Функциональные характеристики

«IDM Crosstech Advanced Edition»

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

Сокращение	Расшифровка
AD	Active Directory
API	Application Programming Interface
BPM	Business Process Management
HR	Human Resources
IDM CAE	Identity Management Crosstech Advanced Edition
IG	Identity Governance
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
RBAC	Role-Based Access Control
REST	Representational State Transfer
SSH	Secure Shell
АРМ	Автоматизированное рабочее место
БД	База данных
БП	Бизнес-процесс
ИС	Информационная система
МКР	Матрица конфликтных ролей
ОС	Операционная система
РМ	Ролевая модель
УЗ	Учётная запись

Термин	Определение
Архетип	Формальное определение подтипа объекта в IDM CAE. Архетипы могут придавать специфические свойства основным типам IDM CAE, таким как пользователь, роль или организация. Например, архетипы можно использовать для дальнейшего уточнения понятия «пользователь», чтобы представить работников, студентов, подрядчиков и партнеров
Исполняемый экземпляр модели процесса	Уникальное событие, которое создаётся при каждом выполнении процесса. Каждый исполняемый экземпляр модели процесса работает независимо и имеет потенциально разные данные, состояния и результаты
Коннектор	Часть IDM CAE, используемая для связи с ресурсом. Коннектор представляет собой специальный программный интерфейс, которые позволяют IDM CAE взаимодействовать с различными ресурсами
Матрица конфликтных ролей	Часть РМ. Определяет, какие роли могут назначаться одновременно (совмещаются), а какие нет (конфликтуют)

Термин	Определение
Модель процесса	Графическое представление БП, которое определяет последовательность действий, событий и условий для его выполнения
Пользователь	Структура данных в IDM CAE, описывающая человека
Пользовательская задача	Этап БП, который требует участия человека
Проекция	Способ хранения информации в репозитории IDM CAE. Представляет собой объекты в ресурсах (УЗ, права доступа, организационные единицы)
Ресурс	Сторонние ИС, в которых IDM CAE управляет учётными записями. Кроме того, ресурсами считаются все ИС, подключенные к IDM CAE в разделе Resources
Ролевая модель	Формализованный способ описания ролей, заключающийся в отражении информации о том: • какие роли (бизнес-роли) предусмотрены в ИС для пользователей; • какие функции и права эти роли предоставляют; • совокупностью каких объектов (групп AD, ролей / групп внутри ИС) эти роли задаются; какие роли могут назначаться одновременно (совмещаются), а какие нет (конфликтуют)
Роль	Набор прав доступа
Учётная запись	Хранимая в ИС совокупность данных о пользователе
Целевая ИС	ИС, в которой IDM CAE управляет УЗ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. О документе

Руководство администратора – документ, предоставляющий администратору инструкции по управлению и работе с программным комплексом IDM Crosstech Advanced Edition (далее – IDM CAE). Он включает в себя:

- описание архитектуры;
- методы интеграции со сторонними решениями;
- описание основных операций по управлению;
- инструкции по мониторингу состояния компонентов;
- другую информацию по управлению.

Настоящее руководство администратора предназначено для администраторов, в обязанности которых входит выполнение работ по настройке и администрированию программных средств. Материал, изложенный в данном документе, предполагает у читателя наличие знаний в области операционных систем (далее – ОС) и сетевых технологий, понимание концепции безопасности и умение обеспечивать её на уровне системы.

1.2. Об IDM CAE

IDM CAE предоставляет возможность централизованного управления учётными записями (далее – УЗ) и правами пользователей различных информационных систем (далее – ИС) компании с помощью ключевых модулей: Base, Monitoring, Identity Governance (далее – IG) и Request Management. IDM CAE получает данные о ра-

ботниках и организационно-штатной структуре из доверенных источников, таких как системы кадрового учёта, а также информацию о пользователях и их полномочиях из других ИС компании.

В IDM CAE настраиваются процессы управления доступом к ИС. Эти процессы могут быть как полностью автоматизированными (например, автоматическая блокировка доступа при увольнении), так и требовать вмешательства определённых работников (например, для согласования запросов).

Пользователи взаимодействуют с IDM CAE через веб-интерфейсы модулей. Доступ к различным функциям и объектам IDM CAE (разделам веб-интерфейса, отчётам и т. п.) может быть различным

2. АРХИТЕКТУРА

2.1. Общее описание

Модуль Base в составе IDM CAE предоставляет основную функциональность для управления УЗ пользователей, осуществляет автоматический сбор информации об активности пользователей, контроль безопасности доступа к ресурсам, анализ, отчётность, настройка и исполнение бизнес-процессов (далее – БП).

Модуль Base состоит из следующих компонентов:

- Provisioning Management;
- Workflow Management;

2.2. Компонент Provisioning Management

Provisioning Management предоставляет основную функциональность для управления идентификацией и авторизацией пользователей, автоматический сбор информации об активности пользователей, контроль безопасности доступа к ресурсам, анализ и отчетность.

2.3. Компонент Workflow Management

Workflow Management является ключевым компонентом, отвечающим за исполнение БП. С помощью него возможно автоматизировать БП, а также определять и контролировать последовательность выполнения задач, управлять процессами с высокой степенью гибкости и при этом обеспечивать соответствие правилам и политикам безопасности.

2.4. Схема взаимодействия компонентов модуля Base

Архитектурная схема модуля Base, включающая элементы каждого компонента модуля и их функции, представлена в Приложении 1.

Основные сценарии взаимодействия компонентов модуля Base представлены ниже:

- **автоматизация рабочих процессов:**

  компонент Workflow Management может использовать компонент Provisioning Management для выполнения действий, связанных с управлением УЗ, ролями и правами доступа, например:

  - автоматическое создание УЗ в компоненте Provisioning Management;
  - назначение ролей пользователям в соответствии с бизнес-правилами;
  - согласование изменений в правах доступа через компонент Workflow Management;

- **взаимодействие через REST API:**

  компонент Workflow Management – это BPM-платформа, которая управляет БП и автоматизацией рабочих задач. В рамках этих процессов компонент Workflow Management использует специальные программные компоненты – делегаты, сервисы или скрипты, которые реализуют конкретную бизнес-логику.

В БП компонент Workflow Management вызывает программный модуль, который отправляет запросы (например, создание пользователя, назначение ролей и т.п.) к REST API компонента Provisioning Management, обеспечивая автоматизацию управления УЗ, ролями и правами доступа;

- **интеграция с задачами (tasks):**
  компонент Workflow Management может отслеживать или управлять задачами в компоненте Provisioning Management (tasks), например:
  - назначать задачи на проверку изменений в УЗ;
  - автоматически завершать задачи по завершении БП.

В некоторых сценариях компонент Workflow Management может считывать данные напрямую из БД Provisioning Management, минуя REST API. Это используется в тех случаях, когда:

- необходимые атрибуты или внутренние состояния объектов недоступны через API;
- требуется высокая скорость доступа к данным;
- нужно получить историческую или техническую информацию, не предназначенную для внешнего использования.

REST API компонента Provisioning Management предоставляет богатый набор возможностей для взаимодействия с компонентом

Workflow Management, обеспечивая эффективное управление идентификацией и правами доступа в рамках автоматизированных процессов.

Таблица сетевых соединений представлена в таблице 1.

Таблица 1 – Таблица сетевых соединений

№	Источник	Назначение	Протокол / порт	Предназначение
1.	Подсистема управления репозиторием Provisioning Management	БД Provisioning Management	JDBC / 5432	Хранение данных
2.	Подсистема управления репозиторием Workflow Management	БД Workflow Management	JDBC / 5432	Хранение данных
3.	Подсистема REST	Подсистема публичного API	HTTPS / 8080	Взаимодействие с Provisioning Management
4.	Подсистема публичного API	Подсистема REST	HTTPS / 8080	Взаимодействие с Workflow Management

3. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Для корректной работы модуля Base на автоматизированном рабочем месте (далее – АРМ) администратора должен быть установлен хотя бы один из следующих браузеров последних версий:

- Google Chrome;
- Microsoft Edge;
- Яндекс Браузер;
- Opera;
- Mozilla Firefox.

Также должен быть настроен SSH-клиент для подключения к серверу.

4. ИНТЕГРАЦИЯ С ДРУГИМИ РЕШЕНИЯМИ

Модуль Base может быть интегрирован с различными ИС, выступающими в качестве ресурсов. **Ресурс** – это представление источника данных / целевой ИС, в которой IDM CAE управляет УЗ. Строгого разграничения между источником и целевой ИС нет, они определяются одинаково. Ресурс может быть одновременно и целевой ИС, и источником данных. В качестве ресурса могут быть подключены такие ИС как:

- Microsoft Active Directory;
- почтовый сервис;
- ИС, интегрируемые посредством коннекторов.

Интеграция с ИС НЕ в качестве ресурса может быть осуществлена с помощью REST API или через подключение к БД.

5. ПОЛЬЗОВАТЕЛИ И ПРАВА ДОСТУПА

5.1. Разграничение доступа к разделам компонента Provisioning Management

В компоненте Provisioning Management есть роли, которые устанавливаются автоматически при развёртывании:

- *Approver* – роль, позволяющая утверждать / отклонять запросы на доступ;
- *Delegator* – роль, позволяющая делегировать свои полномочия другим пользователям временно или постоянно;
- *End user*– роль, предоставляющая доступ только к разделу SELF SERVICE, подробнее о данном разделе см. в Руководстве пользователя для модуля Base;
- *Reviewer*– роль, позволяющая запускать ресертификацию доступов;
- *Superuser*– роль, предоставляющая доступ ко всей функциональности компонента.

Также компонент Provisioning Management позволяет создавать и настраивать роли под конкретные требования.

Шаги по назначению роли см. в разделе 7.1.5.4.

5.2. Разграничение доступа к компоненту Workflow Management и модулю IG

Права доступа к компоненту Workflow Management настраиваются через предоставление / изменение / отзыв прав доступа (подробнее см. в разделе 7.2.3) к категориям. Подробнее про категории см. в Приложении 2.

Права доступа к модулю IG настраиваются в соответствии с шагами, описанными в Руководстве администратора для модуля IG.

6. ОПИСАНИЕ IDM CAE

6.1. Сущности компонента Provisioning Management

6.1.1. Объект

Каждый элемент компонента Provisioning Management представляет из себя объект. Таким образом, объектами являются ресурсы, роли, УЗ, организационные единицы и т. д., которые отражены в виде классов объектов. Объект состоит из набора элементов, которые разнятся в зависимости от типа объекта. Набор элементов объекта представляет собой типизированную схему конфигурации объекта (представление объекта).

Для просмотра схемы конфигурации сначала перейдите к просмотру всех объектов через **Repository objects -> All objects** в разделе **CONFIGURATION** (рисунок 1) и выберите нужный объект из общего списка (при необходимости воспользуйтесь фильтром **Type**). В результате откроется окно со схемой конфигурации выбранного объекта (рисунок 2).

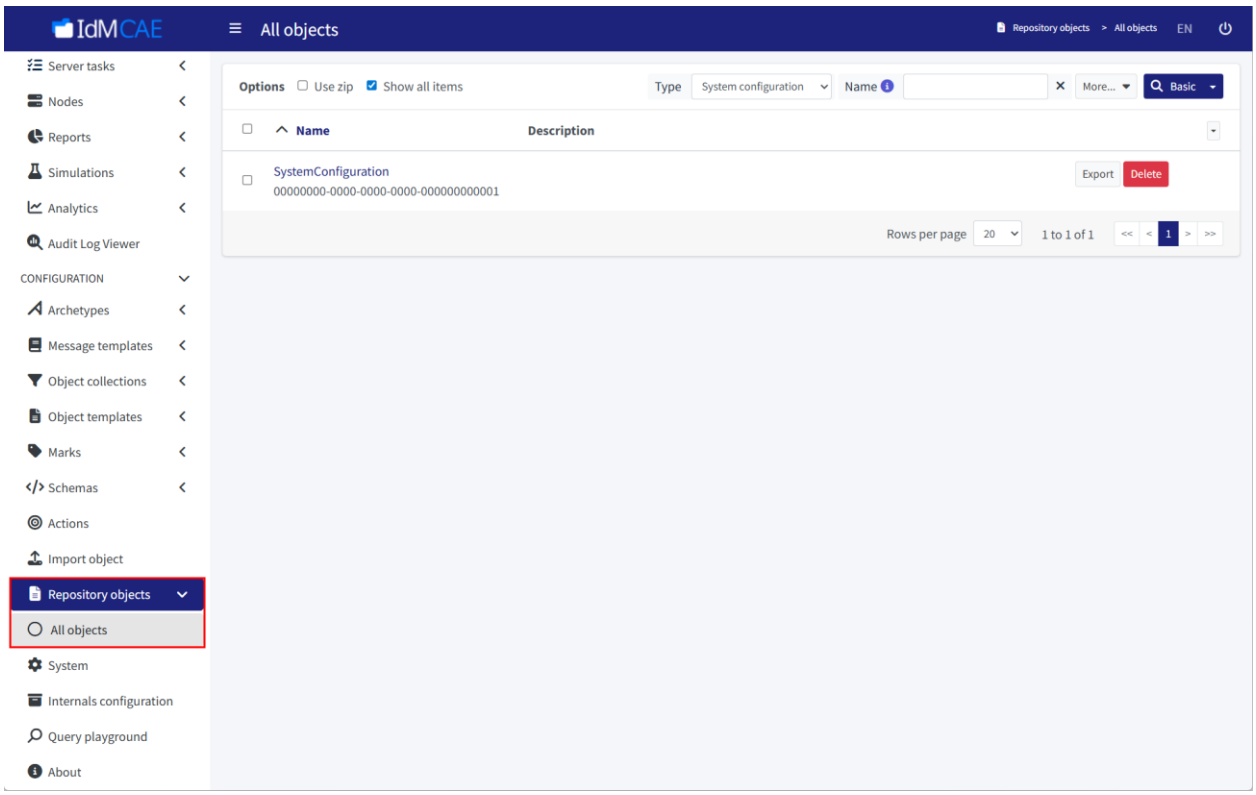


Рисунок 1 – Список объектов

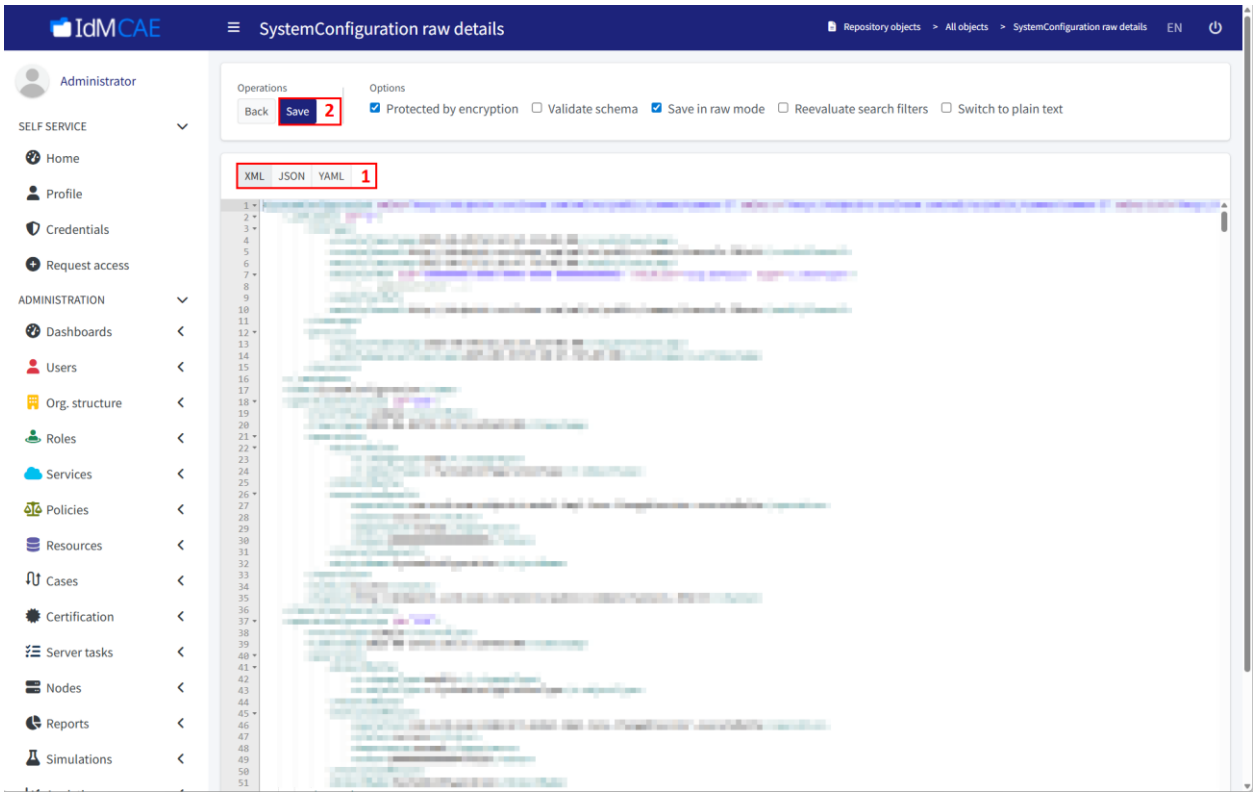


Рисунок 2 – Схема конфигурации объекта

Каждый объект имеет свой идентификатор **OID**. Значение OID является уникальным и постоянным в IDM CAE, он присваивается

объекту и не изменяется. Также каждый объект имеет имя (**name**). Имя представлено в человекочитаемой форме и может быть изменено. Имя объекта отображается пользователям.

Просмотр / редактирование схемы конфигурации объекта доступно в форматах **.XML / .JSON / .YAML**. Выберите подходящий формат с помощью соответствующих кнопок (1, рисунок 2) и сохраните изменения, нажав на **Save** (2, рисунок 2) (при необходимости).

6.1.2. Ресурс

6.1.2.1. Общие сведения

Понятие **ресурса** введено в разделе 4.

Для взаимодействия с ресурсом в IDM CAE требуется выполнить настройку определения ресурса. Определение ресурса обычно содержит:

- имя ресурса и его описание;
- ссылку на коннектор, который используется для связи с ресурсом;
- свойства конфигурации коннектора, определяющие имя хоста ресурса, порт, параметры связи и т. д. (используются для инициализации коннектора);
- определения типов объектов, используемых в данном ресурсе (обычно это определение, описывающее, как выглядит типичная УЗ, группы, роли, организационные единицы и прочие объекты);
- сопоставления (определяют, как атрибуты синхронизируются из IDM CAE в ресурс или из ресурса в IDM CAE);

- параметры синхронизации, определяющие действия IDM CAE при различных сценариях выполнения синхронизации т.д.

Для просмотра имеющихся в IDM CAE ресурсов выберите **Resources -> All resources** в разделе **ADMINISTRATION** (рисунок 3).

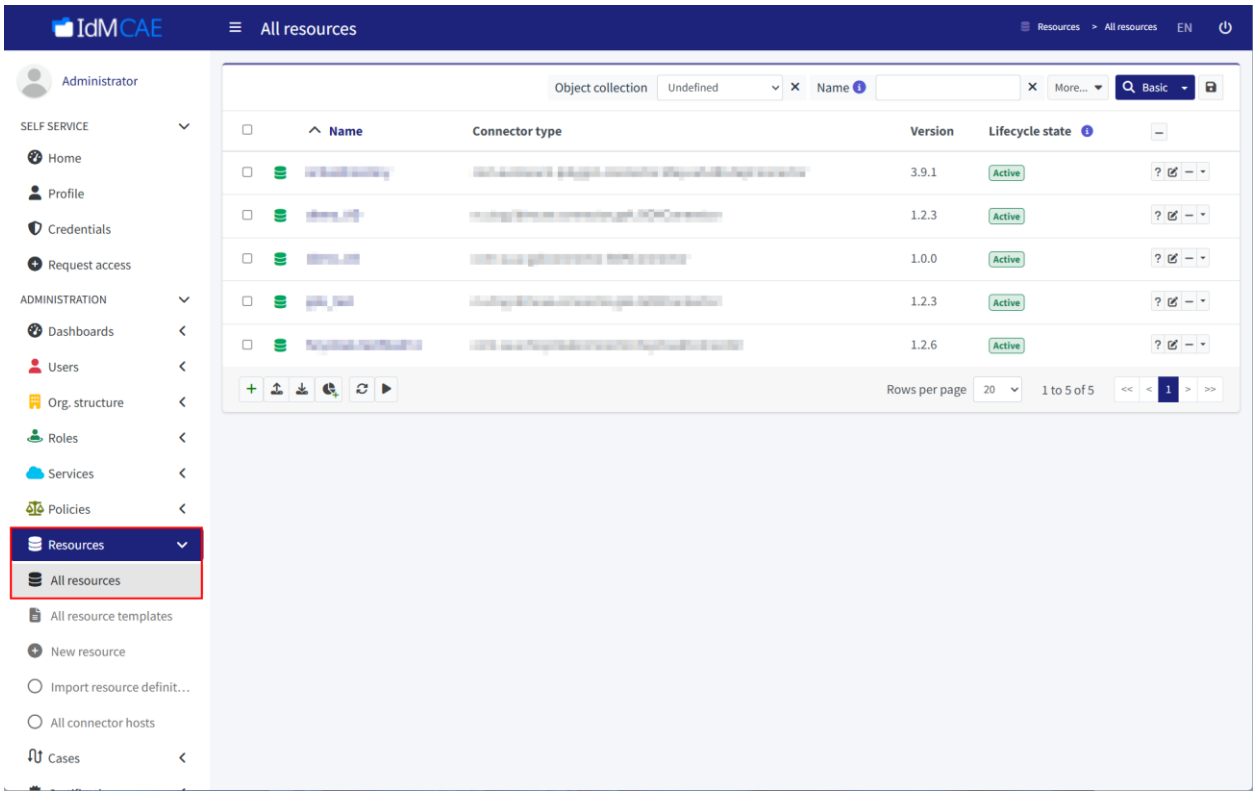


Рисунок 3 – Список ресурсов

Окно просмотра свойств ресурса представлено на рисунке 4.

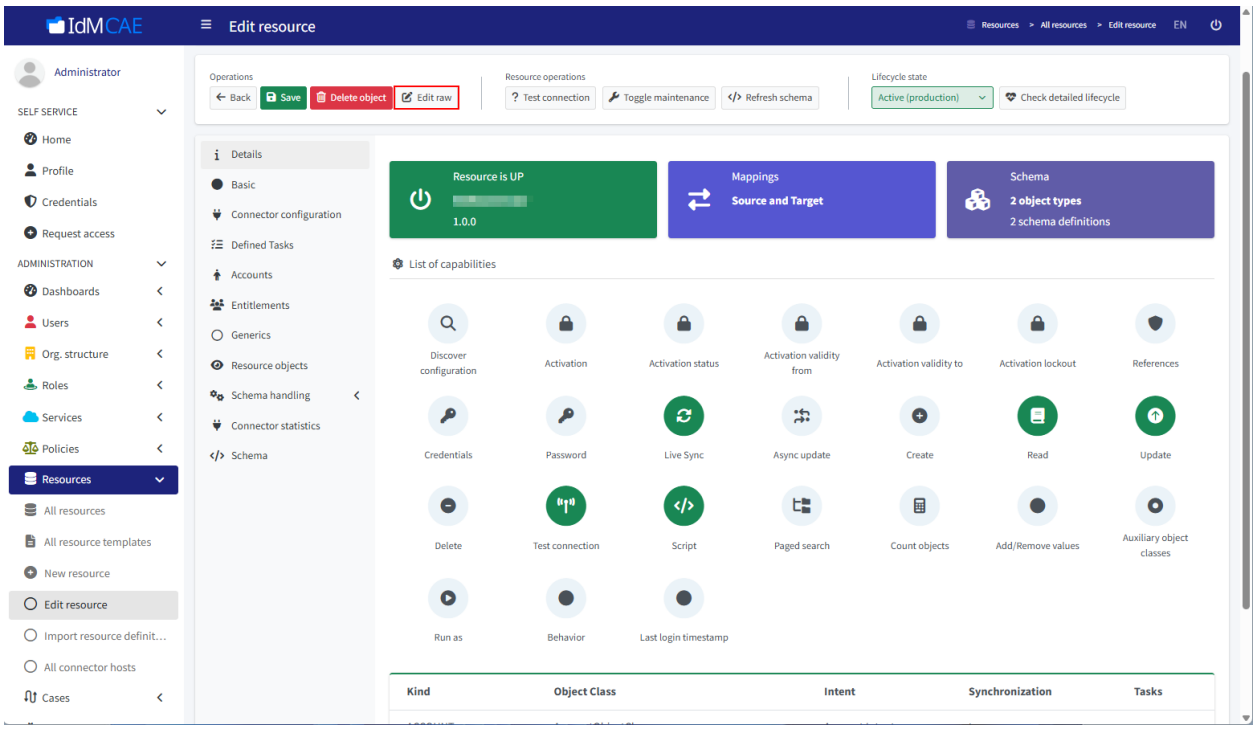


Рисунок 4 – Просмотр свойств ресурса

Просмотр / редактирование определения ресурса доступно в форматах **.XML / .JSON / .YAML**. Для перехода к определению ресурса нажмите на **Edit raw** (рисунок 4) и выберите подходящий формат (1, рисунок 5). Сохраните изменения, нажав на **Save** (2, рисунок 5) (при необходимости).

Рисунок 5 – Определение ресурса

Также перейти к определению ресурса можно через список объектов, установив предварительно в фильтре **Type** значение **Resource** (подробнее см. в разделе 6.1.1).

Возможные операции с ресурсами описаны в разделе 7.1.1.5.

6.1.2.2. Схема ресурса

Минимальный ресурс поддерживает объекты класса УЗ (account), но типичный ресурс поддерживает больше классов объектов. **Схема ресурса** представляет из себя набор определений классов объектов с их атрибутами, с которыми ресурс взаимодействует по умолчанию. Схема ресурса для каждого ресурса индивидуальна.

Представленная на рисунке 6 схема сообщает IDM CAE, что УЗ по умолчанию на данном ресурсе имеет объектный класс **inetOrgPerson**. Такие ресурсы, как серверы LDAP, могут иметь де-

сятки объектных классов, при этом существует несколько альтернативных классов объектов, которые могут быть использованы для создания УЗ. Важно указать, какой объектный класс является правильным. После того как это определение задано, УЗ появляются в подробной информации о ресурсе. Это признак того, что определение работает корректно.

Установка значения **kind** указывает на то, что данное определение класса объекта представляет собой УЗ.

```
<resource oid="b4101662-7902-11e6-9f14-53e18426fe81">
    <name>My LDAP Server</name>
    ...
    <schemaHandling>
        <objectType>
            <kind>account</kind>
            <default>true</default>
            <objectClass>ri:inetOrgPerson</objectClass>
        </objectType>
    </schemaHandling>
</resource>
```

Рисунок 6 – Типовая схема ресурса

Секция **schemaHandling** в определении ресурса – это место, где задаётся базовое поведение атрибутов класса объектов (рисунок 7).

```
<resource oid="b4101662-7902-11e6-9f14-53e18426fe81">
    <name>My LDAP Server</name>
    ...
    <schemaHandling>
        <objectType>
            <kind>account</kind>
            <default>true</default>
            <objectClass>ri:inetOrgPerson</objectClass>
            <attribute>
                <ref>ri:dn</ref>
                <!-- behavior of "dn" attribute defined here -->
            </attribute>
            <attribute>
                <ref>ri:cn</ref>
                <!-- behavior of "cn" attribute defined here -->
            </attribute>
            ...
        </objectType>
    </schemaHandling>
</resource>
```

Рисунок 7 – Пример описания класса объекта в схеме ресурса

Секция **schemaHandling** также может быть использована для дополнения (или переопределения) некоторых частей схемы ресурса. Например, в примере на рисунке 8 задаётся отображаемое имя для данного класса объекта. Это имя будет выведено в веб-интерфейсе при отображении УЗ.

```
<resource oid="b4101662-7902-11e6-9f14-53e18426fe81">
    <name>My LDAP Server</name>
    ...
    <schemaHandling>
        <objectType>
            <kind>account</kind>
            <displayName>Default account</displayName>
            <default>true</default>
            <objectClass>ri:inetOrgPerson</objectClass>
        </objectType>
    </schemaHandling>
</resource>
```

Рисунок 8 – Пример расширения секции schemaHandling

6.1.3. Роль

6.1.3.1. Общие сведения

IDM CAE реализует идею управления доступом на основе ролей – Role-Based Access Control. Она заключается в том, что права объединяются в роли, роли назначаются пользователям.

IDM CAE поддерживает все обычные возможности RBAC, такие как: иерархия ролей, автоматическое назначение ролей, определение прав доступа и т. д.

Роли могут быть **условными**, тогда одна роль включается в другую роль, но только в том случае, если выполняется определенное условие.

Роли могут быть **параметрическими**, тогда роль может определять конкретный набор прав на основе данных пользователя или параметра назначения роли.

Рассмотрим пример использования параметрических ролей. Работники организации объединены в команды. Каждая команда может иметь руководителя и рядовых членов. Членство в команде представлено пользовательскими атрибутами на сервере LDAP. У каждого пользователя есть два пользовательских многозначных атрибута: *exampleTeamMember* и *exampleTeamManager*. Оба атрибута предполагают в качестве значения имя команды.

При использовании параметрических ролей будет только две роли: член команды и менеджер команды. Эти роли будут принимать в качестве параметра пользовательское свойство *teamName*. Это свойство берётся из расширения назначения. Каждый раз, когда

назначается роль команды, в назначении должен присутствовать параметр (рисунок 9).

```
<user>
    <name>alice</name>
    ...
    <assignment>
        <extension>
            <exmpl:teamName>x-force</exmpl:teamName>
        </extension>
        <!-- Team Manager role -->
        <targetRef oid="aaa6cde4-0471-11e9-9b50-c743da469067" type="RoleType"/>
    </assignment>
</user>
```

Рисунок 9 – Параметры при назначении роли

Также должен использоваться параметр *teamName* в объекте роли (рисунок 10).

```
<role oid="aaa6cde4-0471-11e9-9b50-c743da469067">
    <name>Team Manager</name>
    ...
    <inducement>
        <construction>
            <!-- OpenLDAP resource -->
            <resourceRef oid="8a83b1a4-be18-11e6-ae84-7301fdab1d7c"/>
            <kind>account</kind>
            <attribute>
                <ref>ri:exampleTeamManager</ref>
                <outbound>
                    <expression>
                        <path>$assignment/extension/teamName</path>
                    </expression>
                </outbound>
            </attribute>
        </construction>
    </inducement>
</user>
```

Рисунок 10 – Объект роли с учётом параметров

Результирующая УЗ LDAP будет выглядеть так, как представлено на рисунке 11.

```
dn: uid=alice,ou=people,dc=example,dc=com
objectclass: inetOrgPerson
...
exampleTeamManager: x-force
...
```

Рисунок 11 – Результирующая УЗ LDAP

Процесс показан на рисунке 12.

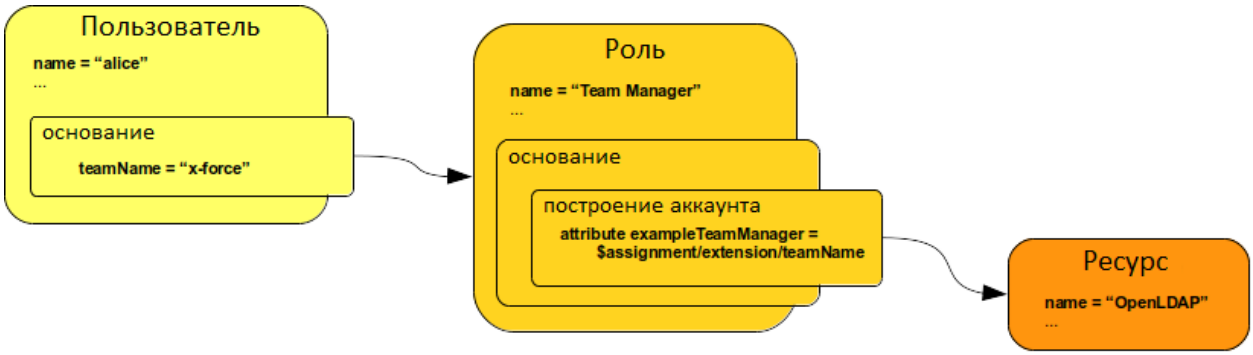


Рисунок 12 – Использование параметрической роли

Роль имеет следующую структуру, представленную на рисунке 13. Как и любой объект, роль имеет OID и имя. В остальной части роли обычно указываются привилегии, которые эта роль предоставляет пользователям.

```
<role oid="aaa6cde4-0471-11e9-9b50-c743da469067">
    <name>Business Analyst</name>
    ...
</user>
```

Рисунок 13 – Объект роли (1)

Назначение роли производится через тег **assignment**. Объект пользователя с назначенной ролью в этом случае выглядит так, как представлено на рисунке 14. Пользователю назначена роль **Business Analyst**. При назначении используется стиль объектных ссылок в IDM CAE, ссылающийся на роль по её OID. Назначение остается неизменным в случае переименования роли или пользователя.

```
<user>
    <name>alice</name>
    ...
    <assignment>
        <targetRef oid="aaa6cde4-0471-11e9-9b50-c743da469067" type="RoleType"/>
    </assignment>
</user>
```

Рисунок 14 – Назначение роли

Назначение – это связь между пользователем и ролью. Назначения имеют несколько свойств:

- **назначения могут иметь срок действия**. Это может использоваться для назначения ролей на временный период. Это также может использоваться для назначения ролей, которые будут активированы в будущем (рисунок 15);

```
<user>
    <name>bob</name>
    ...
    <assignment>
        <!-- Deputy Cheerleader role -->
        <targetRef oid="0c87d8f8-c9a4-11e9-81b8-e7d43e9f9a2b" type="RoleType"/>
        <activation>
            <validTo>2019-12-31T23:59:59Z</validTo>
        </activation>
    </assignment>
</user>
```

Рисунок 15 – Пример назначения роли на время

- **назначения имеют административный статус**. Статус может быть использован для ручного отключения или включения конкретного назначения. Это может быть использовано для управления исключениями из политик или может быть очень полезно в чрезвычайных ситуациях;
- **назначения могут содержать параметры**. Параметры используются для поддержки параметрических ролей;
- **назначения подчиняются политикам, механизмам управления и соответствия**. Назначения имеют свой

жизненный цикл, они подвергаются кампаниям переаттестации, для них могут быть зарегистрированы исключения из политики и т. д.

В одном пользователе может сочетаться множество типов и вариантов назначений. Сроки действия назначений могут пересекаться, для одной и той же роли могут быть одновременно отключённые и включённые назначения, может быть несколько назначений на одну и ту же роль с различными параметрами и т.д.

В IDM CAE поддерживаются различные комбинации, что позволяет моделировать очень сложные схемы, такие как мультиаффилированность, несколько трудовых договоров и т. д.

Назначение ролей в IDM CAE автоматизировано. Роль должна определять все привилегии, которые необходимы пользователям этой роли. Поэтому объект роли **Business Analyst** может выглядеть так, как представлено на рисунке 16. Как правило, каждый работник должен иметь базовый доступ к функционалу компании. В дополнение к базовой УЗ LDAP бизнес-аналитикам необходим доступ к CRM системе. Роль объединяет все привилегии (УЗ), необходимые бизнес-аналитику. Когда эта роль будет назначена пользователю, IDM CAE обработает все части определения роли и применит их к пользователю так, как если бы всё было указано в назначении пользователя.

```
<role oid="aaa6cde4-0471-11e9-9b50-c743da469067">
    <name>Business Analyst</name>
    <inducement>
        <construction>
            <!-- OpenLDAP resource -->
            <resourceRef oid="8a83b1a4-be18-11e6-ae84-7301fdab1d7c"/>
            <kind>account</kind>
        </construction>
    </inducement>
    <inducement>
        <construction>
            <!-- CRM resource -->
            <resourceRef oid="04afeda6-394b-11e6-8cbe-abf7ff430056"/>
            <kind>account</kind>
        </construction>
    </inducement>
</user>
```

Рисунок 16 – Объект роли (2)

Политика предписывает наличие двух УЗ, но в реальности таких записей нет. Поэтому IDM CAE создаёт УЗ. IDM CAE также создает соответствующие теневые объекты и связывает их с пользователем.

Алгоритм назначения роли пользователю представлен на рисунке 17.

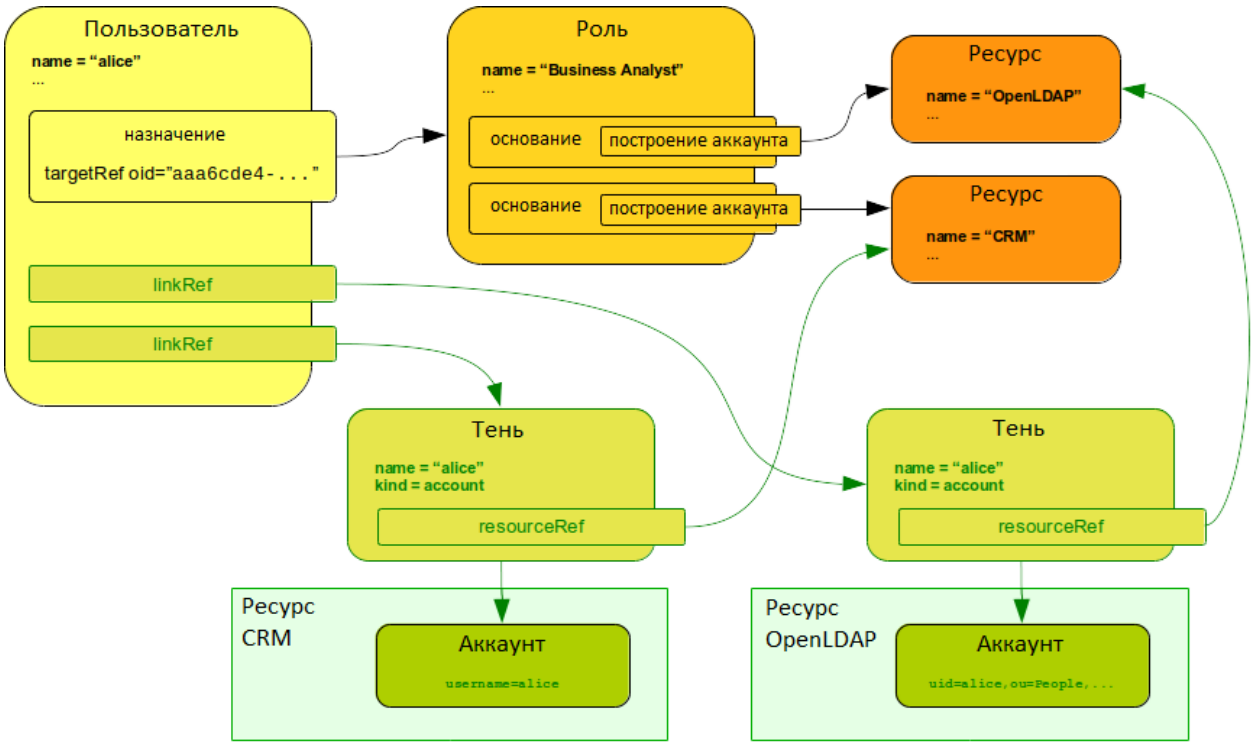


Рисунок 17 – Алгоритм назначения роли пользователю

6.1.3.2. Особенности представления ролей

Представление ролей может содержать исходящие маппинги, которые используются для настройки атрибутов УЗ; пример такого представления роли приведён на рисунке 18. При назначении указанной роли пользователю будет создана УЗ на сервере OpenLDAP. УЗ будет инициализирована обычным образом. Для настройки УЗ будут применены все исходящие маппинги из определения ресурса. Но есть одно отличие – роль задаёт один дополнительный маппинг для УЗ. Этот маппинг будет включён в набор обычных маппингов УЗ при её инициализации. Таким образом, для УЗ будет установлен атрибут Business Analyst.

```
<role oid="aaa6cde4-0471-11e9-9b50-c743da469067">
    <name>Business Analyst</name>
    <inducement>
        <construction>
            <!-- OpenLDAP resource -->
            <resourceRef oid="8a83b1a4-be18-11e6-ae84-7301fdab1d7c"/>
            <kind>account</kind>
            <attribute>
                <ref>ri:title</ref>
                <outbound>
                    <expression>
                        <value>Business Analyst</value>
                    </expression>
                </outbound>
            </attribute>
        </construction>
    </inducement>
    ...
</role>
```

Рисунок 18 – Представление роли, содержащее исходящий маппинг

6.1.3.3. Способы задания атрибутов ролей

IDM CAE поддерживает несколько способов задания атрибутов ролей:

- **общие и обычные значения атрибутов**, задающиеся исходящими маппингами в определении ресурса (schemaHandling);
- **специфичные атрибуты**, определяющиеся в самих ролях.

В тот момент, когда IDM CAE собирается создать УЗ, все маппинги обрабатываются вместе. Несколько ролей могут иметь маппинги для одной и той же УЗ. Все эти маппинги от всех таких ролей добавляются к маппингам, указанным в определении ресурса, и используются для вычисления конечных значений атрибутов УЗ.

Большинство атрибутов УЗ являются однозначными. Попытка задать более одного значения для такого атрибута приведёт к ошибке. Поэтому не имеет смысла задавать более одного маппинга

для такого атрибута. Маппинг может быть задан в ресурсе или в роли, но только одно из них должно быть активным в конкретный момент времени.

Однако, некоторые атрибуты являются многозначными. В этом случае IDM CAE объединяет значения из всех маппингов. В этом случае несколько ролей могут внести свой вклад в конечный набор значений атрибутов, как и маппинги в определении ресурса.

Назначенные роли объединяются вместе, то есть объединяются с исходящими маппингами, права доступа объединяются и т. д.

Например, не существует простого способа, как одна роль может «устранить» значение атрибута, заданное другой ролью. Если роль указывает, что атрибут УЗ должен иметь значение A, то этот атрибут будет иметь значение A. Он также может иметь значения B и C, заданные другими ролями. Но значение A будет всегда, независимо от того, что делают другие роли.

6.1.3.4. Иерархия ролей

Иерархия ролей – это набор оснований между ролями. На рисунке 19 приведено представление роли *Clerk*, на рисунке 20 – роли *Supervisor*.

Основание включает роль *Clerk* в роль *Supervisor*. Когда IDM CAE оценивает роль *Supervisor*, будут получены все основания от ролей *Supervisor* и *Clerk*, включая все маппинги. Таким образом, *Supervisor* получит все те же привилегии (УЗ), что и *Clerk*, плюс несколько дополнительных привилегий (рисунок 21).

```
<role oid="48d4ef98-20e3-46ab-cd78-548d38364a6b">
    <name>Clerk</name>
    <!-- Privileges needed to do clerk's work will be here. -->
</role>
```

Рисунок 19 – Представление роли Clerk

```
<role oid="86e58643-d5e7-36a8-04f6-38dc3754f04e">
    <name>Supervisor</name>
    <!-- Privileges that are unique to supervisor's work will be here. -->
    <inducement>
        <!-- This "includes" all the clerk's privileges in this role -->
        <targetRef oid="48d4ef98-20e3-46ab-cd78-548d38364a6b" type="RoleType"/>
    </inducement>
</role>
```

Рисунок 20 – Представление роли Supervisor

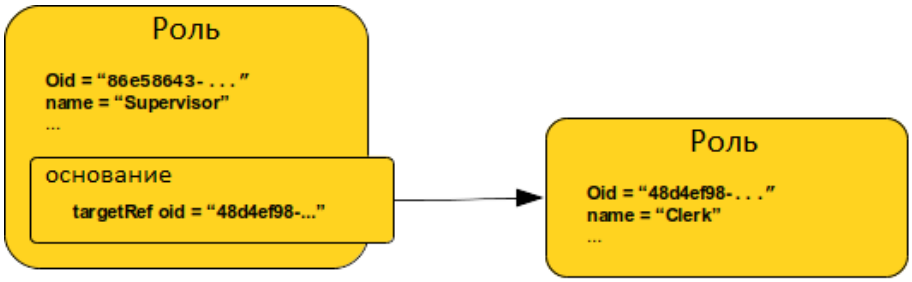


Рисунок 21 – Наследование привилегий роли

Поскольку назначение и основание фактически являются одной и той же структурой данных, аналогичный подход может быть использован и для отключения частей иерархии ролей (рисунок 22).

```
<role>
    <name>Marketing Research Undersecretary</name>
    ...
    <indudement>...</indudement>
    <indudement>...</indudement>
    ...
    <indudement>
        <description>
            Employee access to the lab is disabled because the lab burned down
            during an ugly accident. Will be re-enabled when the lab is rebuilt.
        </description>
        <!-- Experimental Research Lab Access role -->
        <targetRef oid="e8ef819c-c9a4-11e9-80a8-1bddb446391e" type="RoleType"/>
        <activation>
            <administrativeStatus>disabled</administrativeStatus>
        </activation>
    </inducement>
</user>
```

Рисунок 22 – Пример отключения частей иерархии ролей

Существует несколько способов построения иерархии ролей. Один из них – создание всех ролей как ролей конечного пользователя, которые должны быть непосредственно назначены пользователю. Примером такого случая может служить назначение ролей Clerk и Supervisor одному пользователю. В таком примере реализован принцип объединения ролей низкого уровня в роли более высокого уровня, и такое объединение может продолжаться до тех пор, пока не появятся роли, которые необходимы пользователю (рисунок 23).

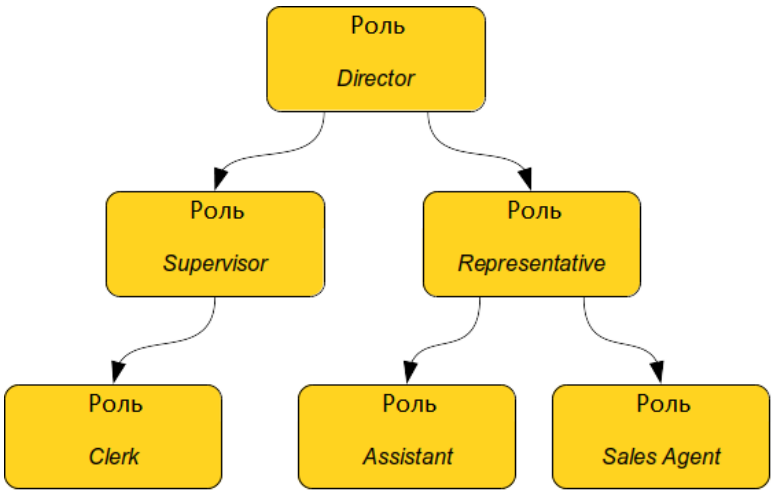


Рисунок 23 – Иерархия ролей

В IDM CAE существует также другой способ организации ролей. Например, роли низкого уровня могут создаваться как прикладные (роли с архетипом Application role). Эти роли связаны с доступом к одному ресурсу, но они не предназначены для прямого назначения пользователям. Они должны быть абстрактными, являться базовым материалом для создания других ролей. Такие роли более высокого уровня часто называют бизнес-ролями (ролями с архетипом Business role), поскольку они отражают потребности бизнеса, например,

конкретную работу или ответственность в бизнес-процессе. Эти роли назначаются пользователям.

Одной из серьезных проблем рассмотренного выше способа являются прикладные роли. Их обычно огромное количество, и их приходится поддерживать вручную. Обычно для каждой привилегии в ресурсе существует своя прикладная роль, для каждой группы – своя организационная единица и так далее. Прикладные роли дублируют информацию, которая уже присутствует на стороне ресурса. А поскольку прикладные роли поддерживаются вручную, то почти наверняка эта информация станет противоречивой.

6.1.3.5. Метароли

Роли могут быть применены практически к любому объекту IDM CAE (к пользователям, организационным единицам, службам и даже к самим ролям.

Обычная роль применяет свои характеристики к пользователю. **Метароль** применяет свои характеристики к другой роли, а не к пользователю. Роли, организационные единицы, сервисы и другие ролевые объекты, как правило, достаточно похожи. Поэтому к ним могут быть применены метароли. Вместо дополнения в таком случае используется назначение (рисунок 24, 25).

```
<role oid="6924fb9c-a184-11e9-840e-2feb476335f4">
    <name>Account Manager</name>
    <description>
        This is business role that corresponds to account manager job.
    </description>
    <assignment>
        <!-- Metarole assignment -->
        <targetRef oid="a3065910-a183-11e9-835c-0b6edc3d44c3" type="RoleType"/>
    </assignment>
    <inducement>
        <!--
             Privileges specific to account manager.
        -->
    </inducement>
</role>
```

Рисунок 24 – Применение метароли

```
<role oid="a3065910-a183-11e9-835c-0b6edc3d44c3">
    <name>Business metarole</name>
    <inducement>
        <!--
            Policies and constructions that should be applied to all
            business roles.
        -->
    </inducement>
</role>
```

Рисунок 25 – Представление метароли

6.1.4. Коннектор

6.1.4.1. Общие сведения

Коннектор – часть системы, используемая для связи с ресурсом. Для работы каждого ресурса необходим коннектор. Коннектор представляет собой специальный программный интерфейс, которые позволяют IDM CAE взаимодействовать с различными ресурсами (БД, приложения, службы каталогов и др.). Они служат связующими звеньями между IDM CAE и этими ресурсами, обеспечивая обмен информацией о пользователях, их правах доступа и других идентификаторах.

К основным функциям коннекторов относятся:

- **синхронизация данных**: коннектор позволяет синхронизировать данные между IDM CAE и ресурсом. Например, при изменении информации о пользователе в одной ИС эти изменения могут автоматически передаваться в другую ИС через коннектор;
- **импорт / экспорт пользователей**: коннекторы могут использоваться для импорта новых пользователей из ресурсов или экспорта существующих пользователей в другие ИС. Это особенно полезно при миграции данных или настройке нового IDM-решения;
- **управление доступом:** через коннекторы система IDM CAE может управлять правами доступа пользователей к различным ресурсам. Например, когда пользователь получает новый доступ в одной ИС, этот доступ может быть автоматически предоставлен и в других связанных ИС;
- **аудит и отчётность**: коннекторы помогают собирать информацию об изменениях, сделанных пользователями, и предоставлять отчёты для аудита безопасности. Это важно для соблюдения нормативных требований и обеспечения безопасности данных.

При запуске компонент Provisioning Management ищет доступные коннекторы и автоматически создаёт новый объект конфигурации для каждого обнаруженного коннектора (объект коннек-

тора). Перейти к просмотру обнаруженных коннекторов можно через список объектов, установив предварительно в фильтре **Type** значение **Connector** (подробнее см. в разделе 6.1.1).

Пример объекта коннектора представлен на рисунке 26.

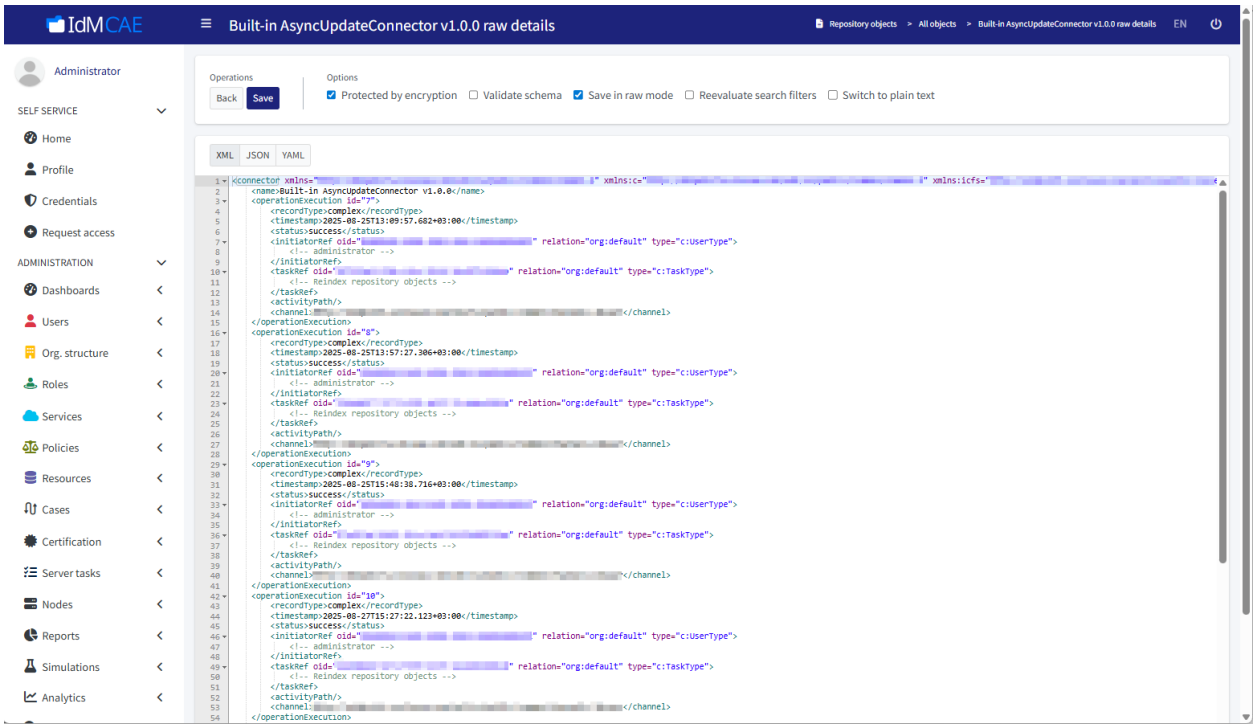


Рисунок 26 – Объект коннектора

Определение ресурса указывает на соответствующий объект коннектора, в качестве указателя используется OID (рисунок 27), однако IDM CAE создаёт объекты коннекторов автоматически, поэтому OID объектов коннектора не являются фиксированными. В итоге каждый экземпляр IDM CAE будет иметь различные OID для обнаруженных коннекторов. Вместо фиксированного OID можно использовать поисковый фильтр (рисунок 28).

```
<resource>
    <name>My LDAP Server</name>
    <connectorRef oid="028159cc-f976-457f-be70-9e9fa079bcf7"/>
    ...
</resource>
```

Рисунок 27 – Определение ресурса с фиксированным OID объекта коннектора

```
<resource>
    <name>My LDAP Server</name>
    <connectorRef type="ConnectorType">
        <filter>
            <q:equal>
                <q:path>connectorType</q:path>
                <q:value>[illegible]</q:value>
            </q:equal>
        </filter>
    </connectorRef>
    ...
</resource>
```

Рисунок 28 – Определение ресурса с поисковым фильтром вместо фиксированного OID

6.1.4.2. Схема коннектора

Схема коннектора – это определение свойств, которые поддерживает коннектор: их имена, типы, кратность и т. д. Схема коннектора хранится в объекте конфигурации коннектора под тегом **schema**.

Схема коннектора также определяет пространство имён коннектора. Свойства коннектора определяются по пространству имен (рисунок 29).

```
<resource oid="690f9f44-8027-11e6-a248-3b5fe08dea36">
    <name>LDAP Minimal</name>
    <connectorRef oid="028159cc-f976-457f-be70-9e9fa079bcf7"/>
    <connectorConfiguration
            xmlns:icfc="[illegible]"
            xmlns:icfcldap="[illegible]">
        <icfc:configurationProperties>
            <icfcldap:port>389</icfcldap:port>
            <icfcldap:host>localhost</icfcldap:host>
            <icfcldap:baseContext>dc=example,dc=com</icfcldap:baseContext>
            ...
        </icfc:configurationProperties>
    </connectorConfiguration>
    ...
</resource>
```

Рисунок 29 – Схема коннектора

Схема описывает, как выглядят объекты в ресурсе. Например, схема может определить, что ресурс поддерживает классы объектов *УЗ* и *группа*. Объекты *УЗ* имеют атрибуты *fullName* и *homeDir*, при этом *fullName* является обязательным, а *homeDir* – дополнительным. Объекты групп имеют многозначный атрибут *members*.

Каждый ресурс может иметь свою собственную схему. Некоторые ресурсы имеют фиксированную схему, то есть схема всегда будет одинаковой, независимо от того, с каким ресурсом коннектор взаимодействует. В этом случае схема может быть жёстко закодирована в коннекторе, и коннектор всегда будет возвращать одну и ту же схему.

Однако многие ресурсы достаточно гибки. Схема может изменяться в зависимости от конфигурации ресурса. Например, LDAP-сервер может иметь расширения схемы, которые определяют совершенно произвольные атрибуты. Схема Active Directory изменяется, если установлен Exchange. Схема ресурсов БД зависит от структуры таблицы БД, с которой они взаимодействуют.

6.1.4.3. Список коннекторов

Для каждого класса ресурсов подходит свой коннектор. В IDM CAE есть несколько универсальных коннекторов:

- **LDAP Connector bundle**, содержащий:
  - LDAP-коннектор, работающий с большинством LDAPv3-совместимых серверов;
  - коннектор Active Directory, работающий с Microsoft Active Directory по протоколу LDAP;

- набор коннекторов **DatabaseTable** с коннектором, позволяющим подключаться к общим таблицам реляционных БД;
- **CSV-коннектор** для работы с текстовыми файлами, разделенными запятыми.

6.1.5. Организационная единица

6.1.5.1. Общие сведения

Организационная единица – это базовый элемент организационной структуры, ведущейся в IDM CAE, с классом объекта **org**. В качестве организационной единицы может выступать компания, подразделение, отдел, секция, команда, географическое положение и т. д.

Организационные единицы могут использоваться для создания иерархических структур. Для просмотра существующей организационной структуры в виде дерева выберите **Org.structure -> Organization tree** в разделе **ADMINISTRATION** (рисунок 30), в виде списка – **Org.structure -> All organization** в том же разделе (рисунок 31).

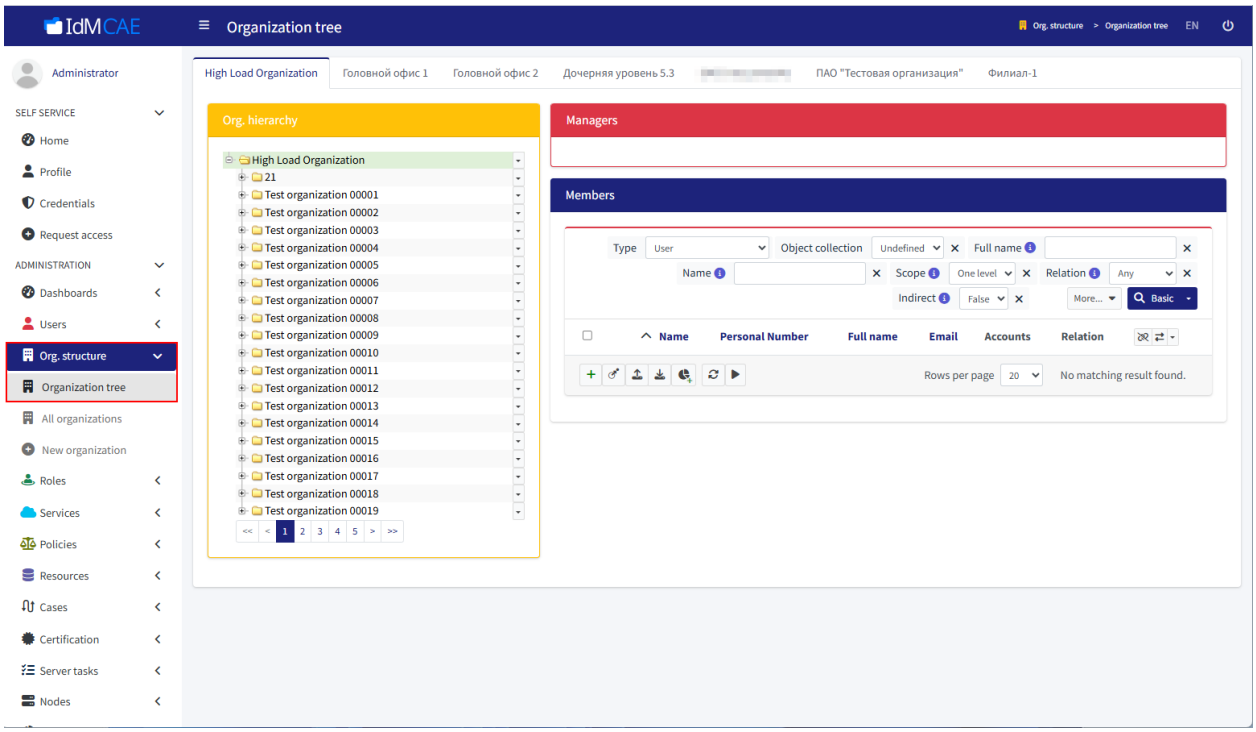


Рисунок 30 – Представление организационной структуры в виде дерева

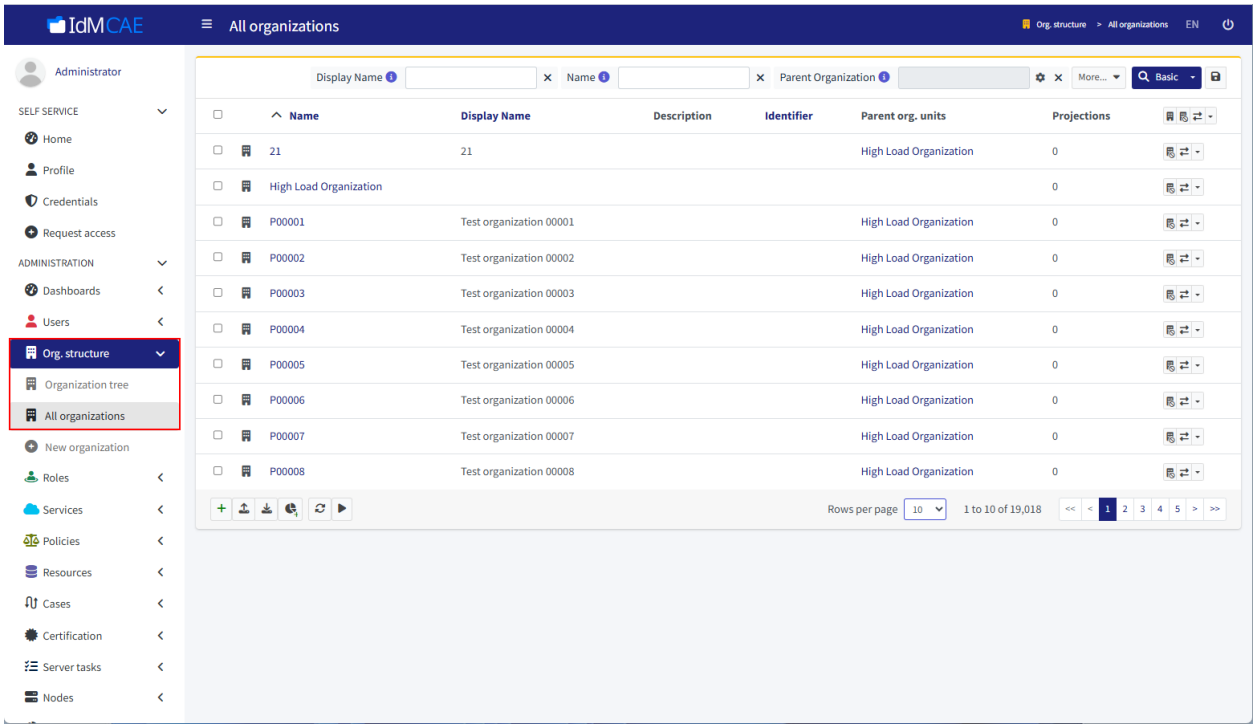


Рисунок 31 – Представление организационной структуры в виде списка

Пример представления организационной единицы представлен на рисунке 32. Имя организационной единицы должно быть

уникальным, так как имена организационных единиц фактически являются идентификаторами или генерируются автоматически.

```
<org oid="4d12c1ac-440c-11ea-80af-2b314d06ba95">
    <name>F10000</name>
    <displayName>ExAmPLE, Inc.</displayName>
</org>
```

Рисунок 32 – Представление организационной единицы

6.1.5.2. Иерархия организационной структуры

Организационная структура создается путём размещения одних организационных единиц в других организационных единицах. Пример представления организационной единицы, содержащей дополнительный идентификатор **identifier**, необходимый для синхронизации организационных структур, приведён на рисунке 33.

```
<org oid="7a1feb50-471f-11ea-8aab-1b2627541f15">
    <name>F11000</name>
    <description>Expensive people that make money.</description>
    <displayName>Sales and Marketing Division</displayName>
    <identifier>11000</identifier>
</org>
```

Рисунок 33 – Представление организационной единицы с дополнительным идентификатором

При импорте организационной единицы она становится организацией верхнего уровня. Для её перемещения внутрь структуры выполните назначение, как это показано на рисунке 34. В результате организационная единица *Sales* and *Marketing Division* будет помещена внутрь организационной структуры.

```
<org oid="7a1feb50-471f-11ea-8aab-1b2627541f15"
    xmlns='[illegible]'
       xmlns:org='[illegible]'>
    <name>F11000</name>
    <description>Expensive people that make money.</description>
    <displayName>Sales and Marketing Division</displayName>
    <identifier>11000</identifier>
    <assignment>
       <targetRef oid="4d12c1ac-440c-11ea-80af-2b314d06ba95" type="OrgType"/>
    </assignment>
</org>
```

Рисунок 34 – Назначение организационной единицы

Пользователи становятся частью организационных единиц, когда эти единицы назначаются им. Следовательно, и организационные единицы становятся частью других организационных единиц, когда они им назначаются. Каждый тип объекта, который может быть назначен держателем, может быть помещен в организационную структуру путем назначения ему организационной единицы.

Для построение иерархической структуры данных используется ссылка на родительский элемент **parentOrgRef**. *ParentOrgRef* указывает на те организационные единицы, в которых в данный момент состоит объект. Т.е. он отражает только те назначения, которые в данный момент активны и действительны. Поэтому для назначений, срок действия которых истёк или которые ещё не действуют, значение *parentOrgRef* будет отсутствовать.

ParentOrgRef представляет все организационные назначения (как прямые, так и косвенные). Организационные единицы, которые непосредственно назначены пользователям, будут присутствовать

в *parentOrgRef*. Организационные единицы, которые индуцированы в роли, назначенной пользователю, также будут присутствовать в parentOrgRef.

6.1.5.1. Организационные единицы и роли

Организации единицы и роли в IDM CAE имеют много общего. Роли предоставляют привилегии своим членам. Люди, имеющие одну и ту же роль, обычно обладают одинаковым набором привилегий. Люди, относящиеся к одной организационной единице, также часто имеют одинаковые привилегии. Фактически, организационные единицы ведут себя практически так же, как и роли. Поэтому нет необходимости настраивать сложные конфигурации, назначающие членам определённой организационной единицы определенную роль. В качестве роли выступает сама организационная единица. Привилегии, которые нужны членам организационной единицы, могут быть добавлены в саму организационную единицу в виде привилегий.

В примере на рисунке 35 приведено представление организационной единицы Indirect Sales Department. Работникам, входящим в Indirect Sales Department, необходимо предоставить доступ к CRM системе. Одновременно на рисунке 36 приведено представление организационной единицы Agent Management Section, входящей в Indirect Sales Department, работники которой НЕ имеют доступ CRM системе.

```
<org oid="8887e0b0-4726-11ea-96b0-5f5ced221e42">
    <name>F11200</name>
    <description>Suits that talk to other suits that talk to customers.</description>
    <displayName>Indirect Sales Department</displayName>
    <identifier>11200</identifier>
    <assignment>
        <!-- Assignment of parent organizational unit -->
        <targetRef oid="7a1feb50-471f-11ea-8aab-1b2627541f15" type="OrgType"/>
    </assignment>
    <inducement>
        <!-- Inducement that grants CRM privileges to all members of this department -->
        <construction>
            <!-- CRM resource -->
            <resourceRef oid="04afeda6-394b-11e6-8cbe-abf7ff430056"/>
            ...
        </construction>
    </inducement>
</org>
```

Рисунок 35 – Представление Indirect Sales Department

```
<org oid="f5e619a6-4726-11ea-888c-ab25c098d8b3">
    <name>F11210</name>
    <description>People that deal with agents (no James Bond here).</description>
    <displayName>Agent Management Section</displayName>
    <identifier>11210</identifier>
    <assignment>
        <!-- Assignment of parent organizational unit. This creates organizational hierarchy. -->
        <targetRef oid="8887e0b0-4726-11ea-96b0-5f5ced221e42" type="OrgType"/>
    </assignment>
    <inducement>
        <!-- Inducement to parent organizational unit. This creates "inheritance" of privileges.
-->
        <targetRef oid="8887e0b0-4726-11ea-96b0-5f5ced221e42" type="OrgType"/>
    </assignment>
</org>
```

Рисунок 36 – Представление Agent Management Section

6.2. Процессы компонента Provisioning Management

6.2.1. Отношение

Отношение определяет характер связи между двумя объектами. Например, пользователь может быть членом организационной единицы, менеджером проекта или владельцем роли. В таких случаях член, менеджер и владелец– это отношения, которые пользователь может иметь к объекту.

Наиболее распространенным способом использования отношения является его указание в назначении в секции **targetRef**. Пример на рисунке 37 иллюстрирует обычный способ назначения владельца для роли.

```
<user>
    <name>aanderson</name>
    ...
    <assignment>
        <!-- Business Analyst role -->
        <targetRef oid="aaa6cde4-0471-11e9-9b50-c743da469067" type="RoleType" relation="owner"/>
    </assignment>
    ...
</user>
```

Рисунок 37 – Назначение владельца для роли

В IDM CAE существует несколько встроенных отношений, описанных в таблице 2.

Таблица 2 – Виды отношений

№	Отношение	Объект назначения	Описание
1.	default	Все	Наиболее распространенное, неспецифическое отношение к объекту. При использовании с ролью означает, что пользователь имеет эту роль. При использовании с организационными единицами обычно интерпретируется как член (member). Это отношение по умолчанию. Если другое отношение не указано, то используется это отношение
2.	manager	Организационные единицы	Менеджер организационного подразделения, руководитель проекта, руководитель группы и т.д. Обычно наделяет полномочиями лицо (или группу лиц), занимающее лидирующее положение в организации. При этом обычно указываются исполнительные или оперативные привилегии
3.	owner	Роли, организационные единицы	Лицо, ответственное за управление объектом. Часто используется для назначения владельцев ролей, которые отвечают за определение и сопровождение ролей. Может использоваться вместе с организационными единицами для указания спонсора проекта или владельца бизнеса. Указывает лицо, ответственное за управление и принятие политических решений высокого уровня, а не за повседневное управление
4.	approver	Роли, организационные единицы	Лицо, ответственное за принятие решений о членстве в ролях и организациях (модератор). Утверждающие лица обычно

№	Отноше-ние	Объект назначения	Описание
			решают, может ли кто-то иметь роль или быть членом организационной единицы. В отличие от владельцев, утверждающие лица не создают и не изменяют определение роли, не могут изменить роль. Они могут только решать, кто может иметь эту роль, а кто нет
5.	meta	Метароли	Отношение специального назначения, которое иногда используется с метаролями. Метаролевые структуры и политики, которые ими управляют, могут быть упрощены, если отношения «роль-метароль» обозначены специальным образом. Данное отношение разработано специально для этой цели. Не является обязательным

6.2.2. Маппинг

6.2.2.1. Общие сведения

Маппинг — это комплексное решение для преобразования одного значения в другое. Например, маппинг используется для переноса значения фамилии пользователя в атрибут УЗ LDAP. Он также может использоваться совместно с выражениями для формирования сложных преобразований, комбинирования значений из нескольких источников, задания значения на основе условия или выполнения почти любых возможных действий.

