



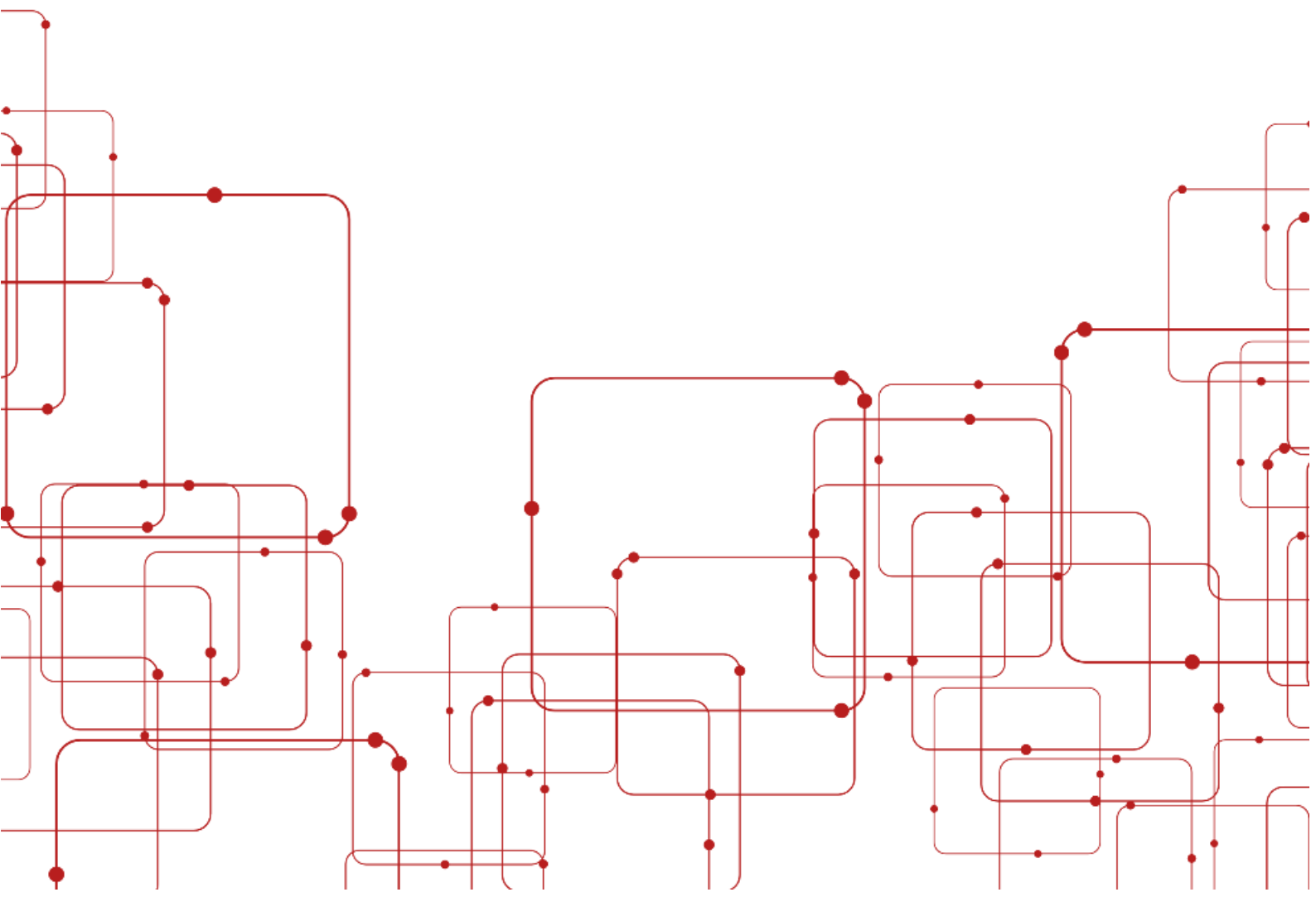
ассистент **PRO**

безопасное удаленное управление

руководство пользователя ЛИЧНЫЙ КАБИНЕТ

РЕДАКЦИЯ: Корпорация+

Воронеж



Аннотация

Настоящий документ представляет собой руководство пользователя web-портала **Личный кабинет** системы удаленного мониторинга и управления **Ассистент PRO**.

В руководстве пользователя описаны общие принципы работы с web-порталом, порядок действий пользователей при выполнении операций в рамках определенных полномочий. Функционал **Личного кабинета** может быть ограничен в зависимости от редакции **Ассистент PRO**.

Руководство пользователя основано на том предположении, что вся необходимая инфраструктура для функционирования системы удаленного мониторинга и управления **Ассистент** развернута и готова к использованию, **Личный кабинет** доступен по назначенному адресу, а **Клиентское приложение** уже установлено на устройствах пользователей. Если вам необходима помощь в установке, ознакомьтесь с документом **Руководство администратора**.

Содержание

1. Общие сведения.....	6
1.1. Назначение личного кабинета	6
1.2. Принцип работы	6
2. Авторизация.....	8
2.1. Регистрация	8
2.2. Вход в личный кабинет	9
2.3. Восстановление пароля	9
3. Мой ассистент.....	11
3.1. Мои устройства	11
3.1.1. Создание группы устройств	12
3.1.2. Добавление устройства	12
3.2. Профиль	14
3.2.1. Мои данные	14
3.2.2. Безопасность	15
3.2.3. Мои организации	15
4. Мои организации.....	17
4.1. Организации	17
4.1.1. Управление организациями	20
4.1.2. Политики доступа	22
4.1.3. Политики инвентаризации	33
4.1.4. Сотрудники	35
4.1.5. Устройства	45
4.1.6. Коллекции	60
4.1.7. Сервисные организации	67
4.1.8. Клиенты	71
4.2. Домены служб каталогов	73
4.3. Заявки	74
5. Журналы и протоколы.....	76
5.1. Протоколы соединений	76
5.2. Журнал организации	77
5.3. Системный журнал	77
6. Статистика и сессии.....	79
6.1. Сессии устройств	79
6.2. Статистика	79

7. Администрирование.....	82
7.1. Устройства	82
7.1.1. Автодобавление в организацию.....	83
7.1.2. Добавление в организацию.....	84
7.2. Транспортные серверы	86
7.3. Виды лицензий	87
7.4. Лицензии	88
7.5. Роли доступа	89
7.6. Учетные записи	90
7.6.1. Создание учетной записи.....	91
7.6.2. Привязка учетной записи Ассистент PRO к учетной записи домена	92
7.6.3. Импорт учетных записей из домена	92
7.6.4. Добавление в организацию.....	94
7.6.5. Активация лицензии для учетной записи.....	95
7.7. Категории заявок	95
7.8. Настройки	96
7.8.1. Параметры.....	96
7.8.2. Безопасность	100
7.8.3. Политика доступа по умолчанию.....	104
8. Управление конфигурациями.....	105
8.1. Шаблоны	105
8.1.1. Создание группы шаблонов	105
8.1.2. Создание шаблона	106
8.1.3. Добавление сценария в шаблон конфигурации	107
8.1.4. Атрибуты.....	108
8.1.5. Тест выполнения	108
8.1.6. Готов к выполнению	109
8.2. Задачи	110
8.2.1. Создание задачи конфигурации.....	111
8.2.2. Расписание выполнения задач	111
8.2.3. Устройства и коллекции	112
8.2.4. Шаблоны задачи	114
8.2.5. История выполнения	115

Список иллюстраций

Рисунок 1 Страница Регистрация учетной записи	8
---	---

Рисунок 2	Страница Вход в личный кабинет	9
Рисунок 3	Окно Мои устройства	11
Рисунок 4	Страница Создание группы устройств	12
Рисунок 5	Страница Добавление устройства	13
Рисунок 6	Страница Профиль. Вкладка Мои данные	14
Рисунок 7	Страница Мои организации	18
Рисунок 8	Страница Создание организации	20
Рисунок 9	Вкладка Политики доступа страницы Организация	22
Рисунок 10	Вкладка Общие данные окна Создание политики доступа	23
Рисунок 11	Вкладка Правила доступа окна Создание политики доступа	24
Рисунок 12	Вкладка Безопасность окна Создание политики доступа	26
Рисунок 13	Вкладка Протоколирование окна Создание политики доступа	27
Рисунок 14	Вкладка Ограничения окна Создание политики доступа	28
Рисунок 15	Вкладка Общие данные окна Создание политики доступа	29
Рисунок 16	Вкладка Правила доступа окна Создание политики доступа	30
Рисунок 17	Вкладка Ограничения окна Создание политики доступа	32
Рисунок 18	Окно Создание политики мониторинга	34
Рисунок 19	Страница Создание отдела	36
Рисунок 20	Вкладка Синхронизация с доменом	37
Рисунок 21	Параметры синхронизации сотрудников из каталога домена	37
Рисунок 22	Страница Добавление сотрудника	39
Рисунок 23	Вкладка Сотрудники страницы Отдел «Наименование отдела»	41
Рисунок 24	Окно Доступ для отдела	42
Рисунок 25	Страница Служебные устройства	43
Рисунок 26	Страница Редактирование сотрудника «Фамилия Имя»	44
Рисунок 27	Вкладка Устройства страницы Организация	45
Рисунок 28.	Окно Назначение политик	46
Рисунок 29	Страница Создание группы устройств	47
Рисунок 30	Страница синхронизации группы с доменом	48
Рисунок 31	Окно Синхронизация группы устройств	48
Рисунок 32	Окно Генерация ключа	50
Рисунок 33	Страница Добавление устройства	52
Рисунок 34	Окно Приглашение в организацию	52
Рисунок 35	Окно Сообщение	53
Рисунок 34	Окно Уведомление	53
Рисунок 37	Окно Введите номер лицензии	54
Рисунок 38	Окно Доступ для своих сотрудников	55
Рисунок 39	Окно Доступ для отделов	57
Рисунок 40	Окно Отправка запроса на сбор данных	59
Рисунок 41	Страница Создание коллекции устройств	61
Рисунок 42	Окно Редактирование коллекции устройств	62
Рисунок 43	Окно Добавление правила	62
Рисунок 44	Окно Добавление правила – По данным инвентаризации	64
Рисунок 45	Окно Добавление правила – по информации об устройстве	65
Рисунок 46	Окно Заявка на обслуживание в сервисную организацию	69
Рисунок 47	Окно Настройка доступа для устройства	70
Рисунок 48	Окно Назначение отделов для обслуживания	72
Рисунок 49	Список доменов служб каталогов	73
Рисунок 50	Создание домена служб каталогов	74
Рисунок 51	Страница Системный журнал действий	78

Рисунок 52	Окно Статистика	80
Рисунок 53	Панель Фильтр	80
Рисунок 54	Окно графика	81
Рисунок 55	Страница Устройства	82
Рисунок 56	Окно Настройки автодобавления устройств в организацию	84
Рисунок 57	Окно Добавление в организацию	85
Рисунок 58	Страница Создание лицензии	88
Рисунок 59	Страница Роли доступа	89
Рисунок 60	Окно Учетная запись	91
Рисунок 61	Страница Категории заявок	95
Рисунок 62	Страница Категории заявок. Создание	96
Рисунок 63	Режимы работы	97
Рисунок 64	Группа настроек SMTP-сервер	98
Рисунок 65	Группа настроек Сервер обновления клиентского приложения	98
Рисунок 66	Группа настроек Директории для хранения файлов	99
Рисунок 67	Группа настроек Информационные сообщения	100
Рисунок 68	Группа настроек Режимы аутентификации	100
Рисунок 69	Группа настроек параметры аутентификации через Keycloak	101
Рисунок 70	Группа настроек Учетная запись	102
Рисунок 71	Вкладка Политика доступа по умолчанию	104
Рисунок 72	Подраздел Шаблоны конфигураций	105
Рисунок 73	Страница Создание группы шаблонов конфигурации	106
Рисунок 74	Страница Создание шаблона конфигурации	106
Рисунок 75	Страница Редактирование шаблона конфигурации	107
Рисунок 76	Вкладка Сценарий шаблона	107
Рисунок 77	Вкладка Атрибуты	108
Рисунок 78	Вкладка Тест выполнения	109
Рисунок 79	Вкладка Общие данные	110
Рисунок 80	Страница Создание задачи конфигурации	111
Рисунок 81	Вкладка Общие сведения задачи	112
Рисунок 82	Вкладка Устройства задачи	112
Рисунок 83	Окно Добавление устройств	113
Рисунок 84	Вкладка Коллекции задачи	113
Рисунок 85	Окно Добавление коллекции	114
Рисунок 86	Вкладка Шаблоны задачи	114
Рисунок 87	Окно Добавление шаблонов	115
Рисунок 88	Вкладка История выполнения	115
Рисунок 89	Записи запусков	116
Рисунок 90	Шаблоны устройства задачи	116
Рисунок 91	Лог выполнения шаблона	117

1. ОБЩИЕ СВЕДЕНИЯ

Система удаленного мониторинга и управления «Ассистент PRO» (далее – **Система, Ассистент PRO**) предназначена для удаленного мониторинга, управления, обслуживания персональных компьютеров и серверов, организации и оказания удаленной технической поддержки, организации удаленной работы и обучения.

Система состоит из **серверной** и **клиентской** частей. **Личный кабинет** относится к серверной части, клиентская состоит из **Клиентского приложения**.

Серверная часть предназначена для обеспечения взаимодействия между клиентскими частями, управления настройками, хранения пользовательской информации и т.д. Управление различными частями инфраструктуры **Системы** осуществляется посредством **Личного кабинета**.

1.1. Назначение личного кабинета

Личный кабинет системы удаленного мониторинга и управления «Ассистент PRO» (далее – **Личный кабинет**) представляет собой **web-портал**, предназначенный для работы с личными кабинетами пользователей и конфигурирования **Системы**.

Личный кабинет пользователя предназначен для управления реестром собственных и обслуживающих (сервисных) организаций, адресными книгами пользователей, политиками доступа и протоколирования, управления заявками на обслуживание и прочими настройками различных компонентов **Системы**. Он поддерживает работу в основных популярных браузерах, обновленных до актуальной версии.

Личный кабинет пользователя позволяет:

- вести личный список устройств;
- управлять организациями;
- объединять устройства в динамические группы (коллекции);
- управлять политиками доступа к устройствам;
- предоставлять доступ к устройствам сотрудникам организации;
- предоставлять доступ к устройствам сторонним сервисным организациям;
- настраивать протоколирование;
- анализировать статистику работы компонентов;
- настраивать правила сбора параметров при инвентаризации устройств;
- управлять конфигурациями устройств;
- импортировать и синхронизировать устройства и пользователей с доменами;
- настраивать различные компоненты **Системы**.

1.2. Принцип работы

Личный кабинет представляет собой **web-портал**, который доступен после развёртывания **Системы**. В личном кабинете пользователям доступны инструменты для настройки **Системы**, ведения адресных книг, просмотра и управления журналами Подсистемы протоколирования и прочие операции.

В данном документе описаны основные возможности **Личного кабинета**. Наличие разделов, подразделов и функций вашего **Личного кабинета** будет зависеть от предоставленных вам **прав** и **параметров лицензии**.

2. АВТОРИЗАЦИЯ

В главе описываются процессы регистрации, авторизации и восстановления пароля пользователя.

Для получения доступа к средствам **Личного кабинета** необходимо **Авторизоваться**. Для авторизации необходимо получить учетные данные – **имя пользователя** (в этом качестве используется адрес электронной почты) и **пароль**.

2.1. Регистрация

Получить учетную запись пользователь может как в **Клиентском приложении**, так и в **Личном кабинете Системы**.

Внимание! Если вы воспользовались для регистрации в Системе средствами Клиентского приложения, используйте для входа в Личный кабинет полученные ранее учетные данные. Для работы с Личным кабинетом и Клиентским приложением используется единая учетная запись!

Примечание: О процедуре регистрации посредством Клиентского приложения читайте в документе **Руководство пользователя. Клиентское приложение**.

Для регистрации учетной записи:

1. Введите в адресную строку браузера адрес, по которому доступен сервис **Личный кабинет**.



Откроется страница **Вход в личный кабинет**.

2. Нажмите кнопку **Регистрация учетной записи**.



Откроется страница **Регистрация учетной записи**.

3. На странице **Регистрация учетной записи** заполните поля:
 - о Электронная почта;
 - о Имя;
 - о Пароль;
 - о Подтвердите пароль;
 - о Введите код с картинки.
4. Нажмите кнопку **Зарегистрировать учетную запись**.

Рисунок 1 Страница Регистрация учетной записи



На указанный адрес электронной почты будет отправлено **письмо** с инструкциями для продолжения регистрации.

5. Для подтверждения регистрации перейдите по ссылке, указанной в письме.



Откроется страница **Завершение регистрации**. Ваша учетная запись успешно активирована. Регистрация в **Системе** завершена.

Внимание! Для защиты системы от множественной автоматической регистрации роботами-программами возможно включить подтверждение компьютерного текста (капчу) на этапе регистрации пользователя и при смене электронной почты в профиле. Для этого требуется добавить строку `<UseCaptcha>true</UseCaptcha>` между `<ConnectionsConfig...>` и `</ConnectionsConfig>` в файл настроек личного кабинета `assistant.config`. По-умолчанию файл находится в каталоге `C:\inetpub\MyAssistant.Office` для Windows и `\usr\share\assistant\ast-office` для Linux.

2.2. Вход в личный кабинет

Чтобы войти в **Личный кабинет**, пользователю необходимо авторизоваться в **Системе**, указав **Логин** (адрес электронной почты) и **Пароль**.

Для входа в **Личный кабинет**:

1. Откройте в браузере адрес, по которому находится сервис.



Откроется страница **Вход в личный кабинет**.

2. Введите данные учетной записи и нажмите кнопку **Вход** или **Вход через Keucloak** (при необходимости выберите домен для выхода в учетную запись).



Откроется страница **Мои устройства**. Имя вашей учетной записи будет указано на панели в правом верхнем углу страницы.

Рисунок 2 Страница Вход в личный кабинет

Примечание: Если адрес **Личного кабинета** вам неизвестен, уточните его у ответственного сотрудника или воспользуйтесь для доступа в **Личный кабинет** **Клиентским приложением**. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

Также на странице **Вход в личный кабинет** вы можете:

- перейти к восстановлению пароля;
- перейти к регистрации новой учетной записи;
- повторно запросить инструкции для окончания регистрации.

2.3. Восстановление пароля

Если по каким-то причинам пароль был утерян, его можно восстановить, воспользовавшись функцией восстановления пароля.

Для восстановления пароля:

1. Введите в браузер адрес, по которому доступен **Личный кабинет**.



Откроется страница **Вход в личный кабинет**.

2. Перейдите по ссылке для восстановления пароля.



Откроется страница **Восстановление доступа**.

3. Укажите адрес электронной почты, для которого необходимо восстановить пароль и нажмите кнопку **Восстановить доступ**.



Откроется страница **Восстановление пароля**. На указанный адрес электронной почты будет отправлено письмо с дальнейшими инструкциями по восстановлению пароля.

4. Выполните приведенные в письме инструкции.



Откроется страница **Изменение пароля**.

5. Введите новый пароль и подтверждение пароля.

6. Нажмите кнопку **Сохранить новый пароль**.



Вы будете авторизованы в **Личном кабинете** с новым паролем. Откроется страница **Мои устройства**. Пароль успешно изменен.

3. МОЙ АССИСТЕНТ

В главе приводится описание работы с личным списком устройств, добавления устройств в организации, описание профиля пользователя, настроек безопасности и работы с организациями.

Раздел **Мой ассистент** предназначен для ведения списка личных устройств и управления профилем пользователя. Раздел включает два подраздела:

- **Устройства** – предназначен для управления личным списком устройств пользователя.
- **Профиль** – содержит настройки профиля пользователя.

3.1. Мои устройства

Подраздел **Устройства** предназначен для ведения личного списка устройств пользователя.

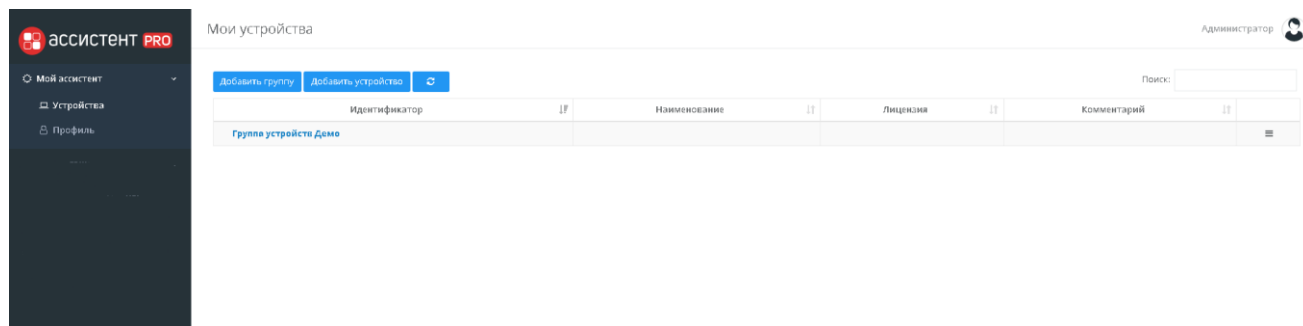


Рисунок 3 Окно Мои устройства

Примечание: Личный список устройств пользователя также доступен авторизованному пользователю в **Клиентском приложении** в списке **Мои устройства** раздела главного окна **Устройства**. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

Личный список устройств позволяет быстро находить часто используемые устройства, сохранять пароли для подключения к ним, группировать устройства, хранить описания.

Подраздел содержит следующие элементы управления:

Добавить группу	Все устройства распределяются по группам. Группы могут иметь любой уровень вложенности и позволяют объединять и систематизировать списки личных устройств.
Добавить устройство	Добавляет новое устройство.
Обновить	Обновляет список устройств.
Действия	Позволяет изменять и удалять группы и устройства.

3.1.1. Создание группы устройств

Для добавления устройства в личный список устройств необходимо указать **Группу устройств**. Для создания группы устройств:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет).

»»» Откроется страница **Мои устройства**.

2. Нажмите кнопку **Добавить группу** в списке групп.

»»» Откроется страница **Создание группы устройств**.

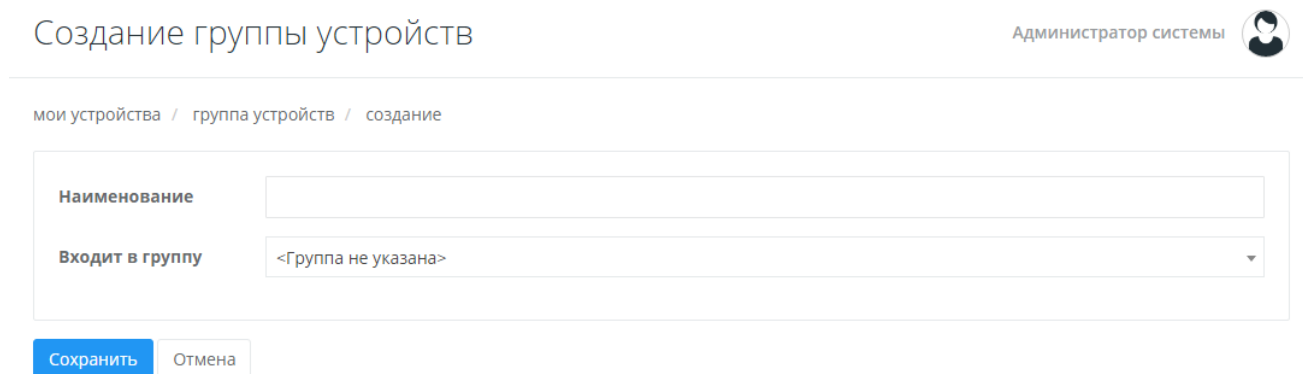


Рисунок 4 Страница Создание группы устройств

3. Заполните **Наименование**.
4. При необходимости укажите, в какую группу входит создаваемая группа.
5. Нажмите кнопку **Сохранить**.

»»» Откроется страница **Мои устройства**. Созданная **группа** появится в списке устройств.

3.1.2. Добавление устройства

Для добавления нового устройства в список:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет).

»»» Откроется страница **Мои устройства**.

2. Удостоверьтесь, что в списке устройств есть хотя бы одна **Группа устройств**. Если список устройств пуст, перед продолжением выполните действия, описанные в пункте 3.1.1 Создание группы устройств.

3. Нажмите кнопку **Добавить устройство** в списке устройств.

»»» Откроется страница **Добавление устройства**.

мои устройства / создание

Группа	группа поддержки ▾
Идентификатор	
Наименование	
Комментарий	
Пароль	
Подтверждение пароля	

Рисунок 5 Страница Добавление устройства

4. Заполните обязательные поля страницы:
 - **Группа** – выберите из списка групп.
 - **Идентификатор** – введите идентификатор устройства.
 - **Наименование** – введенное наименование будет отображаться в списках **Клиентского приложения** вместо идентификатора устройства.
5. При необходимости заполните:
 - **Комментарий**;
 - **Пароль** и **Подтверждение пароля**.
6. Нажмите кнопку **Сохранить**.

