Система управления виртуальными рабочими местами «РЕД ВРМ». Терминальная редакция версия 1.0.0.

Руководство администратора.

Оглавление

1 Введение

Руководство описывает терминальную редакцию РЕД ВРМ. Отличием от стандартной редакций является возможность работы с терминальными серверами, обеспечивается функционал мультиподключения.

1.1 Назначение и состав системы

1.1.1. Система управления рабочими местами «РЕД ВРМ» (далее – РЕД ВРМ) является программным продуктом, разработанным компанией «РЕД СОФТ».

РЕД ВРМ обеспечивает централизованное управление инфраструктурой виртуальных рабочих мест (далее – ВРМ).

1.1.2. В настоящем документе описана процедура настройки РЕД ВРМ для администраторов, которые будут непосредственно использовать данную систему. Процесс установки описан в Руководстве по установке.

1.1.3. Развёрнутая система РЕД ВРМ предоставляет:

– страницу администратора для настройки подключений и создания ВРМ с использованием агентов, которые могут быть объединены в терминальные пулы;

– страницу пользователя с витриной ресурсов для доступа и подключения к опубликованным ВРМ.

1.1.4. Для аутентификации и закрепления ВРМ за пользователем используется либо встроенная база данных, либо существующая служба каталогов.

1.1.5. РЕД ВРМ имеет модульную структуру и включает в себя следующие компоненты:

– «Брокер» – основной компонент, отвечающий за централизованное управление и доступ к системе РЕД ВРМ;

– «Агент» – серверное ПО для управления и организации доступа к ВРМ;

– «Клиент» – клиентское ПО для доступа и подключения к ВРМ;

– «База Данных» – используется для хранения настроек системы РЕД BPM, автоматически устанавливается при развёртывании брокера.

Дополнительно для своей работы РЕД BPM может использовать LDAP-аутентификаторы для интеграции со службами каталога РЕД АДМ и Active Directory, а также поставщиков для подключения к кластерам платформы РЕД Виртуализация – при использовании динамических пулов для управления их жизненным циклом.

1.2 Двухфакторная аутентификация по смарткартам в РЕД BPM.

1.2.1 Предварительные требования:

1.2.1.1. Контроллер домена на базе РЕД АДМ либо Active Directory;
1.2.1.2. Службы сертификатов Active Directory, которые используются для выдачи пользовательских сертификатов;
1.2.1.3. Для аутентификации по смарт-карте необходимы установленные драйвера соответствующих смарт-карт на Клиенте и Агенте РЕД BPM;
1.2.1.4. Для аутентификации на рабочем месте Клиент и Агент РЕД BPM должны быть введены в домен, где доступны и развернуты Службы сертификатов;
1.2.1.5. Наличие корневого сертификата центра сертификации в списке доверенных на стороне Клиента и Агента РЕД BPM, при входе в домен выполняется автоматически;
1.2.1.6. Наличие пользовательского сертификата на смарт-карте для входа в РЕД BPM.

1.2.2 Требования к настройке Брокера РЕД BPM:

1.2.2.1. На портале Администратора в разделе “Аутентификаторы” необходимо выбрать контроллер домена, который будет использоваться для аутентификации по смарт-картам;
1.2.2.2. На вкладке «Редактирование» активировать пункт «Смарт-карты».

1.2.3 Требования к настройке Клиента РЕД BPM:

1.2.3.1. Для аутентификации по смарт-карте на Web-портале необходимы установленные плагины для браузера соответствующих смарт-карт;
1.2.3.2. На Клиенте РЕД BPM пользователю необходимо выбрать Аутентификатор, который настроен для аутентификации по смарт-картам;
1.2.3.3. Нажать кнопку «Войти другим способом»;
1.2.3.4. Во всплывающем окне ввести пин-код от смарт-карты и выбрать пользовательксий сертификат для входа в РЕД BPM;
1.2.3.5. Для аутентификации по смарт-карте на Агенте РЕД BPM, при подключении к BPM, выбрать необходимое устройство в разделе «Смарт-карты» для проброса в сессию пользователя.

Важно! Поддерживаемые смарт-карты: Рутокен ЭЦП 3.0 или USB-токен JaCarta PKI.

■

1.3 Вход в систему

1.3.1. Для входа в систему в адресной строке браузера введите IP-адрес брокера. Откроется окно авторизации (рисунок 1).

1.3.2. Вы можете зайти, введя логин, пароль и аутентификатор. При первом входе введите логин администратора и пароль, заданные при установке брокера (по умолчанию – `login` и `password`), аутентификатор – `DataBase`.

Нажмите кнопку «Войти», и при правильности введённых данных откроется веб-интерфейс (при первом входе нужно будет принять лицензионное соглашение перед продолжением работы).

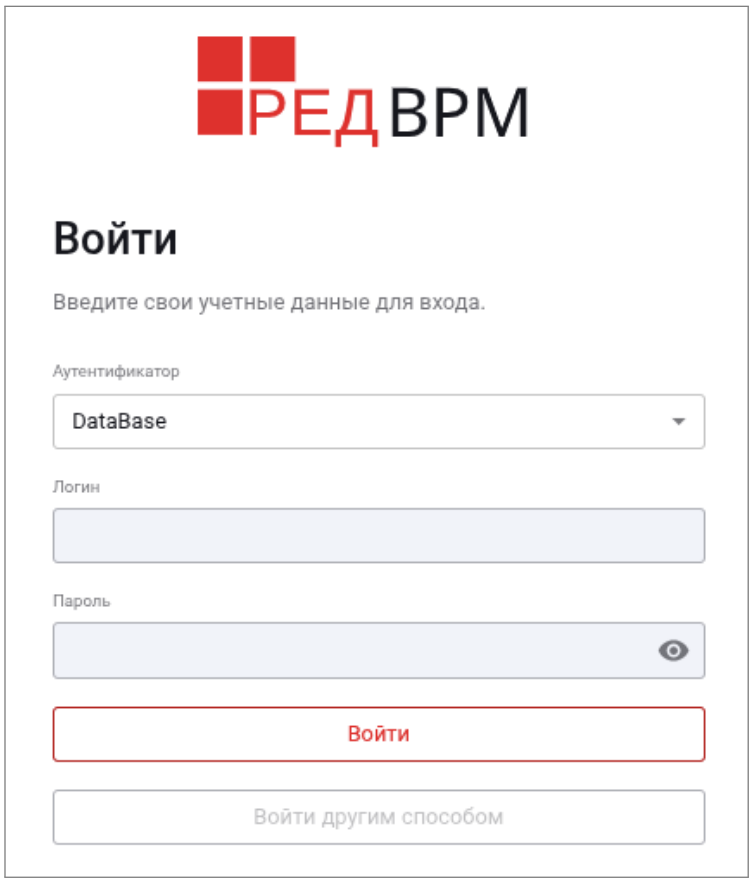

Рисунок 1 – Авторизация через логин/пароль

1.3.3. Кнопка «Войти другим способом» переключает между авторизацией через логин/пароль и смарт-картой. Для авторизации укажите аутентификатор и сертификат (рисунок 2).

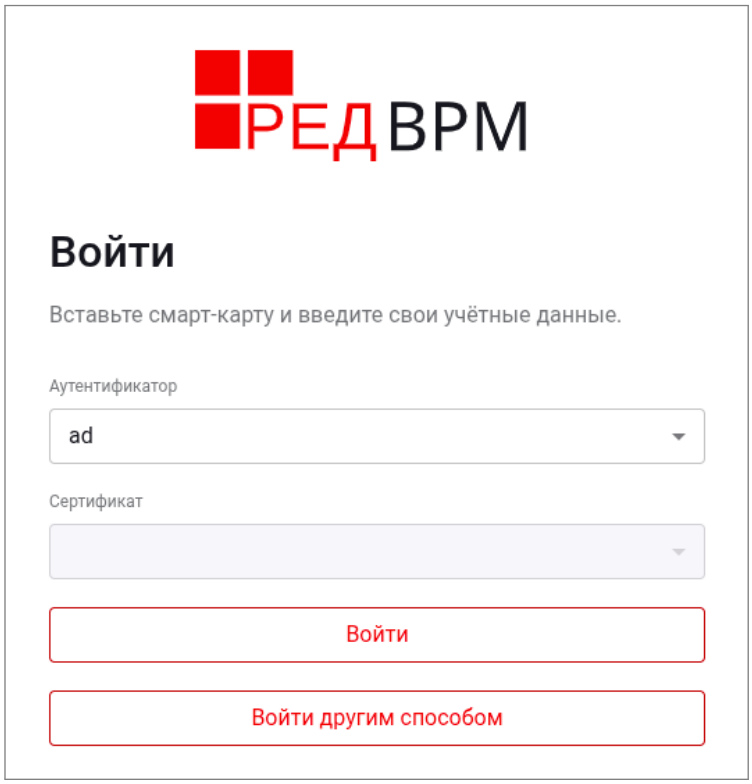

Рисунок 2 – Авторизация через смарт-карту

Способы аутентификации устанавливаются в разделе «Аутентификаторы» (см. 2.1.3 «Аутентификаторы типов «РЕД АДМ» и «Active Directory»»).

1.4 Страница администратора и страница пользователя

1.4.1. При входе в систему, в зависимости от роли авторизующегося пользователя системы («Администратор» или «Пользователь»), откроется либо страница администратора, либо витрина ресурсов (страница пользователя).

1.4.2. Страница администратора (рисунок 3) позволяет администрировать BPM и сопутствующую инфраструктуру.

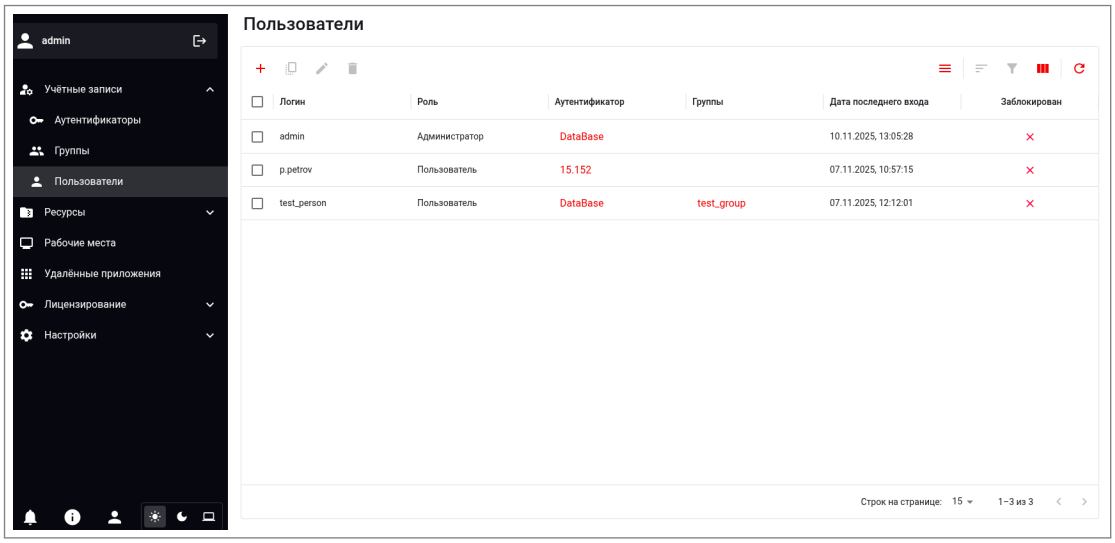

Рисунок 3 – Страница администратора

В главном меню панели администратора, расположенном слева, отображены следующие разделы (вкладки) и кнопки:

- «Учётные записи»:
  - «Аутентификаторы»,
  - «Группы»,
  - «Пользователи»;
- «Ресурсы»:
  - «Терминальные агенты»,
  - «Терминальные пулы»,
  - «Контроллеры доменов»;
- «Рабочие места»;
- «Удаленные приложения»;
- «Лицензирование»:
  - «Лицензии»,
  - «Сессии»;
- «Настройки»:
  - «Разрешения»,
  - «Группы доступа»;
- «Уведомления»;
- «Информация о программе»;
- «Страница пользователя»;
- «Смена темы».

1.4.3. Кнопки, расположенные в левом нижнем углу интерфейса осуществляют (слева направо): вывод недавних уведомлений (а), вывод информации о программе (б), переход на витрину ресурсов (в), набор кнопок смены темы (г).

Чтобы выбрать тему оформления (тёмную, светлую или системную), нажмите на соответствующую кнопку (рисунок 4).

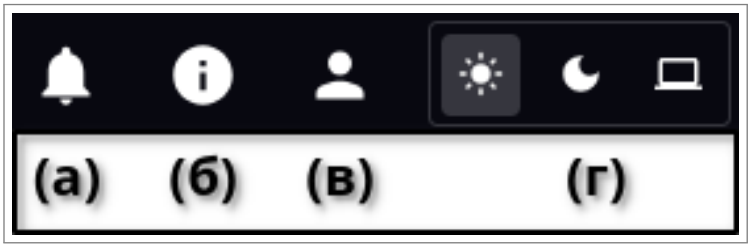

Рисунок 4 – Нижний интерфейс

1.4.4. В верхней части таблицы с данными присутствует ряд кнопок. Красным цветом подсвечивается кнопка в активном состоянии, серым - в неактивном. В разных разделах и подразделах могут присутствовать не все кнопки.

Слева расположены:

– «Создать» – создает новую сущность;

– «Копировать» – копирует уже имеющуюся сущность;

– «Редактировать» – редактирует имеющуюся сущность;

– «Подробнее» – открывает данные сущности (двойной клик по строке с данными делает то же самое);

– «Удалить» – удаляет сущность.

Рисунок 5 – Кнопки слева

Слева расположены:

– «Меню» – вкладка дублирует кнопки, расположенные слева, и может содержать дополнительный функционал;

– «Сортировать» – сортирует сущности в выбранном порядке;

– «Фильтровать» – позволяет отфильтровать сущности;

– «Столбцы» – позволяет настроить список столбцов в таблице;

– «Обновить» – обновляет данные.

Рисунок 6 – Кнопки справа

1.4.5. Страница пользователя даёт доступ к «Витрине ресурсов» со списком доступных рабочих столов и приложений. Выбор «рабочего стола» предоставляет пользователю доступ к виртуальной машине. Выбор из списка «приложений» позволяет запустить в отдельном окне только приложение, необходимое для работы. (рисунок 8). Переключение между кнопками «рабочие столы» и «приложение» отображает только ресурсы выбранной категории.