Маппинги очень гибкие. Существует возможность указать фиксированные значения, сослаться на другие атрибуты с использованием пути или использовать скрипты.

Можно сказать, что маппинги являются «мозговым центром» всех функций синхронизации, они применяются в структурах ролей и шаблонах объектов, их присутствие можно заметить в продукте повсеместно. Они «осведомлены» не только о значениях источника данных, но также знают, как меняются значения источника, и могут

эффективно отразить эти изменения уже в целевых значениях. Маппинг также знает, какие у него источники и целевые значения, и, следовательно, компенсирует правильные преобразования типов данных.

6.2.2.2. Структура маппинга

Составляющие маппинга представлены в таблице 3.

Таблица 3 – Составляющие маппинга

№	Составляющая	Описание
1.	Имя (Name)	Уникальное имя маппинга, которое используется для идентификации значений, генерируемых этим маппингом. Имя не должно изменяться после его создания
2.	Источник (Source)	Определяет источники данных, из которых маппинг получает информацию. Источником данных для маппинга служат ресурсы, предоставляющие информацию, которую маппинг использует для своей работы. Когда данные в источнике изменяются, маппинг производит пересчёт. Для правильной работы маппингу необходим соответствующий источник. Входящие (**inbound**) маппинги, отвечающие за перенос данных из ИС в IDM CAE, используют ресурсы в качестве источника. Исходящий (**outbound**) маппинг же полагается на IDM CAE как источник данных. Подробнее о типах маппинга см. в разделе 6.2.2.3
3.	Выражение (Expression)	Скрипт или логика, управляющая трансформацией данных. Это наиболее гибкая часть маппинга, позволяющая использовать различные сценарии для обработки данных. Выражения включают в себя логику, позволяющую преобразовать входные данные из источника в форму, соответствующую требованиям цели. Эта логика может варьироваться от простых выражений типа **as is**, которые передают значения без изменений, до подстановки фиксированных значений, генераторов и скриптов. Любые выражения получают переменные в качестве входных данных. Маппинг передаёт источники в выражение в форме переменных. Итоговый результат выражения становится значением, присваиваемым цели маппинга
4.	Условия (Conditions)	Устанавливают правила и ограничения для управления потоком данных. Они определяют, когда и при каких условиях данные будут обрабатываться. Условие маппинга — это механизм, предназначенный для создания маппингов, которые возвращают значения на основе определенного условия. Если условие выполняется, значение передаётся как выходной результат маппинга и записывается в целевой параметр объекта. Если условие не выполнено, значение не передается. Выражение маппинга задаёт значение для записи, тогда как условие определяет, когда именно

№	Составляю-щая	Описание
		это значение будет записано. Условия полезны для записи условных значений в параметры, автоматического назначения ролей и решения других задач
5.	Цель (Target)	Цель маппинга определяет не только направление передачи исходящих данных, но также влияет на их структуру, формат и возможные варианты использования. Связывая параметры с маппингом через цель, она устанавливает типы данных, их количество и допустимые значения. Более того, цель маппинга управляет обработкой изменений и формированием дельт. Определение цели в маппинге происходит аналогично определению источника. Ключевым элементом является путь, который связывает маппинг с целевым объектом.
6.	Дополнительные настройки	Включают различные параметры и ограничения, которые могут влиять на поведение маппинга, такие как временные рамки и специфические условия для обработки данных. Эти компоненты работают вместе, чтобы обеспечить эффективное управление данными в IDM CAE, позволяя проводить интеграцию с различными источниками и настройку процессов обработки информации в соответствии с бизнес-требованиями

6.2.2.3. Типы маппингов

В IDM CAE существуют два основных типа маппингов, описание которых представлено в таблице 4.

Таблица 4 – Типы маппингов

№	Тип маппинга	Описание	Пример использования
1.	Входящий маппинг (Inbound Mapping)	Используются для обработки данных, поступающих из ресурсов в IDM CAE. Они позволяют определять, как данные из источников будут преобразовываться и записываться в IDM CAE.	**Синхронизация:** обновление данных пользователей из другой ИС. **Корреляция:** связывание записей из разных ИС на основе общих атрибутов (подробнее см в разделе 6.2.4)
2.	Исходящий маппинг (Outbound Mapping)	Предназначены для передачи данных из IDM CAE в ресурсы. Они определяют, как данные, хранящиеся в IDM CAE, будут отправляться в другие приложения или БД	**Передача атрибутов**: отправка обновленных данных о пользователях в IDM CAE.

№	Тип маппинга	Описание	Пример использования
			Интеграция с другими сервисами: обмен данными с другими ИС

Каждый тип маппинга может иметь свои настройки и условия, определяющие, когда и как данные будут обрабатываться и передаваться.

6.2.2.4. Атрибуты для маппинга

Атрибут можно определить как отличительный признак или характеристику, которая помогает описать или классифицировать определённые данные. Наиболее часто «маппят» атрибуты, связанные с идентификацией пользователей, их ролями, членством в группах и контактной информацией. Ниже представлены основные категории атрибутов, которые чаще всего подвергаются маппингу:

- идентификаторы пользователей:
  - uid (уникальный идентификатор пользователя в IDM CAE);
  - name (имя пользователя);
  - employeeNumber (номер работника);
- основные атрибуты пользователя:
  - givenName (имя);
  - familyName (фамилия);
  - fullName (полное имя);
  - emailAddress (адрес электронной почты);
  - telephoneNumber (номер телефона);

- организационные атрибуты:
    - organizationalUnit (организационное подразделение);
    - title (должность);
    - employeeType (тип работника);
    - manager (менеджер);
    - locality (местоположение);
- роли и группы:
    - roles (роли пользователя);
    - groups (группы, в которых состоит пользователь);
    - accountType (тип учетной записи);
- статус УЗ:
    - activation/enabled (активация/включение УЗ);
    - activation/validFrom (дата начала действия УЗ);
    - activation/validTo (дата окончания действия УЗ).

6.2.3. Корреляция

Корреляция используется для связывания и объединения данных из различных источников. Корреляция в IDM CAE позволяет сопоставлять информацию о пользователях, ролях и других объектах, чтобы создать целостное представление об их идентификации и доступе.

К основным аспектам корреляции относятся:

- связывание данных: корреляция позволяет связывать данные из разных ИС на основе общих атрибутов;

- сопоставление информации: помогает сопоставлять информацию о пользователях, ролях и других объектах;
- создание целостного представления: корреляция используется для создания единого представления об идентификации и доступе пользователей.

6.2.4. Симуляция

6.2.4.1. Общие сведения

Симуляция в IDM CAE — это функция, позволяющая проводить «what-if»-анализ, чтобы оценить ожидаемые последствия действий без риска повреждения состояния IDM CAE. Это особенно полезно при тестировании новых конфигураций ресурсов или при внесении изменений в настройки управления доступом.

Симуляция в IDM CAE позволяет администраторам и разработчикам безопасно тестировать изменения и оптимизировать процессы управления идентификацией и доступом, минимизируя риски для производственных данных.

Ниже представлены основные аспекты симуляции в IDM CAE:

- режимы выполнения:
    - полное выполнение: все вычисленные изменения применяются с постоянными эффектами;
    - симуляция (или предварительный просмотр): изменения только моделируются, без реального воздействия на данные в IDM CAE или на ресурсах;

    - симуляция управления тенями: специальная низкоуровневая симуляция изменений, связанных с классификацией и корреляцией теней;
- результаты симуляции: симуляция создаёт специальные объекты результатов, которые собирают информацию о наблюдаемых объектах и вычисленных изменениях. Эти результаты могут включать метрики, предоставляющие общее представление о проведенной симуляции;
- типичные сценарии использования:
    - введение новой конфигурации ресурса: позволяет безопасно настраивать и тестировать определения ресурсов перед их применением в производственной среде;
    - корреляция объектов: упрощает связывание объектов ресурсов с объектами фокуса (например, пользователями или ролями) без риска изменения данных.

6.2.4.2. Типы симуляции

В IDM CAE симуляции делятся на два ключевых типа, которые определяются режимом выполнения и конфигурацией:

- симуляция с постоянными эффектами (Persistent-Effects Mode):
    - действия, выполненные в рамках этой симуляции, сохраняют изменения в IDM CAE;

    - используется для тестирования изменений, которые должны быть внедрены в продуктивной среде;
- симуляция без постоянных эффектов (Simulation Execution Mode):
    - действия не приводят к реальным изменениям в IDM CAE;
    - применяется для анализа «what-if» без риска повредить состояние IDM CAE.

6.2.4.3. Конфигурации симуляции

В IDM CAE есть две конфигурации симуляции:

- производственная конфигурация (Production Configuration): используется для тестирования сценариев, которые будут применяться в реальной среде;
- конфигурация разработки (Development Configuration): позволяет тестировать новые функции или изменения в контролируемой среде перед их внедрением.

6.2.5. Синхронизация

При работе в IDM CAE часто можно столкнуться с понятием **синхронизация**. Синхронизация – это обобщающий термин, используемый для описания нескольких связанных механизмов в IDM CAE. Все механизмы синхронизации имеют одну и ту же цель: убедиться, что информация в IDM CAE и реальное состояние ресурсов соответствуют друг другу.

Репозиторий IDM CAE содержит информацию о том, в каком состоянии должны находиться:

- назначенные ресурсам УЗ и роли;
- значения атрибутов, полученные из свойств пользователя;
- другие сущности.

Однако фактическое положение УЗ может быть иным. Некоторые УЗ, которые должны существовать, могут вовсе отсутствовать, потому что операция создания завершилась ошибкой или кто-то удалил их. УЗ могут принадлежать к неправильному набору групп и не соответствовать ролям. Могут существовать УЗ, которые никому не принадлежат и являются «осиротевшими».

Синхронизация – это согласование состояния, которое должно быть (назначения, роли, производные атрибуты), с состоянием, которое есть (реальные атрибуты УЗ).

В IDM CAE используется три разновидности синхронизации:

- provisioning synchronization – распространение изменений из IDM CAE в целевые ИС;
- live synchronization – внесение изменений в режиме real-time;
- reconciliation – получение изменений из целевых ИС в IDM CAE.

6.2.6. Реконсиляция

Реконсиляция — это процесс, который позволяет сравнивать и синхронизировать данные между IDM CAE и ресурсами. Этот процесс критически важен для обеспечения целостности данных и актуальности информации о пользователях, ролях и ресурсах.

Реконсиляция начинается с извлечения данных из ресурса и их сравнения с данными в IDM CAE. Если обнаруживаются расхождения, продукт принимает меры для их устранения, что может включать обновление данных в IDM CAE или в ресурсе.

Основная цель реконсиляции заключается в выявлении расхождений между данными в IDM CAE и данными в ресурсах. Это может включать добавление новых пользователей, обновление существующих атрибутов или удаление устаревших УЗ.

Реконсиляция может быть настроена как односторонняя (например, только из ресурса в IDM CAE) или двусторонняя (синхронизация изменений в обе стороны).

Как правило, для настройки реконсиляции необходимо определить правила сопоставления (корреляции) между объектами в IDM CAE и ресурсами. Это может включать в себя использование уникальных идентификаторов (например, sAMAccountName) для пользователей.

После завершения процесса реконсиляции IDM CAE генерирует отчёты о выявленных расхождениях и действиях, предпринятых для их устранения, что позволяет администраторам IDM CAE отслеживать состояние данных.

Наиболее часто подвергаемыми реконсиляции объектами в IDM CAE являются:

- пользователи (Users):
    - атрибуты пользователей (имена, фамилии, логины и адреса электронной почты);

    - статус УЗ (активная, неактивная, заблокированная);
- УЗ (Accounts):
    - связанные с пользователями УЗ в ресурсах (например, Active Directory);
    - атрибуты УЗ (sAMAccountName, пароли и статусы);
- роли (Roles):
    - названия и описания ролей, а также права и привилегии, связанные с ними;
    - членство пользователей в ролях;
- группы (Groups):
    - названия групп и их описания;
    - членство пользователей и ролей в группах;
- ресурсы (Resources):
    - конфигурация ресурсов, включая параметры подключения;
    - статус доступности ресурсов.

6.2.7. Активация

Термин **активация** используется для обозначения набора свойств, описывающих, является ли объект активным. Сюда входят свойства, описывающие, включен ли пользователь, отключён, архивирован, с какого момента он должен быть включён, до какого момента он должен быть активен и т.д.

Наиболее важной концепцией активации является административный статус, т.е. явное решение администратора о том, разблокирован или заблокирован пользователь. Возможные значения административного статуса с описаниями приведены в таблице *5*. Кроме административного статуса, существуют также время действия, статус блокировки, различные временные метки и метаданные.

Таблица 5 – Возможные значения поля Administrative status

№	Значение	Описание
1.	Undefined	Явное переопределение не предусмотрено. Другие свойства активации определяют результирующий статус
2.	Enabled	Объект активен. Он включён и полностью готов к работе
3.	Disabled	Объект неактивен. Он был отключён административным действием. Это означает временную неактивность и намерение включить объект позже
4.	Archieved	Объект неактивен. Он был отключён административным действием. Это означает, что объект отключён навсегда, и нет намерения включить его позже

И у пользователя, и у УЗ есть свойства активации, они практически одинаковы. При активации пользователя и УЗ используются одни и те же имена свойств, их значение и форматы данных. Например, если пользователь отключён, то и все его УЗ должны быть отключены. Активация пользователя и активация УЗ совместимы.

Определение активации выполняется в секции работы со схемой ресурсов (рисунок 38).

```
<resource oid="b4101662-7902-11e6-9f14-53e18426fe81">
    <name>My LDAP Server</name>
    ...
    <schemaHandling>
        <objectType>
            <kind>account</kind>
            <default>true</default>
            <objectClass>ri:inetOrgPerson</objectClass>
            <!-- attribute handling comes here -->
            <activation>
                <administrativeStatus>
                    <outbound/>
                </administrativeStatus>
            </activation>
        </objectType>
    </schemaHandling>
</resource>
```

Рисунок 38 – Определение активации

6.3. Сущности компонента Workflow Management

6.3.1. Пользовательская задача

БП представляет из себя набор шагов, направленных на достижение определённой цели.

Пользовательская задача – это этап БП, который требует участия человека. В отличие от автоматизированных задач, выполняемых сервисами или скриптами, такие задачи предполагают ручной ввод данных, принятие решений или выполнение определённых действий через пользовательский веб-интерфейс.

При моделировании БП пользовательская задача включает в себя:

- назначение исполнителей;
- формы для ввода данных;
- управление переменными;
- контроль сроков выполнения.

Исполнители могут назначаться **статически**, когда задача сразу закрепляется за конкретным пользователем, или **динамически**, когда она становится доступной группе кандидатов и берётся в работу одним из них.

6.3.2. Модели процесса

При моделировании процесса, он становится видимым. Вместо того чтобы держать в голове, кто и когда должен что-то сделать, процесс предоставляет готовую структуру. Это даёт сразу несколько выгод:

- упрощается обучение новых работников;
- устраняется дублирование действий;
- можно увидеть узкие места;
- появляется возможность автоматизации;
- облегчается контроль и аудит.

Моделирование в компоненте исполнения процесса производится с помощью нотации BPMN 2.0.

Для взаимодействия с моделями процессов в компоненте Workflow Management используется система, основанная на XML-формате. Модели процессов, созданные в Camunda Modeler или других инструментах моделирования, хранятся в виде файлов BPMN в каталоге *configuration/resources* на серверах приложений.

В этих файлах хранится основная информация о БП, включая:

- идентификаторы элементов. Уникальные идентификаторы для каждого элемента процесса;

- элементы БП. Задачи (tasks), события (events), шлюзы (gateways) и другие компоненты процесса;
- потоки управления. Определяют порядок выполнения задач и взаимодействие между элементами;
- атрибуты. Дополнительные свойства и параметры, такие как таймеры, условия выполнения, обработчики ошибок и так далее;
- группы и тегирование. Могут быть предусмотрены для организации и документирования элементов процесса.

Пример определения простого процесса в XML-формате выглядит следующим образом:

```
    <?xml version="1.0" encoding="UTF-8"?>
    <definitions
xmlns="http://www.omg.org/spec/BPMN/20100524/MODEL"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:schemaLoca-
tion="http://www.omg.org/spec/BPMN/20100524/MODEL
BPMN20.xsd"
                id="Definitions_1">
        <process id="Process_1" isExecutable="true">
            <startEvent              id="StartEvent_1"
name="Start"></startEvent>
            <sequenceFlow                  id="Flow_1"
sourceRef="StartEvent_1"      targetRef="Task_1"></se-
quenceFlow>
            <task    id="Task_1"    name="Do    some-
thing"></task>
```

```
            <sequenceFlow                    id="Flow_2"
sourceRef="Task_1"  targetRef="EndEvent_1"></sequence-
Flow>
            <endEvent                    id="EndEvent_1"
name="End"></endEvent>
        </process>
    </definitions>
```

Описание содержимого примера:

- <definitions>. Корневой элемент, который определяет пространство имён и связывает процесс со схемой BPMN;
- <process>. Элемент, представляющий модель процесса с уникальным идентификатором;
- <startEvent>. Элемент, обозначающий начало процесса;
- <task>. Задача, которую необходимо выполнить в рамках процесса;
- <sequenceFlow>. Поток управления, указывающий порядок выполнения между элементами;
- <endEvent>. Элемент, обозначающий окончание процесса.

Развёртывание (deployment) – процесс публикации модели процесса в компоненте Workflow Management.

Возможные операции с моделями процессов описаны в разделе 7.2.5.

6.3.3. Экземпляры моделей процессов

Модели процессов фактически являются шаблонами для создания **исполняемых экземпляров моделей процессов**. Так, из одной модели может быть создано сразу несколько исполняемых экземпляров, а в рамках каждого экземпляра может быть создана пользовательская задача, если модель этого процесса это подразумевает.

Исполняемый экземпляр модели процесса – уникальное событие, которое создаётся при каждом выполнении процесса. Каждый исполняемый экземпляр модели процесса работает независимо и имеет потенциально разные данные, состояния и результаты.

Возможные операции с экземплярами моделей процессов описаны в разделе 7.2.6.

7. УПРАВЛЕНИЕ IDM CAE

7.1. Компонент Provisioning Management

7.1.1. Веб-интерфейс Provisioning Management

7.1.1.1. Общее описание

Веб-интерфейс администратора компонента Provisioning Management представляет собой расширенный веб-интерфейс пользователя с добавлением новых разделов **ADMINISTRATION** (1, рисунок 39) и **CONFIGURATION** (2, рисунок 39) слева в меню.

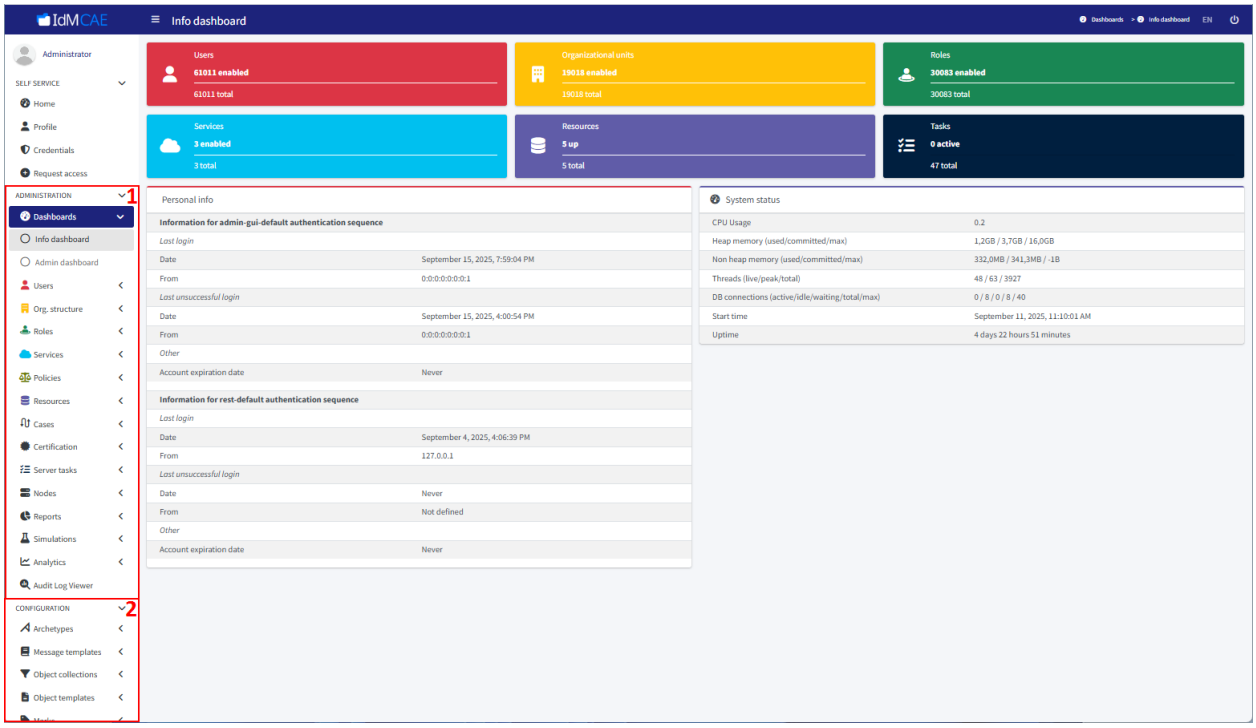


Рисунок 39 – Веб-интерфейс администратора

В веб-интерфейсе используется единая цветовая кодировка, облегчающая навигацию (рисунок 40). Пользователи, роли и другие объекты имеют свой цвет и пиктограмму. Цвет указывает на тип объекта и используется везде, где это возможно: разделы, информационные блоки, списки объектов и т.д. Ниже приведено соответствии цветовой кодировки:

- **красный** – связан с пользователем;

- **оранжевый** – связан с организационной единицей;
- **зелёный** – связан с ролью;
- **голубой** – связан с сервисом;
- **фиолетовый** – связан с ресурсом;
- **чёрный** – связан с задачей.

Рисунок 40 – Цветовая кодировка веб-интерфейса

Аналогичный цветовой код применяется при отображении списка пользователей (рисунок 41), однако используемый там цвет указывает не на тип объекта, а на архетип. Внешний вид и поведение таких объектов настраивается. Стандартная конфигурация содержит всего несколько архетипов, которые отображаются с помощью **красного** цвета. Цвет архетипа указывает на состояние объекта:

- **чёрный** – нормальное состояние;
- **жёлтый** – обозначает наличие возможности управления. Например, пользователи, являющиеся менеджерами организационных подразделений;
- **серый** – неактивное состояние. Означает, что объект отключен, заархивирован или существует другая причина, по которой он неактивен;
- **синий** – обозначает наличие типичного доступа для конечного пользователя. Это означает, что к объекту есть

доступ, но он ограничен только безопасными, непривилегированными операциями. Например, пользователи с ролью конечного пользователя.

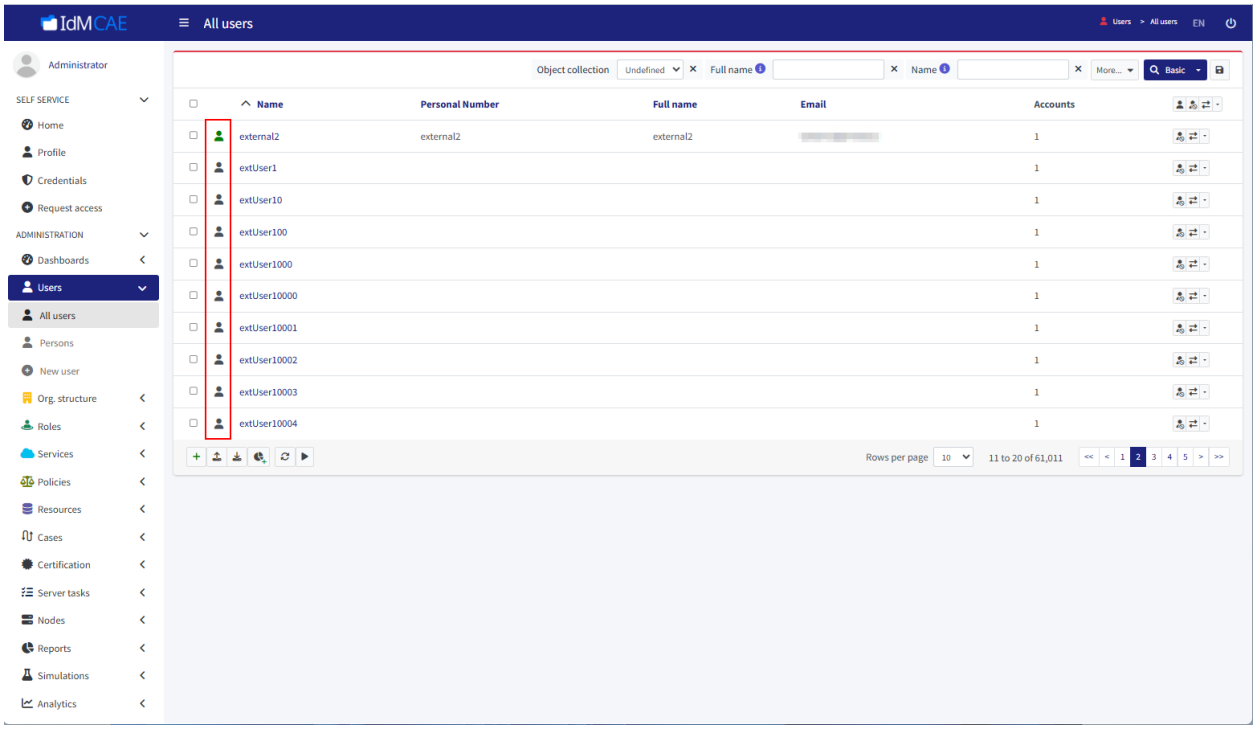


Рисунок 41 – Список пользователей

Раздел **ADMINISTRATION** позволяет управлять УЗ пользователей, организационной структурой, ролями, ресурсами и другими объектами, присутствующими в компоненте Provisioning Management.

Раздел **CONFIGURATION** позволяет осуществлять настройку компонента. Он используется для установки правил и политик, которые представляют собой основу развёртывания IDM CAE.

Раздел **ADMINISTRATION** содержит следующие подразделы:

- **Dashboards**: подраздел представляет собой панели мониторинга, которые отображают ключевую информацию и метрики в визуальном формате. В нём можно

просматривать информацию о пользователях, ролях, сервисах, ресурсах, задачах, об организационных единицах;

- **Users**: подраздел предназначен для управления УЗ и правами доступа пользователей IDM CAE. Здесь администратор может добавлять, редактировать или удалять пользователей, а также назначать им роли и права. Пользователи могут быть сгруппированы с помощью механизма фильтрации по различным критериям для удобного управления. Прозрачность и контроль доступа обеспечивают безопасность данных и IDM CAE в целом;
- **Org. structure**: подраздел отображает иерархию организационной структуры, которая помогает визуализировать то, как различные команды и отделы связаны между собой, а также позволяет управлять структурой в зависимости от изменений в организации. С помощью данного подраздела администратор может вносить изменения в организационную структуру и управлять ролями работников. Информация в этом разделе помогает определить уровни ответственности и исключает путаницу в коммуникациях;
- **Roles**: подраздел позволяет управлять правами и доступом пользователей к различным функциям и ресурсам

IDM CAE. В этом интерфейсе администратор может просматривать существующие роли, создавать новые, назначать им соответствующие разрешения и группировать пользователей по этим ролям. Это обеспечивает гибкость в управлении доступом, а также помогает поддерживать безопасность IDM CAE. Пользователи могут иметь несколько ролей для работы с различными частями IDM CAE;

- **Services**: подраздел предоставляет информацию о доступных в компоненте сервисах и их состояниях. Здесь пользователи могут увидеть активные сервисы, их характеристики и условия использования;
- **Resources**: подраздел содержит список доступных ресурсов. Интерфейс обеспечивает поиск и навигацию по ресурсам IDM CAE. Этот подраздел помогает контролировать, какие ресурсы используются и какие доступны для новых пользователей. Управление ресурсами также включает в себя возможность оценки их использования и производительности. Подраздел содержит информацию о подключённых ИС к IDM CAE;
- **Cases**: подраздел предназначен для управления инцидентами и запросами пользователей. Здесь можно создавать новые запросы, отслеживать их статус и взаимодействовать с другими пользователями для их реше-

ния. Подраздел позволяет систематизировать и упростить процесс обработки запросов, что повышает общую эффективность работы. Фильтры и категории помогают быстро находить нужные запросы. Данный раздел также может использоваться для анализа повторяющихся проблем и разработки стратегий их устранения;

- **Server tasks**: подраздел позволяет отслеживать выполнение фоновых процессов и задач, запущенных на сервере. Здесь отображается информация о существующих задачах, их статусах и возможных ошибках. Данный раздел позволяет отслеживать производительность IDM CAE и выявлять проблемы;
- **Nodes**: подраздел отвечает за управление и отображение нод, которые участвуют в инфраструктуре IDM CAE. Здесь администраторы могут контролировать состояние каждого узла, его загруженность и производительность. Этот интерфейс необходим для мониторинга распределенной системы и управления ресурсами. Визуализация узлов помогает понимать структуру системы и реагировать на возможные сбои;
- **Reports**: подраздел позволяет создавать, просматривать и анализировать различные отчёты по работе IDM CAE. Этот подраздел позволяет настраивать отчёты под

конкретные требования, выводить необходимые метрики и статистику. Компонент Provisioning Management предлагает готовые шаблоны для отчётов, а также возможность создания собственных отчётов. Отчёты могут использоваться для анализа производительности, безопасности и выполнения задач. Экспорт данных помогает делиться отчётами с другими пользователями IDM CAE;

- **Simulations**: подраздел предоставляет возможности для просмотра результатов моделирования сценариев и процессов в компоненте. В нём можно просматривать результаты различных вариантов поведения IDM CAE без воздействия на реальные данные. Этот подраздел позволяет оценивать различные ситуации и находить оптимальные решения. Симуляции помогают улучшить процессы и снизить риски перед внедрением изменений;
- **Audit Log Viewer** подраздел позволяет отслеживать совершённые действия в рамках аудита. Здесь можно фильтровать, сортировать и анализировать различные события, что помогает обеспечивать безопасность IDM CAE. Подраздел полезен для выявления подозрительных действий и контроля соблюдения политики безопасности. Логи могут содержать информацию о пользователях, действиях и временных метках.

Раздел **CONFIGURATION** содержит следующие подразделы:

- **Archetypes**: подраздел позволяет создавать архетипы объектов и управлять архетипами, которые используются в IDM CAE. Здесь можно определять общие характеристики для групп объектов, что упрощает управление ими. Архетипы помогают стандартизировать данные и их представление в IDM CAE. Шаблонами можно делиться и адаптировать их под свои нужды. Данная функциональность важна для структурирования данных и повышения их взаимодействия;
- **Message templates**: подраздел позволяет создавать шаблоны сообщений и управлять теми шаблонами, которые используются в различных коммуникациях IDM CAE. С помощью данного подраздела упрощается процесс отправки сообщений и уведомлений с учётом согласованности. Шаблоны сообщений можно изменять, в том числе включать значения переменных для автоматического заполнения данных, и сохранять их для дальнейшего использования;
- **Object collections**: подраздел предназначен для управления группами объектов в IDM CAE. В этом подразделе можно создавать, редактировать и удалять коллекции, а также добавлять объекты в них. Такой подход упрощает организацию и контроль больших объёмов данных,

позволяя находить необходимую информацию и управлять ей. Для сортировки объектов в коллекциях предусмотрены фильтры и группировка;

- **Object templates**: подраздел предназначен для создания и управления шаблонами объектов. В данном подразделе можно задавать общие параметры и характеристики для объектов, что упрощает создание новых записей и поддержание согласованности данных. Шаблоны объектов могут включать в себя предустановленные поля и значения, что ускоряет процесс работы;
- **Marks**: подраздел позволяет устанавливать отметки для объектов в IDM CAE. Отметки являются полезным инструментом для классификации и быстрой идентификации данных с помощью визуальных индикаторов к объектам, облегчая последующую работу с ними. Это особенно удобно для выделения объектов, требующих внимания или дополнительной обработки. Таким образом, метки помогают улучшить общую организацию данных и повысить их доступность;
- **Actions**: подраздел предоставляет возможность выполнять однотипные операции над несколькими объектами одновременно, что позволяет более быстро и эффективно управлять данными. Подраздел позволяет вы-

бирать множество объектов и применять к ним действия (изменение статуса, удаление или добавление новых свойств и т. д.);

- **Import object**: подраздел позволяет загружать данные из таких источников, как текстовый файл или текст, написанный во встроенном текстовом редакторе. Данные могут быть загружены в различных форматах, что делает универсальной интеграцию информации. Параметры импорта можно настраивать, что обеспечивает правильное сопоставление данных;
- **Repository objects**: подраздел позволяет управлять объектами, хранящимися в IDM CAE, для поддержания целостности и актуальности информации. Для поиска и группировки объектов можно использовать сортировку и фильтрацию. Данный подраздел позволяет получать информацию о статусе объектов, их свойствах и связанных данных, также доступны инструменты для редактирования и удаления объектов;
- **System**: подраздел предоставляет возможность просмотра информации о настройках и конфигурации компонента Provisioning Management. С помощью данного подраздела можно управлять системными параметрами и получать данные о производительности и состояниях компонентов в рамках мониторинга и обслуживания IDM CAE;

- **Internals configuration**: подраздел предоставляет доступ к более подробным техническим настройкам компонента. С помощью данного подраздела можно изменять системное время компонента, проводить отладку работы компонента, просматривать активные системные потоки, что позволяет оптимизировать производительность и безопасность IDM CAE на уровне конфигурации;
- **Query playground**: подраздел позволяет создавать запросы Query API для обращения к компоненту Provisioning Management, транслировать их в запросы на языке SQL и исполнять их в API компонента;
- **About**: подраздел предоставляет информацию об основных настройках развёртывания компонента IDM CAE, таких как: информация о версии сборки компонента, информация о подключённой СУБД, информация о системных настройках и настройках JVM, информация о ноде компонента.

7.1.1.2. Отображение объекта в веб-интерфейсе компонента Provisioning Management

Компонент Provisioning Management поддерживает единый стиль отображения объектов. Объект на примере ресурса представлен на рисунке 42.

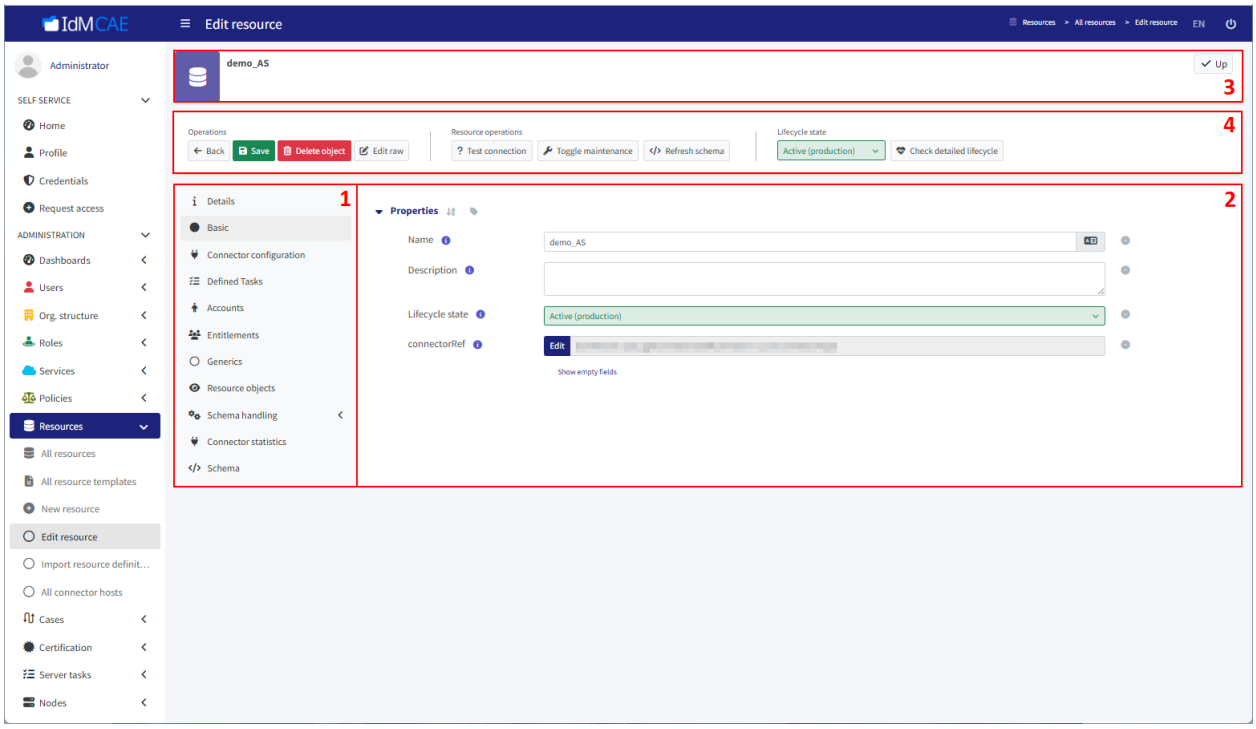
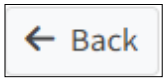


Рисунок 42 – Отображение объекта

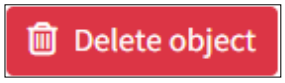
Слева расположена панель со вкладками (1, рисунок 42), содержащими свойства / атрибуты объекта, отражённые в центральной части окна (2, рисунок 42).

Сверху расположена панель (3, рисунок 42) с основной информацией об объекте.

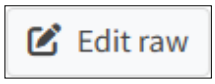
Ниже панели с основной информацией (4, рисунок 42) находится панель с кнопками для управления объектом (набор кнопок отличается в зависимости от типа объекта). Ниже представлено описание кнопок, встречающихся для каждого объекта:

- 

– возврат в предыдущее окно;
- 

– сохранение настроек объекта;
- 

– удаление объекта;

-  – переход к редактированию объекта в .XML-, JSON-, YAML-форматах.

7.1.1.3. Элементы управления объектами в компоненте Provisioning Management

Компонент Provisioning Management поддерживает единые элементы управления над списком объектов. Список объектов на примере организационных единиц представлен на рисунке 43.

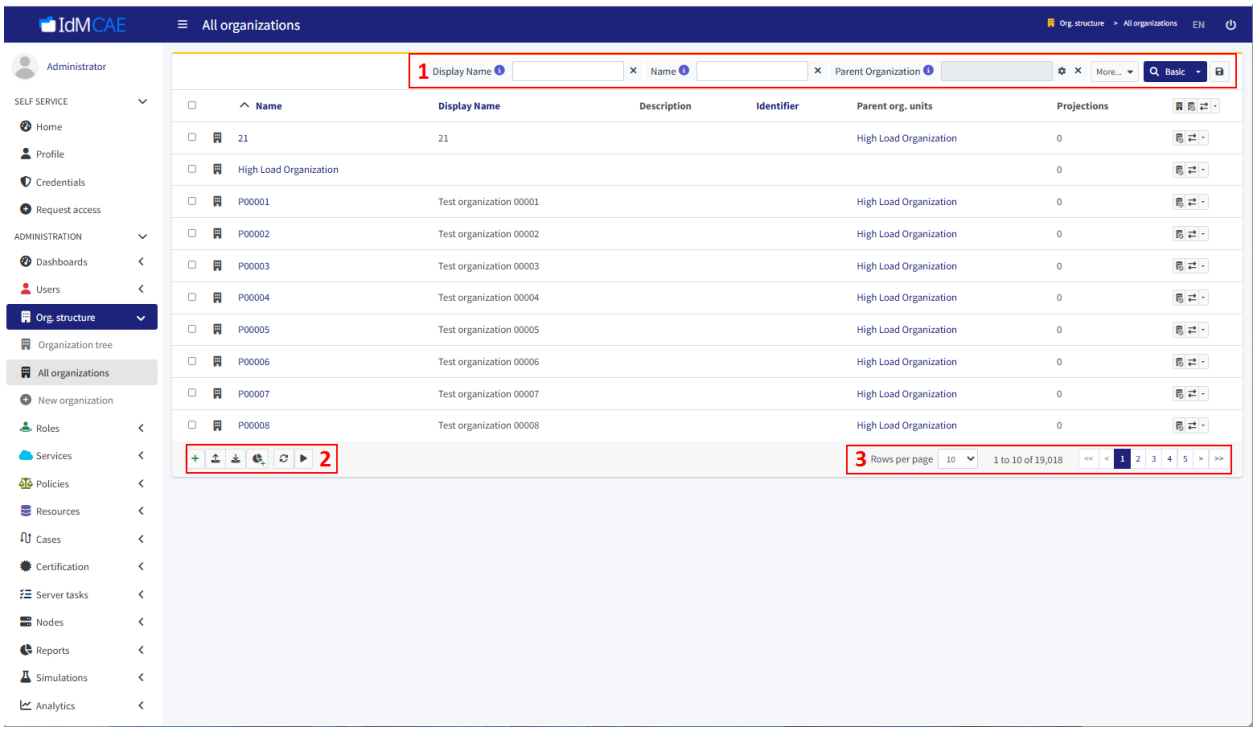


Рисунок 43 – Элементы управления объектами

Над списком объектов расположена панель с фильтрами для удобного поиска (1, рисунок 43). Есть предустановленные фильтры (**Display Name**, **Name**), а также присутствует возможность добавления фильтра с помощью  . Управлять добавленным фильтром можно с помощью  и последующего выбора действия; для удаления добавленного фильтра нажмите на  справа от него. Для использования языка запросов в фильтре переключите режим с **Basic**

на **Advanced** с помощью 

. Для сохранения состояния фильтра используйте  .

Внизу списка объектов расположена панель с элементами управления над списком объектов (2, рисунок 43), ниже представлено их описание:

-  – создание нового объекта;
-  – импорт нового объекта;
-  – экспорт объектов в виде файла;
-  – создание отчёта;
-  – обновление списка объектов;
-  – запуск обновления.

Также в веб-интерфейсе присутствует панель для управления количеством отображаемых объектов (3, рисунок 43). Ниже представлено описание элементов:

- 

– изменение количества отображаемых на странице строк;
-  – переход на первую страницу;
-  – переход на предыдущую страницу;
-  – переход на следующую страницу;
-  – переход на последнюю страницу.

7.1.1.4. Вход в веб-интерфейс компонента Provisioning Management

Для входа в веб-интерфейс компонента Provisioning Management IDM CAE выполните следующие шаги:

1. В адресной строке браузера введите адрес https://<host>/base, где host – адрес сервера, на котором установлен компонент Provisioning Management IDM CAE. После перехода по ссылке отобразится окно аутентификации (рисунок 44).
2. В поле **Username** (1, рисунок 44) введите имя пользователя, в поле **Password** – пароль (2, рисунок 44).
3. Нажмите на **Sign in** (3, рисунок 44).
    a. В случае правильно введённых данных отобразится окно с домашней страницей (рисунок 45).
    b. В случае неправильно введённых данных будет выведена ошибка над окном ввода логина и пароля (рисунок 46). Повторите попытку входа.

При необходимости можно сменить язык, выбрав нужный в выпадающем списке (4, рисунок 44)

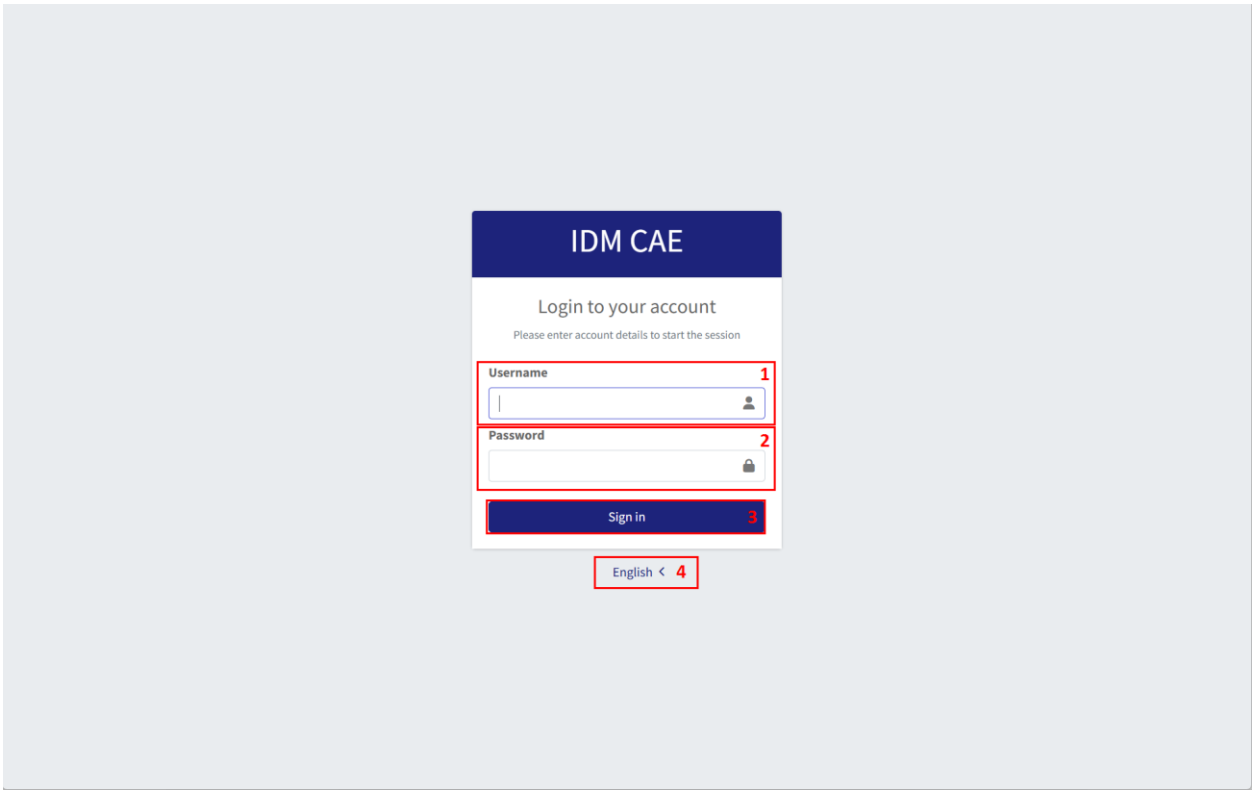


Рисунок 44 – Окно аутентификации компонента Provisioning Management

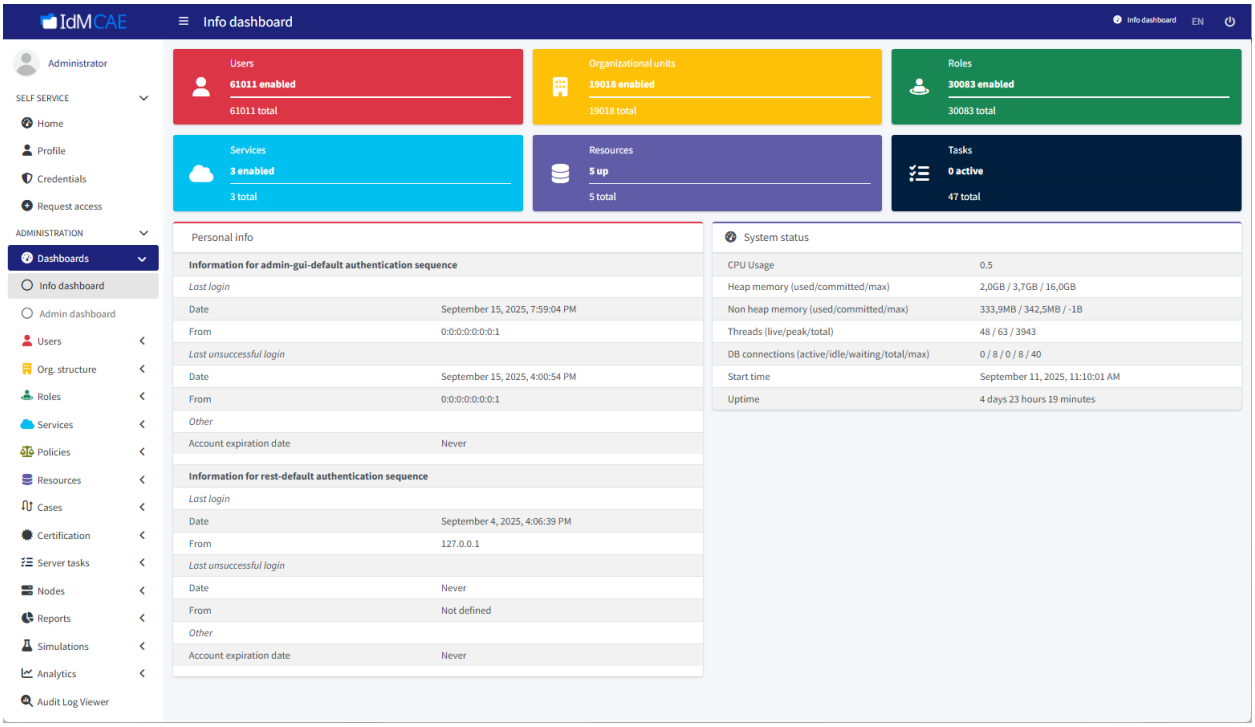


Рисунок 45 – Окно с домашней страницей

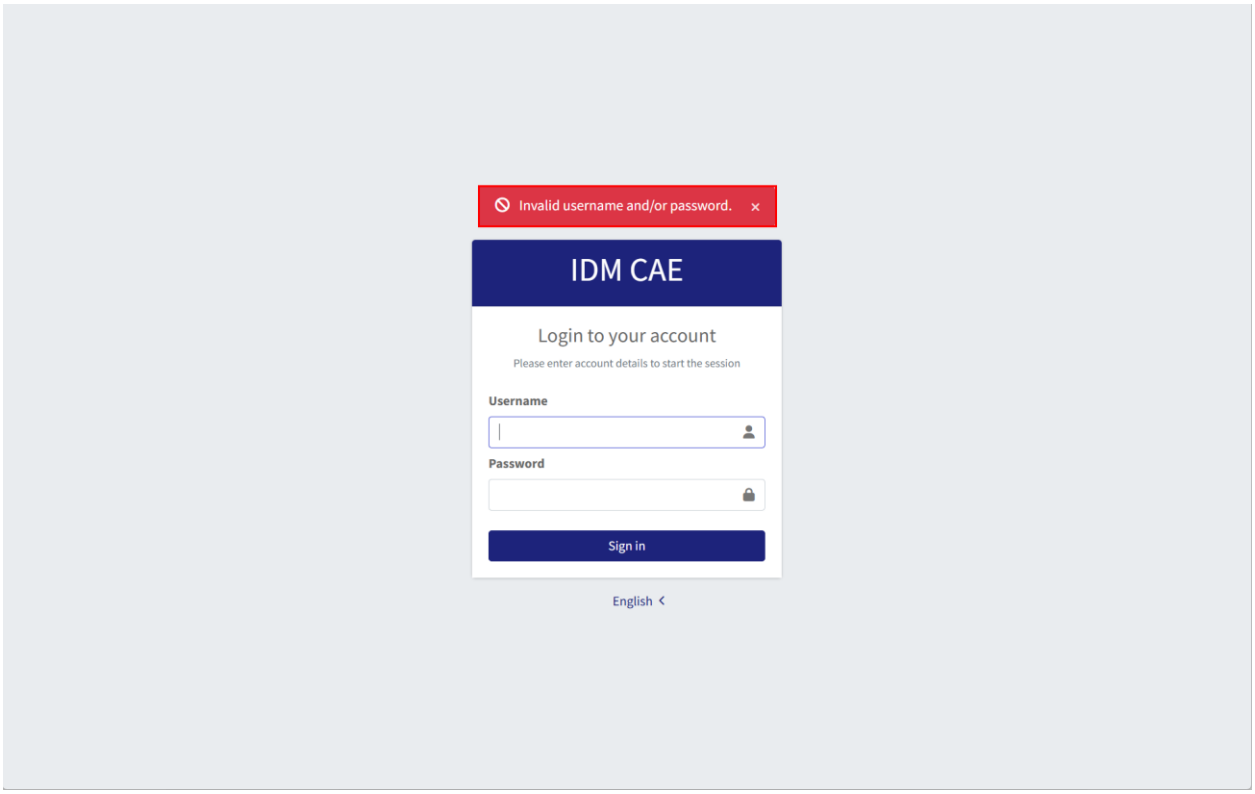


Рисунок 46 – Ошибка при попытке аутентификации

7.1.1.5. Настройка LDAP-аутентификации

В данном разделе описаны шаги для настройки LDAP-аутентификации для входа администратора IDM CAE в веб-интерфейс компонента Provisioning Management.

Для настройки LDAP-аутентификации выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Перейдите к **Default Security policy** через список объектов, установив предварительно в фильтре **Type** значение **Security policy** (подробнее см. в разделе 6.1.1).
3. Вставьте в секцию `modules` листинг, подставив нужные значения (1, рисунок 47)

```
<ldap>
```

```
    <identifier>ldapAuth</identifier>
        <host>ldap://<ip-адрес-домен-
контроллера>:389/DC=example,DC=com</host>
        <userDn>CN=idm           admin,OU=Users,DC=exam-
ple,DC=com</userDn>
        <userPassword>
            <t:clearValue>Пароль          администратора
</t:clearValue>
        </userPassword>
        <search>
            <pattern>(sAMAccountName={0})</pattern>
            <namingAttr>sAMAccountName</namingAttr>
        </search>
</ldap>
```

4. Вставьте в секцию `sequence` листинг (2, рисунок 47).

```
<module>
    <identifier>ldapAuth</identifier>
    <order>1</order>
    <necessity>sufficient</necessity>
</module>
```

Нажмите на **Save** (3, рисунок 47).

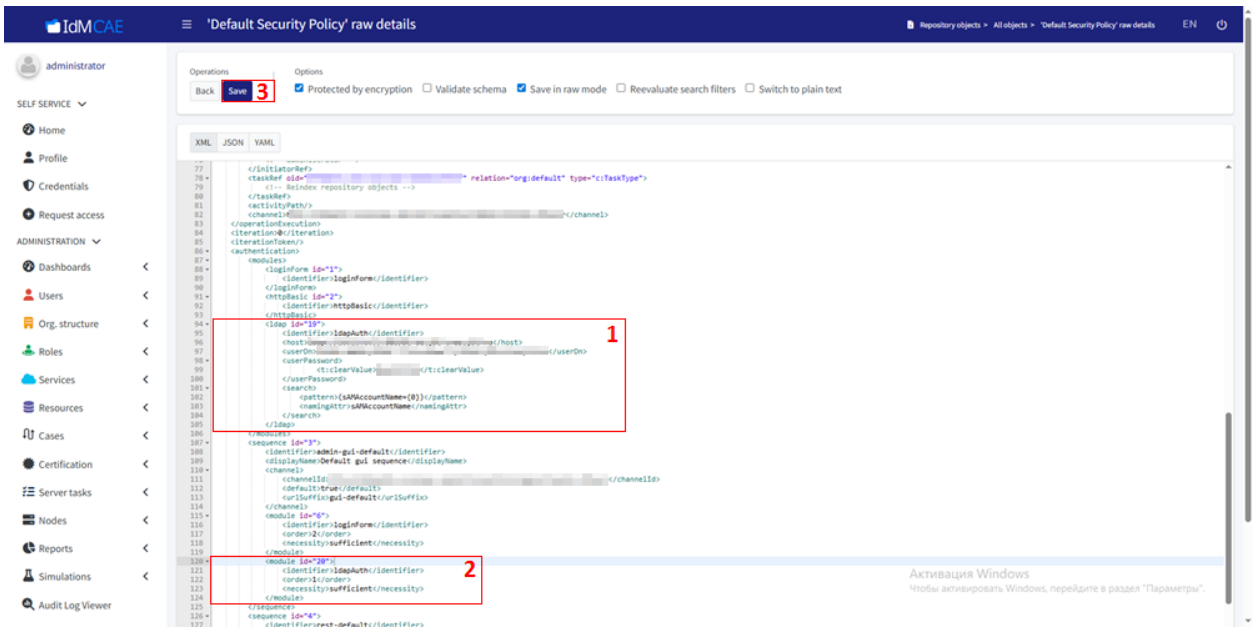


Рисунок 47 – Сохранение изменений

5. Создайте нового пользователя (подробнее см. в разделе 7.1.3.1) с учётом следующих правил:

- в поле **Name** введите значение sAMAccountName пользователя из Active Directory;
- не указывайте пароль;
- назначьте пользователю роль Superuser.

  В результате созданный пользователь сможет войти в Provisioning Management с помощью УЗ Active Directory.

7.1.2. Управление ресурсами

7.1.2.1. Импорт ресурса

Компонент Provisioning Management поддерживает импорт ресурсов в виде объектов в формате .XML.

Для импорта ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).

2. Слева в меню выберите **Resources -> All resources** (1, рисунок 48). Нажмите на  внизу окна (2, рисунок 48).

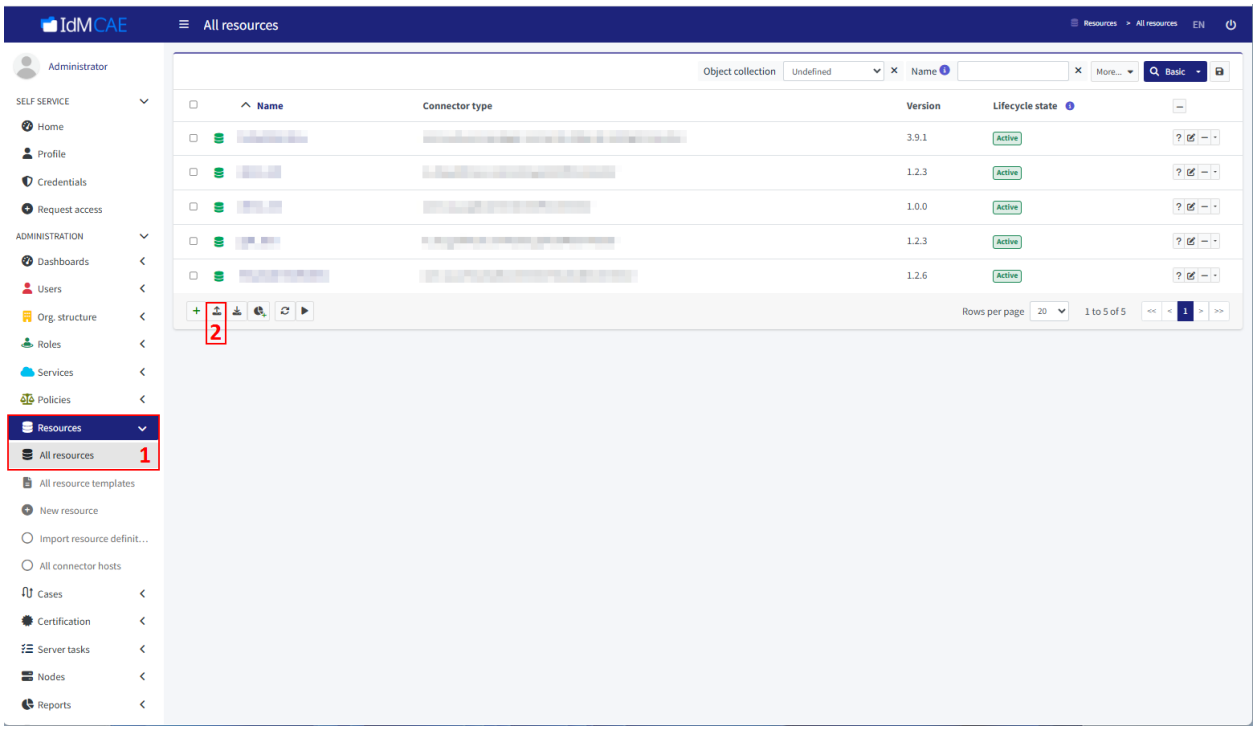


Рисунок 48 – Переход к импорту ресурса

3. Нажмите **Выберите файл** (1, рисунок 49) и в открывшемся окне для выбора файлов с АРМ выберите нужный файл. Нажмите на **Import object** (2, рисунок 49).

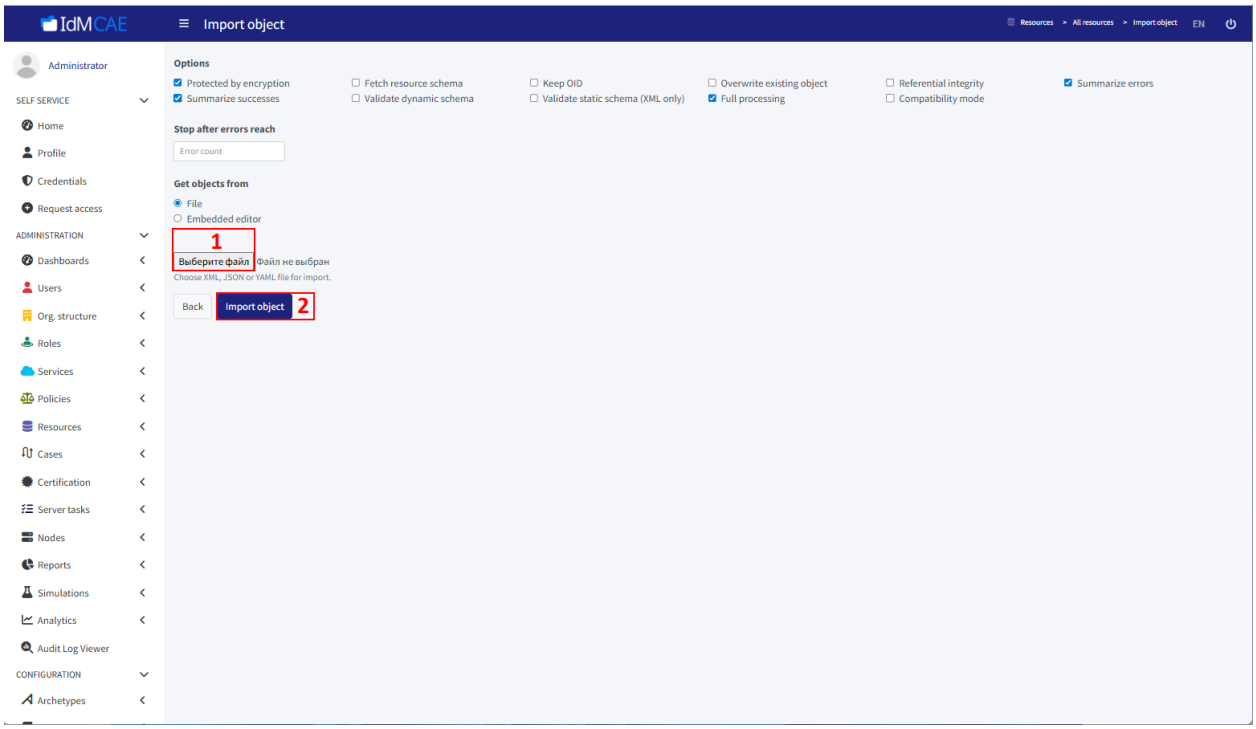


Рисунок 49 – Импорт ресурса

7.1.2.2. Создание ресурса

Для создания ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> New resource** (1, рисунок 50). В открывшемся окне **New resource** будут отражены три способа создания ресурса (2, рисунок 50):
    a. **Inherit Template** – посредством наследования и доработки шаблона. Данный способ позволяет автоматически заполнять стандартные параметры (схему, настройки синхронизации), при этом унаследованные настройки можно изменить;
    b. **From Scratch** – создание «с нуля». Данный способ требует ручной настройки атрибутов и политик;

c. **Copy From Template** – посредством копирования шаблона, включая все его настройки. В отличие от **Inherit Template** при данном способе происходит копирование всех параметров без возможности наследования изменений (т.е. это "статичная" копия).

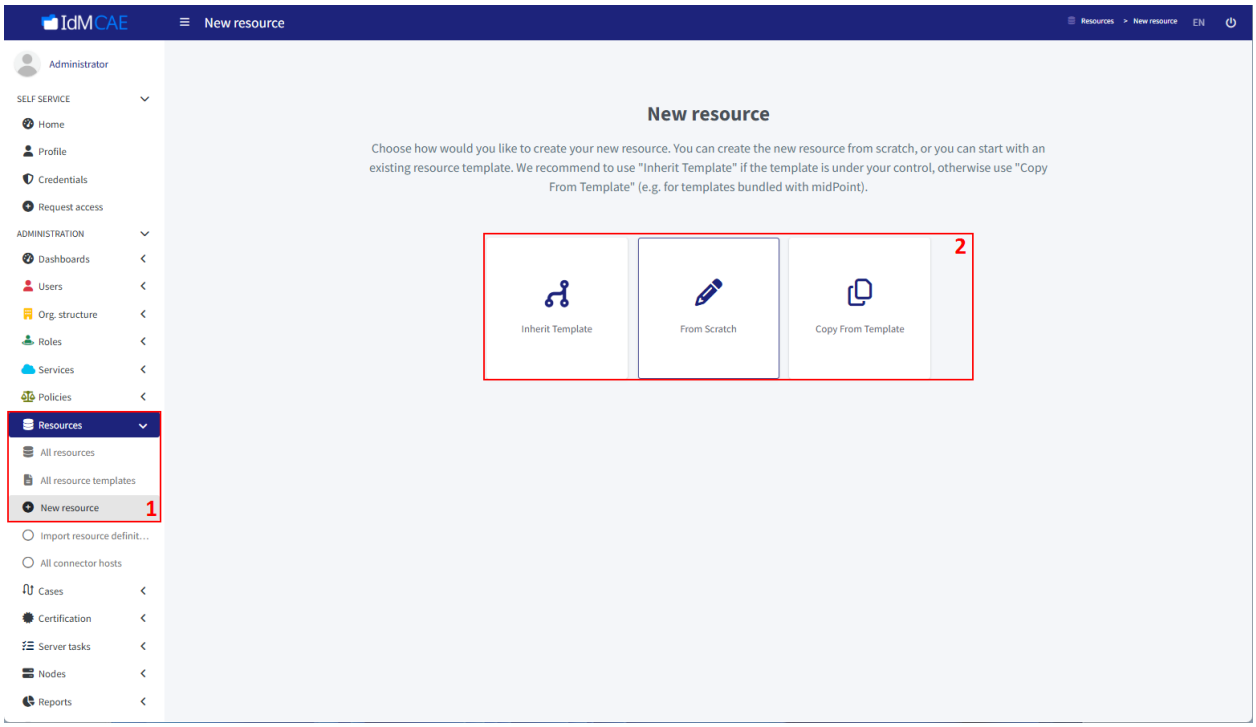


Рисунок 50 – Переход к добавлению ресурса

3. Выберите подходящий способ и следуйте инструкциям мастера настройки. Далее будет рассмотрен способ **From Scratch**.
4. Выберите нужный доступный коннектор (рисунок 51).

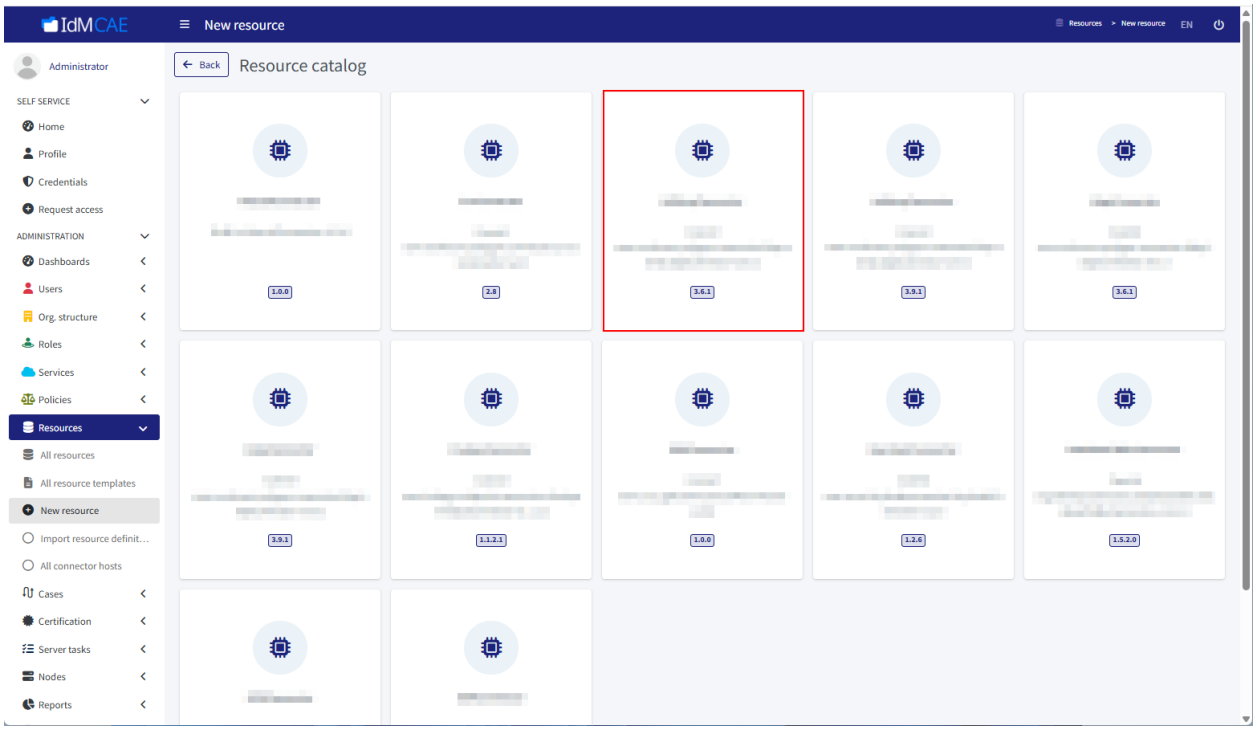


Рисунок 51 – Выбор коннектора

5. Укажите параметры для подключения к ресурсу в окнах **Basic information / Configuration / Discovery / Schema** (рисунок 52) и нажмите **Create resource**. Убедитесь в создании, дождавшись соответствующего сообщения в правом верхнем углу окна (рисунок 53).

