
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60

Параметр	Описание	Возможные значения	Значение по умолчанию
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-
time_change_interval	Периодичность обновления времени на устройстве, задается в минутах. Рекомендуется использовать, если время на терминале сбивается.	Целые числа больше нуля	60

21.2. BioSmart

- Поддерживаемые устройства: BioSmart Quasar.
- Поддерживаемые версии прошивки: 2.3.0.46.

21.2.1. Настройка параметров для подключения к BioSmart Quasar

Настройки для создания нового устройства (Таблица 82):

Таблица 82. Настройки BioSmart Quasar

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя сервера с установленным Quasar	IP адрес в виде X.X.X.X. или site.domain.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
port	Порт сервера, на котором развернут Quasar	-	80
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
luna_id	Выбор имени сервиса Luna в Access.	-	-
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

Для подписки на события необходимо на терминале зайти в «Настройки» → «Серверная идентификация», выбрать тип сервера: BioSmartLite, ввести эндпоинт для отправки данных: `http://IP/v1-access/webhook/biosmart/` и сохранить настройки.

Девайс не генерирует событий и не кладет ничего в очередь. Запросы в Luna отправляются напрямую из эндпоинтов.

21.3. Dahua

Определенные модели камер Dahua имеют реле и возможность для его программного управления.

При реализации проекта осуществляется интеграция LP5 с данным функционалом, что позволяет управлять реле при появлении в кадре лица из определенного списка.

Далее возможно, например, передать сигнал на электронный замок двери, чтобы дверь открылась или не открылась.

Девайс запускает stream соединение, генерирует и помещает событие детекции лица в очередь.

21.3.1. Настройка параметров для подключения к камере Dahua

Настройки устройства и возможные значения (Таблица 83):

Таблица 83. Настройки Dahua

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
device_id	Внутренний идентификатор устройства. Указан в настройка устройства.	-	-
host	IP адрес или доменное имя камеры Dahua	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере Dahua	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
login	Логин пользователя Dahua. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в камере	-
password	Пароль пользователя Dahua. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-

21.4. DahuaThermo

Определенные модели камер Dahua имеют реле и возможность для его программного управления.

При реализации проекта осуществляется интеграция LP5 с данным функционалом, что позволяет управлять реле при появлении в кадре лица из определенного списка.

Далее возможно, например, передать сигнал на электронный замок двери, чтобы дверь открылась или не открылась.

Поддерживает версию системы 2.631.0000000.31.T, Build Date: 2020-07-06.

Устанавливает HTTP соединение с тепловизором и фиксирует лица отправляя событие тепловой детекции лица в очередь.

21.4.1. Настройка параметров для подключения к тепловизору DahuaThermo

Для запуска необходимо указать следующие настройки (Таблица 84):

Таблица 84. Настройки DahuaThermo

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя камеры Dahua Thermo	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере Dahua Thermo	-	-
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off

Off – неактивно

Параметр	Описание	Возможные значения	Значение по умолчанию
login	Логин пользователя Dahua Thermo. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в камере	-
password	Пароль пользователя Dahua Thermo. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
timeout	Время таймаута при неудачной попытке соединения с сервисом. Необходимо увеличивать время, если имеется большая задержка между серверами.	Время выбирается исходя из задержки в сети, для поддержания работоспособности.	50
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

21.5. Fortuna315

Устройство создает события Thermo в очереди SendThermalEventToLuna по полученным данным от устройств. Включает в себя спаренные устройства - тепловизор и камера.

Поддерживаемые версии прошивки камеры V4.02.00 и тепловизора 2.20.0.0.R26130.alpha8 V1.0. Аппаратные версии V1.0. Версии алгоритма smart2.0.0-06-2020.06.17.16:06:42.

21.5.1. Настройка параметров для подключения к Fortuna315

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 85):

Таблица 85. Настройки Fortuna315

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
device_id	Внутренний идентификатор устройства. Указан в настройка устройства.	-	-
host	IP адрес или доменное имя камеры Fortuna315	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере Fortuna315	-	-
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
thermo_host	IP адрес тепловизора Fortuna315	IP адрес в виде X.X.X.X. или site.domain.	-
thermo_port	Порт тепловизора Fortuna315	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

21.6. GrgFaster

Терминал GrgFaster имеет возможность отображать сообщение на экране и отправлять номер карты на подключенный контроллер.