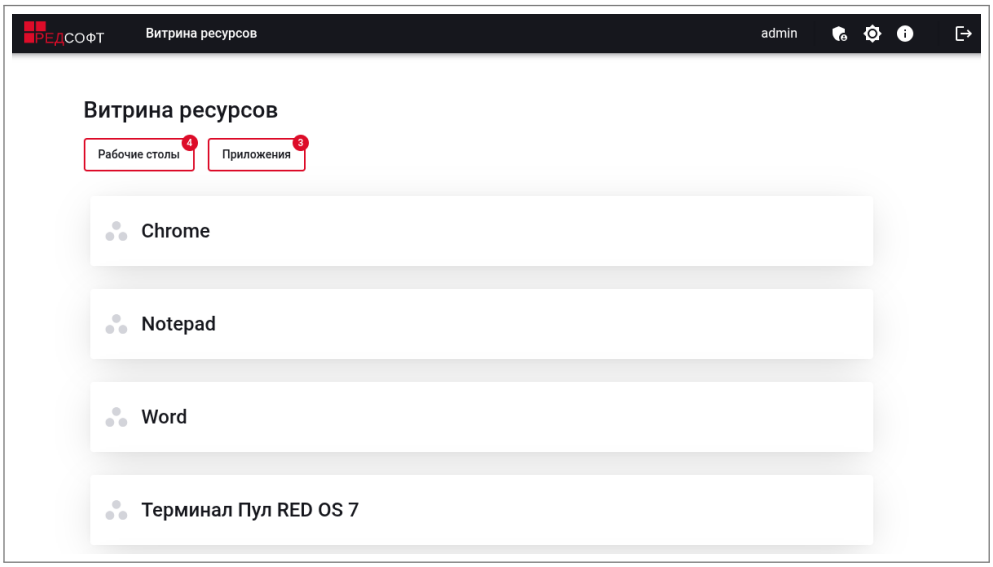

Рисунок 7 – Витрина ресурсов)

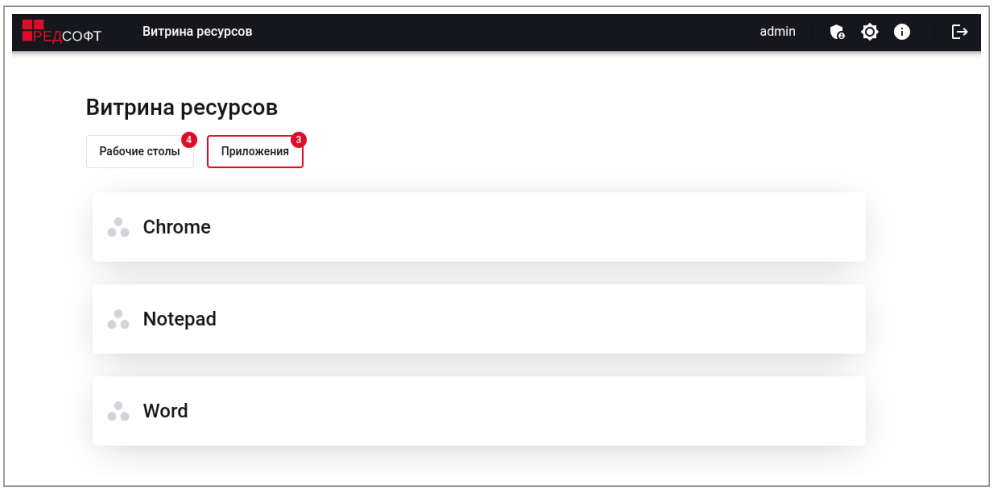

Рисунок 8 – Выбор списка ресурсов

Обычный пользователь (пользователь системы, которому присвоена роль «Пользователь») при входе в систему попадает именно на витрину доступных для него ресурсов и не имеет доступа к панели администратора.

Администратор (пользователь системы, которому присвоена роль «Администратор») при входе в систему попадает на страницу администратора, и может перейти на витрину доступных для него ресурсов, нажав на кнопку «Страница пользователя» в левом нижнем углу (рисунок 4). Для выхода обратно на страницу администратора нужно нажать на самую левую кнопку в правом верхнем углу (при наведении на неё выводится надпись «Страница администратора») (рисунок 9).

Рисунок 9 – Кнопки, расположенные в правом верхнем углу интерфейса страницы пользователя (перечисление слева направо): переход на страницу администратора (только для пользователя, являющегося администратором системы) (а), кнопка смены темы (б), вывод информации о программном обеспечении (в), выход из системы (г).

1.5 Лицензии

1.5.1. Для работы с лицензиями предназначен раздел «Лицензирование», подраздел «Лицензии» (рисунок 10). Здесь перечислены имеющиеся лицензионные ключи и отображены их свойства.

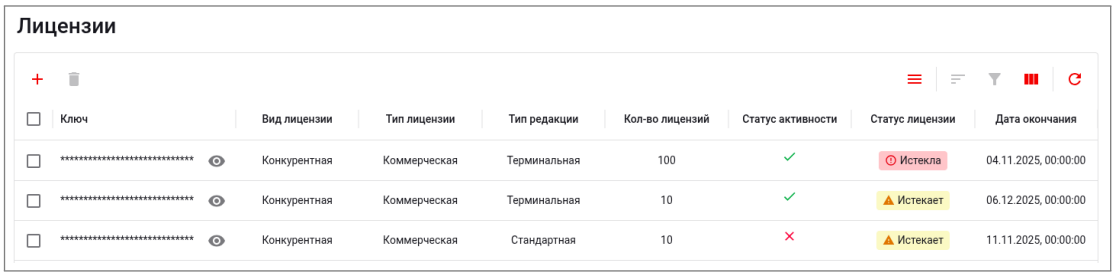

Рисунок 10 – Лицензионные ключи

Для добавления новой лицензии нажмите кнопку «Создать». В открывшемся модальном окне введите лицензионный ключ и нажмите кнопку «Создать» (рисунок 12).

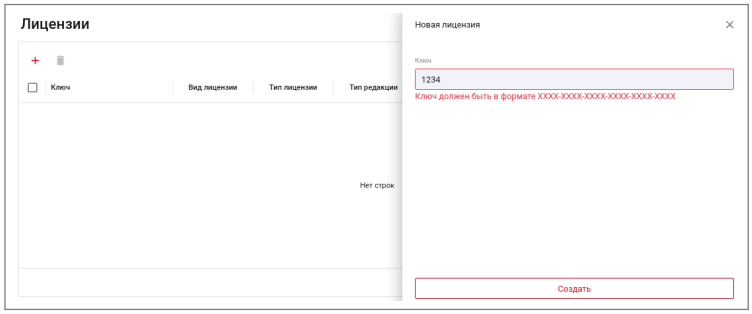

Рисунок 11 – Добавление новой лицензии

Важно! После добавления лицензии её необходимо активировать, выбрав нужную модель работы. Лицензия может быть:

– по виду – конкурентная или именная;

– по типу – коммерческая, тестовая или учебная.

> **Важно!** При активации лицензия должна быть выдана именно на терминальную редакцию.
>
> ■

В системе может использоваться одновременно только одна модель лицензирования. Пример: если уже активировали конкурентные коммерческие лицензии, то конкурентные учебные или именно коммерческие становятся недоступны.

При наведении на статус в столбце «статус лицензии» теперь отображается оставшееся время.

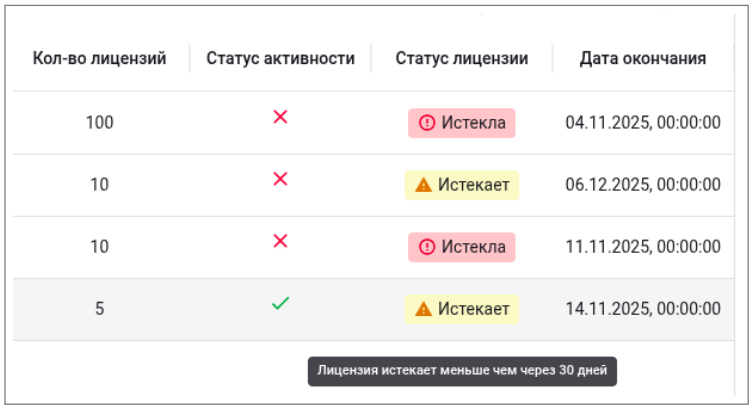

Рисунок 12 – Добавление новой лицензии

1.5.2. В разделе «Сессии», подразделе «Лицензирование», приводится информация обо всех активных сессиях пользователей, подключённых к BPM (рисунок 13).

Рисунок 13 – Сессии

2 Работа с учётными записями

Раздел «Учётные записи» включает в себя следующие разделы (вкладки):
– «Аутентификаторы»;
– «Группы»;
– «Пользователи».

2.1 Аутентификаторы

2.1.1 Раздел «Аутентификаторы»

2.1.1.1. При переходе в раздел «Аутентификаторы» открывается список имеющихся аутентификаторов (рисунок 14).

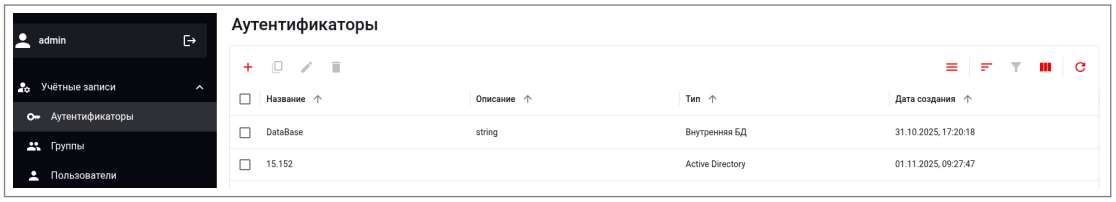

Рисунок 14 – Раздел «Аутентификаторы»

2.1.1.2. Для того чтобы создать новый аутентификатор, нажмите кнопку «Создать». В открывшемся окне выберите тип аутентификатора и затем введите параметры. Есть три возможных типа аутентификаторов (рисунок 15): «Внутренняя БД», «Active Directory», «РЕД АДМ» .

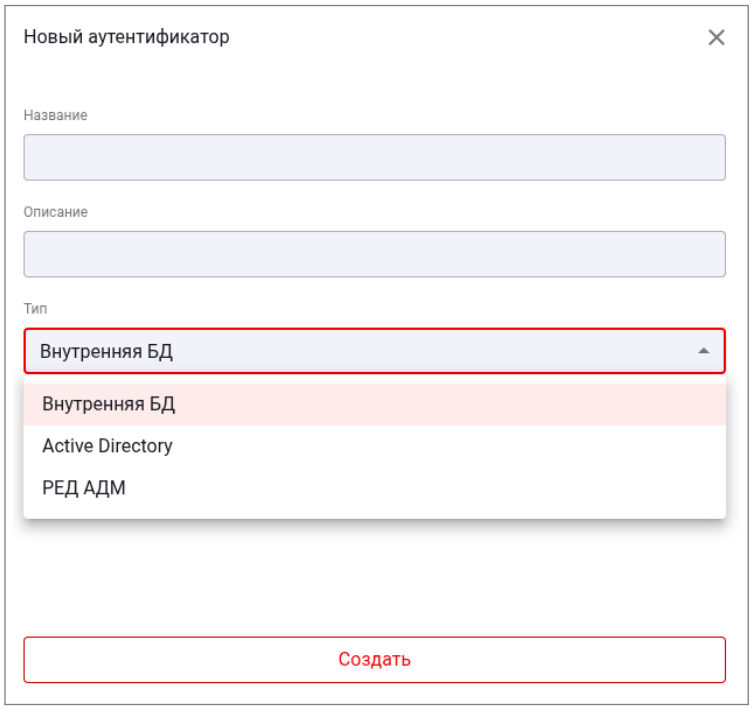

Рисунок 15 – Выбор типа создаваемого аутентификатора

2.1.2 Внутренняя база данных

2.1.2.1. Для создания аутентификатора типа «Внутренняя БД» достаточно ввести имя в поле «Название». Введя название и, при необходимости, описание, нажмите расположенную в этом же окне внизу кнопку «Создать».

2.1.2.2. Созданный аутентификатор появится в списке аутентификаторов. С ним можно будет выполнять следующие операции (рисунок 16) – активными станут соответствующие кнопки:

– «Копировать»;
– «Редактировать»;
– «Удалить»;
– «Меню» («Проверить соединение» заблокировано);
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

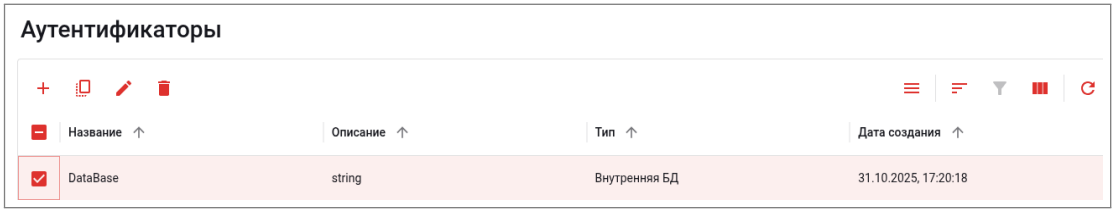

Рисунок 16 – Выбор аутентификатора типа «Внутренняя БД» для работы с ним

2.1.3 Аутентификаторы типов «РЕД АДМ» и «Active Directory»

РЕД BPM поддерживает добавление аутентификаторов для служб каталогов на основе РЕД АДМ и Microsoft Active Directory. Для добавления сначала требуется создать контроллер домена (см. раздел 3.3.3 «Контроллеры доменов») Продемонстрируем работу с аутентификаторами этих типов на примере аутентификатора типа «РЕД АДМ».

2.1.3.1. При создании аутентификатора «РЕД АДМ» для подключения к службе каталогов нужно указать следующие параметры (рисунок 17):

– название нового аутентификатора;
– описание (опционально);
– тип;
– выбрать контроллер домена из списка (не применяется при типе "Внутренняя БД");
– зону видимости (опционально).

Выбрать способ аутентификации:

– Смарт-карта;
– Логин/Пароль.

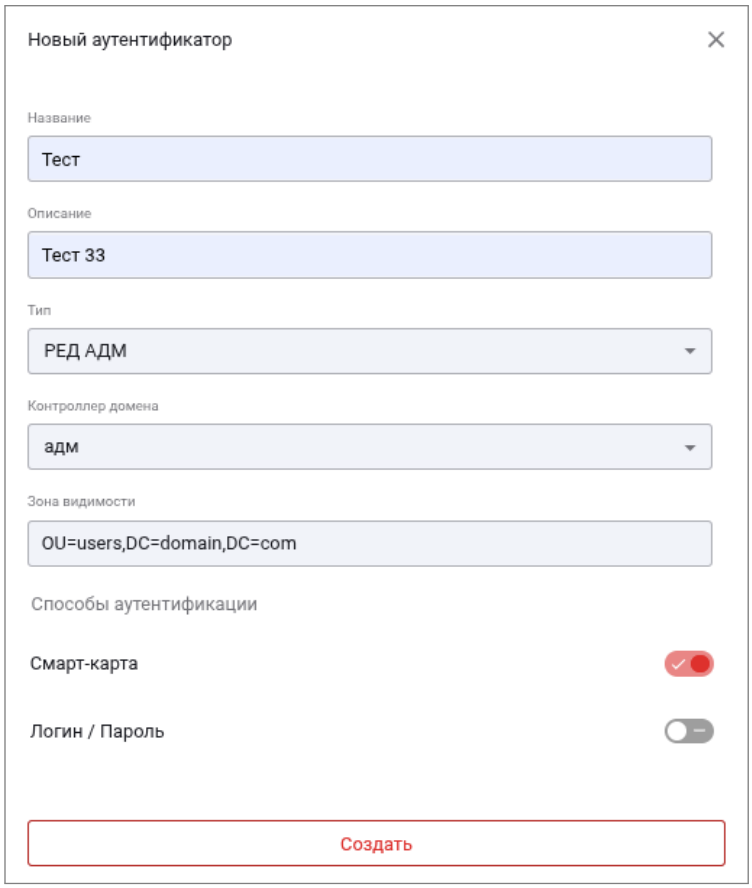

Рисунок 17 – Основные параметры создаваемого аутентификатора типа «РЕД АДМ»

Закончив ввод значений параметров, нажмите кнопку «Создать», расположенную в этом же окне в самом низу .