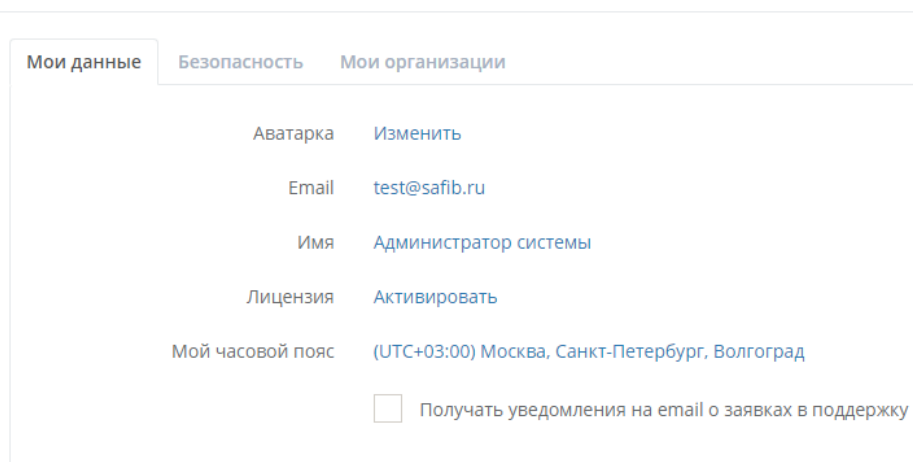


Откроется страница **Мои устройства**. Созданное устройство отобразится на странице в выбранной группе.

3.2. Профиль

Подраздел **Профиль** предназначен для настройки личных и контактных данных пользователя, параметров безопасности учетной записи, а также для работы с организациями.

Профиль



Мои данные	Безопасность	Мои организации
Аватарка	Изменить	
Email	test@safib.ru	
Имя	Администратор системы	
Лицензия	Активировать	
Мой часовой пояс	(UTC+03:00) Москва, Санкт-Петербург, Волгоград	
☐ Получать уведомления на email о заявках в поддержку		

Рисунок 6 Страница Профиль. Вкладка Мои данные

Данные профиля разделены на вкладки:

- **Мои данные** – вкладка предназначена для хранения и редактирования личных данных пользователя;
- **Безопасность** – вкладка предназначена для настройки пароля, управления параметрами аутентификации и прочими параметрами безопасности;
- **Мои организации** – во вкладке отображаются организации, в которых пользователь является сотрудником.

Примечание: При выключенной настройке **Самостоятельная регистрация пользователей** для изменения доступен только атрибут **Аватарка** на вкладке **Мои данные** и **Пароль** на вкладке **Безопасность**. Подробнее о настройке **Самостоятельная регистрация пользователей** в пункте 7.8 Настройки.

3.2.1. Мои данные

Вкладка **Мои данные** содержит информацию, которую пользователь указал при регистрации. Её можно изменить, дополнить графическим изображением и указать свой часовой пояс.

На вкладке хранится следующая информация:

- **Аватарка** – графическое изображение, используемое для персонификации профиля.
- **Email** – используется в качестве логина при входе в **Систему**.
- **Имя** – имя, отображаемое в компонентах **Системы**.
- **Лицензия** – лицензия, активированная для текущей учетной записи.

- **Мой часовой пояс** – влияет на отображение даты и времени в разделах **Личного кабинета**.
- **Получать уведомления на email о заявках в поддержку** – включает отправку почтовых уведомлений о поступивших заявках в поддержку.

Для изменения личных данных достаточно нажать на поле, информацию в котором необходимо поменять и, произведя изменения в открывшемся окне **Изменение**, сохранить новые данные.

Примечание: При изменении адреса электронной почты **новый адрес** необходимо будет подтвердить **Кодом безопасности**. Код будет направлен на новый адрес электронной почты.

3.2.2. Безопасность

На вкладке **Безопасность** сосредоточены основные настройки безопасности профиля.

Доступные для настройки параметры безопасности:

- **Телефон** – номер телефона для двухфакторной аутентификации через **Telegram**. Ввод кода подтверждения и его повторная отправка.
- **Пароль** – пароль учетной записи для аутентификации в **Личном кабинете** и в **Клиентском приложении**. Для его изменения достаточно нажать на значение поля и, указав в открывшемся окне старый пароль и новый пароль с его подтверждением, сохранить данные.
- **Требуется двухфакторная аутентификация** – признак включения двухфакторной аутентификации по **E-mail** или **Telegram**.

Двухфакторная аутентификация – это метод контроля доступа, при котором пользователю требуется подтвердить личность не только стандартным вводом пароля, но и дополнительным кодом, который он получит по известному только ему каналу связи.

В **Системе** двухфакторная аутентификация реализована с использованием **электронной почты** и **Telegram**.

Примечание: Управление двухфакторной аутентификацией и прочими настройками профиля пользователя также доступно в **Клиентском приложении**. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

Для включения **Двухфакторной аутентификации** установите соответствующий признак и в случае, если доступно несколько методов аутентификации, выберите нужный.

3.2.3. Мои организации

На вкладке **Мои организации** подраздела **Профиль** содержится список организаций, к которым пользователь присоединился. В списке отображается информация об организации и статус вашего пользователя:

- **Активен** – пользователь **добавлен** в организацию.

- **Заблокирован** – пользователь **заблокирован** либо **покинул** организацию.

Для выхода из организации **Активный** пользователь должен нажать кнопку  **Действия**, выбрать пункт **Выйти из организации** и подтвердить действие.

Внимание! Учетная запись Пользователя, который покинул организацию, помечается как архивная. Пользователь не сможет самостоятельно вернуться в организацию.

4. МОИ ОРГАНИЗАЦИИ

В главе приведено описание подразделов раздела **Мои организации**. Раздел содержит информацию об организациях, их отделах, политиках доступа, сотрудниках и устройствах.

Раздел **Мои организации** предназначен для настройки организаций, обработки заявок на техническую поддержку и распределения прав сотрудников организаций.

Раздел **Мои организации** может содержать следующие подразделы:

- **Организации** – подраздел содержит информацию об организациях, в которых вы являетесь сотрудником и организациях, к устройствам которых Вам предоставлен доступ.
- **Заявки в поддержку** – подраздел содержит информацию о заявках на техподдержку:
 - о созданных на устройствах организаций, в которых вы состоите;
 - о адресованных организациям, в которых вы состоите.

4.1. Организации

Подраздел содержит перечень собственных организаций и организаций клиентов. Функционал подраздела позволяет управлять свойствами организаций и настраивать их взаимодействие.

Организация объединяет в себе следующие сведения:

- **О компании** – общие сведения об организации, включая ее наименование, контактную информацию, признаки ведения журнала действий и отношение к сервисным организациям.
- **Устройства** – содержит перечень устройств организации.
- **Коллекции** – набор предустановленных фильтров для удобного поиска устройств.
- **Политики доступа** – содержит список политик, назначаемых устройствам и отделам для распределения полномочий.
- **Сотрудники** – перечень сотрудников и список отделов организации. В рамках отдела определяется модель доступа сотрудников к устройствам организации.
- **Сервисные организации** – перечень сервисных организаций, на обслуживании которых находится организация. Для Сервисной организации определяется список устройств и права доступа к ним у сотрудников сервисной организации.
- **Клиенты** – перечень обслуживаемых организаций. Для устройств обслуживаемой организации определяется отдел, ответственный за обслуживание.
- **Политики мониторинга** – содержит список политик, назначаемых устройствам для последующего сбора данных о программной и аппаратной конфигурации.

Примечание: Набор свойств организации определяется **статусом** организации и **правами** пользователя. Некоторые вкладки могут быть недоступны.

Система позволяет настроить **внутреннюю** и **внешнюю** техническую поддержку устройств организаций.

Внутренняя поддержка подразумевает, что к устройствам организации будут иметь доступ только сотрудники этой организации. Им будут адресоваться заявки на техподдержку от пользователей **Клиентского приложения**.

Примечание: Подробнее о создании и работе с **Заявками на техническую поддержку** читайте в документе **Руководство пользователя. Клиентское приложение**.

Сторонняя поддержка подразумевает, что к устройствам организации будут иметь доступ пользователи других организаций, которые в **Системе** называются **Сервисными**. Заявки на техподдержку от пользователей **Клиентского приложения** могут быть адресованы как сотрудникам **Сервисной организации**, так и внутренней службе поддержки.

Организации, доступные пользователю в **Личном кабинете**, представлены в виде **Карточек организаций**. Карточки разделяются на 2 группы:

- **Мои организации** – организации, в которых вы являетесь сотрудником;
- **Клиенты** – сторонние организации, к устройствам которых пользователю предоставлен доступ.

Мои организации

Администратор системы



Добавить организацию

ООО "Клиент"

* Активная

Email:

Адрес:

Контакты:



1



1

ООО "Организация"

Сервисная организация * Активная

Email:

Адрес:

Контакты:



2



2



0



0

Рисунок 7 Страница Мои организации

В зависимости от **статуса** пользователя **Карточка организации** может содержать следующие пиктограммы:

	Количество подтвержденных устройств в организации.
	Количество активных сотрудников в организации.
	Количество устройств на обслуживании.
	Количество необработанных заявок на аутсорсинг от организации.

4.1.1. Управление организациями

Создание организации

Создание организации доступно только **Администратору системы**. Редактирование организации доступно **Администратору организации** с включенной ролью **Организации**.

Для создания организации:

1. Войти в **Личный кабинет** под учетной записью **Администратора системы**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите кнопку **Добавить организацию**.



Откроется страница **Создание организации**.

Создание организации

Администратор системы



организации / создание

Наименование	<input type="text" value="ООО " организация"=""/>
Адрес месторасположения	г. Воронеж
Контактный телефон	+7(473)239-96092
Адрес электронной почты	office@organization.ru
	☒ Включить ведение журнала действий
	☐ Является сервисной организацией

Рисунок 8 Страница Создание организации

4. Введите общие данные о организации и нажмите кнопку **Сохранить**.

Примечание: При создании организации автоматически создается группа устройств с названием **Новая группа**, отдел с названием **Новый отдел** и политика доступа **Базовая**, которая использует права доступа, указанные в системных настройках.

Изменение организации

Для изменения свойств организации:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, которую необходимо изменить.



Откроется страница **Организация «Наименование организации»**.

4. Для изменения сведений **О компании** нажмите кнопку **Изменить**.



Откроется страница **Редактирование организации**. Атрибуты организации доступны для коррекции.

5. Внесите необходимые изменения.

6. Нажмите кнопку **Сохранить**.



Внесенные изменения сохранены.

Сервисная организация

Если организация будет осуществлять техническую поддержку других организаций, то ее необходимо сделать **Сервисной**. Для этого в общих сведениях об организации установите флаг **Является сервисной организацией**.

Сервисной организации будет присвоен **Код сервисной организации**, сообщив который клиенту, вы сможете взять его на обслуживание.

Примечание: Подробнее о работе с **Сервисными организациями** в пункте 4.1.7 Сервисные организации.

Удаление организации

Полное удаление организации возможно только в случае, если в ней отсутствуют устройства, сотрудники, а также если организация не является **Сервисной** или **Клиентом**. Если в организации остались сотрудники, находящиеся в архиве, то организация полностью не удаляется, а помещается в архив, принимая соответствующий статус.

Удаление организации доступно **Администратору системы**.

Для удаления организации воспользуйтесь кнопкой **Удалить организацию** на странице редактирования организации.

Восстановление организации

Если организация была помещена в архив (статус организации **В архиве**), ее можно восстановить и возобновить с ней работу.

Восстановление организации доступно **Администратору** организации, с включенной ролью **Организации**.

Для восстановления организации воспользуйтесь кнопкой **Восстановить из архива** на странице просмотра архивной организации.

4.1.2. Политики доступа

Политики доступа предназначены для хранения настроек прав доступа, протоколирования и установки ограничений на использование устройств по дням недели и времени. **Политики доступа** распределены по отдельным категориям:

- **Политики для устройств** – определяют права доступа при подключении к устройствам;
- **Политики для сотрудников** – применяются при назначении доступа на уровне отделов;
- **Политики инвентаризации** – определяют параметры сбора информации о программной и аппаратной конфигурации устройства.

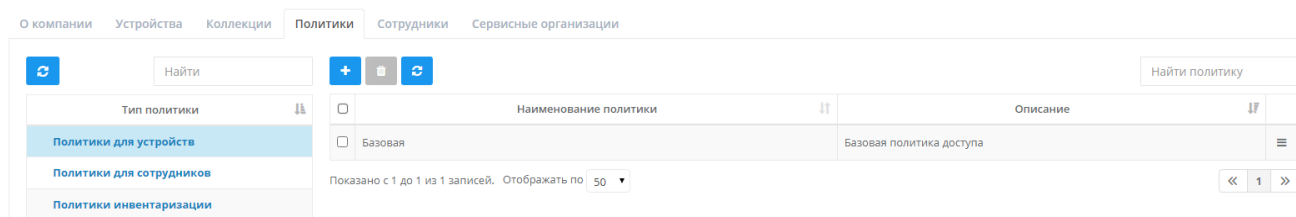


Рисунок 9 Вкладка Политики доступа страницы Организация

Политики доступа применяются при подключении к устройству.

При создании организации на основе **Политики доступа по умолчанию**, указанной в **Системных настройках** (подробнее в пункте 7.8 **Настройки**), автоматически создается **Базовая** политика доступа. **Администратор Организации**, с включенной ролью **Организации** может создавать любое количество политик доступа.

4.1.2.1. Создание новой политики для устройств

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 **Вход в личный кабинет**) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать новую политику доступа.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Политики**, раздел **Политики для устройств**.

»»» Откроется список политик доступа для устройств.

5. Нажмите кнопку **Добавить политику**.

»»» Откроется страница **Создание политики для устройств**. Вкладка **Общие данные**.

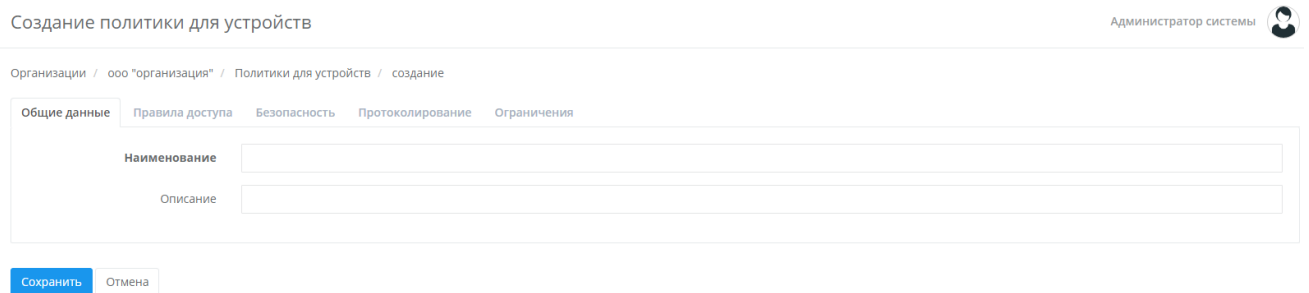


Рисунок 10 Вкладка Общие данные окна Создание политики доступа

6. Заполните поля:

- о **Наименование** – название политики доступа.
- о **Описание** – краткое текстовое описание (необязательно).

7. Перейдите на вкладку **Правила доступа**.

»»» Откроется вкладка **Правила доступа**.

Общие данные
Правила доступа
Безопасность
Протоколирование
Ограничения

При назначении политики доступа сотрудникам настройки раздела имеют приоритет перед настройками политики устройства.

Соединение	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Управление рабочим столом	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Обмен файлами	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр ☐ С ограничениями
Редактор реестра	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Диспетчер задач	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Диспетчер устройств	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Информация о системе	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Командная строка	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Управление питанием	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Удаленная печать	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Подключение usb-токенов	☐ Разрешено ☒ С подтверждением ☐ Запрещено
TCP туннель	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Чат	☒ Разрешено ☐ Запрещено
Обмен сторонами	☒ Разрешено ☐ Запрещено

☐ Доступ к модулям до входа в ОС
☒ Удаленное управление настройками
☒ Разрешать блокировку средств ввода
☒ Разрешать блокировать устройство после завершения соединения
☒ Синхронизация буфера обмена
☐ Разрешать соединение до входа в ОС, если доступ "С подтверждением"
☐ Не требовать пароль при подключении

Сообщение при подключении

Сохранить
Отмена

Рисунок 11 Вкладка Правила доступа окна Создание политики доступа

8. Настройте доступ к необходимым модулям.

На вкладке **Правила доступа**, кроме признаков степени доступа к модулям, доступны следующие настройки:

Разрешить повышенные права	Модуль Обмен файлами будет работать с повышенными правами. Внимание! Включение признака не только повысит скорость копирования, но и разрешит доступ в системные папки.
Доступ к модулям до входа в ОС	До входа в Windows можно будет использовать модули Обмен файлами, Редактор реестра и Командная строка. До входа в Linux можно будет использовать модуль Обмен файлами. Внимание! Доступ осуществляется с использованием системной учетной записи. «Система» для Windows и «root» для Linux.
Удаленное управление настройками	Разрешить менять настройки приложения Ассистент PRO и делать выбор в окнах подтверждения Ассистент PRO.
Разрешить блокировку средств ввода	Определяет возможность блокировки средств ввода удаленным устройством при активном сеансе управления.
Разрешить блокировать устройство после завершения соединения	Определяет возможность автоматического перехода устройства на экран блокировки после разрыва соединения.
Синхронизация буфера обмена	Определяет возможность включения синхронизации буфера обмена при активном сеансе управления.
Разрешать соединение до входа в ОС, если доступ «С подтверждением»	Определяет возможность подключения к устройству, если в качестве правила доступа используется С подтверждением , но пользователь не авторизован с учетной записью Ассистент PRO .
Не требовать пароль при подключении	Отключает необходимость ввода пароля при подключении удаленного устройства.
Сообщение при подключении	Позволяет ввести текст, который будет отображаться в качестве сообщения при подключении на стороне устройства, к которому будет применена вновь создаваемая политика доступа. Поле доступно при включенной настройке политики доступа Соединение: С подтверждением.

Примечание: вариант правил доступа **С ограничениями** к модулю **Обмен файлами** разрешает копирование файлов на удаленное устройство, а также просмотр без возможности копирования и удаления с ведомого устройства.

9. Перейдите на вкладку **Безопасность**



Откроется вкладка **Безопасность**.

Общие данные Правила доступа **Безопасность** Протоколирование Ограничения

Настройки раздела применяются только при назначении политики доступа устройству и не применяются при назначении сотруднику.

Динамический пароль Безопасный (6 символов)

☐ Менять пароль

Фиксированный пароль

Подтверждение пароля

☐ Разрешить аутентификацию Windows

☐ Запретить выход из Ассистент неавторизованным пользователям

☒ Разрешить неконтролируемый доступ

☐ Разрешить скрытое подключение

☐ Только если нет активных сессий

☒ Автоматическое обновление клиентского приложения

☒ Запускать при старте ОС

☒ Блокировать Ассистент при бездействии

Время бездействия (минуты) 5

Сохранить Отмена

Рисунок 12 Вкладка Безопасность окна Создание политики доступа

10. Настройте параметры безопасности для **Клиентского приложения**:
- **Динамический пароль** – сложность генерируемого пароля.
 - **Менять пароль** – настройки периодичности смены динамического пароля.
 - **Фиксированный пароль** – пароль для постоянного доступа.
 - **Подтверждение пароля** – подтверждение пароля для постоянного доступа.
 - **Разрешить аутентификацию в Windows** – разрешение использовать для авторизации учетные данные операционной системы.
 - **Только с учетными данными Администратора** – разрешает авторизацию только посредством учетной записи обладающей правами Администратора Windows.
 - **Даже если активен другой пользователь** – разрешает авторизацию посредством учетной записи операционной системы с принудительным завершением текущего активного сеанса.

Примечание: Признаки **Даже если активен другой пользователь** и **Только с учетными данными Администратора** доступны при включении **Разрешить аутентификацию в Windows**.

- **Запретить выход из Ассистент PRO неавторизованным пользователям** – только авторизованные пользователи смогут закрыть **Ассистент PRO**.
- **Разрешить неконтролируемый доступ** – разрешить использование неконтролируемого доступа на устройствах.

Примечание: Флаг **Разрешить неконтролируемый доступ** позволяет предоставить доступ к управлению удаленным рабочим столом и прочим возможностям **Ассистент PRO**, включая доступ к файлам и реестру устройства даже в случае, если **Приложение** не запущено. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

- **Разрешить скрытое подключение** – разрешить подключение к устройству без участия пользователя.
- **Только если нет активных сессий** – запрещает подключение к устройству, если на устройстве запущена активная сессия **Windows**.

Примечание: Флаг **Разрешить скрытое подключение** позволяет предоставить доступ к управлению удаленным рабочим столом и прочим возможностям **Ассистент PRO** без ведома пользователя устройства, к которому осуществляется подключение. Для включения данной настройки необходимо предварительно активировать флаг **Разрешить неконтролируемый доступ**.

Подробнее в документе **Руководство пользователя. Клиентское приложение**.

- **Автоматическое обновление клиентского приложения** – разрешить обновление клиентского приложения на устройстве без участия пользователя.
- **Запускать при старте ОС** – автоматически запускать приложение при старте операционной системы.
- **Блокировать Ассистент PRO при бездействии** – блокирование работы приложения если нет активных действий в течение указанного времени.

11. Перейдите на вкладку **Протоколирование**.



Откроется вкладка **Протоколирование**.

Создание политики для устройств

Администратор системы

Организации / ооо "организация" / Политики для устройств / создание

Общие данные Правила доступа Безопасность **Протоколирование** Ограничения

Настройки раздела применяются только при назначении политики доступа устройству и не применяются при назначении сотруднику.

☐ События взаимодействия

☐ Записи видео сеансов

☐ Снимки экрана

☐ Технические протоколы

Срок хранения технических протоколов (дней) 14

Сохранить Отмена

Рисунок 13 Вкладка **Протоколирование** окна **Создание политики доступа**

12. Отметьте события, сведения о которых необходимо хранить на сервере:
- **События взаимодействия** – протоколирование всех действий в **Клиентском приложении**, совершаемых при управлении удаленным устройством.
 - **Записи видео сеансов** – записи видео сеансов управления удаленным устройством будут храниться на сервере
 - **Снимки экрана** – снимки экрана при управлении удаленным устройством будут храниться на сервере.
 - **Технические протоколы** – файлы протоколов **Клиентских приложений** будут храниться на сервере.
 - **Срок хранения технических протоколов (дней)** – период, в течение которого протоколы **Клиентских приложений** будут храниться на сервере.
13. В случае если необходимо ограничить время работы по дням недели или рабочему времени, перейдите на вкладку **Ограничения**.

»»» Откроется вкладка **Ограничения**.

Создание политики для устройств Администратор системы 

Организации / ооо "организация" / Политики для устройств / создание

Общие данные Правила доступа Безопасность Протоколирование **Ограничения**

При назначении политики доступа сотруднику настройки раздела имеют приоритет перед настройками политики устройства.

Дни недели

☒ Понедельник

☒ Вторник

☒ Среда

☒ Четверг

☒ Пятница

☒ Суббота

☒ Воскресенье

Время доступа ☒ Круглосуточно ☐ с 8:00 до 17:00 ☐ с 9:00 до 18:00 ☐ с 10:00 до 19:00

Рисунок 14 Вкладка Ограничения окна Создание политики доступа

14. Установите необходимые настройки ограничения доступа по дням недели или рабочему времени.
15. Нажмите кнопку **Сохранить**.

»»» Созданная **Политика** отобразится в **Списке политик для устройств**.

4.1.2.2. Создание новой политики для сотрудников

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать новую политику доступа.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Политики**, раздел **Политики для сотрудников**.

»»» Откроется список политик доступа для сотрудников.

5. Нажмите кнопку **Добавить политику**.

»»» Откроется страница **Создание политики для сотрудников**. Вкладка **Общие данные**.

Создание политики для сотрудников Администратор системы 

Организации / ооо "организация" / Политики для сотрудников / создание

Общие данные

Правила доступа

Ограничения

Наименование

Описание

Сохранить

Отмена

Рисунок 15 Вкладка Общие данные окна Создание политики доступа

6. Заполните поля:
 - о **Наименование** – название политики доступа.
 - о **Описание** – краткое текстовое описание (необязательно).
7. Перейдите на вкладку **Правила доступа**.

»»» Откроется вкладка **Правила доступа**.

Общие данные
Правила доступа
Безопасность
Протоколирование
Ограничения

При назначении политики доступа сотрудникам настройки раздела имеют приоритет перед настройками политики устройства.