- Поддерживаемые устройства: GRG Banking Faster.
- Поддерживаемые модели: SV-M082f-C2.
- Поддерживаемые версии прошивки (FW): 1.004.30.3bb324.R.
- Поддерживаемые версии аппаратного обеспечения (HW): 1.0.0

21.6.1. Настройка параметров для подключения к GrgFaster

Настройки устройства и возможные значения (Таблица 86):

Таблица 86. Настройки GrgFaster

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя сервера с установленным GrgFaster	IP адрес в виде X.X.X.X. или site.domain.	-

enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
login	Логин пользователя GrgFasterd. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный в GrgFaster	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 35 символов.	-

21.7. HikvisionCamera

Камера для формирования видеопотока для LP5 с последующей интеграцией со СКУД.

- Поддерживаемые устройства: DS-2CD3126G2-IS
- Поддерживаемые версии прошивки: V5.5.134 build 200430

Устройство создает события типа FaceDetectionEvent.

21.7.1. Настройка параметров для подключения к HikvisionCamera

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 87):

Таблица 87. Настройки HikvisionCamera

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
timeout	Время в секундах таймаута при неудачной попытке соединения с сервисом. Необходимо увеличивать время, если имеется большая задержка между серверами.	Время выбирается исходя из задержки в сети, для поддержания работоспособности.	10
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

21.8. HikvisionCameraThermo

Камера с функциями измерения температуры и передачи данных в LP5.

- Поддерживаемые устройства: DS-2CD3126G2-IS
- Поддерживаемые версии прошивки: V5.5.134 build 200430

Устройство создает события типа ThermalEvent.

21.8.1. Настройка параметров для подключения к HikvisionCameraThermo

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 88):

Таблица 88. Настройки HikvisionCameraThermo

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя камеры HikvisionCameraThermo	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере HikvisionCameraThermo	-	-
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
login	Логин пользователя HikvisionCameraThermo. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный для доступа к устройству	-
password	Пароль пользователя HikvisionCameraThermo. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-

Параметр	Описание	Возможные значения	Значение по умолчанию
timeout	Время в секундах таймаута при неудачной попытке соединения с сервисом. Необходимо увеличивать время, если имеется большая задержка между серверами.	Время выбирается исходя из задержки в сети, для поддержания работоспособности.	10
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

21.9. HikvisionRecognitionOnBoard

Биометрический терминал с функцией распознавания лиц.

- Поддерживаемые устройства: DS-K1T341AMF, DS-K1T341AM, DS-K1T680D-E1
- Поддерживаемые версии прошивки: V3.2.30 build 220210

Откройте веб-интерфейс устройства, перейдите в раздел «Configuration» → «Access Control» → «Face Recognition Parameters» → «Working Mode» и убедитесь, что выставлен режим `Permission Free Mode`.

После добавления, лица из указанного списка будут реплицированы в память устройства. Можно добавлять/удалять лица в Luna, изменения автоматически будут применены к устройству.

- необходим следующий формат поля `user_data`:

```
name;card_number
```

- поле `external_id` не допускается задавать и изменять.

Не поддерживается обновление данных лица при редактировании. Если необходимо обновить данные лица, удалите это лицо и добавьте снова с необходимыми данными.

События в очереди имеют тип `FaceDetectionEvent`.

21.9.1. Настройка параметров для подключения к HikvisionRecognitionOnBoard

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 89):

Таблица 89. Настройки HikvisionRecognitionOnBoard

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя камеры	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере	-	-
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
login	Логин пользователя. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный для доступа к устройству	-

Параметр	Описание	Возможные значения	Значение по умолчанию
password	Пароль пользователя. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
luna_id	Выбор сервиса Luna в Access.	-	-
face_recognition_interval	Интервал между запуском распознавания. Задается в зависимости от потока людей.	1...10	1
liveness_level	Степень проверки уровня liveness.	low – быстрая скорость обработки, точность уменьшена	low
		middle – средняя точность распознавания и скорость работы	
		high – точное определение, повышенное потребление ресурсов	
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60

Параметр	Описание	Возможные значения	Значение по умолчанию
time_change_interval	Периодичность обновления времени на устройстве, задается в минутах. Рекомендуется использовать, если время на терминале сбивается.	Целые числа больше нуля	60

21.10. HikvisionTerminalThermo

Биометрический терминал с функциями измерения температуры, определения маски и встроенным реле.

- Поддерживаемые устройства: DS-K1TA70MI-T, DS-K1T671TM-3XF, DS-K5671-3XF/ZU.
- Поддерживаемые версии прошивки: V3.2.32 build 210525.

Обрабатываться будут только события типа AccessControllerEvent (имеющие измеренную температуру), события такого типа приходят с терминала.

События в очереди имеют тип ThermalEvent.

Для отключения вывода приветствия на экране терминала, необходимо отключить пайплайн LunaEventListener.