2.1.3.2. После создания аутентификатора он появится в списке аутентификаторов. Аналогично аутентификатору типа «Внутренняя БД», для выделенного аутентификатора можно (рисунок 18):

– «Копировать»;
– «Редактировать»;
– «Удалить»;
– «Меню» («Проверить соединение» активно);
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

Также для выделенного аутентификатора типов «Active Directory» и «РЕД АДМ» с помощью кнопки «Проверить соединение» можно проверить соединение и корректность заданных параметров (Расположена во вкладке «Меню»).

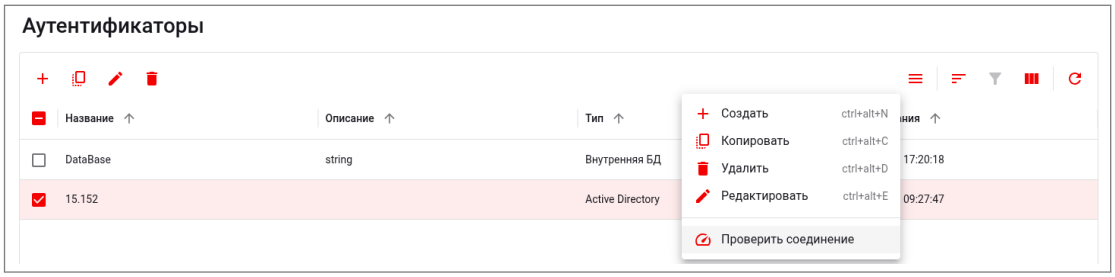

Рисунок 18 – Выбор аутентификатора типа «РЕД АДМ» для работы с ним

2.2 Группы

2.2.1. Для работы с группами предназначен подраздел «Группы», расположенный в разделе «Учётные записи» (рисунок 19).

РЕД BPM использует следующие типы групп:

– «Пользовательские группы». Расположены в разделе «Учётные записи» и могут содержать учётные записи из разных аутентификаторов. Далее под группами подразумеваются пользовательские группы, если не указано иное;

– «Группы доступа». Расположены в разделе «Настройки» и включают набор разрешений, пользователей, пользовательские группы для публикации BPM. При использовании нескольких групп доступа порядок их применения определяется значением поля «Приоритет». Чем ниже значение, тем выше приоритет.

Рисунок 19 – Раздел «Группы»

2.2.2. Для добавления новой группы нажмите кнопку «Создать». В открывшемся модальном окне введите имя новой группы и нажмите кнопку «Создать», расположенную в самом низу модального окна (рисунок 20).

2.2.3. Созданная группа появится в списке групп. С ней можно выполнить операции: (рисунок 21):

– «Копировать»;
– «Редактировать»;
– «Подробнее» (открывает список пользователей в группе (рисунок 22));
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

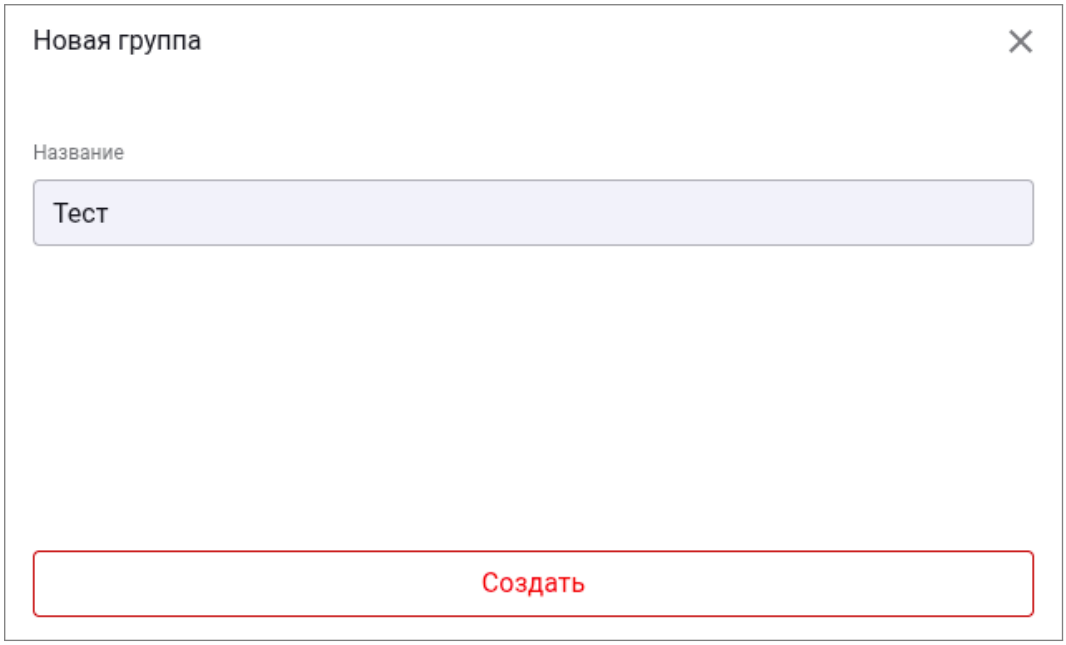

Рисунок 20 – Добавление группы

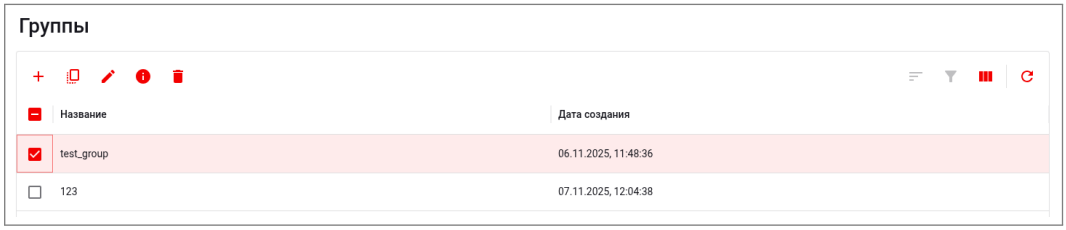

Рисунок 21 – Доступные действия с выбранной группой

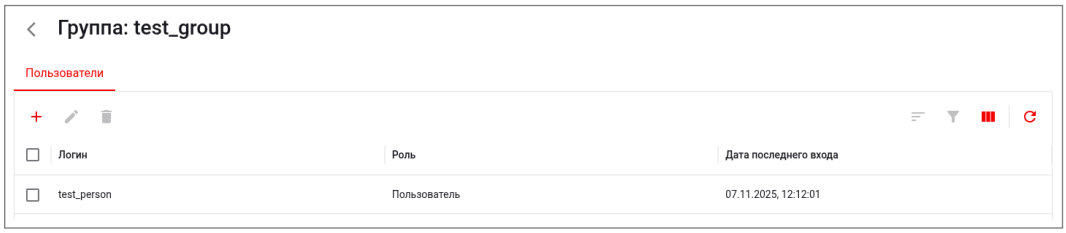

Рисунок 22 – Пользователи выбранной группы

2.3 Пользователи

2.3.1. Для работы с пользователями предназначен подраздел «Пользователи», расположенный в разделе «Учётные записи» (рисунок 23).

2.3.2. Для аутентификаторов типа «Внутренняя БД» учётные записи должны быть созданы в явном виде на странице администратора.

Для аутентификаторов типа «РЕД АДМ» и «Active Directory» учётные записи пользователей создаются автоматически после первой успешной аутентификации, а также могут быть добавлены вручную, например, когда пользователю необходимо назначить роль «Администратор» либо добавить его в пользовательскую группу.

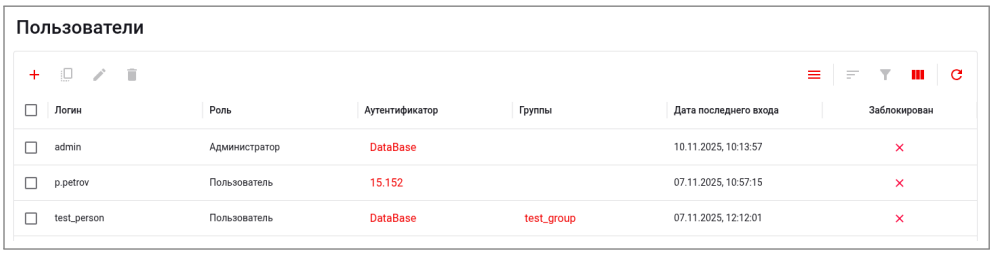

Рисунок 23 – Раздел «Пользователи»

2.3.3. Для добавления пользователя нажмите кнопку «Создать», и в открывшемся модальном окне введите параметры нового пользователя (рисунок 24):

– имеющийся аутентификатор (любого типа – «Внутренняя БД», «РЕД АДМ» или «Active Directory»);

– логин пользователя;

– пароль пользователя – для аутентификатора типа «Внутренняя БД»;

– выбрать роль – «Пользователь» (по умолчанию) или «Администратор».

2.3.4. Созданный пользователь появится в списке пользователей. Можно выполнить операции:

– «Копировать»;

– «Редактировать»;

– «Удалить»;

– «Меню» («Заблокировать» активна);

– «Сортировать»;

– «Фильтровать»;

– «Столбцы»;

– «Обновить».

Вхождение пользователя в группы можно отредактировать, перейдя в раздел «Группы» и отредактировав состав нужных групп (см. подраздел 2.2).

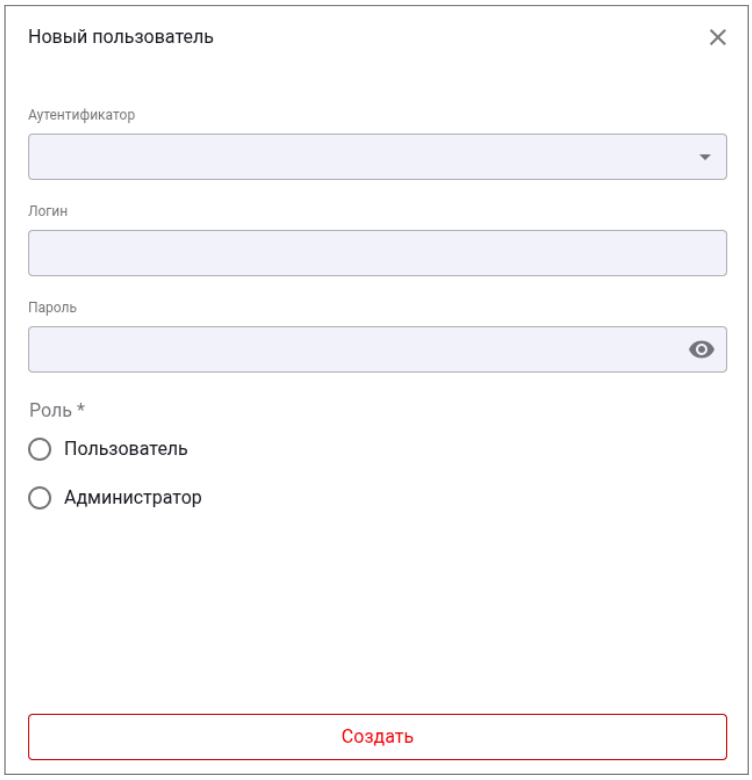

Рисунок 24 – Создание нового пользователя

3 Работа с ресурсами

3.1 Терминальные агенты

3.1.1. Агент используется для создания BPM, к которому пользователи подключаются по протоколу удалённого доступа. Агент устанавливается на физической либо виртуальной машине. Подраздел «Агенты» расположен в разделе «Ресурсы» (рисунок 25).

Рисунок 25 – Раздел «Терминальные агенты»

3.1.2. Для создания нового агента нажмите кнопку «Создать». В открывшемся модальном окне укажите IP-адрес машины, на которой развёрнут агент, и порт (по умолчанию – 8010). Нажмите кнопку «Создать» (рисунок 26).

Созданный агент появится в списке. Если после добавления агента, у него отображаются только IP-адрес и порт, валидация проведена неудачно.

Важно! Валидация агента возможна только на одном брокере. При необходимости перевалидировать агент с одного брокера на другой, нужен перезапуск сервера РЕД BPM и службу агента.

Возможные причины:
– машина выключена;
– не доступен IP-адрес;

– закрыт порт 8010.

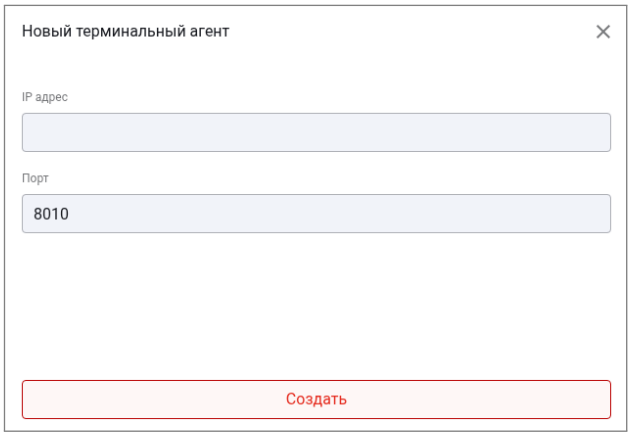

Рисунок 26 – Добавление нового агента

Выделив агента нажатием, с ним можно будет выполнять следующие операции :

– «Редактировать» (отредактировать ip адрес нет возможности. Для изменения, удалите и создайте заново агента. При смене порта, новый порт должен быть открыт);
– «Подробнее» (открывает данные о ресурсе);
– «Удалить»;
– «Меню» («Проверить соединение» активно);
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

3.1.3. Двойной клик на агента или нажатие кнопки «подробнее» открывает данные о ресурсах агента (рисунок 27).

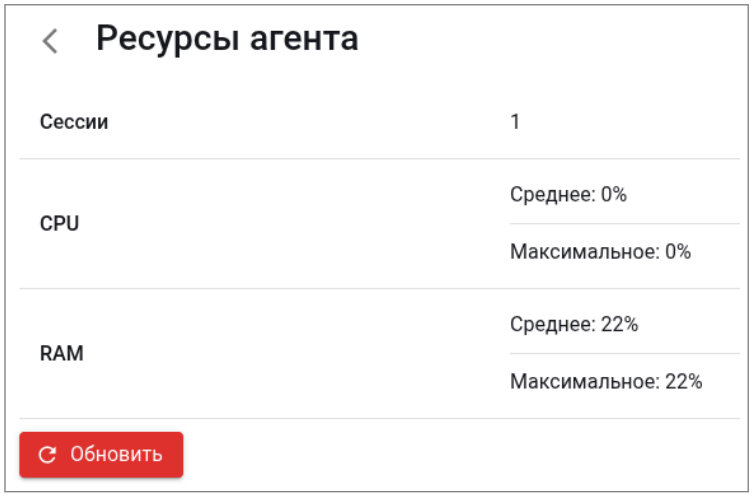

Рисунок 27 – Ресурсы агента

3.2 Терминальные пулы

Предполагается, что в терминальных пулах используются консистентные серверы, следовательно, настроены они одинаково.