Соединение	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Управление рабочим столом	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Обмен файлами	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр ☐ С ограничениями
Редактор реестра	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Диспетчер задач	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Диспетчер устройств	☐ Разрешено ☒ С подтверждением ☐ Запрещено ☐ Только просмотр
Информация о системе	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Командная строка	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Управление питанием	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Удаленная печать	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Подключение usb-токенов	☐ Разрешено ☒ С подтверждением ☐ Запрещено
TCP туннель	☐ Разрешено ☒ С подтверждением ☐ Запрещено
Чат	☒ Разрешено ☐ Запрещено
Обмен сторонами	☒ Разрешено ☐ Запрещено

☐ Доступ к модулям до входа в ОС
☒ Удаленное управление настройками
☒ Разрешать блокировку средств ввода
☒ Разрешать блокировать устройство после завершения соединения
☒ Синхронизация буфера обмена
☐ Разрешать соединение до входа в ОС, если доступ "С подтверждением"
☐ Не требовать пароль при подключении

Сообщение при подключении

Сохранить
Отмена

Рисунок 16 Вкладка Правила доступа окна Создание политики доступа

8. Настройте доступ к необходимым модулям.

На вкладке **Правила доступа**, кроме признаков степени доступа к модулям, доступны следующие настройки:

Разрешить повышенные права	Модуль Обмен файлами будет работать с повышенными правами. Внимание! Включение признака не только повысит скорость копирования, но и разрешит доступ в системные папки.
Доступ к модулям до входа в ОС	До входа в Windows можно будет использовать модули Обмен файлами, Редактор реестра и Командная строка. До входа в Linux можно будет использовать модуль Обмен файлами. Внимание! Доступ осуществляется с использованием системной учетной записи. «Система» для Windows и «root» для Linux.
Удаленное управление настройками	Разрешить менять настройки приложения Ассистент PRO и делать выбор в окнах подтверждения Ассистент PRO.
Разрешить блокировку средств ввода	Определяет возможность блокировки средств ввода удаленным устройством при активном сеансе управления.
Разрешить блокировать устройство после завершения соединения	Определяет возможность автоматического перехода устройства на экран блокировки после разрыва соединения.
Синхронизация буфера обмена	Определяет возможность включения синхронизации буфера обмена при активном сеансе управления.
Разрешать соединение до входа в ОС, если доступ «С подтверждением»	Определяет возможность подключения к устройству, если в качестве правила доступа используется С подтверждением , но пользователь не авторизован с учетной записью Ассистент PRO .
Не требовать пароль при подключении	Отключает необходимость ввода пароля при подключении удаленного устройства.
Сообщение при подключении	Позволяет ввести текст, который будет отображаться в качестве сообщения при подключении на стороне устройства, к которому будет применена вновь создаваемая политика доступа. Поле доступно при включенной настройке политики доступа Соединение: С подтверждением.

Примечание: вариант правил доступа **С ограничениями** к модулю **Обмен файлами** разрешает копирование файлов на удаленное устройство, а также просмотр без возможности копирования и удаления с ведомого устройства.

9. В случае если необходимо ограничить время работы по дням недели или рабочему времени, перейдите на вкладку **Ограничения**.

» Откроется вкладка **Ограничения**.

При назначении политики доступа сотруднику настройки раздела имеют приоритет перед настройками политики устройства.

Дни недели

- ☒ Понедельник
- ☒ Вторник
- ☒ Среда
- ☒ Четверг
- ☒ Пятница
- ☒ Суббота
- ☒ Воскресенье

Время доступа ☒ Круглосуточно ☐ с 8:00 до 17:00 ☐ с 9:00 до 18:00 ☐ с 10:00 до 19:00

Сохранить

Отмена

Рисунок 17 Вкладка Ограничения окна Создание политики доступа

10. Установите необходимые настройки ограничения доступа по дням недели или рабочему времени.
11. Нажмите кнопку **Сохранить**.

» Созданная **Политика** отобразится в **Списке политик для сотрудников**.

4.1.3. Политики инвентаризации

Политики инвентаризации предназначены для хранения параметров инвентаризации аппаратных средств и программного обеспечения устройств, включенных в организацию. **Политики инвентаризации** закрепляются за отдельными устройствами с помощью функций **Личного кабинета** или **Клиентского приложения** и позволяют осуществлять сбор данных о текущей конфигурации программного и аппаратного обеспечения.

Совет: Групповое назначение **политик инвентаризации** возможно при приглашении устройств посредством **доменов**. Подробнее в пункте [4.1.5 Устройства](#).

Для создания **политики мониторинга**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать политику мониторинга.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Политики**, раздел **Политики инвентаризации**.

»»» Откроется список политик инвентаризации организации.

5. Нажмите кнопку **Добавить политику**.

»»» Откроется страница **Создание политики инвентаризации**.

Наименование

Описание

Инвентаризация

☐ Сбор данных автоматически

☒ Информация об оборудовании
 ☒ Установленное ПО
 ☐ Информация об обновлениях Windows
 ☐ История обновлений Windows
 ☒ Содержимое Program files
 ☒ Антивирусное ПО / Брандмауэр
 ☒ Кодеки
 ☒ Содержимое автозапуска
 ☒ Переменные среды
 ☒ Папки с общим доступом
 ☒ Службы
 ☒ Драйверы
 ☒ Пользователи ОС
 ☒ Запрашивать данные с контроллера домена
 ☒ Назначенные задания Windows

Сохранить

Отмена

Рисунок 18 Окно Создание политики мониторинга

6. Заполните поля:

- **Наименование** – название политики инвентаризации.
- **Описание** – краткое текстовое описание (необязательно).
- **Периодичность** – периоды сбора данных.

Возможные варианты:

- По запросу;
- 1 час;
- 1 неделя;
- 30 дней.

7. Отметьте **типы данных**, которые необходимо собирать в рамках создаваемой политики:

Информация об оборудовании	Сведения об аппаратной конфигурации устройства.
Установленное ПО	Информация, содержащаяся в разделе Программы и компоненты операционных систем семейства Windows и данные об установленных пакетах операционных систем семейства Linux .
Информация об обновлениях Windows	Набор обновлений операционной системы семейства Windows .

История обновлений Windows	Сведения об установленных пакетах обновлений операционных систем семейства Windows .
Содержимое Program Files	Содержимое папки Program Files .
Антивирусное ПО / Брандмауэр	Установленные антивирусные программы, брандмауэры и их настройки.
Кодеки	Список кодеков, установленных на устройстве.
Содержимое автозапуска	Содержимое папки Автозапуск .
Переменные среды	Список переменных среды и их значений.
Папки с общим доступом	Перечень папок, к которым предоставлен общий доступ.
Службы	Список установленных служб.
Драйверы	Список установленных драйверов.
Пользователи ОС	Перечень пользователей операционной системы.
Назначенные задания Windows	Перечень назначенных заданий планировщика операционной системы

8. Нажмите кнопку **Сохранить** в окне **Добавление новой политики**.

Созданная политика отобразится в списке вкладки **Политики инвентаризации** окна организации и будет доступна для назначения устройству.

4.1.4. Сотрудники

В разделе **Сотрудники** осуществляется управление персоналом организации:

- сотрудники группируются по отделам;
- назначаются права доступа к устройствам;
- настраиваются лицензии
- настраиваются служебные устройства,
- формируется структура организации.

Отделы

Отделы предназначены для настройки групповых прав доступа к обслуживаемым устройствам. **Отдел** хранит информацию о политиках доступа, применяемых для доступа сотрудников отдела к конкретным устройствам.

Создание отдела

Для создания отдела:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать новый отдел.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сотрудники**.

»»» Откроется список **сотрудников** и **отделов** организации.

5. Нажмите кнопку  **Добавить отдел**.

»»» Откроется страница **Создание отдела**.



Создание отдела

Администратор системы

Организации / тест varq / Сотрудники / создание

Наименование

Описание

Группы Keycloak

Возможно указание нескольких групп, например, "группа 1; группа 2".

Сохранить Отмена

Рисунок 19 Страница Создание отдела

6. Заполните **Наименование**, при необходимости, **Описание** и **Группы Keycloak**.

Примечание: При входе через **Keycloak** пользователей указанных групп, учетные записи будут автоматически добавлены в **Отдел**.

7. Нажмите кнопку **Сохранить**.

»»» Новый отдел будет сохранен. В окне **Отдела** появятся вкладки **Доступ к устройствам** и **Сотрудники**. Кнопка **Сохранить** изменится на **Изменить**.

С инхронизация с доменов

Вкладка **Синхронизация с доменом** на странице отдела организации предназначена для **импорта** учетных записей и **синхронизации** списка сотрудников отдела из **выбранного домена**.

Для синхронизации сотрудников отдела с **доменом**:

1. Откройте список **Отделов** организации во вкладке **Сотрудники**.
2. Выберите отдел, нажмите кнопку  **Действия** и выберите пункт **Открыть**.



Откроется страница **Отдел «Наименование отдела»**

3. Перейдите на вкладку **Синхронизация с доменом**.



Откроется вкладка **Синхронизация с доменом**

Организации / Новая / Сотрудники / Новый отдел

Общие данные Доступ к устройствам Доступ к коллекциям Синхронизация с доменом

Домен	
Уточняющий запрос	
Фильтр	
Периодичность	По запросу
Часовой пояс	
Если учетная запись была загружена ранее, обновлять атрибуты	Нет
Если найдена учетная запись с таким же Email, привязать	Нет
Удалять из отдела ранее импортированные, если не найдены в службе каталогов	Нет

[Изменить](#)

[Назад](#)

Рисунок 20 Вкладка Синхронизация с доменом

4. Нажмите кнопку **Изменить**.



Откроется страница редактирования параметров синхронизации

Организации / Новая / Сотрудники / Новый отдел / Синхронизация / редактирование

Домен	Не выбрано
Уточняющий запрос	
	По умолчанию: не указан
Фильтр	
	По умолчанию: не указан
Периодичность	По запросу
Часовой пояс	(UTC+03:00) Москва, Санкт-Петербург, Волгоград
☐ Если учетная запись была загружена ранее, обновлять атрибуты	
☐ Если найдена учетная запись с таким же Email, привязать	
☐ Удалять из отдела ранее импортированные, если не найдены в службе каталогов	

[Сохранить](#) [Отмена](#)

Рисунок 21 Параметры синхронизации сотрудников из каталога домена

5. Заполните поля:

- **Домен** – ранее созданный **домен**.
- **Уточняющий запрос** – **LDAP** запрос.
- **Фильтр** – фильтрация запроса по параметрам.

6. Укажите **Периодичность** синхронизации и прочие необходимые параметры.

7. Нажмите кнопку **Сохранить**.

Добавление сотрудника в организацию

Сотрудник – это зарегистрированный **пользователь** Системы, который был **добавлен** в состав **организации**. Права **Сотрудника** организации на доступ к **модулям** управления, настройки **времени доступа** и **протоколирования** определяются **политиками доступа**. **Сотруднику** организации доступен для быстрого доступа **перечень устройств**, определенный для **отдела**.

Добавление **Сотрудника** в **Организацию** происходит, в зависимости от настройки **Самостоятельная регистраций пользователей**:

- При **выключенной** настройке **Самостоятельная регистраций пользователей** состав **пользователей** организации определяется путем **добавления** новых пользователей в организацию. **Пользователь** получает уведомление о вступлении в организацию на адрес электронной почты. **Самостоятельно** пользователь зарегистрироваться **не может**.
- При **включенной** настройке **Самостоятельная регистраций пользователей** сотрудник добавляется в организацию сразу после регистрации в **Системе**.

Примечание: **Личный кабинет** позволяет добавить в организацию одновременно **несколько учетных записей**.

Для добавления сотрудника в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в которую необходимо добавить сотрудника.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сотрудники**.

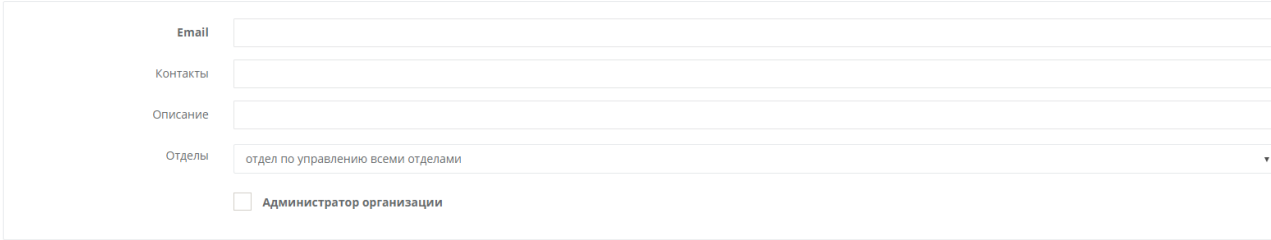


Откроется список сотрудников организации.

5. Нажмите кнопку  **Добавить сотрудника**.



Откроется страница **Добавление сотрудника**.



Email

Контакты

Описание

Отделы отдел по управлению всеми отделами ▼

☐ Администратор организации

Сохранить Отмена

Рисунок 22 Страница Добавление сотрудника

6. Заполните все обязательные поля. Нажмите кнопку **Сохранить**.

Примечание: На указанный **адрес электронной почты** будет отправлено **письмо с уведомлением** о добавлении в организацию. Если у пользователя на момент добавления в организацию нет учетной записи в **Системе**, её необходимо создать, используя в качестве логина **адрес электронной почты, на который пришло уведомление** о добавлении.

Прочие операции с сотрудниками

После добавления **Сотрудника** в организацию **Администратор Организации** посредством кнопки  **Действия** может:

- **заблокировать** активного сотрудника,
- **активировать** заблокированного,
- **удалить** сотрудника из отдела,
- **отправить** сотруднику **сообщение**,
- активировать сотруднику **лицензию**.

При выборе **нескольких** сотрудников нажатием на кнопку **Изменить** можно массово **заблокировать/разблокировать**, **поставить/убрать** признак **Администратор**, **добавить в отделы** и **назначить/очистить лицензию** у выбранных учётных записей.

Настройка отдела

Настройка отдела заключается в **определении состава** сотрудников отдела и их **полномочий**. Для определения состава отдела необходимо добавить в него пользователей, а для определения полномочий сотрудников отдела настроить доступ к устройствам.

Для добавления сотрудников в отдел:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в которую необходимо добавить сотрудника.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сотрудники**.



Откроется список сотрудников организации.

5. Выберите **отдел**, нажмите кнопку  **Действия** и выберите пункт **Просмотр**.



Откроется страница **Отдел «Наименование отдела»**.

6. Перейдите на вкладку **Сотрудники**.



Откроется список сотрудников отдела.

7. Нажмите кнопку **Добавить сотрудника**.



На странице **Отдел «Наименование отдела»** откроется список сотрудников организации.

8. Выберите сотрудников, которых необходимо добавить в отдел, и нажмите кнопку **Добавить**.



Выбранные сотрудники будут добавлены в отдел.

Общие данные Доступ к устройствам Коллекции устройств **Сотрудники** Синхронизация с доменом

[Добавить сотрудника](#) [Исключить сотрудника](#) 

Поиск:

☐	Статус	Имя сотрудника	Email сотрудника	Администратор
☐	Активен	admin	admin@IPA.LOCAL	Нет

Показано с 1 до 4 из 4 записей. Отображать по:

« 1 »

[Назад](#)

Рисунок 23 Вкладка Сотрудники страницы Отдел «Наименование отдела»

Примечание: Если необходимо исключить сотрудника из отдела, на вкладке **Сотрудники** выберите необходимую запись в перечне и нажмите кнопку **Исключить сотрудника**.

Сотрудник может состоять **в нескольких отделах одновременно**. Если для отделов сотрудника назначены разные права доступа, то при попытке подключения такого сотрудника к устройству **Система** определит для него **максимальные** из доступных прав.

Политики доступа

Для настройки политики доступа для отдела:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

 Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в которую необходимо добавить сотрудника.

 Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сотрудники**.

 Откроется список сотрудников организации.

5. Выберите отдел, нажмите кнопку  **Действия** и выберите пункт **Открыть**.

 Откроется страница **Отдел «Наименование отдела»**

6. Перейдите на вкладку **Доступ к устройствам**.

 Откроется список устройств организации.

7. Выберите устройства либо группу устройств и нажмите кнопку **Изменить доступ**.

»»» Откроется окно **Доступ для отдела**.

8. Определите, **разрешен ли доступ** к выбранным устройствам для сотрудников отдела и выберите **Политику доступа**.

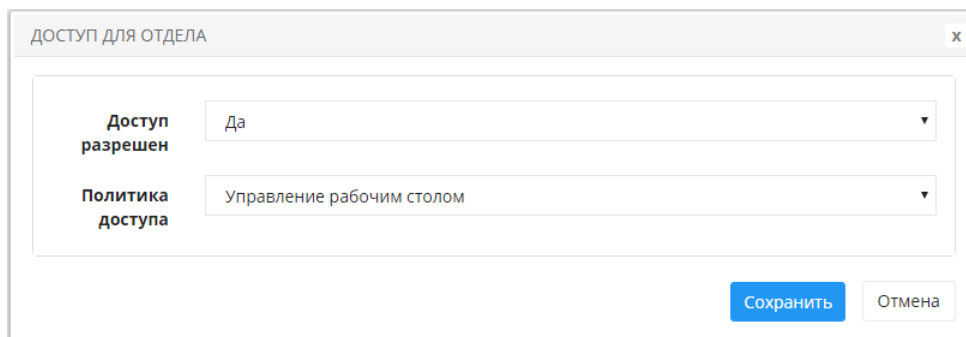


Рисунок 24 Окно Доступ для отдела

9. Нажмите кнопку **Сохранить**.

»»» Изменения будут сохранены. Откроется список устройств организации с обновленным данными.

Примечание: Настройка доступа к устройствам для отдела может быть произведена в списке устройств организации. Подробнее в пункте 4.1.5 Устройства.

Служебные устройства

Из соображений безопасности каждому сотруднику организации можно определить список служебных устройств. Если сотрудник авторизуется в **Клиентском приложении** на одном из своих служебных устройств, то ему будет доступен список устройств организации, и он сможет подключаться к ним в соответствии с настроенными политиками доступа. С других устройств пользователю будет доступна только **Базовая политика безопасности**.

Для настройки служебных устройств пользователя:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в которую необходимо добавить сотрудника.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сотрудники**.

Откроется **список сотрудников** организации.

5. В строке нужного **Сотрудника** нажмите кнопку  **Действия** и выберите **Просмотр**.

Откроется страница **Сотрудник фамилия Имя**.

6. Перейдите на вкладку **Служебные устройства**. Нажмите кнопку **Изменить**.

Откроется страница **Служебные устройства**.

Служебные устройства Администратор системы 

организации / ооо "сафиб" / сотрудники / Иванов Иван / служебные устройства / редактирование

Любые устройства

Нет

Внутренние устройства



Поиск:

	Устройство	Наименование
☐	Бухгалтерия	
☐	003 795 113	Главный бухгалтер
☐	150 959 522	astra

Внешние устройства

Сохранить

Отмена

Рисунок 25 Страница Служебные устройства

- а. Если сотруднику необходимо предоставить доступ ко всем устройствам организации установите в поле **Любые устройства** значение **Да**. Сотрудник сможет просматривать список устройств организации и подключаться к ним с любого устройства.
- б. Если сотруднику необходимо предоставить доступ к ограниченному перечню устройств установите в поле **Любые устройства** значение **Нет** и определите перечень устройств, к которым сотрудник должен иметь доступ.
7. Нажмите кнопку **Сохранить**.

Откроется обновленный список устройств сотрудника на вкладке **Служебные устройства** страницы **Сотрудник фамилия Имя**.

Администратор организации

Администратор Организации обладает следующими правами:

- изменение информации **О компании**;
- приглашение **Устройств** в организацию;
- добавление **Сотрудников** в организацию;
- управление **Устройствами** и **Сотрудниками** организации;
- ведение **Политик доступа**;
- управление **Отделами**;
- настройка обслуживания **Сервисными организациями**;
- управление **Организациями – клиентами**.

Назначение сотрудника **Администратором Организации** доступно **Администратору Организации** с включенной ролью **Организации**.

Для назначения сотрудника **Администратором Организации**:

1. Откройте список сотрудников организации.
2. В строке нужного **Сотрудника** нажмите кнопку  **Действия** и выберите **Просмотр**.



Откроется страница **Сотрудник фамилия Имя**.

3. Нажмите кнопку **Изменить**.



Откроется страница **Редактирование сотрудника «Фамилия Имя»**.

4. Включите настройку **Администратор организации** и нажмите кнопку **Сохранить**.

Редактирование сотрудника "test_fn test_ln"

Администратор системы 

Организации / test varg / Сотрудники / test_fn test_ln / редактирование

Email	testast@mailforspam.com
ФИО	test_fn test_ln
Статус	Активен
Контакты	
Описание	
Отделы	Не состоит
☐ Администратор организации	

Сохранить **Отмена**

Рисунок 26 Страница Редактирование сотрудника «Фамилия Имя»

5. Выбранный сотрудник будет назначен **Администратором Организации**.

4.1.5. Устройства

Вкладка **Устройства** на странице организации предназначена для управления списком устройств организации. **Группы** и **Устройства** в организацию могут добавлять пользователи с включенной ролью **Организации**.

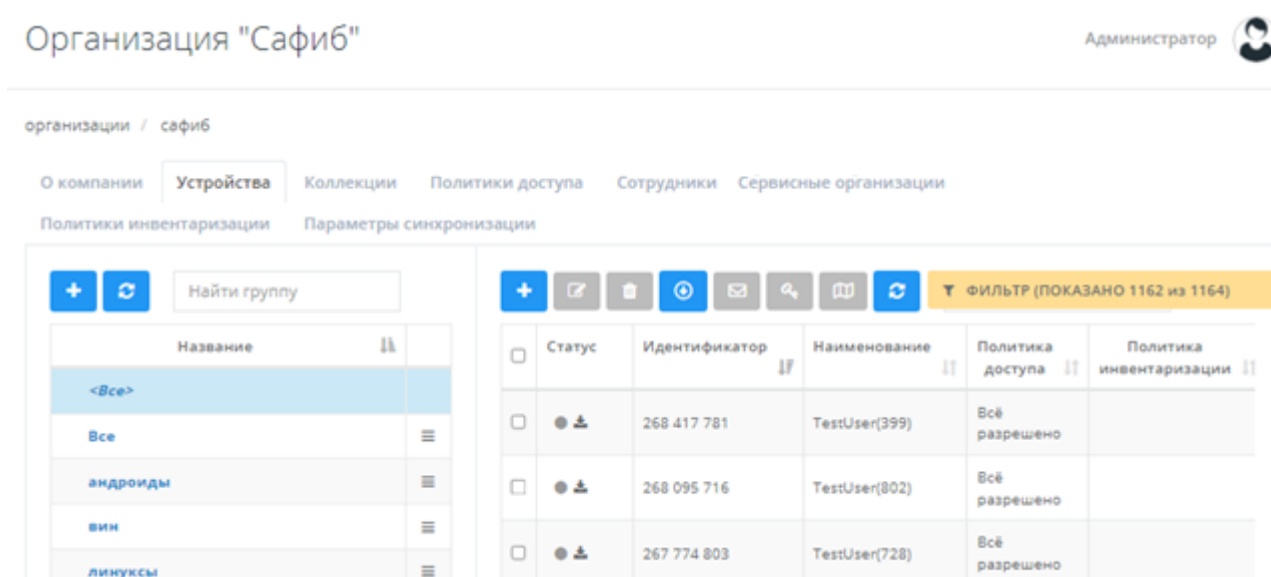


Рисунок 27 Вкладка Устройства страницы Организация

В один момент времени устройство может состоять только в одной организации.

Политики доступа и мониторинга

Политики доступа и мониторинга, могут быть настроены для **одного, нескольких** или **группы устройств**, входящих в организацию.

Для назначения политик устройствам, входящим в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Выберите организацию, для устройств которой необходимо назначить политики.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

5. Выберите несколько устройств и нажмите кнопку .

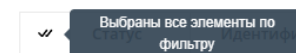
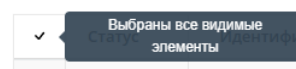
»»» Откроется окно **Групповое изменение устройств**.

Рисунок 28. Окно Назначение политик

6. Выберите значения, которые требуется изменить и нажмите кнопку **Сохранить**.
7. Изменения будут сохранены. Откроется список устройств организации с обновленным данными.

Примечание: В заголовке столбца, который используется для выделения элементов в списке, при первом нажатии выделяются все элементы на текущей странице.

При повторном нажатии выделяются все элементы с учётом фильтров на всех страницах.



Группы устройств

Все устройства организации всегда находятся в группах. **Группа** – обязательное поле при добавлении устройства в организацию.

Для создания группы устройств:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать группу устройств.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

5. Нажмите кнопку  в списке групп.

»»» Откроется страница Создание группы устройств.