21.10.1. Настройка параметров для подключения к HikvisionTerminalThermo

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 90):

Таблица 90. Настройки HikvisionTerminalThermo

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Не рекомендуется вводить более 33 символов.	Добро пожаловать
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 33 символов.	Лицо не идентифицировано
display_message_time_sec	Время отображения текста на экране в секундах. Работает только в сторону увеличения стандартного значения установленного в прошивке.	Целые числа больше нуля	-
host	IP адрес или доменное имя камеры HikvisionTerminalThermo	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере HikvisionTerminalThermo	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
login	Логин пользователя HikvisionTerminalThermo. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный для доступа к устройству	-
password	Пароль пользователя HikvisionTerminalThermo. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60
card_recognition_interval	Интервал между распознаваниями карт.	0...10	3
face_recognition_interval	Интервал между распознаваниями изображений с лицами.	1...10	3

Параметр	Описание	Возможные значения	Значение по умолчанию
liveness	Отвечает за активацию системы liveness	On – активно Off – неактивно	On
liveness_level	Степень проверки уровня liveness.	low – быстрая скорость обработки, точность уменьшена middle – средняя точность распознавания и скорость работы high – точное определение, повышенное потребление ресурсов	middle
attempts_check_liveness	Количество попыток прохождения проверки liveness. Необходимо увеличивать количество попыток проверки при сложных ракурсах и условиях съемки для предотвращения ложноположительных распознаваний.	5...15	10
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
light_brightness_led	Уровень яркости LED подсветки. Чем темнее зона перед терминалом, тем ярче должна быть подсветка	0...100	50

Параметр	Описание	Возможные значения	Значение по умолчанию
light_brightness_ ir	уровень яркости инфракрасной (ИК) подсветки. Чем темнее зона перед терминалом, тем ярче должна быть подсветка	0...100	50
voice_prompt	Голосовые подсказки терминала о событиях прохода или ошибках. Настройку подсказок см. в официальной документации терминала.	On/Off	Off
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-
time_change_ interval	Периодичность обновления времени на устройстве, задается в минутах. Рекомендуется использовать, если время на терминале сбивается.	Целые числа больше нуля	60
clear_old_ events_interval	Периодичность удаления старых событий (в секундах), для предотвращения переполнения памяти терминала	300...1200	600
wiegand_ direction	Направление работы wiegand	input - принимать карту от считывателя output - отправлять карту на контроллер	input

21.11. LunaFast2NextGen

21.11.1. Настройка параметров для подключения к LunaFast2NextGen

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 91):

Таблица 91. Настройки LunaFast2NextGen

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО . Не рекомендуется вводить более 33 символов.	-

Пример с выводом ФИО:
Добро пожаловать,
{fullname}.

[illegible]

Параметр	Описание	Возможные значения	Значение по умолчанию
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
event_receiving_mode	Режим для получения событий от LP5 (от версии 5.53.0).	rtsp - протокол с использованием постоянного соединения webhook - обратные вызовы по протоколу HTTP. Клиент - Luna Platform, сервер - Luna Access	webhook

21.12. LunaFast4A1

Биометрический терминал LUNA FAST 4A1 с функцией распознавания.

- Поддерживаемые устройства: DS-K1T341CMF, DS-K1T680D-E1, DS-K1T341AMF, DS-K1T341AM, VL LUNA FAST 4A1, VL LUNA FAST 8A1, 671, DS-K1T671M, ACT-T1341M, DS-K1T680DF-E1, DS-K5671-ZU.
- Поддерживаемые версии прошивки: V3.3.40 build 250106, V3.2.30 build 210415, V3.2.30 build 210525, V3.2.30 build 210526, V3.2.30 build 210812, V3.2.30 build 211025, V3.2.30 build 220607, V3.2.30 build 220803, V3.2.30 build 221027, V3.2.33 build 210816, V3.2.35 build 220415, V3.2.35 build 220817.

События в очереди имеют тип FaceDetectionEvent.

Для отключения вывода приветствия на экране терминала, необходимо отключить пайплайн LunaEventListener.

Может отправлять номер карты на [контроллер](#) через [устройство](#).

Статус поддержки функционала отправки номера карты отображается в блоке «info» в параметре hardware_with_card_sending, после того как компонент подключен.