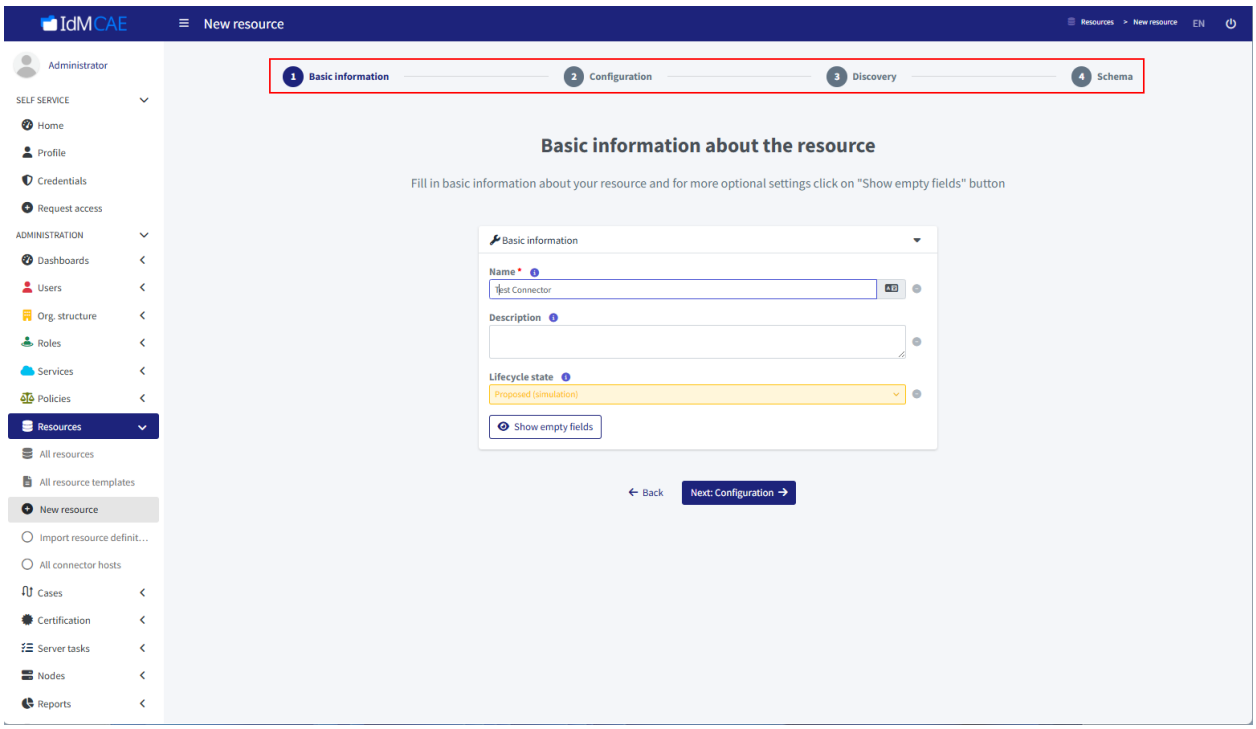


Рисунок 52 – Параметры подключения к ресурсу

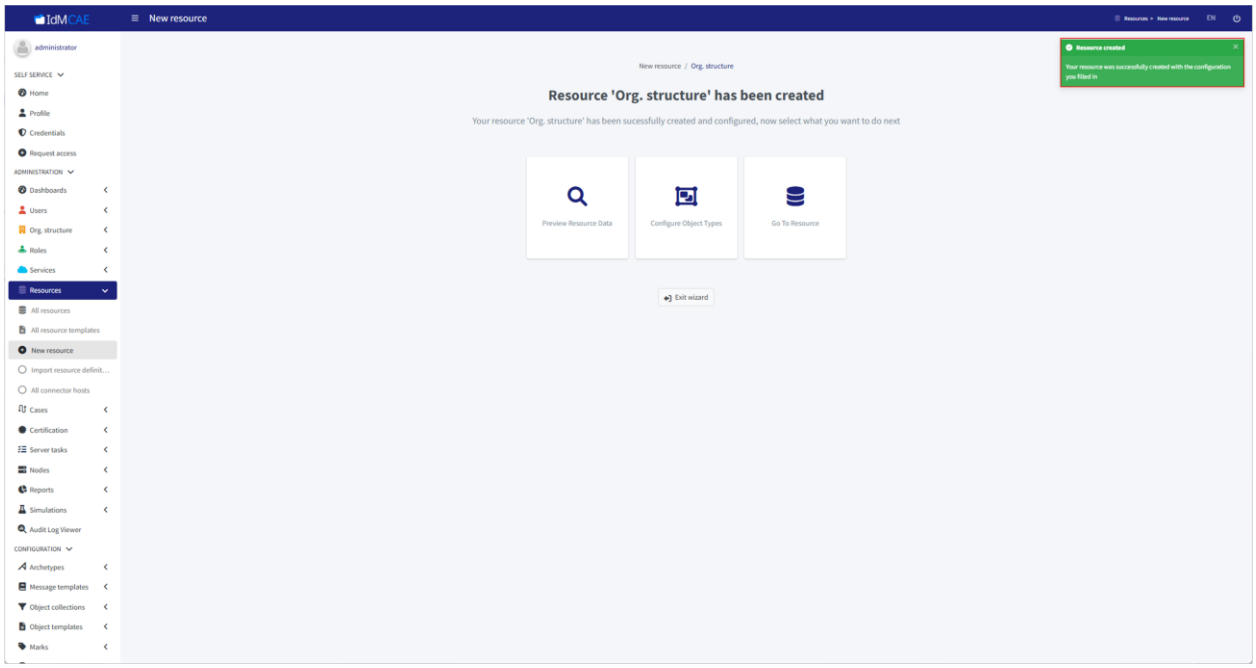


Рисунок 53 – Сообщение об успешном создании ресурса

6. Откройте созданный ресурс (слева в меню выберите **Resources -> All resources**) и перейдите на вкладку **Accounts / Entitlements / Generics** (1, рисунок 54). Далее выберите **Configure -> Mappings** (2, рисунок 54).

Подсказка: каждая из вкладок Accounts / Entitlements / Generics содержит свой набор маппингов:

- Accounts – маппинги УЗ;
- Entitlements – маппинги прав доступа и ролей;
- Generics – другие маппинги (обычно, организационных единиц).

Отображение возможности настройки маппингов зависит от поддержки маппингов на уровне коннектора к ресурсу.

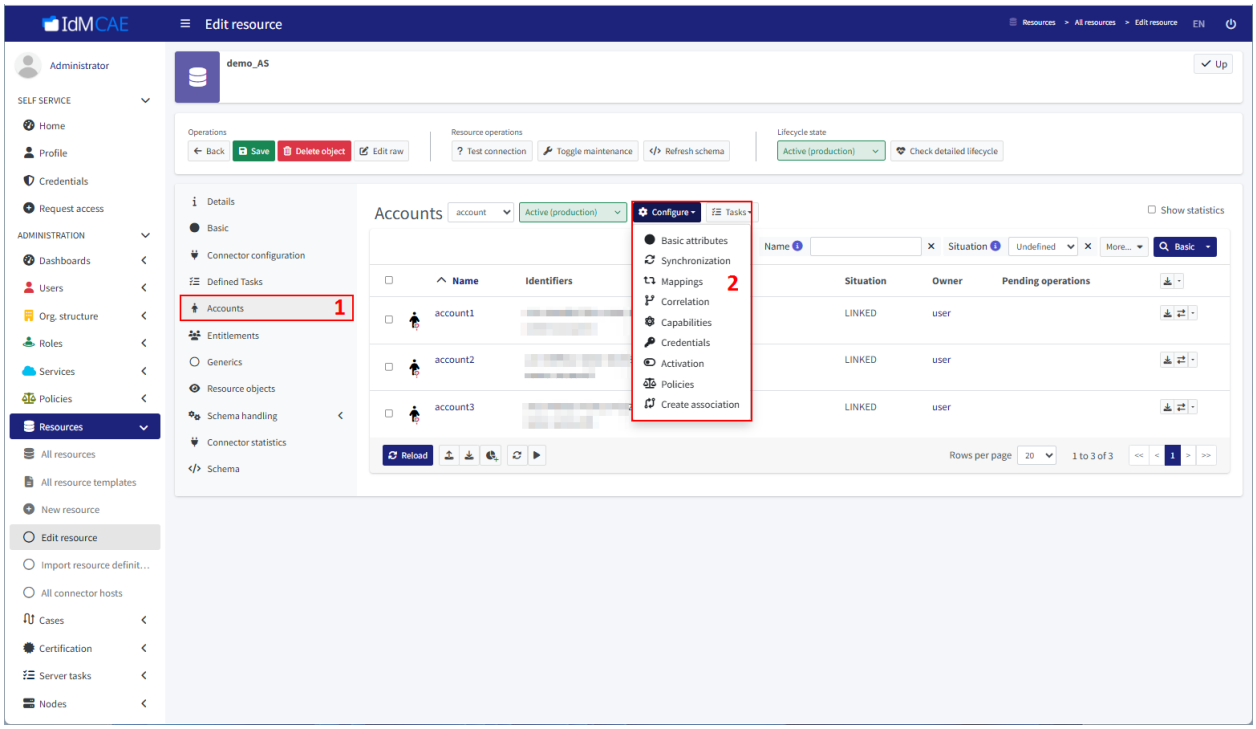


Рисунок 54 – Переход к добавлению маппингов

7. Укажите маппинги для передаваемых атрибутов, используя 

для добавления строчек (1, рисунок 55). Сохраните настроенные маппинги, нажав на **Save mappings** (2, рисунок 55).

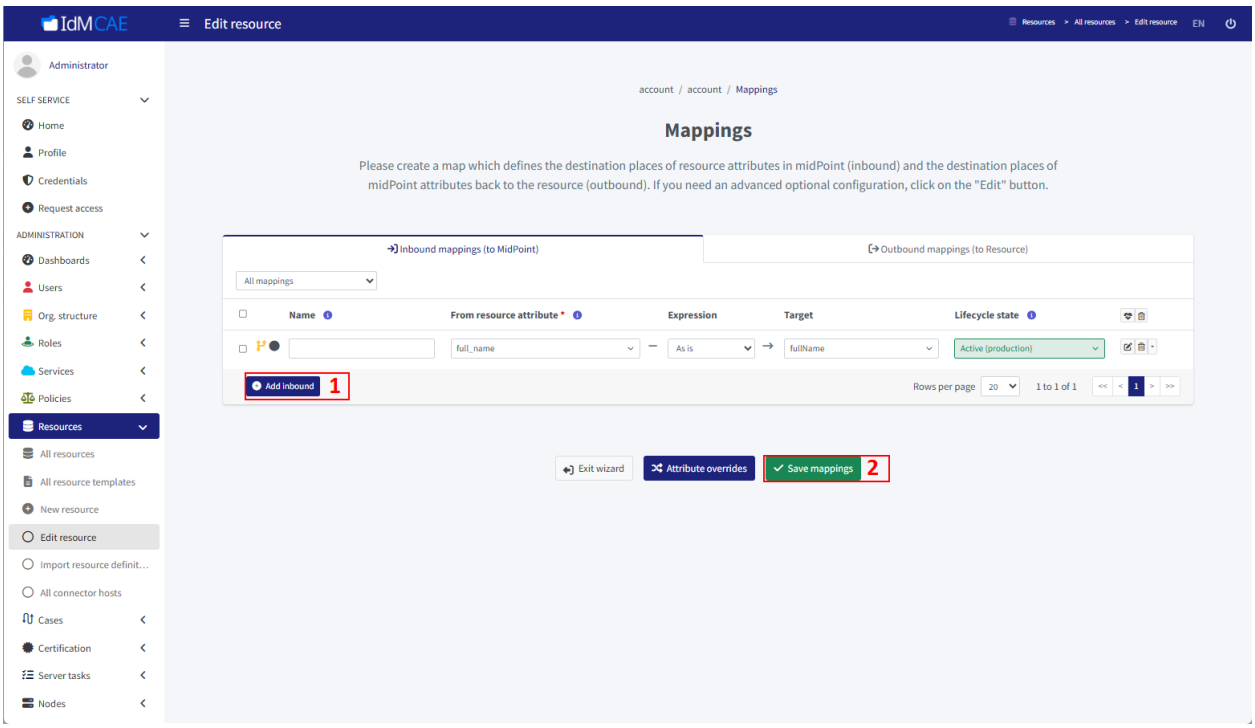


Рисунок 55 – Добавление маппингов

7.1.2.3. Изменение ресурса

Для изменения ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 56). Выберите нужный ресурс в общем списке (2, рисунок 56).

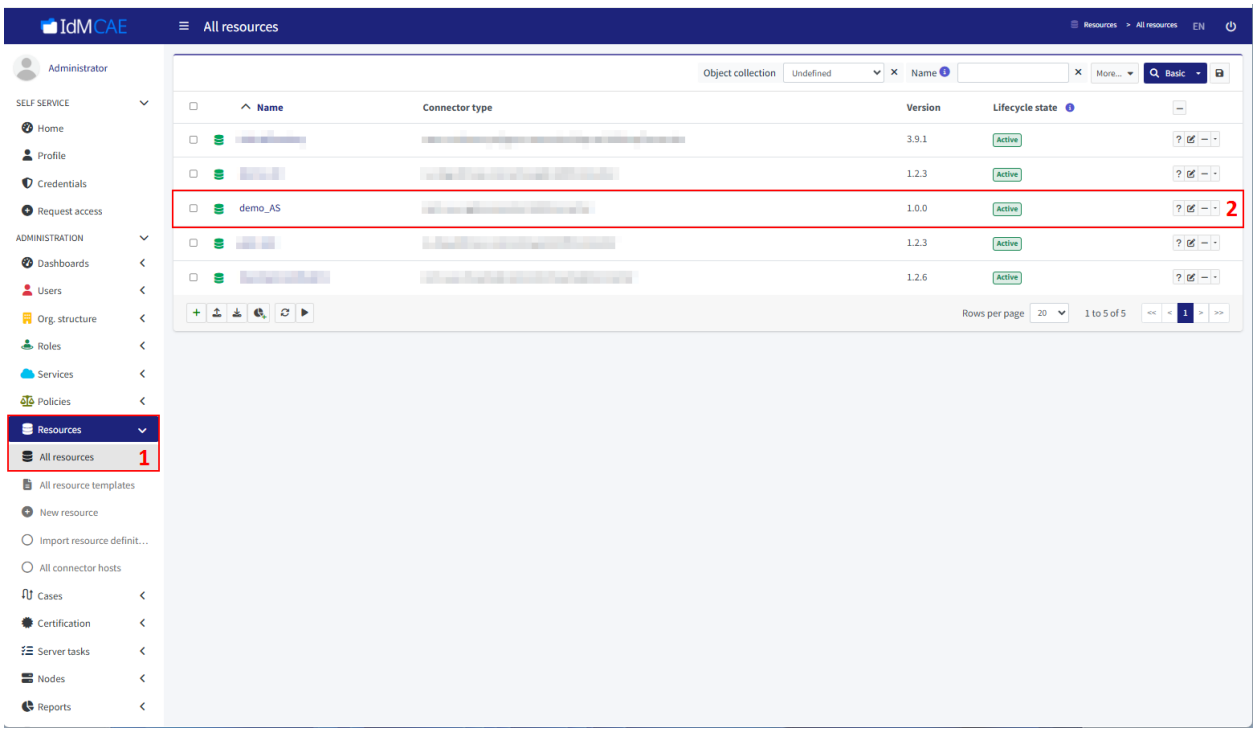


Рисунок 56 – Переход к ресурсу

3. Перейдите на вкладку **Connector configuration** (1, рисунок 57) и введите новые значения полей (2, рисунок 57) (также можно менять значения полей на других вкладках). В зависимости от конкретного ресурса, набор настроек коннектора может быть разным, но обязательными будут поля для указания имени и пароля ТУЗ и адрес для подключения к ИС. Сохраните изменения, нажав на **Save** (3, рисунок 57).

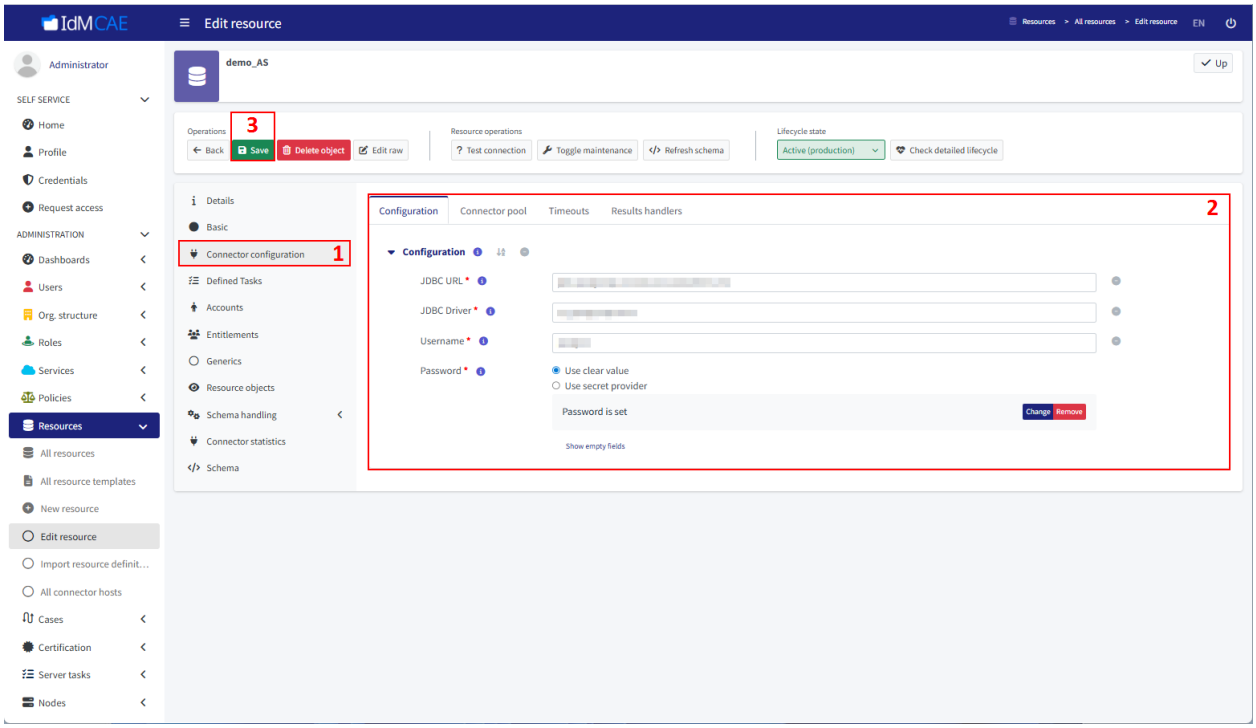


Рисунок 57 – Изменение ресурса

7.1.2.4. Тестирование соединения с ресурсом

Определить состояние ресурса можно с помощью цвета иконки слева от названия в списке ресурсов (рисунок 58). **Чёрный** цвет означает, что состояние не определено, **красный** – ошибка подключения, **зелёный** – исправное состояние.

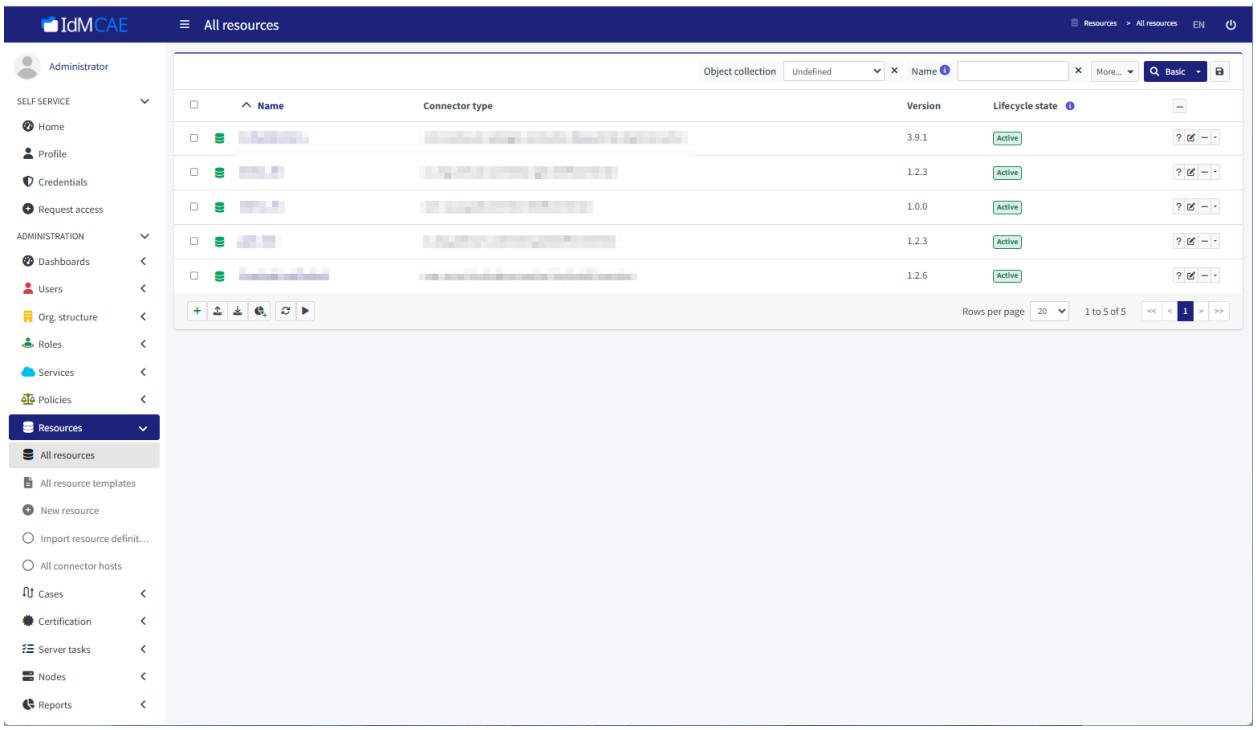


Рисунок 58 – Список ресурсов

Для проверки соединения с ресурсом выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 59). Выберите нужный ресурс в общем списке (2, рисунок 59).

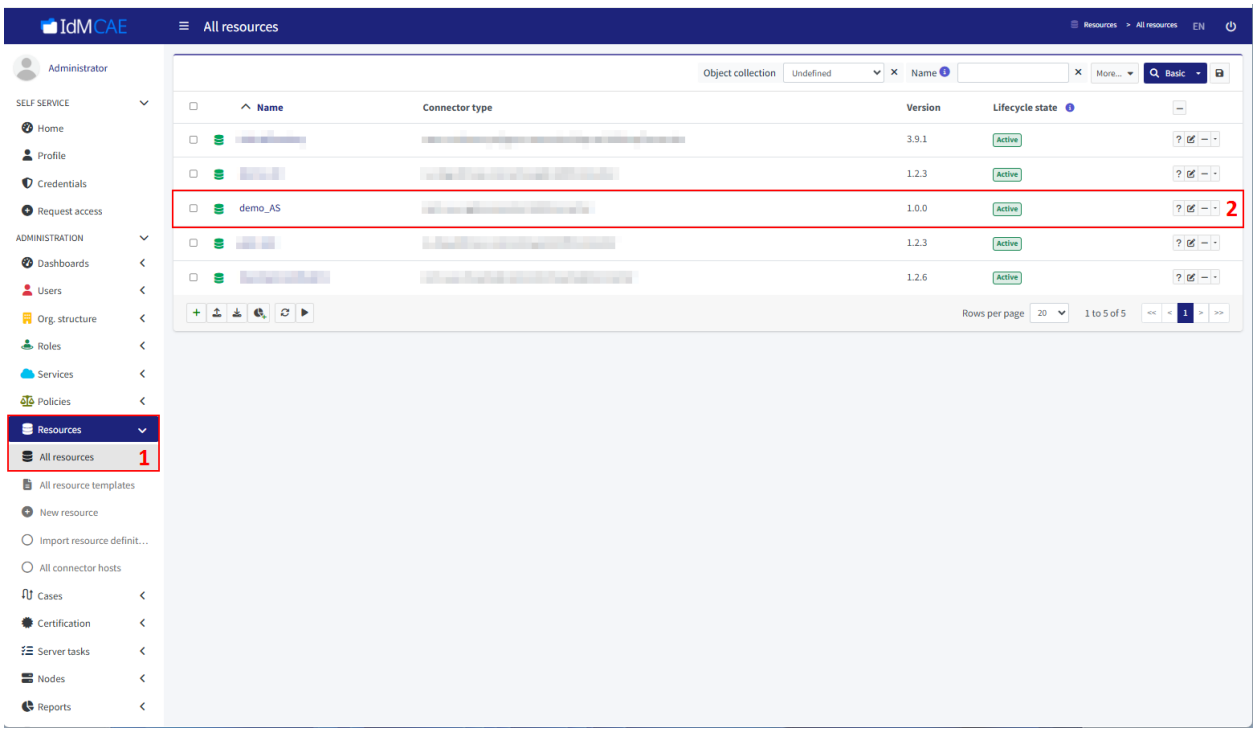


Рисунок 59 – Переход к ресурсу

3. Нажмите на **Test connection** (рисунок 60). В результате запустится тестирование соединения с ресурсом, результат которого будет отображён в этом же окне (рисунок 61).

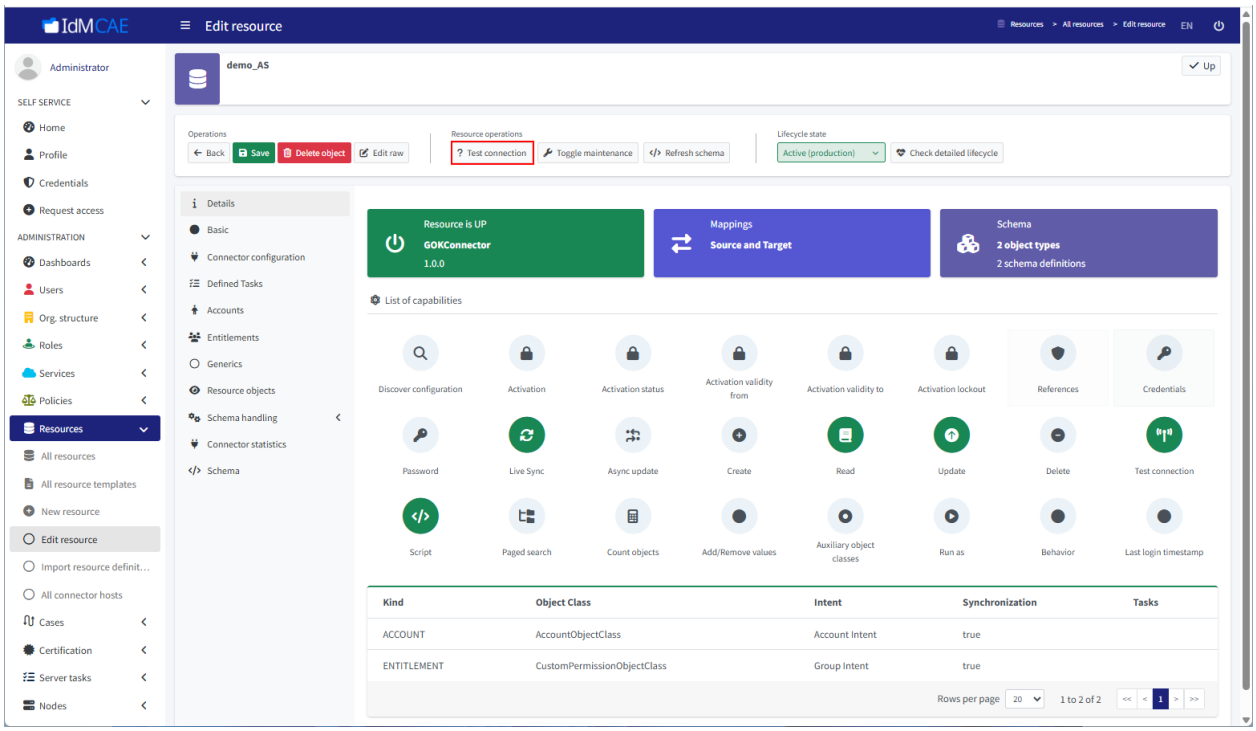


Рисунок 60 – Запуск тестирования соединения с ресурсом

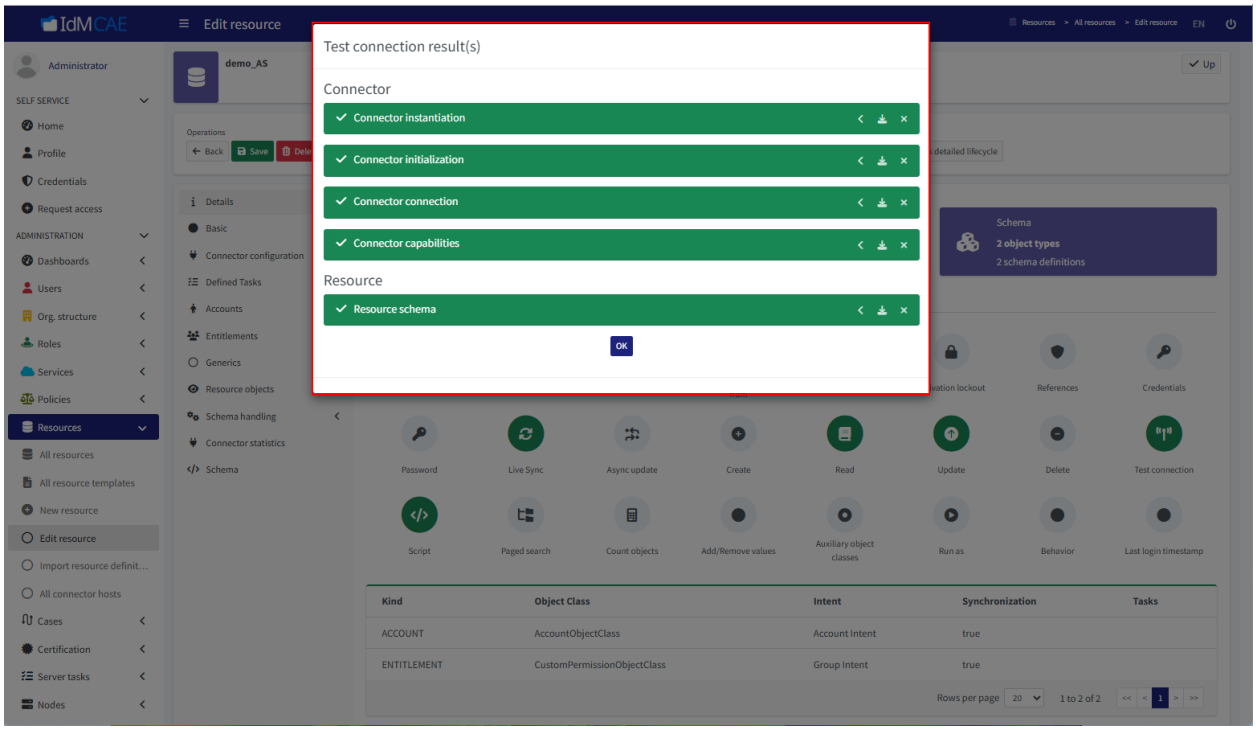


Рисунок 61 – Результаты тестирования соединения

7.1.2.5. Импорт УЗ из HR-ресурса

Для импорта УЗ из ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 62). Выберите HR-ресурс, из которого требуется импортировать УЗ (2, рисунок 62).

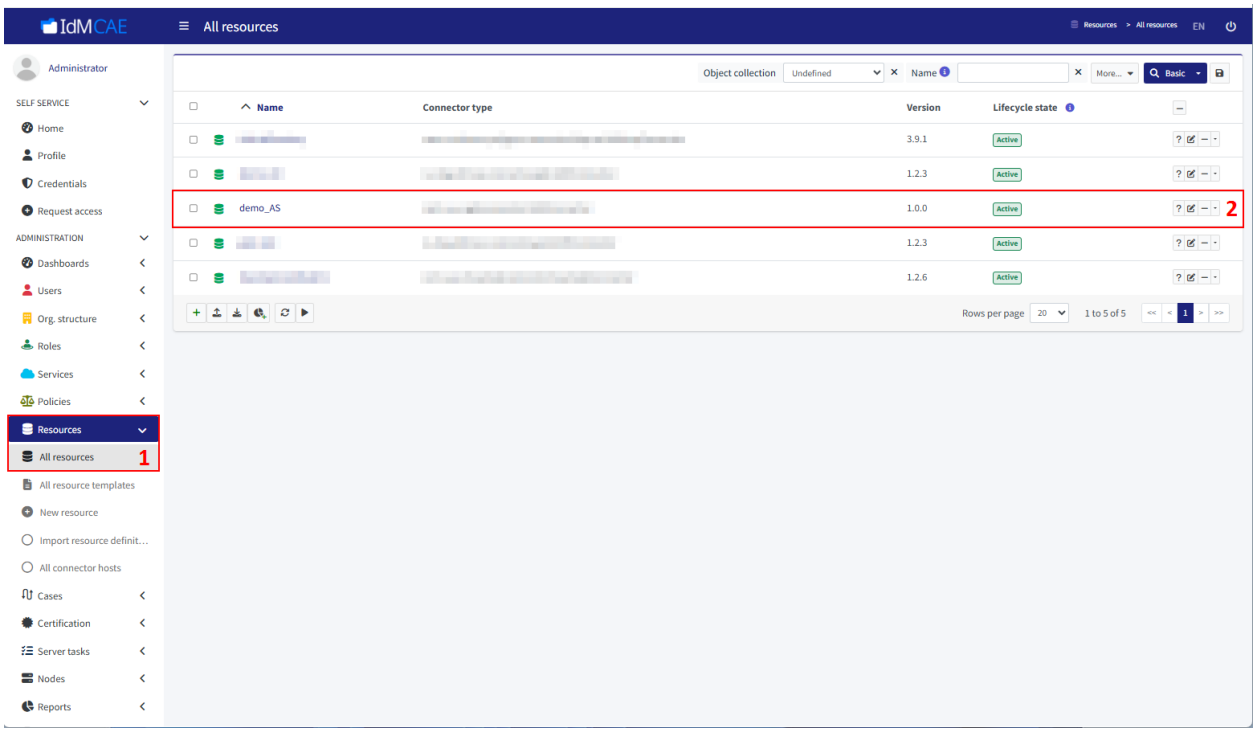


Рисунок 62 – Выбор HR-ресурса

3. Перейдите на вкладку **Accounts** (1, рисунок 63). Нажмите на **Configure** (2, рисунок 63) и в выпадающем выберите **Basic attributes** (3, рисунок 63).

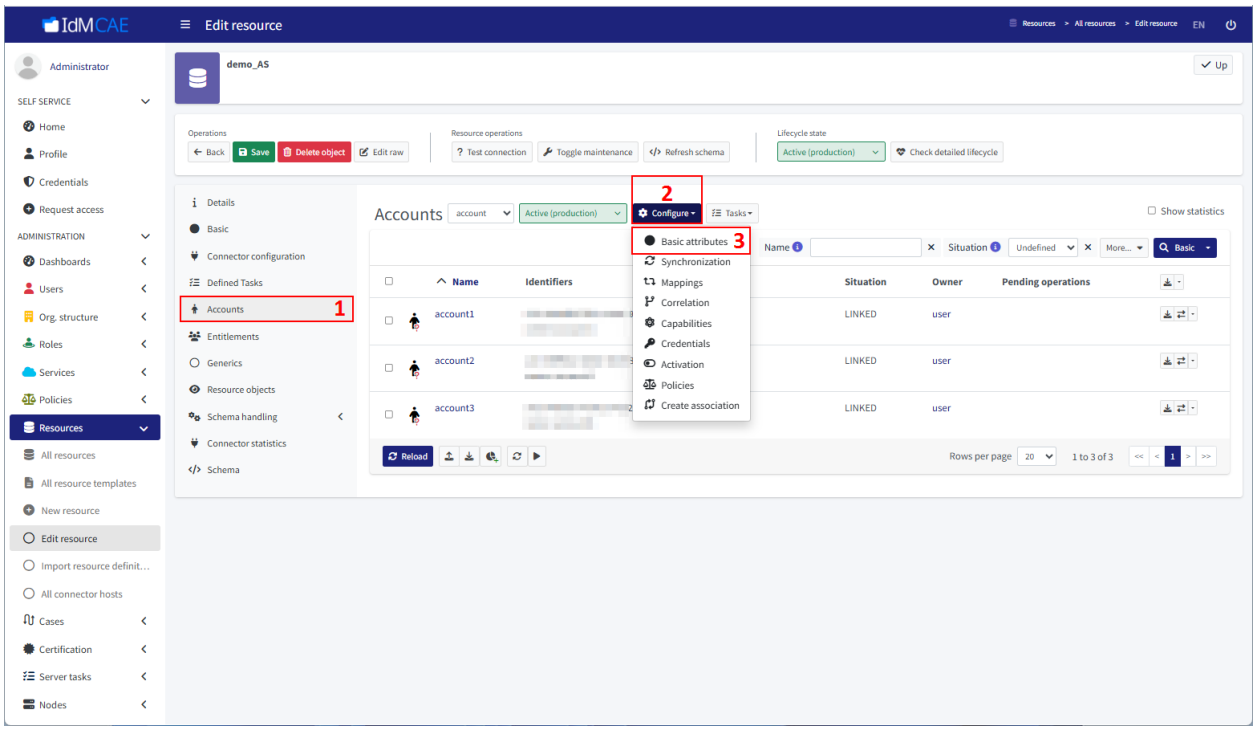


Рисунок 63 – Переход к базовым атрибутам

4. В окне **Basic information** в поле **Kind** выберите **Account** (рисунок 64), в окне **Resource data** в поле **Object class** – нужный класс объекта (рисунок 65), в окне **MidPoint data** в поле **Type** – **User** (1, рисунок 66). Остальные поля заполните при необходимости, например, можно указать используемый архетип (2, рисунок 66). Сохраните настройки, нажав на **Save settings** (3, рисунок 66).

   В результате произойдёт переход в окно с общим списком УЗ (пока пустым). Для того чтобы настройки были применены и IDM CAE смог загрузить УЗ из HR-ресурса, нажмите на **Reload** (рисунок 67).

   Обратите внимание, что на данном этапе импортированные УЗ никак не связаны с пользователями IDM CAE.

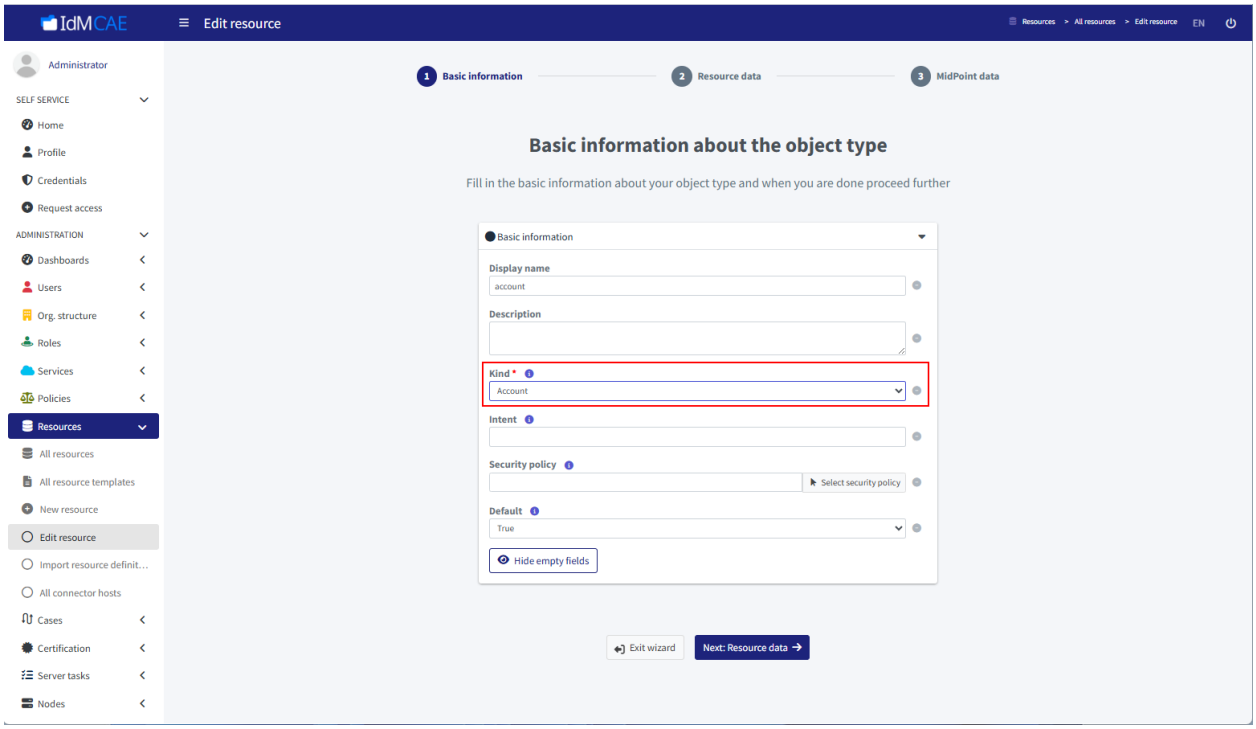


Рисунок 64 – Окно Basic information

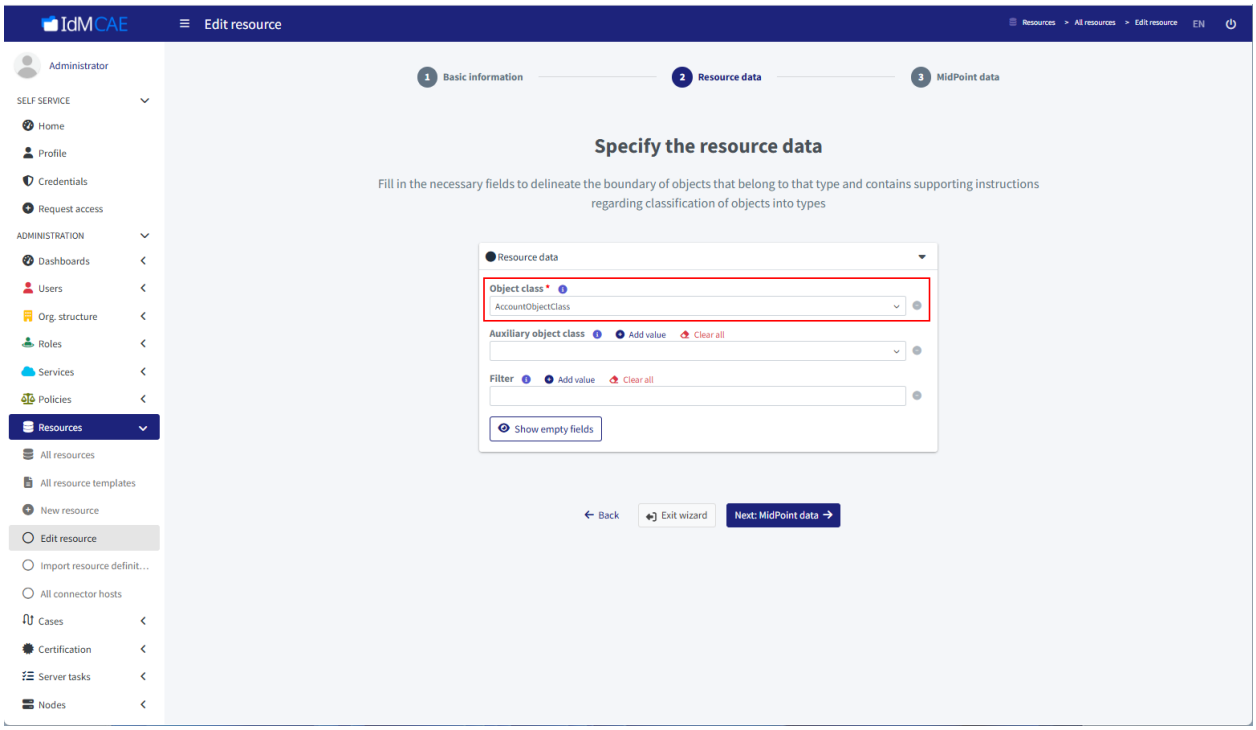


Рисунок 65 – Окно Resource data

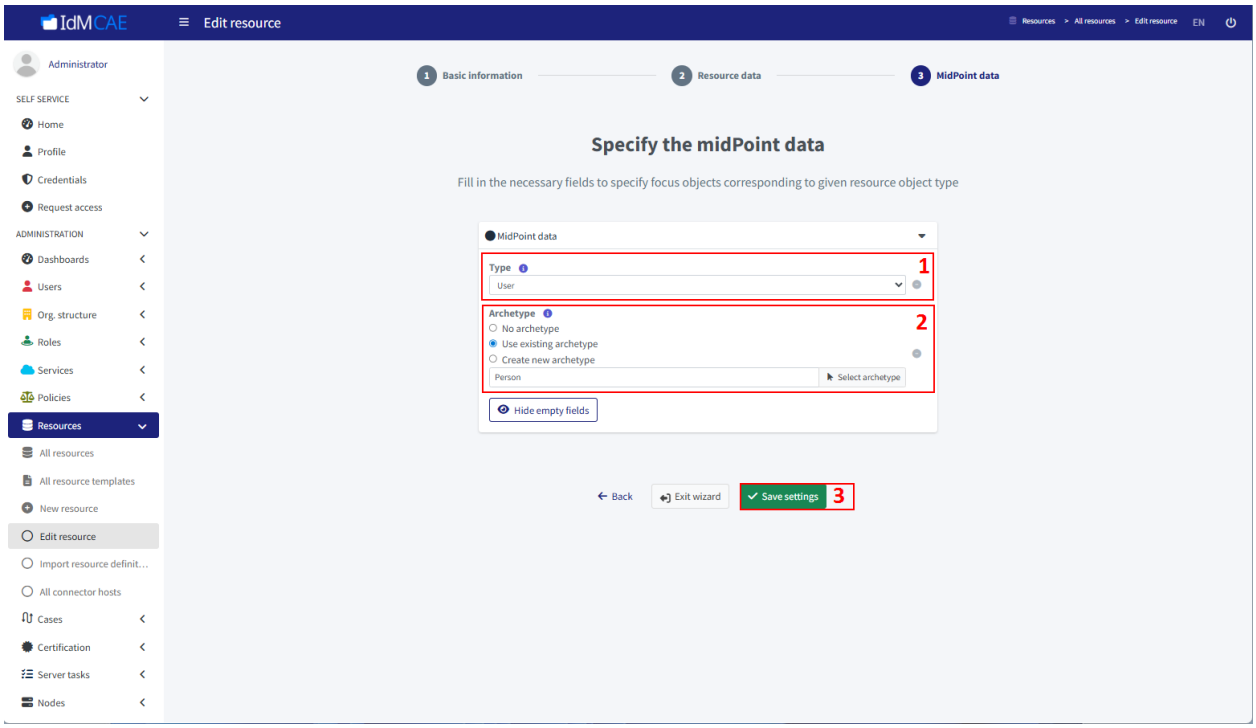


Рисунок 66 – Окно MidPoint data

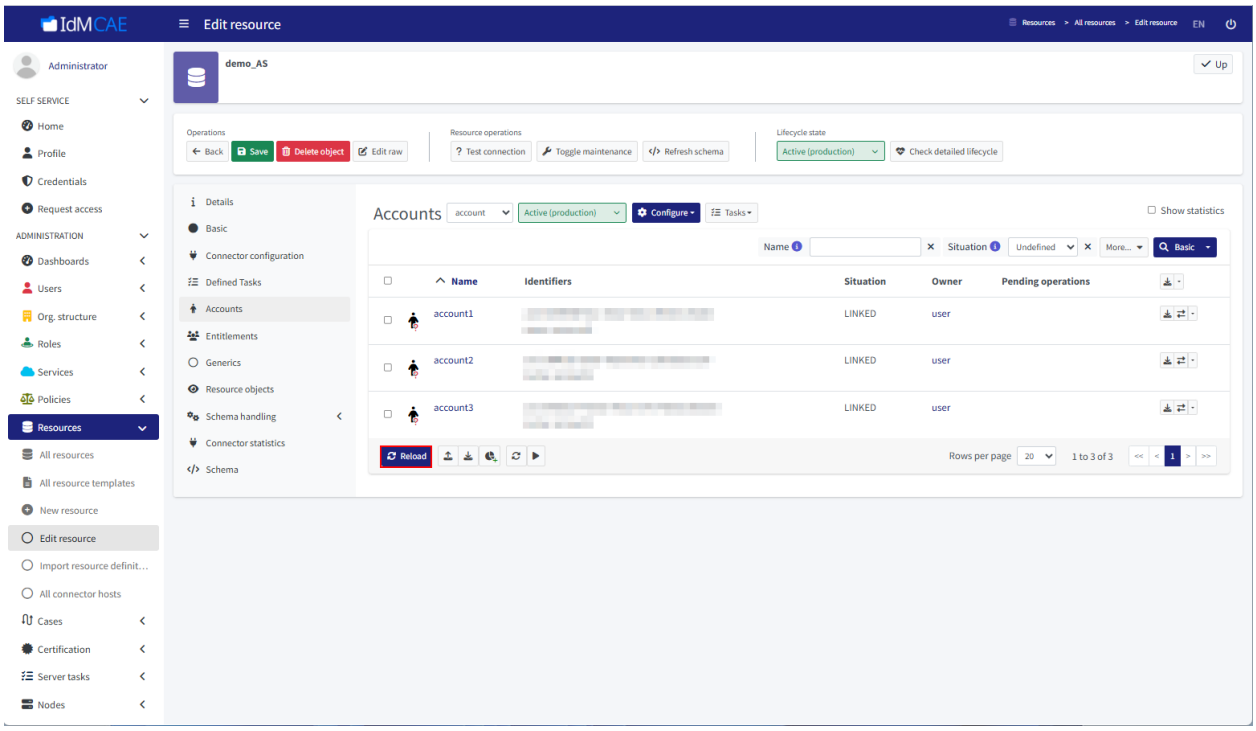


Рисунок 67 – Загрузка УЗ

7.1.2.6. Создание УЗ ресурса через импорт

В разделе рассматривается пример создания УЗ ресурса (целевой ИС) на основе имеющихся в IDM CAE пользователей.

Для импорта УЗ ресурса выполните шаги, описанные в разделе 7.1.2.5, настроив соответствующие синхронизации, маппинги и корреляции. Обратите внимание, что в отличие от настроек маппингов с HR-ресурсом требуется задать исходящие маппинги (outbound)!

7.1.2.7. Создание УЗ ресурса через принадлежность к организационной единице / роли

В разделе рассматривается создание УЗ в ресурсе при принадлежности пользователя к определённой организационной единице или роли. Данное действие требует, чтобы в ресурсе, в котором создаётся УЗ, были настроены исходящие маппинги и правила корреляции.

Для создания УЗ ресурса через принадлежность к организационной единице / роли выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Org. structure -> All organizations** (1, рисунок 68) или **Roles -> All roles**. Перейдите к нужной организационной единице (2, рисунок 68) или роли.

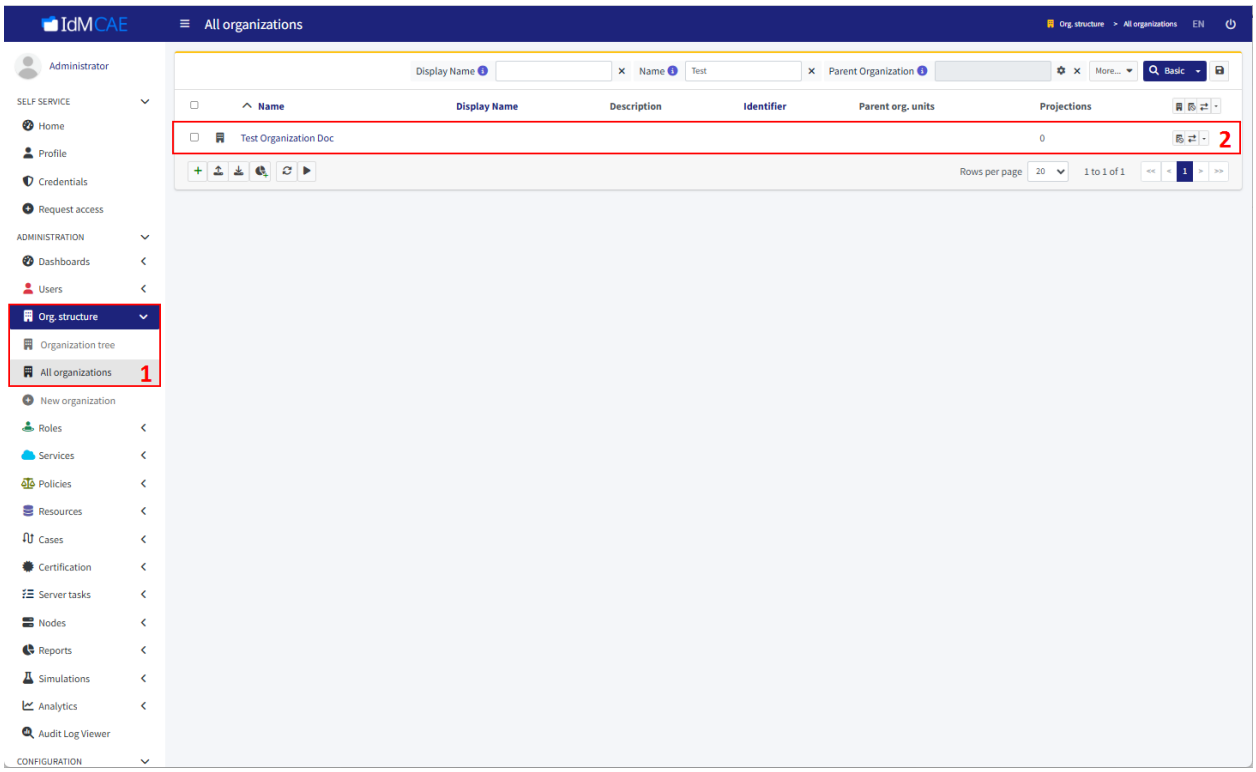


Рисунок 68 – Выбор организационной единицы / роли

3. Перейдите на вкладку **Inducements -> All** (1, рисунок 69). Нажмите на  (2, рисунок 69).

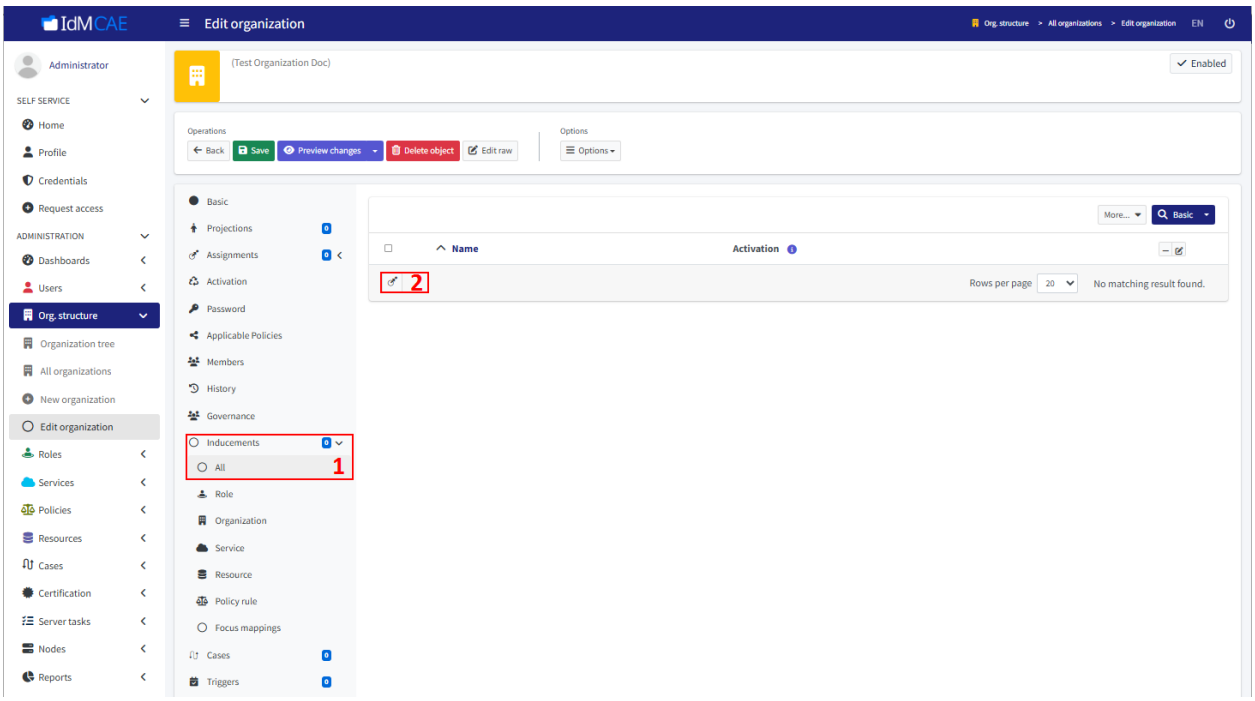


Рисунок 69 – Переход к выбору ресурса

4. Перейдите на вкладку **Resource** (1, рисунок 70). Выберите нужный ресурс (2, рисунок 70). В параметре **Kind** укажите **Account** (3, рисунок 70), а в **Intent** – нужное значение intent (4, рисунок 70). Нажмите на **Add** (5, рисунок 70).

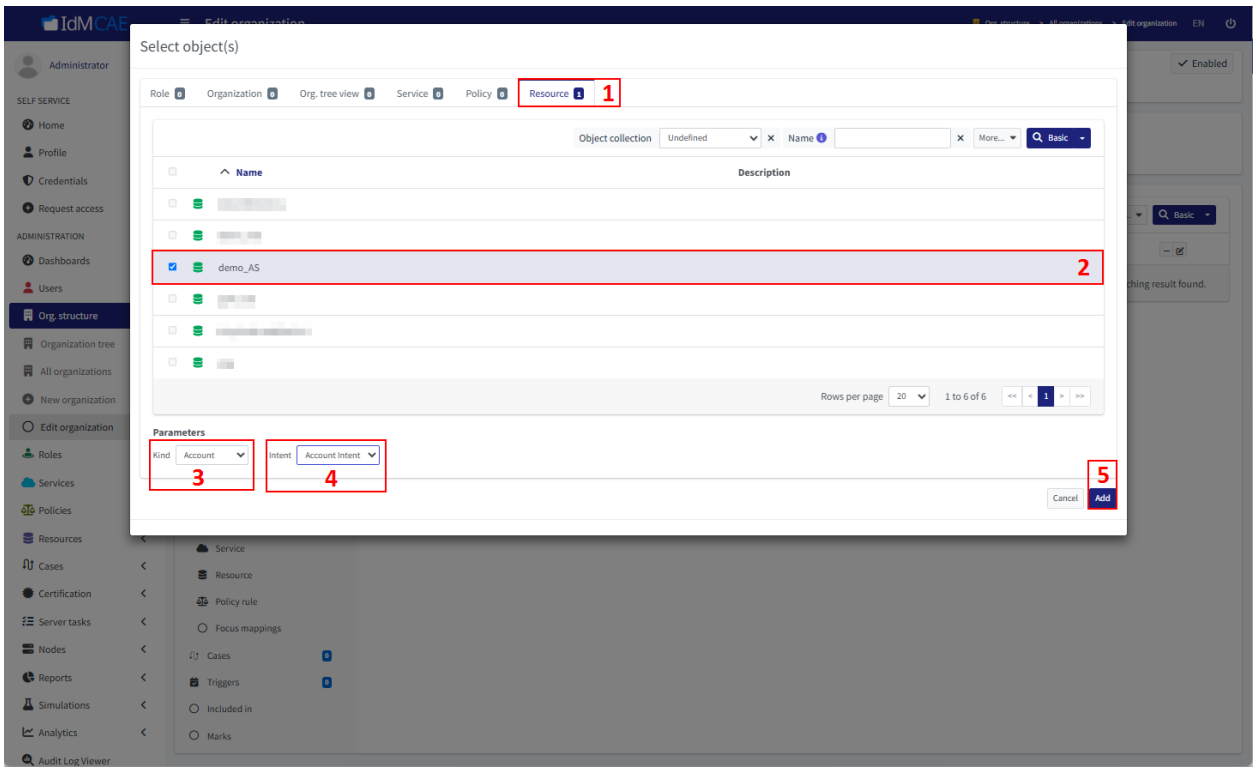


Рисунок 70 – Настройка ресурса

5. Сохраните изменения, нажав на **Save** (рисунок 71).

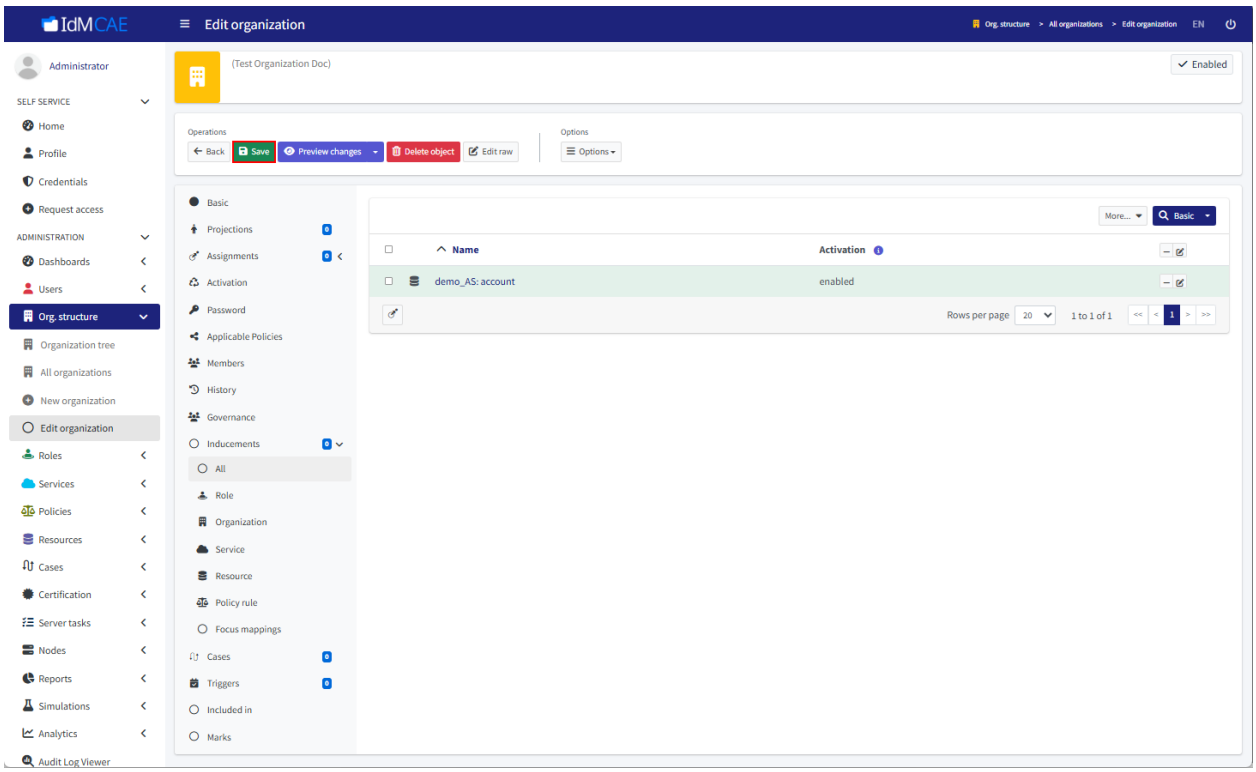


Рисунок 71 – Сохранение изменений

После указанных настроек пользователю при назначении организационной единицы / роли IDM CAE автоматически создаст УЗ в ресурсе.

7.1.2.8. Привязка УЗ к пользователю

Для привязки УЗ к пользователю выполните следующие шаги:

6. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
7. Слева в меню выберите **Resources -> All resources** (1, рисунок 72). Выберите нужный ресурс в общем списке (2, рисунок 72).

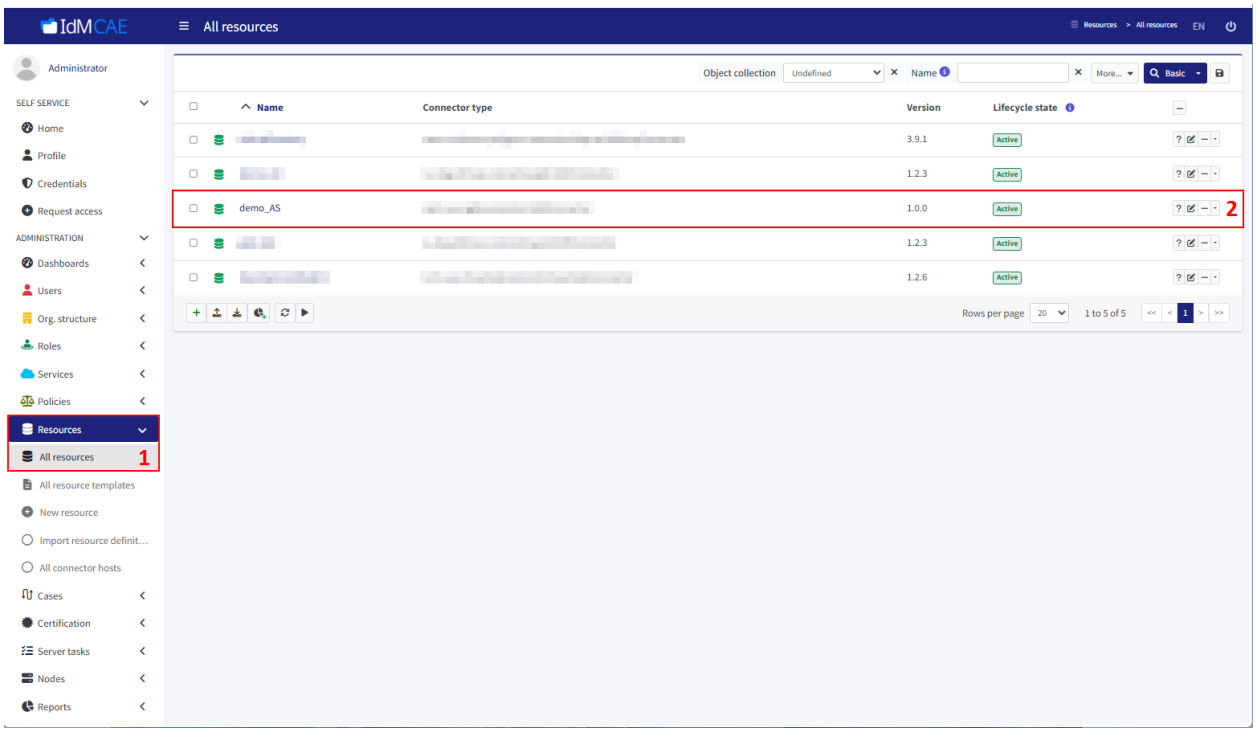


Рисунок 72 – Переход к ресурсу

8. Перейдите на вкладку **Accounts** (1, рисунок 73) и нажмите на ▾ (2, рисунок 73) справа от УЗ без пользователя. В выпадающем списке выберите **Change owner**.

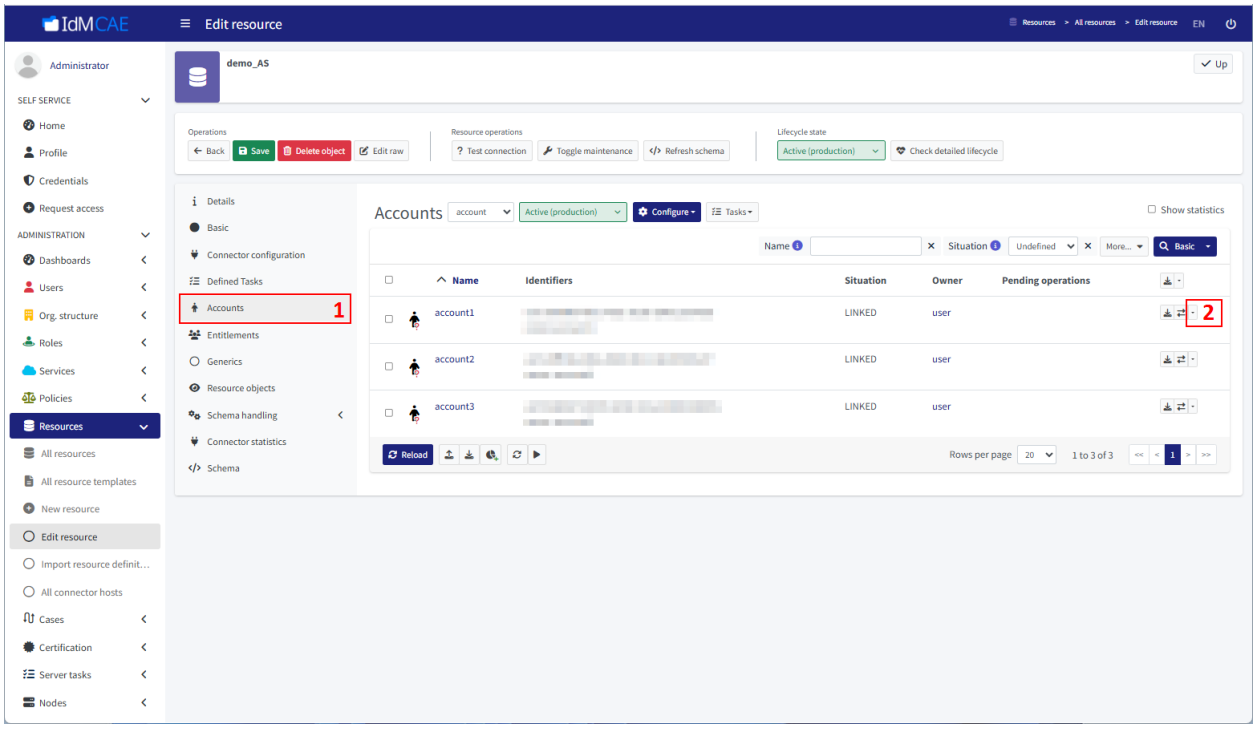


Рисунок 73 – Выбор УЗ

9. Появится окно с общим списком пользователей. Выберите нужного (рисунок 74).

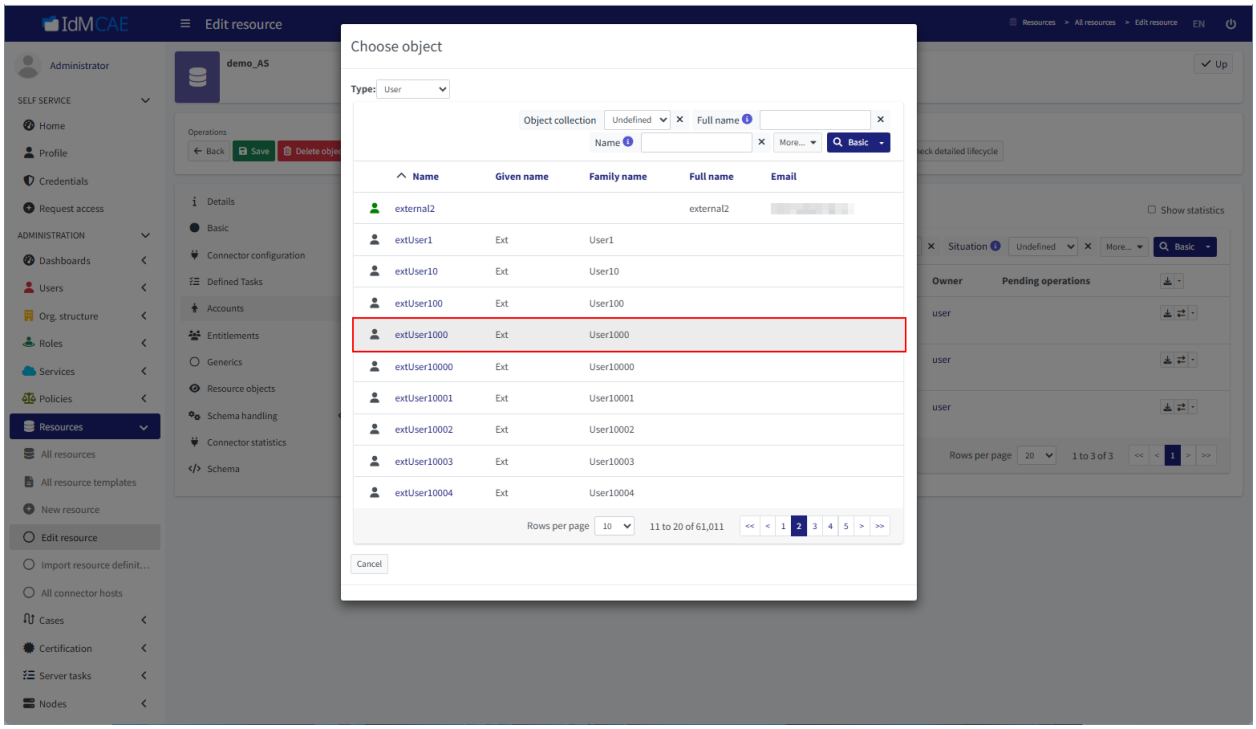


Рисунок 74 – Выбор пользователя

10. В результате произойдёт автоматический переход на страницу редактирования ресурса и напротив УЗ появится имя выбранного пользователя (1, рисунок 75). Сохраните изменения, нажав на **Save** (2, рисунок 75).