3.2.1 Типы пулов

Подраздел «Пулы» расположен в разделе «Ресурсы» (рисунок 28).

Рисунок 28 – Раздел «Пулы»

3.2.2 Создание пула

3.2.2.1. Для создания нового пула:
– нажмите кнопку «Создать» в разделе «Пулы»;
– в открывшемся модальном окне введите название пула (рисунок 29)
– укажите режим балансировки (рисунок 30);
– нажмите кнопку «Создать».
Созданный пул появится в списке пулов.

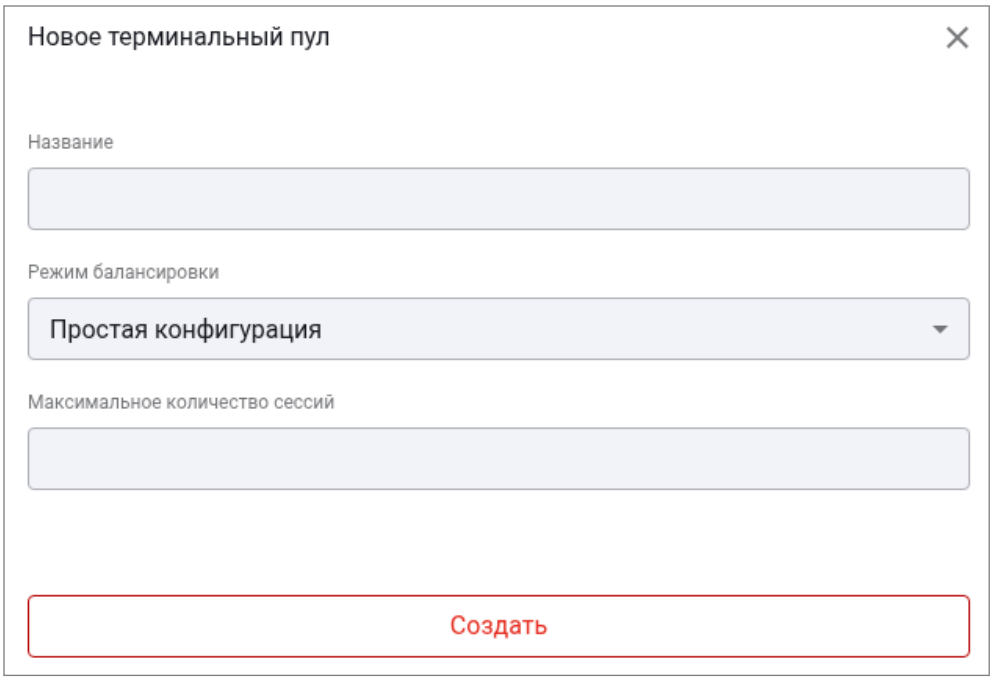

Рисунок 29 – Создание терминального пула

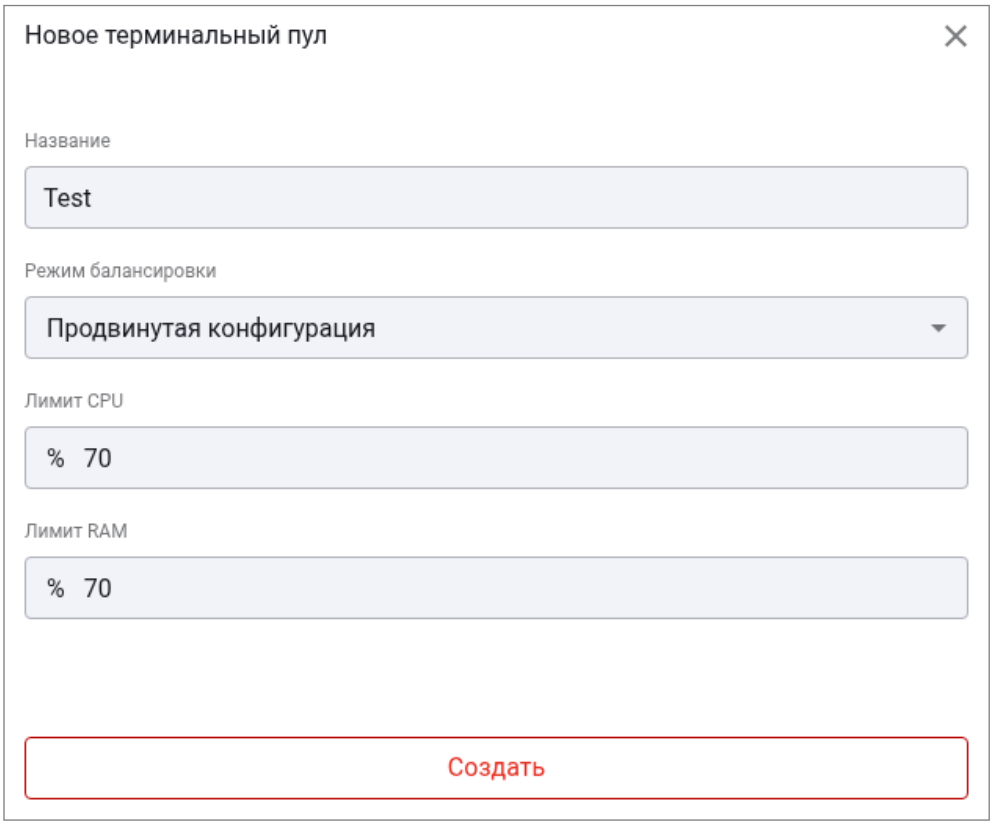

Рисунок 30 – Продвинутая конфигурация

Режим балансировки предоставляет простую либо продвинутую конфигурацию. При простой конфигурации устанавливается только максимальное количество сессий. В случае превышения установленного количества нагрузка направляется на менее загруженный сервер. При продвинутой конфигурации устанавливается процентная загруженность CPU и RAM. При превышении одного из показателей нагрузка, направляется на другой сервер.

3.2.2.2. Выделив имеющийся пул в списке, с ним можно будет выполнять следующие операции:

– «Редактировать»;
– «Подробнее» (открывает список терминальных агентов, входящих в пул);
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

Для добавления агентов в терминальный пул откройте нужный пул и нажмите на кнопку «Добавить». В открывшемся модальном окне в выпадающем списке выберите нужных терминальных агентов и нажмите кнопку «Добавить» (рисунок 31).

Важно! После добавления терминальных агентов в терминальный пул, они остаются в нем и перестают отображаться во вкладке «Терминальные агенты». ■

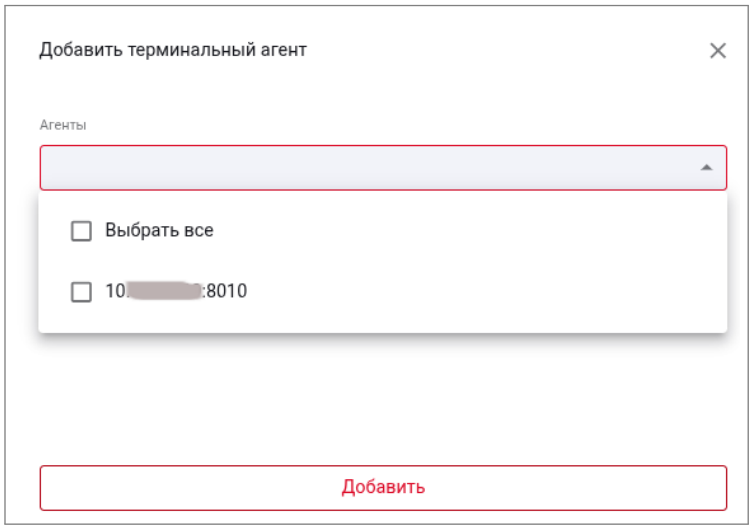

Рисунок 31 – Выбор агентов для добавления в пул

При прикреплении терминального агента мы не управляем лимитами сессии, это находится в ведении администратора.

Важно! В терминальной редакции присутствует балансировка сервера. Сервер для пользователя подбирается наименее загруженный. Чтобы была балансировка в рамках терминального агента, следует создать пул на основе единственного агента — и прописать лимиты. ■

3.3 Контроллеры доменов

Подраздел «Контроллеры доменов» расположен в разделе «Ресурсы» (рисунок 32). Контроллер домена представляет собой сервер, обеспечивающий централизованное управление сетевыми ресурсами в рамках одного домена (группы сетей или хостов с общей политикой безопасности).

Рисунок 32 – Раздел «Контроллеры доменов»

3.3.1 Создание контроллера

3.3.1.1. Нажмите кнопку «Создать». В открывшемся модальном окне (рисунок 33) задайте значение параметров:

– название нового контроллера;
– его тип;
– укажите основной IP-адрес;
– укажите порт сервера;
– укажите логин и пароль администратора;

– укажите название домена;
– нажмите кнопку «Создать».

В отдельной секции «Расширенные настройки» можно установить (рисунок 34):
– использование SSL протокола;
– время ожидания ответа от сервера LDAP («Таймаут»);
– пользовательский класс;
– ID атрибут;
– атрибут пользователя;
– атрибут группы;
– альтернативный класс.

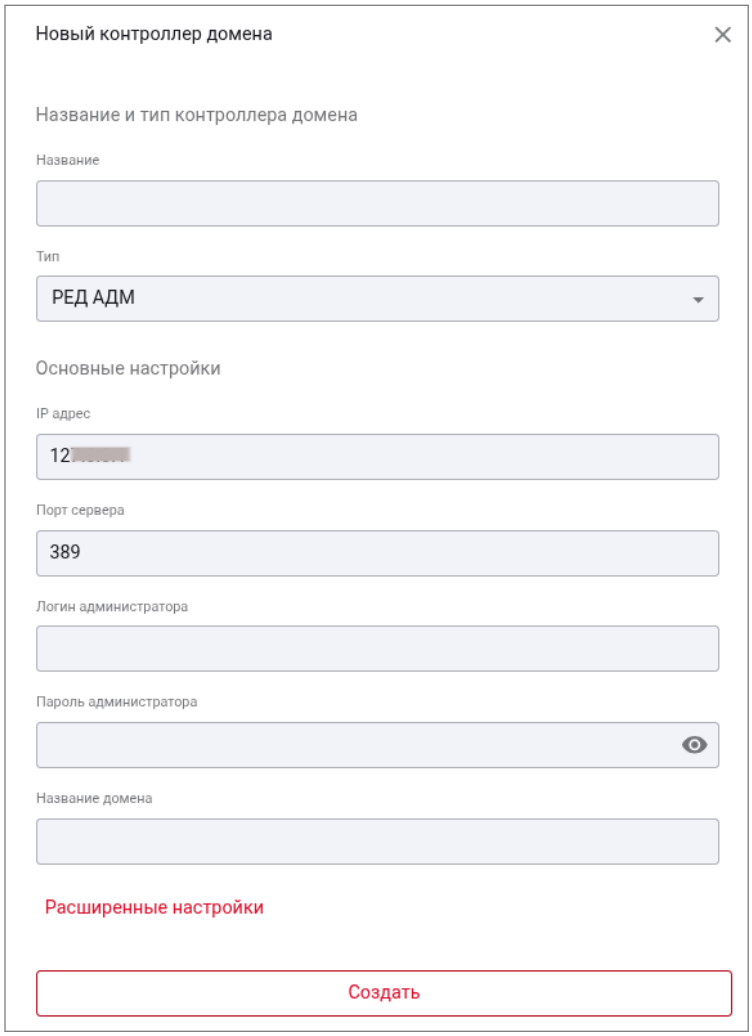

Рисунок 33 – Модальное окно при создании контроллера доменов

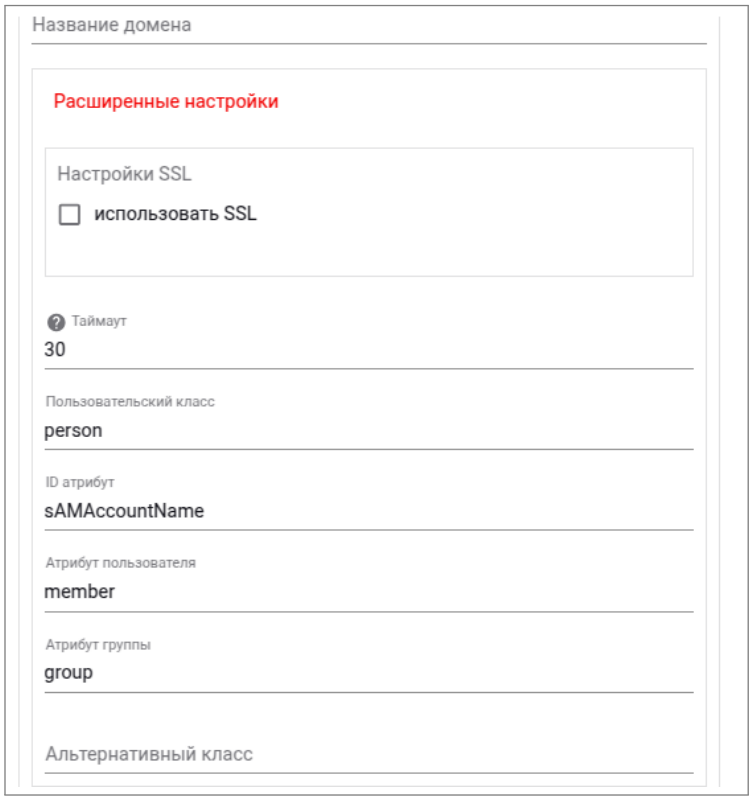

Рисунок 34 – Расширенные настройки при создании контроллера доменов>

3.3.1.2. Для редактирования контроллера
Выделив имеющийся контроллер в списке, можно выполнить операции:
– «Редактировать»;
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

Рисунок 35 – Раздел «Редактирование контроллера доменов»

4 Рабочие места

4.1 Управление виртуальными рабочими местами

Управление виртуальными рабочими местами осуществляется в разделе «Рабочие места» (рисунок 36).