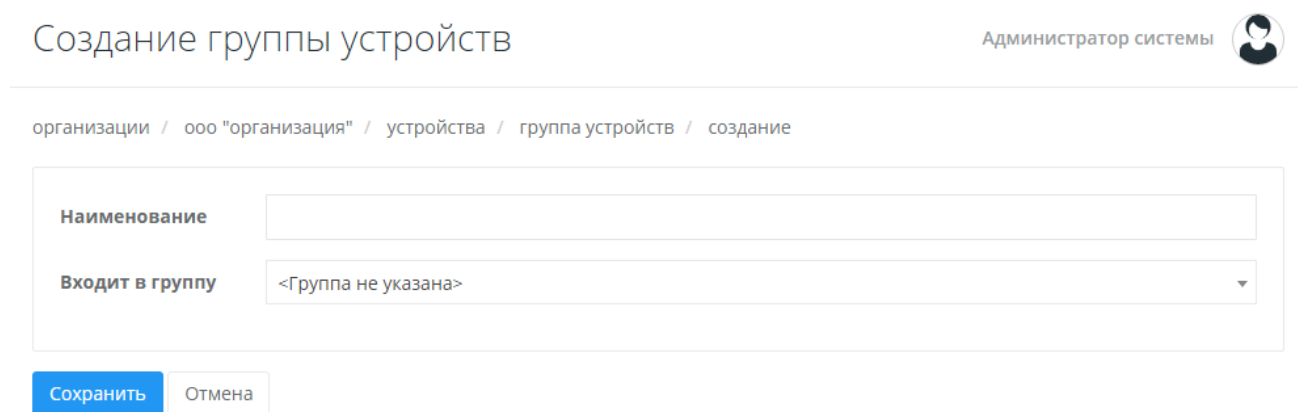


Рисунок 29 Страница Создание группы устройств

6. Введите **Наименование**.
7. При необходимости выберите группу, в которую будет входить создаваемая группа.
8. Нажмите кнопку **Сохранить**.

»»» Откроется вкладка **Устройства**. В списке устройств отобразится созданная группа.

Для **изменения** и **удаления** группы устройств воспользуйтесь соответствующими пунктами меню кнопки  **Действия**.

Синхронизация с доменом

Существует возможность настроить автоматическое добавление устройств из **домена** в определенные группы устройств организации.

Для настройки автоматического добавления устройств из **домена** в группы:

1. Войдите в Личный кабинет (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать группу устройств.

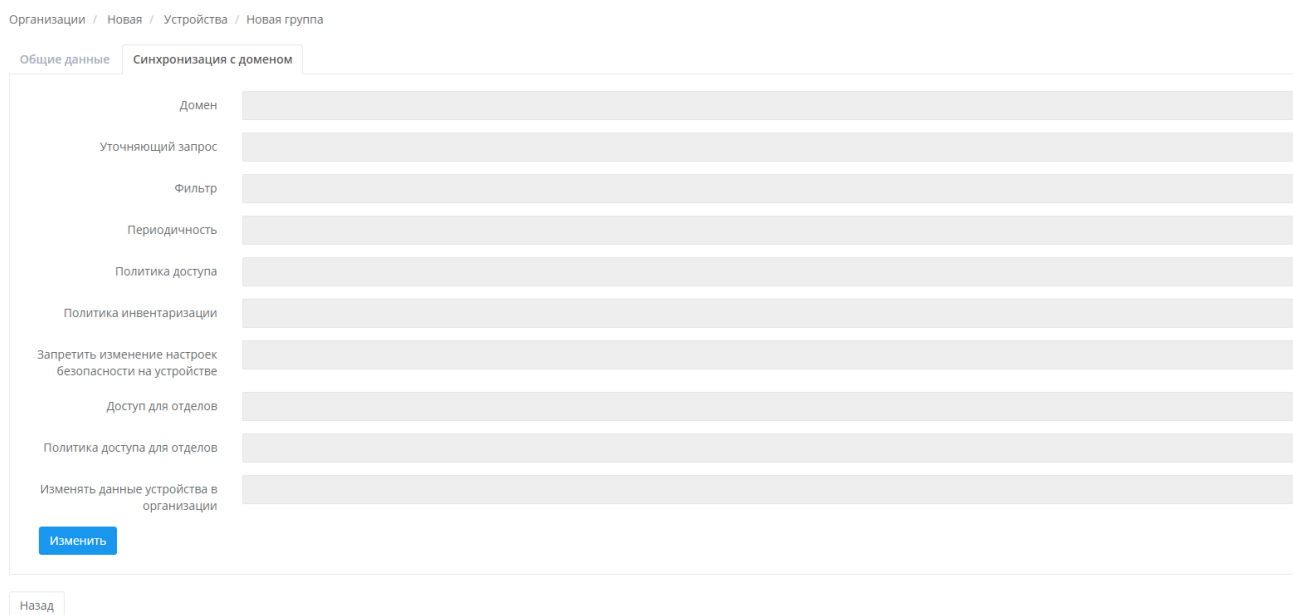
»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

5. Выберите необходимую группу, нажмите кнопку  **Действия** и пункт **Просмотр**.

 Открывается страница **Группа устройств «Наименование группы»**.

6. Перейдите на вкладку **Синхронизация с доменом**.



Организации / Новая / Устройства / Новая группа

Общие данные Синхронизация с доменом

Домен	
Уточняющий запрос	
Фильтр	
Периодичность	
Политика доступа	
Политика инвентаризации	
Запретить изменение настроек безопасности на устройстве	
Доступ для отделов	
Политика доступа для отделов	
Изменять данные устройств в организации	

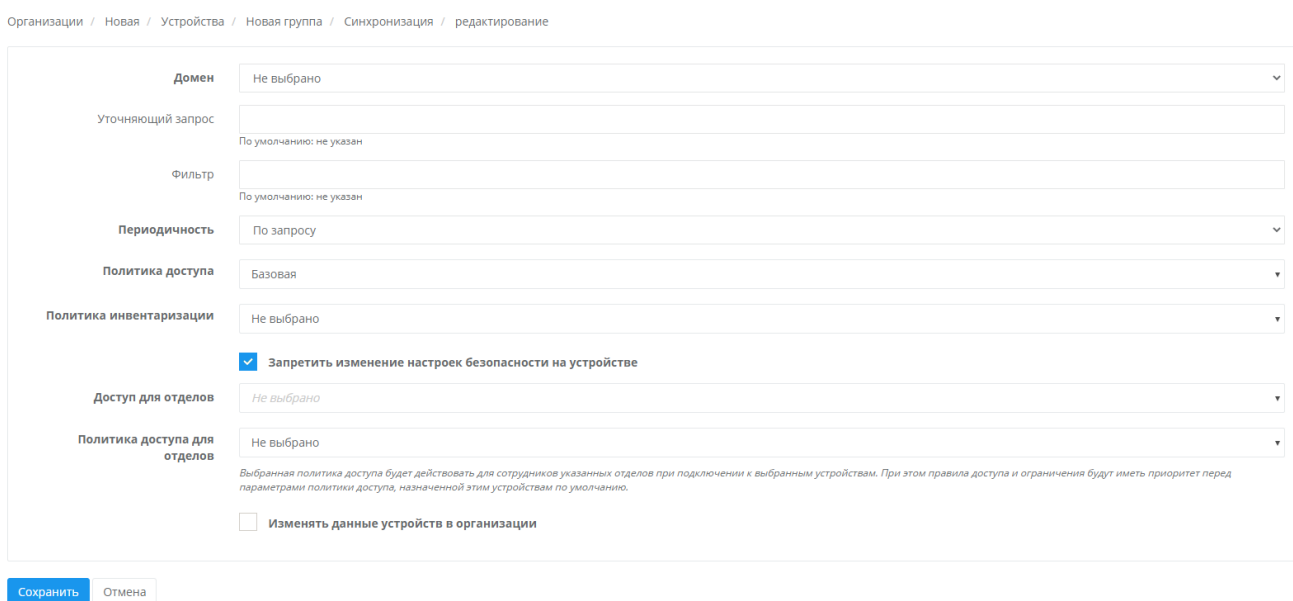
Изменить

Назад

Рисунок 30 Страница синхронизации группы с доменом

7. Нажмите кнопку **Изменить**.

 Откроется страница **Синхронизация группы устройств "Наименование группы"**.



Организации / Новая / Устройства / Новая группа / Синхронизация / редактирование

Домен	Не выбрано
Уточняющий запрос	По умолчанию: не указан
Фильтр	По умолчанию: не указан
Периодичность	По запросу
Политика доступа	Базовая
Политика инвентаризации	Не выбрано
Запретить изменение настроек безопасности на устройстве	☒
Доступ для отделов	Не выбрано
Политика доступа для отделов	Не выбрано

Выбранная политика доступа будет действовать для сотрудников указанных отделов при подключении к выбранным устройствам. При этом правила доступа и ограничения будут иметь приоритет перед параметрами политики доступа, назначенной этим устройствам по умолчанию.

☐ Изменять данные устройств в организации

Сохранить Отмена

Рисунок 31 Окно Синхронизация группы устройств

8. Заполните все **обязательные поля** и нажмите кнопку **Сохранить**.



Настройки автоматического добавления устройств будут сохранены. Откроется окно **Синхронизация**.

Примечание: В названии групп, для которых настроена Синхронизация с доменом появляется значок , при наведении на который курсора мыши отображается всплывающая подсказка о периодичности синхронизации и статусе.

9. Для немедленной синхронизации с **доменом**, или в случае выбора периода синхронизации **По запросу**, воспользуйтесь кнопкой **Синхронизировать** окна **Синхронизация группы устройств "Наименование группы"**.

Примечание: Кнопка **Синхронизировать** появляется на окне **Синхронизация группы устройств "Наименование группы"** только в случае, если настройки синхронизации указаны верно и синхронизация включена (установлен флаг **Включено**).

Сгенерировать ключ.

При запуске или установке **Клиентского приложения** со сгенерированным **ключом**, устройство будет добавлено в выбранную **группу устройств** организации с указанными **политиками доступа**.

Для генерации файла ключа:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо создать группу устройств.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

5. Выберите необходимую группу, нажмите кнопку  **Действия** и пункт **Сгенерировать ключ**.



Откроется окно **Генерация ключа**.

Рисунок 32 Окно Генерация ключа

6. Заполните все обязательные поля и нажмите кнопку **Сгенерировать**.



Файл ключа **autoadd.key** будет сгенерирован и начнется его загрузка.

Примечание: **Файл ключа** может быть использован при развёртывании **Клиентского приложения**. Подробнее в документе **Руководство администратора**.

Приглашение в организацию

Для включения устройств в состав организации необходимо, чтобы на устройстве было установлено **Клиентское приложение**. В **Личном кабинете** пользователя с включенной ролью **Организации** создается **Приглашение** на вступление в организацию, которое доставляется на устройство посредством **Клиентского приложения**. После его принятия пользователем устройство входит в состав организации.

Для включения устройства в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в состав которой необходимо включить устройство.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

5. Нажмите кнопку **Добавить устройство**.

»»» Откроется страница **Добавление устройства**.

6. На странице **Добавление устройства** заполните поля:

- **Группа** – выберите из списка созданных групп;
- **Идентификатор** – укажите идентификатор устройства;
- **Наименование** – введите название устройства;
- **Комментарий** – краткое текстовое описание устройства, необязательно;
- **Политика доступа** – укажите политику доступа, которая будет использоваться при подключении к устройству пользователей, для которых политика доступа не указана явно.
- **Политика инвентаризации** – укажите политику инвентаризации, которая будет использоваться для сбора данных о текущей конфигурации программного и аппаратного обеспечения устройства.
- **Запретить изменение настроек безопасности на устройстве** – установите признак, если необходимо запретить изменение настроек безопасности, правил доступа и адреса id-сервера в клиентском приложении.
- **Отделы** – выбор отделов, в которые добавить устройство (строка появляется только при прямом управлении субъектами).
- **Политика доступа для отделов** – назначаемая политика доступа для выбранных отделов (строка появляется только при прямом управлении субъектами).

Добавление устройства

Администратор 

организации / сафиб / устройства / добавление

Группа	Все
Идентификатор	
Наименование	
Комментарий	
Политика доступа	Без пароля
Политика инвентаризации	Нет
	☒ Запретить изменение настроек безопасности на устройстве
Отделы	Не выбрано
Политика доступа для отделов	Не выбрано

Сохранить

Отмена

7. Нажмите кнопку **Сохранить**.

Добавленное устройство отобразится в списке устройств организации со статусом **Не подтверждено**. Устройству посредством **Клиентского приложения** будет отправлено **Приглашение в организацию**.

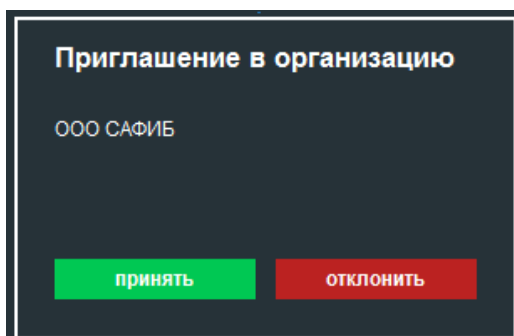


Рисунок 34 Окно Приглашение в организацию

После принятия пользователем запроса на включение в организацию, статус устройства в списке изменится на **Активно**. Устройство будет включено в состав организации.

Примечание: При включенной настройке **Прямое управление субъектами** устройство будет добавлено в организацию без запроса на включение в организацию. Подробнее о настройке в пункте 7.8 Настройки.

Отправка сообщения

Для отправки сообщения на устройство:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, на устройство которой необходимо отправить сообщение.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

»»» Откроется список устройств организации.

5. Выберите устройства, на которые необходимо отправить сообщение, и нажмите кнопку  **Отправить сообщение**.

»»» Откроется окно **Сообщение**.

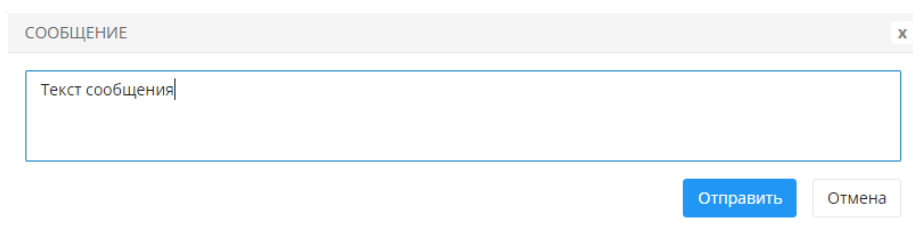


Рисунок 35 Окно Сообщение

6. Введите текст и нажмите кнопку **Отправить**.

»»» Сообщение будет отправлено на выбранные устройства и отобразится в окне **Уведомление Клиентского приложения**.

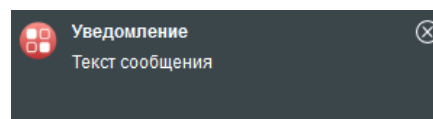


Рисунок 36 Окно Уведомление

Активировать лицензию

Для активации на устройстве лицензии, отличной от **Базовая**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в состав которой входит устройство, на котором необходимо активировать лицензию.

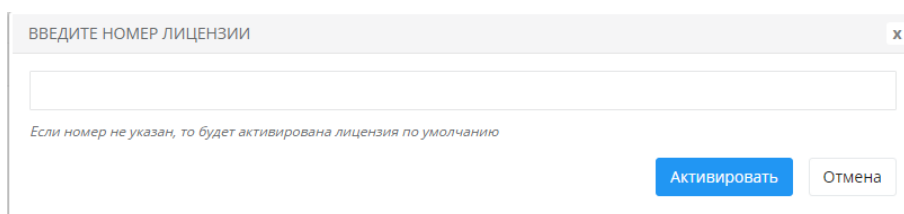
»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

»»» Откроется список устройств организации.

5. Выберите устройства, на которых необходимо активировать лицензию, и нажмите кнопку  **Активировать лицензию**.

»»» Откроется окно **Введите номер лицензии**.



ВВЕДИТЕ НОМЕР ЛИЦЕНЗИИ

Если номер не указан, то будет активирована лицензия по умолчанию

Активировать Отмена

Рисунок 37 Окно Введите номер лицензии

6. Введите номер и нажмите кнопку **Активировать**.

»»» Введенная лицензия будет активирована на выбранном устройстве.

Примечание: Активация лицензии может быть произведена непосредственно из **Клиентского приложения**. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

Совет: Для возврата к **Базовой** лицензии в окне **ВВЕДИТЕ НОМЕР ЛИЦЕНЗИИ** оставьте поле пустым и нажмите кнопку **Активировать**.

Доступ для сотрудников

Настройка прав доступа сотрудника осуществляется включением сотрудника в отдел и назначением политики доступа для отдела.

Для настройки доступа сотрудников:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для сотрудников которой необходимо настроить доступ.

»»» Откроется страница **Организация «Наименование организации»**.

4. Убедитесь в наличии настроенных должным образом **Политик доступа**. При необходимости добавьте необходимые политики. Подробнее в пункте 4.1.2 Политики доступа.
5. Убедитесь в наличии сформированных **Отделов**. При необходимости сформируйте отделы. Подробнее в пункте 4.1.4 Сотрудники.
6. Перейдите на вкладку **Устройства**.

»»» Откроется список устройств организации.

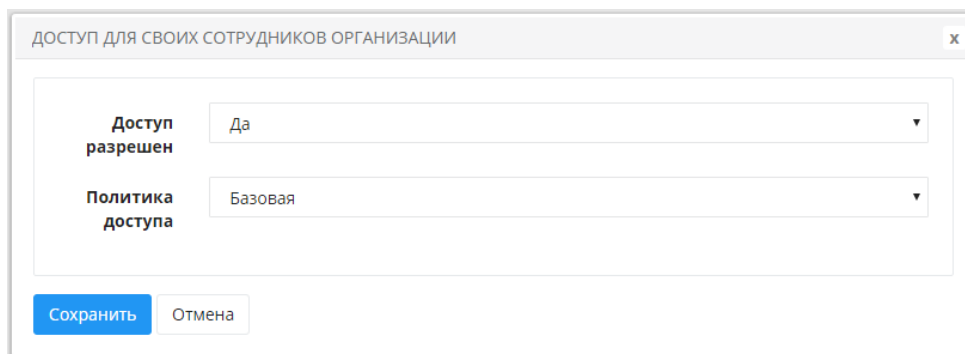
7. Убедитесь в наличии в списке **Устройств**, к которым необходимо настроить доступ. При необходимости **пригласите** недостающие устройства и дождитесь **принятия ими приглашения**.
8. В строке нужного устройства нажмите кнопку  **Действия** и выберите **Просмотр**.

»»» Откроется страница **Редактирование устройства**.

9. Перейдите на вкладку **Доступ для своих сотрудников**.
10. Выберите **Отдел**, для сотрудников которого необходимо изменить **Политику доступа**, и нажмите кнопку **Изменить доступ**.

»»» Откроется окно **Доступ для своих сотрудников организации**.

11. В поле **Доступ разрешен** выберите значение **Да**, а в поле **Политика доступа** необходимую политику.



ДОСТУП ДЛЯ СВОИХ СОТРУДНИКОВ ОРГАНИЗАЦИИ

Доступ разрешен: Да

Политика доступа: Базовая

Сохранить Отмена

Рисунок 38 Окно Доступ для своих сотрудников

12. Нажмите кнопку **Сохранить**.

»»» В поле **Политика** настраиваемого отдела появится выбранная политика доступа. Статус в колонке **Доступ разрешен** примет значение **Да**.

Если необходимо запретить доступ сотрудников отдела к данному устройству, то на вкладке **Доступ для своих сотрудников** выберите необходимый **Отдел** и нажмите кнопку **Запретить доступ**.

Доступ для отделов

Настройка прав доступа сотрудников отделов к устройствам организации может производиться указанием для устройств или групп устройств курирующего отдела и политики доступа.

Для настройки доступа сотрудников отделов к устройствам:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для сотрудников которой необходимо настроить доступ.

»»» Откроется страница **Организация «Наименование организации»**.

4. Убедитесь в наличии настроенных должным образом **Политик доступа**. При необходимости добавьте необходимые политики. Подробнее в пункте 4.1.2 Политики доступа.
5. Убедитесь в наличии сформированных **Отделов**. При необходимости сформируйте отделы. Подробнее в пункте 4.1.4 Сотрудники.
6. Перейдите на вкладку **Устройства**.

»»» Откроется список устройств организации.

7. Убедитесь в наличии в списке **Устройств**, к которым необходимо настроить доступ. При необходимости **пригласите** недостающие устройства и **дождитесь принятия ими приглашения**.
8. Выделите одно, несколько или группу устройств и нажмите кнопку

Доступ для отделов

»»» Откроется окно **Доступ для отделов**.

9. В поле **Отделы** выберите один или несколько отделов. В поле **Политика доступа** укажите необходимую политику.

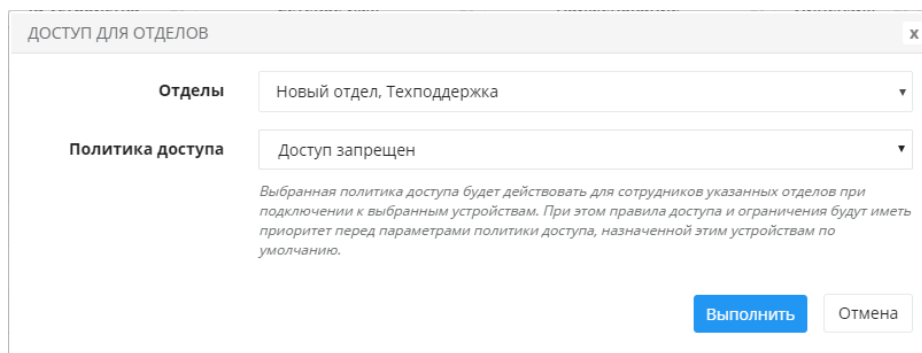


Рисунок 39 Окно Доступ для отделов

10. Нажмите кнопку **Выполнить**.

Откроется список вкладки **Устройства**. Устройствам будет назначена выбранная ранее **Политика доступа**. Статус в колонке **Доступ разрешен** примет соответствующее значение.

Доступ для сервисных организаций

Если организацию, к которой принадлежит устройство, обслуживает одна и более сервисных организаций, доступ к устройствам настраивается для каждой **Сервисной организации**.

Для настройки доступа **Сервисной организации** к устройствам:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для устройств которой необходимо настроить доступ **Сервисной организации**.

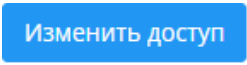
Откроется страница **Организация «Наименование организации»**.

4. Убедитесь в наличии настроенных должным образом **Политик доступа**. При необходимости добавьте необходимые политики. Подробнее в пункте 4.1.2 Политики доступа.
5. Убедитесь в наличии сформированных Отделов. При необходимости сформируйте отделы. Подробнее в пункте 4.1.4 Сотрудники.
6. Перейдите на вкладку **Устройства**.

Откроется список устройств организации.

7. Убедитесь в наличии в списке **Устройств**, к которым необходимо настроить доступ. При необходимости **пригласите** недостающие устройства и **дождитесь принятия ими приглашения**.
8. В строке нужного устройства нажмите кнопку **Действия** и выберите **Просмотр**.

»»» Откроется страница **Редактирование устройства**.

9. Перейдите на вкладку **Доступ для сервисных организаций** выберите **Сервисную организацию**, для которой необходимо изменить доступ, и нажмите кнопку .

»»» Откроется окно **Доступ для сервисных организаций**

10. В поле **Доступ разрешен** выберите значение **Да**, а в поле **Политика доступа** необходимую политику.
11. Нажмите кнопку **Сохранить**.

»»» В поле **Политика** появится выбранная политика доступа. Статус в колонке **Доступ разрешен** примет значение **Да**.

Отправить запрос на сбор данных

Для **сбора информации о конфигурации и состоянии** удаленного устройства необходимо отправить **запрос** на сбор данных. **Запрос на сбор данных** может быть отправлен **автоматически** по расписанию, либо создан **вручную**.

Для ручного создания запроса на сбор данных:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование организации, в состав которой входит устройство.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Устройства**.

»»» Откроется список устройств организации.

5. Убедитесь, что для нужного устройства установлена **Политика инвентаризации** (подробнее в пункте 4.1.3 Политики)

6. Выберите устройства, с которых необходимо собрать данные о программной и аппаратной конфигурации, и нажмите кнопку .

»»» Откроется окно **Отправка запроса на сбор данных**.

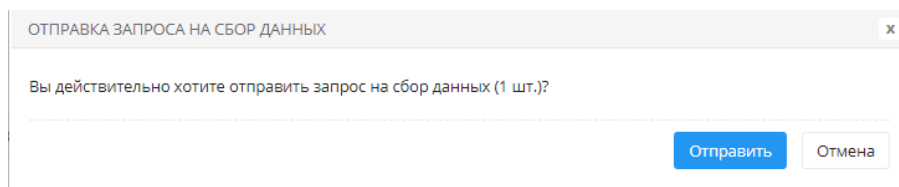


Рисунок 40 Окно Отправка запроса на сбор данных

7. Нажмите кнопку **Отправить**.