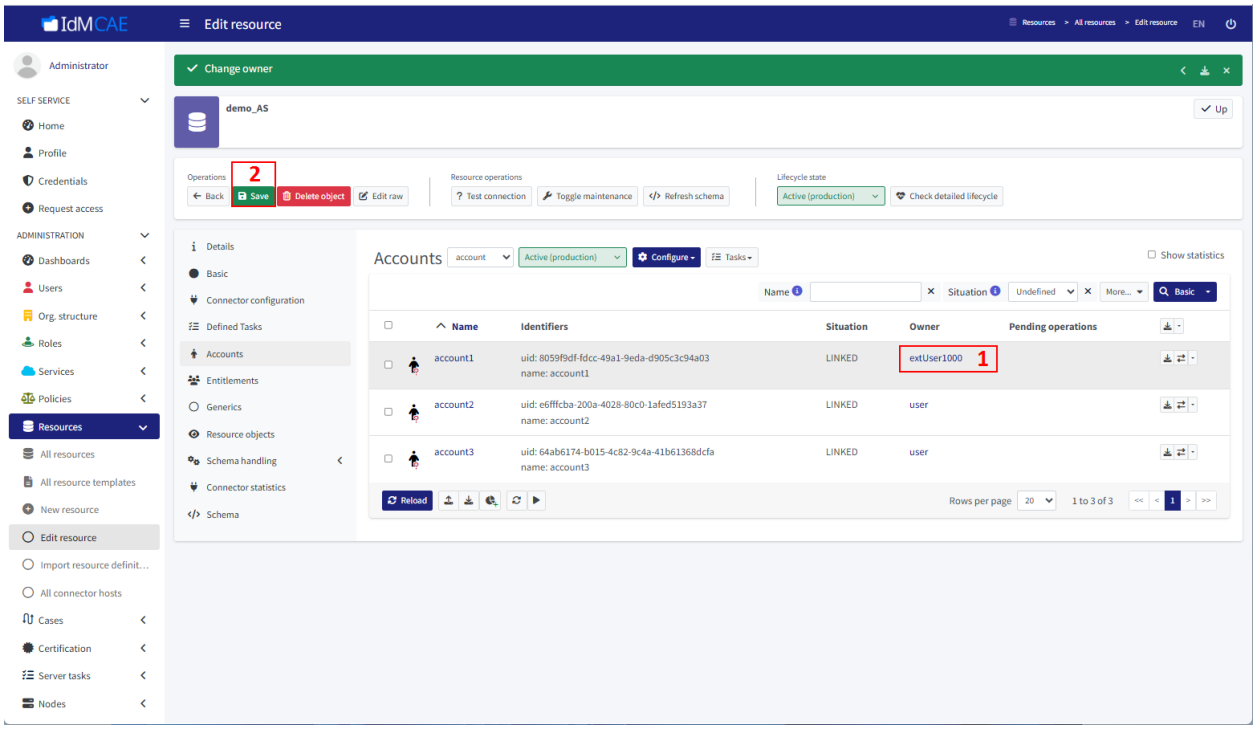


Рисунок 75 – Сохранение изменений

7.1.2.9. Создание заданий ресурса

Задачи ресурса нужны для выполнения операций по выгрузке и управлению объектами в ресурсе.

Для создания задачи в ресурсе выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 76). Выберите нужный ресурс в общем списке (2, рисунок 76).

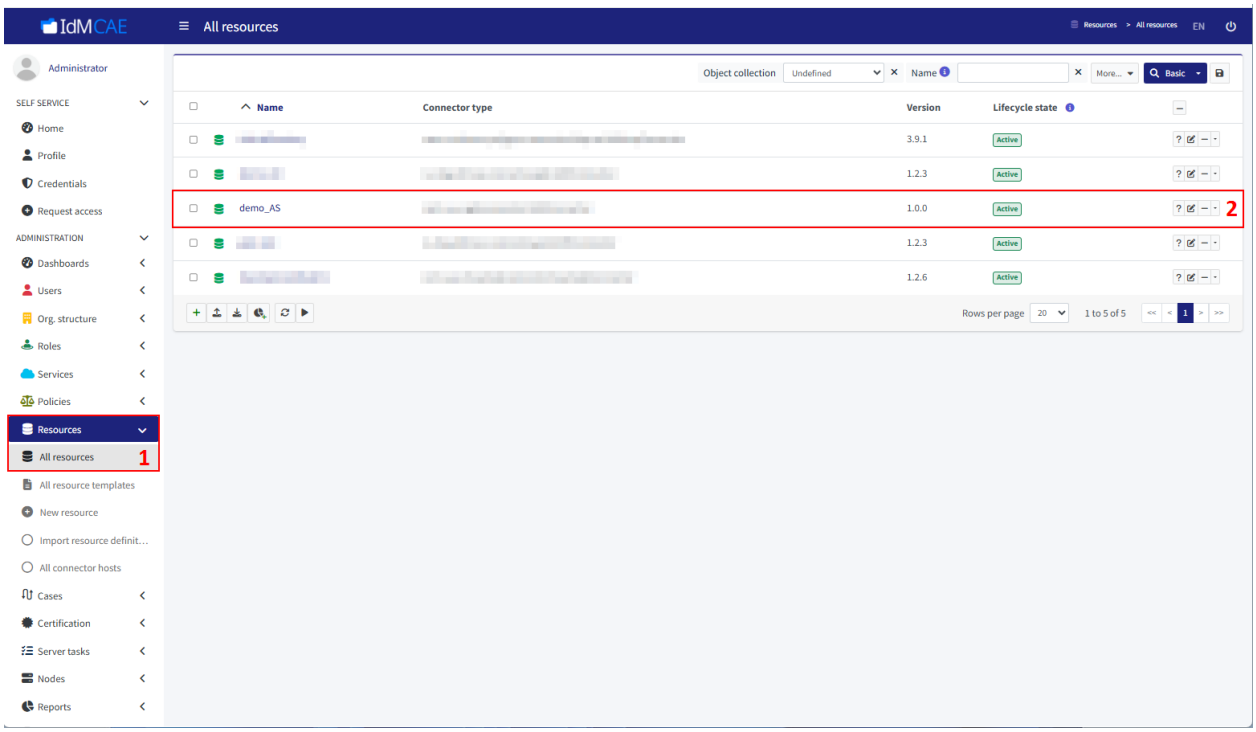


Рисунок 76 – Переход к ресурсу

3. Перейдите на вкладку **Defined Tasks** (1, рисунок 77). Нажмите на [+] (2, рисунок 77), в открывшемся окне выберите **Import task** (рисунок 78).

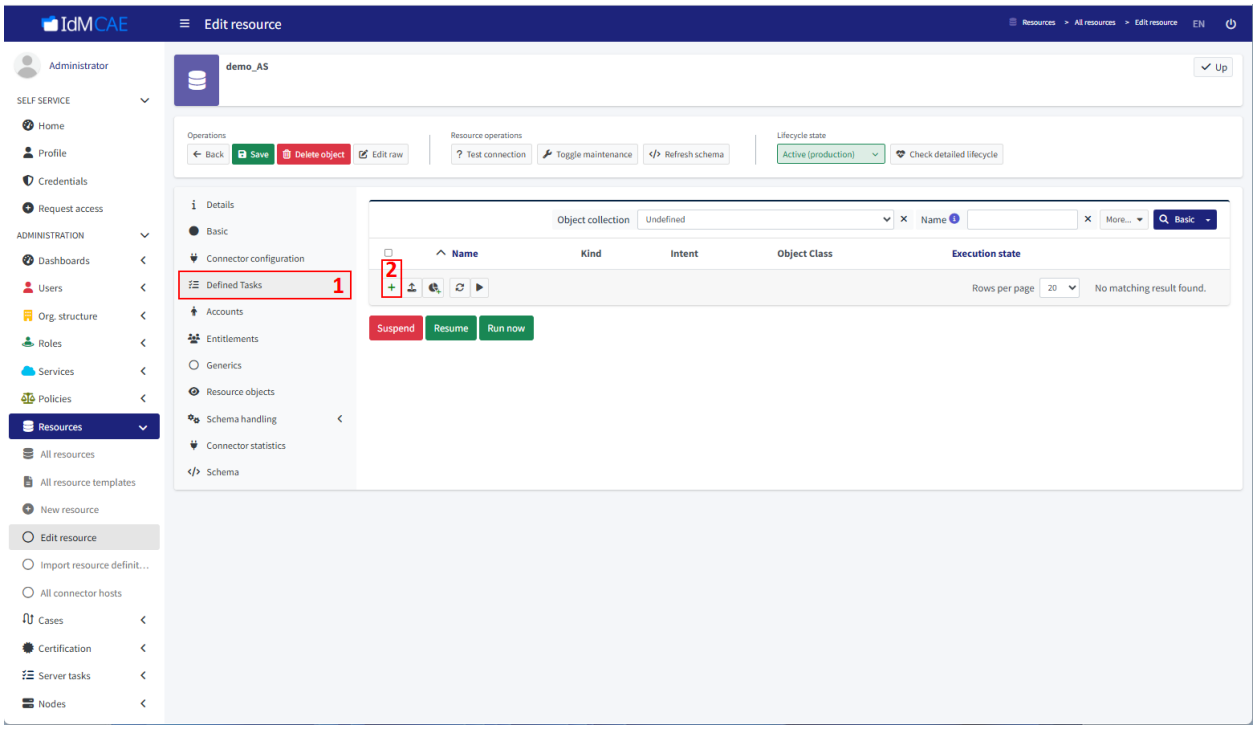


Рисунок 77 – Переход к созданию задания ресурса

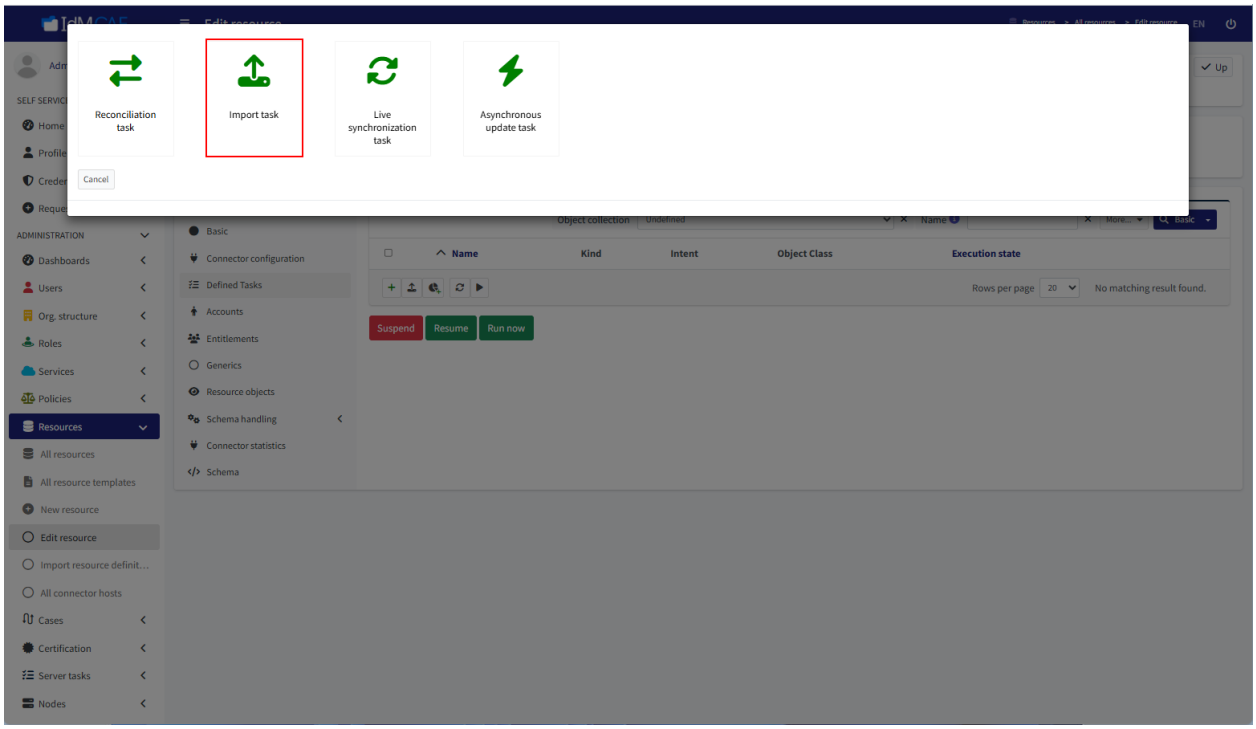


Рисунок 78 – Выбор типа создаваемого задания

4. В последующих окнах **Basic / Resource objects / Distribution** (1, рисунок 79) укажите значения атрибутов. В поле **Kind** укажите **Account**, если задача касается работы с УЗ, **Entitlement** – если задача касается работы с группами / ролями. Для сохранения нажмите **Save&Run** (2, рисунок 79).

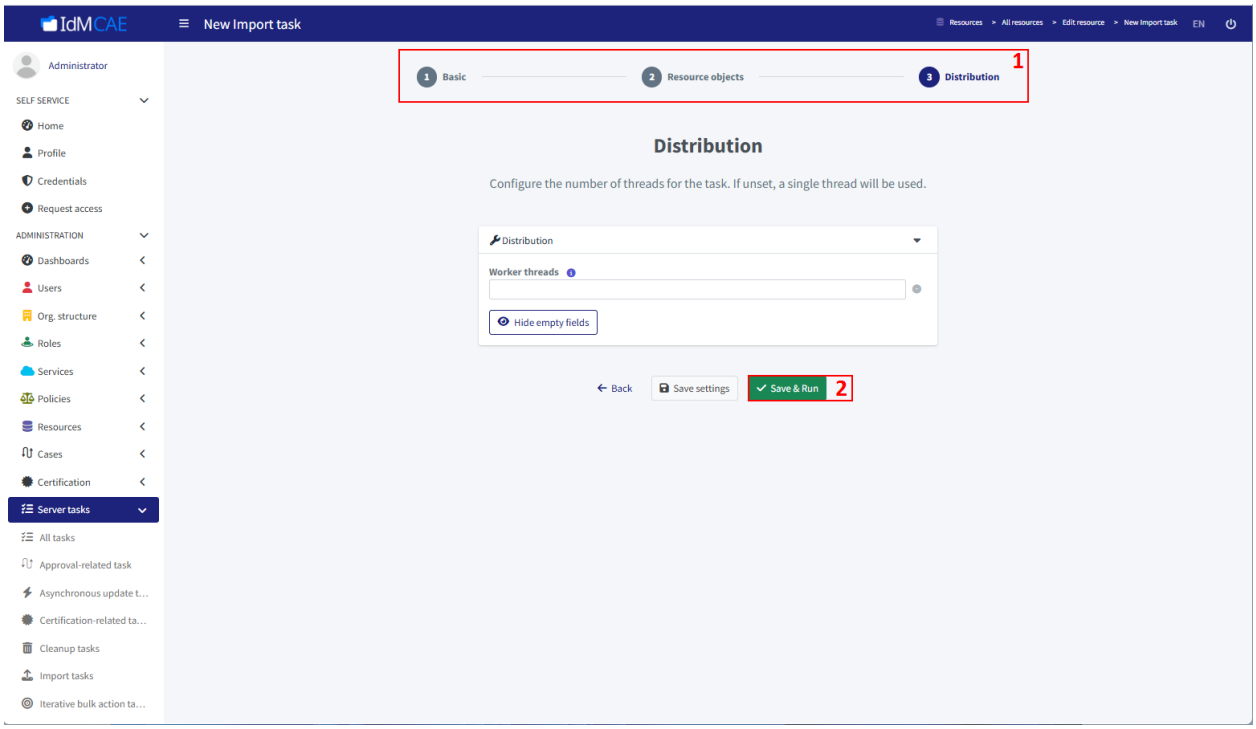


Рисунок 79 – Сохранение создаваемого задания

7.1.2.10. Настройка регулярных заданий ресурса

Для настройки регулярных заданий ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 80). Выберите нужный ресурс в общем списке (2, рисунок 80).

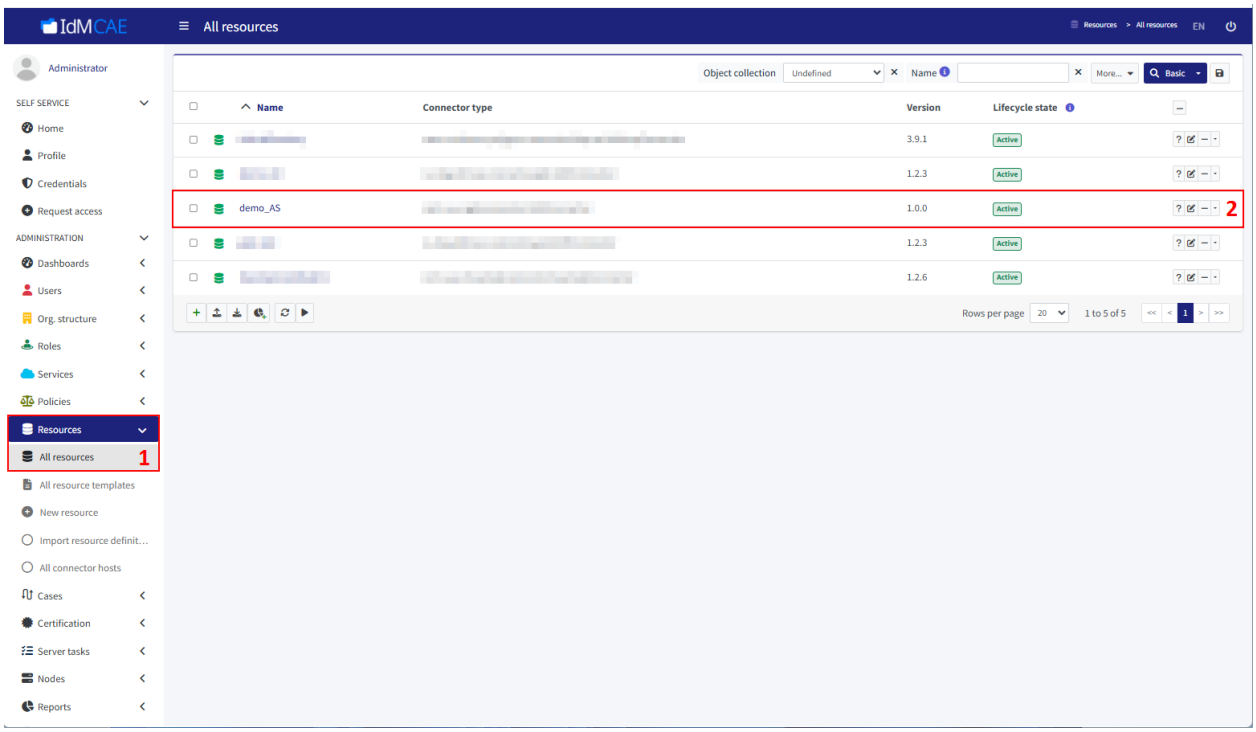


Рисунок 80 – Переход к ресурсу

3. Перейдите на вкладку **Defined Tasks** (1, рисунок 81). Выберите нужное задание (2, рисунок 81).

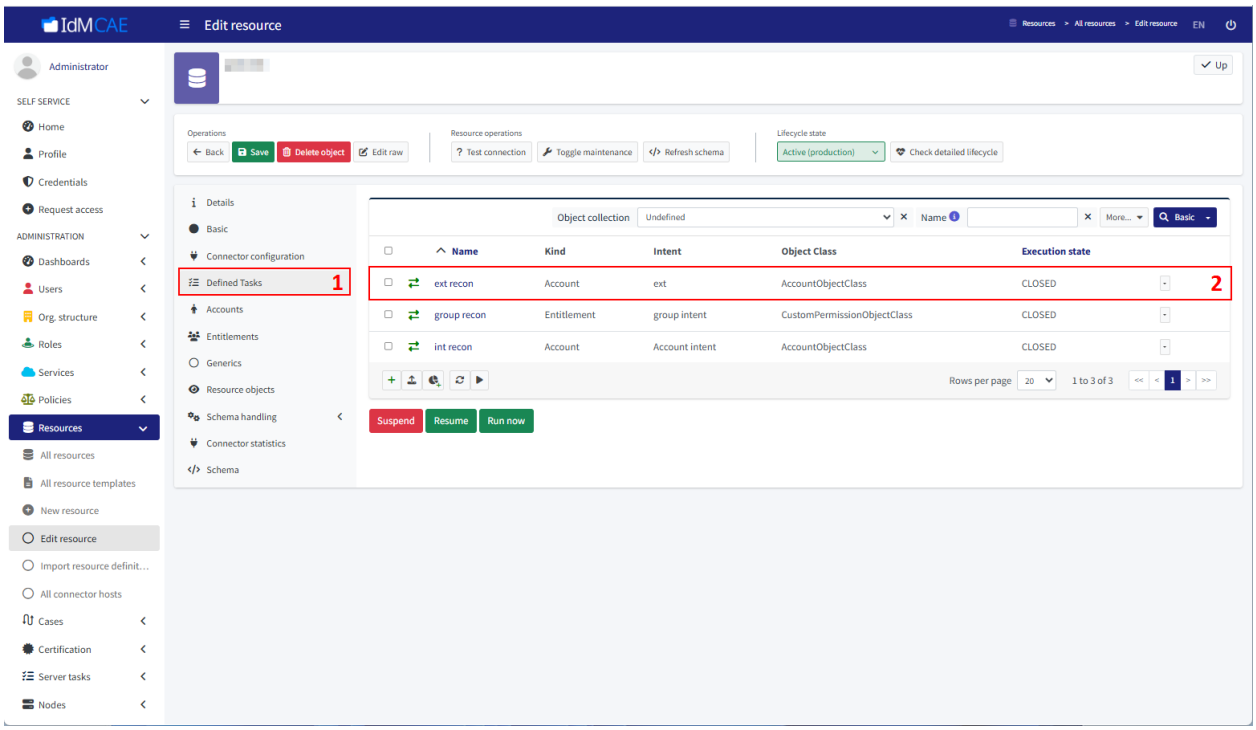


Рисунок 81 – Выбор задания ресурса

4. Перейдите на вкладку **Schedule** (1, рисунок 82) и укажите значения полей (2, рисунок 82):

a. **Interval** – определяет интервал запуска задачи в секундах (задача будет запускаться каждые N секунд);
b. **Cron-like pattern** – определяет расписание запуска задачи (расписание указывается в формате Cron);
c. **Earliest start time** и **Latest start time** – определяется промежуток времени, в который будет запускаться задача.

Сохраните изменение, нажав на **Save** (3, рисунок 82).

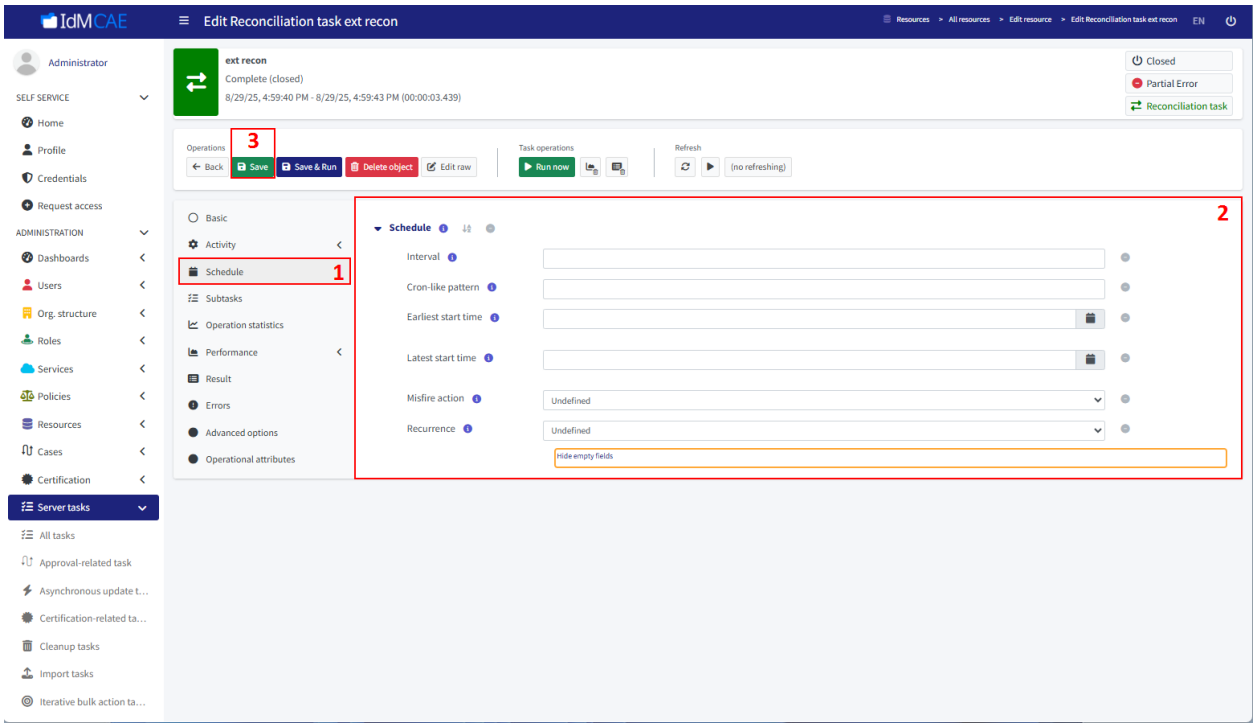


Рисунок 82 – Настройка регулярных заданий

7.1.2.11. Настройка маппинга для объектов ресурса

Для настройки маппинга для объектов ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).

2. Слева в меню выберите **Resources -> All resources** (1, рисунок 83). Выберите нужный ресурс в общем списке (2, рисунок 83).

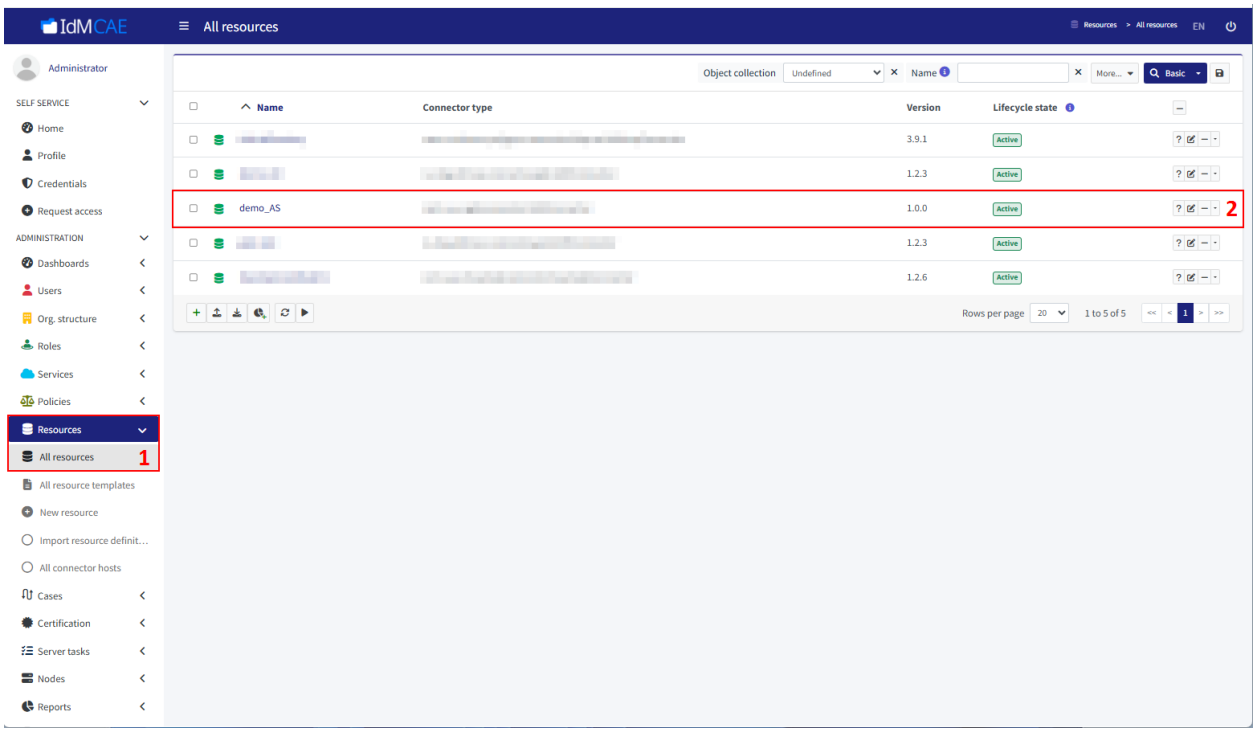


Рисунок 83 – Переход к ресурсу

3. Перейдите на вкладку **Schema handling -> Object types** (1, рисунок 84) и нажмите **Add object type** (2, рисунок 84).

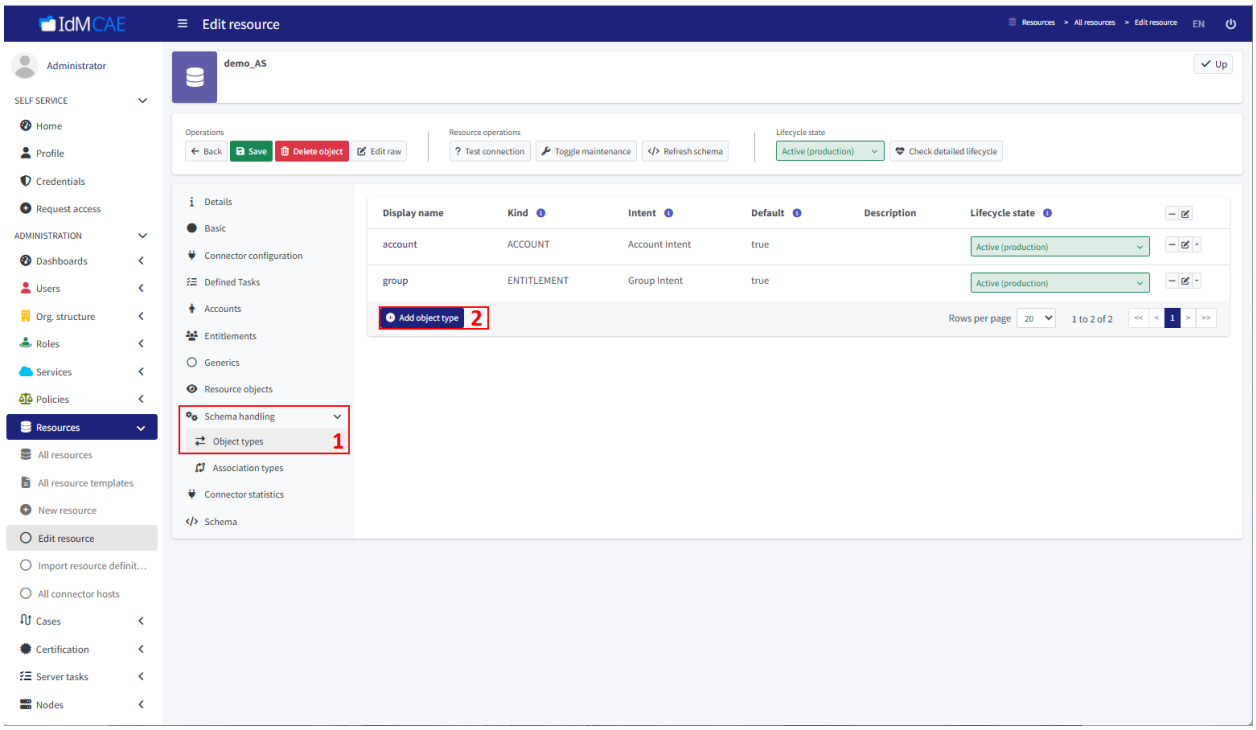


Рисунок 84 – Добавление объекта ресурса

4. В появившемся окне обязательно заполните поле **Kind**, остальные поля – при необходимости и сохраните настройки (рисунок 85).

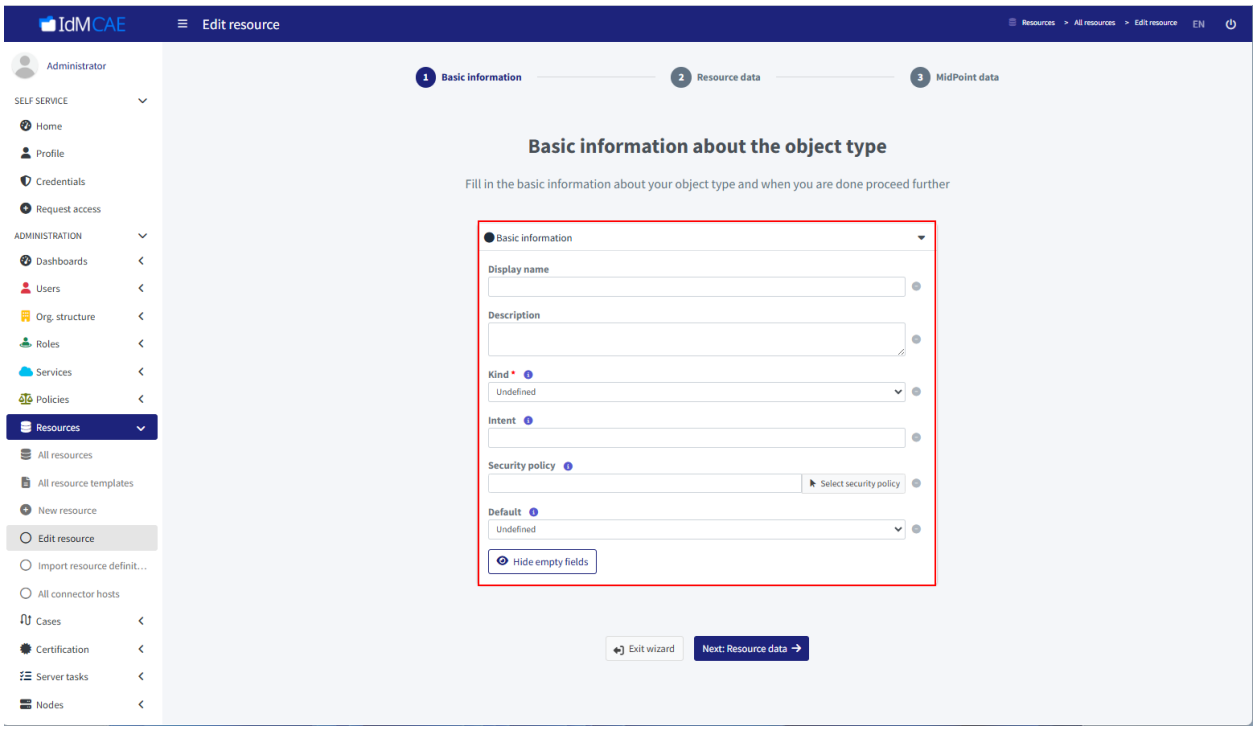


Рисунок 85 – Настройки объекта ресурса

5. На вкладке **Schema handling -> Object types** выберите созданный ранее объект и выберите **Mappings** (рисунок 86).

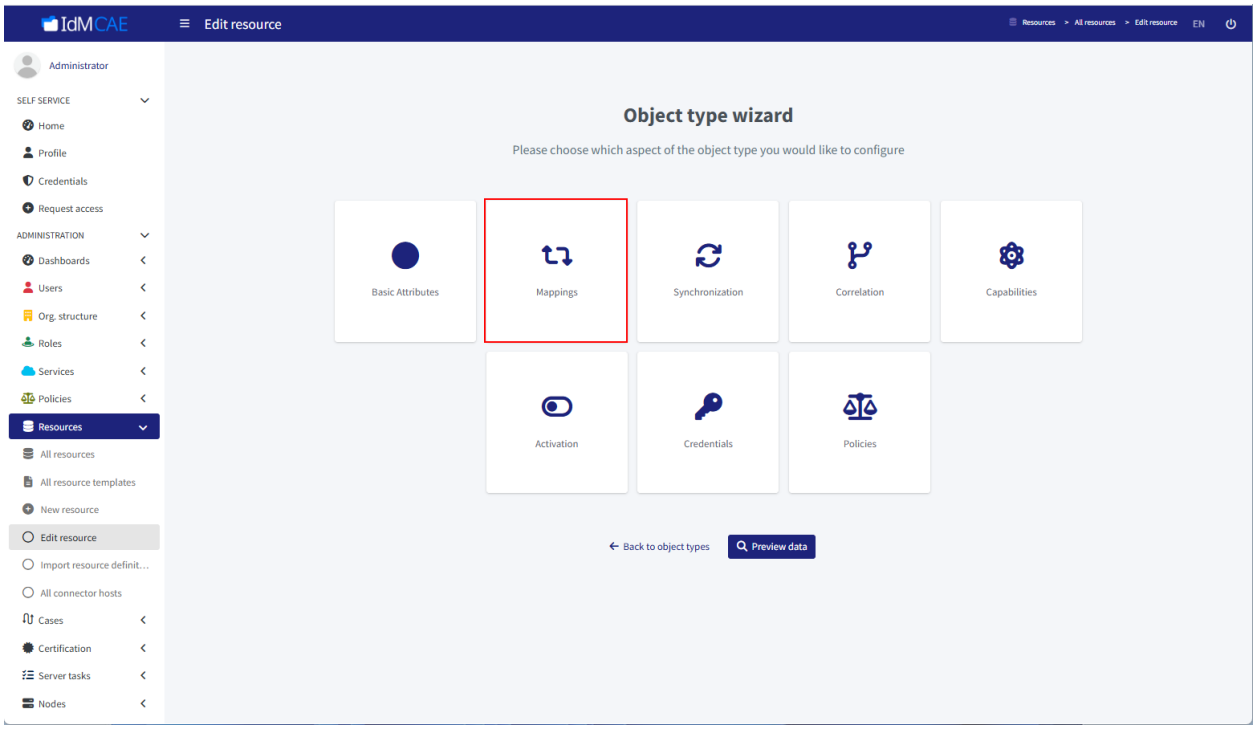


Рисунок 86 – Переход к настройке маппинга

6. Заполните поля и сохраните настройки, нажав на **Save mappings** (рисунок 87). Описание заполняемых полей см. в разделе 6.2.2.2.

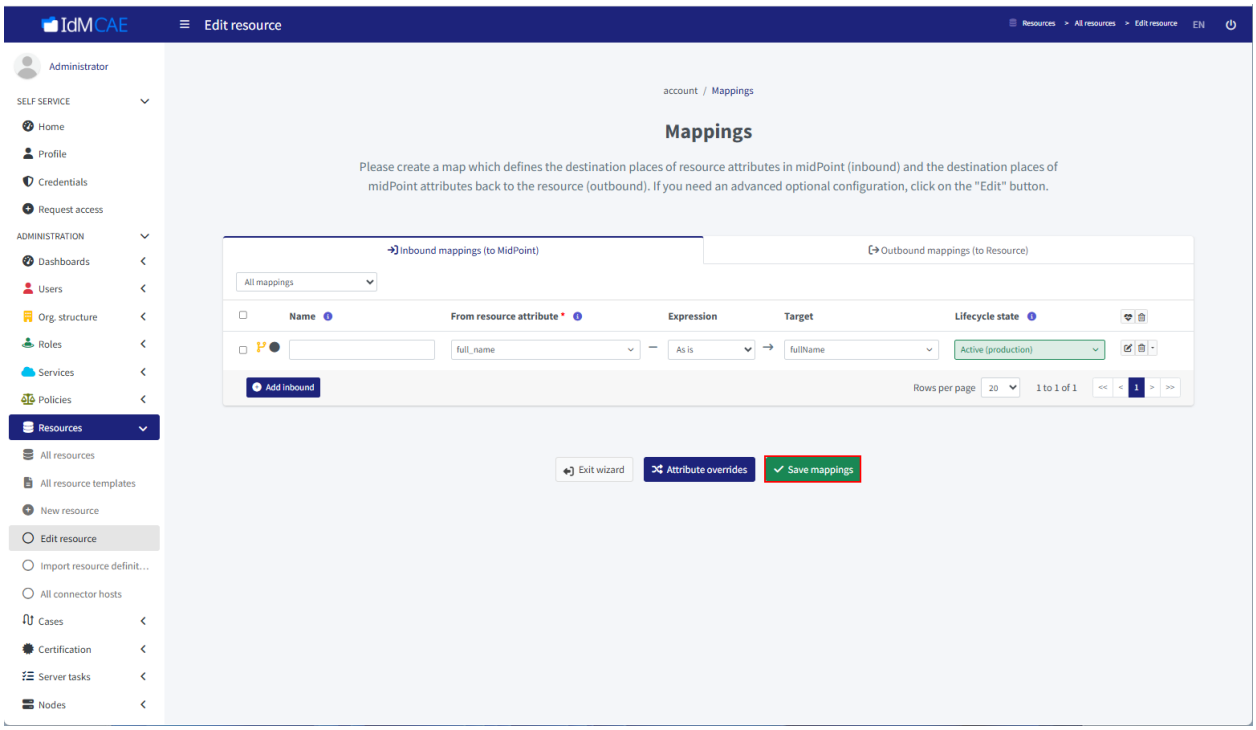


Рисунок 87 – Настройки маппинга

7.1.2.12. Настройка кэширования

Настройка кэширования обязательно требуется для типов объектов ресурса, для которого производится выявление конфликтов полномочий с помощью модуля IG.

Для настройки кэширования типов объектов ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 88). Выберите нужный ресурс в общем списке (2, рисунок 88).

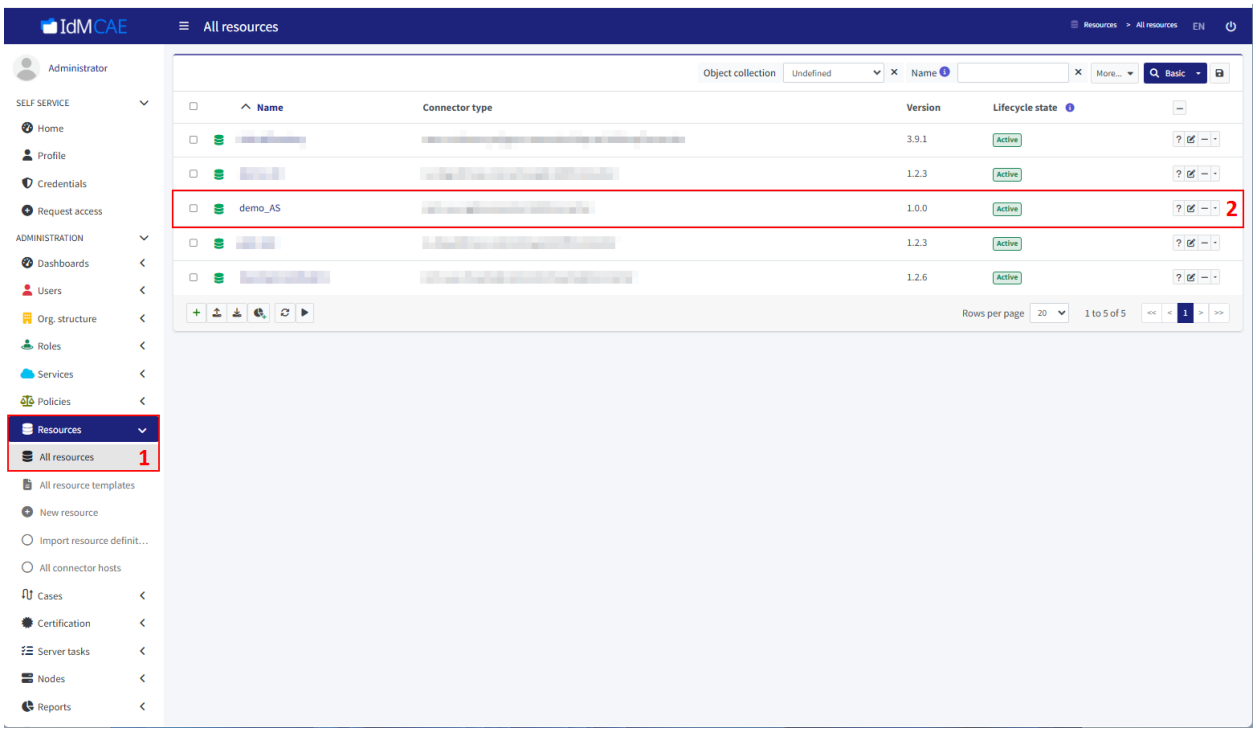


Рисунок 88 – Выбор ресурса

3. Перейдите к редактированию ресурса с помощью **Edit raw** (рисунок 89).

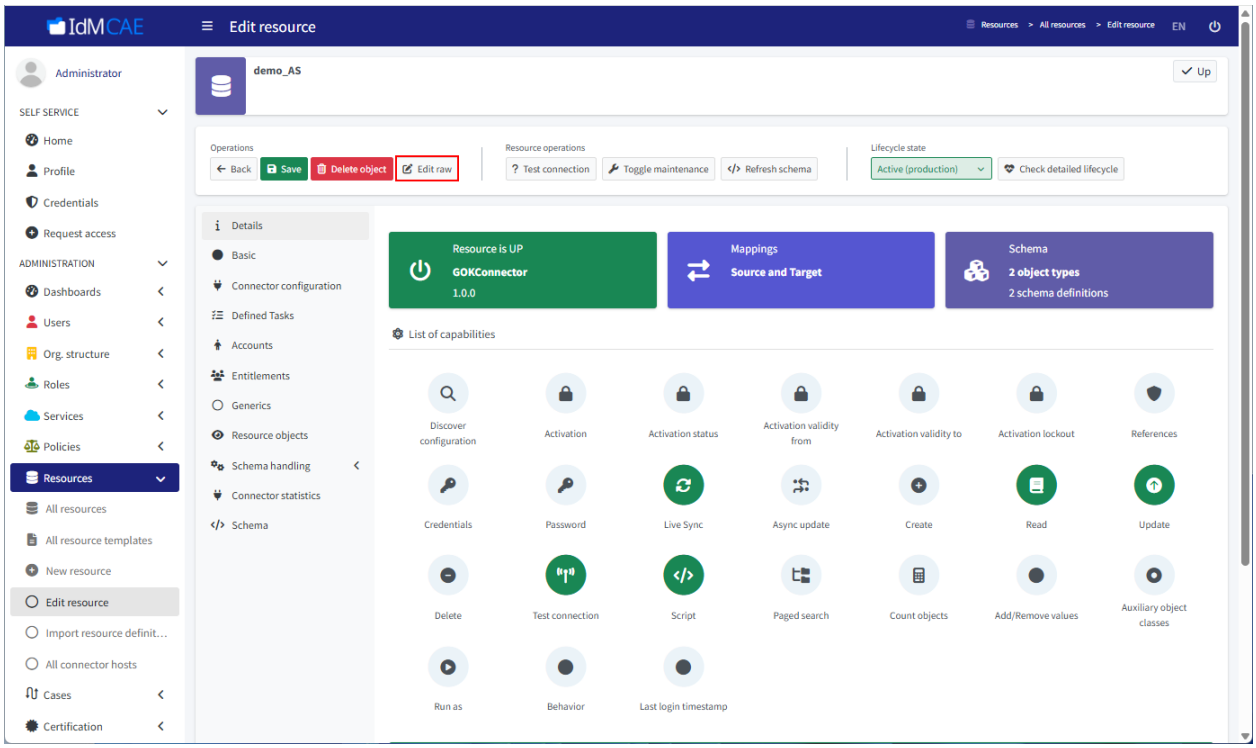


Рисунок 89 – Переход к редактированию ресурса

4. В секции **schemaHandling** для каждого типа объекта (1, рисунок 90) укажите листинг с учётом типа объекта

```
<caching>
    <cachingStrategy>passive</cachingStrategy>
    <scope>
        <attributes>all</attributes>
        <associations>none</associations>
    </scope>
    <timeToLive>P1D</timeToLive>
    <defaultCacheUse>useCachedOrFresh</defaultCacheUse>
</caching>
```

Придерживайтесь следующих правил при редактировании ресурса:

- используйте разные значения параметров для разных типов объектов:
    - для типа объекта **Account** укажите

    `<attributes>none</attributes>`
    `<associations>all</associations>`

    - для типа объекта **Group** укажите

    `<attributes>all</attributes>`
    `<associations>none</associations>`
- в секциии `timeToLive` укажите период, в течение которого закэшированные данные будут являться актуальными (один день в случае указания `P1D`, безлимитно в случае указания `unlimited`);
- в секции `defaultCacheUse` укажите, каким образом будут поступать данные о тенях (данные будут поступать напря-

мую из ресурса в случае указания `useFresh`, будут использоваться доступные закэшированные данные в случае указания `useCachedOrFresh`).

Нажмите на **Save** для сохранения (2, рисунок 90).

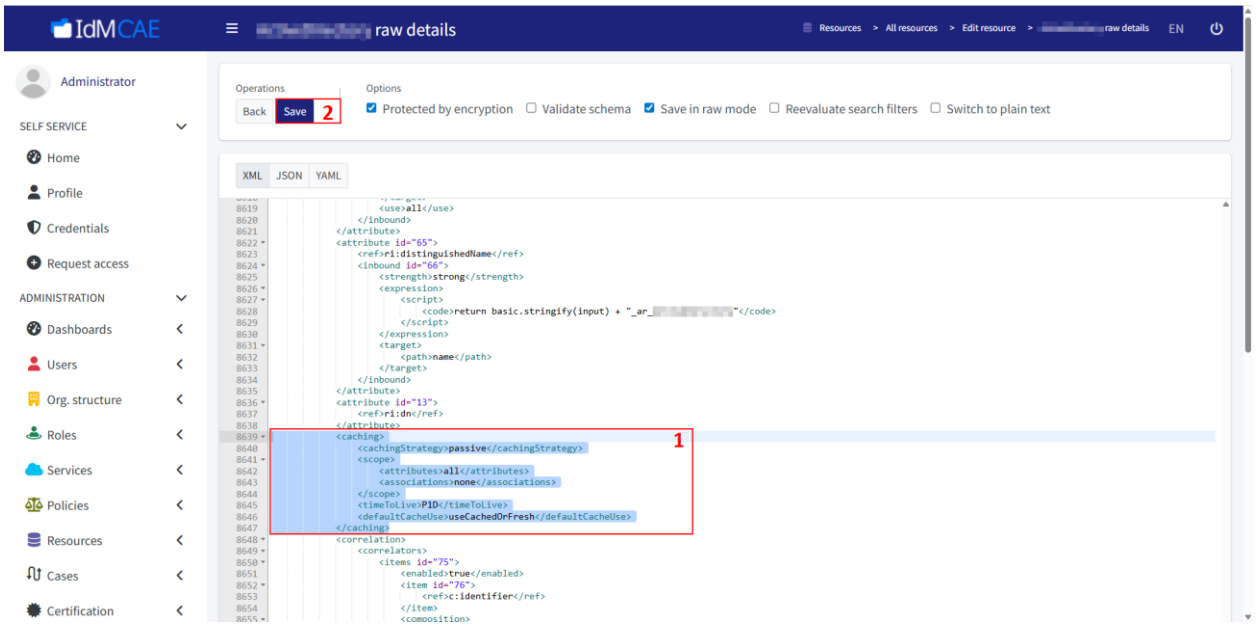


Рисунок 90 – Настройка кэширования типов объекта ресурса

7.1.3. Управление пользователями

7.1.3.1. Ручное создание пользователя

Для ручного создания пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> New user** (1, рисунок 91).

   Выберите тип пользователя:

   - **Person** – если требуется создать пользователя с архетипом Person;
   - **All Users** – если требуется создать пользователя без архетипа.

В открывшемся окне **New user** на вкладке **Basic** (2, рисунок 91) обязательно заполните поле **Name** (3, рисунок 91), остальные – по желанию.

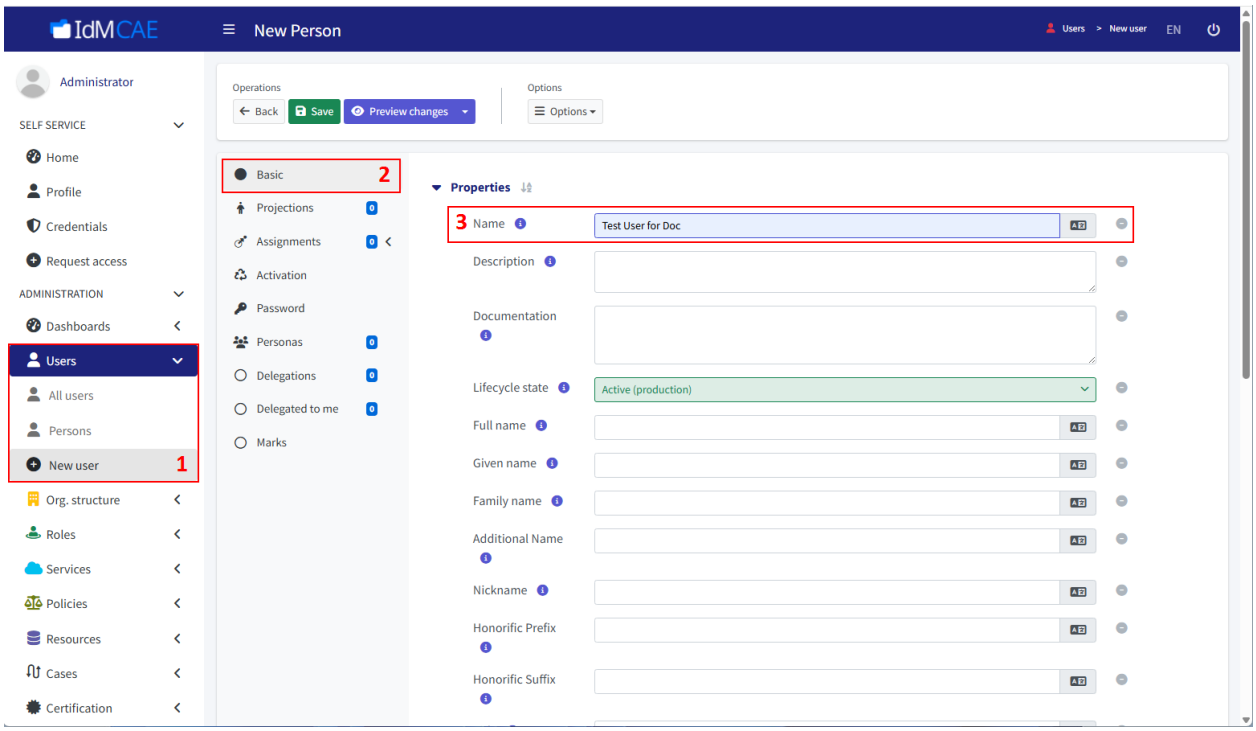


Рисунок 91 – Добавление нового пользователя

3. При необходимости перейдите на вкладку **Password** (1, рисунок 92) и задайте в поле **Value** пароль согласно установленной парольной политике (2, рисунок 93).

Подсказка: необязательно устанавливать пароль в момент создания пользователя, это можно будет сделать позже.

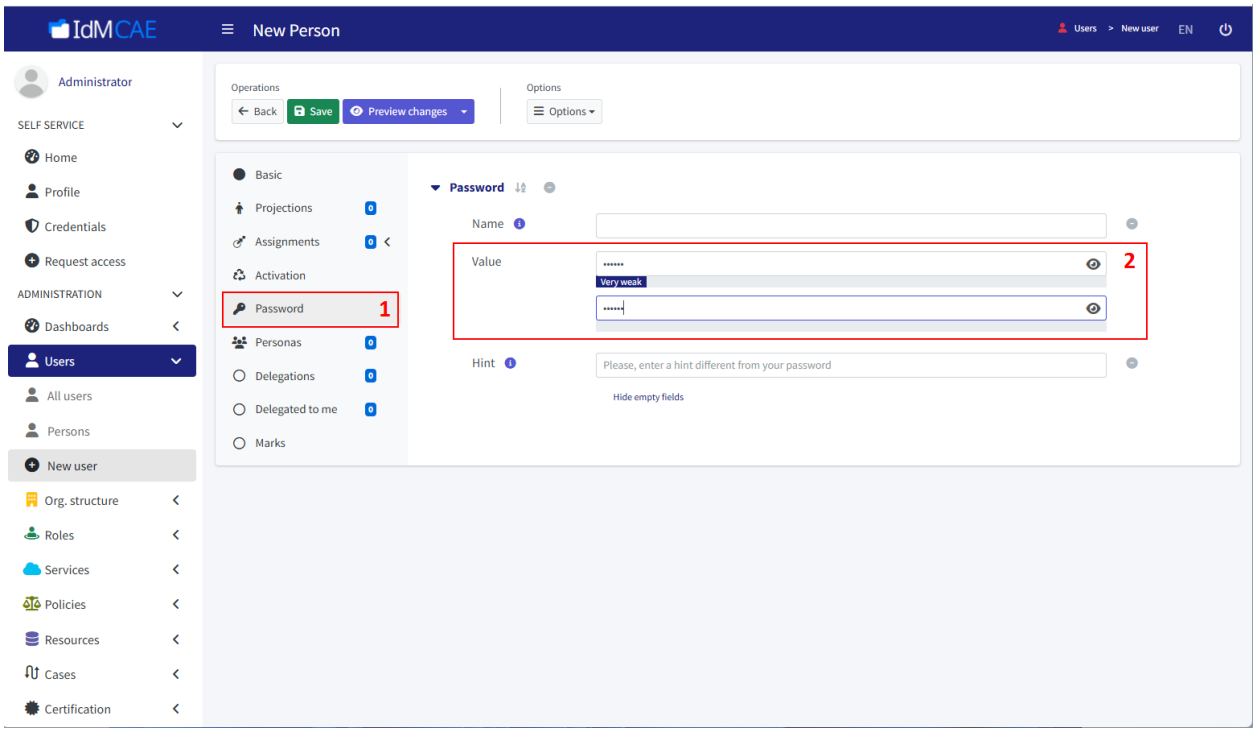


Рисунок 94 – Установка пароля

4. Перейдите на вкладку **Assignments -> Roles** (1, рисунок 95). Нажмите на  для добавления роли (2, рисунок 95). Из списка ролей с помощью проставления флага выберите роль, которую нужно назначить создаваемому пользователю (1, рисунок 96), нажмите на **Add** (2, рисунок 96). Обратите внимание, что назначаемая роль должна содержать необходимый набор прав, в том числе для возможности входа в веб-интерфейс компонента Provisioning Management.

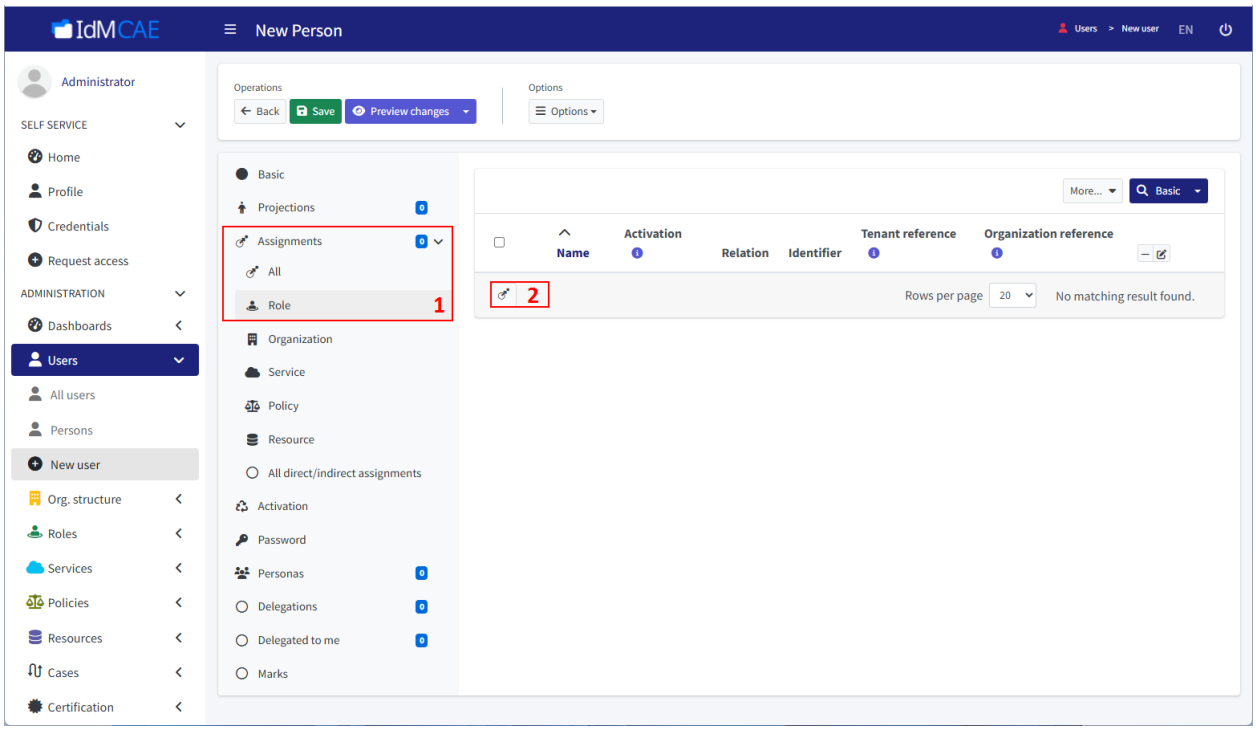


Рисунок 95 – Переход к назначению роли

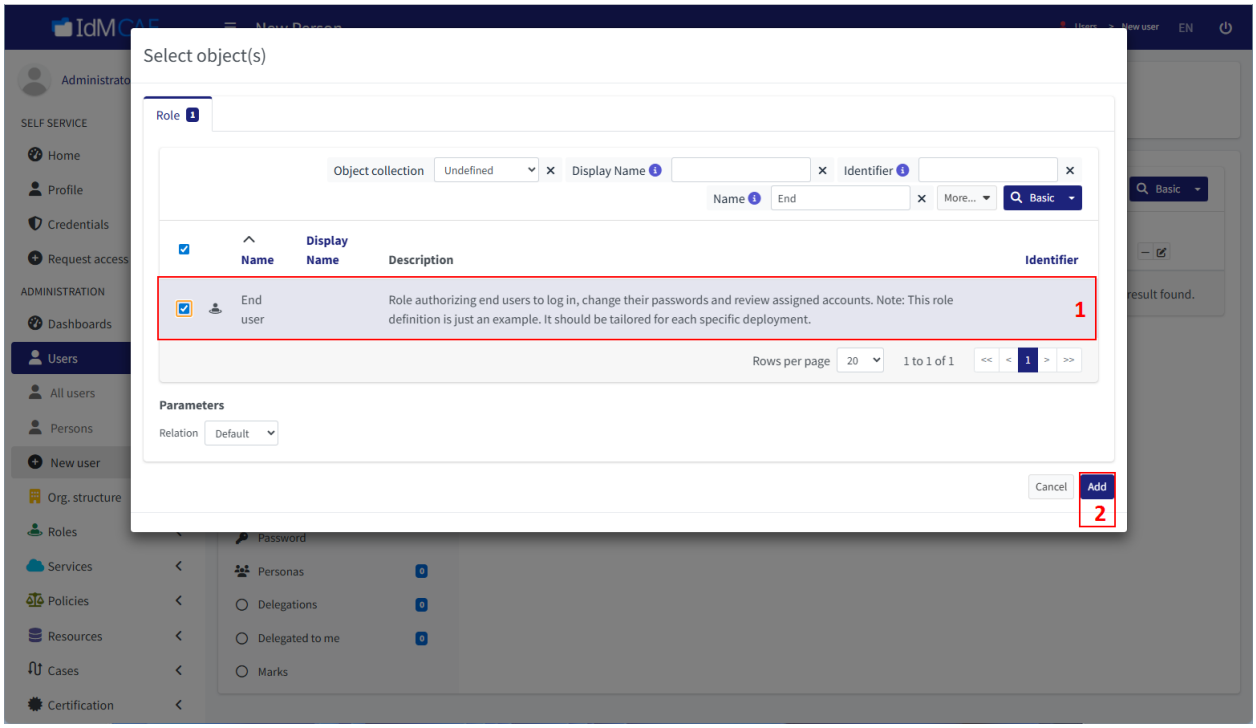


Рисунок 96 – Выбор роли

5. Нажмите на **Save** (рисунок 97). Произойдёт автоматический переход в окно со списком пользователей, где будет отображён и созданный пользователь (рисунок 98).

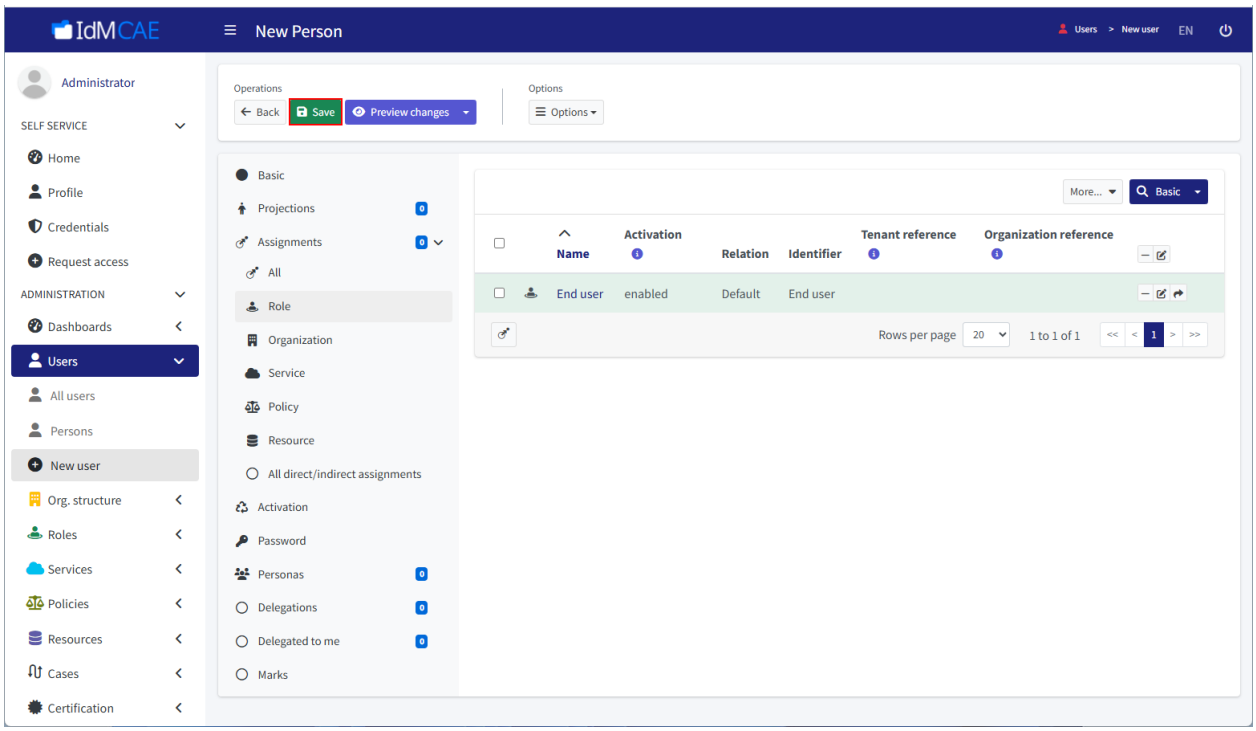


Рисунок 97 – Сохранение созданного пользователя

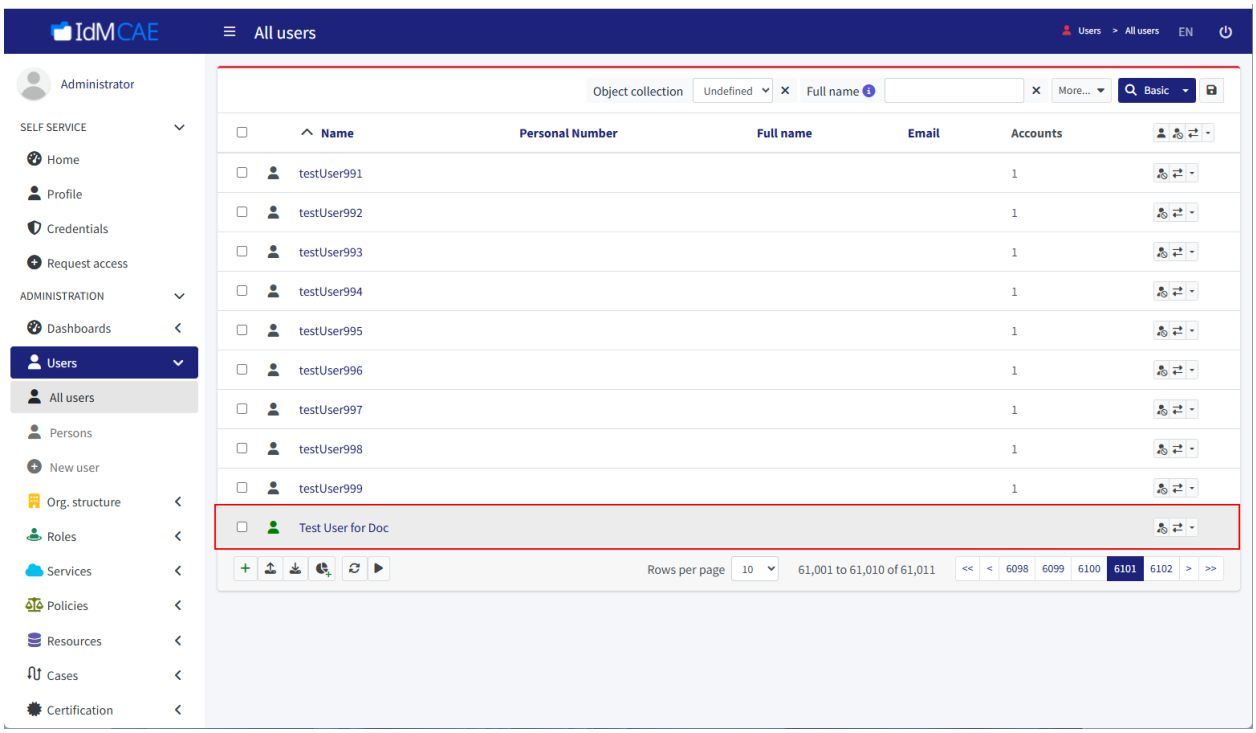


Рисунок 98 – Общий список пользователей

7.1.3.2. Создание пользователей на основе импортированных УЗ

Для создания пользователей на основе импортированных УЗ выполните следующие шаги:

1. Шаги, описанные в разделе 7.1.2.5.
2. Перейдите к настройкам параметров синхронизации через **Configure -> Synchronization** (рисунок 99).