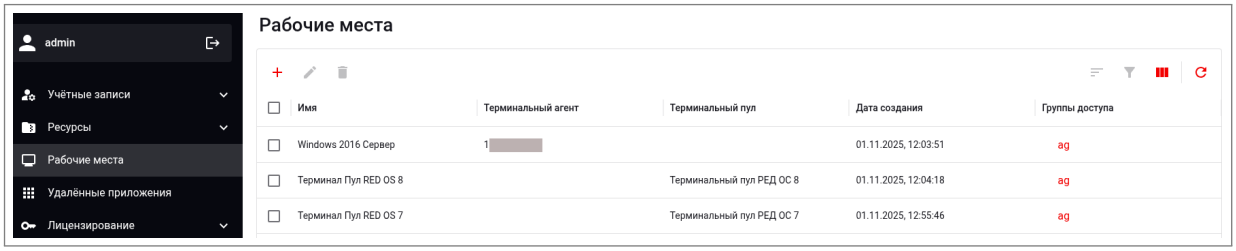

Рисунок 36 – Раздел «Рабочие места»

4.1.1 Создание нового рабочего места

Нажмите кнопку «Создать» (рисунок 37). В открывшемся модальном окне:

– укажите имя рабочего места (обязательный параметр);

– в выпадающем меню «Группы доступа» – выбрать группы, которые определяют пользователей, имеющих доступ к данному рабочему месту;

– в выпадающем меню «Тип ресурса» – выбрать тип;

– в следующем выпадающем окне выбираете из доступных ресурсов данного типа;

Нажмите кнопку «Создать», расположенную в самом низу этого окна.

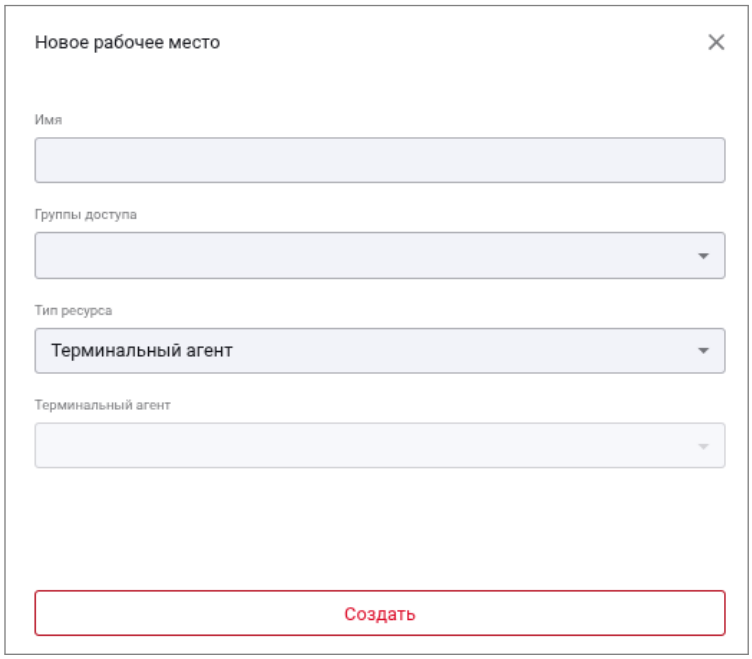

Рисунок 37 – Создание нового рабочего места

После создания рабочего места оно появится в списке. Выделив его, можно выполнить следующие операции:

– «Редактировать»;
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

5 Удаленные приложения

5.1 Создание удаленного приложения

Управление приложениями осуществляется в разделе «Удалённые приложения» (рисунок 38).

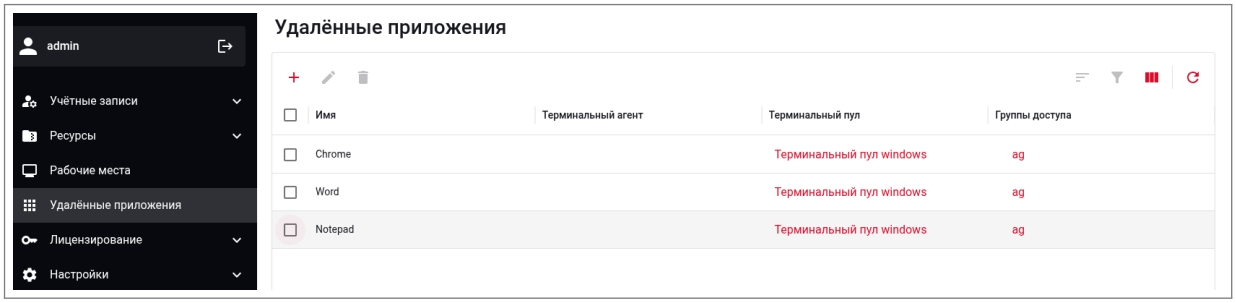

Рисунок 38 – Раздел «Удаленные приложения»

5.1.1 Создание нового удаленного приложения

Нажмите кнопку «Создать» (рисунок 39) и в открывшемся модальном окне:

– укажите имя (обязательный параметр);

– в выпадающем меню «Группы доступа» – выбрать группы доступа, которые определят пользователей, имеющих доступ к данному приложению;

– в выпадающем меню «Тип ресурса» – выбрать тип;

– в следующем выпадающем окне выбираете из доступных ресурсов данного типа;

– укажите «Команду для запуска» (обязательный параметр). Это команда для запуска на самом конечном терминальном сервере, либо путь до исполняемого файла например;

Нажмите кнопку «Создать», расположенную в самом низу этого окна.

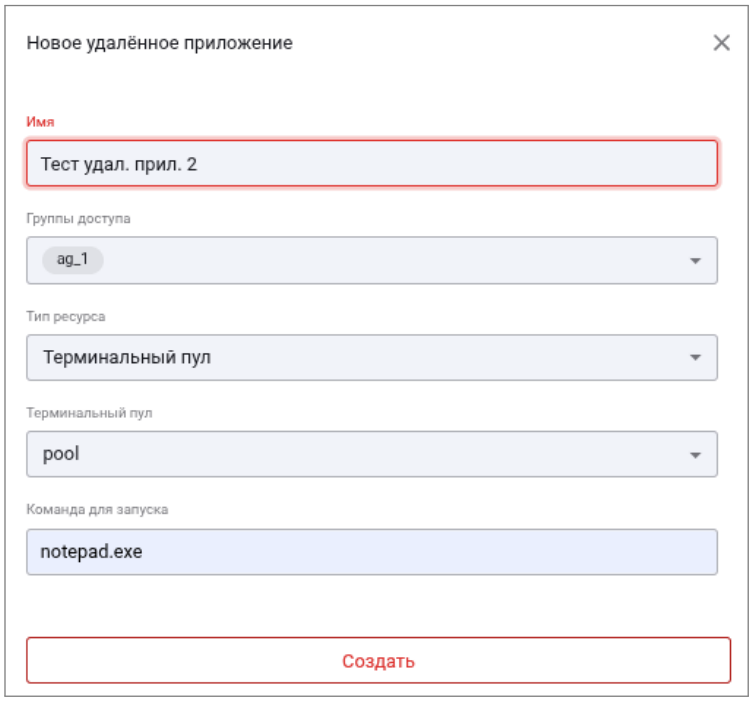

Рисунок 39 – Создание нового удаленного приложения

Для работы с приложением его следует опубликовать, включив в группу доступа. После создания приложения оно появится в списке. Выделив его, можно выполнить следующие операции:

– «Редактировать»;
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить».

6 Настройки

6.1 Разрешения

6.1.1. Разрешение – это набор параметров протокола удаленного доступа при подключении к BPM. Для работы с разрешениями используется подраздел «Разрешения» в разделе «Настройки» (рисунок 40).

Рисунок 40 – Раздел «Разрешения»

6.1.2. Для создания нового разрешения нажмите кнопку «Создать» и установите параметры (рисунок 41):

– протокол WinRDP/RedDirect;

– название (обязательный параметр);

– порт подключения (по умолчанию – 3389);

– (опционально) логин и пароль учётной записи для сессии пользователя на BPM;

– включение буфера обмена – разрешает использовать буфер для передачи файлов между клиентом и сервером, текста при работе с виртуальным рабочим местом.

– проброс учетных данных – доступен при аутентификации с "толстого клиента". На веб-клиенте не действует.

Отдельно выведены «Настройка дисплея» и «Настройки периферии» (рисунок 42):

«Настройка дисплея»:

– разрешение во весь экран;

– установить количество пикселей;
– возможность динамического разрешения;
– возможность подключения нескольких мониторов.

«Настройка периферии»:

– чекбокс «смарт-карта» – разрешает проброс смарт-карты (при её наличии у пользователя) на конечное виртуальное рабочее место и дальнейшее её использование.
– чекбокс «USB Диски» разрешает использовать соответствующую периферию;
– чекбокс «Принтеры» разрешает использовать соответствующую периферию;
– чекбокс «Аудио» разрешает использовать соответствующую периферию;
– чекбокс «Микрофон» разрешает использовать соответствующую периферию;
– чекбокс «Камера» разрешает использовать соответствующую периферию;
– чекбокс «Папки» разрешает использовать соответствующую периферию. (Использовании протокола WIN RDP пробрасывает диск целиком, а не отдельную папку (как физический, так и виртуальный диск).

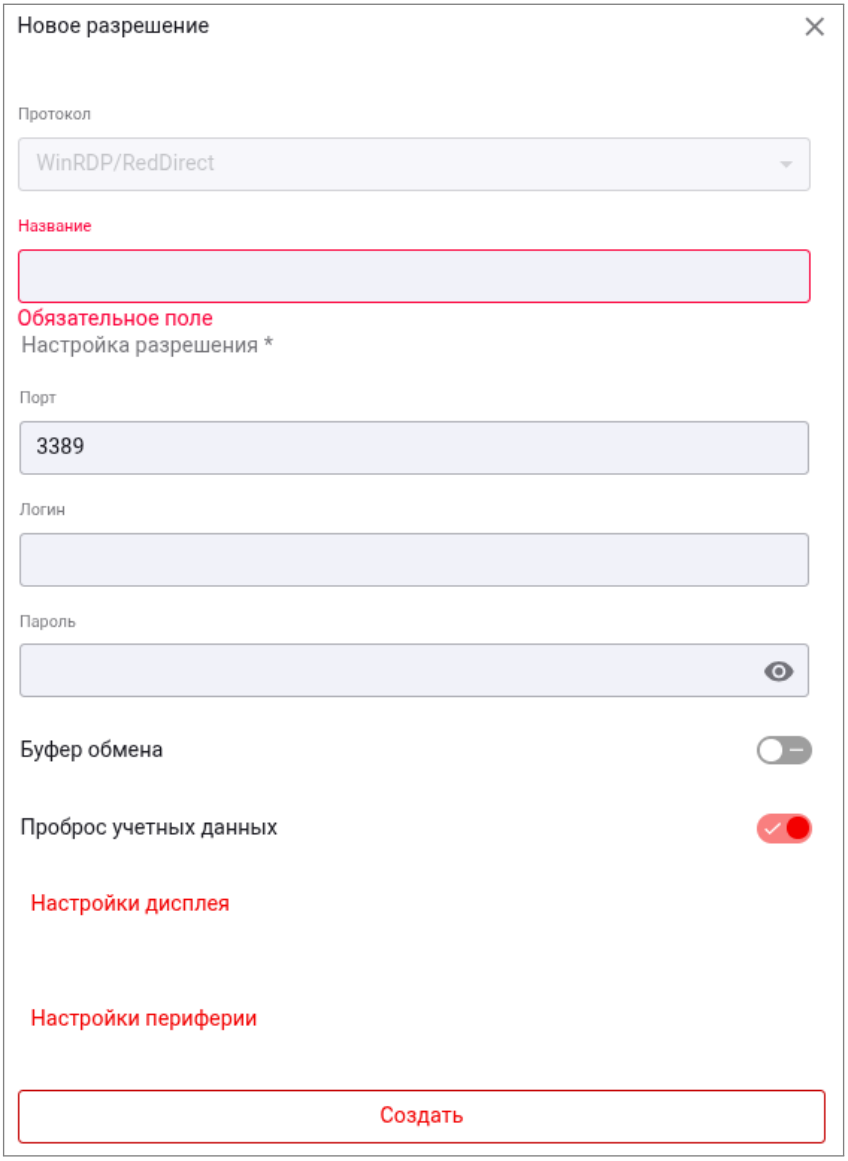

Рисунок 41 – Создание нового разрешения

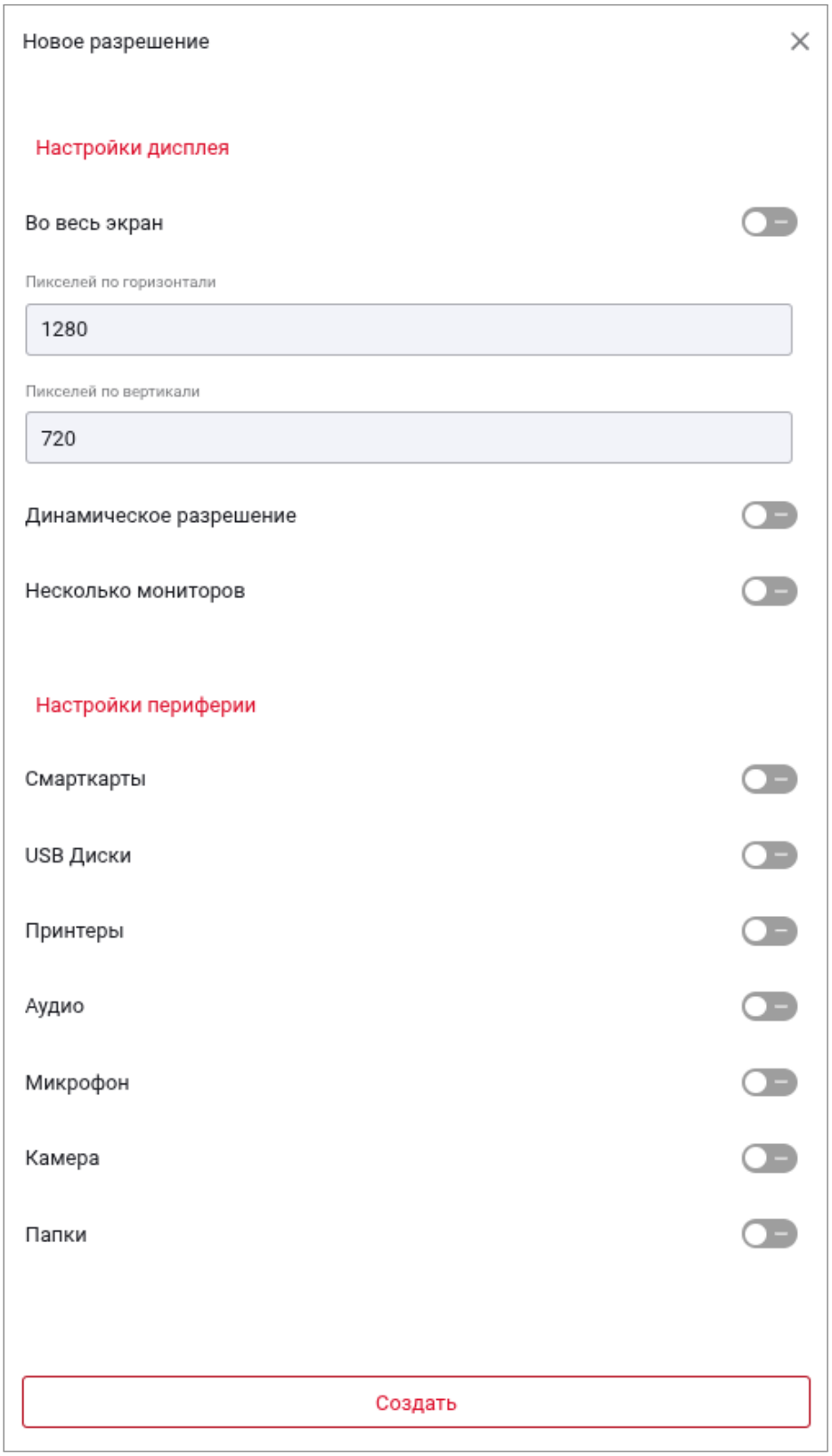

Рисунок 42 – Создание нового разрешения

6.1.3. Созданное разрешение появится в списке. Выделив его, можно выполнить следующие операции:

– «Копировать»;
– «Редактировать»;
– «Удалить»;

– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить» (рисунок 43).