»»» На выбранное устройство придет запрос на сбор данных.

8. Собранные данные будут доступны в модуле **Администрирование Клиентского приложения** на вкладке **Инвентаризация**.

Примечание: Запрос на сбор данных о состоянии программной и аппаратной конфигурации устройства может быть создан из **Клиентского приложения**. Подробнее в документе **Руководство пользователя. Клиентское приложение**.

Параметры записи видео

При редактировании устройства, входящего в организацию, (**принявшего приглашение** на вступление в организацию) можно установить дополнительно **Параметры записи видео**, которые недоступны при приглашении устройств в организацию.

Для редактирования устройства в списке устройств посредством кнопки  **Действия** откройте устройство на **Просмотр** и на странице **Редактирование устройства** нажмите кнопку **Изменить**, установите **Параметры записи видео** и нажмите кнопку **Сохранить**.

4.1.6. Коллекции

Коллекция служит для удобного поиска устройств и представляет собой список, сформированный из **Устройств Организации** с помощью правил формирования (фильтров), либо путем добавления отдельных устройств.

Создание коллекции

Для создания **Коллекции**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Выберите организацию, для устройств которой необходимо создать коллекцию.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Коллекции**.



5. Нажмите кнопку **Добавить коллекцию** в списке коллекций.



Откроется страница **Создание коллекции устройств**.

Общие данные

Наименование

Описание

Период синхронизации

По запросу

Сохранить

Отмена

Рисунок 41 Страница Создание коллекции устройств

6. Заполните **Наименование**, **Описание** (при необходимости) и выберите **Период синхронизации**.
7. Нажмите кнопку **Сохранить**.



Откроется страница **Коллекции**. Созданная коллекция появится в списке.

Добавление правил в коллекцию.

Для добавления правил в коллекцию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 [Вход в личный кабинет](#)) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Выберите **организацию**, для **коллекции** которой необходимо создать **правило**.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Коллекции**.



5. Нажмите на кнопку **Действия** у коллекции, для которой необходимо добавить правило и выберите **Изменить**.



Откроется страница **Редактирование коллекции устройств «Наименование коллекции»**.

организации / сафиб / коллекции устройств / редактирование

Общие данные
Правила добавления устройств
Доступ для сотрудников

Наименование

Коллекция

Описание

Период синхронизации

По запросу

Сохранить
Отмена

Рисунок 42 Окно Редактирование коллекции устройств

6. Откройте вкладку **Правила добавления устройств** и нажмите кнопку **Добавить**.



Откроется окно **Добавление правила**.

ДОБАВЛЕНИЕ ПРАВИЛА ✕

Действие

Включить

Тип фильтра

По данным домена

Домен

Не выбрано

Уточняющий запрос

По умолчанию: не указан

Фильтр

По умолчанию: не указан

Сохранить
Отмена

Рисунок 43 Окно Добавление правила

7. Заполните все обязательные поля и нажмите кнопку **Сохранить**.



Откроется вкладка **Правила добавления устройств**. Правило будет отображаться в списке.

Типы фильтра правила коллекции

Коллекции формируются по трем типам фильтров. **Тип фильтра** определяет источник получения информации о устройстве: данные домена, инвентаризация либо по информации об устройстве в сети. В зависимости от выбранного **Типа фильтра** окно **Добавление правила** может содержать различные наборы атрибутов.

По данным домена правило содержит следующие элементы управления:

Действие	Поле Действие позволяет либо включить устройства в коллекцию, либо исключить устройства из коллекции в соответствии с фильтром. При значении Не использовать правило не применяется.
Тип фильтра	По данным домена.
Домен	Выбор домена.
Уточняющий запрос	Ограничить выбор объектов службы каталогов.
Фильтр	Запрос объектов из службы каталогов.
Сохранить	Сохраняет правило.
Отмена	Не сохранять правило.

По данным инвентаризации правило имеет следующий вид и содержит следующие элементы управления:

ДОБАВЛЕНИЕ ПРАВИЛА

Действие

Включить

Тип фильтра

По данным инвентаризации

Категория

Автозапуск

Атрибут

Название

Фильтр по маске

Укажите маску с использованием *

Сохранить

Отмена

Рисунок 44 Окно Добавление правила – По данным инвентаризации

Действие	Поле Действие позволяет либо включить устройства в коллекцию, либо исключить устройства из коллекции в соответствии с фильтром. При значении Не использовать правило не применяется.
Тип фильтра	По данным инвентаризации.
Категория	Категория атрибутов для поиска.
Атрибут	Атрибут для поиска.
Фильтр по маске	Маска фильтра.
Сохранить	Сохраняет правило.
Отмена	Не сохранять правило.

По информации об устройстве правило имеет следующий вид и содержит следующие элементы управления:

ДОБАВЛЕНИЕ ПРАВИЛА

Действие

Включить

Тип фильтра

По информации об устройстве

Наименование

Укажите маску с использованием *

Идентификатор

Укажите маску с использованием *

IP

Укажите маску с использованием *

Сетевое имя

Укажите маску с использованием *

Сохранить

Отмена

Рисунок 45 Окно Добавление правила – по информаии об устройстве

Действие	Поле Действие позволяет либо включить устройства в коллекцию, либо исключить устройства из коллекции в соответствии с фильтром. При значении Не использовать правило не применяется.
Тип фильтра	По информации об устройстве.
Наименование	Маска имени устройств.
Идентификатор	Идентификатор устройства.
IP	Маска ip-адреса.
Сетевое имя	Маска сетевого имени.
Сохранить	Сохраняет правило.
Отмена	Не сохранять правило.

Синхронизация коллекции – процесс обновления перечня устройств коллекции в соответствии с правилами. **Синхронизация коллекции** происходит с периодичностью, указанной в поле **Период синхронизации** вкладки **Общие данные** коллекции устройств.

Примечание: В случае, если **период** синхронизации коллекции указан как **По запросу** синхронизация коллекции производится **принудительно**.

При каждой **синхронизации коллекции** происходят следующие действия:

1. Коллекция **полностью** очищается.

Внимание! При **синхронизации** коллекции набор устройств, добавленных в коллекцию вручную, будет утерян безвозвратно.

2. Обрабатывают **Правила**, в которых поле **Действие** имеет значение **Включить**. В коллекцию **добавляются Устройства организации**, которые соответствуют фильтрам в правилах.
3. Обрабатывают **Правила**, в которых поле **Действие** имеет значение **Исключить**. Из коллекции **удаляются Устройства организации**, которые соответствуют фильтрам в выполняемых правилах.

Примечание: Правила, в которых поле **Действие** имеет значение **Не использовать** **не выполняются**.

Для **принудительной** синхронизации коллекции:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 **Вход в личный кабинет**) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Выберите **организацию**, для коллекции которой необходимо выполнить синхронизацию.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Коллекции**.

5. Нажмите на кнопку  **Действия** у коллекции, для которой выполнить синхронизацию и выберите **Синхронизировать**.

»»» Содержимое коллекции будет **синхронизировано**.

Доступ для сотрудников

На вкладке **Доступ для сотрудников** окна **Редактирование коллекции** указывается для сотрудников каких отделов будут доступны устройства коллекции, а также какие политики доступа при этом используются.

Примечание: Политики доступа в коллекции имеют приоритет над политиками, назначенные на устройство в организации и в отделах.

Если сотрудник входит в несколько отделов, которые добавлены в список **Доступ для сотрудников** коллекции с разными **Политиками доступа**, то будут получены максимально разрешающие права.

Добавление отдельных устройств в коллекцию

Для добавления устройства в **коллекцию**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **владельца Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Выберите **организацию**, в **коллекцию** которой необходимо добавить **устройство**.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Коллекции** и выберите нужную **коллекцию** в списке.

5. Нажмите кнопку  **Добавить устройство** в списке устройств.

»»» Откроется страница **Добавление устройства**.

6. Введите идентификатор устройства, которое нужно добавить в **коллекцию** и нажмите кнопку **Сохранить**.

»»» **Устройство** будет добавлено в **коллекцию**.

4.1.7. Сервисные организации

При помощи **Системы** может быть организовано как предоставление услуг технической поддержки, так и получение таких услуг. В частности, техническую поддержку сотрудникам организации могут оказывать сотрудники других организаций – **Сервисных**.

Добавление **Сервисной организации** может происходить двумя способами, в зависимости от настройки **Прямое управление субъектами**:

- При выключенной настройке **Организация-клиент** должна подать **Заявку на обслуживание** в сервисную организацию. Сервисная организация, в свою очередь, должна принять эту заявку.
- При включенной настройке принятие заявки на обслуживание от сервисной организации не требуется и добавление сервисной

организации осуществляется непосредственно **Администратором Организации**, с включенной ролью **Организации**.

Организация-клиент настраивает параметры доступа к своим устройствам для сервисной организации, после чего ответственные сотрудники сервисной организации смогут осуществлять техническую поддержку устройств организации-клиента. Организация-клиент, в свою очередь, сможет отправлять **Заявки на поддержку** в сервисную организацию.

Вкладка **Сервисные организации** содержит перечень **Сервисных организаций**, которые обслуживают организацию-клиента, и перечень **Заявок на обслуживание** в сервисные организации. Вкладка служит для управления **Заявками на поддержку**, определения перечня **Сервисных организаций** и настройки для них прав доступа.

Код сервисной организации

Код сервисной организации – это уникальный в пределах копии **Системы** идентификатор, который предназначен для точной идентификации **Сервисной организации** при подаче **Заявки на обслуживание**. Для подачи **Заявки на обслуживание** **Организация-клиент** указывает переданный ей **Код сервисной организации**.

Код сервисной организации является атрибутом **Сервисной организации** и отображается на вкладке **О компании** при выставлении признака **Является сервисной организацией**.

Подача заявки на обслуживание

Перед подачей заявки на обслуживание в сервисную организацию необходимо получить **особый код** от **Сервисной организации**.

Для подачи **Заявки на обслуживание**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 **Вход в личный кабинет**) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо добавить **Сервисную организацию**.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сервисные организации**.



Откроется список сервисных организаций.

5. Нажмите кнопку **Подать заявку на обслуживание**.



Откроется окно **Заявка на обслуживание в сервисную организацию**.

6. Укажите **код сервисной организации**.

7. Нажмите кнопку **Отправить**.

Рисунок 46 Окно Заявка на обслуживание в сервисную организацию



Заявка на обслуживание будет направлена в сервисную организацию. Откроется обновленный список сервисных организаций с новым запросом на обслуживание.

Сервисная организация сможет оказывать техническую поддержку пользователя **Организации-клиента** после приема **Заявки на обслуживание**.

Для отказа от обслуживания в **Сервисной организации** выберите в списке сервисных организаций ту, от обслуживания в которой вы хотите отказаться, нажмите кнопку  **Действия** и выберите **Отказаться от обслуживания**.

Примечание: Если **Запрос на обслуживание** был отправлен ошибочно, то, пока он не принят сервисной организацией, его можно удалить. Для этого в строке нужной сервисной организации нажмите кнопку  **Действия** и выберите **Удалить**.

Добавление сервисной организации

Для добавления **сервисной организации**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 **Вход в личный кабинет**) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.



Откроется страница **Мои организации**.

3. Нажмите на наименование организации, для которой необходимо добавить сервисную организацию.



Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Сервисные организации**.



Откроется список сервисных организаций.

5. Нажмите кнопку **Добавить обслуживающую организацию**.

»»» Откроется окно **обслуживающая организация**.

6. Укажите **код сервисной организации**.

7. Нажмите кнопку **Добавить**.

»»» Откроется страница **Организация «Наименование организации»**. На вкладке **Сервисные организации** будет добавлена новая организация.

Настройка доступа к устройствам

Для настройки доступа для **Сервисной организации**:

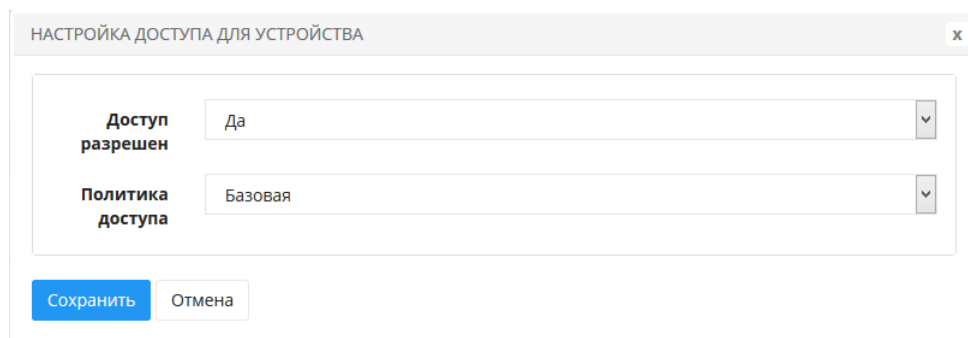
1. Откройте список сервисных организаций (этапы 1-4 пункта Подача заявки на обслуживание).
2. В строке нужной организации нажмите кнопку  **Действия** и выберите **Настроить доступ**.

»»» Откроется страница **Доступ для сервисной организации**.

3. Выберите одно или несколько устройств и нажмите кнопку **Изменить доступ**.

»»» Откроется окно **Настройка доступа для устройства**.

4. Укажите, разрешен ли доступ к выбранным устройствам, и выберите политику доступа.



НАСТРОЙКА ДОСТУПА ДЛЯ УСТРОЙСТВА

Доступ разрешен Да

Политика доступа Базовая

Сохранить Отмена

Рисунок 47 Окно Настройка доступа для устройства

5. Нажмите кнопку **Сохранить**.

»»» Откроется страница **Доступ для сервисной организации** с обновленным списком устройств. Для выбранных устройств применятся указанные разрешения доступа, для сотрудников сервисной организации будет действовать назначенная политика доступа.

Примечание: Настройку доступа к устройствам для **Сервисной организации** можно осуществлять, не дожидаясь принятия **Запроса на обслуживание**.

4.1.8. Клиенты

При помощи **Системы** может быть организовано как получение услуг технической поддержки, так и предоставление таких услуг. В частности, сотрудники организации могут осуществлять техническую поддержку сотрудников других организаций – **Клиентов**. **Организация-клиент** должна подать **Заявку на обслуживание**, которую должна принять **Сервисная организация**. **Организация-клиент** настраивает параметры доступа к своим устройствам для **Сервисной организации**, после чего ответственные сотрудники отделов **Сервисной организации** смогут осуществлять техническую поддержку устройств **Организации-клиента**. **Организация-клиент**, в свою очередь, сможет отправлять **Заявки на поддержку** в **Сервисную организацию**.

Вкладка **Клиенты** страницы **Организация** содержит перечень **Организаций-клиентов**, которые обслуживаются вашей организацией, и перечень **Заявок на обслуживание**. Вкладка служит для управления **Заявками на обслуживание**, определения перечня **Организаций-клиентов** и настройки прав доступа к ним.

Прием заявки на обслуживание

Для приема заявки на обслуживание:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Организации**, с включенной ролью **Организации**.
2. В главном меню выберите пункт **Мои организации – Организации**.

»»» Откроется страница **Мои организации**.

3. Нажмите на наименование **Сервисной организации**.

»»» Откроется страница **Организация «Наименование организации»**.

4. Перейдите на вкладку **Клиенты**.

»»» Откроется список организаций-клиентов.

5. В строке организации со статусом **Запрос на обслуживание** нажмите кнопку  **Действия** и выберите **Взять на обслуживание**.

»»» Статус **Организации-клиента** изменится на **Обслуживается**.

Для снятия организации с обслуживания на вкладке **Клиенты** страницы **Организация** в строке организации, которую необходимо снять с обслуживания, нажмите кнопку  **Действия** и выберите **Снять с обслуживания**.

Настройка доступа

После того, как **Организация-клиент** взята на обслуживание, необходимо назначить **Отделы**, ответственные за обслуживание устройств **Клиента**.

Для назначения отделов, ответственных за обслуживание **Организации-клиента**:

1. Откройте список организаций-клиентов (этапы 1-4 пункта Прием заявки на обслуживание).
2. В строке нужной организации нажмите кнопку  **Действия** и выберите **Открыть**.

»»» Откроется страница **Обслуживаемая организация**.

3. Перейдите на вкладку **Назначение ответственных**.

»»» Откроется список устройств **Организации-клиента**.

4. Выберите устройства, для которых необходимо назначить ответственных.
5. Нажмите кнопку **Назначить отделы**.

»»» Откроется окно **Назначение отделов для обслуживания устройств**.

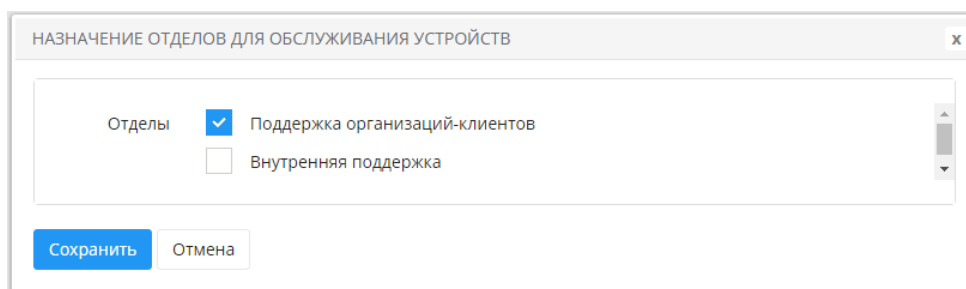


Рисунок 48 Окно Назначение отделов для обслуживания

6. Выберите отделы, сотрудники которых будут ответственными за обслуживание.
7. Нажмите кнопку Сохранить.

»»» Выбранным устройствам будут назначены ответственные отделы.
Откроется обновленный список устройств **Организации-клиента**.

Примечание: Если для устройства не выбран ни один отдел, то данное устройство не будет обслуживаться сервисной организацией.

4.2. Домены служб каталогов

Подраздел предназначен для управления подключениями к LDAP-серверам (Active Directory, Avapost и другие), которые используются для аутентификации и авторизации пользователей, а также для синхронизации учётных записей и устройств.

В подразделе отображается перечень подключенных доменов.

Домены служб каталогов Администратор системы 

Создать Удалить ↺ Поиск:

☐	Наименование	Сервер	Порт	SSL	Уточняющий запрос	Реализация Ldap	Логин	
☐	Avapost					Avapost		
☐	Freeipa					FreeIPA		
☐	safib					Active Directory		
☐	test.local					Active Directory		
☐	Пустой					ALD Pro		
☐	test.local (шифрованный)					Active Directory		
☐	РЕД АДМ					РЕД АДМ		

Показано с 1 до 7 из 7 записей. Отображать по 50

« 1 »

Рисунок 49 Список доменов служб каталогов

Для добавления нового подключения к **домену**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора**.
2. В главном меню выберите пункт **Мои организации – Домены служб каталогов**.



Откроется страница **Домены служб каталогов**.

3. Нажмите на кнопку **Создать**.



Откроется страница **Создание домена служб каталогов**.

Создание домена служб каталогов

Домены служб каталогов / создание

Администратор системы

Параметры подключения

Наименование

Сервер

Порт

SSL

Уточняющий запрос

Логин

Пароль

Тест соединения

Фильтр для устройств

Фильтр для пользователей

Соответствия атрибутов

Реализация Ldap

Идентификатор объекта

Логин в стиле email

Имя учетной записи пользователя

Электронная почта

Описание

Сохранить Отмена

Рисунок 50 Создание домена служб каталогов

4. Заполните все необходимые поля, проверьте соединение с помощью кнопки **Тест соединения**.
5. После успешного соединения нажмите на кнопку **Сохранить**.



Домен службы каталога будет успешно создан.

4.3. Заявки

Подраздел предназначен для контроля состояния **Заявок** на техническую поддержку. Подраздел доступен для:

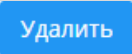
- **Администратора Организации** с включенной ролью доступа **Заявки в техподдержку** – в части заявок, созданных пользователями на устройствах организации.

- **Администратора Сервисной организации** – в части заявок, адресованных пользователям обслуживающей организации.
- **Администратора Системы** – все заявки всех организаций.

Пользователи **Клиентского приложения** со своих устройств отправляют **Заявки** в службу технической поддержки. В зависимости от настроенной структуры эти заявки принимают или собственные сотрудники организации, в которой эти устройства состоят, или сотрудники сервисной организации, которая эти устройства обслуживает.

Примечание: Подробнее о подаче и обработке **Заявок** в документе **Руководство пользователя. Клиентское приложение**.

Подраздел **Заявки** обеспечивает просмотр и управление списком **Заявок**, и содержит следующие элементы управления:

	Удаляет выбранные Заявки .
	Обновляет список заявок.
	Позволяет просматривать, изменять и удалять заявки. Примечание: Для изменения доступны только активные заявки и только ограниченный набор их атрибутов.

5. ЖУРНАЛЫ И ПРОТОКОЛЫ

Раздел **Журналы и протоколирование** предназначен для ведения записей о событиях, происходящих в системе, а также для контроля действий пользователей и администраторов. Журналы позволяют отслеживать изменения конфигураций, фиксировать выполнение задач и анализировать работу системы.

В данном разделе представлены следующие подразделы:

- **Протоколы соединений** – содержат данные о взаимодействиях между устройствами, таких как удаленные подключения и сеансы управления.
- **Журнал организации** – отображает историю событий, связанных с управлением устройствами, настройкой политик доступа и администрированием в рамках организации.
- **Системный журнал** – содержит информацию о всех действиях пользователей, совершенных в Личном кабинете и Клиентском приложении.

Журналы помогают администраторам и пользователям с соответствующими правами отслеживать выполнение задач, выявлять возможные ошибки и обеспечивать безопасность системы. В последующих подразделах подробно рассмотрены функции просмотра, фильтрации, выгрузки данных и очистки журналов.

5.1. Протоколы соединений

Подраздел предназначен для просмотра протоколов взаимодействия между устройствами, собранных подсистемой протоколирования.

События взаимодействия протоколируются по правилам, установленным на стороне **Удаленного устройства**. Настройка протоколирования должна быть включена в политике доступа удаленного устройства (подробнее о настройке политики доступа в пункте 4.1.2 Политики доступа).

Доступ к просмотру протоколов событий удаленного взаимодействия имеют **Администратор Системы** и пользователи с включенной ролью **Протоколы удаленного взаимодействия** в части протоколов своих организаций.

Протоколируемые события могут быть нескольких типов:

- Запись о запущенных на удаленном устройстве модулях с подробной информацией о выполненных в них операциях;
- Снимок экрана удаленного устройства;
- Видеозапись сеанса удаленного управления;
- Технический лог **Клиентского приложения** удаленного устройства.

Подраздел **Протоколы соединений** обеспечивает просмотр и управление списком **Протоколов удаленного взаимодействия** и содержит следующие элементы управления:

	Обновить	Обновляет список протоколов.
---	----------	------------------------------

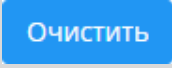
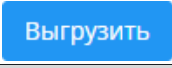
	Действия	Позволяет Открыть протокол для просмотра всех атрибутов и событий взаимодействия.
---	-----------------	--

5.2. Журнал организации

Подраздел **Журнал организации** предназначен для хранения и отображения всех действий, совершенных в **Личном кабинете** и **Клиентском приложении**.

Доступ к просмотру журнала действий имеют **Администратор Системы** и пользователи с включенной ролью **Журнал действий организации** в части протоколов своих организаций. Если пользователь состоит в нескольких организациях, то в журнале действий будут отображаться события от всех организаций, где включено ведение журнала действий организации.

Ведение **Журнала действий** организации включается признаком **Включить ведение журнала действий** на вкладке **О компании** страницы **Организация «Наименование организации»**.

	Очищает журнал действий. Позволяет определить организацию и дату, до которой производить очистку.
	Выгружает журнал действий во внешний файл.
 Обновить	Обновляет список событий.
 Действия	Позволяет Открыть событие журнала для подробного просмотра.

Подраздел **Журнал организации** содержит следующие элементы управления:

5.3. Системный журнал

Подраздел **Системный журнал** раздела **Журналы и протоколы** открывает **Системный журнал действий**. Он предназначен для хранения и отображения всех действий, совершенных в **Личном кабинете** и **Клиентском приложении** всеми пользователями **Системы**.

Подраздел доступен пользователям с включенной ролью **Системный журнал действий**.