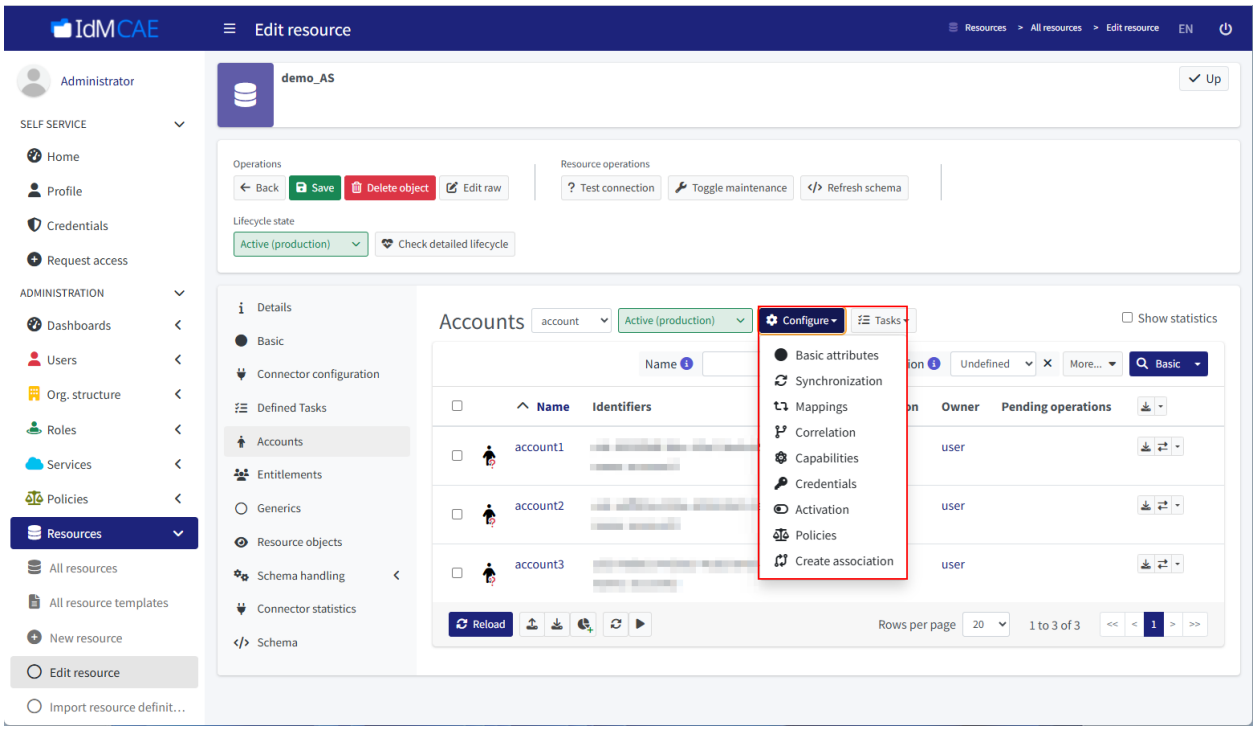


Рисунок 99 – Переход к параметрам синхронизации / маппинга / корреляции

3. Выполните настройку параметров синхронизации в соответствии с разделом 7.1.9.
4. Перейдите к настройкам параметров маппинга через **Configure -> Mappings** и корреляции через **Configure -> Correlation** (рисунок 99) и выполните их настройку.
5. Создайте задание для ресурса (подробнее см. в разделе 7.1.2.9).
6. Запустите созданную задачу и в результате в IDM CAE будут созданы пользователи, связанные с соответствующими УЗ из HR-ресурса (рисунок 100).

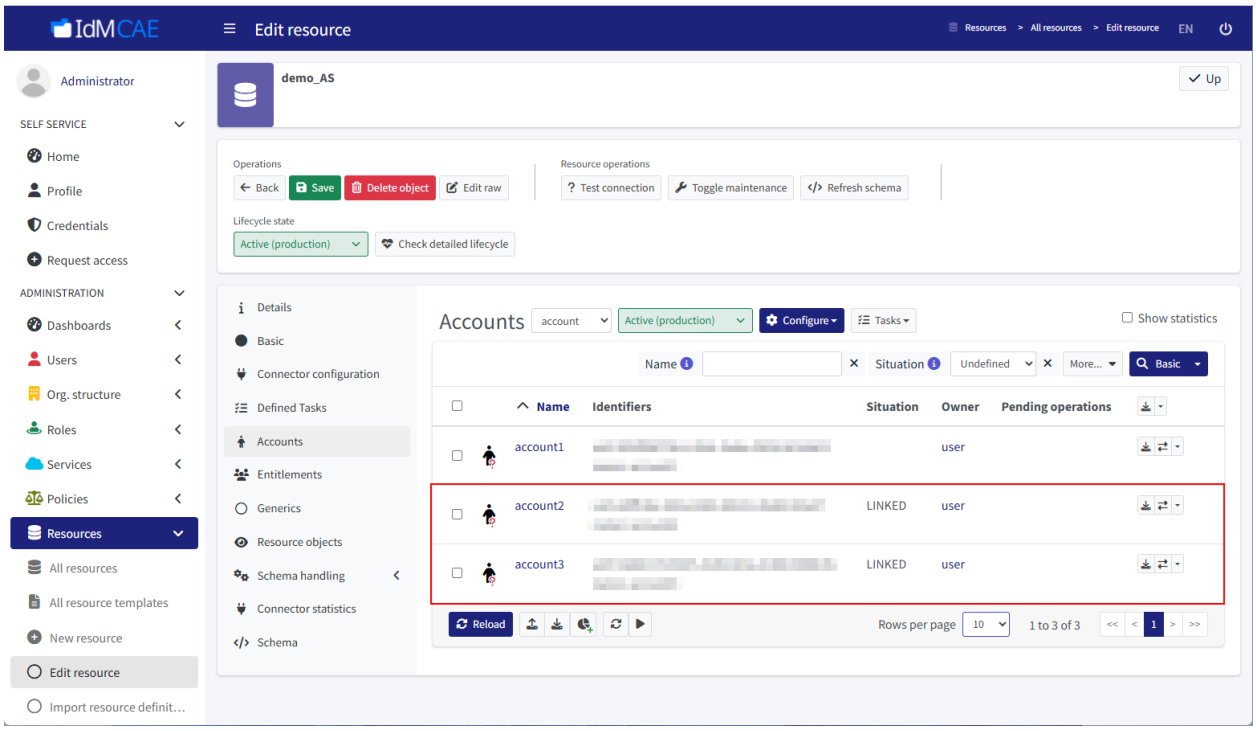


Рисунок 100 – Связанные с пользователями УЗ

7.1.3.3. Ручное изменение пользователя

Для ручного изменения пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> All users** (1, рисунок 101). Выберите нужного пользователя (2, рисунок 101).

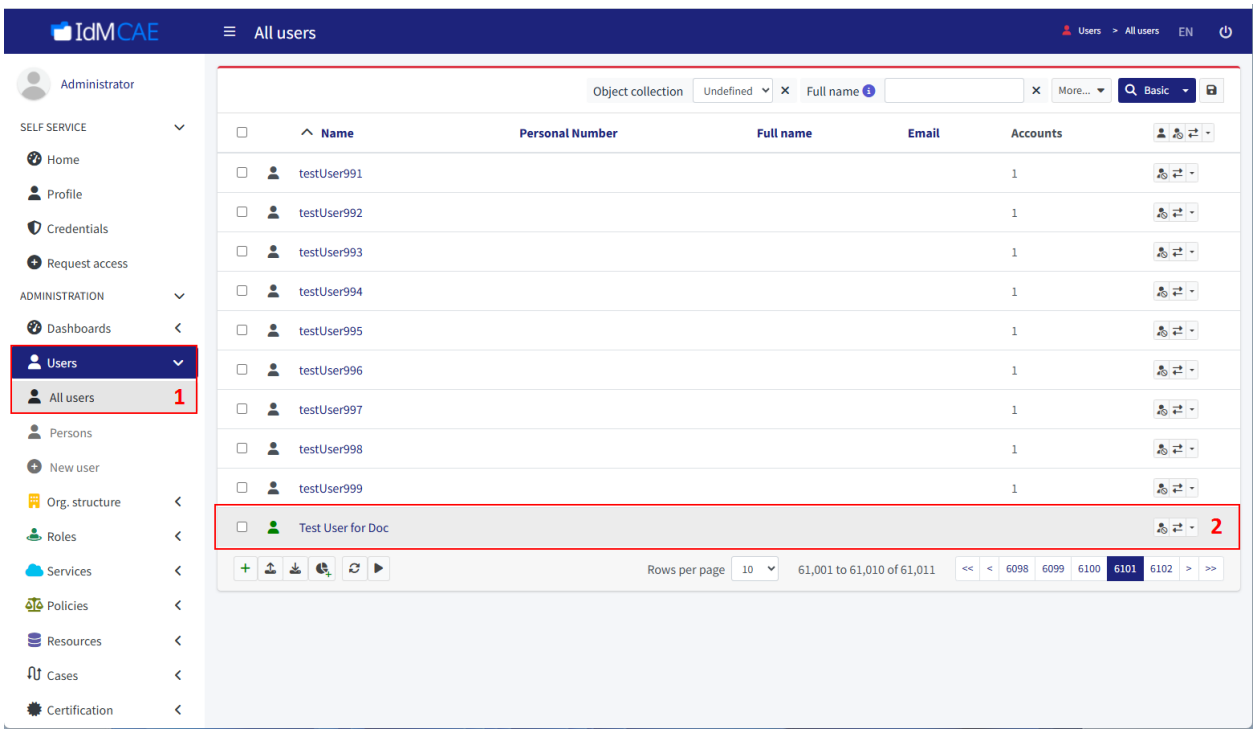


Рисунок 101 – Выбор пользователя

3. Укажите новые параметры на вкладках и сохраните изменения, нажав на **Save** (рисунок 102).

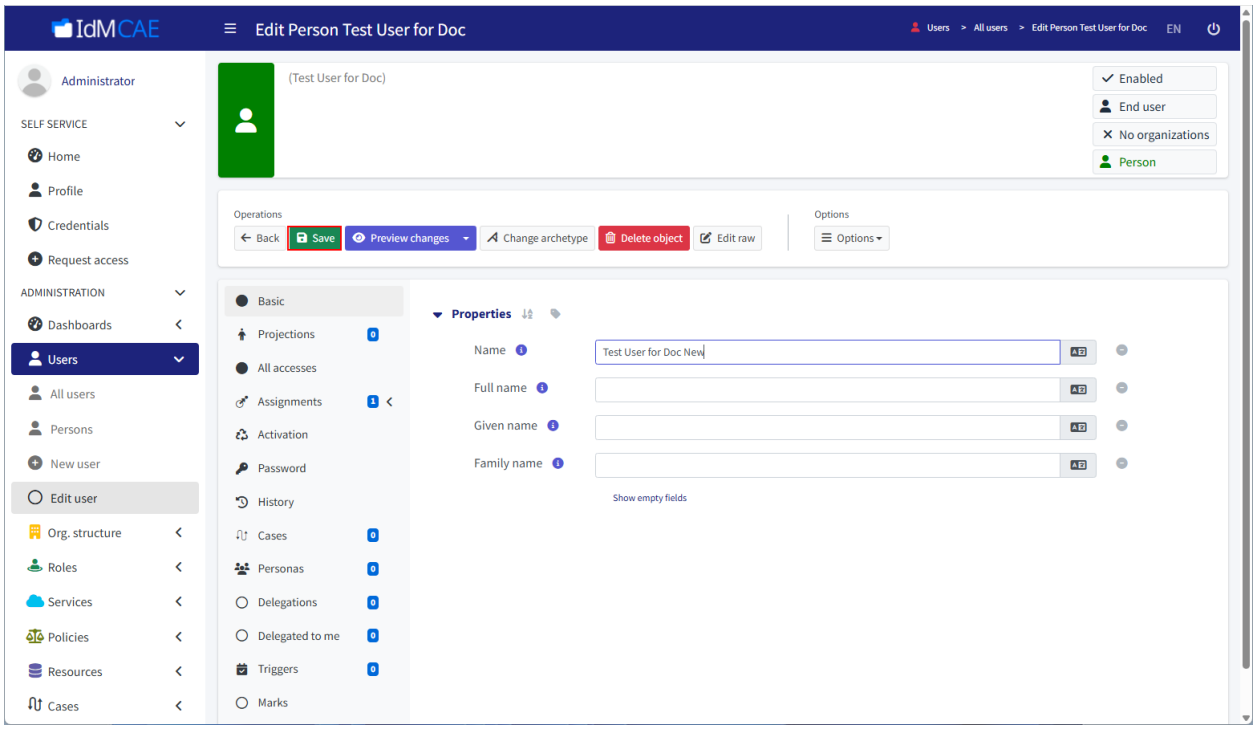


Рисунок 102 – Сохранение изменений пользователя

7.1.3.4. Ручная блокировка / разблокировка пользователя

Для ручной блокировки / разблокировки пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> All users** (1, рисунок 103). Выберите нужного пользователя (2, рисунок 103).

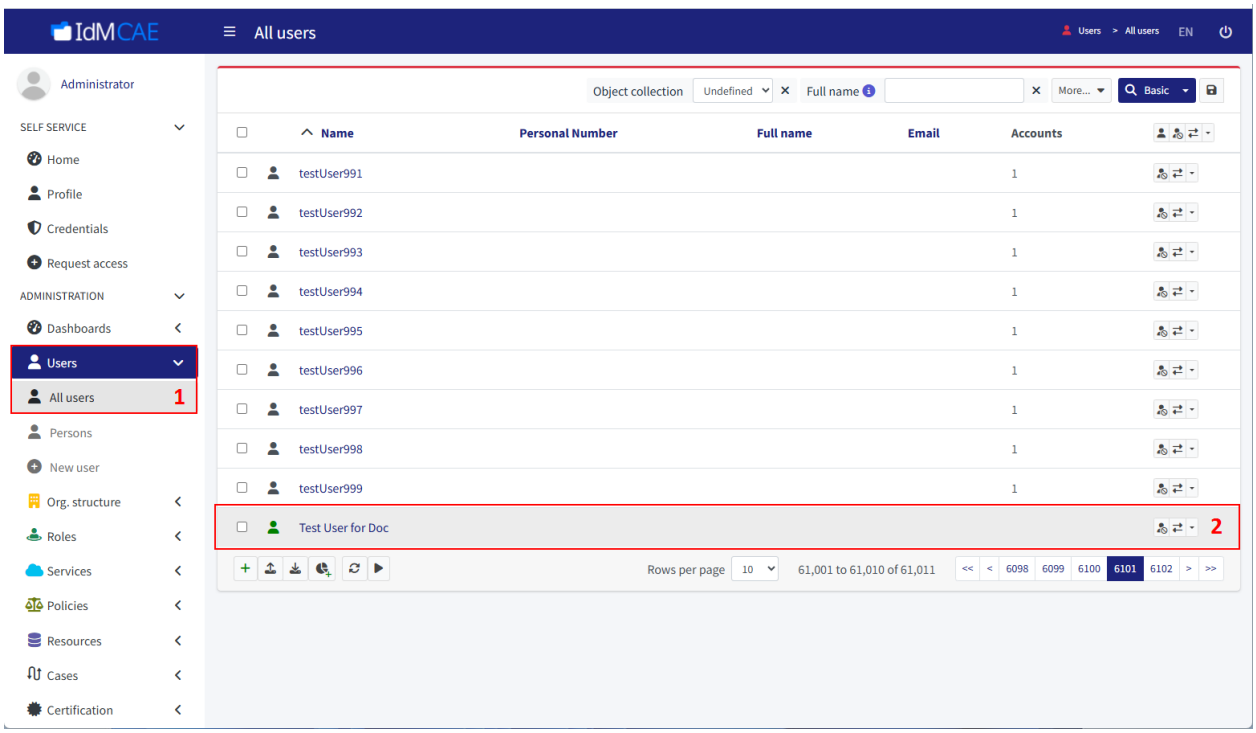


Рисунок 103 – Выбор пользователя

3. Перейдите на вкладку **Activation** (1, рисунок 104). Установите в поле **Administrative status** необходимый статус (2, рисунок 104). Сохраните изменения, нажав на **Save** (3, рисунок 104). Возможные значения статуса с описаниями представлены в таблице 5.

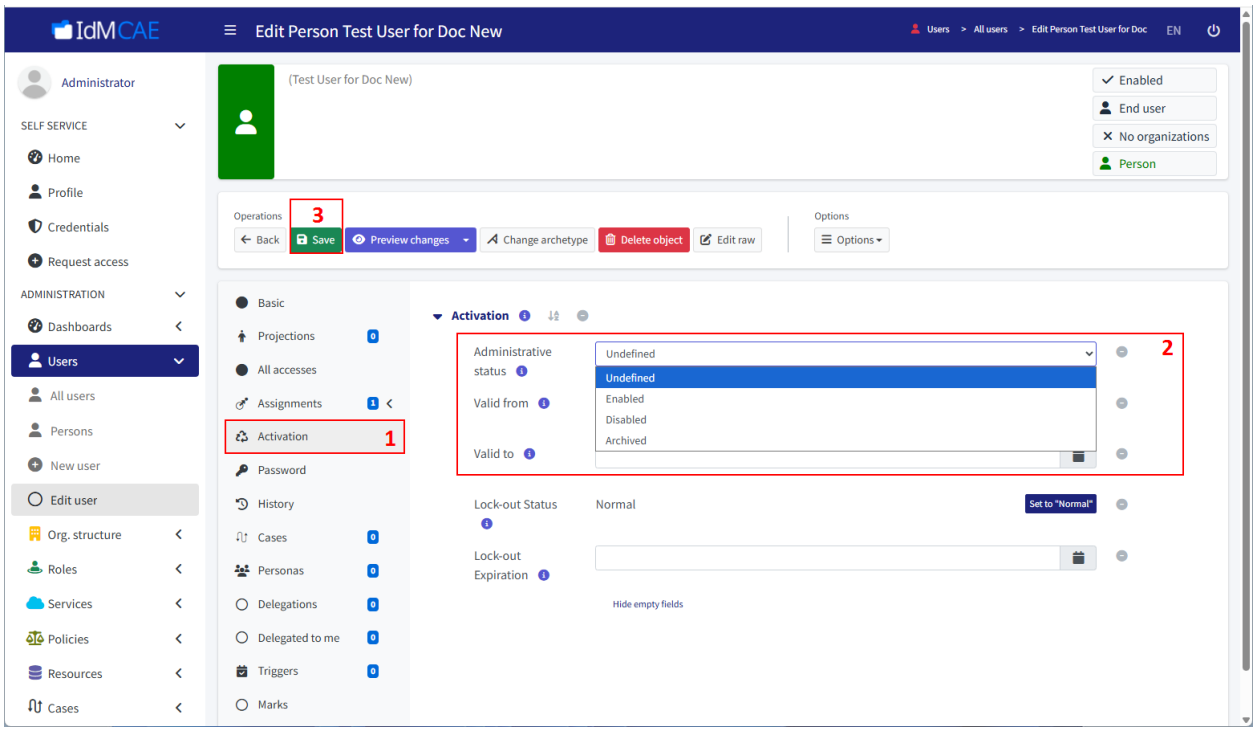


Рисунок 104 – Изменение поля Administrative status

При блокировании пользователя все существующие проекции и назначения сохраняются, пользователь лишается возможности входа.

7.1.4. Управление УЗ пользователей

7.1.4.1. Ручное создание УЗ пользователя

Для ручного создания УЗ пользователей требуется, чтобы в ресурсе, в котором создаётся УЗ, были настроены исходящие маппинги и правила корреляции.

Для создания УЗ пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> All users** (1, рисунок 105). Выберите нужного пользователя (2, рисунок 105).

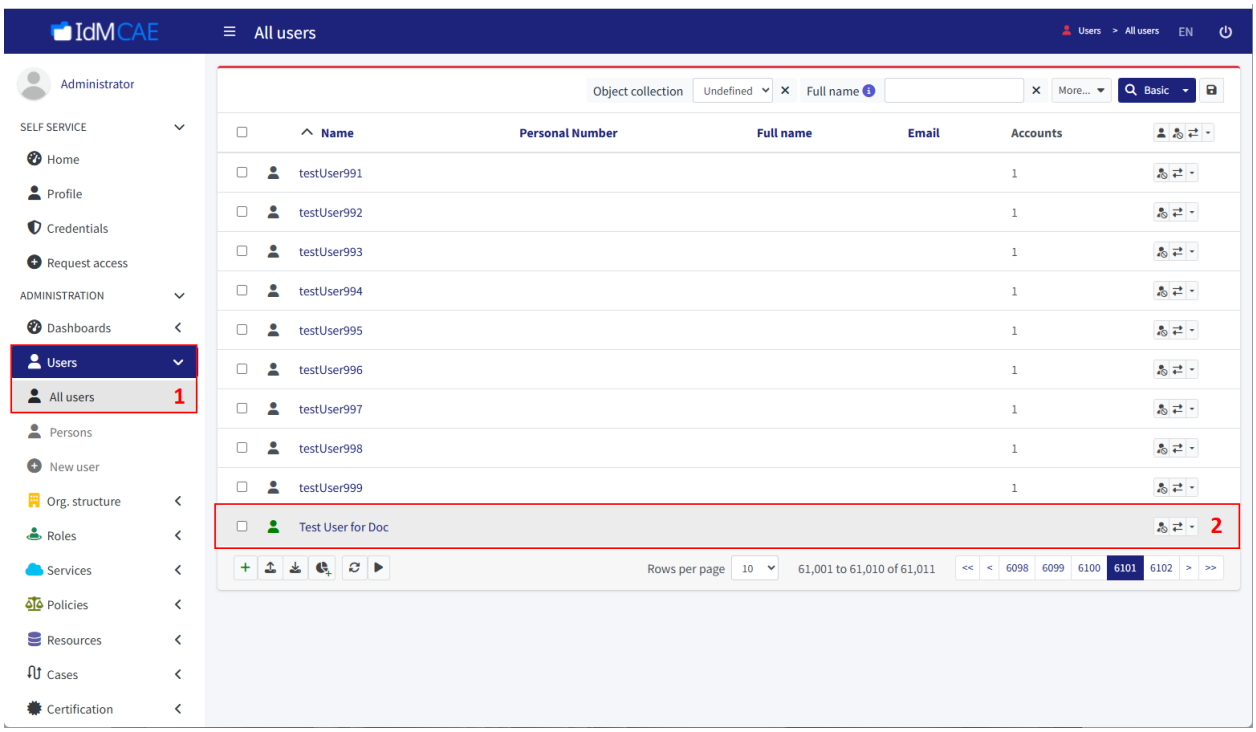


Рисунок 105 – Выбор пользователя

3. Перейдите на вкладку **Projections** (1, рисунок 106) и нажмите на [+] (2, рисунок 106).

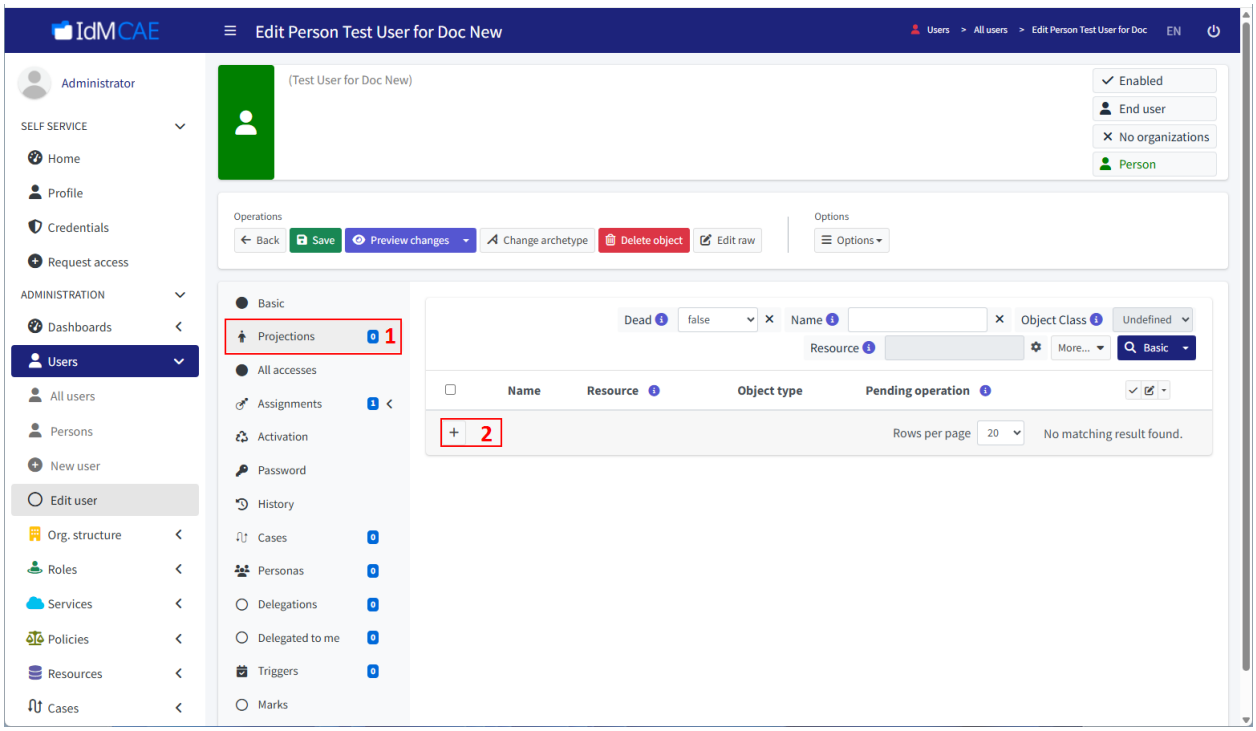


Рисунок 106 – Переход к созданию УЗ пользователя

4. В всплывающем окне проставьте флаг слева ресурса, в котором нужно создать УЗ и нажмите на **Add** (рисунок 107).

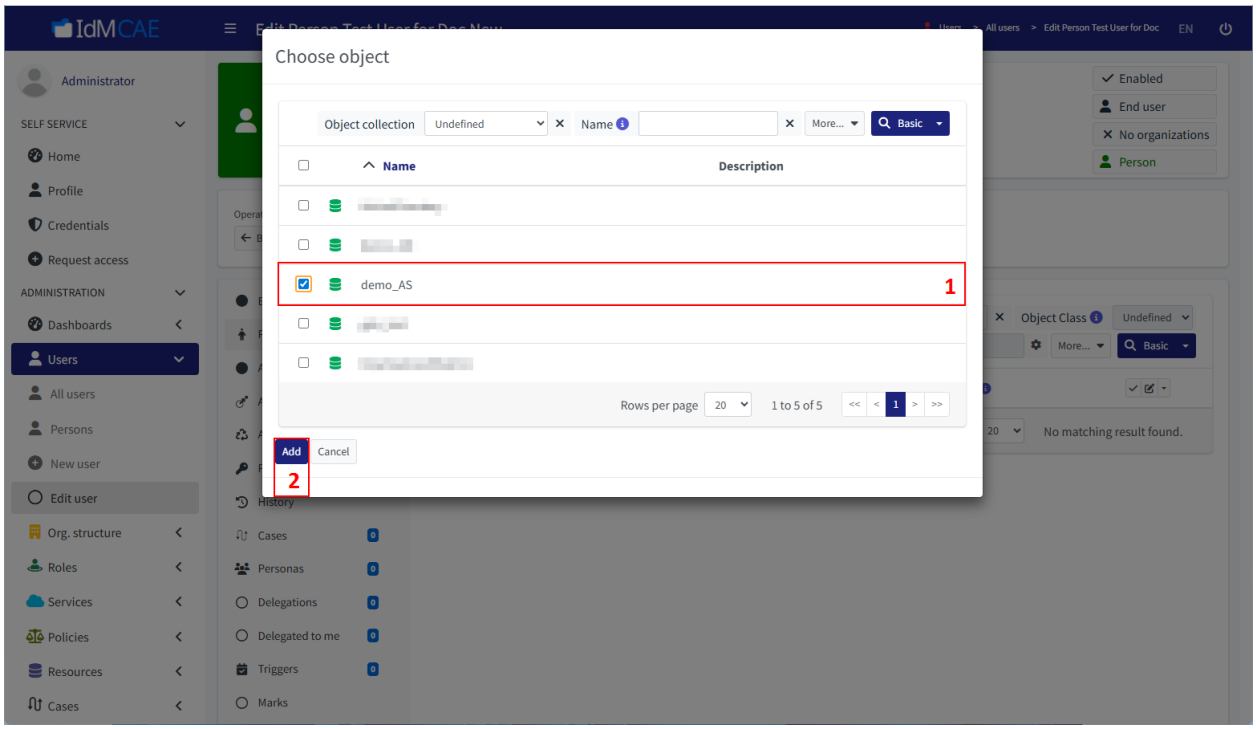


Рисунок 107 – Создание УЗ пользователя

5. Перейдите на вкладку **Password** (1, рисунок 108) и убедитесь, что пароль задан и соответствует парольной политике ресурса. Сохраните изменения, нажав на **Save** (2, рисунок 108).

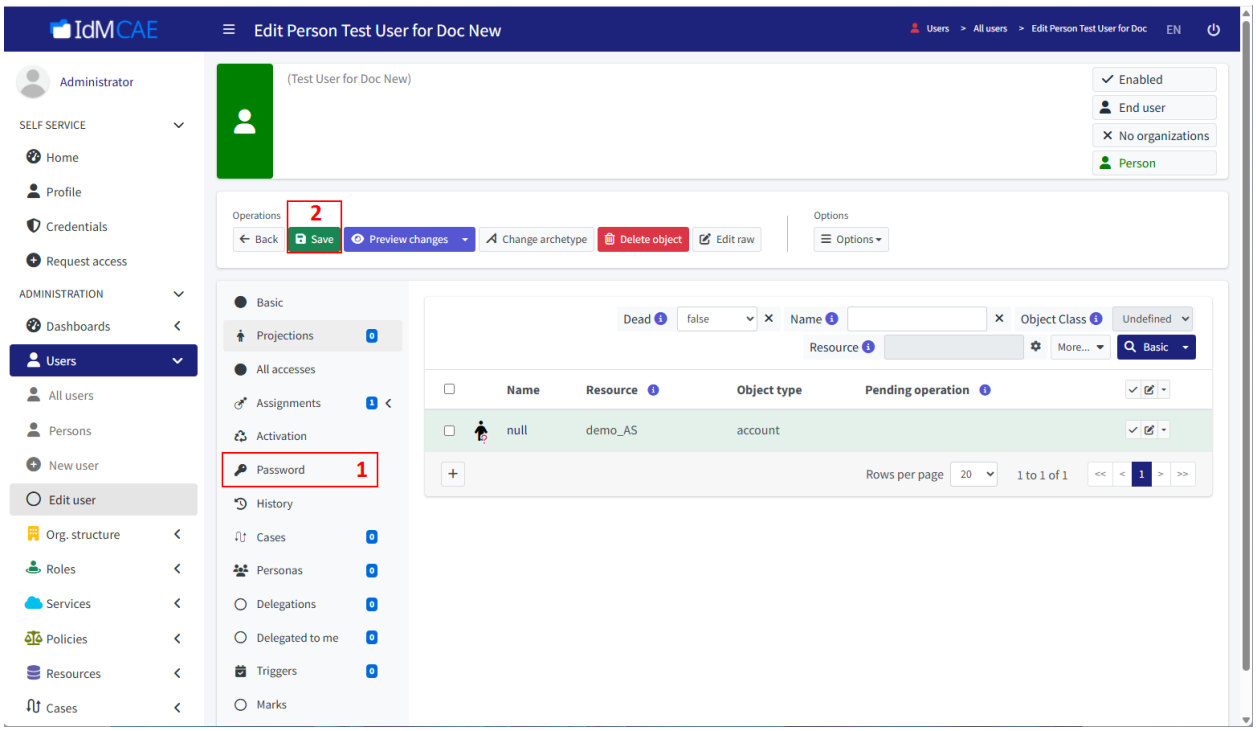


Рисунок 108 – Сохранение изменений

6. Откройте созданную УЗ и убедитесь, что атрибуты (рисунок 109) заполнены в соответствии с существующим маппингом объекта ресурса (слева у таких атрибутов есть иконка). Также можно, нажав внизу окна **Show empty fields**, открыть полный список атрибутов объекта и указать значения к пустым атрибутам.

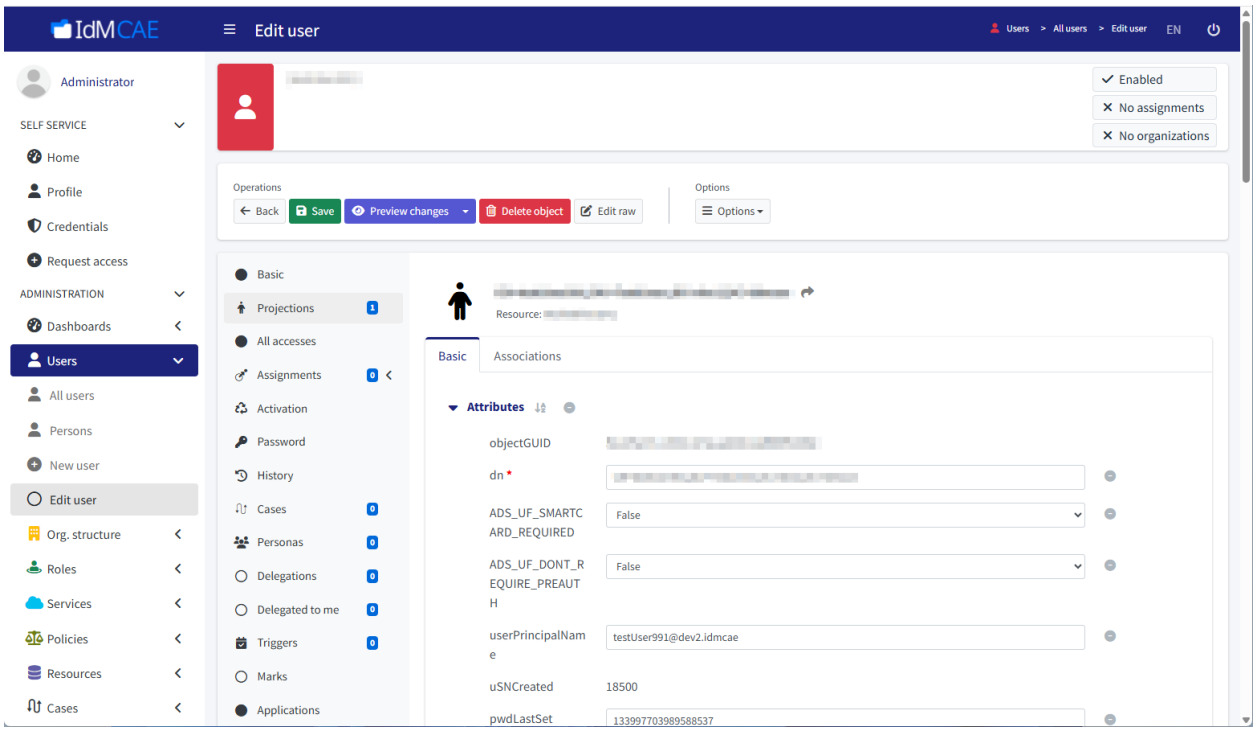


Рисунок 109 – Атрибуты УЗ

7.1.4.2. Ручное изменение УЗ пользователя

Для ручного изменения УЗ пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> All users** (1, рисунок 110). Выберите нужного пользователя (2, рисунок 110).

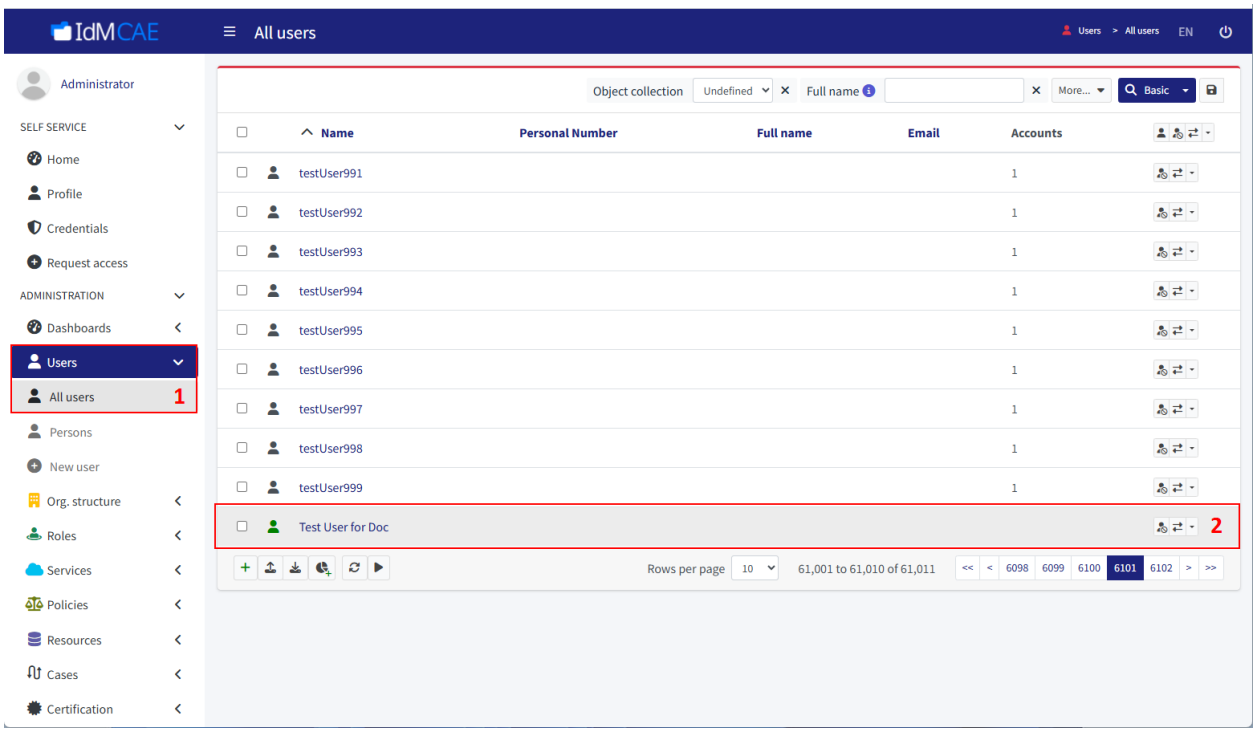


Рисунок 110 – Выбор пользователя

3. Перейдите на вкладку **Projections** (1, рисунок 111) и выберите нужную УЗ пользователя (2, рисунок 111).

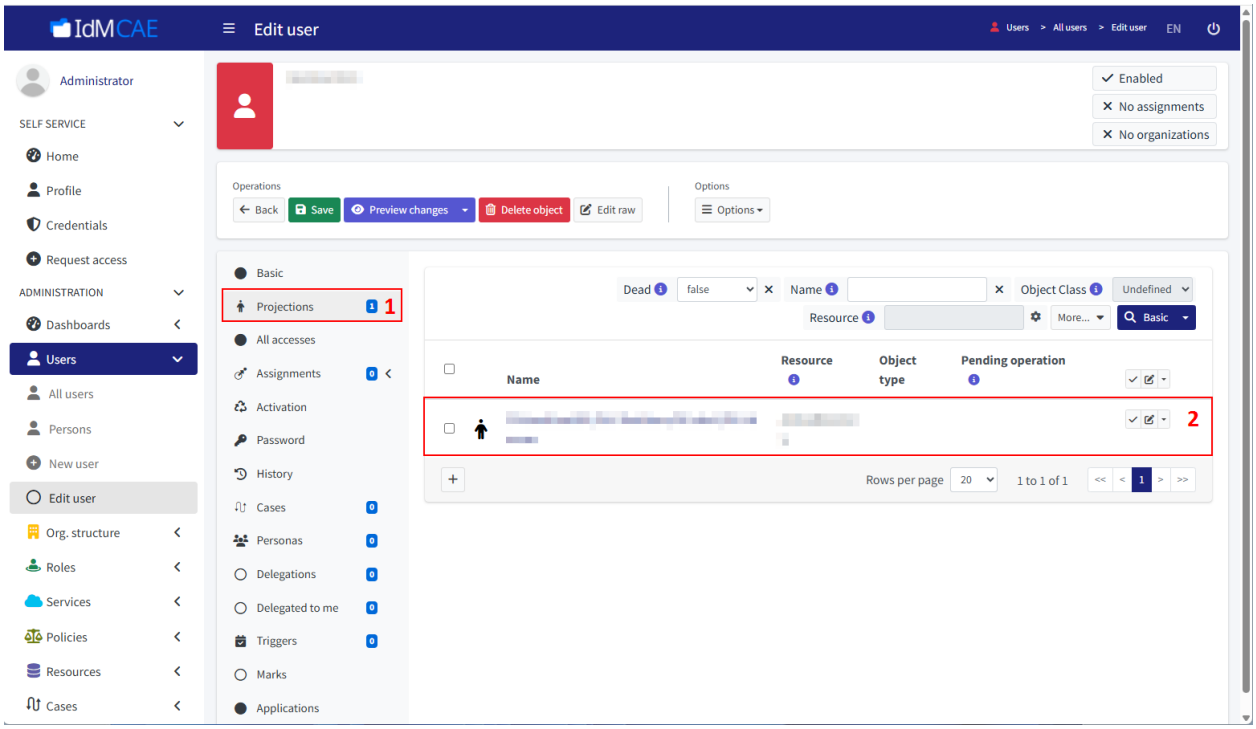


Рисунок 111 – Выбор УЗ пользователя

4. Введите новое значение атрибута (1, рисунок 112). Сохраните изменения, нажав на **Save** (2, рисунок 112).

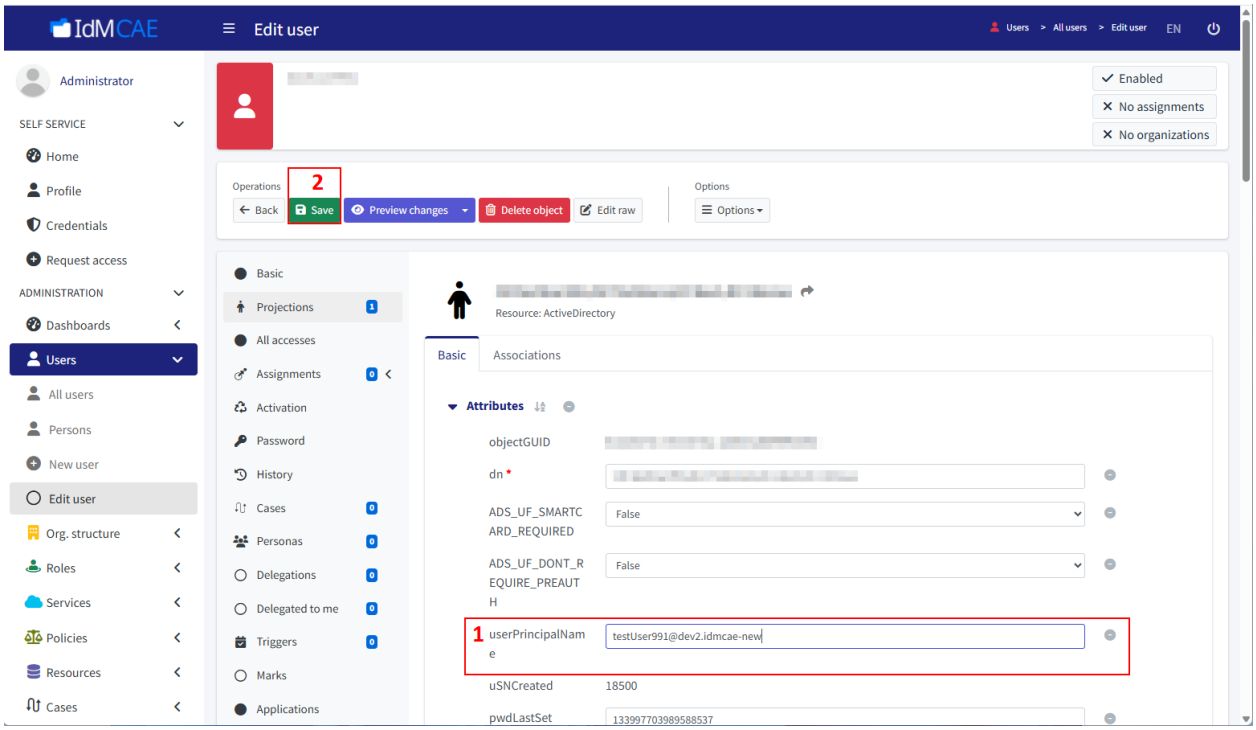


Рисунок 112 – Изменение УЗ пользователя

7.1.5. Управление ролями

7.1.5.1. Создание роли с архетипом Business role

Для создания роли с архетипом **Business role** выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Roles -> New role** (1, рисунок 113). В открывшемся окне будет предложено выбрать архетип роли. Нажмите на **Business Role** (2, рисунок 113).

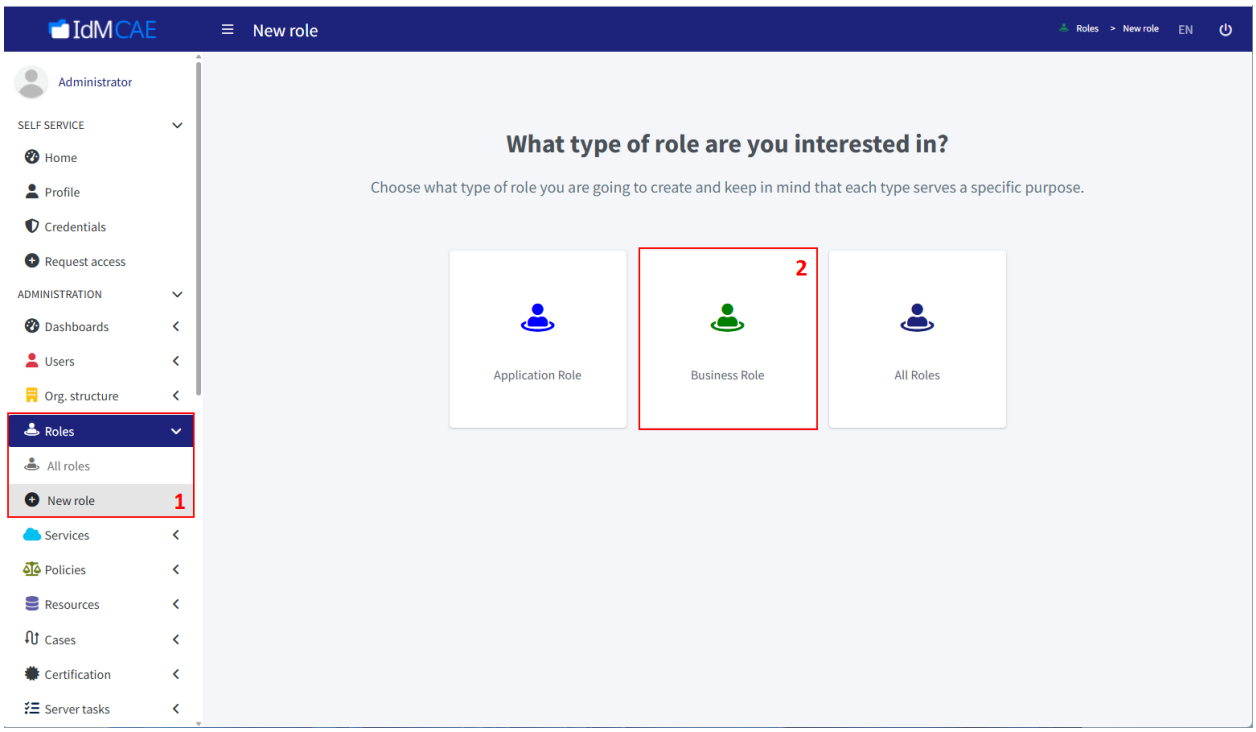


Рисунок 113 – Переход к созданию роли с архетипом Business role

3. Введите наименование роли в поле **Name** (1, рисунок 114). Нажмите на **Next: Access** (2, рисунок 114).

Подсказка: в случае использования модуля IG наименование роли должно соответствовать шаблону

`<название бизнес-роли как в файле РМ и МКР>_<название набора>_br_<название ресурса как на титульном листа файла РМ и МКР>`

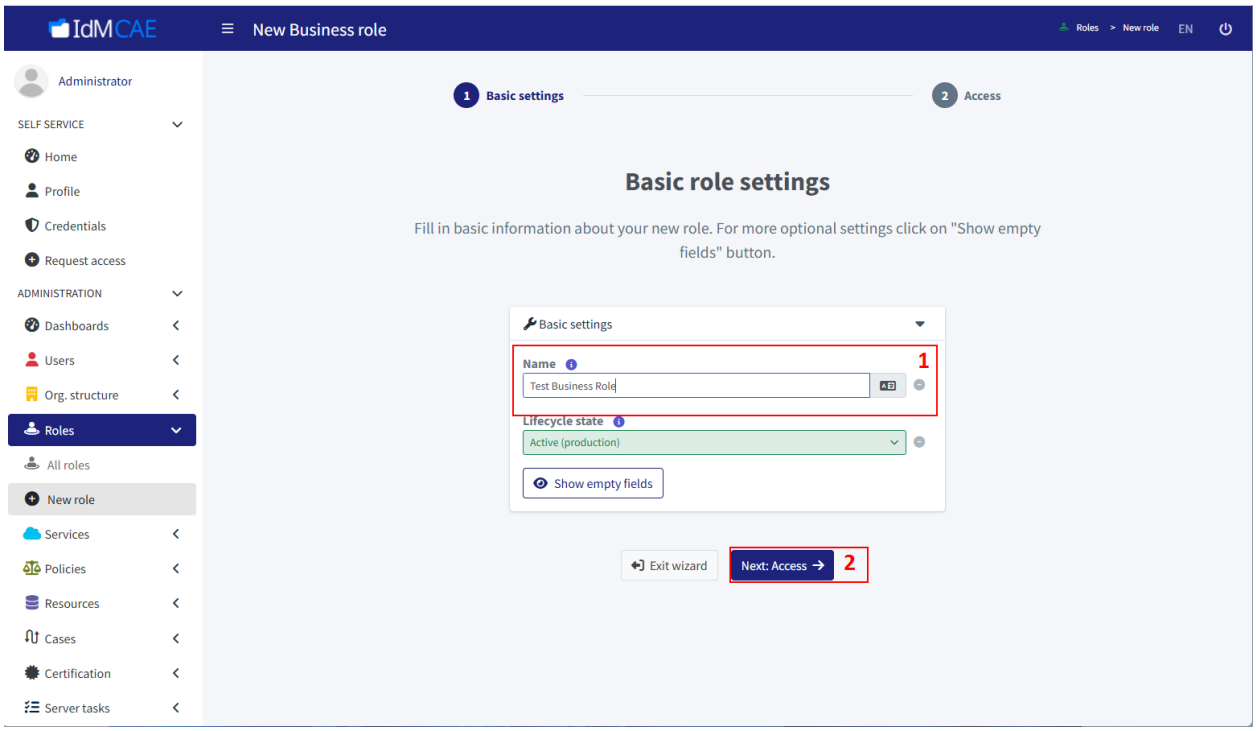


Рисунок 114 – Настройка роли

4. Выберите роли с архетипом **Application role**, которые требуется привязать к создаваемой роли (1, рисунок 115). Нажмите на **Save settings** (2, рисунок 115).

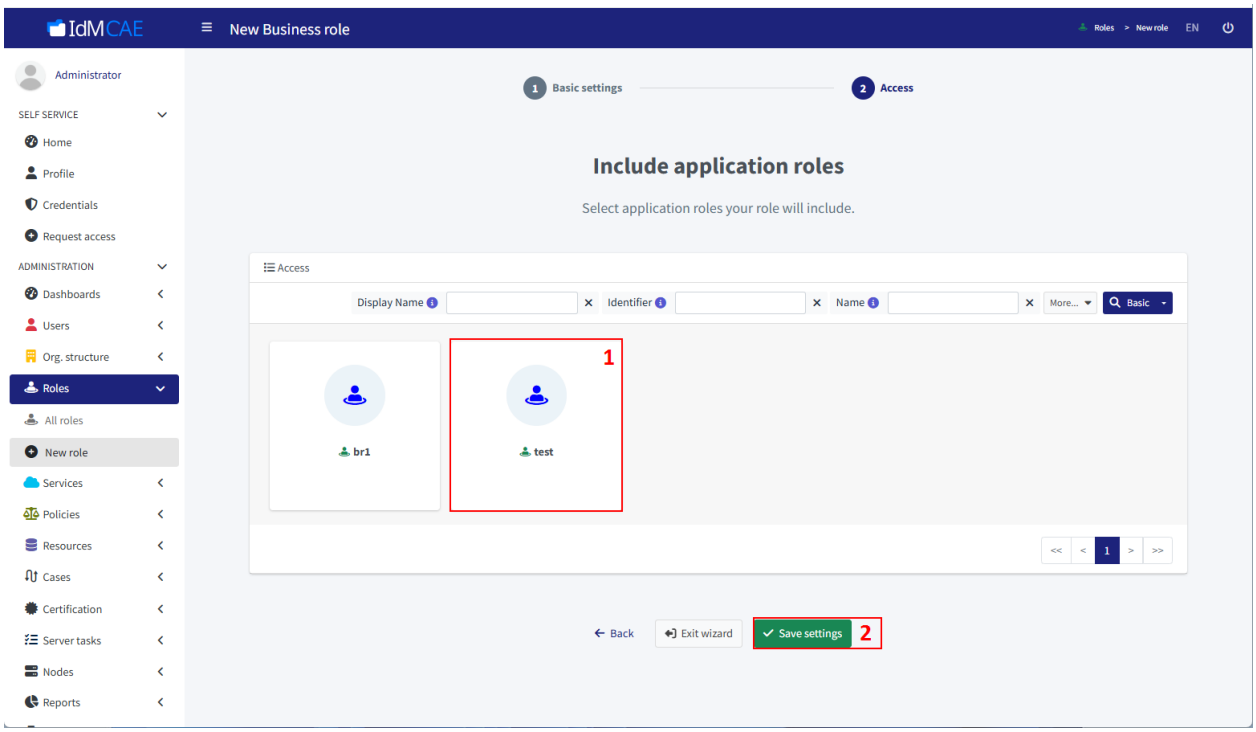


Рисунок 115 – Сохранение роли

7.1.5.2. Импорт ролей из ресурса

В разделе рассматривается пример импорта ролей из ресурса в IDM CAE в роли с архетипом Application role. Обратите внимание, что подобный импорт возможен только при условии поддержки коннектором объектов типа пользователь и группа, атрибуты которых связаны между собой (например, атрибут memberOf объекта типа пользователь связан с атрибутом members объекта типа группа)!

Для импорта ролей из ресурса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Resources -> All resources** (1, рисунок 116) в разделе **ADMINISTRATION**. Выберите нужный ресурс (2, ресурс 116).

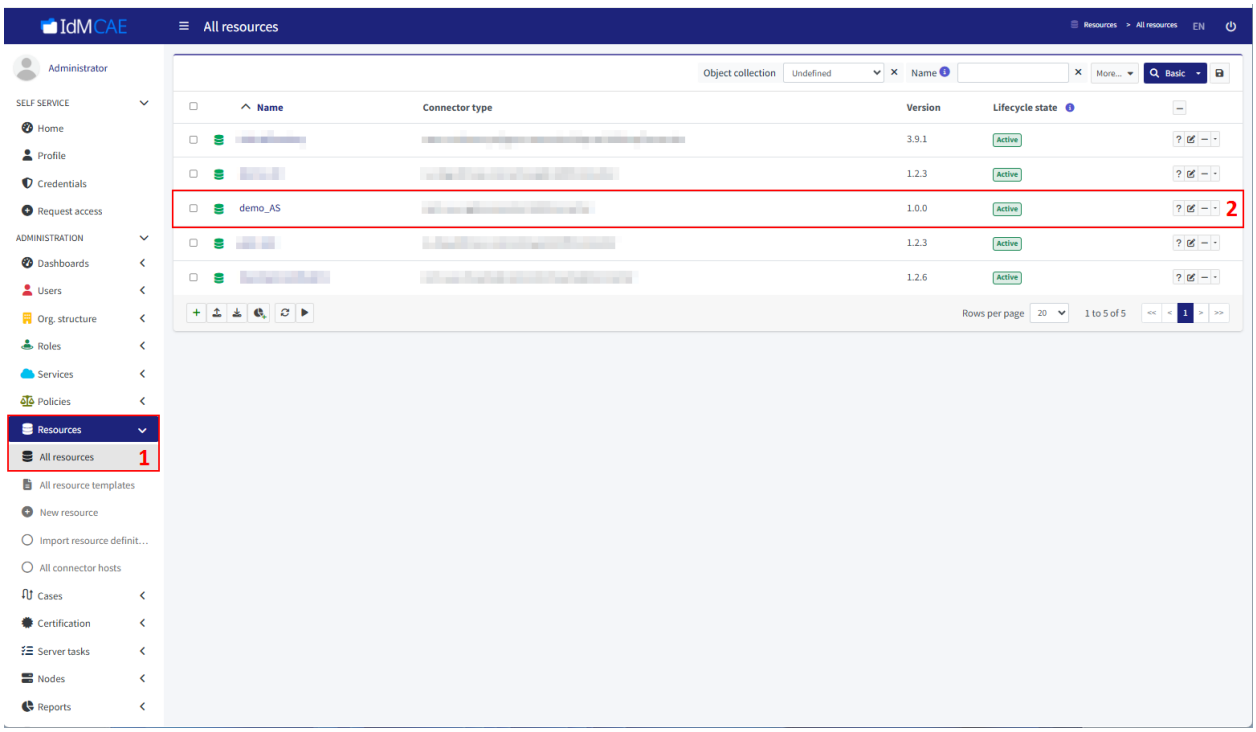


Рисунок 116 – Выбор ресурса

3. Перейдите на вкладку **Entitlements** (1, рисунок 117). Нажмите на **Configure** (2, рисунок 117) и в выпадающем выберите **Basic attributes** (3, рисунок 117).

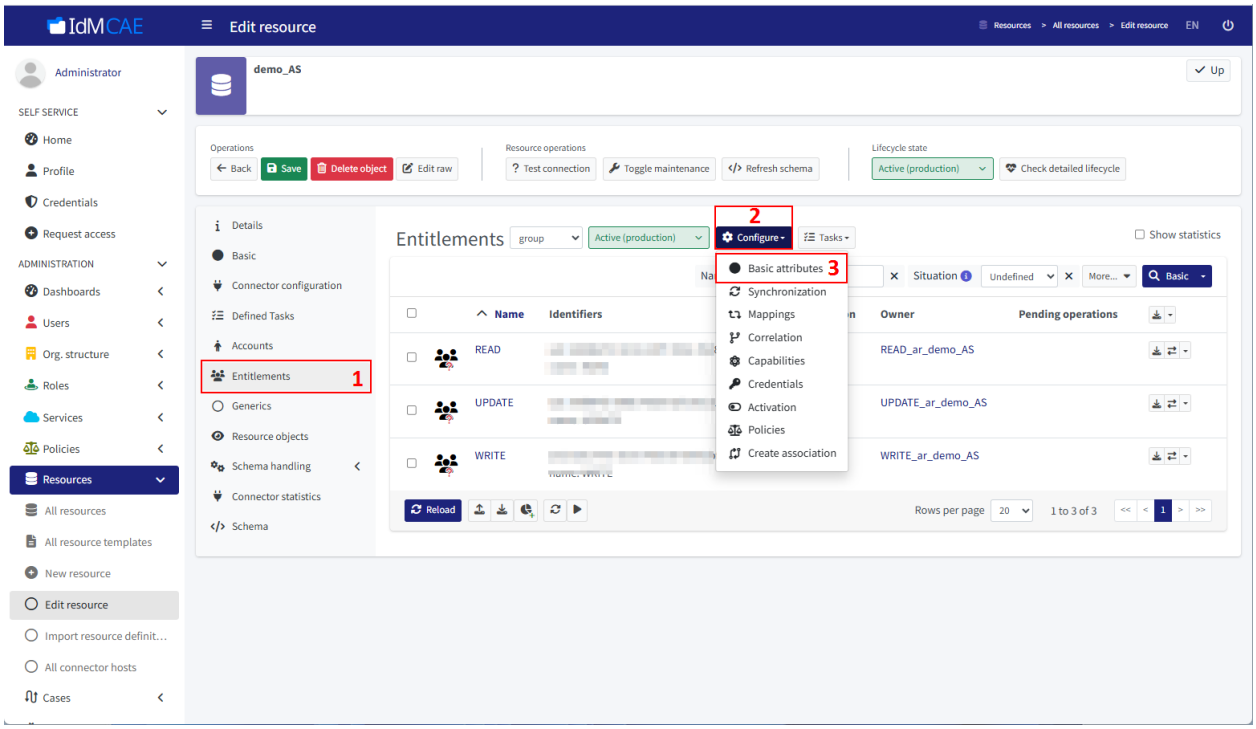


Рисунок 117 – Переход к базовым атрибутам

4. В окне **Basic information** в поле **Kind** выберите **Entitlements** (1, рисунок 118), в поле **Intent** введите любой набор символов (2, рисунок 118), введённое значение понадобится позже. В окне **Resource data** в поле **Object class** выберите нужный класс объекта (рисунок 119), в окне **MidPoint** data в поле **Type** – **Role** (1, рисунок 120). Поле **Archetype** (2, рисунок 120) оставьте пустым. Остальные поля заполните при необходимости. Сохраните настройки, нажав на **Save settings** (3, рисунок 120).

   В результате произойдёт переход в окно с общим списком ролей (пока пустым). Для того чтобы настройки были применены и IDM CAE смог загрузить роли из ресурса, нажмите на **Reload** (рисунок 121).

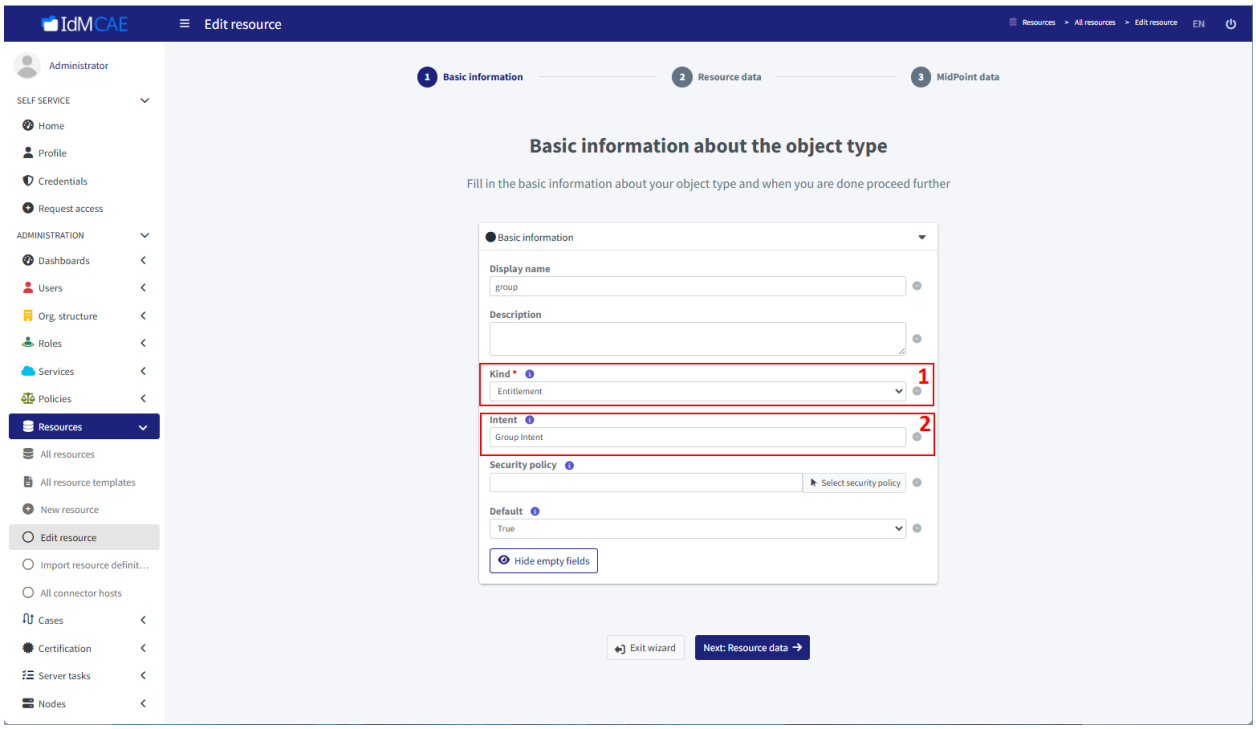


Рисунок 118 – Окно Basic information

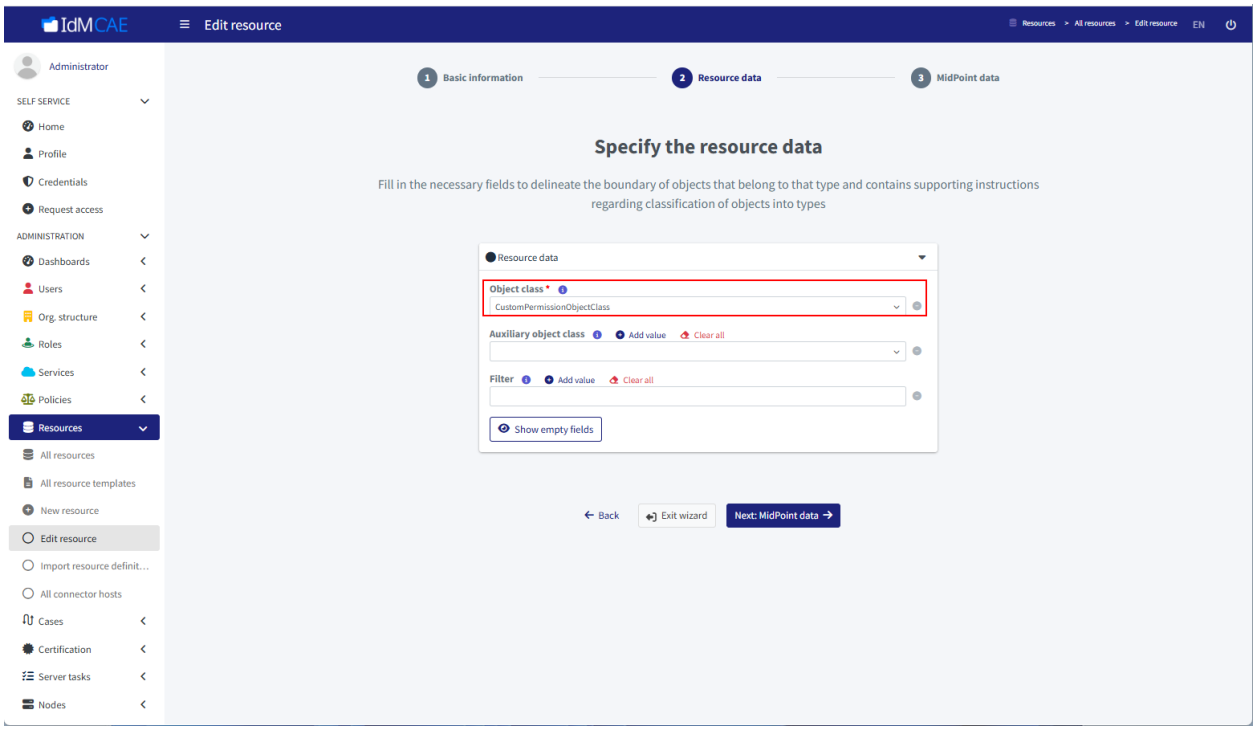


Рисунок 119 – Окно Resource data

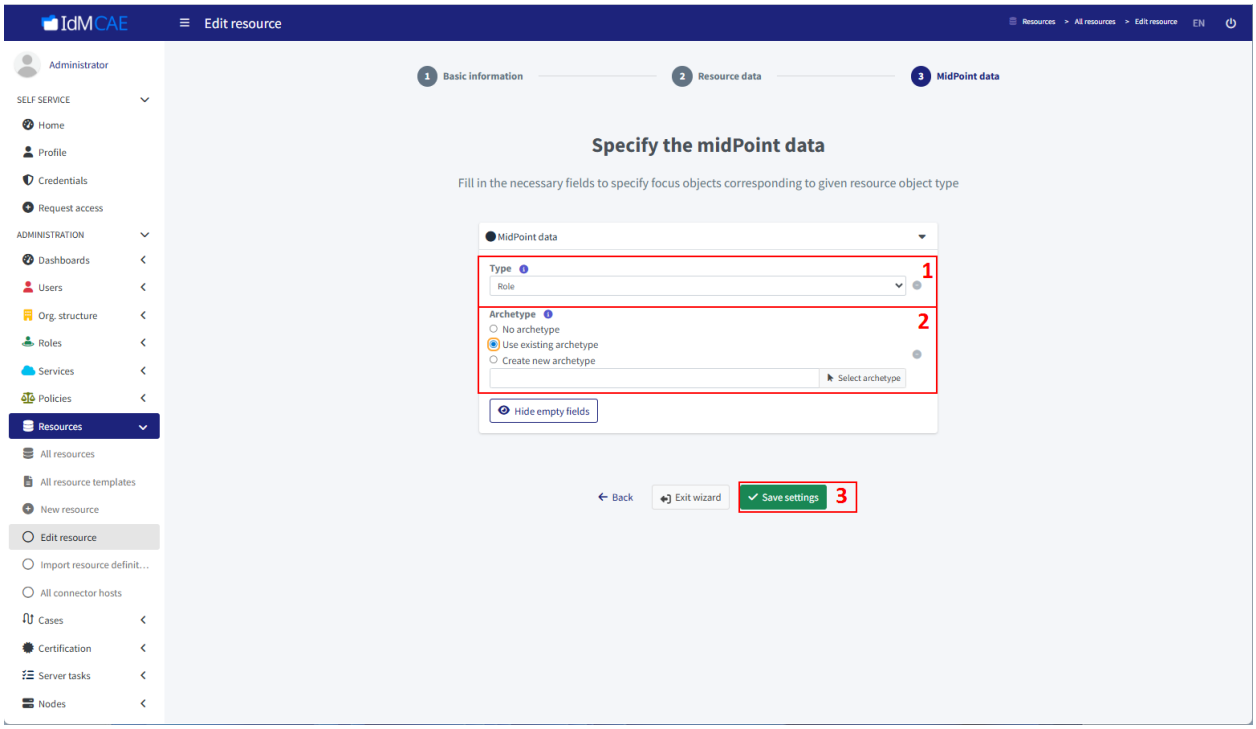


Рисунок 120 – Окно MidPoint data

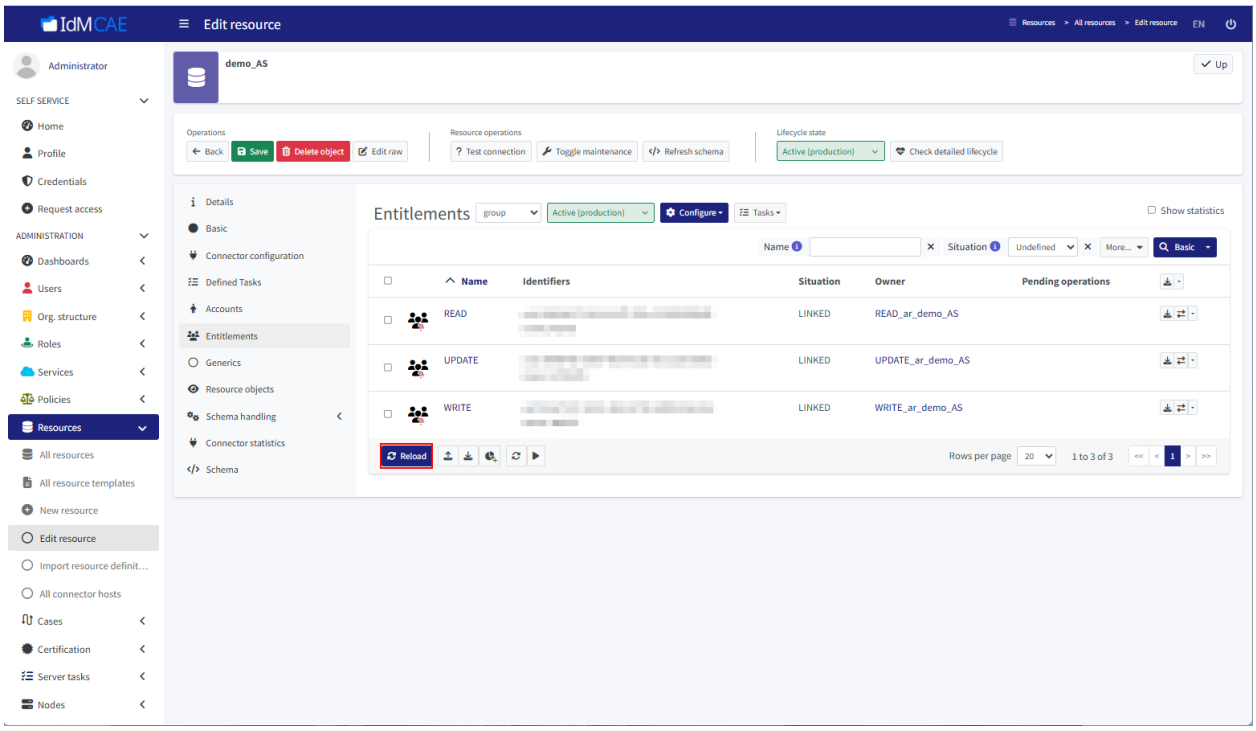


Рисунок 121 – Загрузка ролей

5. Перейдите к настройкам параметров синхронизации через **Configure -> Synchronization** (рисунок 122).