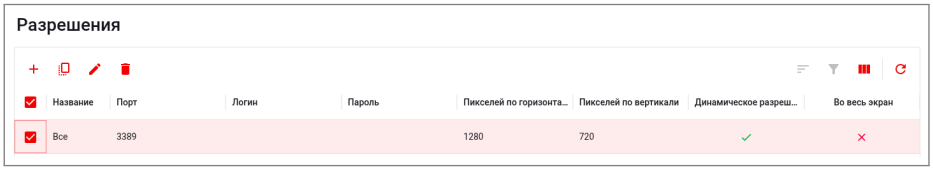

Рисунок 43 – Операции с разрешением

6.2 Группы доступа

6.2.1. Для настройки доступа к виртуальным рабочим местам используются группы доступа, расположенные в подразделе «Группы доступа» разделе «Настройки» (рисунок 44).

Рисунок 44 – Раздел «Группы доступа»

6.2.2. Для создания новой группы доступа нажмите кнопку «Создать» и установите параметры (рисунок 45):
– название (обязательный параметр);
– (опционально) в выпадающем меню «Разрешения» – выберите имеющееся разрешение, которое будет использовано в качестве шаблона.

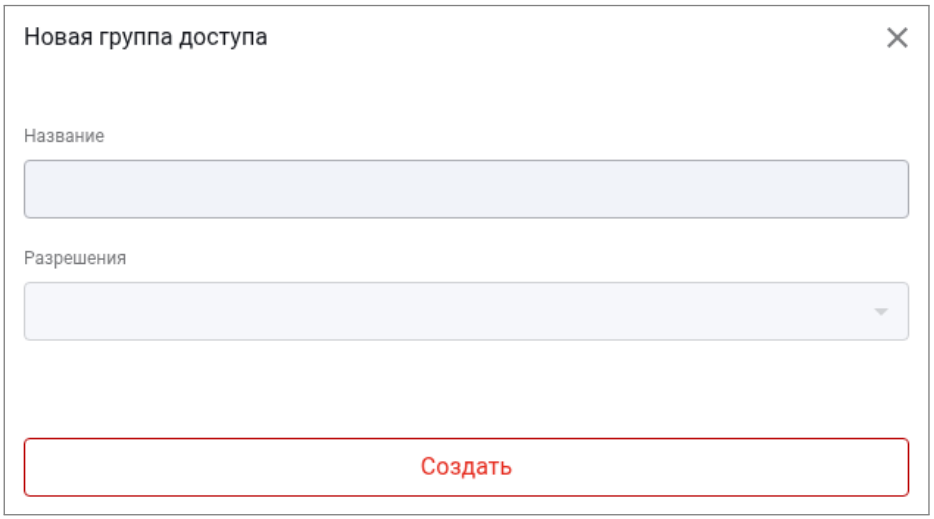

Рисунок 45 – Создание новой группы доступа

Если вы выберете имеющееся разрешение, то появится секция с настройкой параметров разрешения, где в качестве параметров по умолчанию будут указаны параметры выбранного разрешения (рисунки 46–47).

6.2.3. Созданная группа доступа появится в списке, можно выполнить операции :

– «Копировать»;
– «Редактировать»;
– «Подробнее» (открывает список пользователей в группе);
– «Удалить»;
– «Сортировать»;
– «Фильтровать»;
– «Столбцы»;
– «Обновить» (рисунок 48).

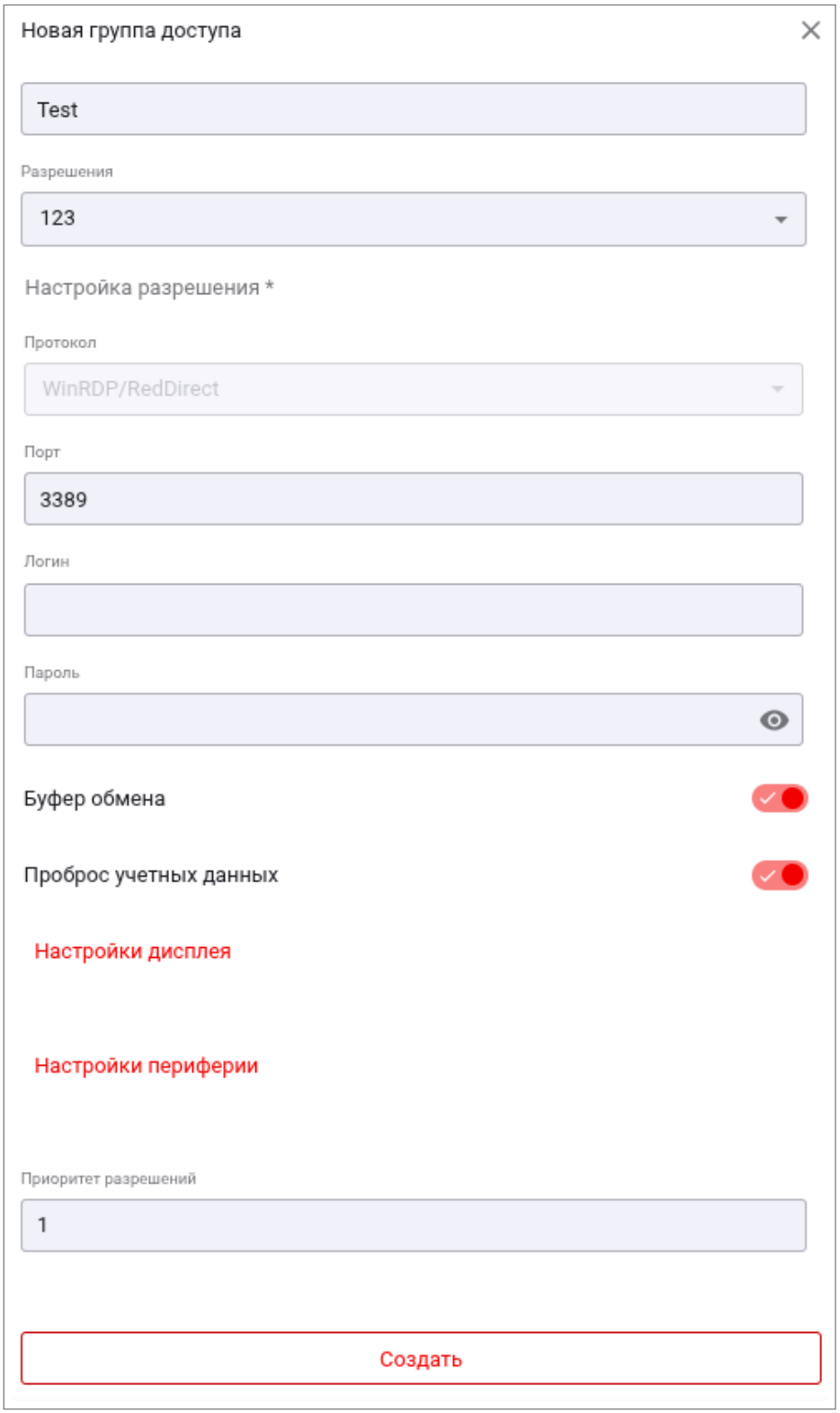

Рисунок 46 – Создание новой группы доступа: настройка разрешения

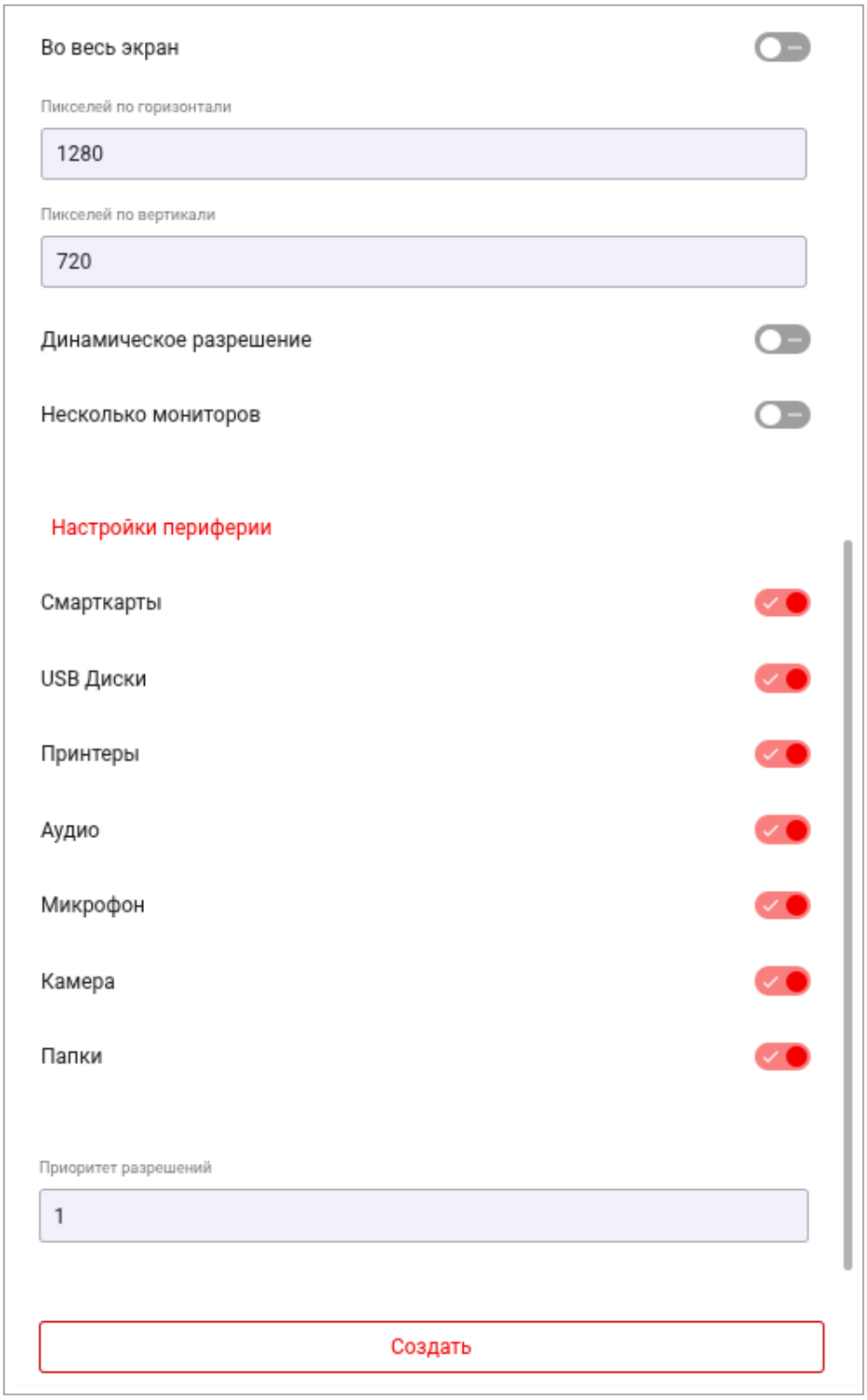

Рисунок 47 – Создание новой группы доступа: настройка разрешения

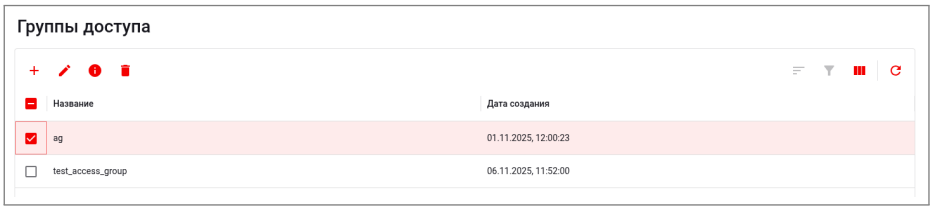

Рисунок 48 – Действия, доступные для выбранной группы доступа

6.2.4. Для добавления в группу доступа пользователей нажмите кнопку «Добавить». В открывшемся модальном окне в выпадающем списке выберите нужных пользователей. Закончив выбор, нажмите кнопку «Добавить» (рисунок 49).

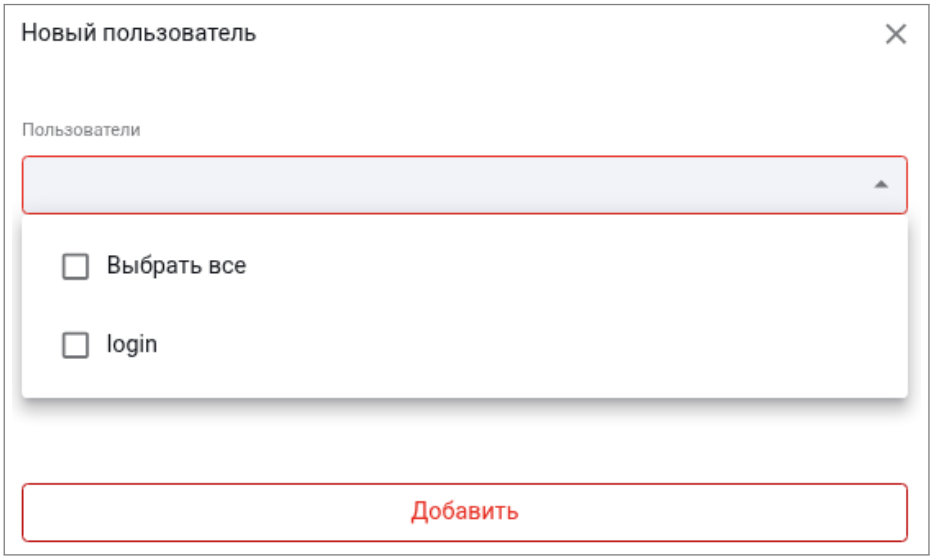

Рисунок 49 – Добавление пользователей из числа существующих

Если выделить пользователя в списке (рисунок 50), то станут активными кнопки:
– «Подробнее» – просмотр и редактирование свойств пользователя;
– «Удалить» – удаление пользователя.