Системный журнал действий					Администратор системы 
Очистить Выгрузить  Поиск: 					
Дата и время события	Категория	Организация	Событие	Пользователь	
28.02.2020 11:48:42	Учетная запись	Не указана	Изменение данных учетной записи в личном кабинете	Администратор системы (test@safib.ru)	
28.02.2020 11:41:58	Контроль учетных записей	Не указана	Аутентификация в личном кабинете выполнена успешно.	Администратор системы (test@safib.ru)	
28.02.2020 10:39:31	Контроль учетных записей	Не указана	Выход из клиентского приложения выполнен успешно	Администратор системы (test@safib.ru)	
28.02.2020 10:39:16	Контроль учетных записей	Не указана	Аутентификация в клиентском приложении выполнена успешно.	Администратор системы (test@safib.ru)	
28.02.2020 10:36:15	Устройства и сессии	Не указана	Зарегистрировано новое устройство. Присвоен HID = 227 364 424	Не указан	
28.02.2020 10:11:37	Контроль учетных записей	Не указана	Выход из клиентского приложения выполнен успешно	Администратор системы (test@safib.ru)	
28.02.2020 10:11:12	Контроль учетных записей	Не указана	Аутентификация в клиентском приложении выполнена успешно.	Администратор системы (test@safib.ru)	
28.02.2020 10:09:24	Контроль учетных записей	Не указана	Неудачная попытка аутентификации в клиентском приложении учетной записи test1@yandex.ru. Ошибка Active Directory: Connect Error. Время ожидания операции истекло	Не указан	

Рисунок 51 Страница Системный журнал действий

Страница **Системный журнал действий** содержит следующие элементы управления:

Очистить	Очищает системный журнал действий . Позволяет определить дату , до которой производить очистку.
Выгрузить	Выгружает системный журнал действий во внешний файл.
 Обновить	Обновляет список событий .
 Действия	Позволяет открыть событие журнала для подробного просмотра.

6. СТАТИСТИКА И СЕССИИ

6.1. Сессии устройств

Подраздел **Сессии устройств** содержит журнал активных сессий устройств и соединений между ними.

Список подраздела содержит следующую информацию:

Начало сессии	Дата создания сессии
Тип сессии	Указывает тип подключения в сессии
ID управляющего устройства	Уникальный идентификатор устройства.
ID управляемого устройства	При наличии подключенного управляющего устройства колонка содержит его уникальный идентификатор.
Транспортный сервер	Наименование транспортного сервера, который обслуживает сессию.
Пользователь управляющего устройства	Имя пользователя Системы.

Для обновления списка и отображения актуального перечня активных сессий служит кнопка **Обновить**. При необходимости можно принудительно **Закрыть сессию** или **Переместить сессию** на другой транспортный сервер (при наличии нескольких транспортных серверов) посредством кнопки  **Действия**.

Подраздел доступен пользователям с включенной ролью **Сессии подключенных устройств**.

6.2. Статистика

Примечание: Вы можете включить параметр автоматической очистки статистики. Подробнее параметр описан в документе **Руководство Администратора v.6.4(К+) в разделе 3.10 Настройка подсистемы статистики**.

Подраздел **Статистика** содержит подробную информацию о сессиях устройств. Функционал подраздела позволяет отфильтровать информацию о сессиях и визуализировать её при помощи набора шаблонов.

Начало сессии	Завершение сессии	Наименование устройства	ID устройства	Учетная запись	Продолжительность сессии
08.09.2025 21:08:54		debian12	190 333 529		17:32:42
08.09.2025 20:18:26		Windows Server 2012	268 242 412	admin@astcorp.ru	18:23:10
08.09.2025 20:18:21		ConfServer	022 680 960		18:23:15
08.09.2025 20:18:21		redos8	041 934 092		18:23:15
08.09.2025 20:18:21		Windows_10	087 787 619		18:23:15
08.09.2025 20:18:21		Windows Server 2012	268 242 412		18:23:15
08.09.2025 16:08:28	08.09.2025 20:05:32	Windows Server 2012	268 242 412	admin@astcorp.ru	03:57:04
08.09.2025 16:08:18	08.09.2025 20:05:32	redos8	041 934 092		03:57:14
08.09.2025 16:08:18	08.09.2025 20:05:32	Windows_10	087 787 619		03:57:14

Рисунок 52 Окно Статистика

Для фильтрации информации о сессиях:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Статистика и сессии – Статистика**.

Откроется страница **Статистика**.

3. Вызовите панель **Фильтр**.

Откроется страница панель **Фильтр**.

4. Укажите параметры фильтрации и нажмите кнопку **Применить**.

Страница **Статистика** обновиться.

Рисунок 53 Панель Фильтр

Примечание: Вы можете экспортировать сформированную статистику в файл, нажав кнопку  **Экспорт статистики в файл**.

Для формирования графиков по данным статистики:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Статистика и сессии – Статистика**.

Откроется страница **Статистика**.

3. **Отфильтруйте** информацию о сессиях, выберите в выпадающем списке **шаблон графика и период сессии**, после нажмите кнопку **Сформировать**

 **график**.



Откроется окно с наименованием графика.

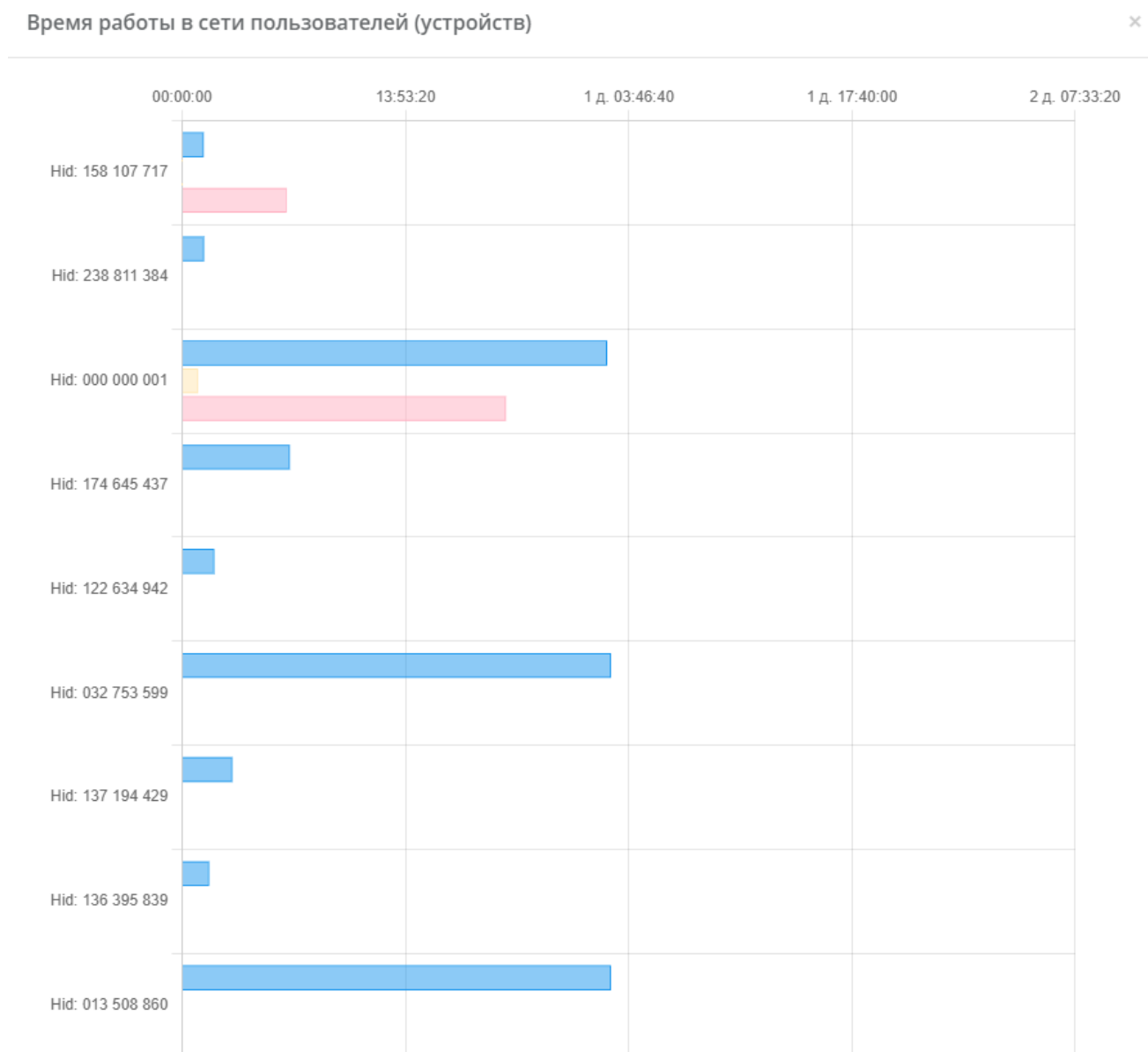


Рисунок 54 Окно графика

Доступны следующие шаблоны графиков:

Время работы в сети пользователей (устройств)	Отображает общее время на устройстве пользователя за определенный период
Количество соединений между устройствами	Отображает количество установленных соединений за указанный период
Продолжительность соединений между устройствами	Отображает время соединения между устройствами за определенный период

7. АДМИНИСТРИРОВАНИЕ

Глава содержит описание раздела, подразделы которого предназначены для тонкой настройки параметров **Системы**, разграничения прав доступа и лицензирования. Сведения, содержащиеся в этой главе, предназначены для пользователя с правами **Администратора Системы**.

Раздел **Администрирование** предназначен для управления устройствами, сессиями, учетными записями и лицензиями. В разделе определяются виды лицензий, роли доступа, системные настройки и атрибуты серверов.

7.1. Устройства

В подразделе **Устройства** отображается список всех устройств, подключенных к управляющему серверу **Системы**.

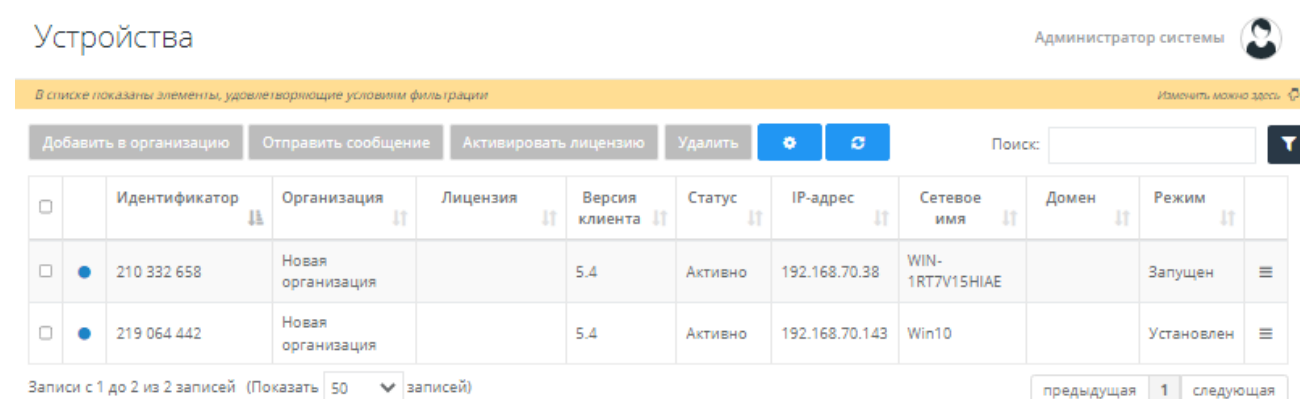


Рисунок 55 Страница Устройства

Доступ к подразделу имеют пользователи с включенной ролью **Устройства**.

Подраздел **Устройства** содержит следующие элементы управления:

	Автоматическое добавляет устройств в организацию. (Описано в пункте 5.1.1)
Добавить в организацию	Добавляет новое устройство в организацию.
Отправить сообщение	Отправляет текстовое сообщение на выбранные устройства. Отправленное сообщение будет отображено на выбранных устройствах во всплывающем окне Уведомление .
Активировать лицензию	Удаленно активирует лицензию на выбранных устройствах.
Удалить	Удаляет устройство.
Обновить	Обновляет список Устройства .

	Действия	Позволяет: ○ Изменить – в том числе Активировать или Заблокировать устройство; ○ Отправить сообщение; ○ Активировать лицензию; ○ Закрыть все сессии – принудительно прервать все соединения ○ Удалить –удалить устройство из списка..
---	-----------------	--

Примечание: Для возврата к **Базовой** лицензии в окне **ВВЕДИТЕ НОМЕР ЛИЦЕНЗИИ** оставьте поле пустым и нажмите кнопку **Активировать**.

7.1.1. Автодобавление в организацию.

Кнопка **Автодобавление в организацию** позволяет настроить автоматическое добавление новых устройств при первой регистрации на сервере в выбранную организацию с выбранными политиками доступа.

Для настройки автоматического добавления новых устройств в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Устройства**.



Откроется страница **Устройства**.

3. Нажмите кнопку .



Откроется окно **Настройка автодобавления устройств в организацию**.

НАСТРОЙКИ АВТОДОБАВЛЕНИЯ УСТРОЙСТВ В ОРГАНИЗАЦИЮ

Все новые устройства при первой регистрации на сервере будут автоматически добавлять в выбранную организацию с указанными политиками доступа.

☐ Включено

Фильтр по IP

В организацию будут добавлены только устройства, подходящие под фильтр

Организация

Не выбрано

Группа

Не выбрано

Политика доступа

Не выбрано

Политика инвентаризации

Не выбрано

☒ Запретить изменение настроек безопасности на устройстве

Доступ для отделов

Не выбрано

Политика доступа для отделов

Не выбрано

Выбранная политика доступа будет действовать для сотрудников указанных отделов при подключении к выбранным устройствам. При этом правила доступа и ограничения будут иметь приоритет перед параметрами политики доступа, назначенной этим устройствам по умолчанию.

Сохранить

Отмена

Рисунок 56 Окно Настройки автодобавления устройств в организацию

4. Заполните все обязательные поля и нажмите кнопку **Сохранить**.

7.1.2. Добавление в организацию

Кнопка **Добавление в организацию** позволяет добавить в организацию устройства, зарегистрированные на сервере.

Для добавления в организацию зарегистрированных на сервере устройств:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Устройства**.

»»» Откроется страница **Устройства**.

3. Нажмите кнопку **Добавить в организацию**.

»»» Откроется окно **Добавление в организацию**.

ДОБАВЛЕНИЕ В ОРГАНИЗАЦИЮ (ВЫБРАНО: 3) ✕

Организация	Сафиб
Группы	Все
Политика доступа	Без пароля
Политика инвентаризации	Не выбрано
☒ Запретить изменение настроек безопасности на устройстве	
Доступ для отделов	Не выбрано
Политика доступа для отделов	Не выбрано

Выбранная политика доступа будет действовать для сотрудников указанных отделов при подключении к выбранным устройствам. При этом правила доступа и ограничения будут иметь приоритет перед параметрами политики доступа, назначенной этим устройствам по умолчанию.

☐ Изменять данные устройства в организации

Выполнить

Отмена

Рисунок 57 Окно Добавление в организацию

4. Заполните все обязательные поля и нажмите кнопку **Выполнить**.

7.2. Транспортные серверы

Подраздел **Транспортные серверы** содержит перечень транспортных серверов **Ассистент PRO**. Первоначальная настройка и конфигурирование серверов осуществляется на этапе развёртывания **Системы**.

Подраздел **Транспортные серверы** предназначен для ручной регистрации и настройки транспортных серверов **Системы**.

Примечание: Подробнее о настройке и конфигурировании транспортных серверов в документе **Руководство администратора**.

Подраздел **Транспортные серверы** содержит следующие элементы управления:

		Открывает страницу добавления нового сервера.
		Останавливает ранее начатый процесс переноса сессий на другой транспортный сервер.
		Удаляет выбранные серверы.
	Обновить	Обновляет список серверов.
	Действия	Позволяет: • Переместить сессии на другой сервер. • Изменить. • Удалить.

Список подраздела содержит следующую информацию:

Наименование	Наименование сервера.
Адрес сервера	IP – адрес транспортного сервера.
Порт для сервера / приложения	Адреса портов для ID-сервера и приложения. По умолчанию: • для сервера – 44344; • для приложения – 44444.
Статус	Текущий статус транспортного сервера.
Регистаций	Текущее количество активных подключений.
% регистаций	Текущий процент активных подключений.
Управлений	Текущее количество активных сессий управления.
% управлений	Текущий процент активных сессий управления.

Подраздел доступен пользователям с включенной ролью **Серверы**.

7.3. Виды лицензий

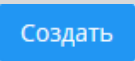
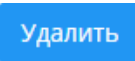
Подраздел **Виды лицензий** предназначен для ведения и настройки видов выдаваемых пользователям лицензий.

В **Виде лицензии** определяется количество одновременных исходящих соединений и доступные модули расширения.

Примечание: при включенном модуле **Соединение** можно ограничить список доступных для соединения устройств с помощью включения флага **Соединение только с разрешенными устройствами**. При его активации пропадет поле ввода идентификатора для подключения, а подключение будет доступно только к устройствам из списка разрешенных. Подробнее о доступе к устройствам в пункте 4.1.5 Устройства.

Общее количество всех исходящих соединений в один момент времени, со всех устройств, на которых активна конкретная лицензия, не может превышать лимит, который установлен в типе лицензии.

Подраздел **Виды лицензий** содержит следующие элементы управления:

		Открывает страницу добавления нового Вида лицензии .
		Удаляет выбранные Виды лицензии .
	Обновить	Обновляет список Видов лицензий .
	Действия	Позволяет: ○ Изменить; ○ Удалить; вид лицензии .

Подраздел доступен пользователям с включенной ролью **Виды лицензий**.

Примечание: Вид лицензии **По умолчанию** удалить нельзя. Это та лицензия, с которой работают **Клиентские приложения**, пока на них не будет активирована другая лицензия. При необходимости можно изменить настройки вида лицензии **По умолчанию**.

7.4. Лицензии

Подраздел **Лицензии** предназначен для ведения перечня лицензий, для функционирования **Клиентского приложения**. При создании **Лицензии** генерируется особый ключ – **Номер лицензии**, который необходимо указать в **Клиентском приложении** для использования отличного от **По умолчанию Вида лицензии**. Одна лицензия (номер лицензии) может быть активирована на неограниченном количестве **Клиентских приложений** и **Учетных записей**. **Видом лицензии** ограничивается число одновременных соединений, возможность подключения к устройствам, не находящимся в списке разрешенных и возможность использования тех или иных модулей расширения.

Для создания новой лицензии:

1. Войдите в **Личный кабинет** под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Лицензии**.

»»» Откроется страница **Лицензии**.

3. Нажмите кнопку **Создать**.

»»» Откроется страница **Создание лицензии**.

Создание лицензии

Администратор системы

лицензии / создание

Статус	Активна
Дата выдачи	03.06.2020
Дата окончания действия лицензии	
Номер лицензии	AA854CC7-C829B74C-92894DAD-FFEE7573
Вид лицензии	30 соединений (соединений: 30)
Комментарий	

Сохранить Отмена

Рисунок 58 Страница Создание лицензии

4. Выберите **Статус**, **Дата выдачи** и **Вид лицензии**. При необходимости укажите **Дата окончания действия лицензии** и **Комментарий**.
5. Если по каким-то причинам создается **Заблокированная** лицензия, вы сможете указать **Причину блокировки**.
6. Нажмите кнопку **Сохранить**.

»»» Откроется список **Лицензии**. В список добавится созданная лицензия.

Сообщите пользователям **Номер лицензии** для ее активации в **Клиентском приложении**, либо активируйте лицензию на устройствах самостоятельно. Подробнее в пунктах [4.1.5 Устройства](#) и [7.1 Устройства](#).

Примечание: Подробнее о активации лицензии посредством **Клиентского приложения** в документе **Руководство пользователя. Клиентское приложение**.

Подраздел доступен пользователям с включенной ролью **Лицензии**.

7.5. Роли доступа

Подраздел содержит информацию о **Ролях доступа** пользователей. **Роли доступа** используются в **Системе** для разграничения доступа к разделам и подразделам **Личного кабинета** и **приложения**.

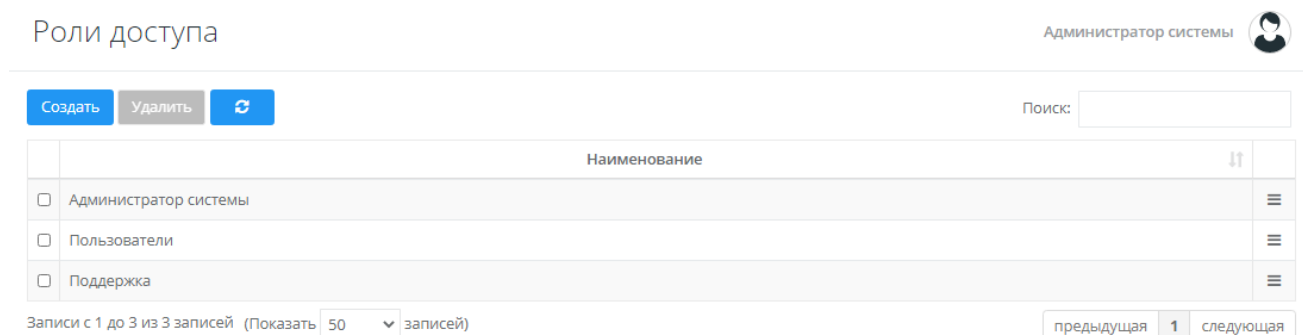


Рисунок 59 Страница Роли доступа

Подраздел **Роли доступа** предназначен для ведения перечня пользовательских ролей **Системы**.

По умолчанию используются две роли:

- «Пользователи»;
- «Администратор системы».

Администратор Системы может определить неограниченное количество **Ролей доступа**.

Если **Роль** обладает включенным параметром **Автоприсваивание**, то эта роль будет **по умолчанию** присваиваться каждому зарегистрированному пользователю. Данный параметр может быть включен только у одной роли и по умолчанию включен для роли **Пользователи**.

Подраздел **Роли доступа** содержит следующие элементы управления:

	Открывает страницу добавления новой Роли доступа .
	Удаляет выбранные Роли доступа .
	Обновляет список Роли доступа .
	Позволяет: • Изменить; • Удалить; Роли доступа .

Отличные от **Автоприсвоенных** роли могут быть назначены пользователям в подразделе **Учетные записи**.

Подраздел доступен пользователям с включенной ролью **Роли доступа**.

7.6. Учетные записи

Подраздел **Учетные записи** предназначен для создания и просмотра списка учетных записей **Системы**.

Пользователь с включенной ролью **Учетные записи** посредством кнопки  **Действия** может **Изменить** учетную запись пользователя, назначить необходимые **Роли доступа**, изменить **Статус** учетной записи и **Активировать лицензию** для учетной записи.

При включенной системной настройке **Прямое управление субъектами Системный Администратор** может изменить основные атрибуты учетной записи пользователя.

Внимание! Удаление учетных записей Системы невозможно. Изменение статуса учетной записи позволяет сделать ее активной, заблокировать, либо отправить в архив.

учетные записи / создание

Адрес электронной почты	admin@corpname.ru
Имя	Администратор
Пароль	 Пароль должен содержать не меньше 1 символа(ов)
Подтвердите пароль	
Статус	Активен
Телефон	
	☐ Двухфакторная аутентификация
Комментарий	
	☐ Получать уведомления на email о заявках в поддержку
Часовой пояс	(UTC+03:00) Москва, Санкт-Петербург, Волгоград
Роли доступа	☒ Пользователи ☒ Администратор системы
Аватар	Выберите файл Файл не выбран

Сохранить

Отмена

Рисунок 60 Окно Учетная запись

Примечание: Для создания ученой записи посредством **Личного кабинета** необходимо, что бы настройка **Самостоятельная регистрация пользователей** была включена. Подробнее о настройке в пункте 7.8 Настройки.

7.6.1. Создание учетной записи

Для создания учетной записи:

1. Войдите в **Личный кабинет** под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Учетные записи**.



Откроется страница **Учетные записи**.

3. Нажмите кнопку **Создать**.

»»» Откроется страница **Учетная запись**.

4. Заполните все обязательные поля.

5. Нажмите кнопку **Сохранить**.

»»» Откроется список **Учетные записи**. В список добавится созданная учетная запись.

7.6.2. Привязка учетной записи Ассистент PRO к учетной записи домена

Если используется режим «Аутентификация через службу каталогов», то возможно привязать к существующей учетной записи **Ассистент PRO** учетную запись из **домена**.

Для привязки учетной записи из **домена**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.

2. В главном меню выберите пункт **Администрирование – Учетные записи**.

»»» Откроется страница **Учетные записи**.

3. Выберите необходимую учетную запись, нажмите кнопку  **Действия** и выберите пункт **Привязать к службе каталогов**.

»»» Откроется окно **Импорт учетных записей из домена**.

4. Выберите необходимый **домен** и нажмите кнопку **Подключиться**.

»»» Откроется страница **Импорт учетных записей из домена**.

5. Выберите учетную запись **домена**, к которой необходимо привязать текущую учетную запись **Ассистент PRO** и нажмите кнопку **Импортировать**.

»»» Появится уведомление об успешном выполнении операции.

7.6.3. Импорт учетных записей из домена

Если в организации используется служба каталогов, то добавить учетные записи в **Систему** возможно посредством импорта из каталогов **домена**.

Внимание! Перед импортом учетных записей домена необходимо убедиться, что включен режим «Аутентификация через службу каталогов» в Системных настройках (подробнее в пункте 7.8.2 Безопасность).