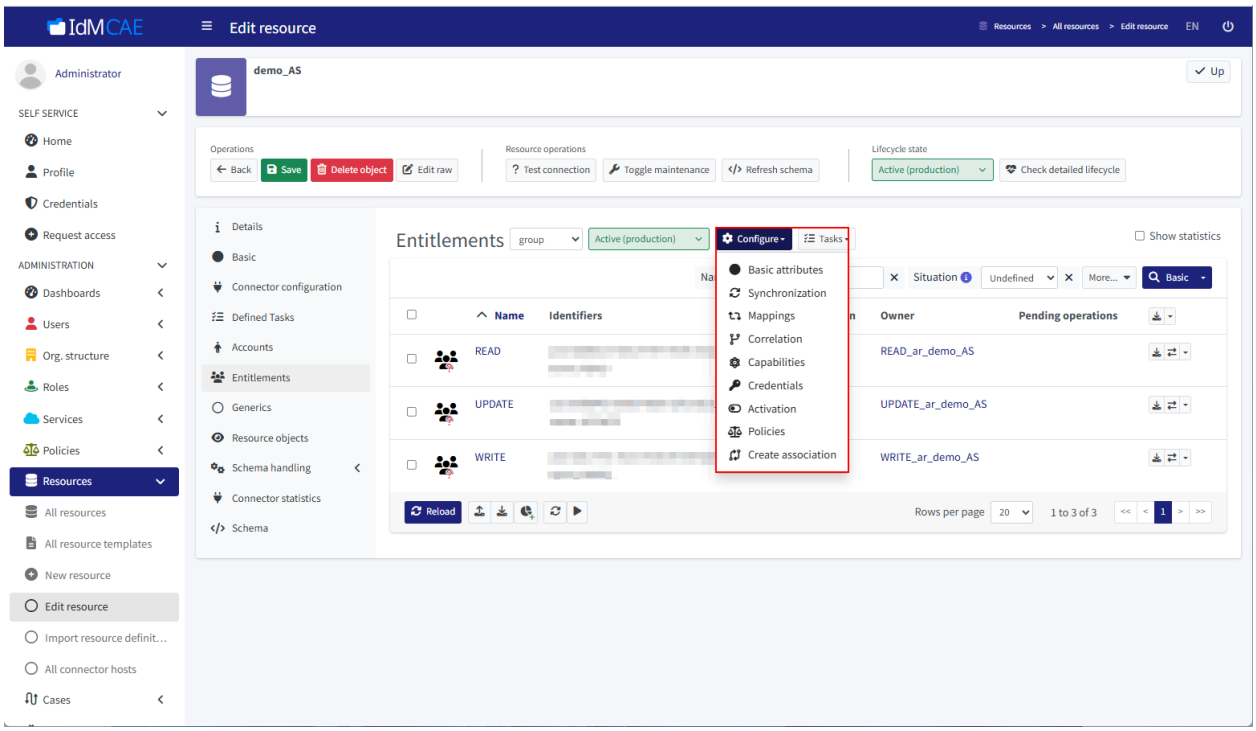


Рисунок 122 – Переход к параметрам синхронизации / маппинга / корреляции

6. Выполните настройку параметров синхронизации в соответствии с разделом 7.1.9.
7. Перейдите к настройкам параметров маппинга через **Configure -> Mappings** и корреляции через **Configure -> Correlation** (рисунок 122) и выполните их настройку. Обратите внимание, что важно настроить входящие маппинги (inbound) по аналогии с HR-ресурсом! Также настройте один из атрибутов во входящем маппинге в качестве уникального идентификатора (1, рисунок 123) и для названия роли (2, рисунок 123) используйте скрипт (рисунок 124) для корректной отработки модуля IG (в случае его использования). Имя роли должно соответствовать шаблону

<Название прикладной роли>_ar_<Название ресурса как в компоненте Provisioning Management>

Пример настройки корреляции представлен на рисунке 125, 126.

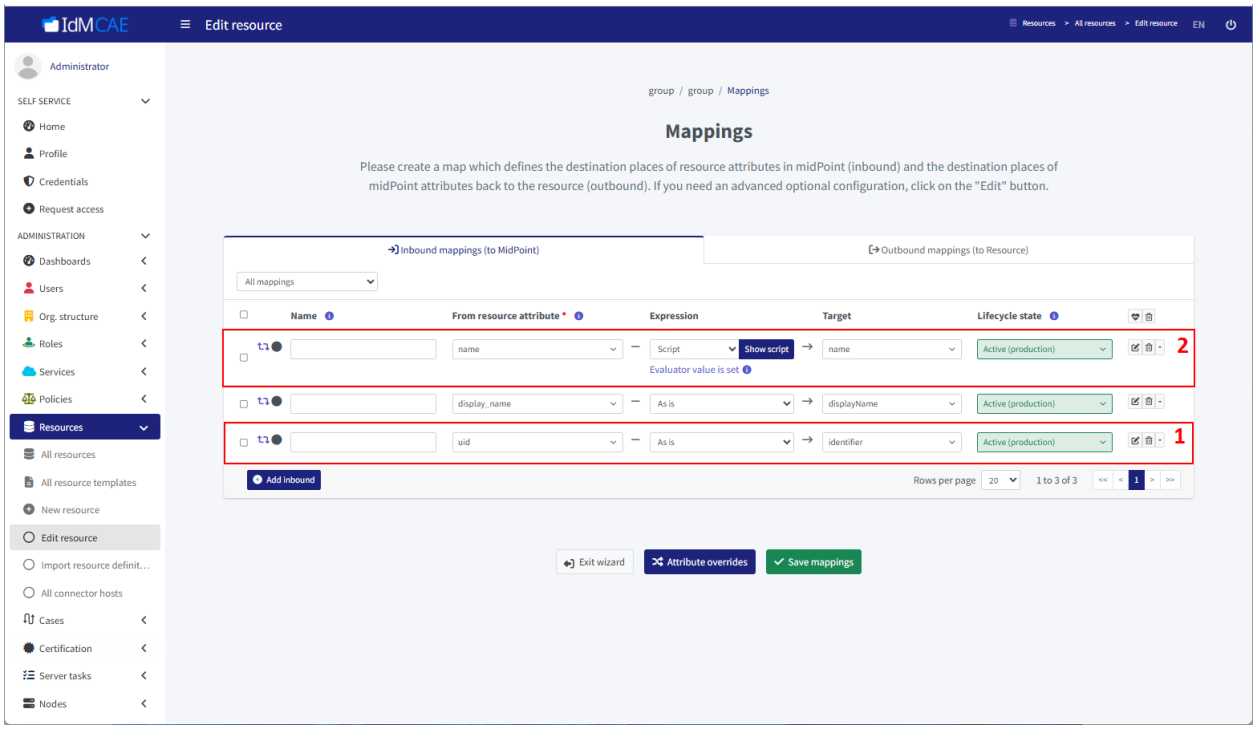


Рисунок 123 – Особенности настройки входящих маппингов

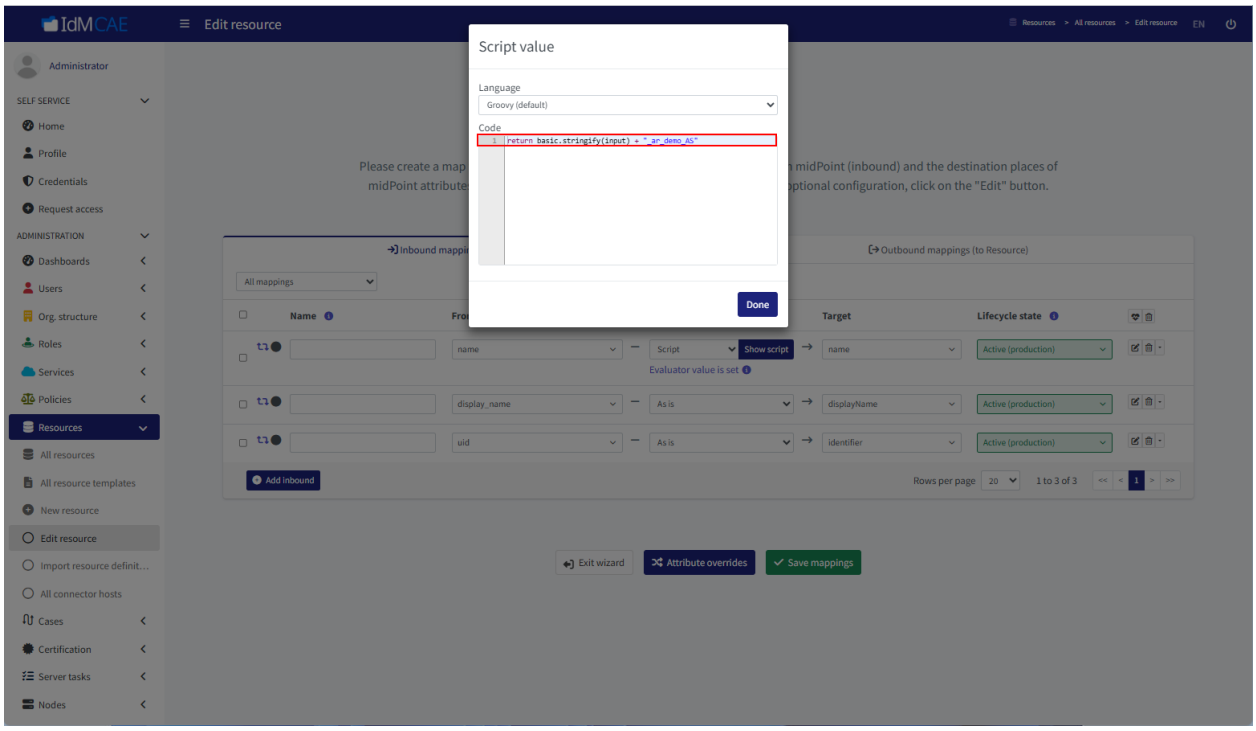


Рисунок 124 – Скрипт для формирования названия роли

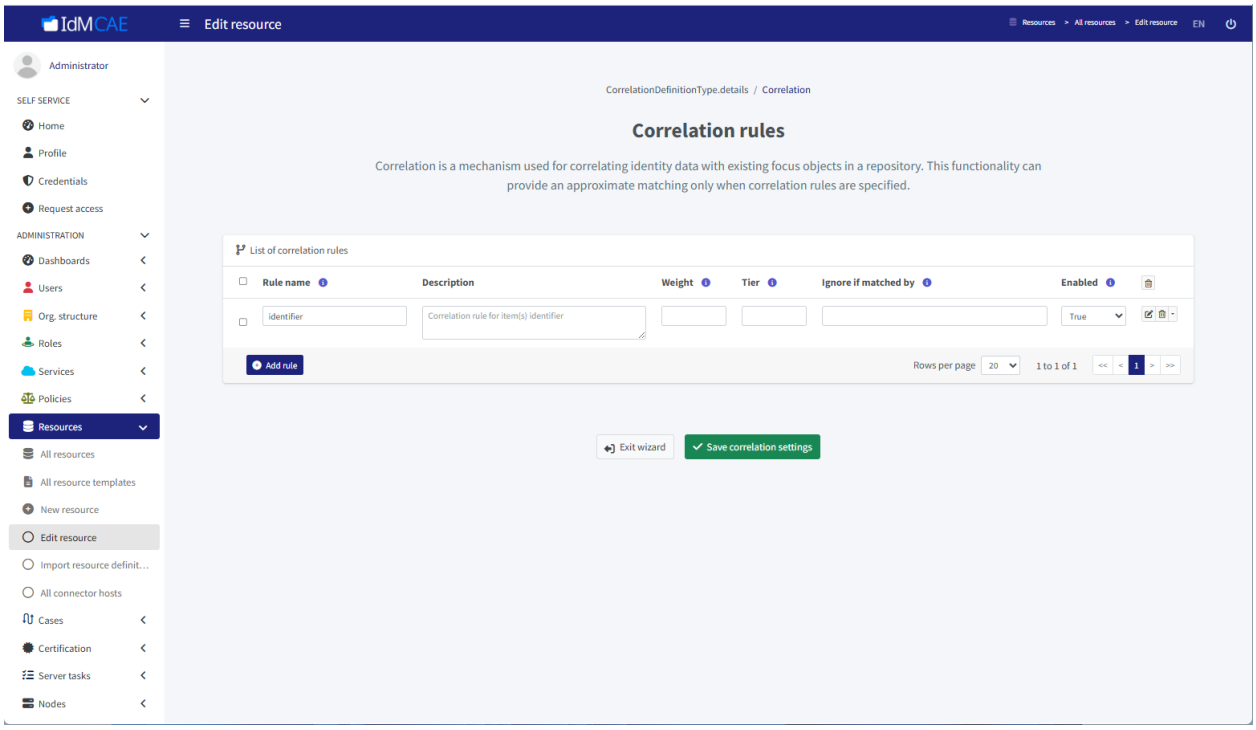


Рисунок 125 – Пример настройки корреляции (1)

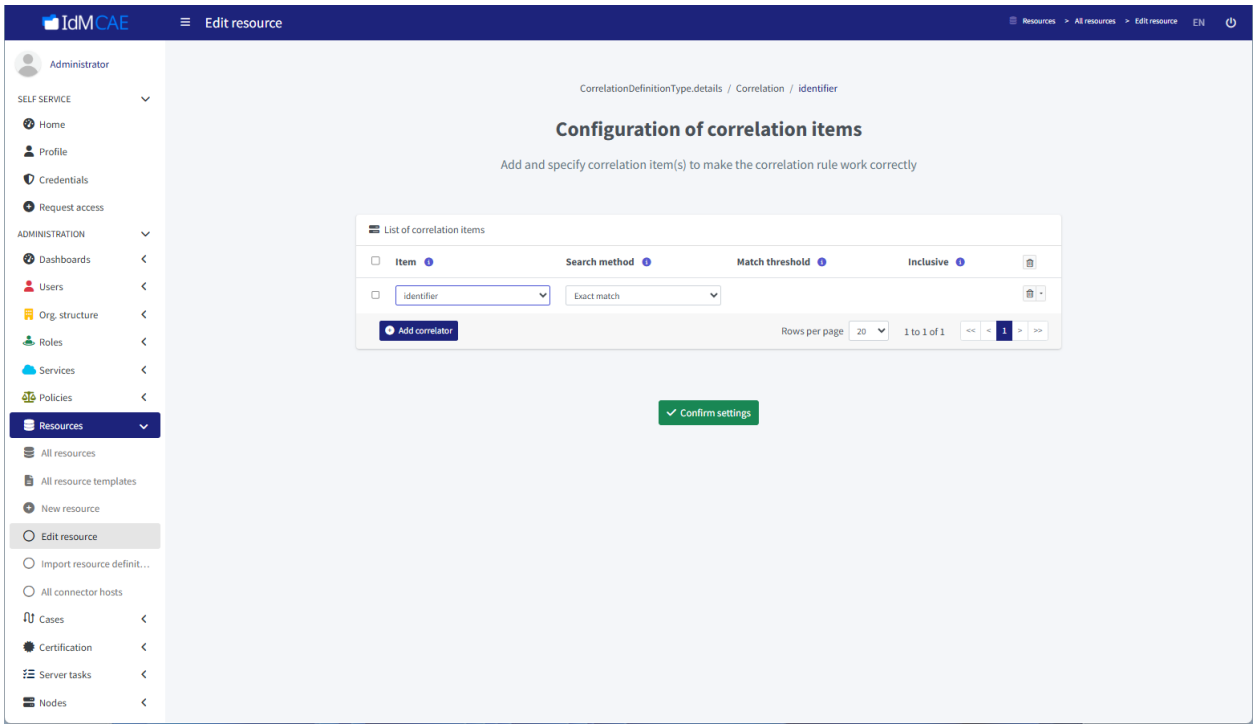


Рисунок 126 – Пример настройки корреляции (2)

8. Нажмите на **Edit raw** (рисунок 127).

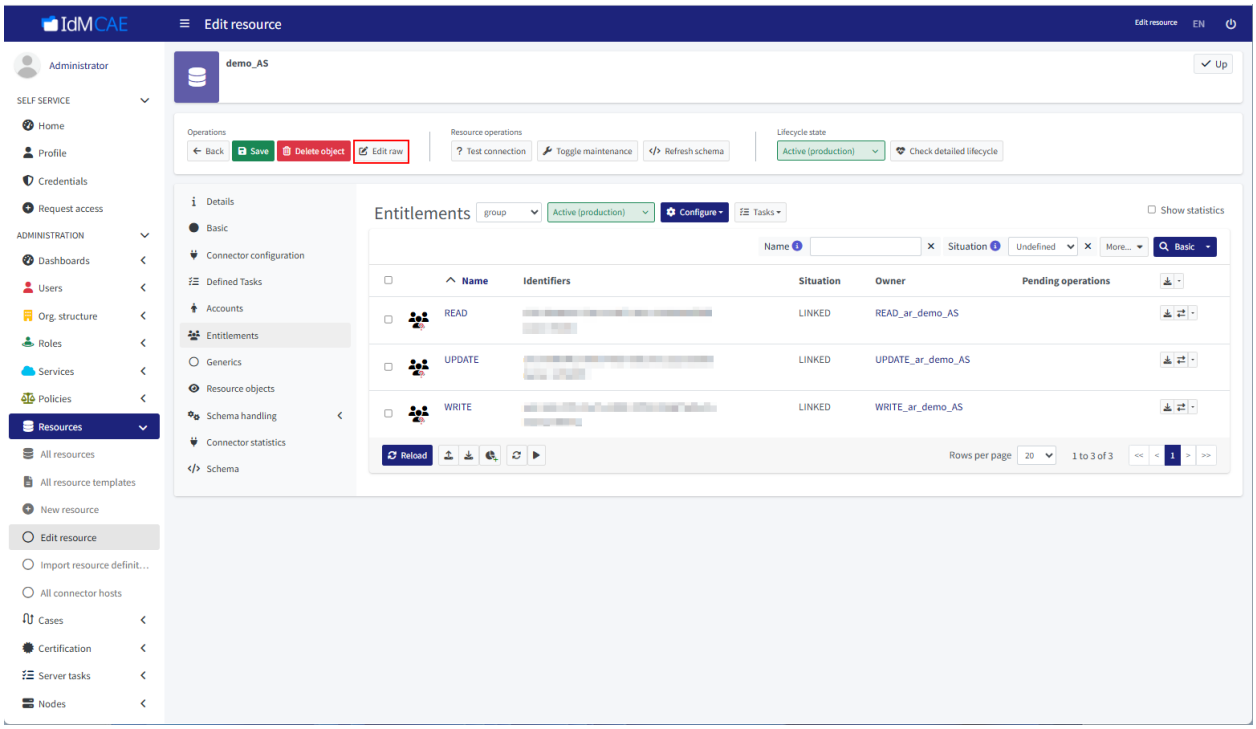


Рисунок 127 – Переход к изменению объекта ресурса

9. Вставьте между секциями attribute и correlation объекта Account код, представленный в Приложении 3, отвечающую за настройку ассоциаций для связи пользователя с ролью (1, рисунок 128):

- в тэге `<ref>` можете любое уникальное слово / сочетание слов;
- в тэге `<intent>` укажите значение поля Intent, указанное при настройке ресурса (2, рисунок 118);
- в тэгах `<associationAttribute>`, `<valueAttribute>`, `<shortcutAssociationAttribute>`, `<shortcutValueAttribute>` укажите наименования атрибутов связи пользователя и группы коннектора, при этом:
    - `ri` пространство дополнительных атрибутов, добавленных при разработке коннектора;
    - `icfs` пространство встроенных атрибутов коннектора (uid, name).

Сохраните изменения, нажав на **Save** (2, рисунок 128).

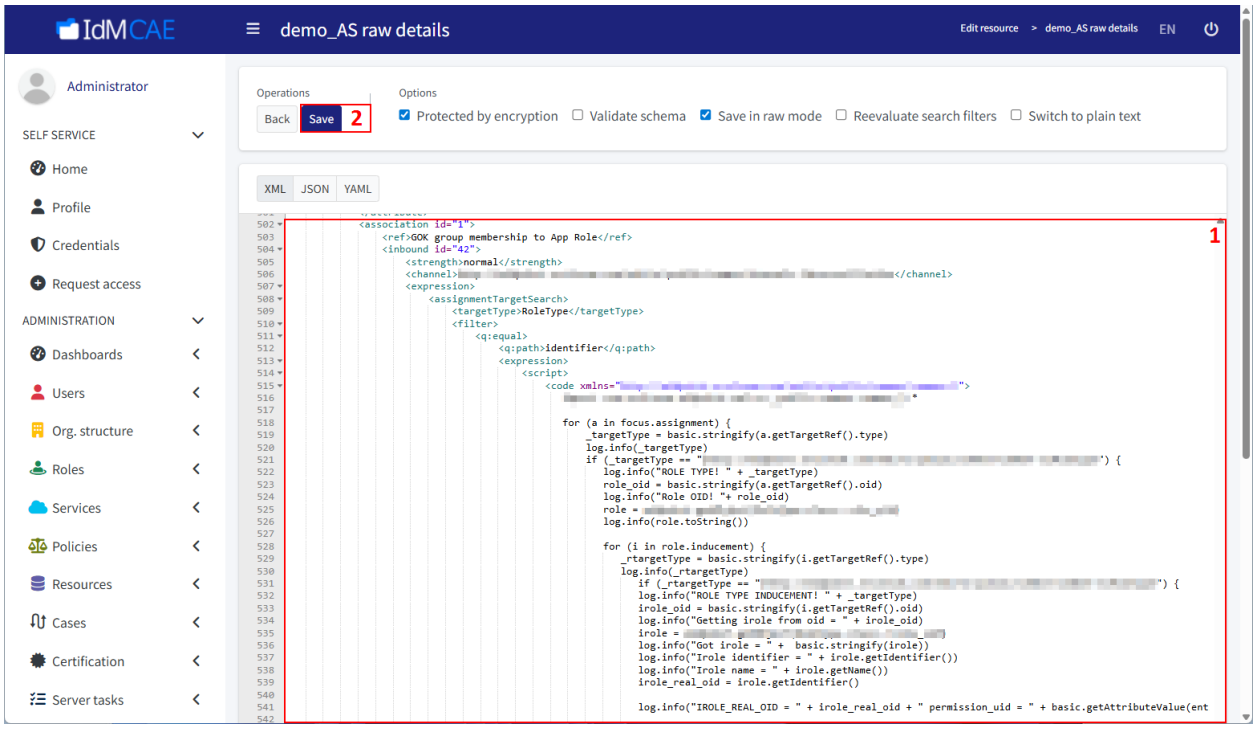


Рисунок 128 – Настройка ассоциаций

10. Создайте архетип для ресурса (подробнее см. в разделе 7.1.8.1). Обратите внимание, что для каждого ресурса требуется создавать свой архетип!

11. Выберите созданный архетип и нажмите на **Edit raw** (рисунок 129).

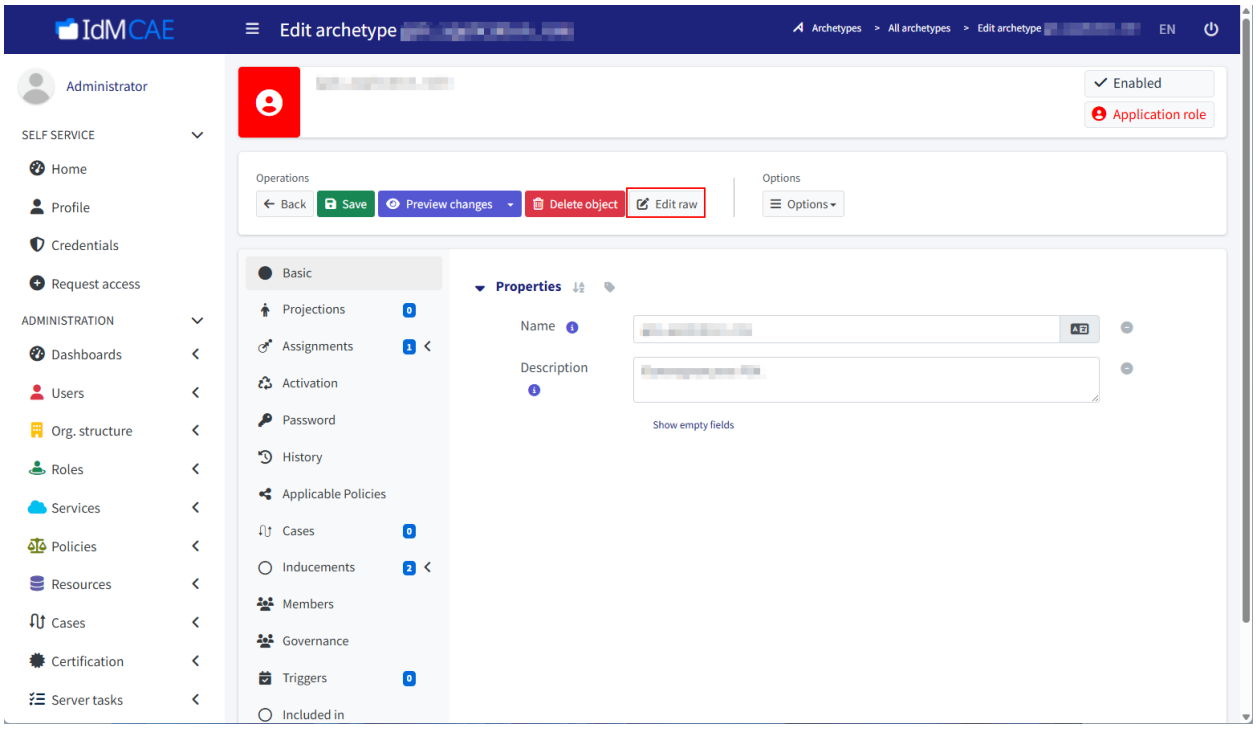


Рисунок 129 – Переход к настройке архетипа

12. Перед `</archetype>` вставьте код (1, рисунок 130)

```
    <inducement>
        <construction>
            <resourceRef oid="c34bb28c-b173-4502-b46c-a9b2c63ab751" relation="org:default" type="c:Resource-Type">
                <!-- GOK_AS -->
            </resourceRef>
            <kind>account</kind>
            <intent>Account Intent</intent>
            <association id="28">
                <ref>GOK group membership to App Role</ref>
                <outbound>
                    <expression>
                        <associationFromLink>
```

```
                                <projectionDiscriminator
xsi:type="c:ShadowDiscriminatorType">
                                    <kind>entitle-
ment</kind>
                                    <intent>Group        In-
tent</intent>
                                </projectionDiscriminator>
                            </associationFromLink>
                        </expression>
                    </outbound>
                </association>
            </construction>
            <order>2</order>
            <focusType>UserType</focusType>
        </inducement>
        <archetypePolicy>
            <display>
                <label>GOK Group Archetype</label>
                <pluralLabel>GOK Group Archetype</pluralLa-
bel>
                <icon>
                    <cssClass>fa fa-people-group</cssClass>
                    <color>#6b0f89</color>
                </icon>
            </display>
        </archetypePolicy>
```

В коде произведите следующие изменения:

- в тэге `<resourceRef>` укажите идентификатор ресурса (подробнее см. в разделе 7.1.7.2);

- в тэге `<intent>Account Intent</intent>` укажите значение из одноимённого поля (рисунок 64);
- в тэге `<intent>Group Intent</intent>` укажите значение из одноимённого поля (2, рисунок 118);
- в тэге `<ref>` укажите значение из одноимённое тэга из п. 9.

  Сохраните изменения, нажав на **Save** (2, рисунок 130).

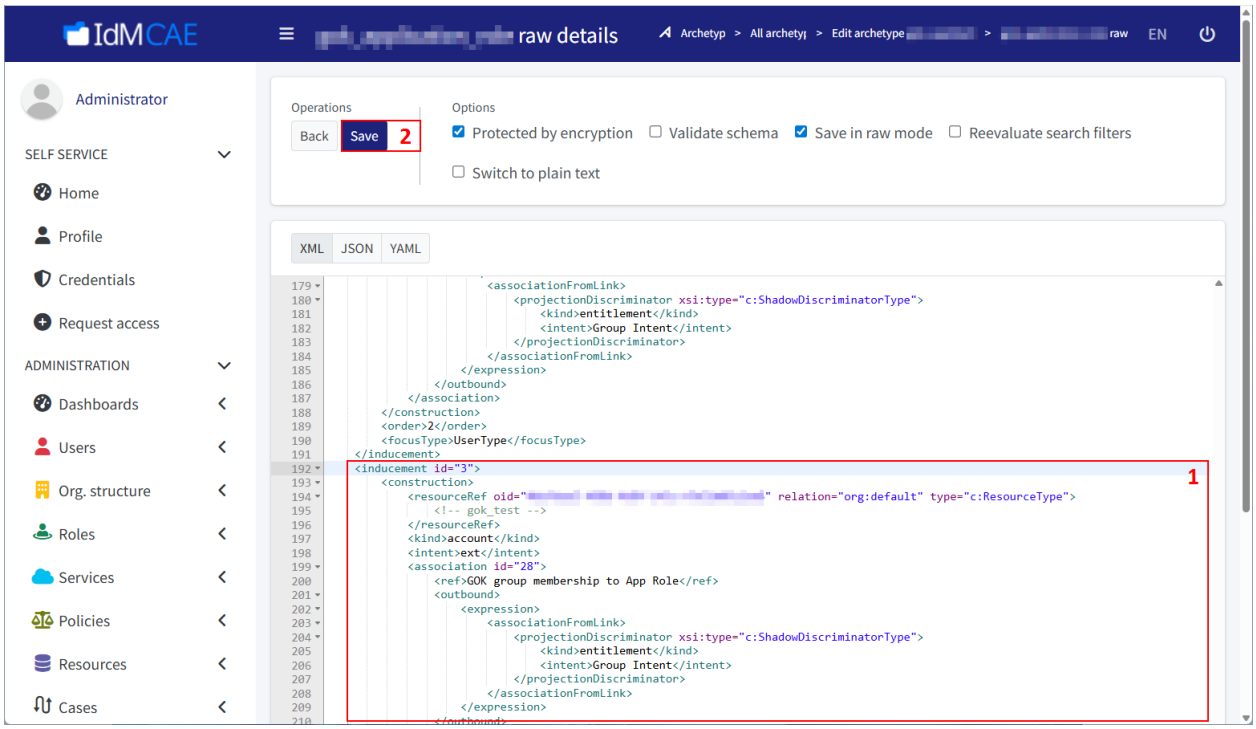


Рисунок 130 – Изменение объекта архетипа

13. Вернитесь к настройке ресурса и нажмите на **Edit raw**. Найдите секцию, относящуюся к Entitlements и вставьте следующий код (1, рисунок 131), изменив значение `archetypeRef oid` на идентификатор созданного архетипа (подробнее см. в разделе 7.1.7.2)

```
<archetypeRef oid="00000000-0000-0000-0000-000000000328" relation="org:default" type="c:ArcheTypeType">
<!-- Application role -->
</archetypeRef>
```

Сохраните изменения, нажав на **Save** (2, рисунок 131).

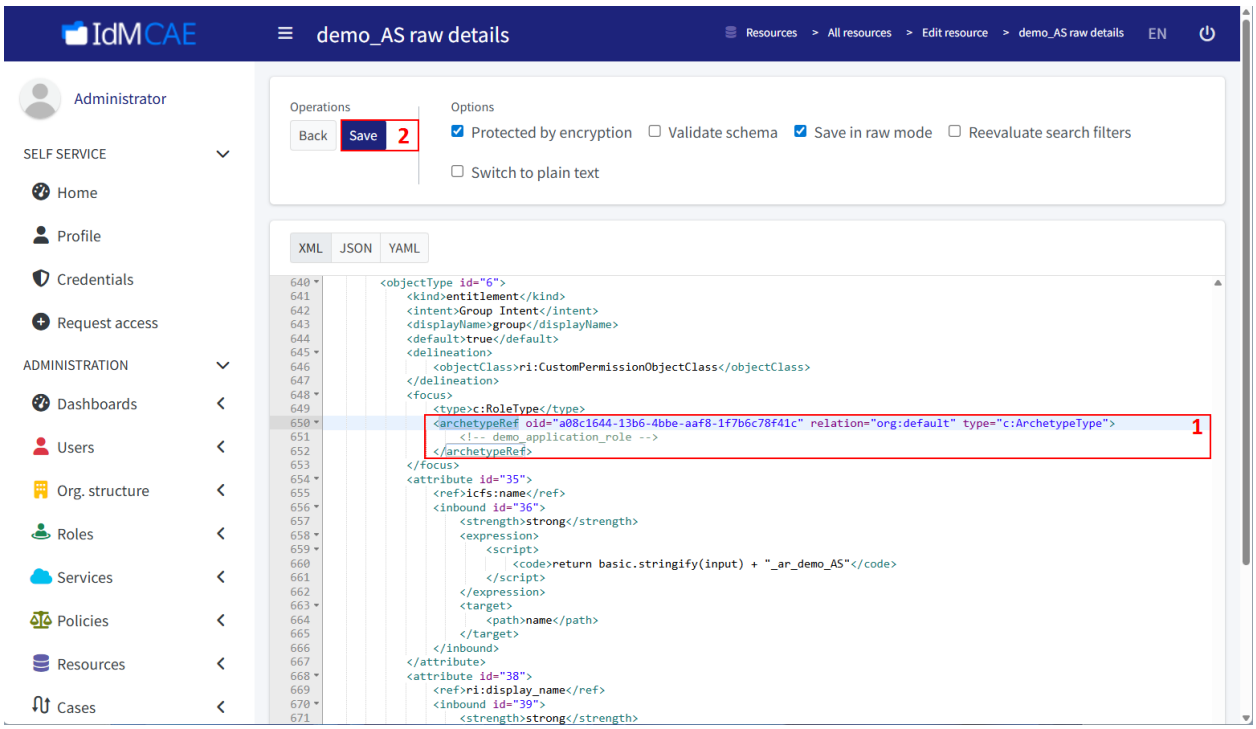


Рисунок 131 – Изменение объекта ресурса

14. Создайте задание для ресурса (подробнее см. в разделе 7.1.2.9). Запустите созданную задачу.

15. На вкладке **Defined Tasks** (1, рисунок 132) нажмите на  (2, рисунок 132). И настройте задачу реконсиляции (рисунок 133) сначала для **Entitlement**, потом для **Account**.

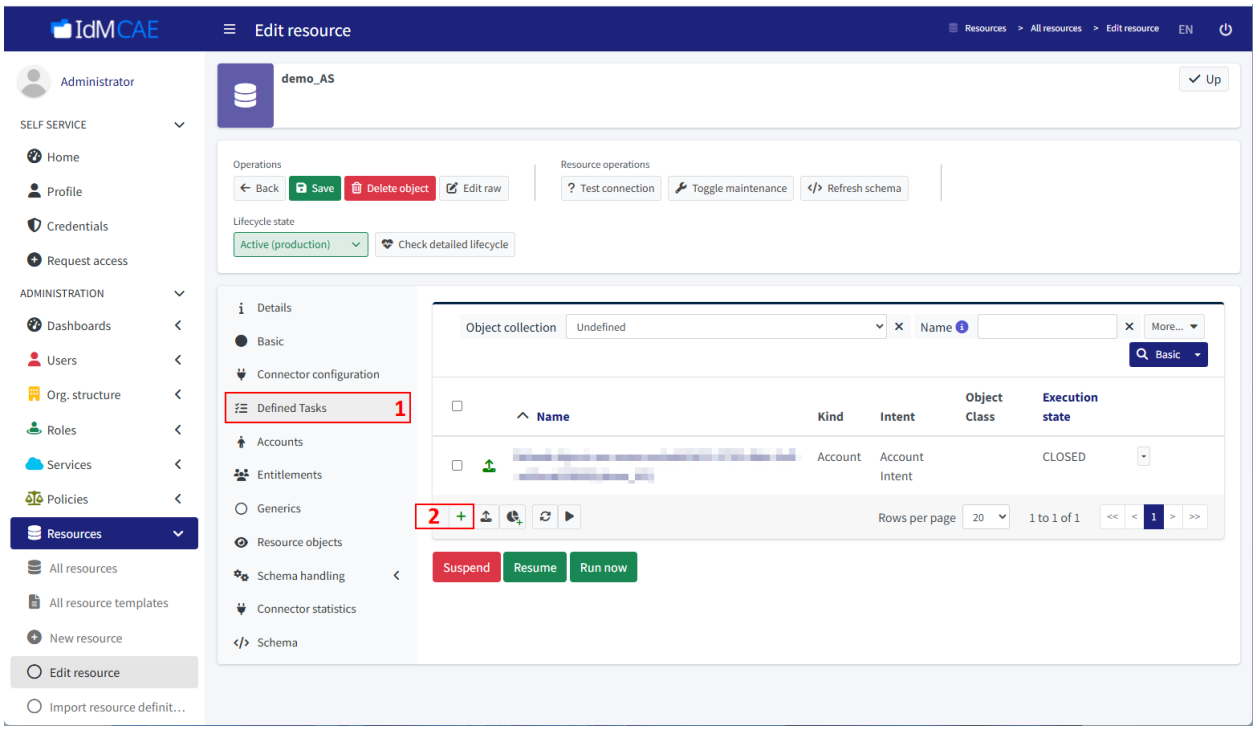


Рисунок 132 – Переход к созданию задачи

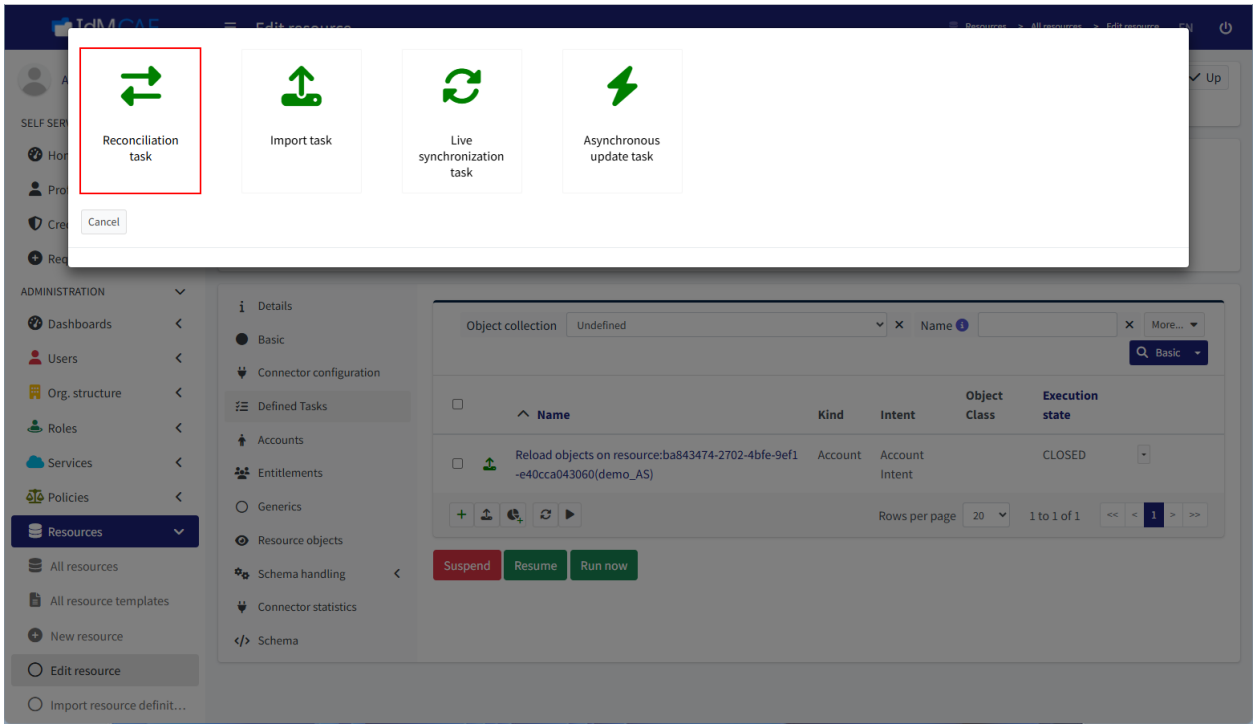


Рисунок 133 – Выбор типа задачи

7.1.5.3. Изменение роли

Для изменения роли выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Roles -> All roles** (1, рисунок 134). Выберите нужную роль (2, рисунок 134).

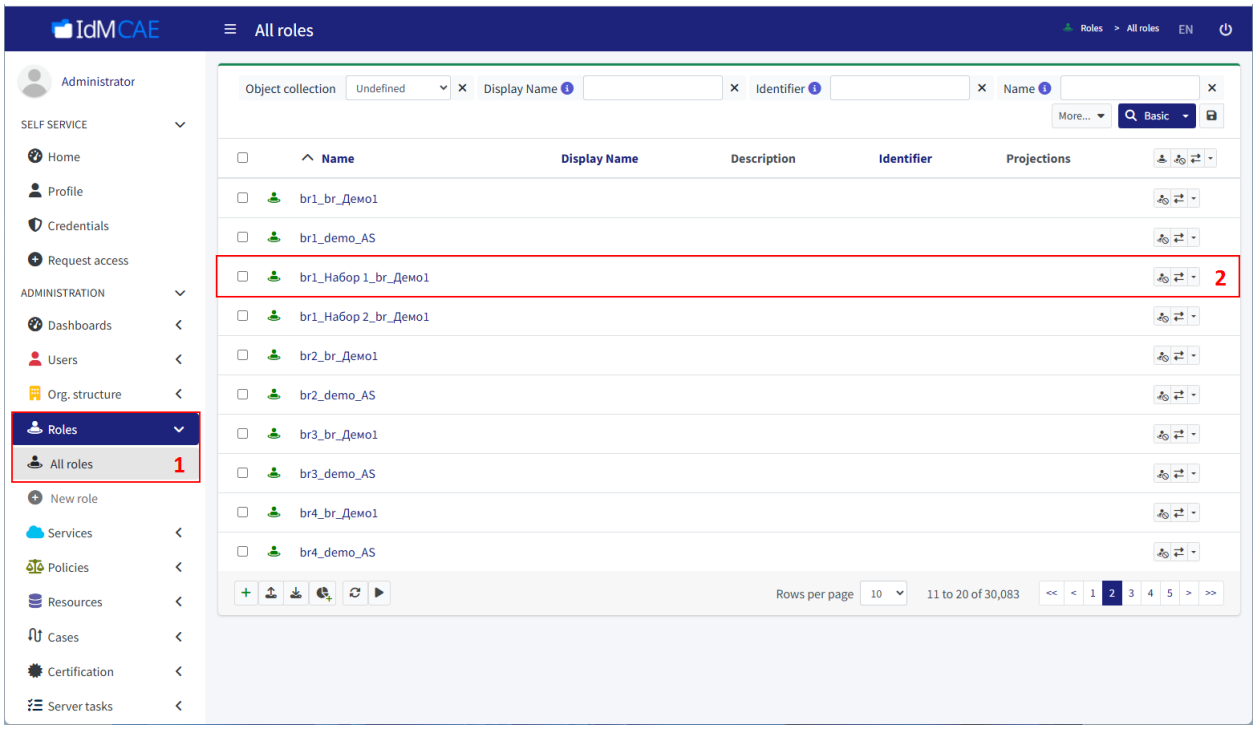


Рисунок 134 – Выбор роли

3. Отредактируйте роль, изменив параметры на нужной вкладке (1, рисунок 135) или непосредственно в объекте роли, нажав на **Edit raw** (2, рисунок 135). Сохраните изменения, нажав на **Save** (3, рисунок 135).

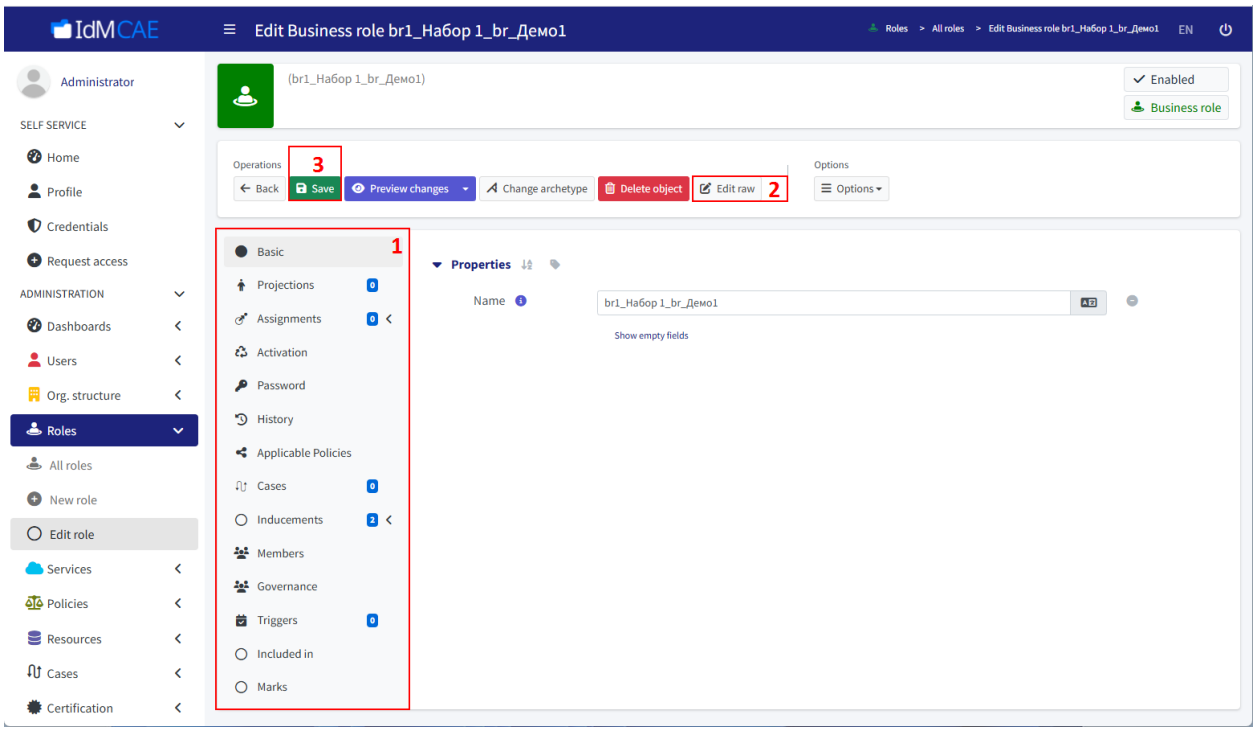


Рисунок 135 – Изменение роли

7.1.5.4. Ручное назначение роли пользователю

Для ручного назначения роли пользователю выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Users -> All users** (1, рисунок 136). В открывшемся окне **All users** выберите нужного пользователя (2, рисунок 136).

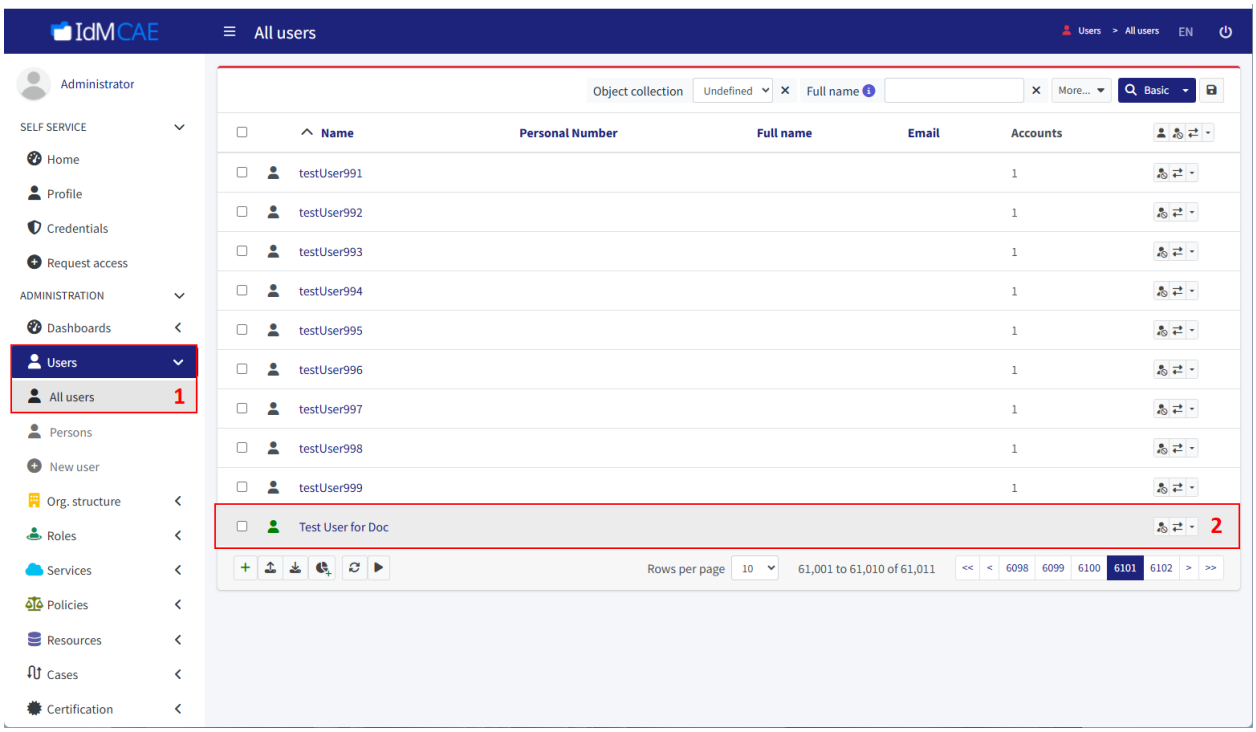


Рисунок 136 – Переход к пользователю

3. Перейдите на вкладку **Assignments -> Roles** (1, рисунок 137). Нажмите на  для добавления роли (2, рисунок 137).

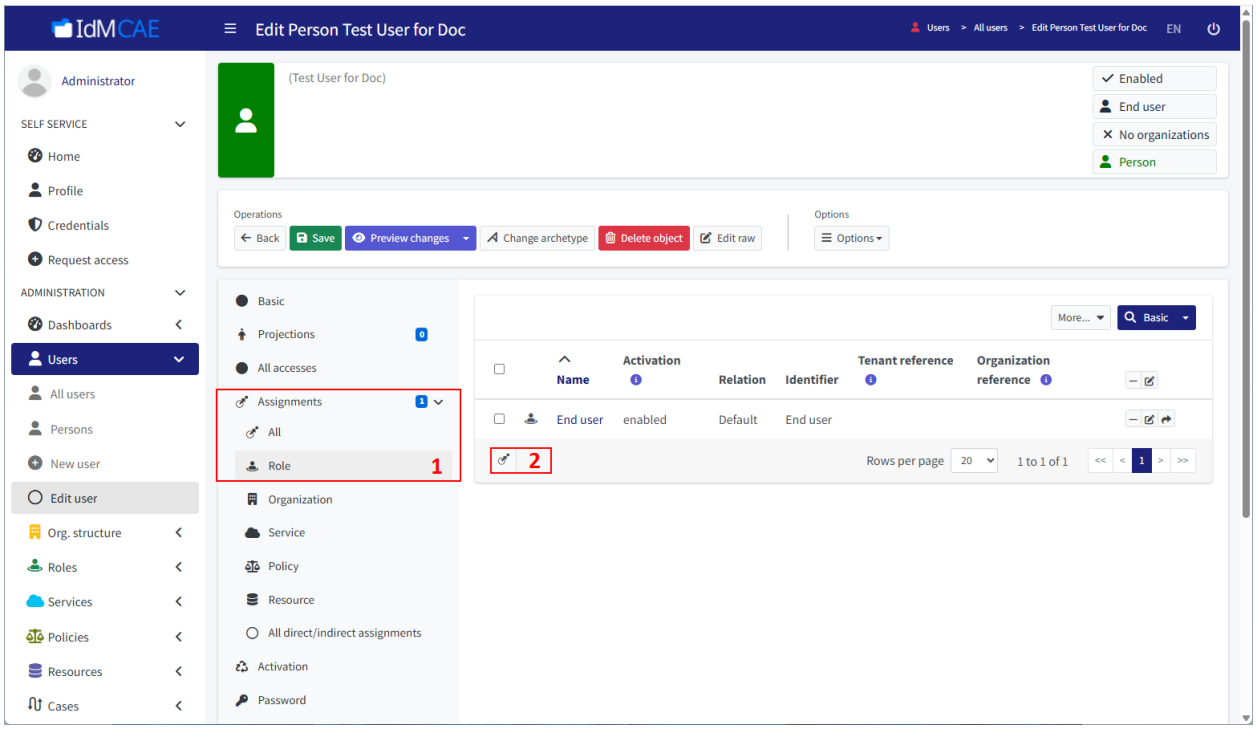


Рисунок 137 – Переход к назначению роли

4. В всплывающем окне **Select object(s)** напротив нужной роли проставьте флаг (1, рисунок 138) и нажмите на **Add** (2, рисунок 138) в правом нижнем углу окна.

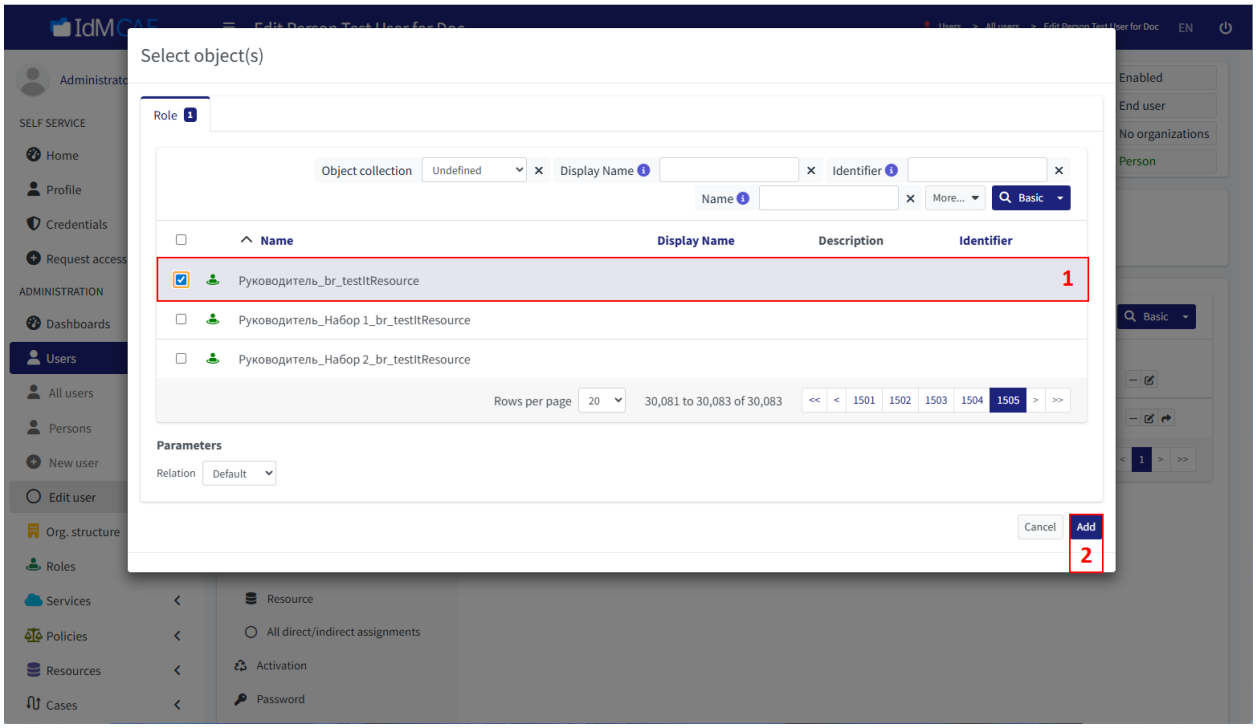


Рисунок 138 – Назначение роли

5. В результате произойдёт автоматический переход в окно для редактирования пользователя, где будет отображена назначенная роль (1, рисунок 139). Сохраните изменения, нажав на **Save** (2, рисунок 139).

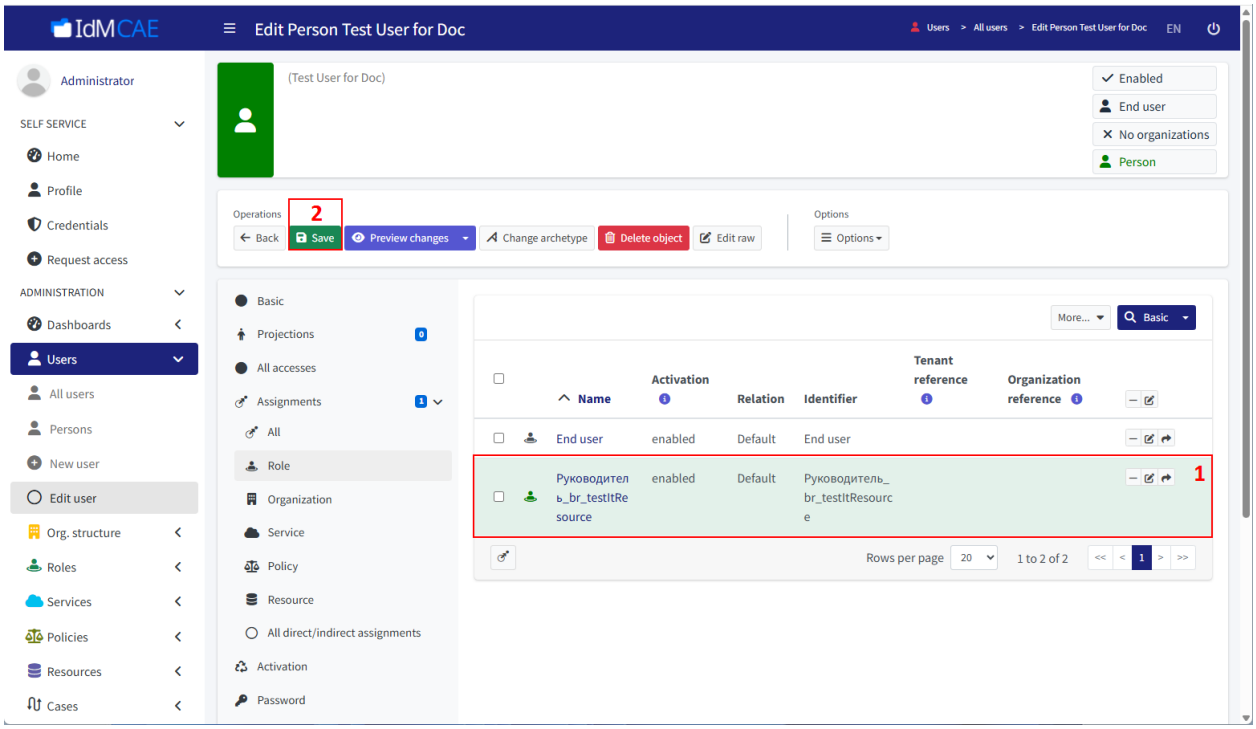


Рисунок 139 – Сохранение изменений

7.1.5.5. Назначение роли через организационную структуру

Для назначения роли пользователю через организационную структуру выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Org. structure -> Organization tree** (1, рисунок 140) в разделе **ADMINISTRATION**. Выберите вкладку с организационной структурой (2, рисунок 140) и справа от нужного узла нажмите на ⋮. В выпадающем списке выберите **Edit** (3, рисунок 140).

   Обратите внимание, что назначение будет производиться только на выбранный узел, а на вложенные нет (если он является головным)!

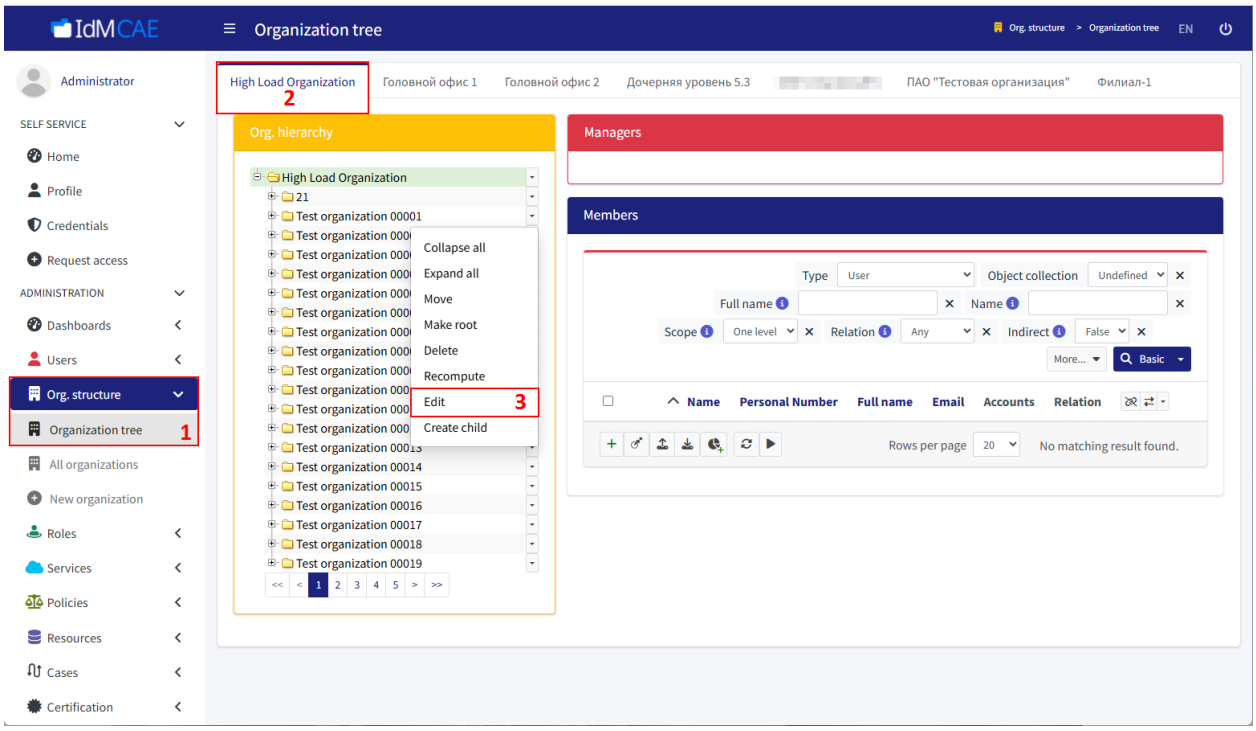


Рисунок 140 – Переход к редактированию узла

3. Перейдите на вкладку **Inducements -> All** (1, рисунок 141) и нажмите на  (2, рисунок 141).

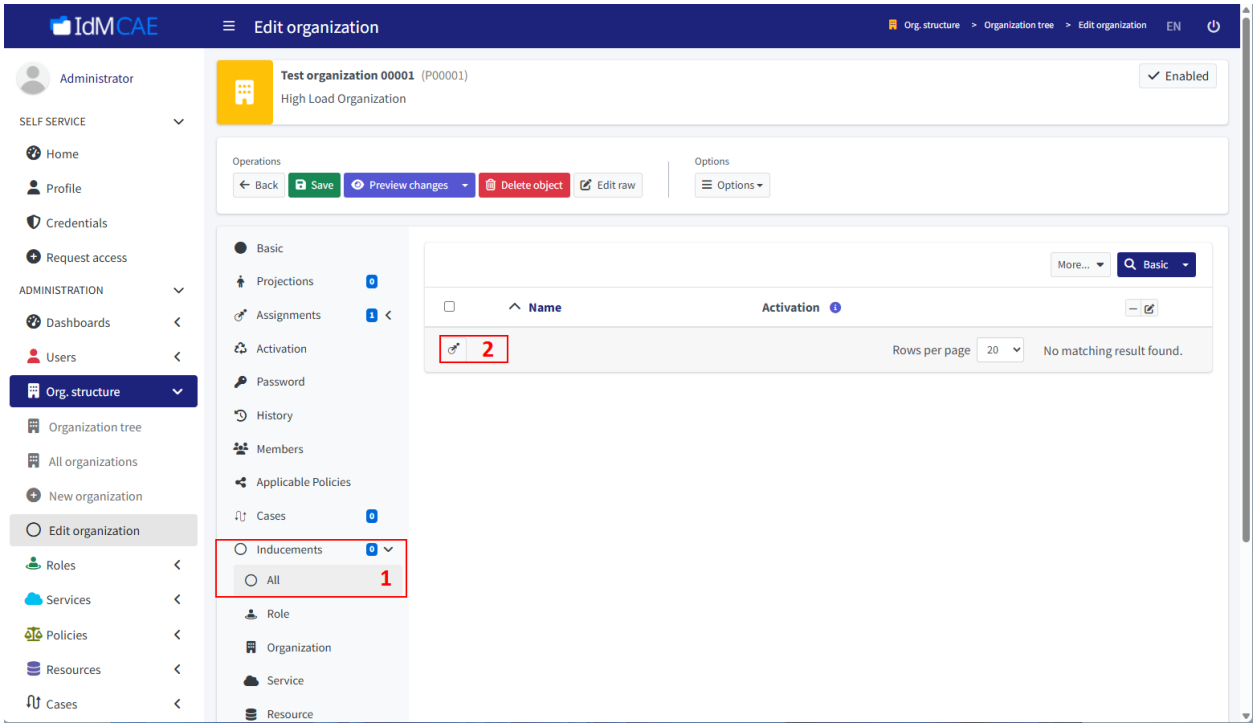


Рисунок 141 – Переход к изменению организационной единицы

4. Выберите вкладку **Role** (1, рисунок 142) и отметьте флагами назначаемые роли (2, рисунок 142). При необходимости измените значения поля в блоке **Parameters** (3, рисунок 142). Нажмите на **Add** (4, рисунок 142).

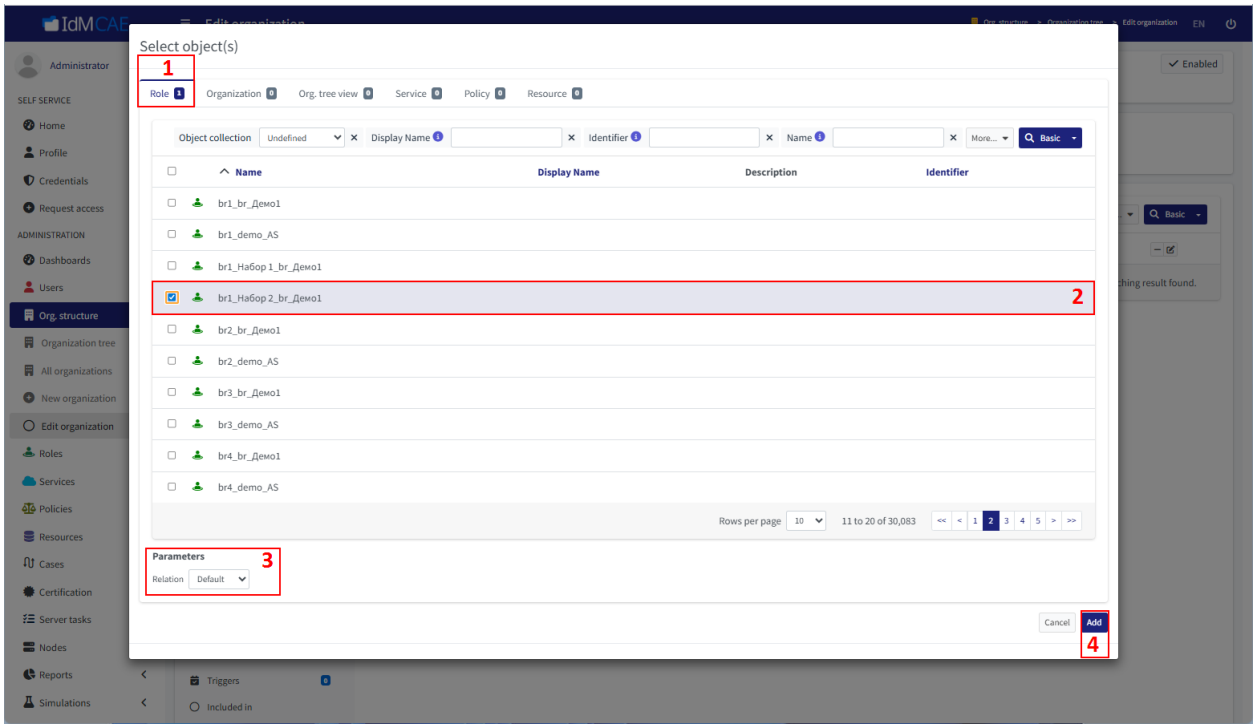


Рисунок 142 – Выбор назначаемых ролей

5. В результате в окне отобразится список назначаемых ролей при условии присутствия пользователя в выбранной организационной единице. Сохраните изменения, нажав на **Save** (рисунок 143).