21.12.1. Настройка параметров для подключения к LunaFast4A1

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 92):

Таблица 92. Настройки LunaFast4A1

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО . Не рекомендуется вводить более 33 символов.	Добро пожаловать
Пример с выводом ФИО: Добро пожаловать, {fullname}.			
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 33 символов.	Лицо не идентифицировано

Параметр	Описание	Возможные значения	Значение по умолчанию
display_message_time_sec	Время отображения текста на экране в секундах. Работает только в сторону увеличения стандартного значения установленного в прошивке.	Целые числа больше нуля	-
host	IP адрес или доменное имя камеры LunaFast4A1	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к терминалу LunaFast4A1	-	80
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
login	Логин пользователя LunaFast4A1. Поддерживается ввод латиницы, цифр и символов.	Пользователь созданный для доступа к устройству	-
password	Пароль пользователя LunaFast4A1. Поддерживается ввод латиницы, цифр и символов.	Пароль пользователя	-

Параметр	Описание	Возможные значения	Значение по умолчанию
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60
card_recognition_interval	Интервал между распознаваниями карт.	0...10	3
face_recognition_interval	Интервал между распознаваниями изображений с лицами.	1...10	3
liveness	Отвечает за активацию системы liveness	On – активно	On
		Off – неактивно	
liveness_level	Степень проверки уровня liveness.	low – быстрая скорость обработки, точность уменьшена	low
		middle – средняя точность распознавания и скорость работы	
		high – точное определение, повышенное потребление ресурсов	

Параметр	Описание	Возможные значения	Значение по умолчанию
attempts_check_liveness	Количество попыток прохождения проверки liveness. Необходимо увеличивать количество попыток проверки при сложных ракурсах и условиях съемки для предотвращения ложноположительных распознаваний.	Значения > 0	10
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
light_brightness_led	Уровень яркости LED подсветки. Чем темнее зона перед терминалом, тем ярче должна быть подсветка	0...100	50
light_brightness_ir	уровень яркости инфракрасной (ИК) подсветки. Чем темнее зона перед терминалом, тем ярче должна быть подсветка	0...100	50
voice_prompt	Голосовые подсказки терминала о событиях прохода или ошибках. Настройку подсказок см. в официальной документации терминала.	On/Off	Off
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

Параметр	Описание	Возможные значения	Значение по умолчанию
time_change_interval	Периодичность обновления времени на устройстве, задается в минутах. Рекомендуется использовать, если время на терминале сбивается.	Целые числа больше нуля	60
clear_old_events_interval	Периодичность удаления старых событий (в секундах), для предотвращения переполнения памяти терминала	300...1200	600
wiegand_direction	Направление работы wiegand	input - принимать карту от считывателя output - отправлять карту на контроллер	input

21.13. Panda

Тепловизионная камера с распознаванием лиц.

- Поддерживаемые устройства: SN-T5/13, SN-F22-13.
- Поддерживаемые версии прошивки: v3.6.0825.1004.1.0.23.0.0, v3.6.0840.1004.1.45.1.0.2.

События в очереди имеют тип ThermalEvent.

21.13.1. Настройка параметров для подключения к Panda

Для подписки на события необходимо создать устройство со следующими настройками (Таблица 93):

Таблица 93. Настройки Panda

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя сервиса задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя камеры Panda	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к камере Panda	-	80
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

Далее необходимо зайти в веб интерфейс устройства, залогиниться, перейти во вкладку «Configuration», на панели слева выбрать раздел «Network Service», а затем «CGI Alarm Service Center».

Далее в разделе «CGIAlarm» заполнить поля: в качестве URL Start и URL End назначить энд-

порт для отправки данных в Access `http://<vl_access_host>:<vl_access_port>/vl-access/webhook/device/<component_id>/event/handle_event/`. Также при необходимости в разделе «Proxy Settings» заполните поля Address и Port: Access host и Access port соответственно. В конце сохраните настройки.

21.14. R20Face

Биометрический терминал с функцией определения наличия защитной маски и централизованым управлением.

- Поддерживаемые устройства: R20-Face-T8
- Поддерживаемые версии прошивки: GD-V32.7267

21.14.1. Настройка параметров для подключения к R20Face

Настройки устройства и возможные значения (Таблица 94):

Таблица 94. Настройки R20Face

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Добро пожаловать
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Лицо не идентифицировано
display_message_time_sec	Время отображения текста на экране в секундах. Работает только в сторону увеличения стандартного значения установленного в прошивке.	Целые числа больше нуля -	
host	IP адрес или доменное имя терминала R20Face	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к терминалу R20Face	-	8080

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
password	Пароль пользователя терминала	Пароль пользователя	-
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60
time_zone	Часовой пояс.	GMT-12...+12	GMT+3
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-
handle_detection_events	Включение режима обработки события детекции от терминала	On/Off	Off

21.15. UniUbi

Биометрический терминал с функциями измерения температуры, определения маски и управлением встроенным реле.

- Поддерживаемые устройства: Uface 8-C temp, Uface 8T temp, R20-Face-T8.
- Поддерживаемые версии прошивки: GD-V30.7219, GD-V32.7247, GD-V32.7267.

При использования терминала без измерения температуры необходимо изменить пайплайн `SendThermalEventToLuna` на `SendToLuna`.

21.15.1. Настройка параметров для подключения к UniUbi

Для подписки на события необходимо создать устройство типа UniUbi.