Примечание: Для получения списка учетных записей необходима учетная запись пользователя **домена** с правами на просмотр.

Для импорта учетных записей из **домена** **aeconomy**:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Учетные записи**.



Откроется страница **Учетные записи**.

3. Нажмите кнопку **Импортировать из домена**.



Откроется окно **Импорт учетных записей из домена**.

4. Выберите необходимый **домен** и нажмите кнопку **Подключиться**.



Откроется страница **Импорт учетных записей из домена**.

5. Выберите необходимые для импорта учетные записи и нажмите кнопку **Импортировать**.



Откроется окно **Назначение атрибутов**.

6. Включите необходимые параметры импорта и нажмите кнопку **Выполнить**.



Откроется окно **Результат импорта учетных записей из домена**.

7.6.4. Добавление в организацию

Функционал **Личного кабинета** Системы позволяет импортировать единичные либо несколько учетных записей пользователей, содержащихся в соответствующем перечне, в выбранную организацию при условии включенной настройки **Прямое управление субъектами**.

Для добавления учетных записей в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Учетные записи**.

 Откроется страница **Учетные записи**.

3. Выберите необходимые учетные записи и нажмите кнопку **Добавить в организацию**

 Откроется окно **Добавить в организацию**.

4. Выберите **организацию** и **отдел** для добавления **пользователей**, при необходимости назначения **администратора организации** проставьте соответствующий **флаг**, и нажмите кнопку **Выполнить..**

 Отобразится сообщение успешного добавления пользователя в организацию.

В случае, если настройка **Прямое управление субъектами** отключена, на странице **Администрирование – Учетные записи** вы можете **Добавить в организацию** одного либо нескольких пользователей.

Для добавления учетных записей в организацию:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Учетные записи**.

 Откроется страница **Учетные записи**.

3. Выберите необходимые учетные записи и нажмите кнопку **Добавить в организацию**

 Откроется окно **Добавление в организацию**.

4. Выберите **организацию** для добавления пользователей, **отдел и роль администратора**, после чего нажмите кнопку **Выполнить..**

 Отобразится сообщение успешного добавления пользователя в организацию.

7.6.5. Активация лицензии для учетной записи

Для получения доступа ко всем возможностям лицензии без привязки к устройству, достаточно активировать эту лицензию для учетной записи. После авторизации в **Клиентском приложении** с этой учетной записью, лицензия будет применена автоматически.

Для активации лицензии в учетной записи:

1. Войдите в **Личный кабинет** (подробнее в пункте 2.2 Вход в личный кабинет) под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Учетные записи**.

»»» Откроется страница **Учетные записи**.

3. Выберите необходимую учетную запись, нажмите кнопку **Активировать лицензию** или кнопку **Действия** и выберите пункт **Активировать лицензию**.

»»» Откроется окно **Введите номер лицензии**.

4. Введите номер лицензии, которую необходимо активировать для учетной записи и нажмите кнопку **Активировать**.

»»» Появится уведомление об успешной активации лицензии.

Внимание! Лицензия, активированная для Учетной записи пользователя, имеет более высокий приоритет чем лицензия, активированная в Клиентском приложении.

7.7. Категории заявок

Подраздел **Категории заявок** содержит перечень категорий, используемых для создания заявок в техподдержку.

Категории заявок Администратор системы 

Создать

Удалить



Поиск:

	Наименование	
☐	Прочие	≡
☐	Железо	≡
☐	Софт	≡
☐	Сеть	≡
☐	Лицензия	≡

Записи с 1 до 5 из 5 записей (Показать записей)

предыдущая

1

следующая

Рисунок 61 Страница Категории заявок

Для создания новой категории:

1. Войдите в **Личный кабинет** под учетной записью **Администратора Системы**.
2. В главном меню выберите пункт **Администрирование – Категории заявок**.



Откроется страница **Категории заявок**.

3. Нажмите кнопку **Создать**.



Откроется страница **Категории заявок. Создание**.

Рисунок 62 Страница Категории заявок. Создание

4. Введите **Наименование** новой категории и нажмите кнопку **Сохранить**.



Откроется страница **Категории заявок**. Новая категория появится в списке.

7.8. Настройки

Подраздел **Настройки** содержит системные настройки, настройки параметров безопасности и политики доступа по умолчанию.

Подраздел доступен пользователям с включенной ролью **Системные настройки**. Параметры и настройки находятся в трех вкладках страницы **Системные настройки**:

- Параметры.
- Безопасность.
- Политика доступа по умолчанию.

7.8.1. Параметры

На вкладке **Параметры** страницы **Системные настройки** содержатся следующие группы настроек:

- **Режимы работы** – настройки работы сервера **Ассистент PRO**.
- **Параметры SMTP-сервера** – параметры почтового сервера, используемого **Системой**.
- **Параметры Telegram-API** – настройки для двухфакторной аутентификации через **Telegram**.
- **Сервер обновления клиентского приложения** – настройки доступа к серверу автоматического обновления.

- **Директории для хранения файлов** – пути к протоколам событий удаленного взаимодействия, файлов видео сеансов, снимков экрана, log-файлов **Клиентских приложений**, syslog-файлов, данных инвентаризации.
- **Информационные сообщения** – информационное сообщение, отображаемое в **Клиентском приложении**.
- **Подсистема техподдержки** – флаг включения подсистемы технической поддержки.

Режимы работы

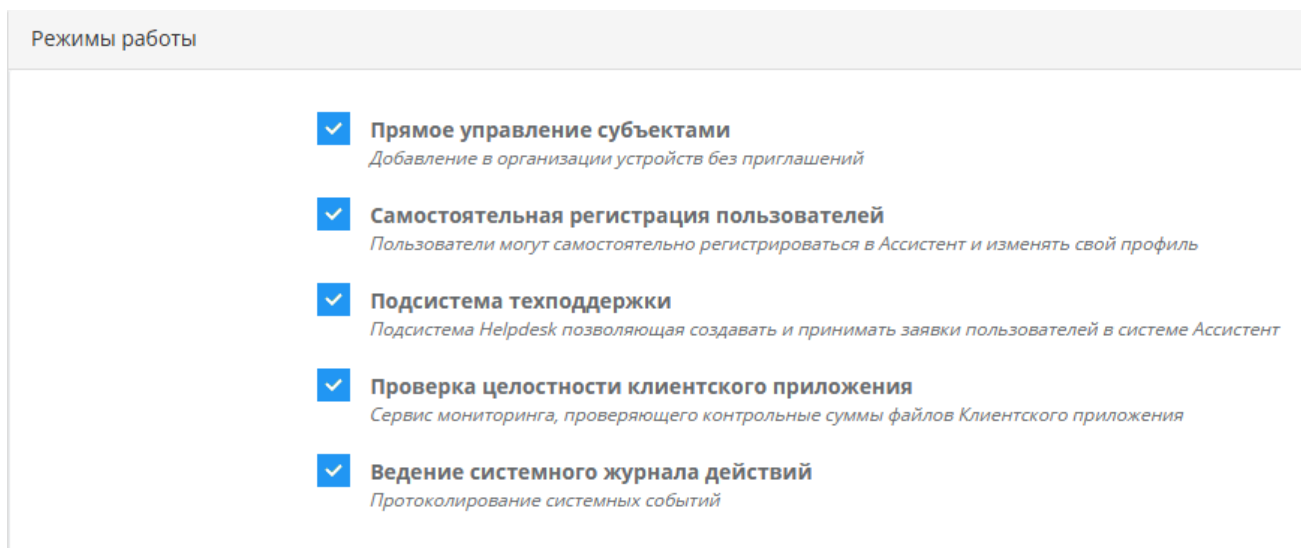


Рисунок 63 Режимы работы

Группа содержит следующие настройки:

Прямое управление субъектами	Добавление в организации устройств без приглашений.
Подсистема техподдержки	Включение подсистемы технической поддержки.
Проверка целостности клиентского приложения	При включении будут проверяться контрольные суммы файлов Клиентского приложения , которое подключается к серверу Системы .
Ведение системного журнала действий	Протоколирование системных событий.
Самостоятельная регистрация пользователей	При включенном признаке пользователи могут самостоятельно регистрироваться в Системе и изменять свой профиль. При выключенном признаке пользователям для изменения доступен только аватар и пароль.

Параметры SMTP-сервера

Группа настроек **Параметры SMTP-сервера** содержит параметры почтового сервера, используемого **Системой**.

Параметры SMTP-сервера

Адрес smtp-сервера: smtp.corpname.ru

Порт: 25

Логин: corpname

Пароль:

Email отправителя: email@corpname.ru

Имя отправителя: Ассистент corp.dev

☐ Требуется SSL

Рисунок 64 Группа настроек SMTP-сервер

Группа содержит следующие настройки:

Адрес smtp-сервера	Адрес сервера исходящих почтовых сообщений.
Порт	Порт сервера для отправки почтовых сообщений.
Логин	Логин сервера исходящих почтовых сообщений.
Пароль	Пароль пользователя для доступа к учетной записи для отправки сервисных почтовых сообщений.
Email отправителя	Адрес электронной почты, с которого будут отправляться сервисные сообщения.
Имя отправителя	Имя, которое будет использовано для отправляемых сообщений.
Требует SSL	Признак использования уровня защищенных сокетов.

Сервер обновления клиентского приложения

Группа настроек **Сервер обновления клиентского приложения** содержит настройки доступа к серверам автоматического обновления.

Сервер обновления клиентского приложения

FTP-адрес с обновлениями клиентского приложения: 2

HTTP-адрес с обновлениями клиентского приложения: http://update.corpname.ru:80

Список HTTP-адресов с обновлениями клиентского приложения: http://update.corpname.ru:80, http://update.corpname.ru:8080

Рисунок 65 Группа настроек Сервер обновления клиентского приложения

Группа содержит следующие настройки:

FTP-адрес с обновлениями клиентского приложения	Адрес FTP-сервера обновлений. Предназначен для обновления Клиентских приложений версии 2.6 и ниже .
HTTP-адрес с обновлениями клиентского приложения	Адрес сервера обновлений. Предназначен для обновления Клиентских приложений версии 2.7 и выше .
Список HTTP-адресов с обновлениями клиентского приложения	Адреса серверов обновлений (через запятую). Предназначены для обновления Клиентских приложений версии 3.3 и выше .

Директории для хранения файлов

Группа настроек **Директории для хранения файлов** содержит пути для хранения файлов протоколов **Системы** и **Клиентского приложения**.

Директории для хранения файлов

Директория для хранения файлов протоколирования

Директория для хранения скриншотов, видеозаписей и протоколов, собираемых подсистемой протоколирования

Директория для хранения syslog файлов

Директория для хранения данных инвентаризации

Рисунок 66 Группа настроек Директории для хранения файлов

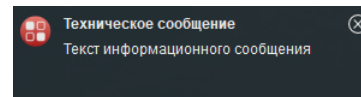
Группа настроек **Директории для хранения файлов** содержит следующие настройки:

Директория для хранения файлов протоколирования	Содержит путь к директории хранения протоколов событий удаленного взаимодействия, файлов видео сеансов, снимков экрана, log-файлов Клиентских приложений .
Директория для хранения syslog файлов	Содержит путь к директории хранения файлов системных протоколов .
Директория для хранения данных инвентаризации	Содержит путь к директории хранения протоколов с информацией об оборудовании и программном обеспечении, установленном на устройствах организации.

Внимание! В случае установки сервисов Системы на разных серверах в настройке должен содержаться сетевой путь.

Информационные сообщения

Блок настроек **Информационные сообщения** содержит текст сообщения, которое будет отображаться пользователям при старте **Клиентского приложения**.



Информационные сообщения

Информационное сообщение в клиентском приложении

Рисунок 67 Группа настроек Информационные сообщения

7.8.2. Безопасность

На вкладке **Безопасность** страницы **Системные настройки** содержатся следующие группы настроек:

- **Режимы аутентификации** – настройки режимов использования учётных записей .
- **Параметры аутентификации через Keycloak.**
- **Правила безопасности локальных учетных записей.**

Режимы аутентификации

Режимы аутентификации

☒ **Аутентификация через службу каталогов**
Вход в систему под учётными записями корпоративного домена (Настроить домены)

☒ **Аутентификация через Keycloak**
Вход в систему под учётными записями Keycloak с применением протокола OAuth 2.0

☒ **Привязывать учетные записи из Keycloak к существующим учетным записям Ассистент**
Если в Ассистент найдена учетная запись с таким же Email, к ней привязывается учетная запись из Keycloak

Рисунок 68 Группа настроек Режимы аутентификации

Группа содержит следующие настройки:

Аутентификация через службу каталогов	Включение аутентификации посредством выбора различных доменов .
Аутентификация через Keycloak	Включение аутентификации посредством Keycloak .
Привязывать учетные записи из Keycloak к существующим учетным записям Ассистент PRO	Привязка учётных записей в Ассистент PRO к записям Keycloak при совпадении электронной почты .

Параметры аутентификации через Keycloak

Параметры аутентификации через Keycloak	
URL формы авторизации	http://192.168.72.42:21037/realms/master/protocol/openid-connect/auth
URL запроса токена доступа	http://192.168.72.42:21037/realms/master/protocol/openid-connect/token
URL проверки токена доступа	http://192.168.72.42:21037/realms/master/protocol/openid-connect/token/introspect
URL выхода	http://192.168.72.42:21037/realms/master/protocol/openid-connect/logout
Client ID	test_client_0
Client Secret	

Рисунок 69 Группа настроек параметры аутентификации через Keycloak

Группа содержит следующие настройки:

URL формы авторизации	/realms/{realm-name}/protocol/openid-connect/auth
URL запроса токена доступа	/realms/{realm-name}/protocol/openid-connect/token
URL проверки токена доступа	/realms/{realm-name}/protocol/openid-connect/token/introspect
URL выхода	/realms/{realm-name}/protocol/openid-connect/logout
Client ID	Идентификатор клиента необходимо скопировать из консоли администратора Keycloak , перейдя в созданный ранее клиент для взаимодействия с Ассистент PRO , находится на вкладке Settings
Client Secret	Секретный код необходимо скопировать из консоли администратора Keycloak , перейдя в созданный ранее клиент для взаимодействия с Ассистент PRO , находится на вкладке Credentials

Примечание: Конечные точки (Endpoints) можно сформировать в соответствии с официальной документацией **Keycloak**, например:

https://www.keycloak.org/docs/22.0.3/securing_apps/index.html

Правила безопасности локальных учетных записей

Правила безопасности локальных **учетных записей** – блок настроек, которые определяют период блокировки для неактивных учетных записей, требования к паролю и параметры аутентификации.

Учетная запись

Период блокирования неактивных учетных записей, дн

3

Максимальное количество неудачных попыток аутентификации

3

Длительность блокировки учетной записи при превышении количества неудачных попыток аутентификации, мин

50000

Период контроля неудачных попыток аутентификации для блокирования учетной записи, мин

1

Период смены пароля, дн

30

Минимальная длина пароля

1

☒ Пароль должен содержать хотя бы один символ, не являющийся цифрой или буквой

☒ Пароль должен содержать хотя бы одну цифру

☒ Пароль должен содержать хотя бы одну строчную букву

☒ Пароль должен содержать хотя бы одну заглавную букву

Рисунок 70 Группа настроек Учетная запись

Группа содержит следующие настройки:

Период блокирования неактивных учетных записей, дн	Количество дней, после которого при условии неиспользования учетной записи она будет заблокирована.
Максимальное количество неудачных попыток аутентификации	Число неудачных попыток аутентификации, по исчерпании которых учетная запись будет заблокирована.
Длительность блокировки учетной записи при превышении количества неудачных попыток аутентификации, мин	Количество минут, на протяжении которых учетная запись будет заблокирована при превышении количества неудачных попыток аутентификации.
Период контроля неудачных попыток аутентификации для блокирования учетной записи, мин	Количество минут, на протяжении которых считаются неудачные попытки аутентификации.
Период смены пароля, дн	Количество дней, после которого потребуется сменить пароль.
Минимальная длина пароля	Минимальное количество символов, из которых может состоять пароль.
Пароль должен содержать хотя бы один символ, не являющийся цифрой или буквой	Признак устанавливает требования к сложности пароля.
Пароль должен содержать хотя бы одну	Признак устанавливает требования к сложности пароля.

цифру	
Пароль должен содержать хотя бы одну строчную букву	Признак устанавливает требования к сложности пароля.
Пароль должен содержать хотя бы одну заглавную букву	Признак устанавливает требования к сложности пароля.

7.8.3. Политика доступа по умолчанию

На вкладке **Политика доступа по умолчанию** настраивается политика доступа к модулям управления **Клиентского приложения** для устройств, которые не состоят в организации и которым не назначена иная политика доступа.

Системные настройки

Параметры

Безопасность

Политика доступа по умолчанию

Соединение	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Управление рабочим столом	☒ Разрешено	☐ С подтверждением	☐ Запрещено	☐ Только просмотр	
Обмен файлами	☒ Разрешено	☐ С подтверждением	☐ Запрещено	☐ Только просмотр	☐ С ограничениями
☒ Разрешить повышенные права					
Редактор реестра	☒ Разрешено	☐ С подтверждением	☐ Запрещено	☐ Только просмотр	
Диспетчер задач	☒ Разрешено	☐ С подтверждением	☐ Запрещено	☐ Только просмотр	
Диспетчер устройств	☒ Разрешено	☐ С подтверждением	☐ Запрещено	☐ Только просмотр	
Информация о системе	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Командная строка	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Управление питанием	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Удаленная печать	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Подключение usb-токенов	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
TCP туннель	☒ Разрешено	☐ С подтверждением	☐ Запрещено		
Чат	☒ Разрешено	☐ Запрещено			
Обмен сторонами	☒ Разрешено	☐ Запрещено			

☐ Доступ к модулям до входа в ОС

☒ Удаленное управление настройками

☒ Разрешать блокировку средств ввода

☒ Разрешать блокировать устройство после завершения соединения

☒ Синхронизация буфера обмена

☒ Разрешать соединение до входа в ОС, если доступ "С подтверждением"

Сохранить

Отмена

Рисунок 71 Вкладка Политика доступа по умолчанию

На вкладке **Политика доступа по умолчанию** доступны настройки аналогичные **Политикам доступа в Организации**. Подробнее о политиках доступа организации в пункте 4.1.2 Политики доступа.

8. УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ

Раздел **Управление конфигурациями** предназначен для автоматизации настройки удаленных устройств в сети, путём написания определённого сценария.

Раздел **Управление конфигурациями** содержит следующие подразделы:

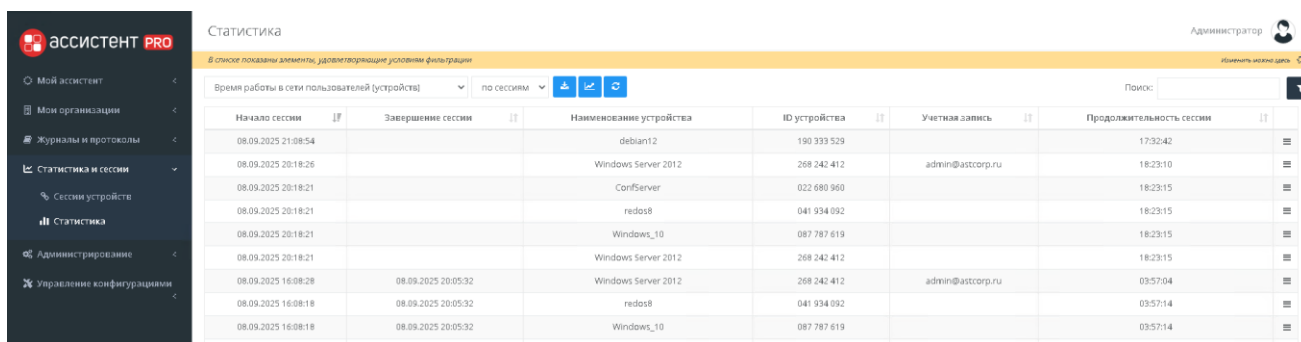
- **Шаблоны** – подраздел содержит сценарии, которые будут выполняться на удаленных устройствах.
- **Задачи** – подраздел позволяет выбрать существующие шаблоны для определённого набора устройств, которые будут выполняться по заданному расписанию.

8.1. Шаблоны

Подраздел **Шаблоны** предназначен для создания и хранения сценариев, которые выполняются на удаленных устройствах. Эти сценарии представляют собой описывающие последовательность команд и настроек для конфигурации устройств.

Функционал раздела **Шаблоны**:

- Создание и редактирование шаблонов.
- Создание группы шаблонов.
- Тестирование шаблонов на выбранных устройствах перед применением.
- Использование переменных в сценариях для повышения гибкости настройки.
- Группировка шаблонов по категориям.
- Редактирование, копирование и удаление существующих шаблонов.



Начало сессии	Завершение сессии	Наименование устройства	ID устройства	Учетная запись	Продолжительность сессии
08.09.2025 21:08:54		debian12	190 333 529		17:32:42
08.09.2025 20:19:26		Windows Server 2012	268 242 412	admin@astcorp.ru	18:23:10
08.09.2025 20:18:21		ConfServer	022 680 960		18:23:15
08.09.2025 20:19:21		redos8	041 934 092		18:23:15
08.09.2025 20:18:21		Windows_10	087 787 619		18:23:15
08.09.2025 20:18:21		Windows Server 2012	268 242 412		18:23:15
08.09.2025 16:08:28	08.09.2025 20:05:32	Windows Server 2012	268 242 412	admin@astcorp.ru	03:57:04
08.09.2025 16:08:18	08.09.2025 20:05:32	redos8	041 934 092		03:57:14
08.09.2025 16:08:18	08.09.2025 20:05:32	Windows_10	087 787 619		03:57:14

Рисунок 72 Подраздел Шаблоны конфигураций

8.1.1. Создание группы шаблонов

Для создания шаблона необходимо указать **Группу шаблонов**. Для создания группы шаблонов:

1. Нажмите кнопку  в списке групп шаблонов.



Откроется страница **Создание группы шаблонов конфигурации**.

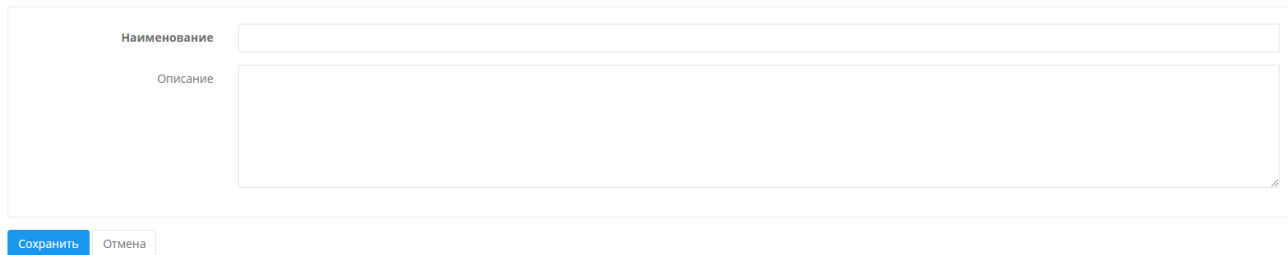


Рисунок 73 Страница Создание группы шаблонов конфигурации

2. Заполните **Наименование**.
3. При необходимости заполните строку **Описание**.
4. Нажмите кнопку **Сохранить**.

8.1.2. Создание шаблона

Примечание: Для создания нового шаблона необходима хотя бы одна группа шаблонов. Если список шаблонов пуст, перед созданием выполните действия, описанные в пункте 8.1.1 Создание группы шаблонов

Для добавления шаблона в список:

1. Нажмите кнопку  в списке шаблонов.



Откроется страница **Создание шаблона конфигурации**.

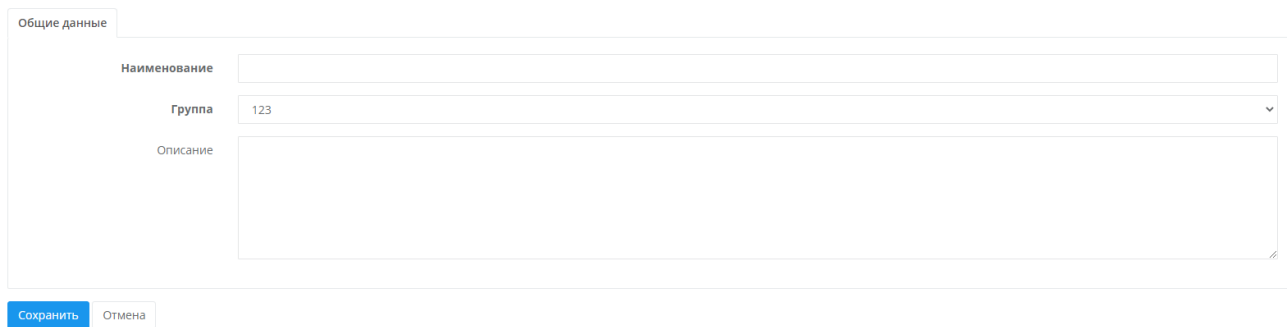


Рисунок 74 Страница Создание шаблона конфигурации

2. Заполните обязательные поля страницы:
 - **Наименование** – введите наименование шаблона.
 - **Группа** – выберите из списка групп шаблонов.
3. При необходимости заполните поле **Описание**.
4. Нажмите кнопку **Сохранить**.