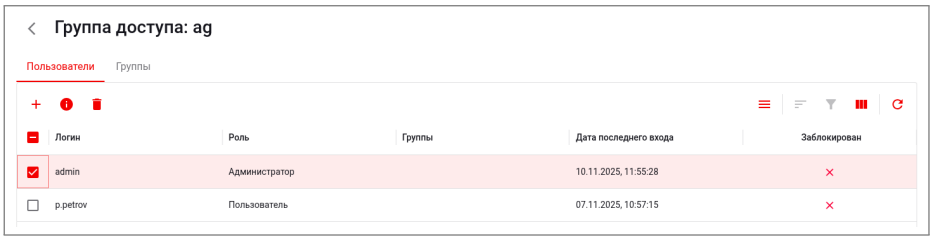

Рисунок 50 – Выбор пользователя для действий с ним

7 Подключение пользователя

В данном разделе рассматривается, подключение клиента к удаленному рабочему месту или приложению. Для подключения, рабочее место и приложение должны быть настроены, а у пользователя должен быть установлен клиент РЕД ВРМ.

В терминальной редакции подключиться можно как через веб-клиент, так и через GUI-клиент. Функционал администратора доступен только через веб-панель.

7.1 Настройка рабочих ресурсов

7.1.1. Администратор подключает к рабочему месту:

– «Ресурс» – в виде агента или пула агентов.

– «Группу доступа» – сюда администратор добавляет пользователя.

Без этих подключений рабочее место не отобразится в витрине ресурсов пользователя.

7.2 Подключение пользователя через веб-интерфейс

7.2.1. Войдите в РЕД ВРМ с логином/паролем или по смарт-карте (см. раздел 1.2).

7.2.2. Нажмите на созданное рабочее место или приложение (рисунок 51).

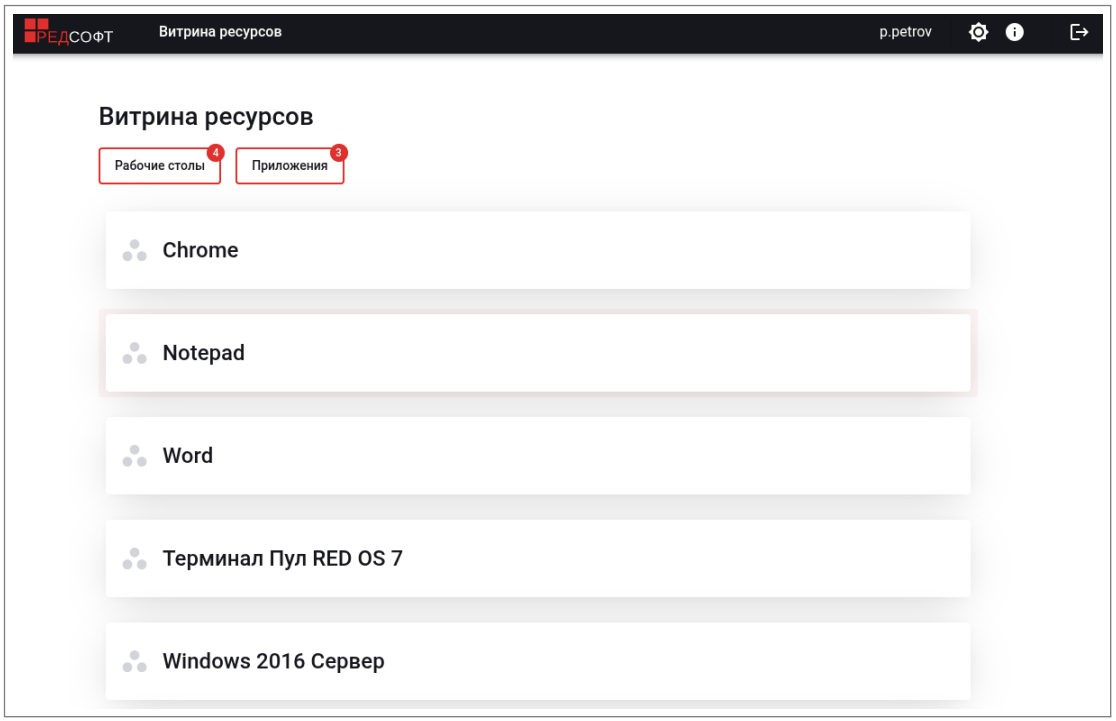

Рисунок 51 – Выбор рабочего ресурса

3) Подтвердите запуск (рисунок 52).

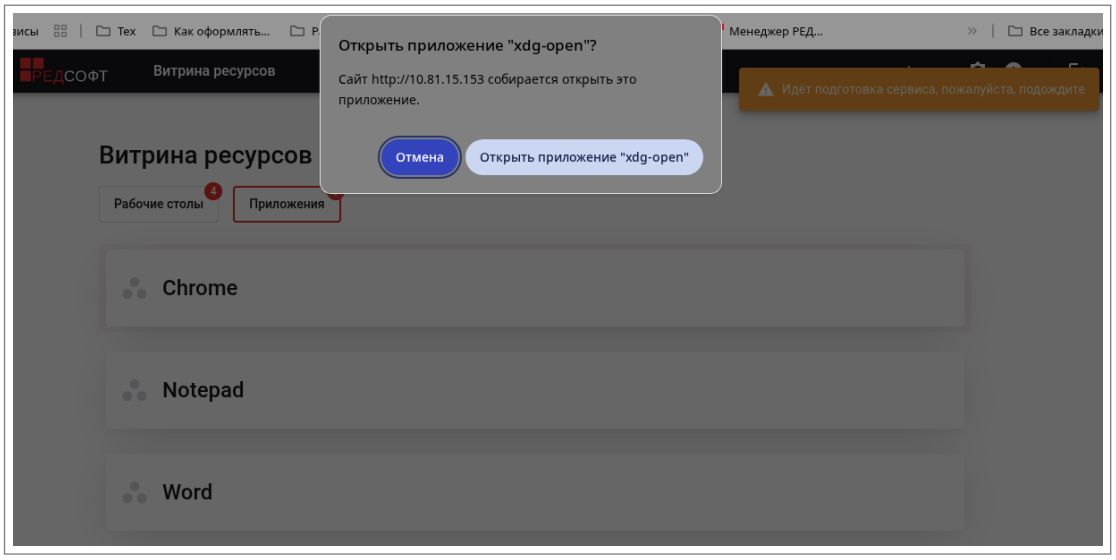

Рисунок 52 – Подключение

4) Подключившись к BPM, пользователь выбирает доступную для работы периферию (выбирается в разделе «Настройки» (см. пункт 6.1.2)). Пользователь может составить свой список устройств, с которыми он работает. Система сохранит список, устройства в нем можно добавить или удалить. Доступна сортировка по типам устройства (рисунок 55).

При подключении папки, нажмите на кнопку «Добавить папку». Откроется список папок данного рабочего места. Выбрав нужную папку, нажмите кнопку "Выбрать"в правом верхнем углу (рисунок 53).

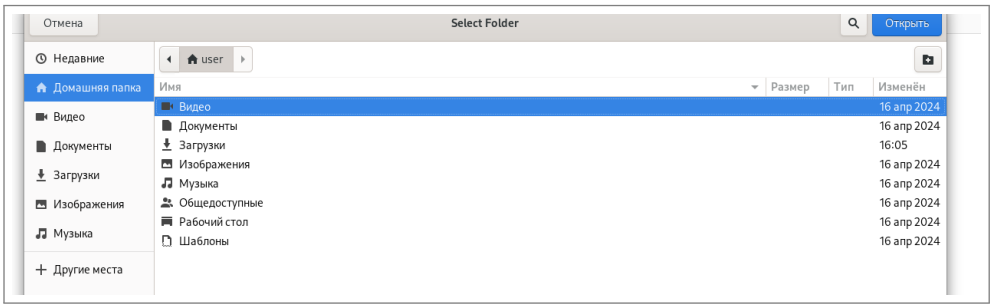

Рисунок 53 – Выбор папок

Можно добавить несколько папок, все они будут проброшены. (рисунок 54).

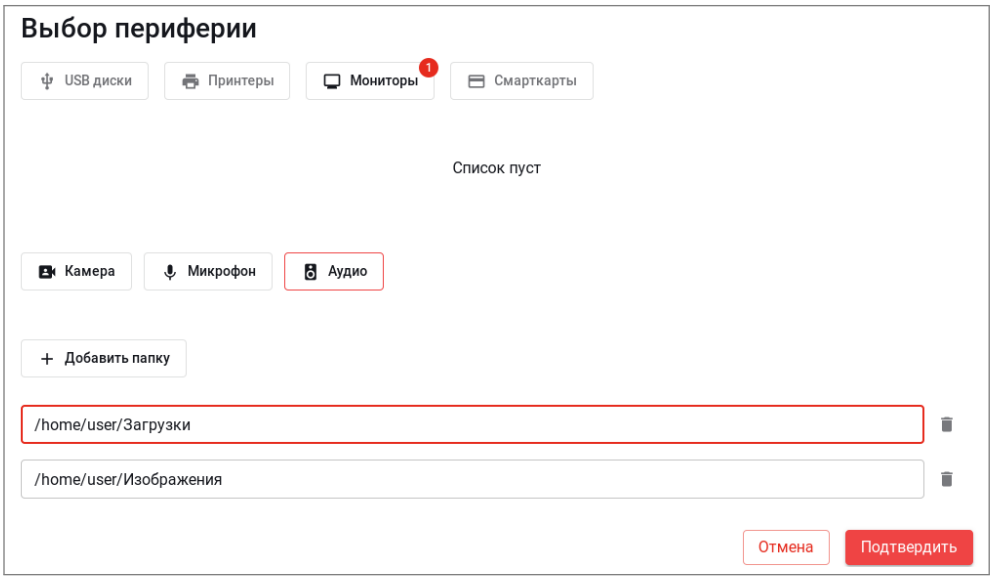

Рисунок 54 – Частичный выбор

Выбранные устройства: «USB диски» «Принтеры», «Мониторы», «Смарт-карты», «камера», «микрофон», «аудио» подсвечиваются красным и отображают список доступных устройств. (рисунок 55).

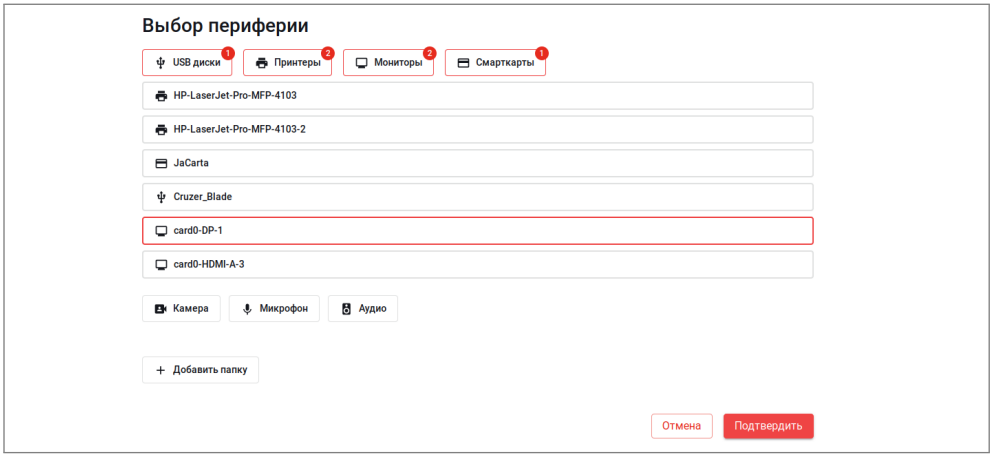

Рисунок 55 – Выбор периферии

В случае отсутствия оборудования определенного типа отобразится информация «Список пуст» (рисунок 56).

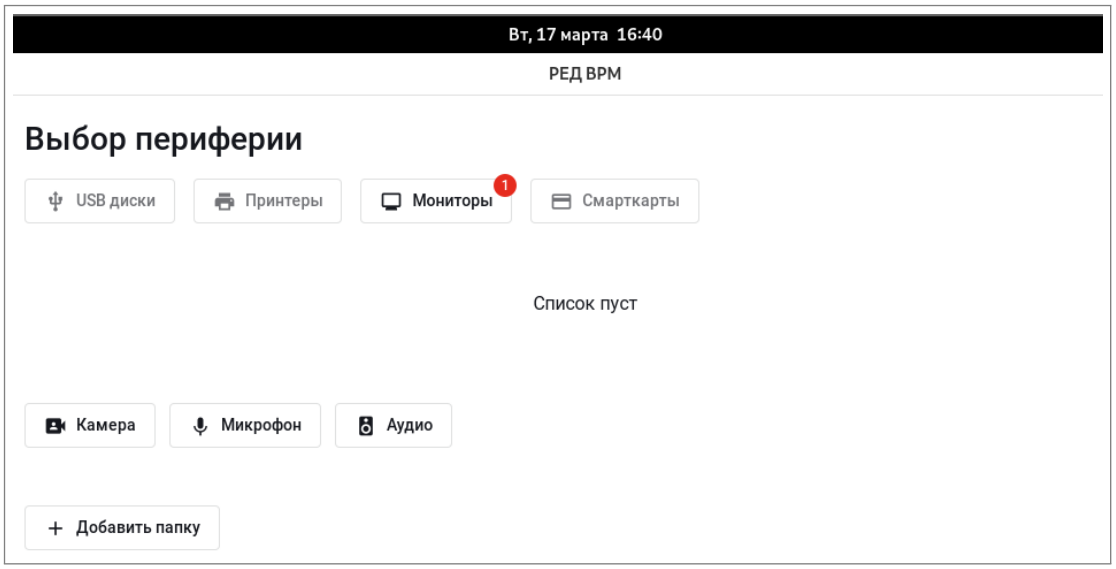

Рисунок 56 – Список устройств

Так происходит выбор оборудование в разделах: «USB диски» «Принтеры», «Мониторы», «Смарт-карты», «камера», «микрофон», «аудио».

Важно!
Выбор USB диска отключен на Windows, т.к. пробрасывается логический диск целиком.

Важно!
С клиента на Windows, возможно подключение либо одного монитора (указанного "по умолчанию"), либо сразу всех доступных.

Важно!
Windows клиент отображает все контейнеры, которые находятся на смарт-карте. Для корректной работы, рекомендуется выбрать из списка само устройство.

Пример:

«Rutoken ECP 0» для Рутокена
«JaCarta 0» для Джакарты

6) Нажмите «Подтвердить». Появится окно ввода данных (рисунок 57).