Настройки устройства и возможные значения (Таблица 95):

Таблица 95. Настройки UniUbi

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО . Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 27 символов.	Добро пожаловать
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 27 символов.	Лицо не идентифицировано
display_message_time_sec	Время отображения текста на экране в секундах. Работает только в сторону увеличения стандартного значения установленного в прошивке.	Целые числа больше нуля -	
host	IP адрес или доменное имя терминала UniUbi	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к терминалу UniUbi	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно	Off
		Off – неактивно	
password	Пароль пользователя UniUbi	Пароль пользователя	-
enabled_temp_mode	Режим измерения температуры. При отключении параметра измените пайплайн SendThermalEventToLuna на SendToLuna.	On – включен	On
			Off – выключен
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-
vl_access_port	Порт сервера, на котором развернут Access	-	9091
event_expiry_time	Время валидности событий в секундах, необходимо уменьшать время, при большом потоке людей, так как может переполняться кэш устройства	>10	60
time_zone	Часовой пояс.	GMT-12...+12	GMT+3

Параметр	Описание	Возможные значения	Значение по умолчанию
handler_id	UUID обработчика для работы с событиями прохода, созданный в Luna.	UUID обработчика	-

21.16. VKVision02

Терминал с функцией видеозаписи и отображения изображений на экран

- Поддерживаемые устройства: VANCOR VK VISION 02

21.16.1. Настройка параметров для подключения к VKVision02

Настройки устройства и возможные значения (Таблица 96):

Таблица 96. Настройки VKVision02

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя устройства задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
group	Название списка для группировки компонентов	Любые числовые и текстовые значения	-
host	IP адрес или доменное имя терминала VKVision02	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт для подключения к терминалу VKVision02	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
enable_ssl	Поддержка шифрования SSL для сообщений. Необходимо активировать при необходимости сохранения конфиденциальности. При активации нагрузка на устройство и время передачи сообщений возрастает	On – активно Off – неактивно	Off
success_status_image_ttl	Время (мс) отображения изображения на терминале в секундах со статусом «Успешно»	5000...20000	10000
denied_status_image_ttl	Время (мс) отображения на терминале изображения в секундах со статусом «Отказано».	5000...20000	10000
luna_id	Выбор имени сервиса Luna в Access.	-	-

22. Пайплайны

Все поля настройки являются обязательными, если не указывается обратное.

22.1. Arcs2FA

Пайплайн Arcs2FA реализует кастомную двухфакторную авторизацию для сервиса Arcs. Прослушиваются события, возникшие при считывании карты, а также события детекции лиц. Они сопоставляются по их source. Когда приходит первый фактор с определенным source, то запускается ожидание второго фактора, время на его ожидание задается в настройке expiry_time, как только он получен, начинается валидация этой пары.

- Схожесть лучшего кандидата матчинга, должна быть не ниже указанной в настройке min_face_similarity.
- Номер карты полученный со считывателя должен совпадать с номером карты лица в списке Luna.

По завершении процедуры аутентификации, на экране устройства отображается соответствующий текст. После успешной валидации номер карты отправляется на соответствующий выход контроллера Gate Ethernet Wiegand или WNetConverter.

Для создания пайплайна требуется указать (Таблица 97):

Таблица 97. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
waiting_time_exceeded_message	Сообщение при превышении времени ожидания второго фактора	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 50 символов.	Превышено время ожидания

Параметр	Описание	Возможные значения	Значение по умолчанию
luna_id	Идентификатор сервиса Luna в Access	Выпадающий список для выбора сервиса	-
apacs_id	Уникальный идентификатор сервиса Apacs в Access	Выпадающий список для выбора сервиса	-
expiry_time	Лимит времени в секундах на получение второго фактора.	>0	5
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00
unknown_card_message	Сообщение при отправке неизвестной карты для принятия решения о доступе	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 50 символов.	Карта считана и отправлена на контроллер
access_denied_card	Номер карты пользователя, заведенного для уведомления о неуспешных проходах. Необходимо указывать номер, чтобы в подключенном СКУД можно было видеть лог о том, что авторизация не прошла.	-	None

Параметр	Описание	Возможные значения	Значение по умолчанию
use_cards_without_face	Использование и отправка на контроллер карт, которые не привязаны к лицам. Рекомендуется использовать для гостевых карт.	On - отправлять Off - не отправлять	On

22.2. CreateBastionEvent

Пайплайн работает совместно со СКУД Bastion.

При включенной однофакторной авторизации на точке доступа прослушивает события ResultMatchEvent и генерирует событие BastionEvent.

При включенном режиме enable_negative_events дополнительно отправляет сообщение на терминал при негативном событии матчинга (требуется только при интеграции с **Бастион 3**).