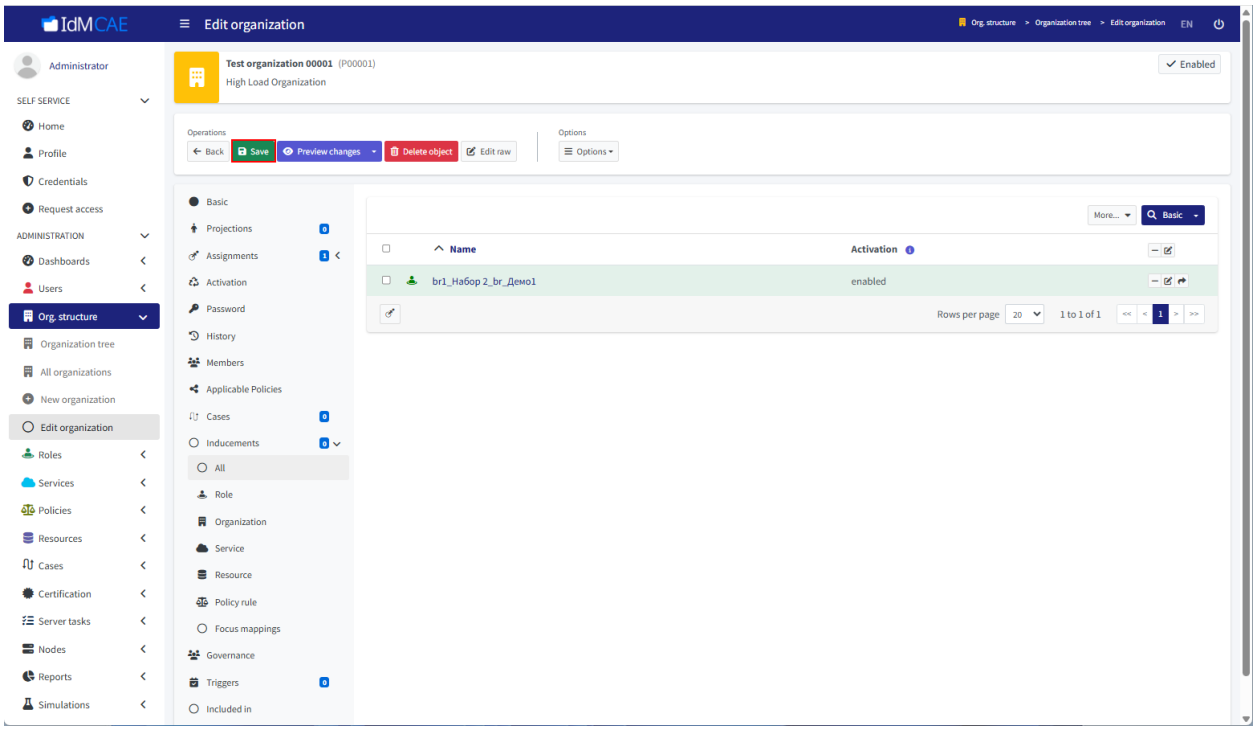


Рисунок 143 – Сохранение изменений

6. Для применения изменений к уже существующим пользователям выберите **Options** (1, рисунок 144) и в выпадающем списке установите флаг напротив **Reconcile** (2, рисунок 144). Ещё раз нажмите на **Save** (3, рисунок 144).

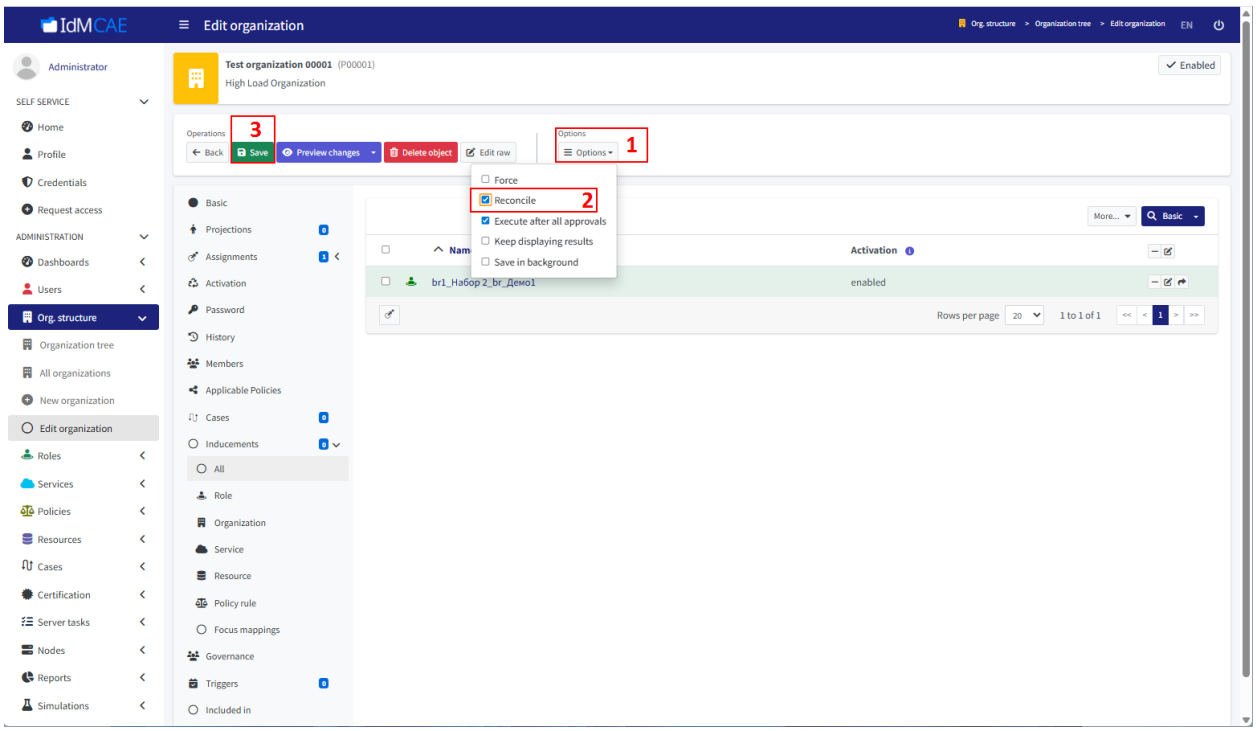


Рисунок 144 – Выполнение реконсиляции

7.1.6. Управление организационными единицами

7.1.6.1. Ручное создание организационной единицы

Для ручного создания организационной единицы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Org. structure -> New organization** (1, рисунок 145) в разделе **ADMINISTRATION**. В открывшемся окне **New organization** на вкладке **Basic** (2, рисунок 145) обязательно заполните поле **Name** (3, рисунок 145), остальные – по желанию. Сохраните изменения, нажав на **Save** (4, рисунок 145).

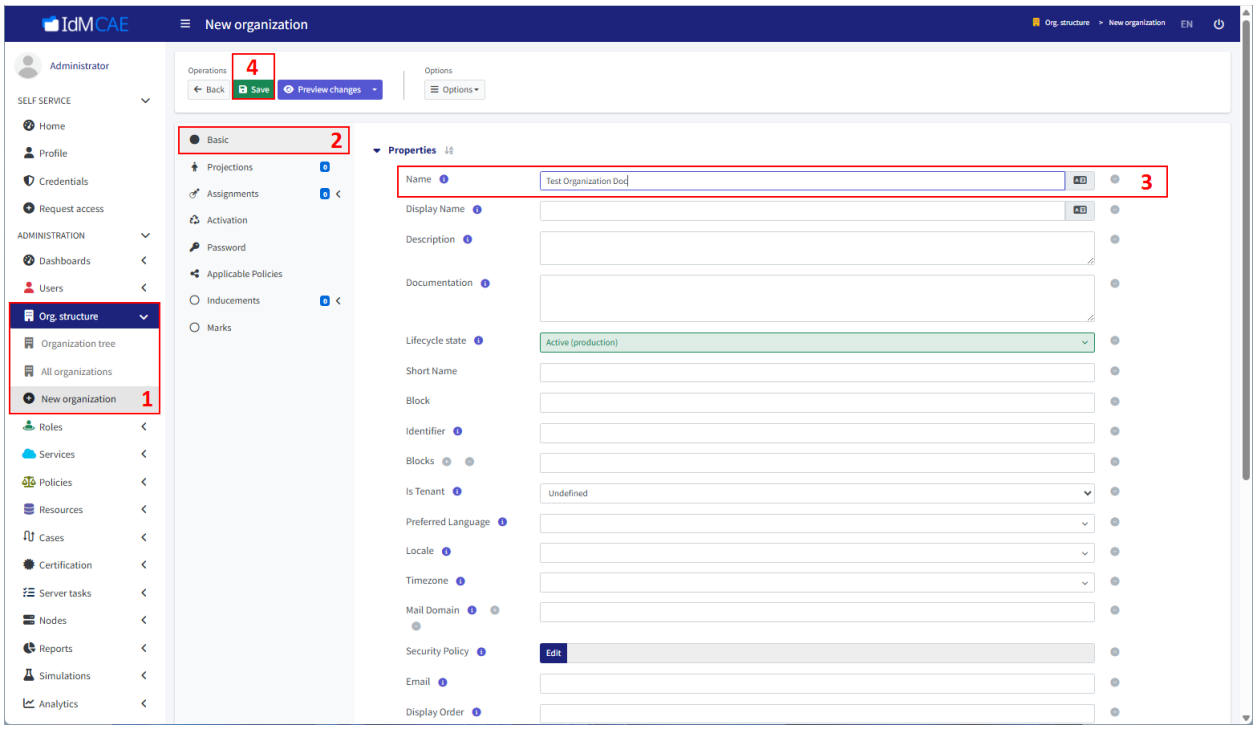


Рисунок 145 – Ручное создание организационной единицы

7.1.6.2. Изменение организационной единицы

Для ручного редактирования организации выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева с вменю выберите **Org. structure -> Organization tree** (1, рисунок 146). Выберите вкладку с нужной организацией (2, рисунок 146). Нажмите на  (3, рисунок 146) и выберите нужную операцию из выпадающего списка (4, рисунок 146). Описание возможных операций представлено в таблице 6.

Таблица 6 – Операции при редактировании организационной единицы

№	Операция	Описание	Когда используется
1.	Collapse all	Сворачивание развёрнутых узлов (подразделений, групп) в иерархии, оставляя только корневые элементы	Упрощение вида дерева и скрытие вложенной структуры
2.	Expand all	Просмотр иерархии (вложенных элементов, таких как подразделения, роли, пользователи)	Полный обзор организационной структуры
3.	Move	Перемещение выбранного элемента в другую часть иерархии	Реорганизация организационной структуры
4.	Make root	Установление выбранного элемента новым корневым элементом (верхним уровнем иерархии) Пример: если **Филиал 1** подчинён **Головному офису**, после операции **Make root Филиал 1** станет независимым коневым объектом	Разделение организаций или изменении структуры управления
5.	Delete	Удаление выбранного элемента из иерархии	Ликвидация устаревшего элемента (подразделения)
6.	Recompute	Принудительный пересчёт зависимостей, ролей и политик доступа для выбранного элемента	Изменение в политиках
7.	Edit	Открытие формы редактирования выбранного элемента (названия, описания, атрибутов, политик)	Тонкая настройка объектов
8.	Create child	Создание дочернего элемента внутри выбранного узла	Расширение организационной структуры

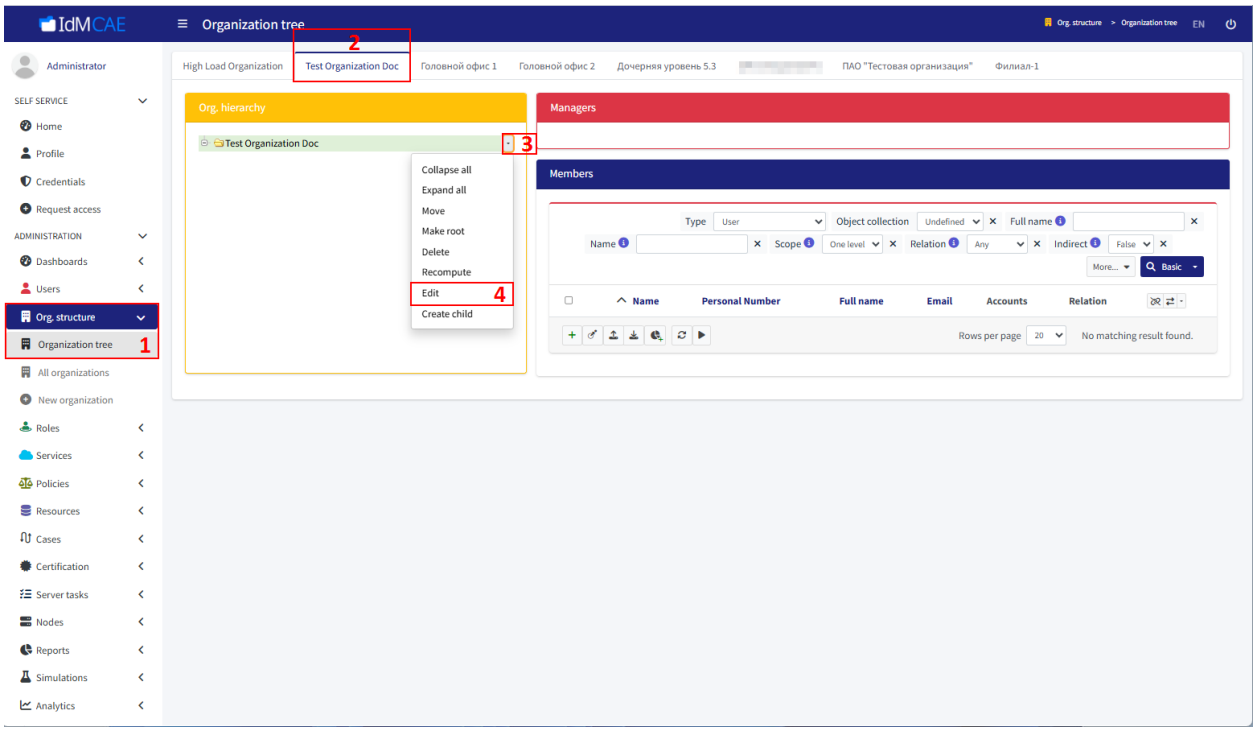


Рисунок 146 – Изменение организационной единицы

Подсказка: Org. hierarchy используется не только для отображения структуры, но и для управления наследованием ролей, политик доступа и атрибутов.

7.1.6.3. Назначение пользователю организационной единицы

Для назначения пользователю организационной единицы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Org. structure -> Organization tree** (1, рисунок 147) в разделе **ADMINISTRATION**. Перейдите на нужную вкладку (2, рисунок 147), раскройте дерево с организационной структурой до необходимого

уровня и выберите организационную единицу (3, рисунок 147). Нажмите на  (4, рисунок 147).

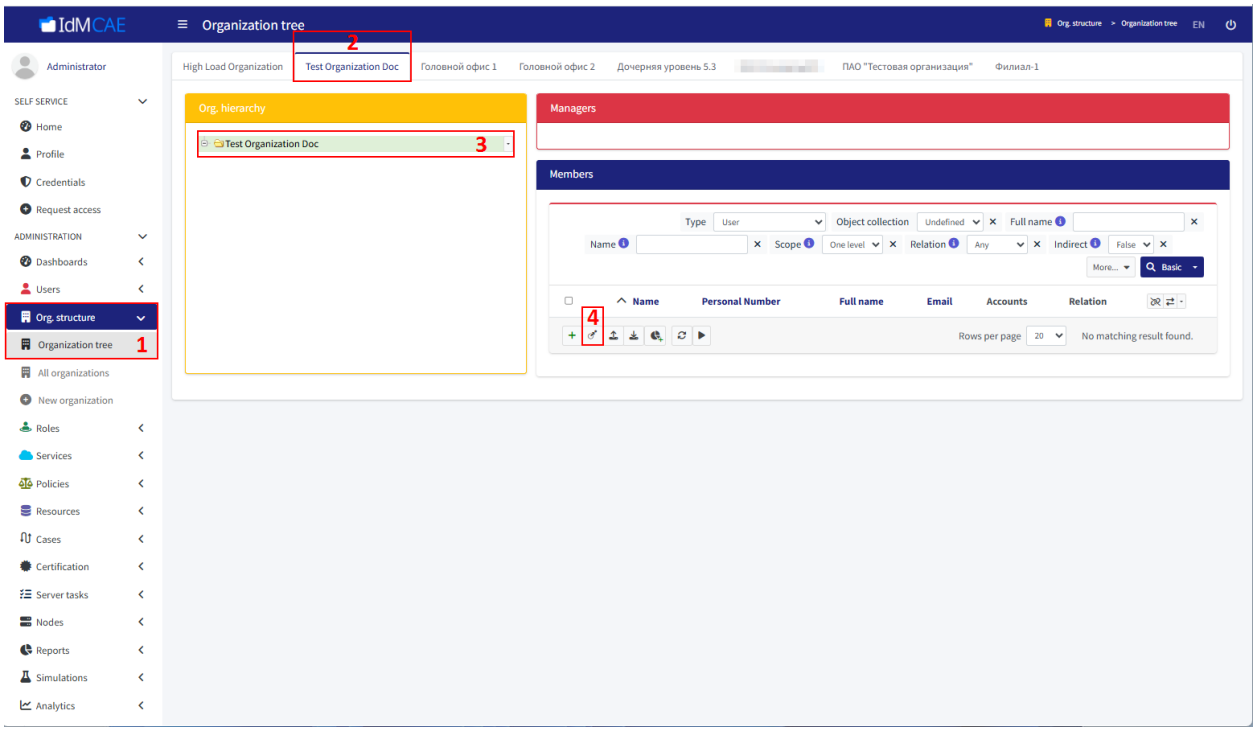


Рисунок 147 – Переход к организационной единице

3. В открывшемся окне **Select Default(s)** найдите пользователя, отметьте его флагом (1, рисунок 148) и нажмите на **Add** (2, рисунок 148).

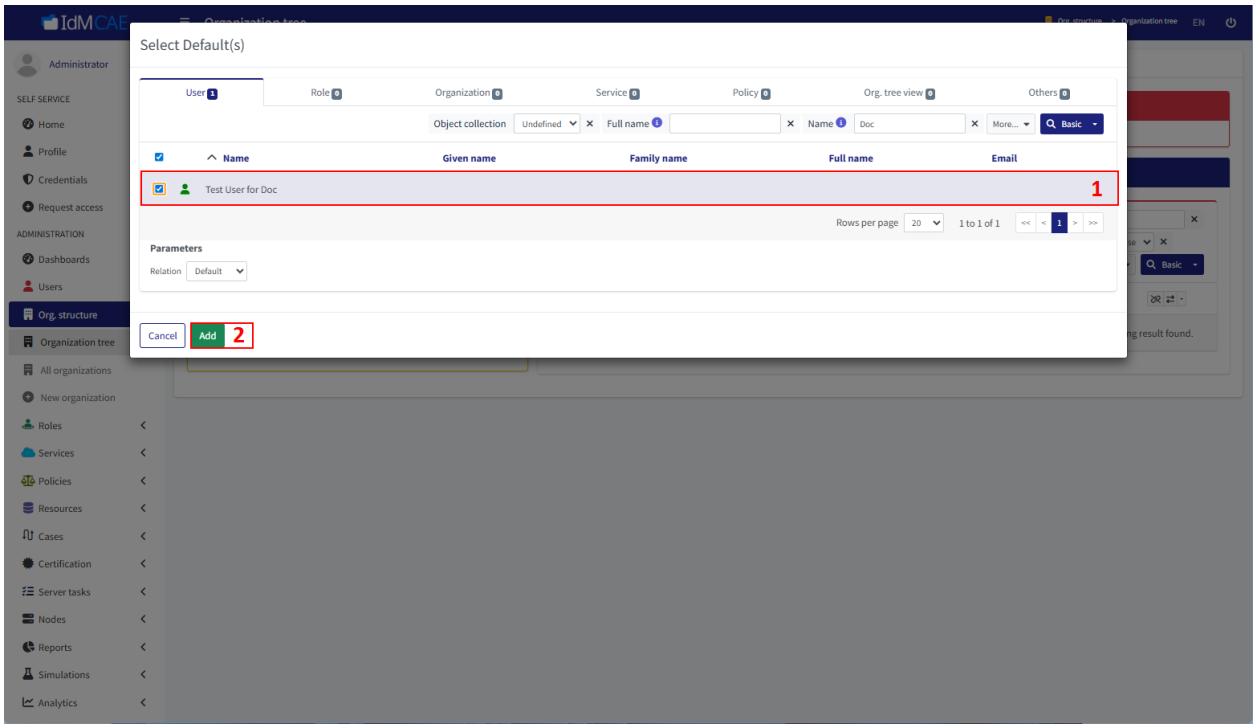


Рисунок 148 – Выбор пользователя

Также назначить пользователю организационную единицу можно через общий список организационных единиц. Для этого выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Org. structure -> All organizations** (1, рисунок 149) в разделе **ADMINISTRATION**. В общем списке найдите нужную организационную единицу и выберите её (2, рисунок 149).

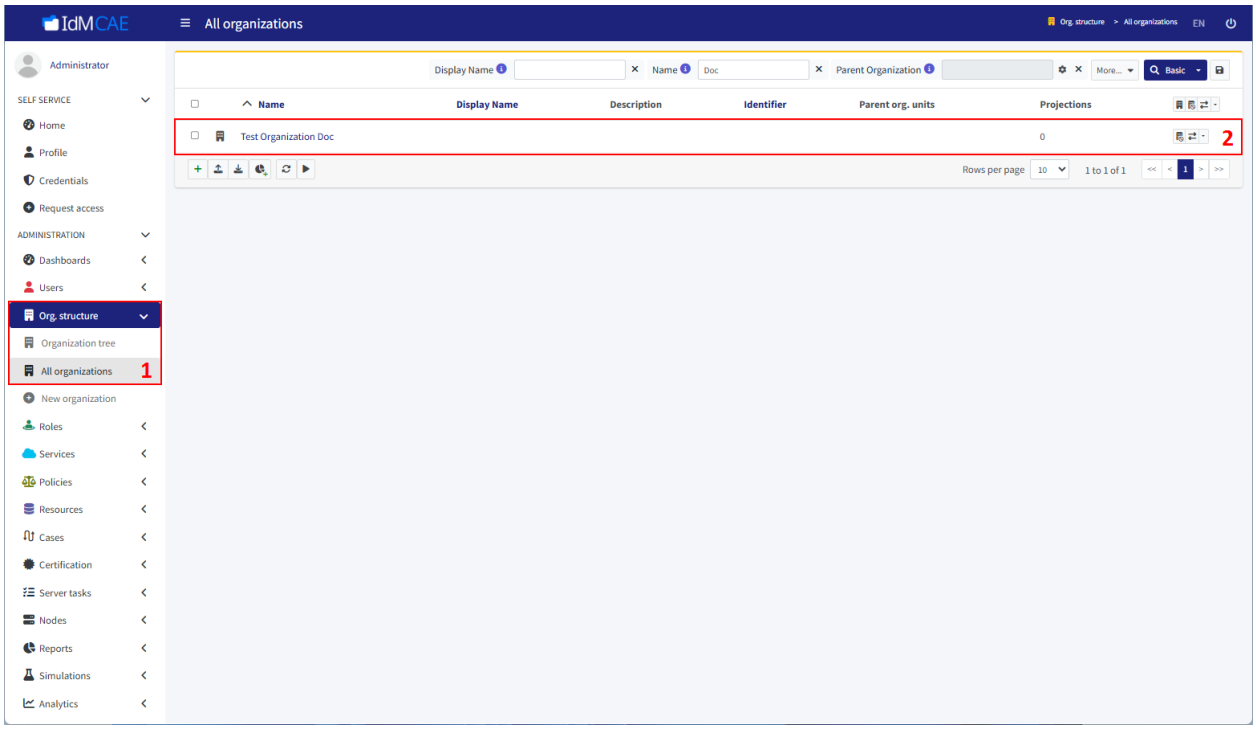


Рисунок 149 – Переход к организационной единице

3. Перейдите на вкладку **Members** (1, рисунок 150). Нажмите на  (2, рисунок 150).

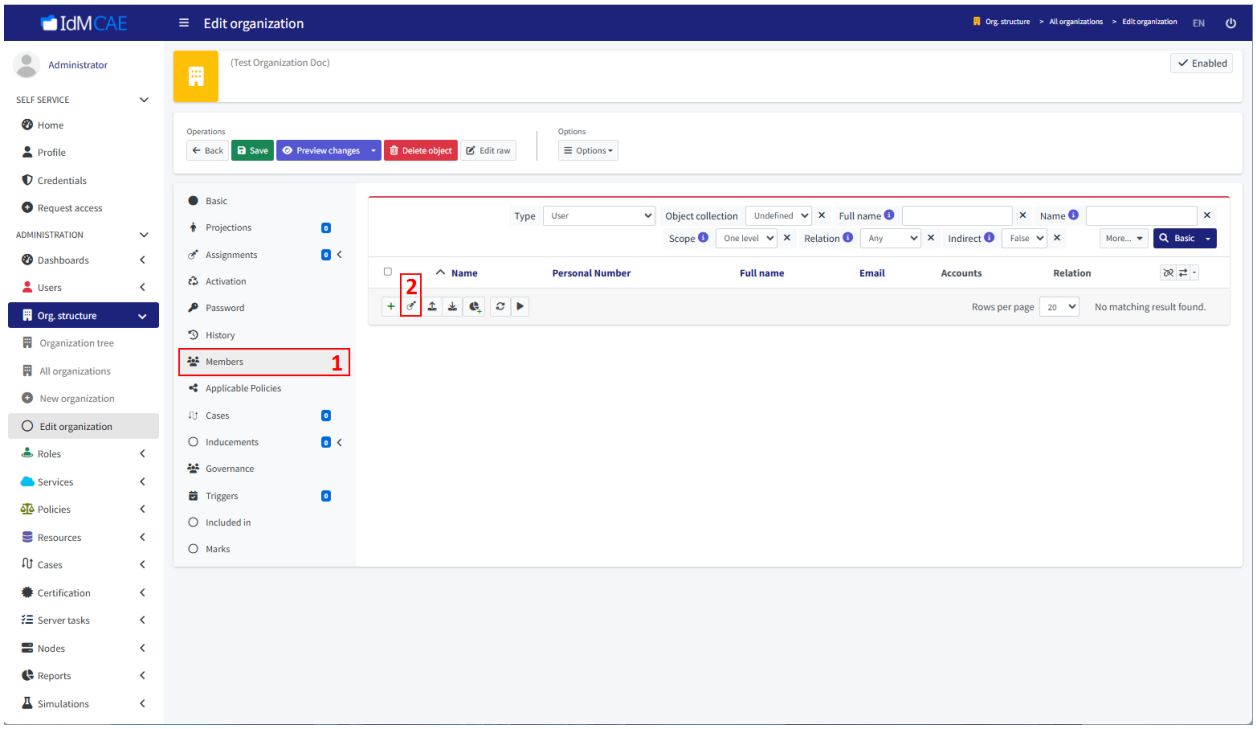


Рисунок 150 – Переход к добавлению пользователя

4. В открывшемся окне **Select Default(s)** найдите пользователя, отметьте его флагом (1, рисунок 151) и нажмите на **Add** (2, рисунок 151).

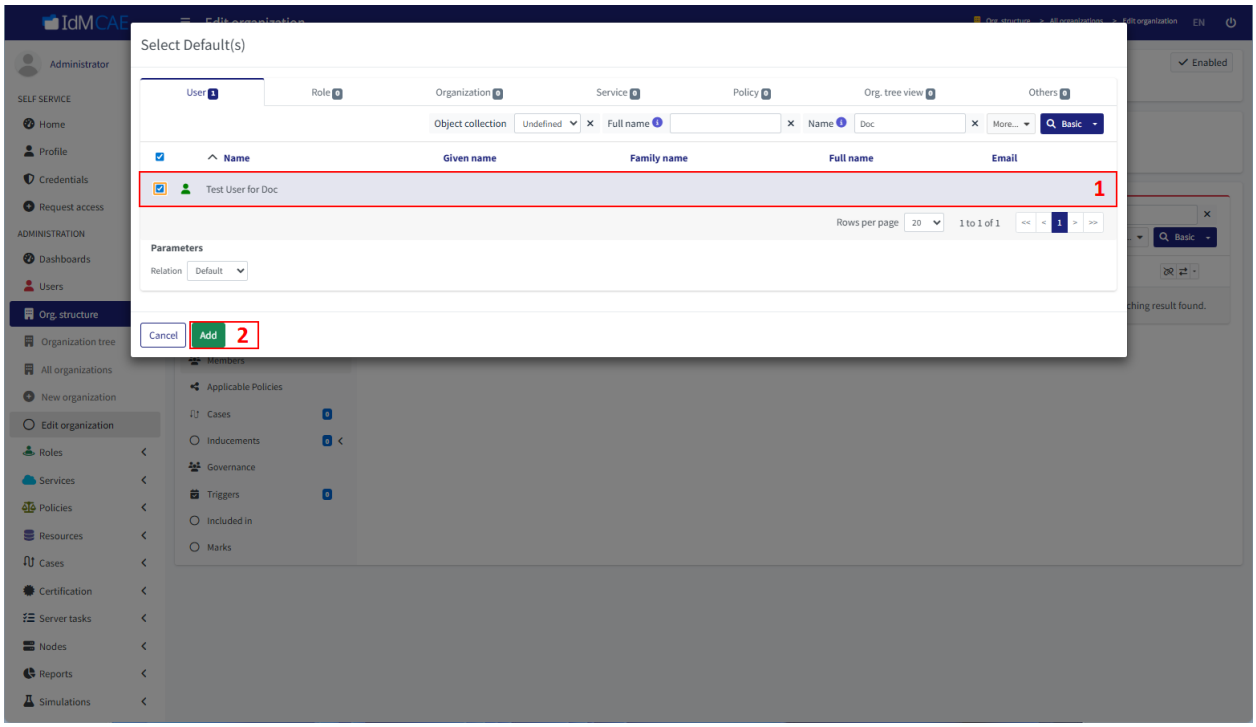


Рисунок 151 – Добавление пользователя

7.1.6.4. Автоматическое назначение пользователям организационной единицы

IDM CAE поддерживает автоматическое назначение пользователям организационной единицы при условии наличия такой информации в ресурсе. Если в качестве источника информации используется CSV-файл, то добавьте идентификаторы назначаемых организационных единиц в подключаемый файл в отдельный столбец **orgnum**.

В рассматриваемом примере представление ресурса выглядит так, как представлено на рисунке 152. Секция **assignmentTargetSearch** ищет нужную организационную единицу,

затем на неё создаётся назначение. После запуска задачи синхронизации ресурса пользователям будут назначены указанные в файле организационные единицы.

```
<attribute>
    <ref>ri:orgnum</ref>
    <inbound>
        <expression>
            <assignmentTargetSearch>
                <targetType>OrgType</targetType>
                <filter>
                    <q:equal>
                        <q:path>identifier</q:path>
                        <expression>
                            <path>$input</path>
                        </expression>
                    </q:equal>
                </filter>
            </assignmentTargetSearch>
        </expression>
        <target>
            <path>$focus/assignment</path>
        </target>
    </inbound>
</attribute>
```

Рисунок 152 – Представление ресурса

7.1.6.5. Импорт организационной структуры

Для импорта организационной структуры из ресурса (HR-ресурса) выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Вручную создайте организационную единицу (подробнее см. в разделе 7.1.6.1), которая будет являться головным узлом иерархии.
3. Создайте (подробнее см. в разделе 7.1.2.2) ресурс или выберите уже существующий, содержащий организационную структуру.

   Обратите внимание, что для предотвращения нежелательных изменений у ресурса в промышленной среде

устанавливайте **Lifecycle state** статус **Proposed (simulation)** (рисунок 153)!

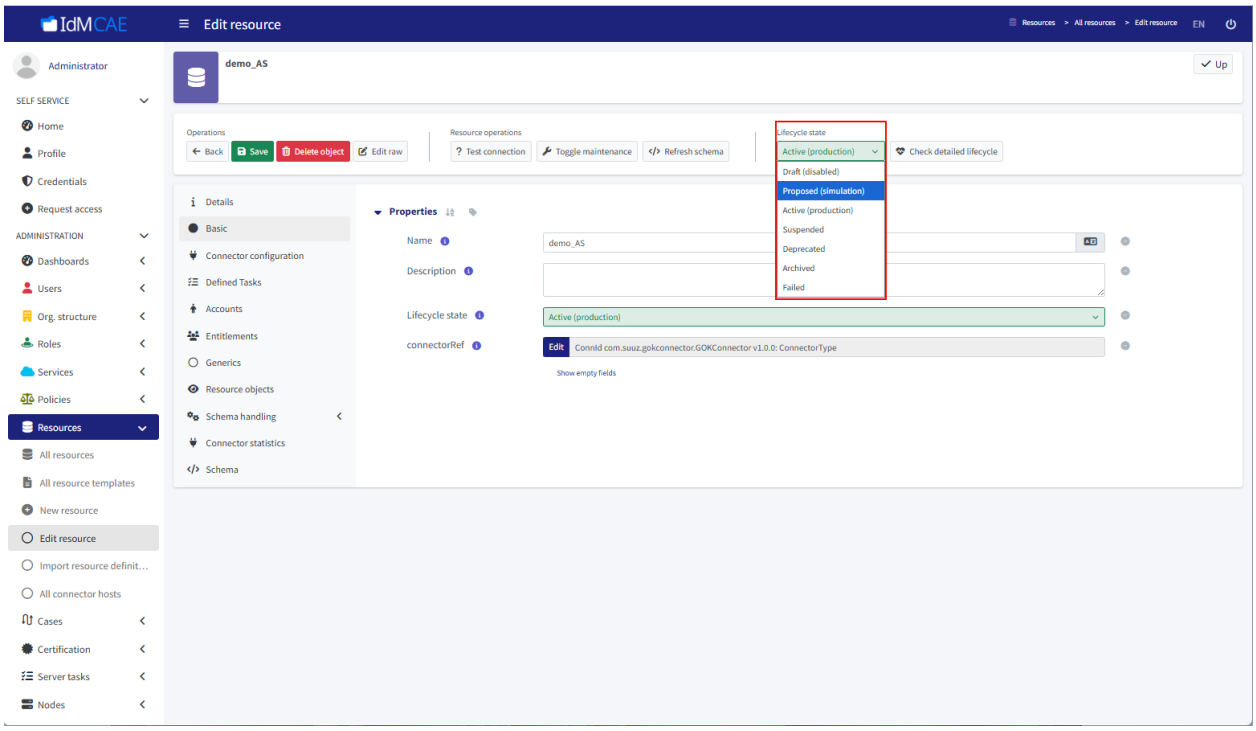


Рисунок 153 – Изменение статуса объекта

4. Перейдите на вкладку **Schema handling -> Object type** (1, рисунок 154) и добавьте тип объекта с помощью Add object type (2, рисунок 154). Введите основную информацию о типе объекта (рисунок 155):
   - Display name: Org;
   - Kind: Generic;
   - Intent: Org.

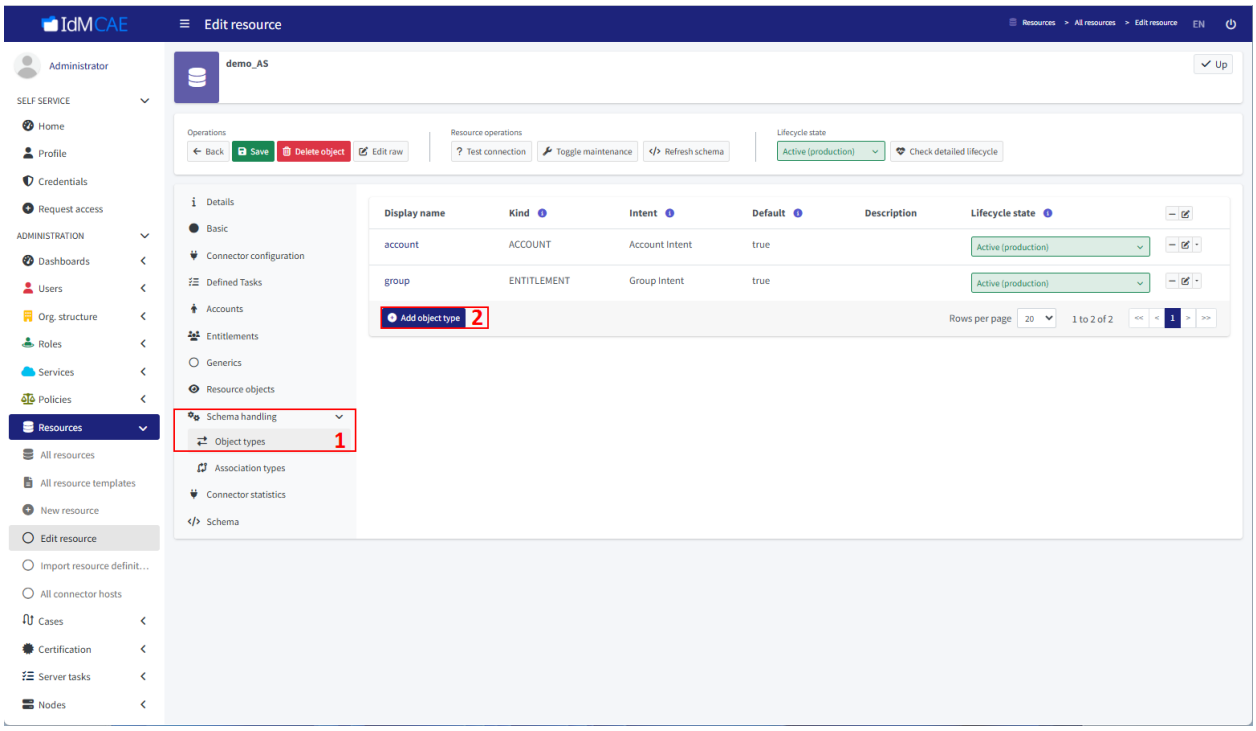


Рисунок 154 – Переход к добавлению типа объекта

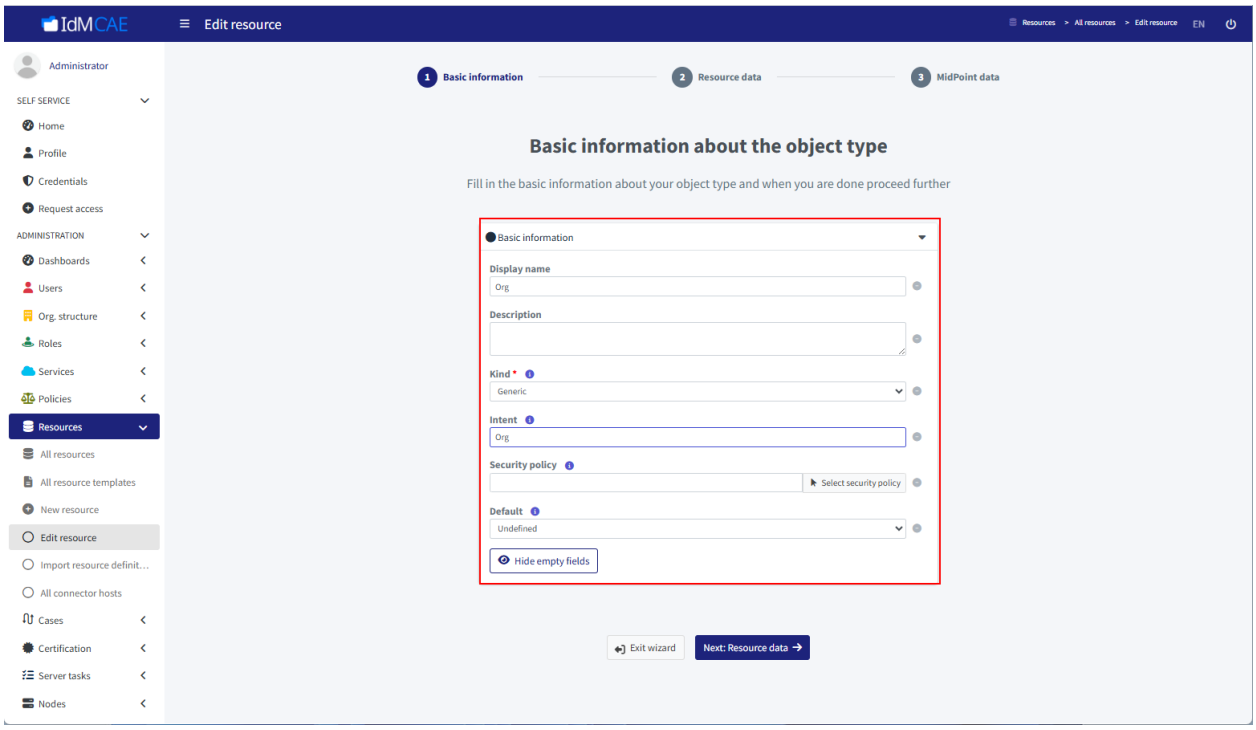


Рисунок 155 – Параметры типа объекта

5. Перейдите в окно **MidPoint data** (1, рисунок 156) и введите в поле **Type** значение **Organization** (2, рисунок 156). Нажмите на **Save settings** (3, рисунок 156).

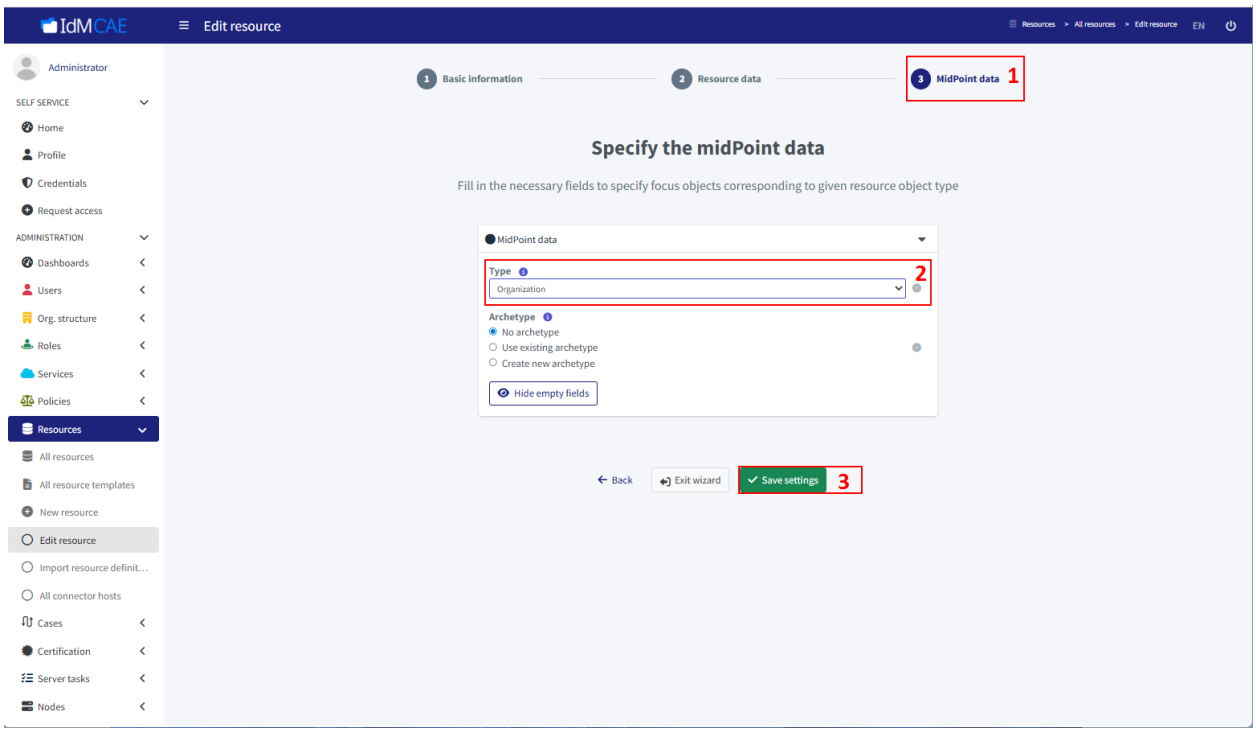


Рисунок 156 – Сохранение типа объекта

6. Перейдите к настройке параметров синхронизации созданного типа объекта, выбрав **Synchronization** (рисунок 157). Также к настройкам синхронизации можно перейти через вкладку **Generics** в окне с параметрами ресурса, нажав на **Configure -> Synchronization**.

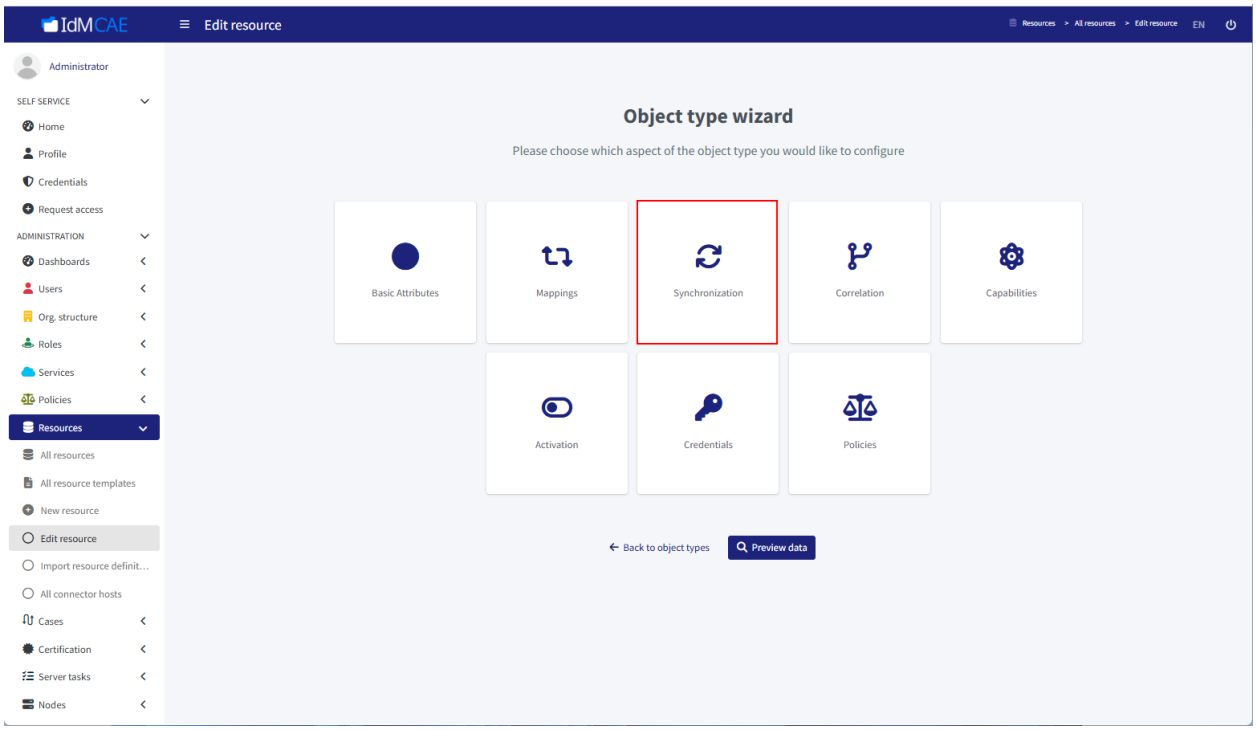


Рисунок 157 – Переход к настройке синхронизации

7. Выполните настройку параметров синхронизации в соответствии с разделом 7.1.9.
8. Перейдите к настройке параметров маппингов созданного типа объекта, выбрав **Mappings** (рисунок 158). Также к настройкам маппингов можно перейти через вкладку **Generics** в окне с параметрами ресурса, нажав на **Configure -> Mappings**.

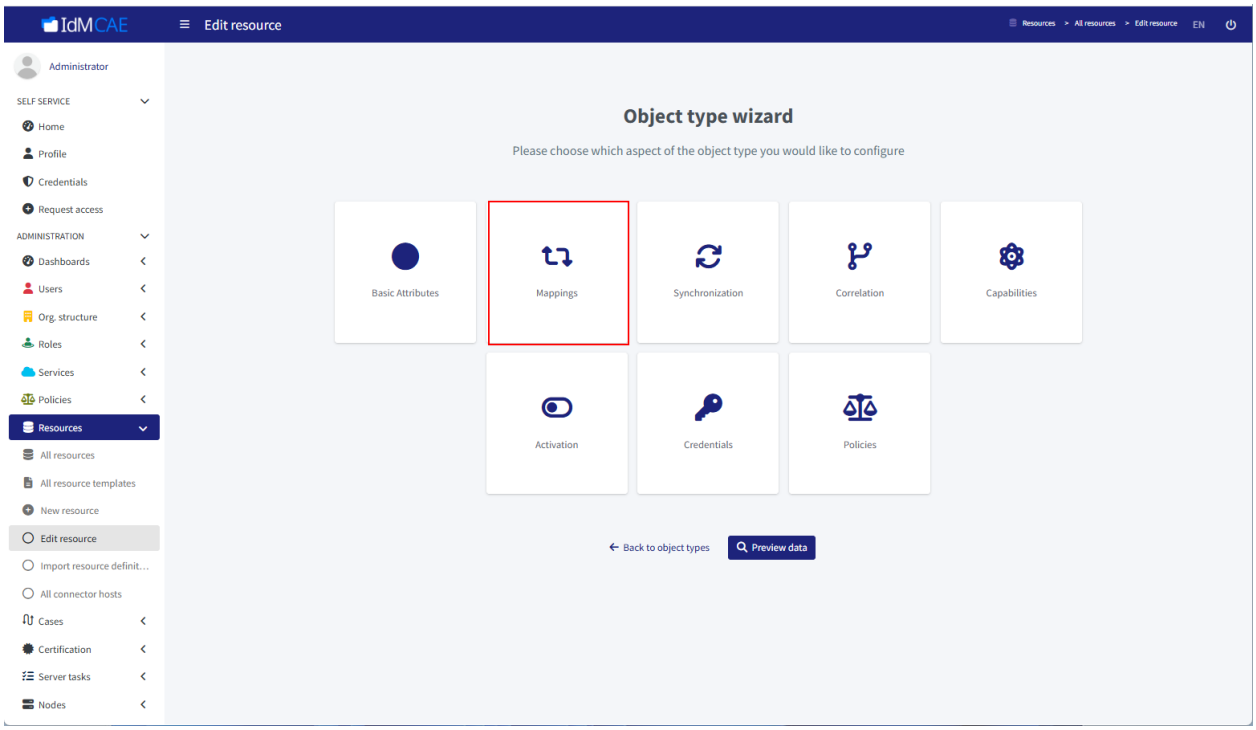


Рисунок 158 – Переход к настройке маппингов

9. Добавьте входящие маппинги с помощью **Add inbound** (1, рисунок 161) со следующими настройками (2, рисунок 161):

- 1:
    - Name: name-script;
    - From resource attribute: name;
    - Expression: Script (оставьте скрипт пустым);
    - Target: assignment (именно так, из списка выбирать не нужно);
    - Lifecycle state: Active;
- 2:
    - Name: name-to-name;
    - From resource attribute: name;
    - Expression: As is;

- Target: name;
- Lifecycle state: Active.

Нажмите на  (3, рисунок 161) справа от каждого маппинга и установите в поле **Strength** значение **Strong** (рисунок 159), а в поле **Use for** – **Undefined** (1, рисунок 160). Нажмите на **Done** (2, рисунок 160).

Сохраните настройки, нажав на **Save mappings** (4, рисунок 161).

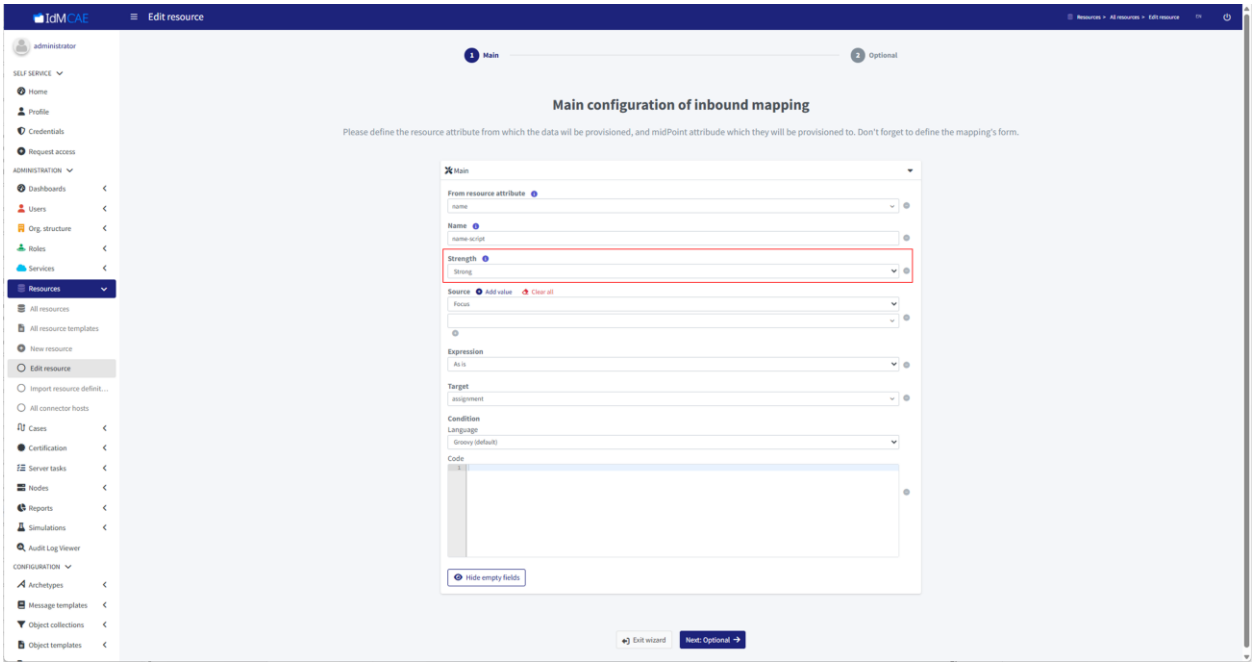


Рисунок 159 – Настройка поля Strength

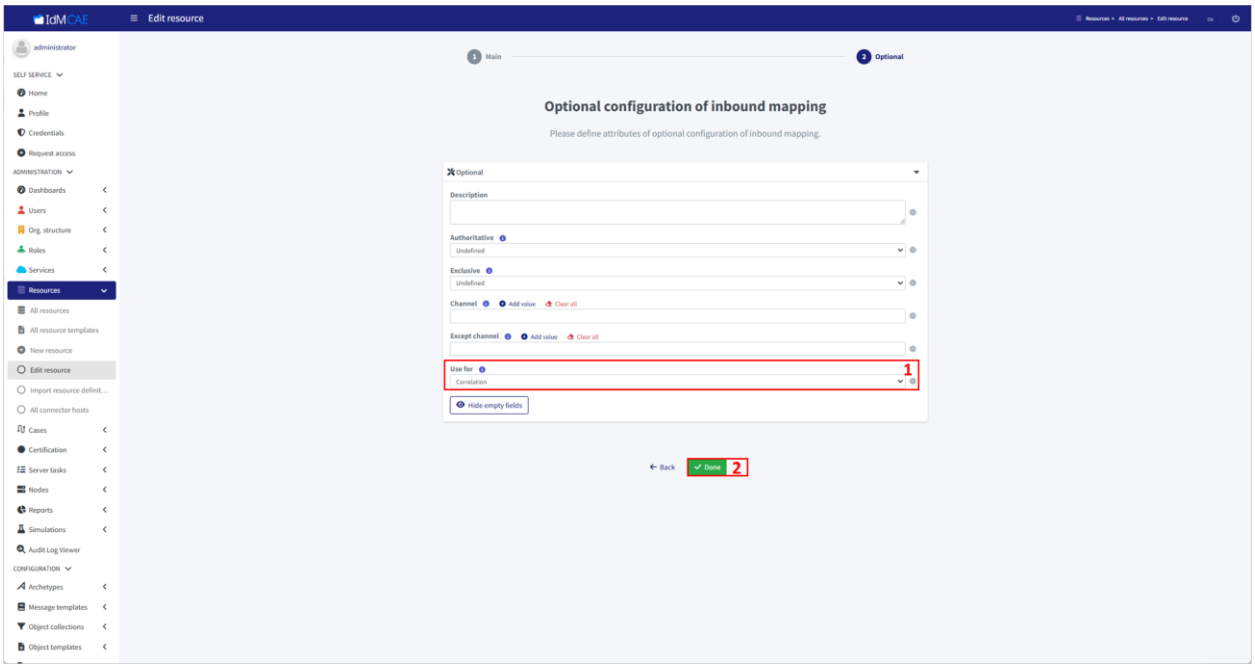


Рисунок 160 – Настройка поля Use for

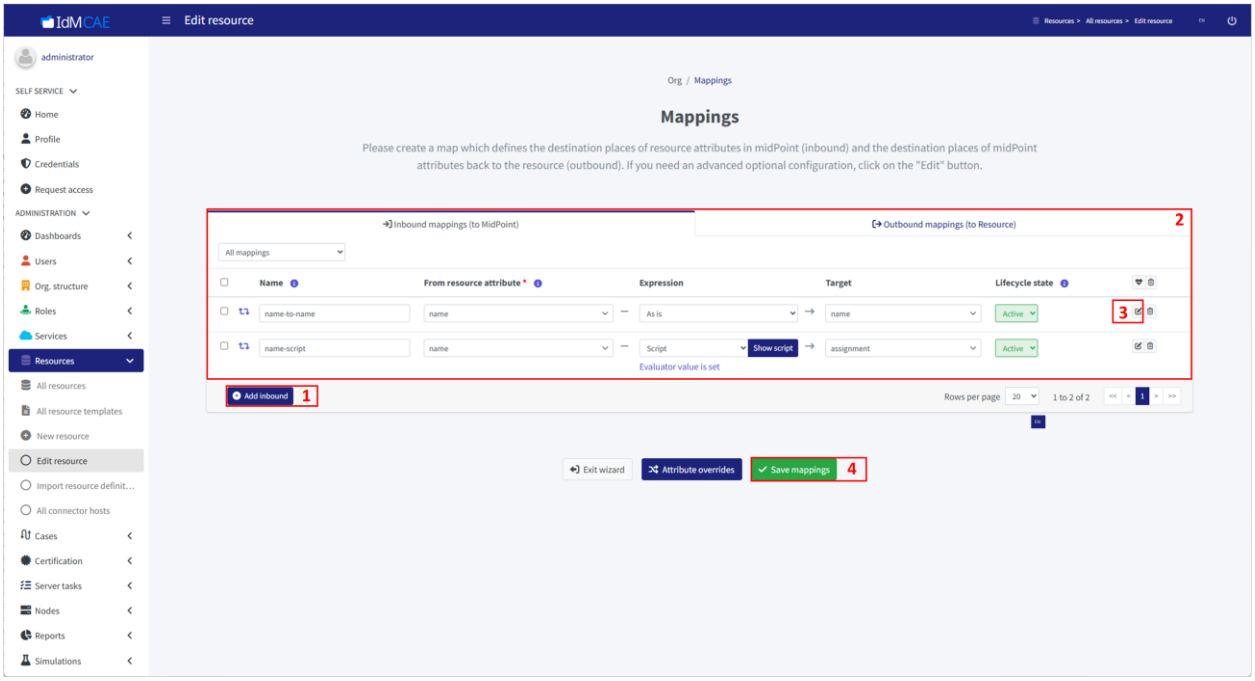


Рисунок 161 – Настройки маппингов

10. Перейдите на вкладку **Basic** (1, рисунок 162) и нажмите на **Edit raw** (2, рисунок 162). Отредактируйте объект ресурса, вставив туда строки для структурирования организационных единиц (иначе импортированные

организационные единицы будут находиться на одном уровне иерархии). Для этого исправьте код в секции **schemaHandling** тэг **inbound**, который относится к маппингу **name-script** (1, рисунок 163), на следующее содержание (в OID пропишите OID головного узла):

```
                <inbound>
                    <name>name-script</name>
                    <strength>strong</strength>
                    <expression>
                        <assignmentTargetSearch>
                            <targetType>c:OrgType</tar-
getType>
                            <filter>
                                <q:equal>
                                    <q:match-
ing>strictIgnoreCase</q:matching>
                                    <q:path>name</q:path>
                                    <expression>
                                        <script>
                                            <code>
                                               paren-
tOrgNum = basic.getAttributeValue(projection, "paren-
tOrgNum");


                                                if(
parentOrgNum == "0" ){

                                                return
"External";
                                                }
                                                return
"Technical Directorate"
                                            </code>
                                        </script>
                                    </expression>
                                </q:equal>
                            </filter>
                            <defaultTargetRef
oid="ace0d857-dd2e-4c67-973c-6478770bfbcc" type="OrgType"
xsi:type="c:ObjectReferenceType"/>
                        </assignmentTargetSearch>
                    </expression>
                    <target>
                        <path>$focus/assignment</path>
                        <set>
                            <predefined>all</predefined>
```

```
            </set>
        </target>
    </inbound>
```

При возникновении пустых строк **НЕ исправляйте** их вручную, так как после сохранения они исчезнут сами.

Сохраните изменённый код, нажав на **Save** (2, рисунок 163).

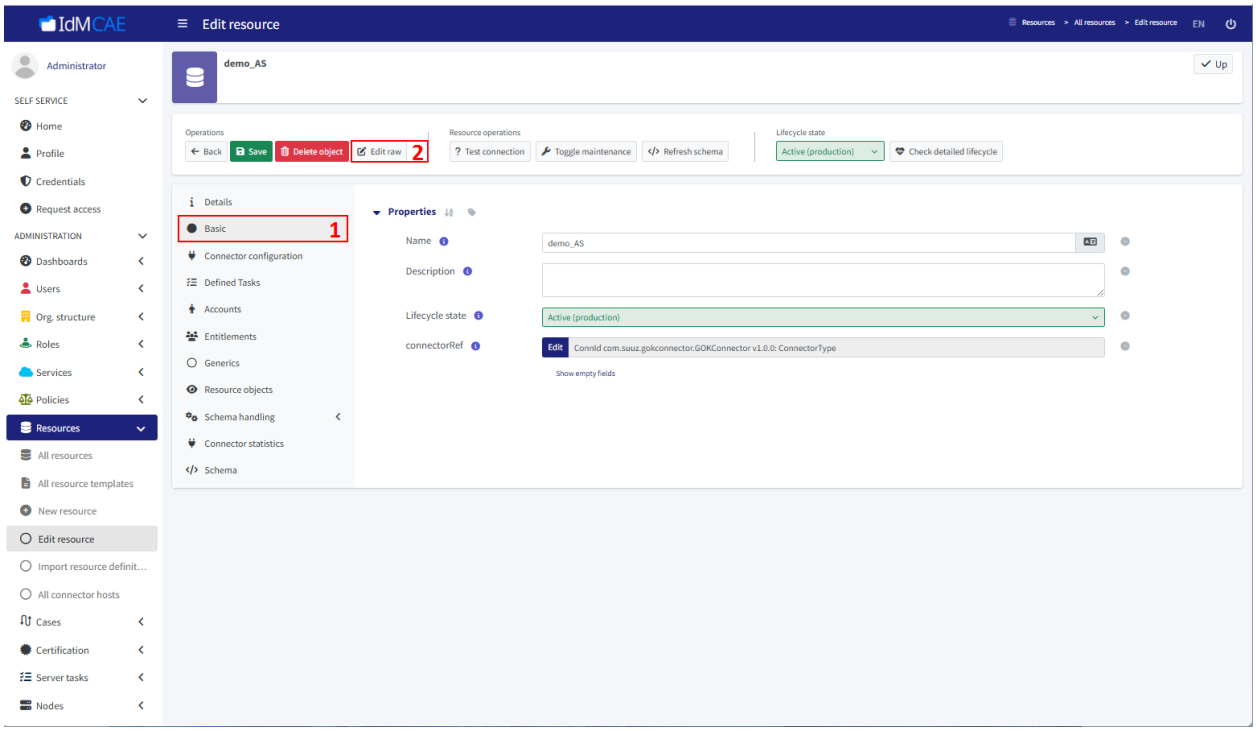


Рисунок 162 – Переход к редактированию объекта ресурса

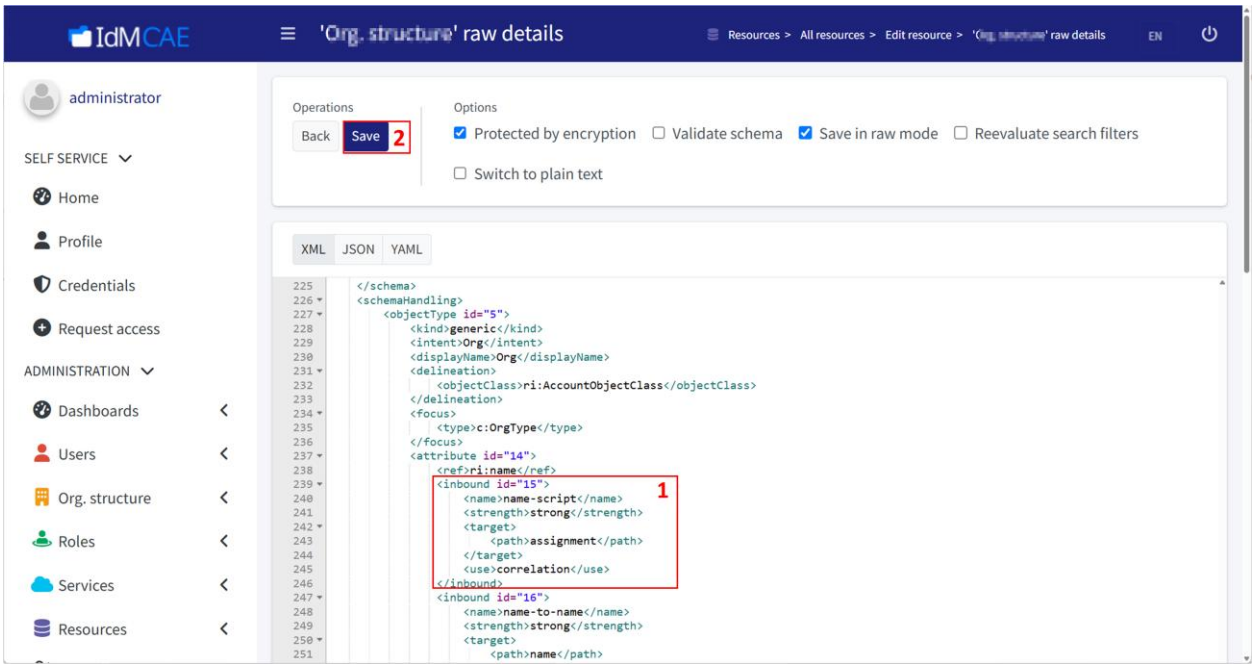


Рисунок 163 – Редактирование schemaHandling

11. Измените значение поля **Lifecycle state** на **Active** на вкладке **Basic** (рисунок 164).

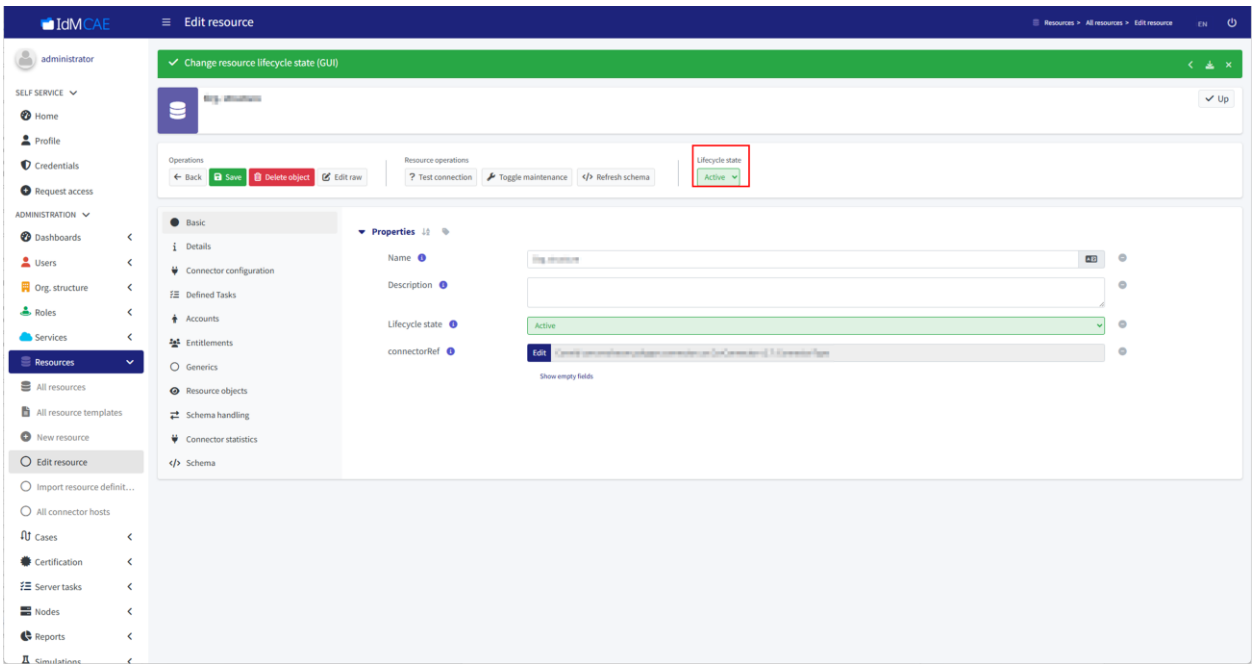


Рисунок 164 – Изменение статуса ресурса

12. Создайте задание для ресурса (подробнее см. в разделе 7.1.2.9), указав следующие параметры (рисунок 165, 166):

- Name: Orgs import;
- Kind: Generic;
- Intent: Org;
- Object class: класс объектов, указанный в момент создания ресурса (в примере AccountObjectClass).

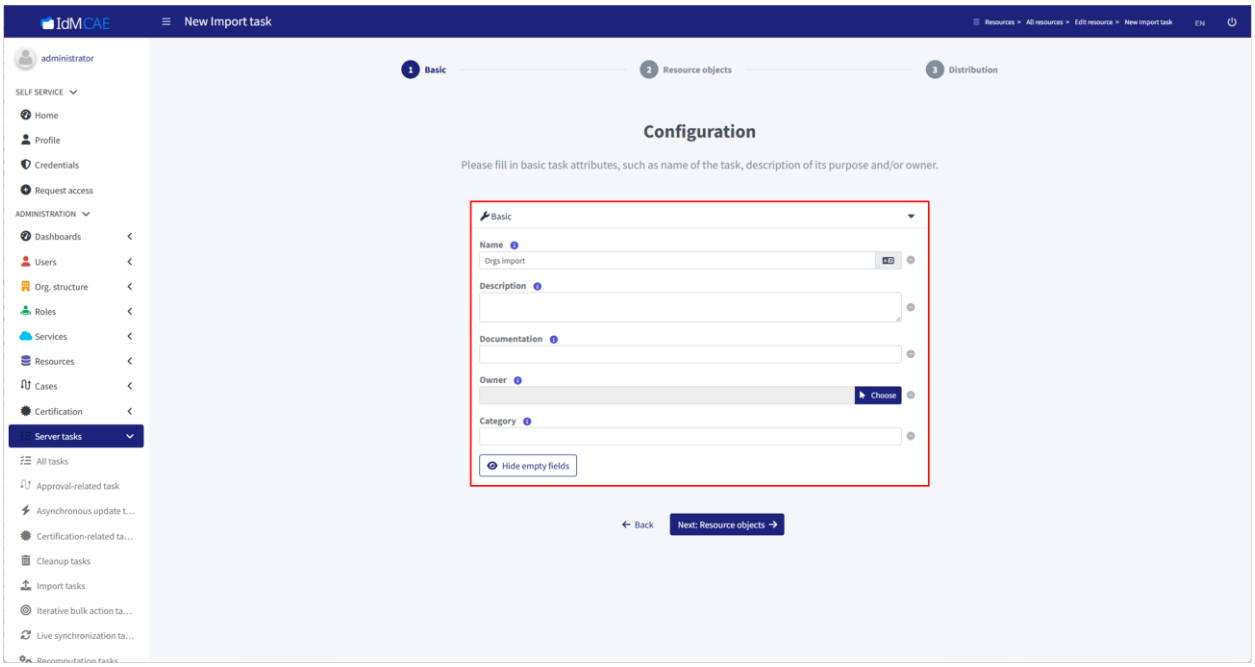


Рисунок 165 – Параметры задачи (1)

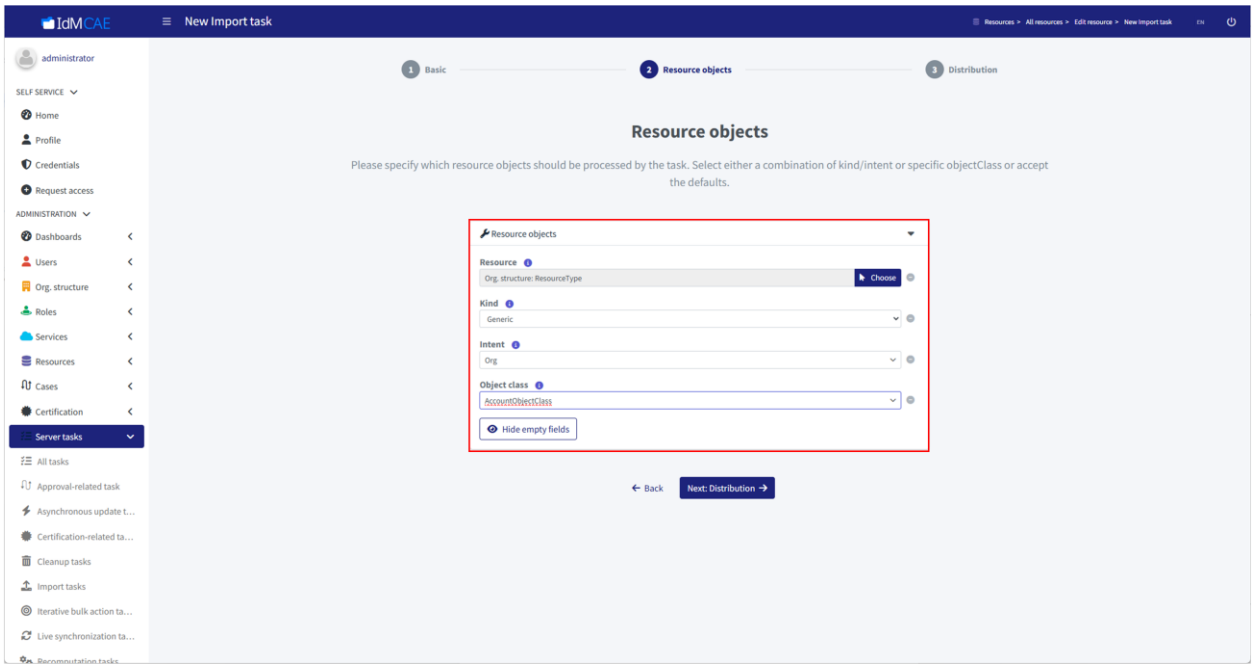


Рисунок 166 – Параметры задачи (2)

Запустите созданную задачу и в результате существующая в ресурсе организационная структура (рисунок 167) будут импортированы в IDM CAE с головным узлом, созданном в шаге 2.