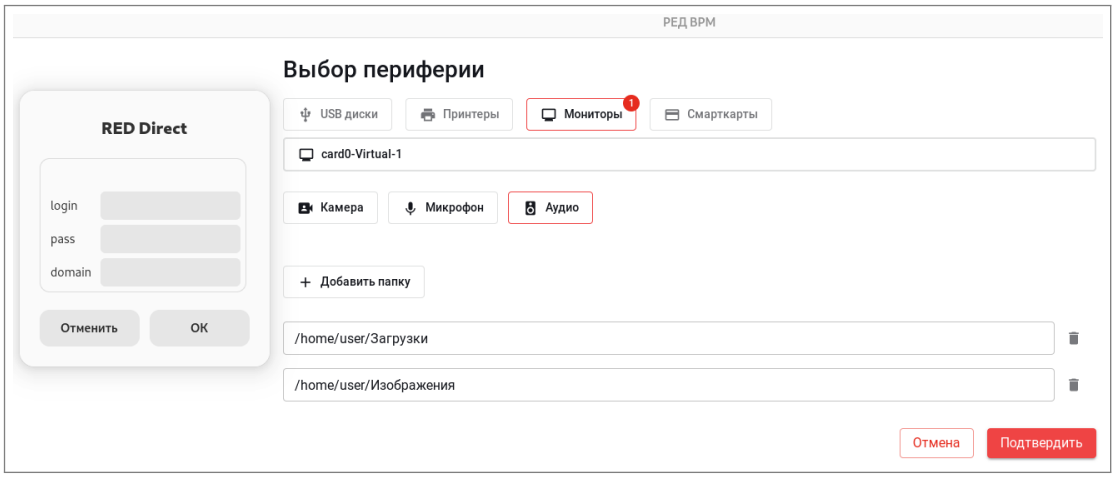

Рисунок 57 – Ввод

После его заполнения пользователь успешно подключается к удалённому рабочему месту (рисунок 58).

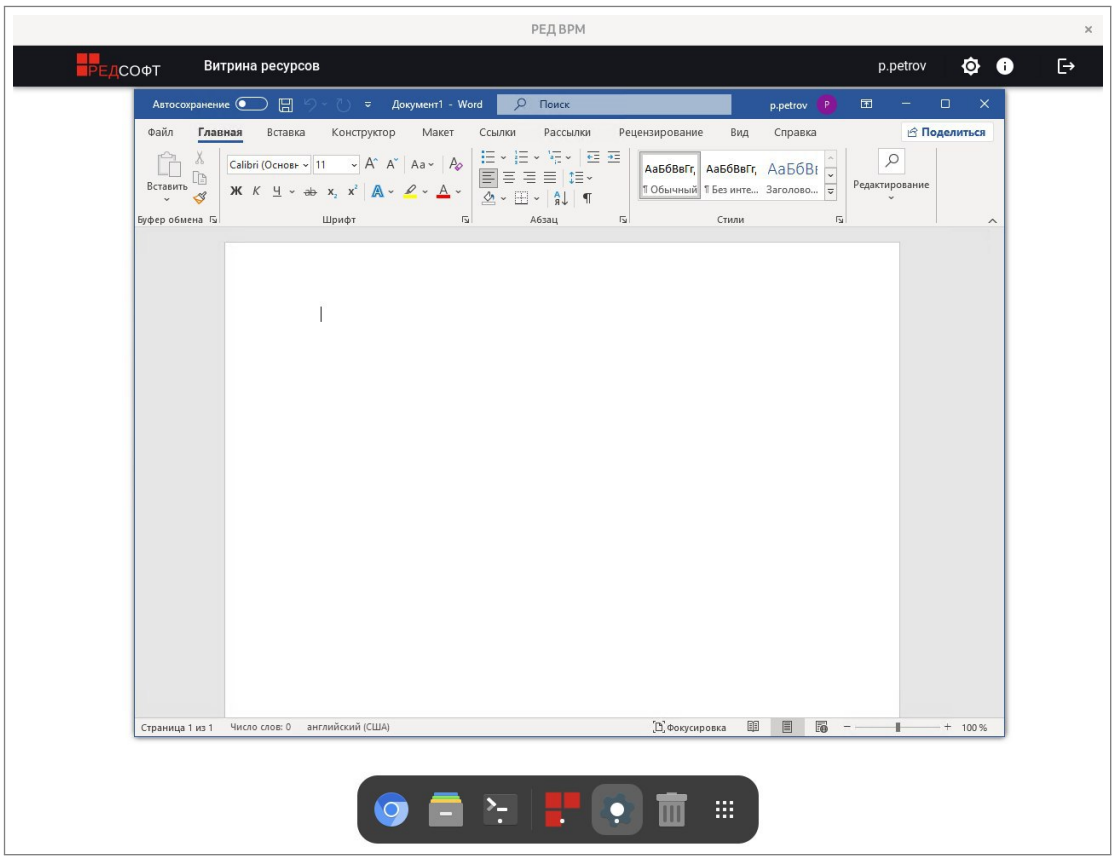

Рисунок 58 – Удалённое приложение

7) Завершите сеанс пользователя. Последовательность и название элементов может отличаться в зависимости от графической оболочки и ОС:

«Главное меню» → «Выход» → «Завершить сеанс».

7.3 Подключение пользователя через GUI-интерфейс

После запуска приложения пользователь попадает на страницу добавления брокера (рисунок 59).

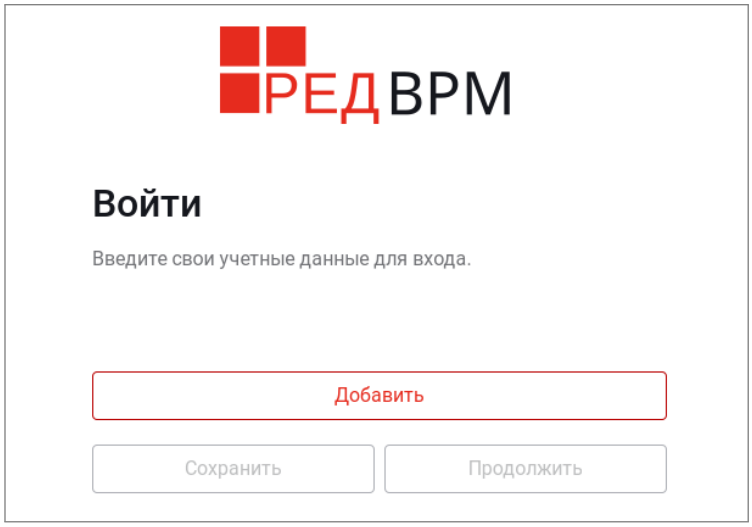

Рисунок 59 – Доступ к рабочему месту

Кнопка "Добавить"позволяет ввести тег и адрес. Кнопка "Сохранить"становится активной при заполнении всех тегов и адресов. Отметьте галочкой одно из рабочих мест и нажмите "Продолжить"(рисунок 60).

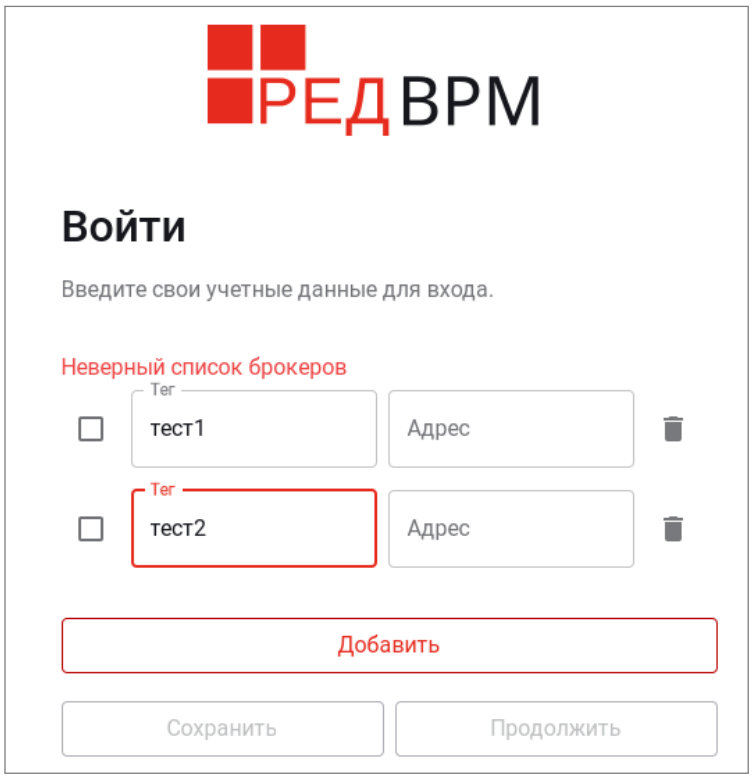

Рисунок 60 – Добавление тега/адреса

На странице аутентификации пользователь вводит логин и пароль, переходит на рабочее место. Кнопка «Войти другим способом» переключает между авторизацией через логин/пароль и смарт-картой.

Дальнейшие шаги аналогичны указанным в разделе 7.2.2.

При последующих заходах автоматически отображается брокер, введенный первым. Остальные скрыты во всплывающем меню слева. (рисунок 61).

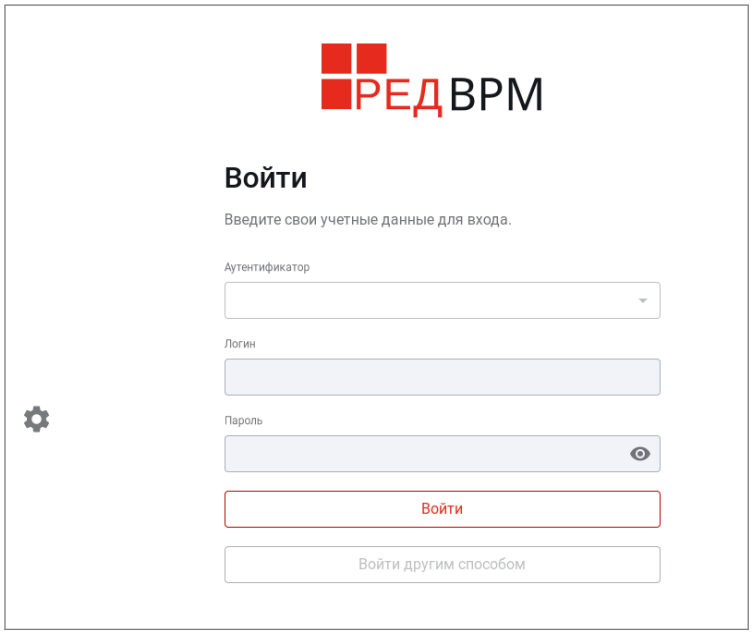

Рисунок 61 – Авторизация

7.3.1. Способы аутентификации устанавливаются в разделе «Аутентификаторы» (см. 2.1.3 «Аутентификаторы типов «РЕД АДМ» и «Active Directory»»).

Важно! При авторизации по смарт-карте на сервер ОС Windows, может использоваться протокол NLA (Network Level Authentication / Проверка подлинности на уровне сети).

В ряде сценариев аутентификации, необходимо убрать ограничение, разрешающее подключение только с компьютеров, поддерживающих NLA».

Подключение на Linux-сервер по смарт-карте происходит, если выполнены оба условия:

1) Пользователь подключается с графического клиента;
2) Включен «Проброс учетных данных» в разрешениях группы доступа.

8 Конфигурационные файлы

В данном разделе рассмотрены важные моменты для конфигурационных файлов брокера.

> **Важно!** Изменение значений указанных ниже параметров приведёт к изменению поведения программного обеспечения, но не выведет его из строя. Изменение остальных значений параметров в этих файлах конфигурации или файлах конфигурации, которые в данном разделе не указаны, могут привести к выходу программного обеспечения из строя. ■

8.1 Сервис администратора

8.1.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_admin/config/server.conf`.

`AUTH_MIDDLEWARE` - булевый параметр, включающий/выключающий необходимость авторизации. Не рекомендуется его менять.

8.1.2. Параметры секции `[AGENTS]`:
`IS_ALIVE_CHECK_INTERVAL_SECONDS` – время между проверками агентов на статус онлайн (в секундах).

8.1.3. После изменения настроек перезапустите службы:

```
  systemctl restart broker_admin.service \
broker_admin_scheduler.service broker_admin_worker.service
```

8.2 Сервис терминала

8.2.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_terminals/config/settings.json`.

8.2.2. Параметры секции `[metric]`:

`period = 10` – период сбора (в секундах).

`freshTimeout` – интервал сбора (в секундах).

`maxLoadIndex` – количество секунд, после истечения которого метрики, отправленные агентом, будут считаться устаревшими.

8.2.3. После изменения настроек перезапустите службу:

```
systemctl restart broker_auth.service
```

8.3 Сервис сессий

8.3.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_sessions/config/settings.json`.

8.3.2. Параметры секции `[metric]`:

`period = 10` – период сбора (в секундах).

`interval = 5` – интервал сбора (в секундах).

8.3.3. После изменения настроек перезапустите службу:

```
systemctl restart broker_sessions.service
```

8.4 Сервис токенов

8.4.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_token/config/settings.json`.

8.4.2. Параметры секции `[metric]`:

`period = 10` – период сбора (в секундах).

`interval = 5` – интервал сбора (в секундах).

`token.access_expire_minutes` – время жизни access-токена (в минутах), обычно период составляет от 5 до 120.

`token.refresh_expire_hours` – время жизни refresh-токена (в часах), обычно период составляет от 1 до 720.

`token.renew_refresh_lifetime` – политика `refreshTT`:

1)Значение `true` делает рефреш токен с конечным временем жизни, указанным в пункте `refresh_expire_hours`.

2)Значение `false` делает рефреш токен бесконечным.

8.4.3. После изменения настроек перезапустите службу:

```
systemctl restart broker_token.service
```

8.5 Сервис аутентификаций

8.5.1. Полный путь к конфигурационному файлу: `/opt/redvrm/broker_auth/config/settings.json`.

8.5.2. После изменения настроек перезапустите службу:

```
systemctl restart broker_auth.service
```

8.6 Сервис API

8.6.1. Полный путь к конфигурационному файлу: `/opt/redvrm/broker_gateway/config/settings.json`.

8.6.2. После изменения настроек перезапустите службу:

```
systemctl restart broker_gateway.service
```

8.7 Сервис мониторинга

8.7.1. Полный путь к конфигурационному файлу: `/opt/redvrm/broker_monitoring/config/settings.json`.

8.7.2. После изменения настроек перезапустите службу:

```
systemctl restart broker_monitoring.service
```

8.8 Сервис ресурсов

8.8.1. Полный путь к конфигурационному файлу: `/opt/redvrm/broker_resources/config/settings.json`.

8.8.2. После изменения настроек перезапустите службу:

```
systemctl restart broker_resources.service
```

8.9 Сервис рабочих мест

8.9.1. Полный путь к конфигурационному файлу: `/opt/redvrm/broker_virtual_workspaces/config/settings.json`.

8.9.2. После изменения настроек перезапустите службу:

```
systemctl restar broker_virtual_workspaces.service
```

9 Просмотр логов

Здесь рассмотрены логи на брокере. Рекомендуем смотреть логи через инструмент `journalctl` для каждого из сервисов отдельно.

9.1. Сервис администратора:

```
journalctl -u broker_admin_scheduler.service
```

```
journalctl -u broker_admin.service
```

```
journalctl -u broker_admin_worker.service
```

9.2. Мониторинг:

```
journalctl -u broker_monitoring.service
```

9.3. Удаленные приложения:

```
journalctl -u broker_remoteapp.service
```

9.4. Терминалы:

```
journalctl -u broker_terminals.service
```

9.5. Клиентский сервис:

```
journalctl -u broker_virtual_workspaces.service
```

9.6. Сервис API:

```
journalctl -u broker_gateway.service
```

9.7. Сервисы аутентификации:

```
journalctl -u broker_auth.service
```

```
journalctl -u broker_resources.service
```

```
journalctl -u broker_token.service
```