Если включена двухфакторная авторизация, то выполняется запрос на подтверждение доступа в СКУД.

При создании нового пайплайна используются следующие настройки (Таблица 98):

Таблица 98. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выбор имени сервиса LP5/КБС в Access.	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
bastion_id	Выпадающий список для выбора идентификатора устройства Bastion, используемого в интеграции. Указывается в Access.	-	-
enable_negative_events	Отправляет сообщения на терминал при результате матчинге ниже порога min_face_similarity (настраивается в пайплайне получения данных от биометрической системы). Только для Bastion 3	On - включить, Off - выключить	Off

22.3. Custom2FA

Пайплайн Custom2FA реализует кастомную двухфакторную авторизацию. Прослушиваются события, возникшие при считывании карты, а также обычные события детекции лиц. События сопоставляются по их source и сохраняются в маппинг. Когда приходит первый фактор с определенным source, то запускается ожидание второго фактора, время на его ожидание задается в настройке expiry_time, как только он получен, начинается валидация этой пары.

- Схожесть лучшего кандидата матчинга, должна быть не ниже указанной в настройке min_face_similarity (настраивается в пайплайне получения данных от биометрической системы);
- Номер карты полученный со считывателя должен совпадать с номером карты лица в списке LP5.

По завершении процедуры аутентификации, на экране устройства отображается соответствующий текст. После успешной валидации номер карты отправляется на соответствующий выход контроллера Gate Ethernet Wiegand.

Для создания пайплайна требуется указать (Таблица 99):

Таблица 99. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выбор сервиса LP5/КБС в Access.	-	-
expiry_time	Лимит времени в секундах на получение второго фактора.	0...10	5
unknown_card_message	Сообщение при отправке неизвестной карты для принятия решения о доступе	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 50 символов.	Карта считана и отправлена на контроллер
waiting_time_exceeded_message	Сообщение при превышении времени ожидания второго фактора	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 50 символов.	Превышено время ожидания
use_cards_without_face	Использование и отправка на контроллер карт, которые не привязаны к лицам	On - отправлять	On
		Off - не отправлять	

22.4. LunaEventListener

LunaEventListener слушает события из Luna генерируемые внутренним сервисом Luna, LunaStreams или любым другим внешним ПО. Отправляет карты на контроллер или преобразователь и может отправлять сообщения на девайс.

При создании нового пайплайна используются следующие настройки (Таблица 100):

Таблица 100. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
luna_id	Идентификатор сервиса Luna в системе	-	-
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00
enable_fake_events	Обработка запросов с не пройденной проверкой Liveness, для просмотра таких событий. Для активации должен быть активен параметр enable_fake_events в пайплайне SendToLuna	On - обрабатывать	Off
Off - не обрабатывать			

22.5. MatchByPhoto

Запрашивает дескриптор в КБС и по его идентификатору извлекает кандидата из своей БД.

При работе с устройствами и контроллерами необходимо подключать пайплайны [SendToDevice](#) и [SendToController](#), соответственно.

При создании нового пайплайна используются следующие настройки (Таблица 101):

Таблица 101. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выбор имени сервиса LP5/КБС в Access.	-	-
pacs_id	Уникальный идентификатор сервиса в Access	Выпадающий список для выбора сервиса	-
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00
retry_entry_sleep_interval	Пауза для повторной попытки прохода.	>0 или None	1

22.6. MatchByPhotoInCbsAlpha

Запрашивает дескриптор в КБС Альфа и по его идентификатору извлекает кандидата из своей БД. С полученными данными (кандидатом и именем источника) создается событие и отправляется SuccessMatchEvent в очередь.

При работе с устройствами и контроллерами необходимо подключать пайплайны [SendToDevice](#) и [SendToController](#), соответственно

При создании нового пайплайна используются следующие настройки (Таблица 102):

Таблица 102. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выбор имени сервиса КБС Альфа в Access.	-	-
pcs_id	Уникальный идентификатор сервиса в Access	Выпадающий список для выбора сервиса	-
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00
retry_entry_sleep_interval	Пауза для повторной попытки прохода.	1...10	5
only_cbs_list	Переключение списков для матчинга	On - переключение на работу только со списком КБС Off - переключение на работу с двумя списками	Off

22.7. MatchInformerWebHook

Отслеживает события от биометрической системы (LP5 или КБС), извлекает информацию о кандидате и отправляет во внешний сервис посредством webhook. Если кандидат не найден, возвращает пустое значение best_candidate.

Пайплайн необходим для решений, когда Access необходимо передавать данные от связанных компонентов во внешние системы за рамками предложенных интеграций.