8.1.3. Добавление сценария в шаблон конфигурации

После создания шаблона необходимо добавить в него сценарий выполнения, который будет применяться к удаленным устройствам.

Для добавления сценария в существующий шаблон:

1. Откройте список **Шаблонов** конфигурации.
2. Выберите шаблон, нажмите кнопку  **Действия** и выберите пункт **Изменить**.

 Откроется страница **Редактирование шаблона**.

Редактирование шаблона "Тест" Администратор системы 

управление конфигурациями / шаблоны конфигураций / редактирование

Общие данные | Атрибуты | Сценарии | Тест выполнения

Наименование:

Группа:

Описание:

☐ Готов к выполнению

Сохранить Отмена

Рисунок 75 Страница Редактирование шаблона конфигурации

3. Перейдите на вкладку **Сценарии**.

 Откроется вкладка **Сценарии**.

Редактирование шаблона "Тест"

управление конфигурациями / шаблоны конфигураций / редактирование

Общие данные | Атрибуты | **Сценарии** | Тест выполнения

```
1 - name: Тест
2 hosts: all
3 vars:
4   prompt: null
5   tasks: null
6
```

Рисунок 76 Вкладка Сценарий шаблона

4. Введите код сценария в формате **YAML**, описывающий необходимые действия.

Примечание: Если в сценарии используются переменные, укажите их в секции `vars_prompt`.

5. Нажмите кнопку **Сохранить**.

8.1.4. Атрибуты

Вкладка **Атрибуты** предназначена для управления переменными в сценарии, которые будут заполняться перед выполнением задачи. Значения этих переменных используются в секции `vars_prompt` сценария и позволяют гибко настраивать выполнение шаблонов.

Для управления атрибутами шаблона:

1. Откройте страницу изменения ранее созданного шаблона в разделе **Шаблоны**.
2. Перейдите на вкладку **Атрибуты**.



Откроется вкладка **Атрибуты**

Редактирование шаблона конфигурации "установка MSI" Администратор системы 

управление конфигурациями / шаблоны конфигураций / редактирование

Общие данные **Атрибуты** Сценарии Тест выполнения

Путь к файлу

Укажите путь к файлу из Хранилища

Параметры запуска

Укажите параметры для запуска MSI

Сохранить Отмена

Рисунок 77 Вкладка Атрибуты

Примечание: Поля атрибутов создаются **автоматически** на основе объявленных переменных в сценарии (`vars_prompt`).

3. При необходимости измените параметры атрибутов.
4. Нажмите кнопку **Сохранить**.

8.1.5. Тест выполнения

Вкладка **Тест выполнения** предназначена для проверки работоспособности сценария перед его применением на устройствах. С ее помощью можно выполнить шаблон на выбранном удаленном устройстве и просмотреть результат работы в режиме реального времени.

Для тестирования шаблона:

1. Откройте страницу изменения ранее созданного шаблона в разделе **Шаблоны**.
2. Перейдите на вкладку **Тест выполнения**.



Откроется вкладка **Тест выполнения**

управление конфигурациями / шаблоны конфигураций / редактирование

Рисунок 78 Вкладка Тест выполнения

3. В поле **Идентификатор устройства** введите одно или несколько устройств, разделяя их запятой.
4. Нажмите кнопку **Выполнить** для запуска теста.



В консоли отобразится **лог выполнения**, показывающий ход работы сценария.

8.1.6. Готов к выполнению

Флаг **Готов к выполнению** подтверждает, что шаблон полностью настроен и может быть использован в задачах. Без этого флага шаблон не будет доступен при создании задач.

Условия для активации флага **Готов к выполнению**.

Флаг становится доступным **только после сохранения шаблона** и его последующего редактирования. Он может быть установлен, если:

- Заполнены **основные данные** (наименование, группа).
- Добавлен **сценарий** во вкладке "Сценарий".
- Заполнены все **обязательные атрибуты** во вкладке "Атрибуты" (если таковые есть).

Для установки флага **Готов к выполнению**:

1. Откройте список **Шаблонов** конфигурации.
2. Выберите шаблон, нажмите кнопку  **Действия** и выберите пункт **Изменить**.
3. Перейдите на вкладку **Общие данные**.



Откроется вкладка **Общие данные шаблона**.

Редактирование шаблона "Тест" Администратор системы 

управление конфигурациями / шаблоны конфигураций / редактирование

Общие данные | Атрибуты | Сценарии | Тест выполнения

Наименование:

Группа:

Описание:

☐ Готов к выполнению

Сохранить Отмена

Рисунок 79 Вкладка Общие данные

4. Установите флаг **Готов к выполнению**.
5. Нажмите кнопку **Сохранить**.

8.2. Задачи

Раздел **Задачи** предназначен для автоматизированного выполнения ранее созданных **шаблонов** на выбранных удаленных устройствах. В этом разделе можно настроить, какие устройства и коллекции будут участвовать в выполнении, а также определить расписание выполнения задач.

Функционал раздела **Задачи**:

- Создание и редактирование задач.
- **Выбор устройств** или **коллекций устройств**, на которых будет выполняться конфигурация.
- **Привязка шаблонов** к задачам.
- **Настройка расписания выполнения** (разовое выполнение, выполнение по времени)
- **Мониторинг выполнения задач** с отображением логов.
- **История выполнения** задач с возможностью анализа ошибок и скачивания отчетов.

8.2.1. Создание задачи конфигурации

Для создания задачи конфигурации:

1. Нажмите кнопку  в списке задач конфигурации.

 Откроется страница **Создание задачи конфигурации**.

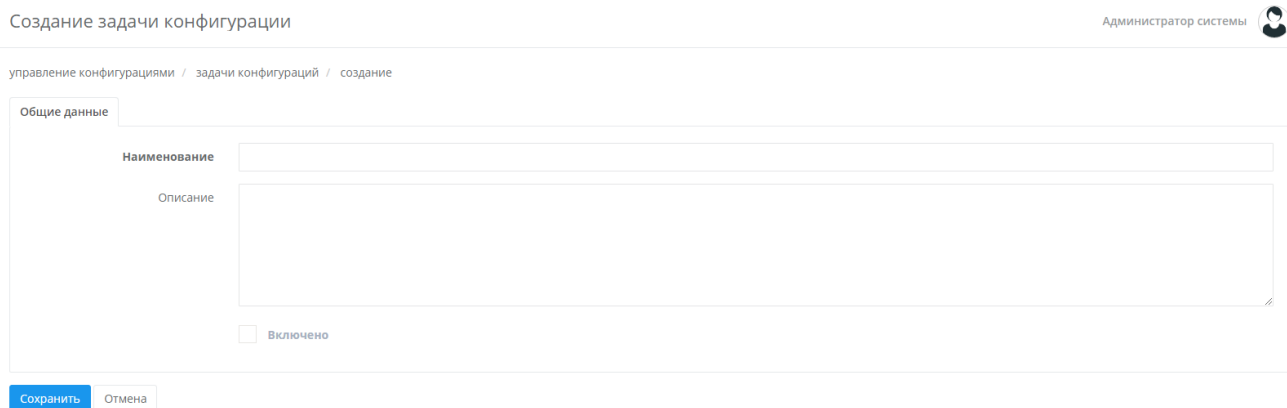


Рисунок 80 Страница Создание задачи конфигурации

2. Заполните **Наименование**.
3. При необходимости заполните строку **Описание**.
4. Нажмите кнопку **Сохранить**.

8.2.2. Расписание выполнения задач

Все задачи выполняются **по расписанию**. Необходимо задать параметры времени выполнения, после чего система автоматически запустит задачу в указанное время.

Примечание: Флаг **Включено** можно активировать только в том случае, если в задаче добавлены **хотя бы одно устройство и шаблон**. Если они отсутствуют, флаг останется недоступным для выбора.

Настройка расписания выполнения:

1. Откройте список **Задач** конфигурации.
2. Выберите задачу, нажмите кнопку  **Действия** и выберите пункт **Изменить**.

 Откроется вкладка **Общие данные** с настройкой расписания задачи.

управление конфигурациями / задачи конфигураций / редактирование

Общие данные
Устройства
Коллекции
Шаблоны
История выполнения

Наименование

Тест123

Описание

123

☐ Включено

Выберите месяц:

Ежемесячно

Пн

Вт

Ср

Чт

Пт

Сб

Вс

Время выполнения:

12

:

00

Сохранить

Отмена

Рисунок 81 Вкладка Общие сведения задачи

3. Выберите периодичность, дни недели, а также время выполнения задачи.
4. Включите задачу, установив флаг **Включено**.
5. Нажмите кнопку **Сохранить**.

8.2.3. Устройства и коллекции

На данном этапе определяется, на каких устройствах или группах устройств (коллекциях) будет выполняться задача. Можно добавить как отдельные ПК, так и целые коллекции, что упрощает управление большими группами устройств.

8.2.3.1. Добавление устройств в задачу

Добавление устройств позволяет вручную выбрать конкретные ПК, на которых будет выполняться задача, для этого:

1. Откройте список **Задач** конфигурации.
2. Выберите задачу, нажмите кнопку  **Действия** и выберите пункт **Изменить**.
3. Перейдите во вкладку **Устройства**.



Откроется вкладка **Устройства** задачи конфигурации.

управление конфигурациями / задачи конфигураций / редактирование

Общие данные
Устройства
Коллекции
Шаблоны
История выполнения

+

✖

↺

Найти устройство

⌵

ФИЛЬТР (ПОКАЗАНО 0 ИЗ 0)

☐	Статус	Идентификатор	Наименование	Сетевое имя	IP-адрес	Домен	Организация
В таблице отсутствуют данные							

Показано с 0 до 0 из 0 записей.
Отображать по 50

«

»

Рисунок 82 Вкладка Устройства задачи

4. Нажмите кнопку  в списке устройств.

 Откроется окно **Добавление устройств** в задачу.

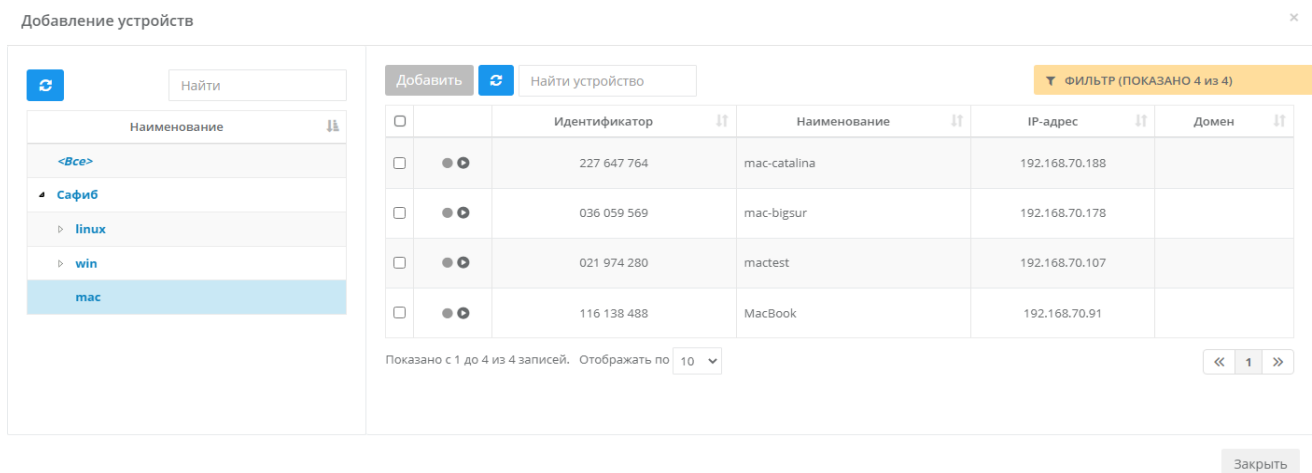


Рисунок 83 Окно Добавление устройств

Примечание: В левой части окна отображается список **организаций**. Чтобы увидеть доступные коллекции, разверните нужную организацию.

5. Выберите одно или несколько устройств и нажмите кнопку **Добавить**.

8.2.3.2. Добавление коллекций в задачу

Коллекция – это предустановленный набор устройств, позволяющий автоматизировать массовое назначение задач. В отличие от одиночного выбора ПК, коллекции могут динамически обновляться – если в коллекцию добавляются новые устройства, они автоматически попадут в задачу.

1. Откройте список **Задач** конфигурации.
2. Выберите задачу, нажмите кнопку  **Действия** и выберите пункт **Изменить**.
3. Перейдите во вкладку **Коллекции**.

 Откроется вкладка **Коллекции** задачи конфигурации.

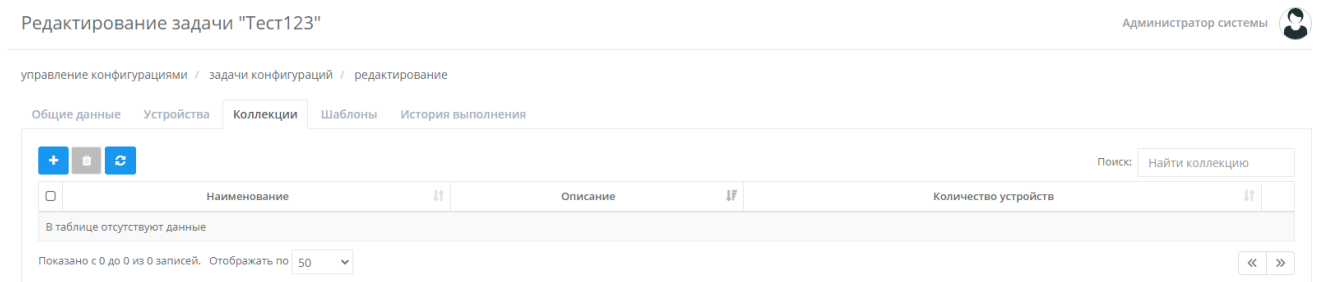


Рисунок 84 Вкладка Коллекции задачи

4. Нажмите кнопку  в списке коллекций.



Откроется окно **Добавление коллекции** в задачу.

Рисунок 85 Окно Добавление коллекции

6. Выберите одну или несколько коллекций и нажмите кнопку **Добавить**.

8.2.4. Шаблоны задачи

В этой вкладке указываются **шаблоны конфигурации**, которые будут выполняться в рамках задачи. Можно назначить несколько шаблонов, а также определить их порядок выполнения путём перемещения в столбце.

Примечание: В задаче можно использовать только шаблоны, которые имеют статус **"Готов"**.

Для добавления шаблона в задачу:

1. Откройте список **Задач** конфигурации.
2. Выберите задачу, нажмите кнопку  **Действия** и выберите пункт **Изменить**.
3. Перейдите во вкладку **Шаблоны**.



Откроется вкладка **Шаблоны** задачи конфигурации.

Рисунок 86 Вкладка Шаблоны задачи

4. Нажмите кнопку **Добавить шаблон** в списке шаблонов.

Откроется окно **Добавление шаблонов** в задачу.

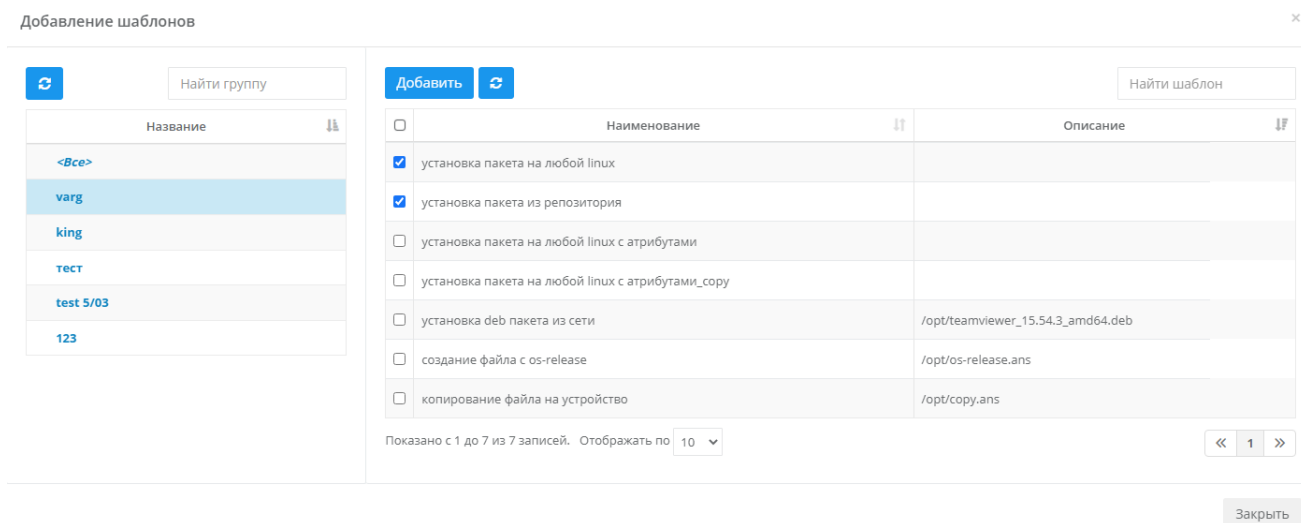


Рисунок 87 Окно Добавление шаблонов

5. Выберите один или несколько шаблонов и нажмите кнопку **Добавить**.

8.2.5. История выполнения

Во вкладке **«История выполнения»** отображается информация о запуске и результатах выполнения задачи конфигурации. Чтобы перейти во вкладку:

1. Откройте список **Задач** конфигурации.
2. Выберите задачу, нажмите  кнопку **Действия** и выберите пункт **Изменить**.
3. Перейдите во вкладку **История выполнения**.

Откроется вкладка **История выполнения** задачи конфигурации.

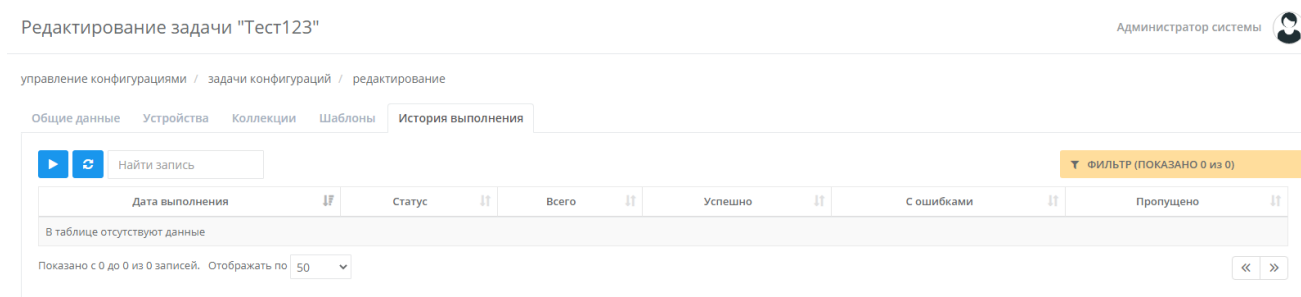


Рисунок 88 Вкладка История выполнения

На данной вкладке есть возможно вручную запустить выполнение задачи, нажав кнопку  .

После запуска задачи в таблице появятся записи с информацией о её статусе:

- **Выполнено** - задача успешно завершена.

- **Есть ошибки** – задача выполнена, но в процессе возникли ошибки.
- **В процессе** – задача выполняется в данный момент.
- **Не доступно**– задача не может быть выполнена из-за недоступности устройств или других причин.

Просмотр деталей выполнения:

1. Записи о запусках задачи на устройствах

- В таблице истории выполнения отображаются все запуски задачи на устройствах с датами выполнения.
- Для просмотра деталей необходимо кликнуть на запись с интересующим запуском.

Редактирование задачи "Unrich"

Администратор системы

управление конфигурациями / задачи конфигураций / редактирование

Общие данные

Устройства

Коллекции

Шаблоны

История выполнения

Найти устройство

Дата выполнения: 11.03.2025 11:12:25

ФИЛЬТР (ПОКАЗАНО 3 из 3)

Статус	Идентификатор	Наименование	Сетевое имя	IP-адрес	Домен	Организация
Не доступно	169 056 621	fedora	fedora	192.168.70.121	(none)	Сафиб
Не доступно	128 750 303	C405Prog06	C405Prog06	192.168.70.173	safib.ru	Сафиб
Выполнено	042 210 152	redos8	alt8sp10	192.168.70.199	TEST.LOCAL	Сафиб

Показано с 1 до 3 из 3 записей.

Отображать по 50

«

1

»

Рисунок 89 Записи запусков

2. Окно с выполненными шаблонами

- После выбора записи откроется новое окно, содержащее список выполненных шаблонов на устройстве.
- Каждый шаблон отображается со своим статусом выполнения.
- Для просмотра деталей выполнения конкретного шаблона нужно кликнуть на его название.

Устройство 042 210 152 (redos8)

Дата выполнения: 11.03.2025 11:12:25

Найти шаблон

Шаблон	Описание	Статус
создание файла с os-release	/opt/os-release.ans	Выполнено

Показано с 1 до 1 из 1 записей.

Отображать по 10

«

1

»

Заккрыть

Рисунок 90 Шаблоны устройства задачи

мойассистентпро.рф

стр. 116

3. Лог выполнения

- После выбора шаблона откроется лог выполнения с подробной информацией о процессе.
- Лог можно просмотреть в интерфейсе или скачать в виде файла для дальнейшего анализа.

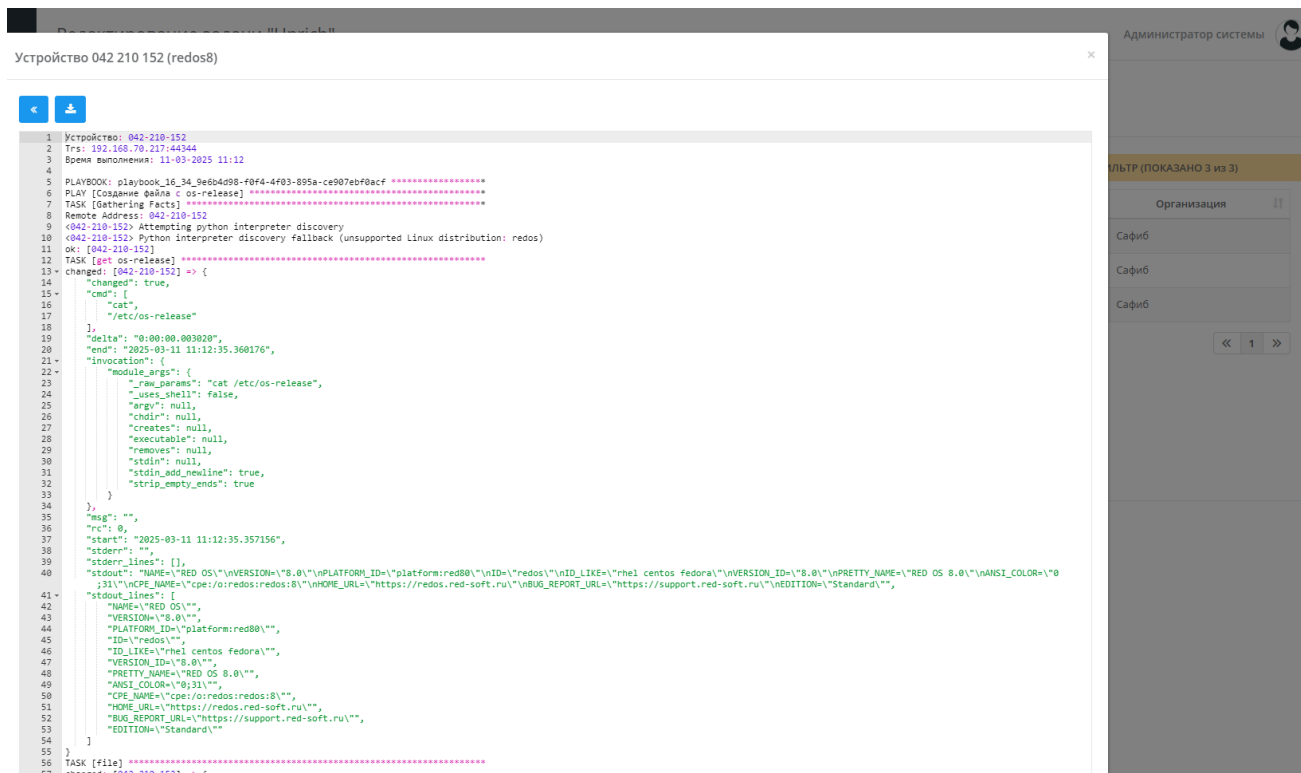


Рисунок 91 Лог выполнения шаблона