Шаблон возвращаемых данных:

```
{
```

```

    source: str, best_candidate:
    {
        person_id: str, fullname: str | None, descriptor_id: str | None =
        None
    }
}

```

Где:

- source - имя устройства;
- best_candidate - данные кандидата;
- person_id - id кандидата в СКУД;
- fullname - полное имя кандидата;
- descriptor_id - id дескриптора.

Для создания пайплайна требуется указать (Таблица 103):

Таблица 103. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
host	IP адрес или доменное имя целевого сервера	IP адрес в виде X.X.X.X. или site.domain.	-
port	Порт целевого сервера	-	-
urn	urn для подключения к внешнему сервису	-	-
enable_ssl	Метод шифрования данных при передачи по сети. Зависит от типа сети в решении.	On - https Off - http	Off

22.8. MatchInformerWebSocket

Отслеживает события ResultMatchEvent от биометрической системы (LP5 или КБС), извлекает информацию о кандидате и отправляет json всем подключенным клиентам посредством websocket. Если кандидат не найден, возвращает пустое значение best_candidate. Для аутентификации, необходимо добавить заголовок «Authentication» с токеном из информации о компоненте.

Пайплайн необходим для решений, когда Access необходимо передавать данные от связанных компонентов во внешние системы за рамками предложенных интеграций.

Шаблон возвращаемых данных:

```
{
  source: str, best_candidate:
  {
    person_id: str, fullname: str | None, descriptor_id: str | None =
      None
  }
}
```

- source - имя устройства;
- best_candidate - данные кандидата;
- person_id - id кандидата в СКУД;
- fullname - полное имя кандидата;
- descriptor_id - id дескриптора;

Для создания пайплайна требуется указать (Таблица 104):

Таблица 104. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
vl_access_host	IP адрес сервера, на котором установлен Access	IP адрес в виде X.X.X.X. или site.domain	-

Параметр	Описание	Возможные значения	Значение по умолчанию
vl_access_port	Порт сервера, на котором развернут Access	-	9091

22.9. SendCardToR20Face

Пайплайн прослушивает очередь событий SuccessMatchEvent, валидирует полученное событие на наличие кандидата, уровень соответствия и наличие номера карты. Затем выполняется поиск устройства по имени источника события и на это устройство отправляется номер карты.

Для создания пайплайна требуется указать (Таблица 105):

Таблица 105. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

22.10. SendCarsToLaurent

Пайплайн слушает события из Luna Cars и отправляет сигнал на замыкание реле контроллера Laurent. Поддерживается работ до четырех реле управления преграждающим устройством.

При создании нового пайплайна используются следующие настройки (Таблица 106):

Таблица 106. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
controller_id	Идентификатор контроллера Laurent в Access	-	-
relay_{N}_-scenario_id	UUID сценария в LUNA CARS Analytics, по которому происходит проверка ГРЗ для реле {N}, N - от 1 до 4.	-	-

22.11. SendCarsToSigur

Пайплайн для отправки событий из LUNA CARS в Sigur. Прослушивает очередь событий CarDetectionEvent и генерирует события SigurCarEvent.

При создании нового пайплайна используются следующие настройки (Таблица 107):

Таблица 107. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

22.12. SendThermalEventToLuna

Прослушивает очередь событий тепловой детекции и генерирует события в Luna. Для запуска необходимо указать component_id запущенного в системе сервиса Luna. Пайплайн выполняет работу с несколькими списками: дефолтный список и черный список; распределяет полученные данные между ними в зависимости установленных порогов допустимого нижнего и верхнего значения температуры.

При создании нового пайплайна используются следующие настройки (Таблица 108):

Таблица 108. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
luna_id	Идентификатор сервиса Luna в системе	-	-
handler_id	UUID обработчика для работы с событиями прохода, созданный в LP5.	-	-
black_list_id	UUID списка LP5, с которым устройство будет синхронизировать людей, для которых доступ закрыт. Необязательный параметр.	Идентификатор списка, созданные в Luna.	-
too_high_temperature	Верхний порог температуры человека при которой его нельзя пропускать.	3...40	37

Параметр	Описание	Возможные значения	Значение по умолчанию
too_low_temperature	Нижний порог температуры человека при которой его нельзя пропускать.	3...40	35
use_lists	Активация распределения данных людей по спискам (по умолчанию, черный).	On – сравнивать	
		Off – не сравнивать	Off
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования.	0,00...1,00

22.13. SendToBars

Прослушивает очередь событий LunaEvent, DoorEvent и генерирует событие BarsEvent.

При создании нового пайплайна используются следующие настройки (Таблица 109):

Таблица 109. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
luna_id	Выбор имени сервиса Luna в Access.	-	-
bars_host	IP адрес, или сетевое имя ПК с установленным БС	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
bars_port	порт, на котором располагается БС	-	-
enable_ssl	Метод шифрования данных при передачи по сети. Зависит от типа сети в решении.	On - https Off - http	Off
min_face_similarity	Минимальный порог схожести лиц при выполнении верификации.	Значение формируется на этапе проектирования и корректируется на этапе тестирования. 0,00...1,00	0,7
time_to_pass	Время ожидания перед следующей идентификацией человека, если человек не прошел через преграждающее устройство.	0...15 секунд	5

22.14. SendToController

Отправляет сигнал на открытие реле в устройство по имени источника события.

При создании нового пайплайна используются следующие настройки (Таблица 110):

Таблица 110. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

22.15. SendToDevice

Отправляет сигнал на открытие реле в устройство по имени источника события и выводит текст на экран. Может отправлять номер карты на [контроллер](#) через [устройство](#).

При создании нового пайплайна используются следующие настройки (Таблица 111):

Таблица 111. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Добро пожаловать
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Лицо не идентифицировано

22.16. SendToGrgFaster

Предназначен для взаимодействия с пайплайном MatchPyPhoto и устройством GrgFaster.

При создании нового пайплайна используются следующие настройки (Таблица 112):

Таблица 112. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	-
facility_code	Параметр для ввода номеров карт для их опознавания системой. Будет добавляться для каждого номера карты перед отправкой на контроллер	-	-

22.17. SendToLuna

Пайплайн отправляет получаемые события FaceDetectionEvent в Luna.

При создании нового пайплайна используются следующие настройки (Таблица 113):

Таблица 113. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
luna_id	Идентификатор сервиса Luna в системе	-	-
enable_fake_events	Отправка лиц с неуспешным liveness, для просмотра попыток взлома Liveness. Для активации должен быть активен параметр enable_fake_events в пайплайне LunaEventListener	On - отправлять Off - не отправлять	Off

22.18. SendToParsec

Прослушивает очередь событий LunaEvent или SuccessMatchEvent в Luna и генерирует событие ParsecEvent.

При создании нового пайплайна используются следующие настройки (Таблица 114):

Таблица 114. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
bio_system_id	Выбор имени сервиса LP5/КБС в Access.	-	-

Параметр	Описание	Возможные значения	Значение по умолчанию
parsec_id	Уникальный идентификатор устройства Parsec, используемого в интеграции. Указывается в Access.	-	-

22.19. SendToSalto

Прослушивает очередь событий ResultMatchEvent от пайплайна MatchByPhoto, в случае успешной валидации лица в событии, отправляет запрос к сервису Salto для прохождения через дверь, а также выводит сообщение об успешности/неуспешности прохода на устройство.

При создании нового пайплайна используются следующие настройки (Таблица 115):

Таблица 115. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-

Параметр	Описание	Возможные значения	Значение по умолчанию
successful_pass_message_template	Сообщение при успешной идентификации. Для отображения имени пользователя на экране терминала при успешной идентификации необходимо использовать переменные ФИО. Порядок слов в приветственном сообщении может быть любым.	Любые текстовые названия и переменные ФИО. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Добро пожаловать
unsuccessful_pass_message	Сообщение при неуспешной идентификации	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 24 символов.	Лицо не идентифицировано

22.20. SendToSigur

Прослушивает очередь событий SuccessMatchEvent в Luna и генерирует событие SigurEvent.

При создании нового пайплайна используются следующие настройки (Таблица 116):

Таблица 116. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
sigur_id	Уникальный идентификатор устройства Sigur, используемого в интеграции. Указывается в Access.	-	-

22.21. Strazh2FA

В случае, если контроллер не находится в режиме 2FA: Прослушивает очередь событий ResultMatchEvent от пайплайна MatchByPhoto, в случае успешной валидации лица в событии, отправляет запрос к сервису Strazh для прохождения через точку доступа.

В случае, если контроллер находится в режиме 2FA: Прослушиваются события, возникшие при считывании карты, а также обычные события детекции лиц. Они сопоставляются по их source. Когда приходит первый фактор с определенным source, то запускается ожидание второго фактора, время на его ожидание задается в настройке second_factor_expiry_time в StrazhController, как только он получен, начинается валидация этой пары.

При создании нового пайплайна используются следующие настройки (Таблица 117):

Таблица 117. Параметры пайплайна

Параметр	Описание	Возможные значения	Значение по умолчанию
name	Имя пайплайна задаваемое пользователем	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 30 символов.	-
waiting_time_exceeded_message	Сообщение при превышении времени ожидания второго фактора.	Любые текстовые названия. Поддерживается ввод латиницы и кириллицы. Не рекомендуется вводить более 50 символов.	Превышено время ожидания
strazh_id	Выбор имени сервиса Strazh в Access.	-	-