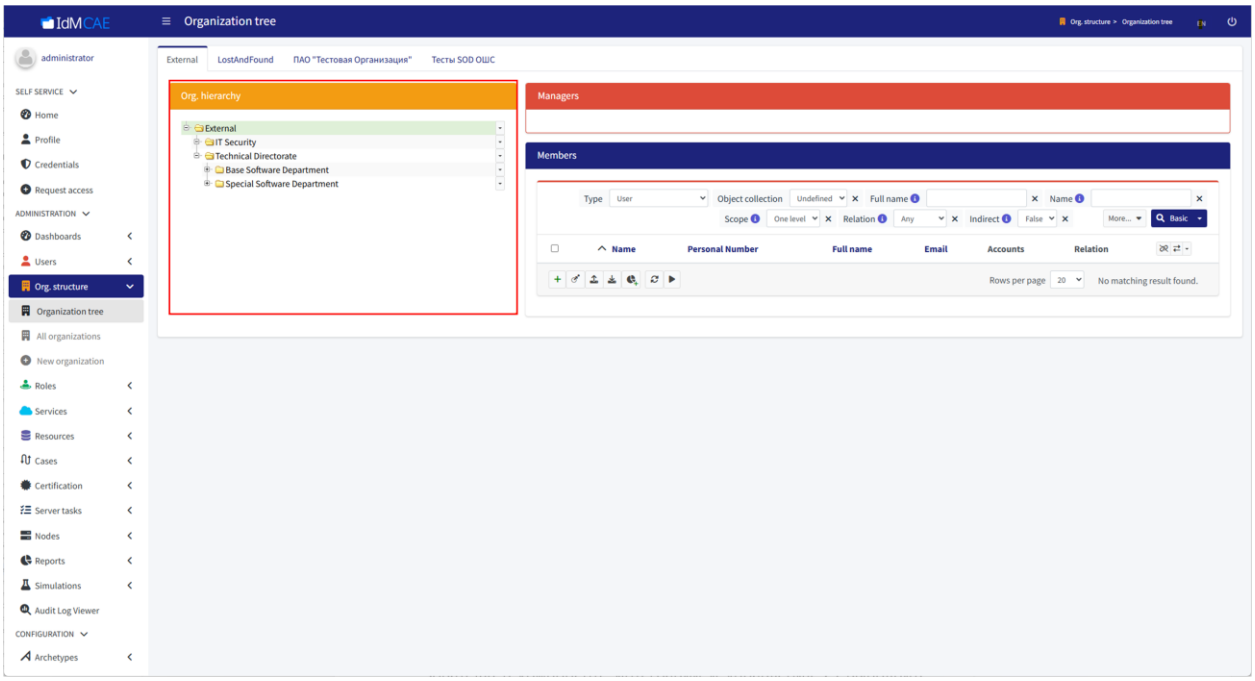


Рисунок 167 – Импортированная организационная структура

7.1.7. Управление объектами

7.1.7.1. Удаление объектов

Для удаления объекта (роли, организационной единицы, пользователя) выполните следующие действия:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите нужный список с объектами (в примере будет использоваться список организационных единиц **Org. structure -> All organizations** (1, рисунок 168) в разделе **ADMINISTRATION**. В общем списке найдите нужный объект и нажмите ▾ справа с окна (2, рисунок 168). В выпадающем списке выберите **Delete** (3, рисунок 168) и подтвердите удаления, нажав на **Yes** в всплывающем окне.

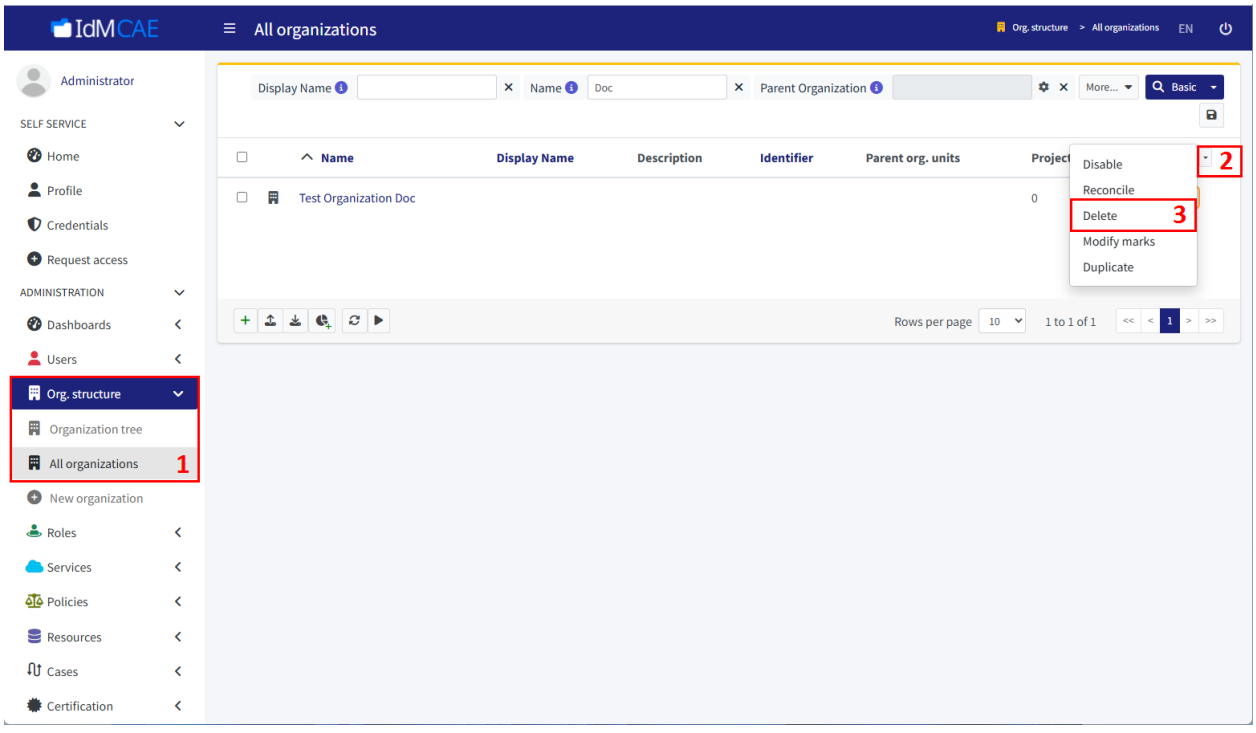


Рисунок 168 – Удаление объекта

7.1.7.2. Определение идентификатора объекта

Для определения идентификатора объекта выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Выберите нужный объект.
3. В адресной строке браузера скопируйте набор символов после **/** и до **?** (рисунок 169) или после **=** и до конца строки (рисунок 170) в зависимости от выбранного объекта.

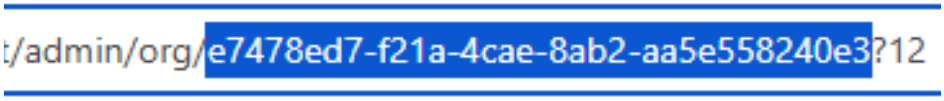


Рисунок 169 – Идентификатор объекта (1)

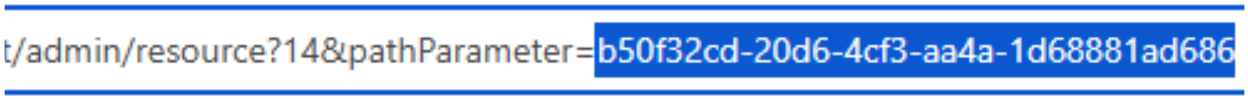


Рисунок 170 – Идентификатор объекта (2)

7.1.8. Управление архетипом

7.1.8.1. Создание архетипа

Для создания архетипа выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Archetypes -> New archetype** (1, рисунок 171). В открывшемся окне на вкладке **Basic** (2, рисунок 171) обязательно заполните поле **Name** (3, рисунок 171), остальные – по желанию. Сохраните изменения, нажав на **Save** (4, рисунок 171).

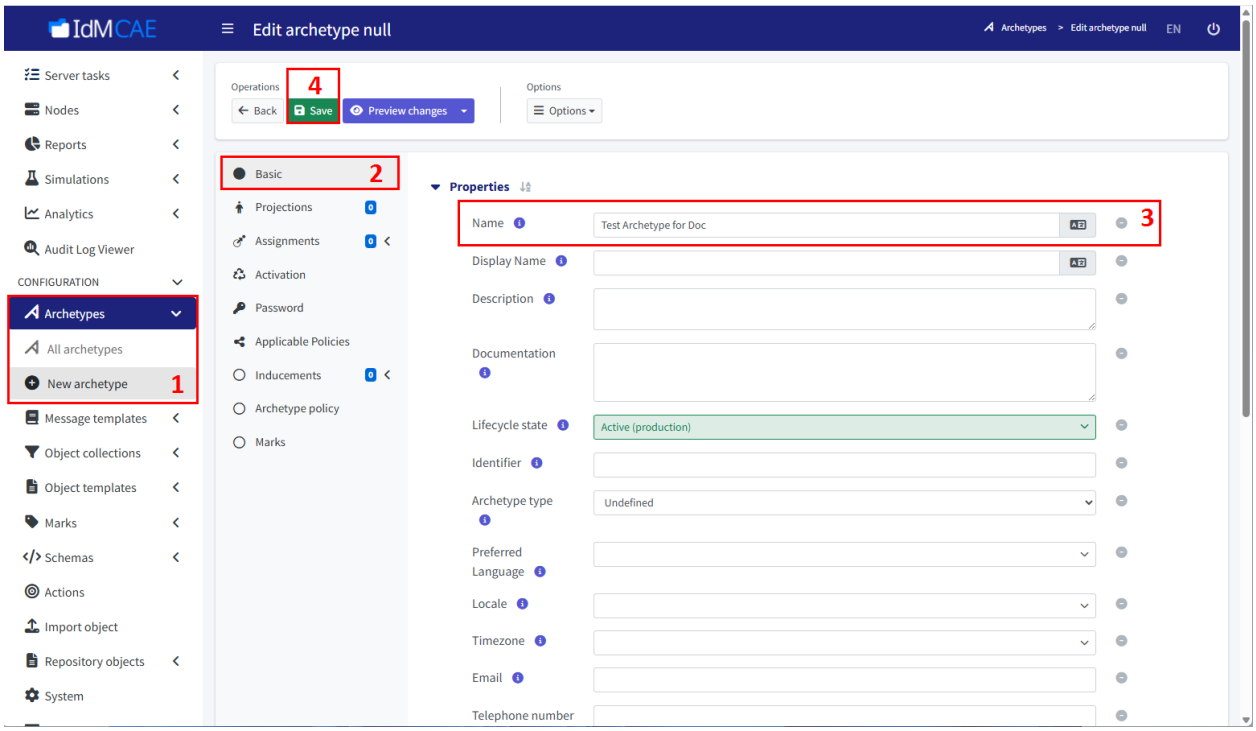


Рисунок 171 – Создание архетипа

7.1.8.2. Изменение архетипа

IDM CAE позволяет настраивать архетипы в зависимости от потребности. В данном разделе приведён пример изменения архетипа пользователя. В результате пользователям с данным архетипом будет предоставляться доступ к выбранному ресурсу.

Для изменения архетипа выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Слева в меню выберите **Archetypes -> All archetypes** (1, рисунок 172) в разделе **CONFIGURATION**. Выберите нужный архетип (2, рисунок 172).

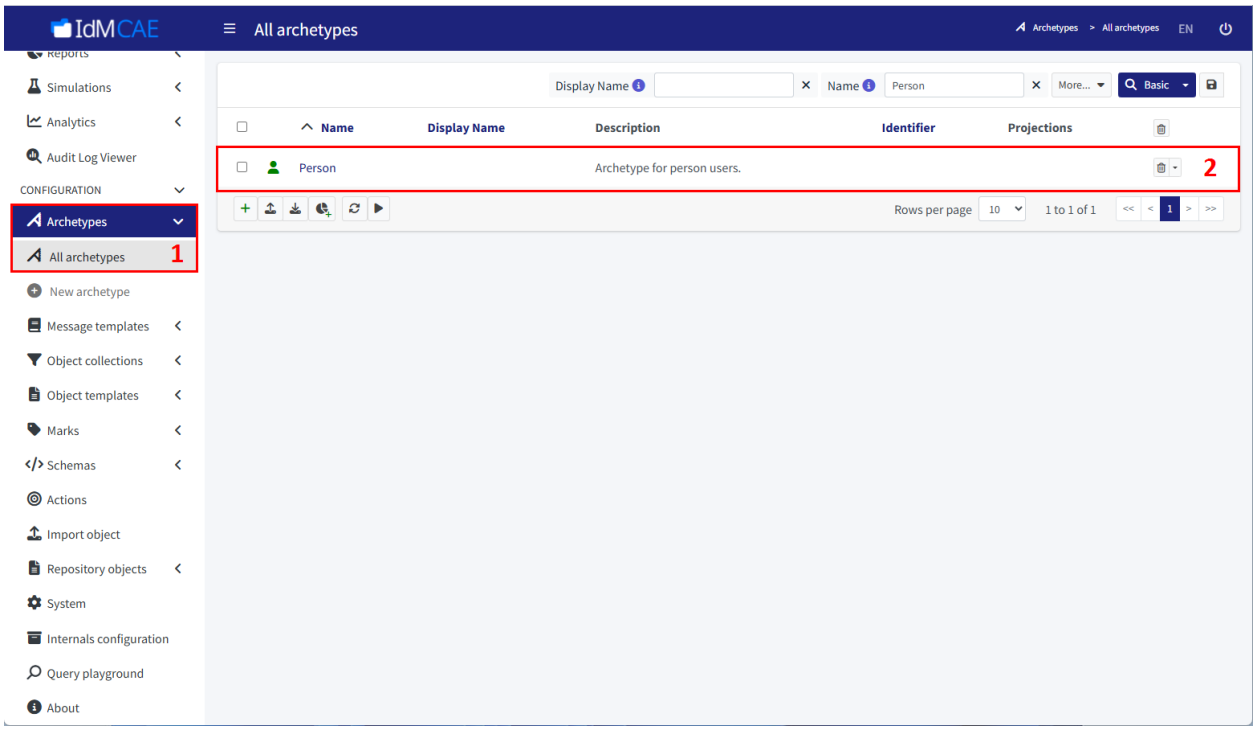


Рисунок 172 – Переход к архетипу

3. Перейдите на вкладку **Inducements -> All** (1, рисунок 173)

и нажмите на  (2, рисунок 173).

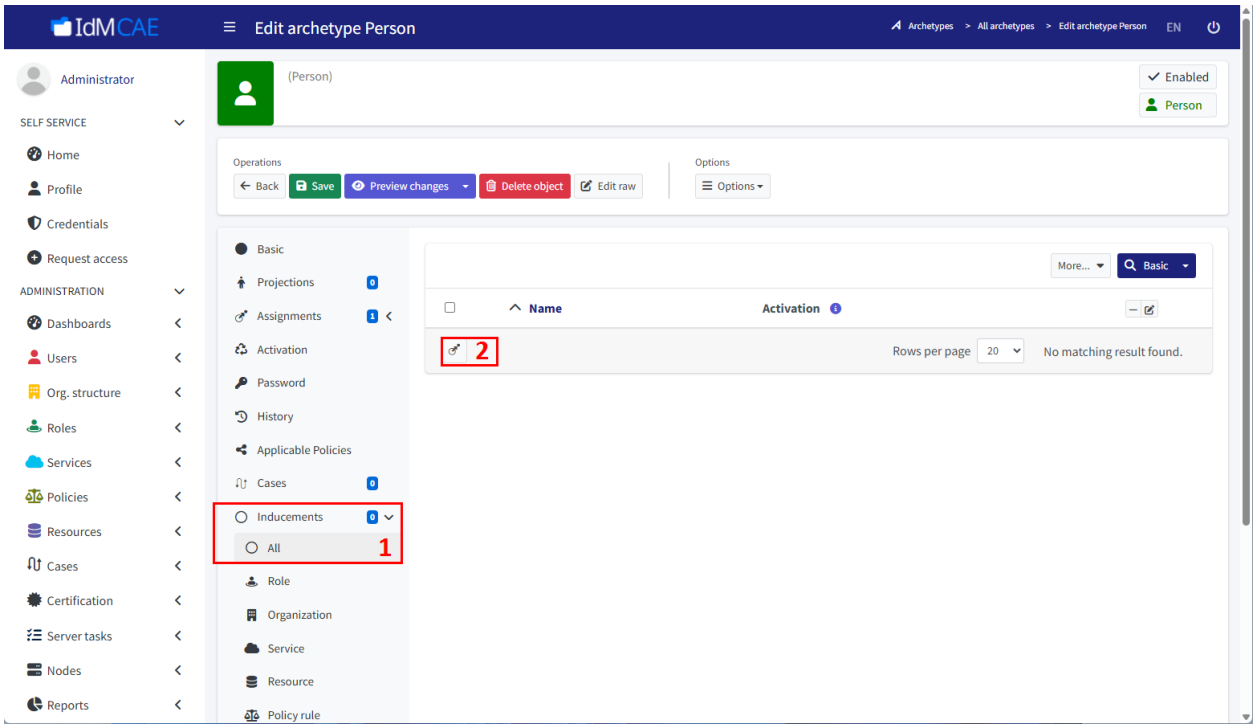


Рисунок 173 – Переход к изменению архетипа

4. Выберите вкладку с нужным классом объектов (1, рисунок 174) и отметьте флагами назначаемые объекты (2, рисунок 174). Измените значения полей в блоке **Parameters** (3, рисунок 174). Нажмите на **Add** (4, рисунок 174).

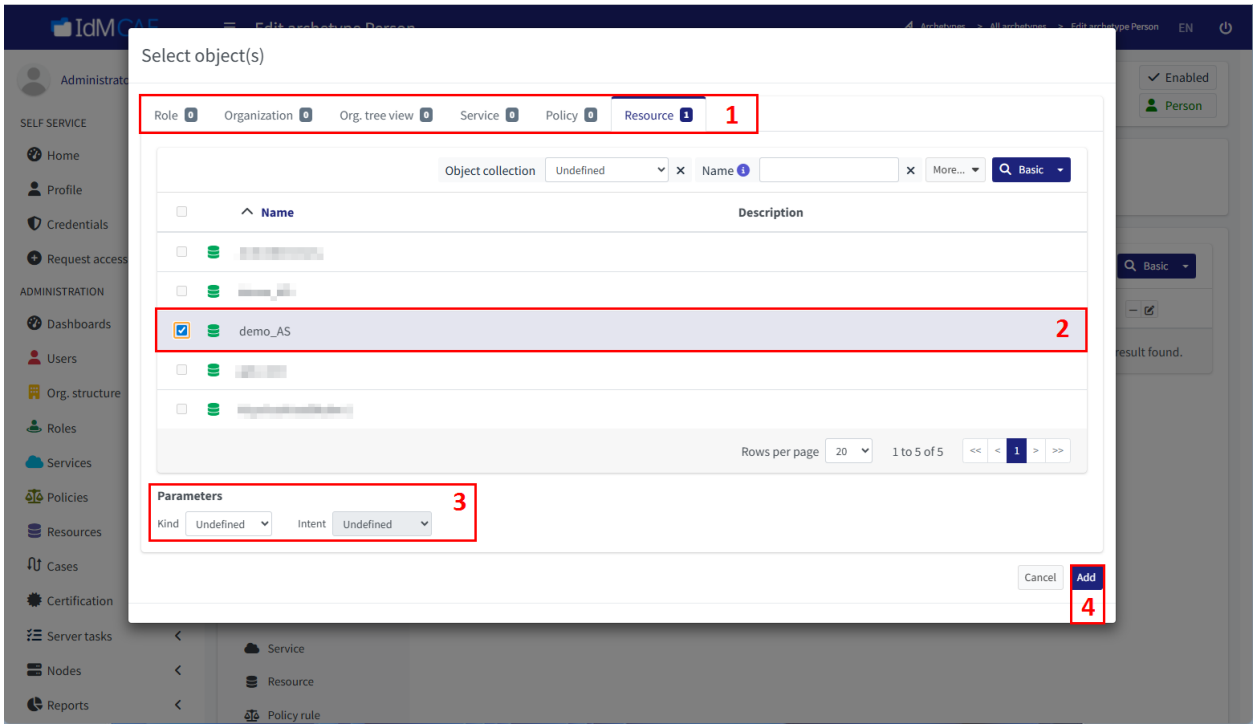


Рисунок 174 – Изменение архетипа

5. В результате в окне отобразится список добавленных объектов. Сохраните изменения, нажав на **Save** (рисунок 175). В результате для новых пользователей будет предоставлен доступ к выбранному ресурсу.

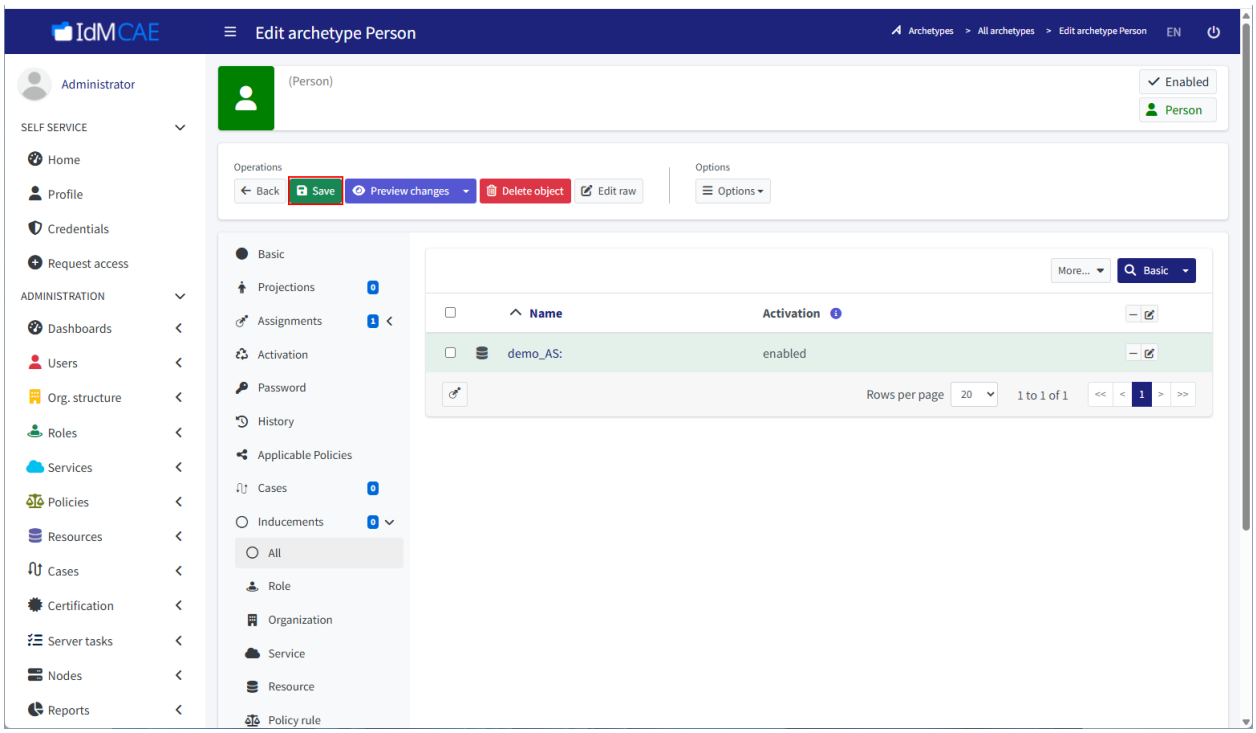


Рисунок 175 – Сохранение изменений

6. Для применения изменений к уже существующим пользователям выберите **Options** (1, рисунок 176) и в выпадающем списке установите флаг напротив **Reconcile** (2, рисунок 176). Ещё раз нажмите на **Save** (3, рисунок 176).

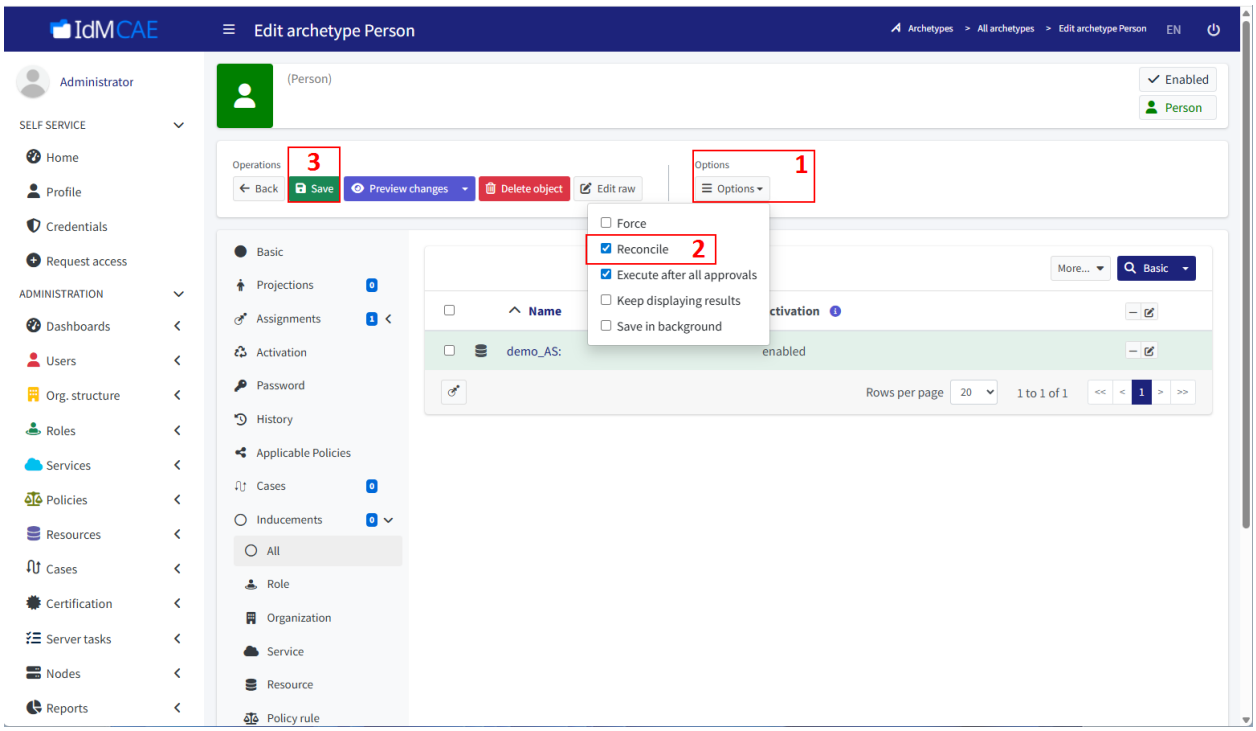


Рисунок 176 – Выполнение реконсиляции

7.1.9. Настройка параметров синхронизации

В данном разделе рассматривается базовый пример настроек параметров синхронизации с ресурсом.

Для настройки параметров синхронизации выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Перейдите к настройке параметров синхронизации удобным способом.
3. С помощью **Add reaction** (1, рисунок 177) укажите следующие параметры синхронизации (2, рисунок 177):

- 1 (может указываться только при настройке синхронизации с HR-ресурсом):
    - Name: 1;

    - Situation: Unmatched;
    - Action: Add focus;
    - Lifecycle state: Active;
- 2 (может указываться при настройке синхронизации с любым ресурсом):
    - Name: 2;
    - Situation: Linked;
    - Action: Synchronize;
    - Lifecycle state: Active;
- 3 (может указываться при настройке синхронизации с любым ресурсом):
    - Name: 3;
    - Situation: Unlinked;
    - Action: Link;
    - Lifecycle state: Active;
- другие параметры в зависимости от требований.

Сохраните настройки, нажав на **Save synchronization settings** (3, рисунок 177).

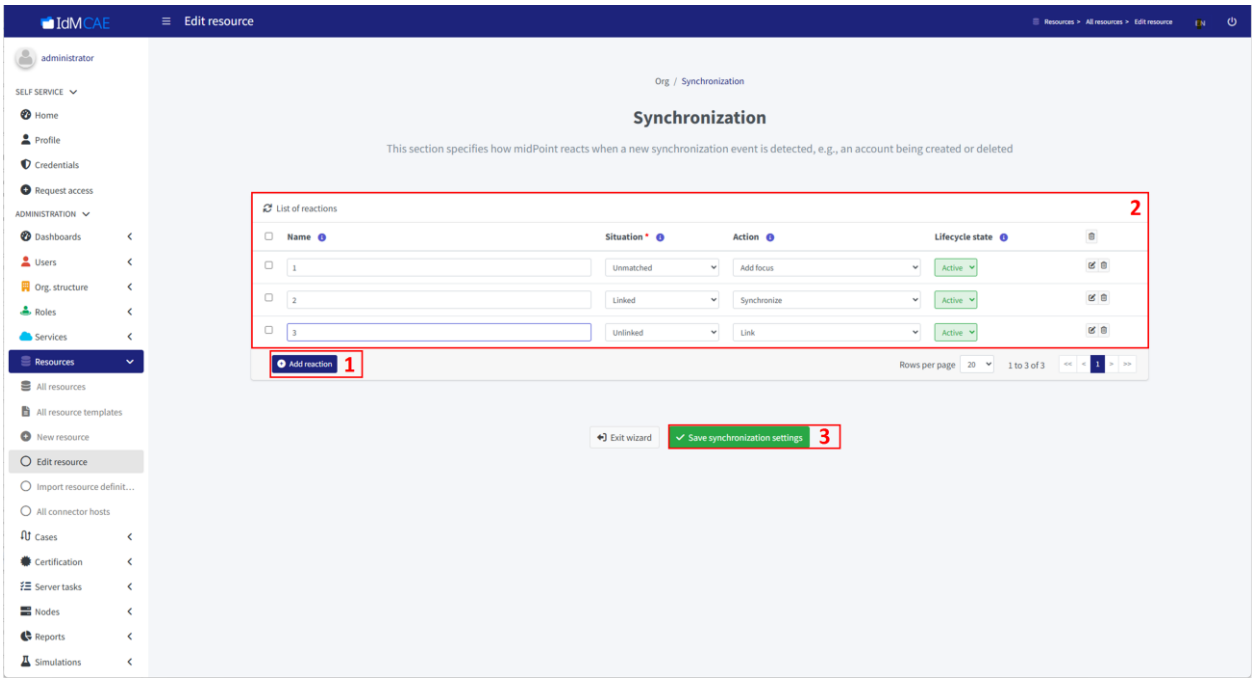


Рисунок 177 – Настройка синхронизации

7.1.10. Управление коннекторами

7.1.10.1. Загрузка коннектора

Для загрузки коннектора выполните следующие шаги:

1. Двоичный файл коннектора (.JAR-файл) скопируйте в каталоги **icf-connectors** и **connid-connectors** в домашнем каталоге IDM CAE.
2. После добавления двоичного файла коннектора в каталоги, коннектор автоматически отобразится в веб-интерфейсе.

   Если добавленный коннектор ранее был установлен и при обновлении не была изменена его версия, выполните перезапуск IDM CAE. IDM CAE автоматически обнаружит загруженный файл и создаст объекты конфигурации коннектора.

7.1.10.2. Установка / обновление коннектора

В данном разделе рассматривается пример обновления коннектора для AD с версии 3.9.1 на версию 3.10.0, а также загрузка коннектора, описанная более лаконично в разделе 7.1.10.1.

Для установки / обновление коннектора выполните следующие шаги:

1. Перейдите в папку, содержащую JAR-файл коннектора.
2. Установите переменную окружения MIDPOINT_HOME, указывающую путь до корневой папки `midpoint` на удалённых серверах.

```
export MIDPOINT_HOME=/opt/midpoint
```

3. Передайте по SSH JAR-файл коннектора на каждую из нод с Provisioning Management версии 4.9.4 и выше в директорию `${MIDPOINT_HOME}/var/connid-connectors`.

```
scp ./connector-ldap-3.10.0.jar root@<ip_address>:${MIDPOINT_HOME}/var/connid-connectors
```

4. Дождитесь загрузки коннектора.
5. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
6. Слева в меню выберите **Resources -> All resources** (1, рисунок 178). Выберите нужный ресурс в общем списке (2, рисунок 178).

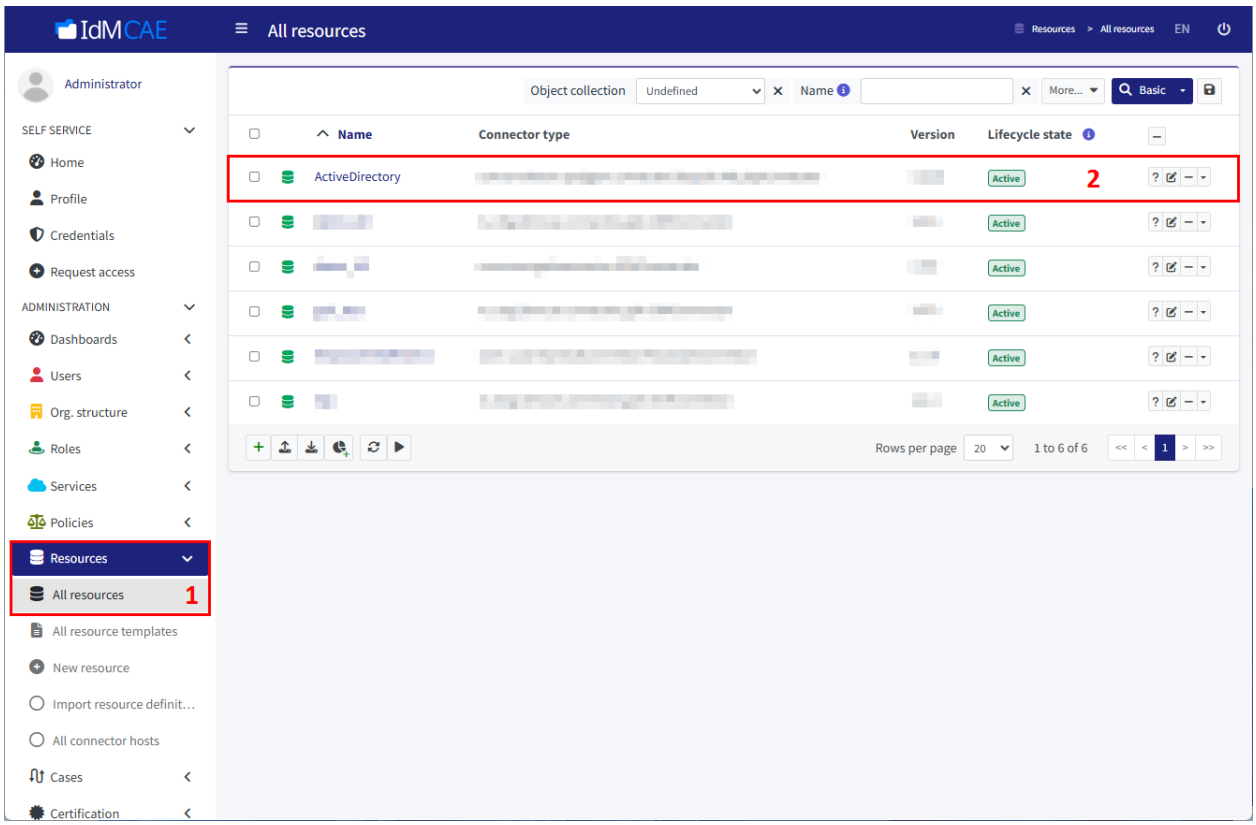


Рисунок 178 – Список ресурсов

7. Перейдите на вкладку **Basic** (1, рисунок 179). Измените коннектор, выбрав нужный в списке, который отобразится после нажатия на **Edit** справа от атрибута **connectorRef** (2, рисунок 179).

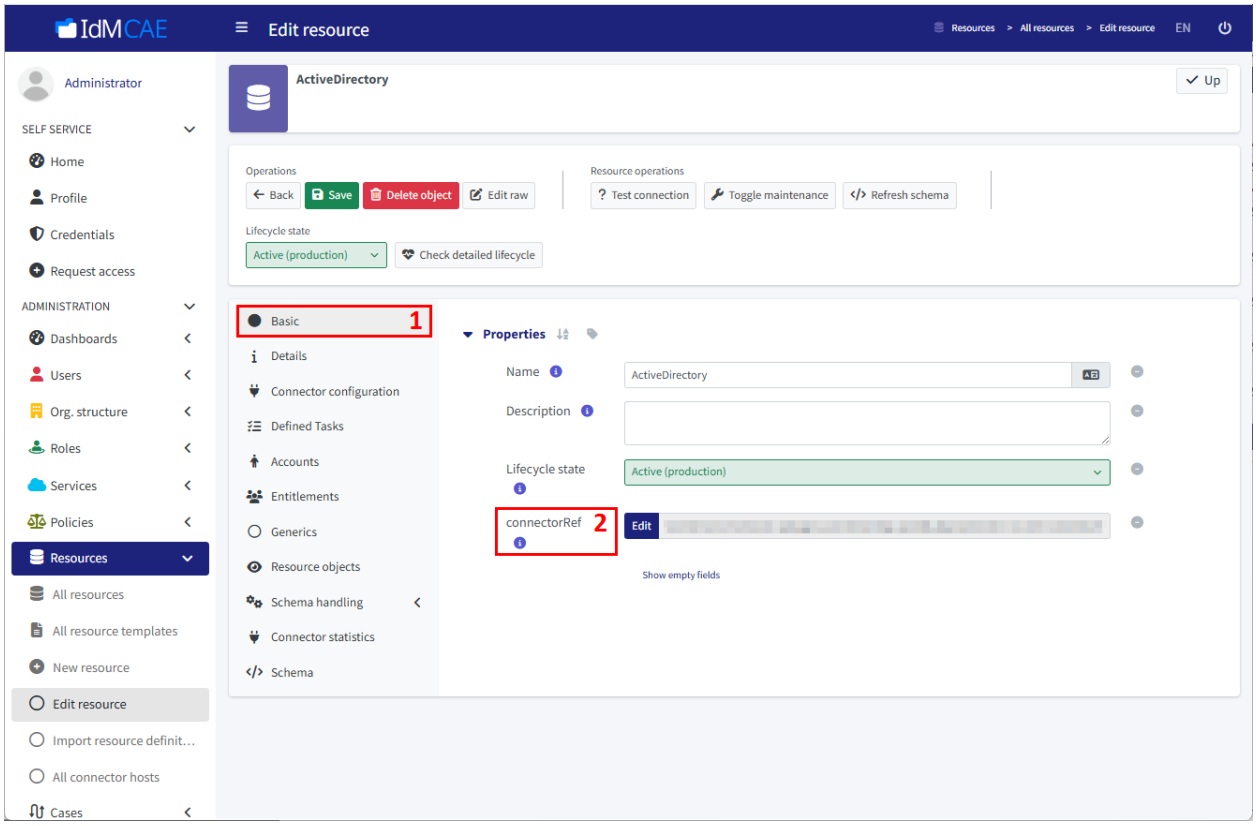


Рисунок 179 – Выбор коннектора

8. Перейдите в режим редактирования ресурса с помощью **Edit raw** (рисунок 180).

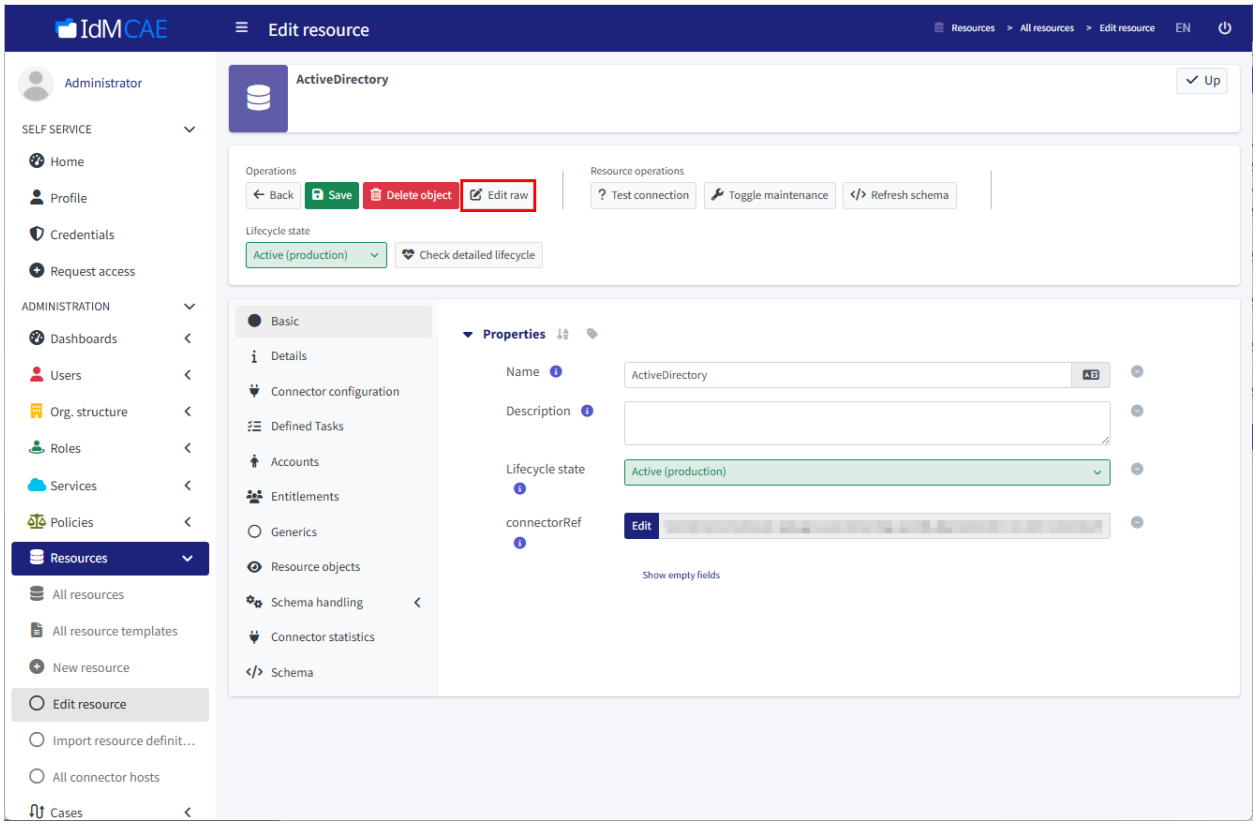


Рисунок 180 – Переход к редактированию ресурса

9. Найдите секцию **lastLogon** (1, рисунок 181) в определении схемы ресурса. Скопируйте данную секцию, вставьте её следующей, заменив при этом **lastLogon** на **lastLogonTimestamp** (2, рисунок 181). Сохраните изменения, нажав на **Save** (3, рисунок 181).

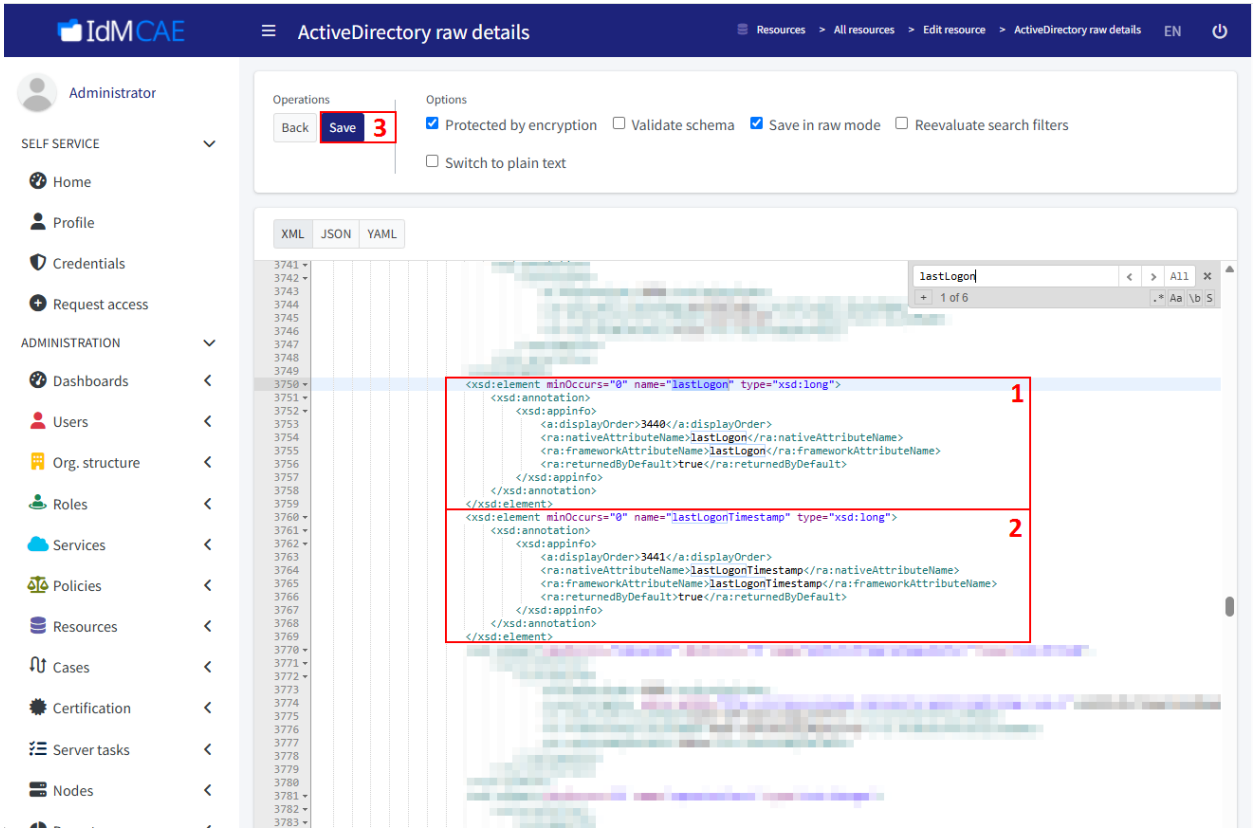


Рисунок 181 – Обновлённая схема ресурса

10. Нажмите на **Refresh schema** (рисунок 182).

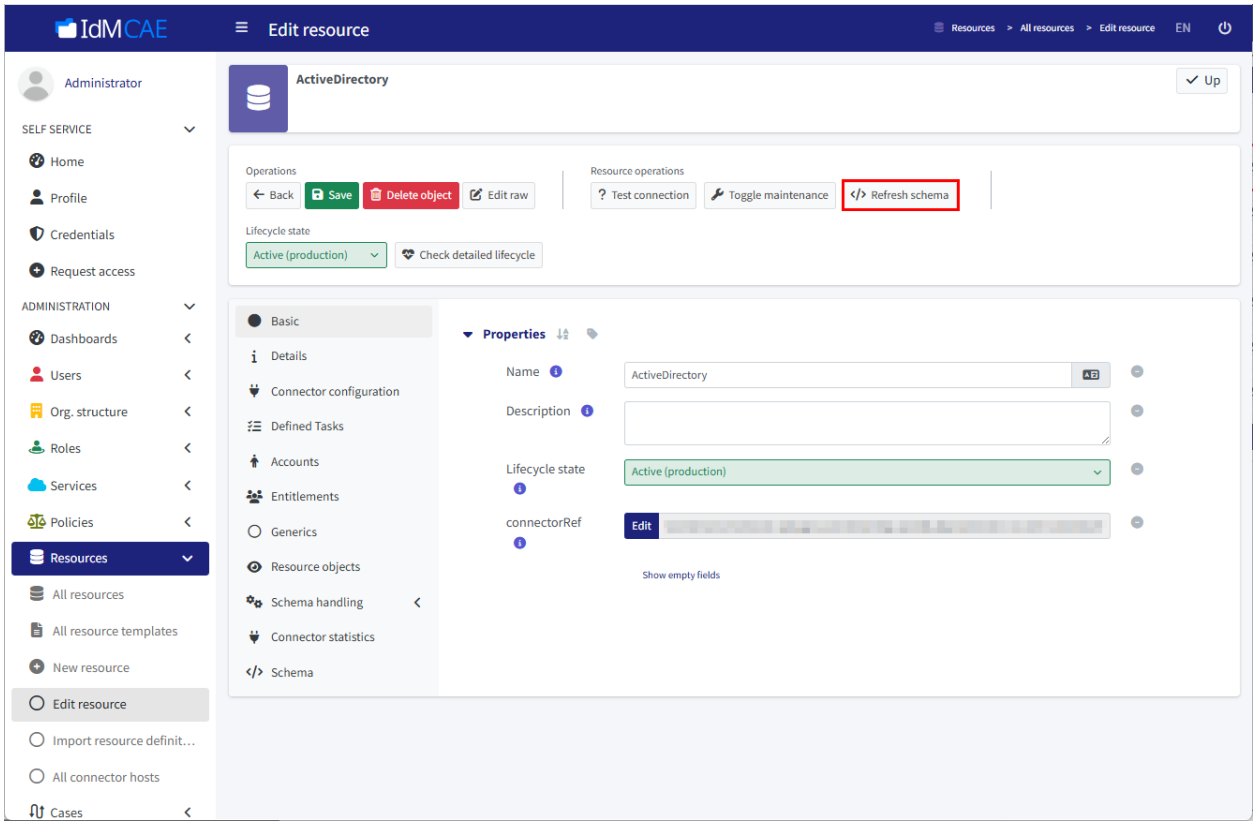


Рисунок 182 – Обновление схемы ресурса

11. (Опционально) перейдите на вкладку **Accounts** (1, рисунок 183). Нажмите на **Reload** (2, рисунок 183). Данный шаг необязателен, так как при повторном импорте тени или при повторном её открытии в браузере будет выполнено обновление атрибутов.

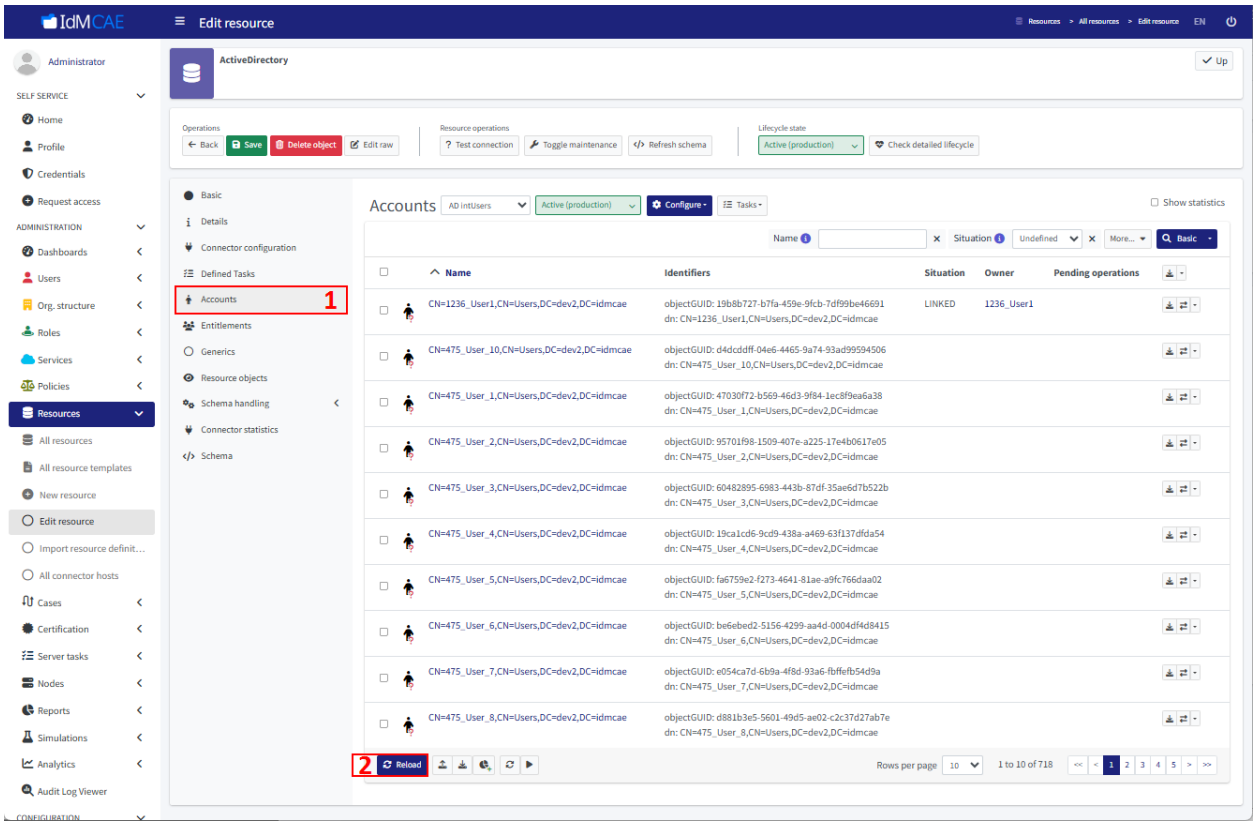


Рисунок 183 – Перезагрузка УЗ ресурса

12. В результате в атрибутах УЗ будет отображён атрибут **lastLogonTimestamp** (рисунок 184).

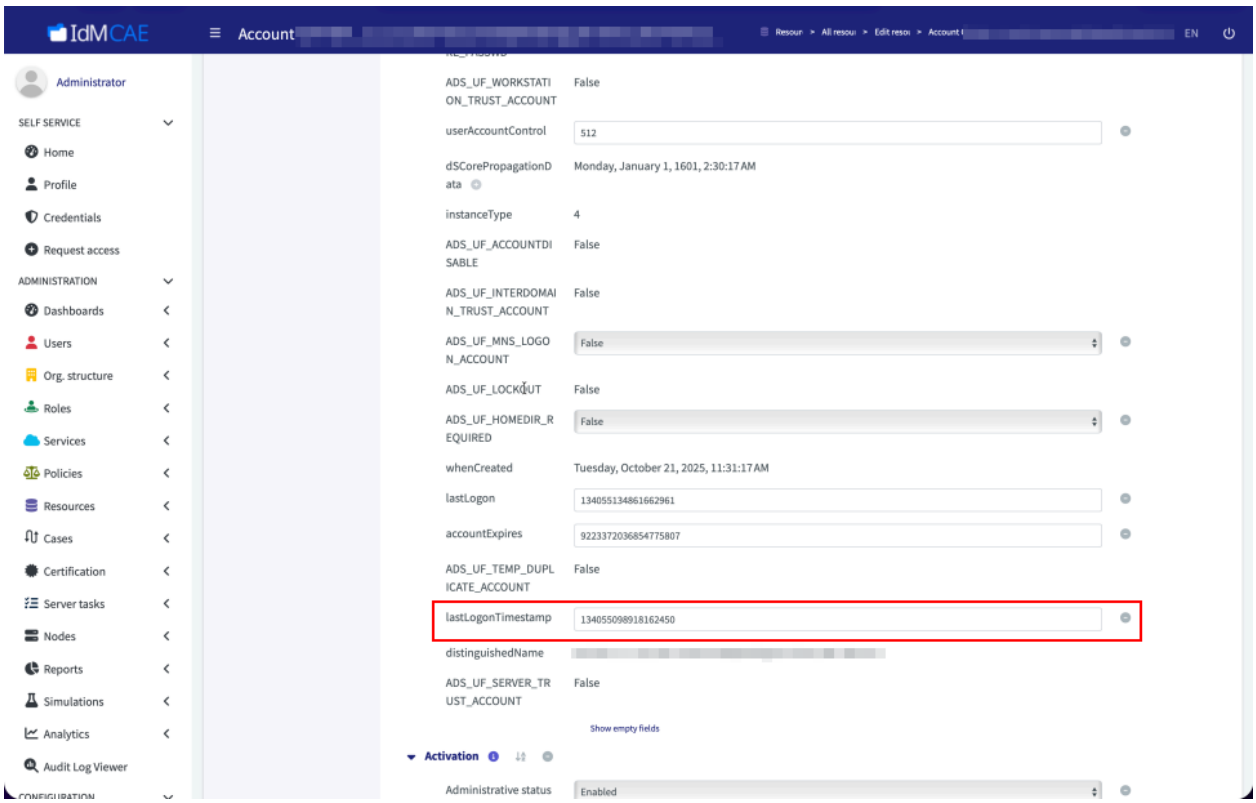


Рисунок 184 – Обновлённые атрибуты УЗ

7.1.10.3. Настройка коннектора

Для работы с ресурсом коннектору необходима настройка. Эта настройка обычно состоит из параметров соединения, таких как:

- имя хоста;
- порт;
- имя администратора;
- пароль;
- настройки безопасности соединения и т. д.

Свойства коннектора указываются в объекте определения ресурса. В упрощенном виде это выглядит так, как представлено на рисунке 185.

```
<resource oid="690f9f44-8027-11e6-a248-3b5fe08dea36">
    <name>My LDAP Server</name>
    <connectorRef oid="028159cc-f976-457f-be70-9e9fa079bcf7"/>
    <connectorConfiguration>
        <configurationProperties>
            <port>389</port>
            <host>localhost</host>
            <baseContext>dc=example,dc=com</baseContext>
            ...
        </configurationProperties>
    </connectorConfiguration>
    ...
</resource>
```

Рисунок 185 – Объект определения ресурса

Набор свойств может быть индивидуальным для каждого коннектора. Для работы с коннекторами в IDM CAE существует мастер создания ресурсов, который берёт определение свойств из схемы коннектора и формирует на её основе конфигурацию.

7.1.11. Управление уведомлениями

В IDM CAE можно настроить отправку почтовых уведомлений об изменениях УЗ пользователей, объектов, исполнении задач и т. д. Виды уведомлений представлены в таблице 7.

Таблица 7 – Виды уведомлений

№	Уведомитель	Тип	Описание
1.	simpleUserNotifier	Уведомление пользователя	Формирует уведомления о записях пользователей.
2.	simpleResourceObjectNotifier	Уведомление об объекте ресурса	Генерирует уведомления об объектах ресурсов (например, УЗ)
3.	userPasswordNotifier	Уведомление пользователя	Генерирует уведомления о паролях пользователей
4.	accountPasswordNotifier	Уведомление об УЗ	Генерирует уведомления о паролях УЗ
5.	simpleWorkflowNotifier	Уведомление о рабочем процессе	Генерирует уведомления о начале/завершении рабочих

№	Уведомитель	Тип	Описание
			элементов (т.е. пользовательских задач) и о запуске/завершении экземпляров рабочих процессов
6.	simpleCampaignNotifier, simpleCampaignStageNotifier	Уведомление о сертификации	Генерирует уведомления о кампаниях по сертификации
7.	simpleTaskNotifier	Уведомление о задаче	Генерирует уведомления о задачах
8.	generalNotifier	Общее уведомление	Это уведомитель общего назначения, управляемый выражениями, преобразующими событие в уведомление.

Для создания уведомлений отредактируйте объект **SystemConfiguration** (подробнее см. в разделе 6.1.1) в соответствии с нижеследующим листингом:

```
<notificationConfiguration>
  <handler>
    <simpleUserNotifier>
      <recipientExpression>
        <value> e-mail_получателя </value>
      </recipientExpression>
      <transport>mail</transport>
    </simpleUserNotifier>
  </handler>
  <mail>
    <server>
      <host>*****</host>
      <port>1234</port>
......<username>INT/user</username>
......<password>*****</password>
    ..<transportSecurity>none</transportSecurity>
... </server>
```

```
    </mail>
</notificationConfiguration>
```

Обратите внимание, что после указания пароля в параметре password и сохранения изменений пароль шифруется автоматически.

7.1.12. Формирование отчёта

Компонент Provisioning Management позволяет работать с внутренними отчётами для анализа и отображения данных о ресурсах, УЗ пользователей и ролей. Можно использовать функциональность отчётов как для изучения причин возникновения сбоев, так и для регулярных мониторингов корректности выполнения запросов в IDM CAE.

Для формирования отчёта выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Provisioning Management (подробнее см. в разделе 7.1.1.4).
2. Выберите **Reports -> All reports** в разделе **ADMINISTRATION** (1, рисунок 186). Нажмите на  справа от интересующего отчёта (2, рисунок 186). В результате в всплывающем окне появится превью отчёта, ознакомьтесь с ним и запустите формирование отчёта, нажав на **Run report** (рисунок 187).

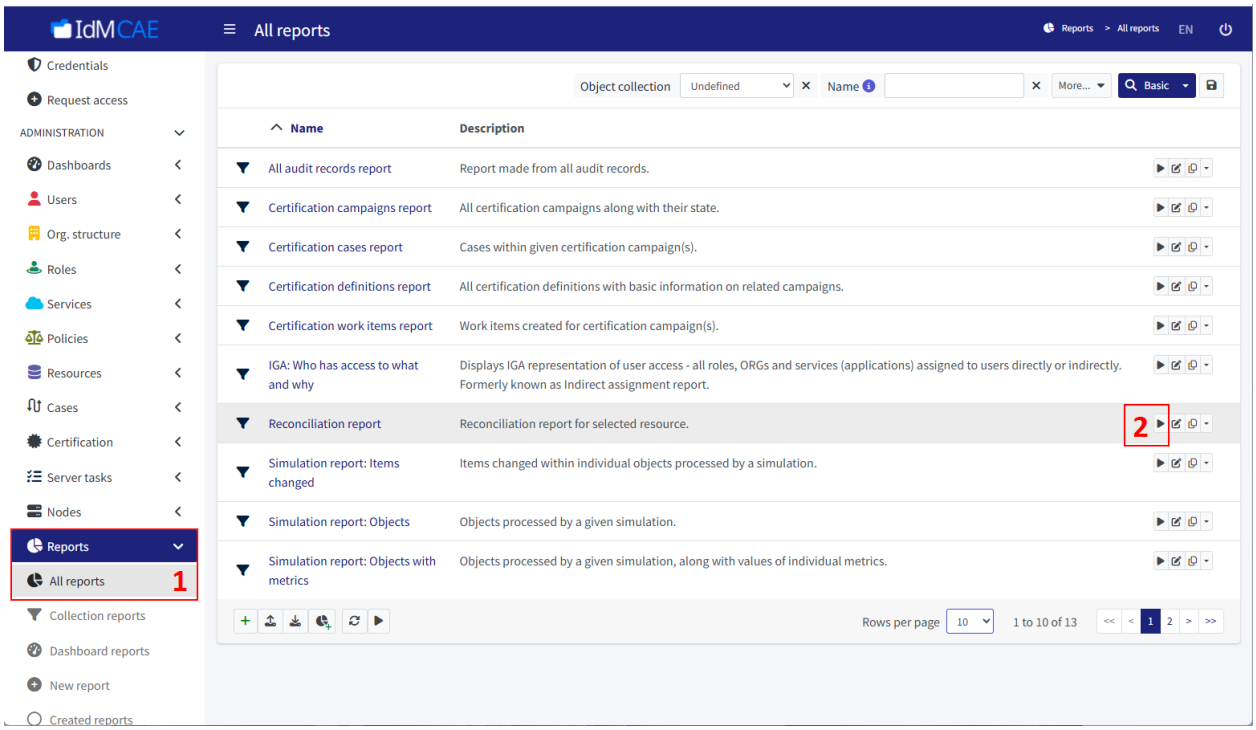


Рисунок 186 – Переход к формированию отчёта

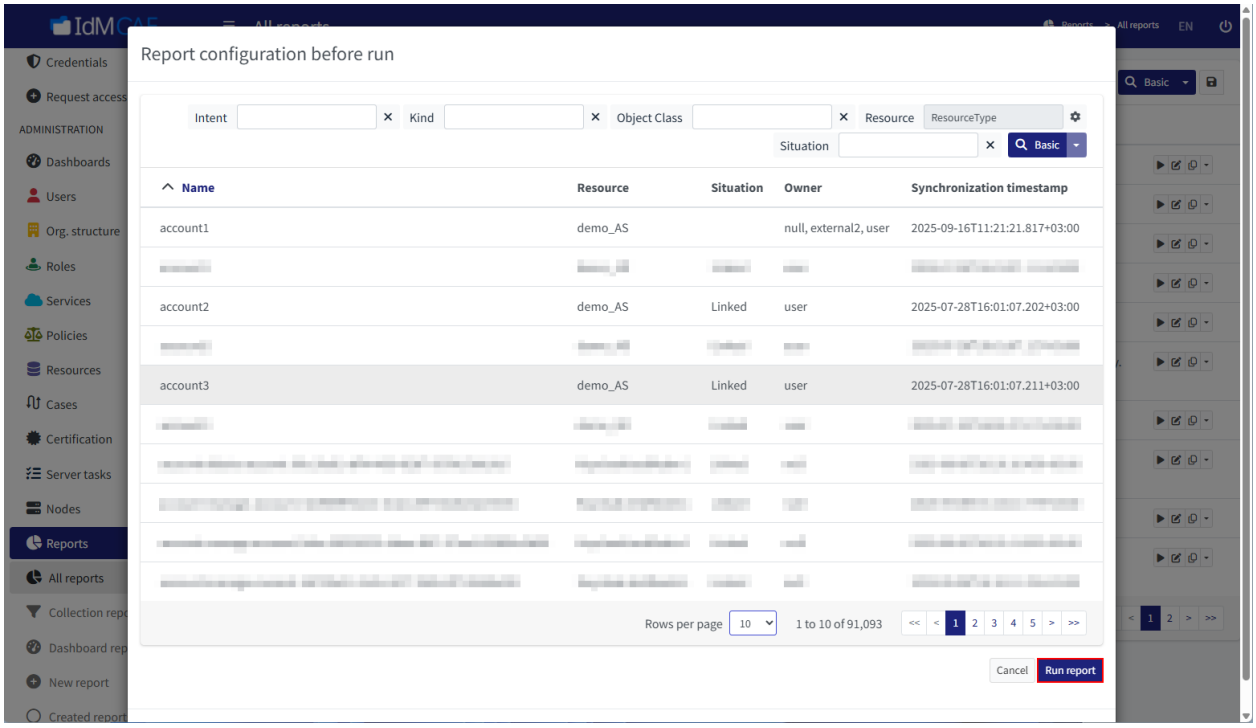


Рисунок 187 – Превью и запуск формирования отчёта

3. В результате запустится задача на формирование отчёта, посмотреть которую можно в **Server tasks -> Report tasks** в разделе **ADMINISTRATION** (рисунок 188).

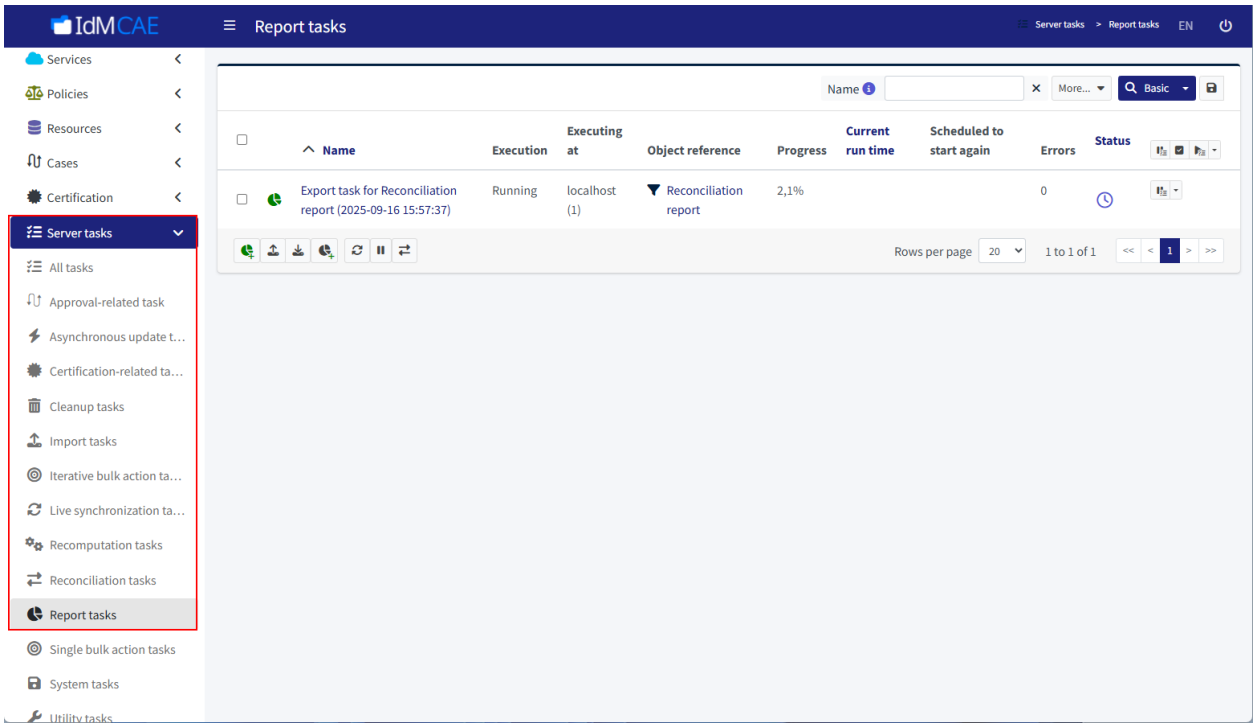


Рисунок 188 – Задача на формирование отчёта

4. Сформированный отчёт можно просмотреть, если выбрать **Reports -> Created reports** в разделе **ADMINISTRATION** (1, рисунок 189) и скачать его, нажав на  (2, рисунок 189).

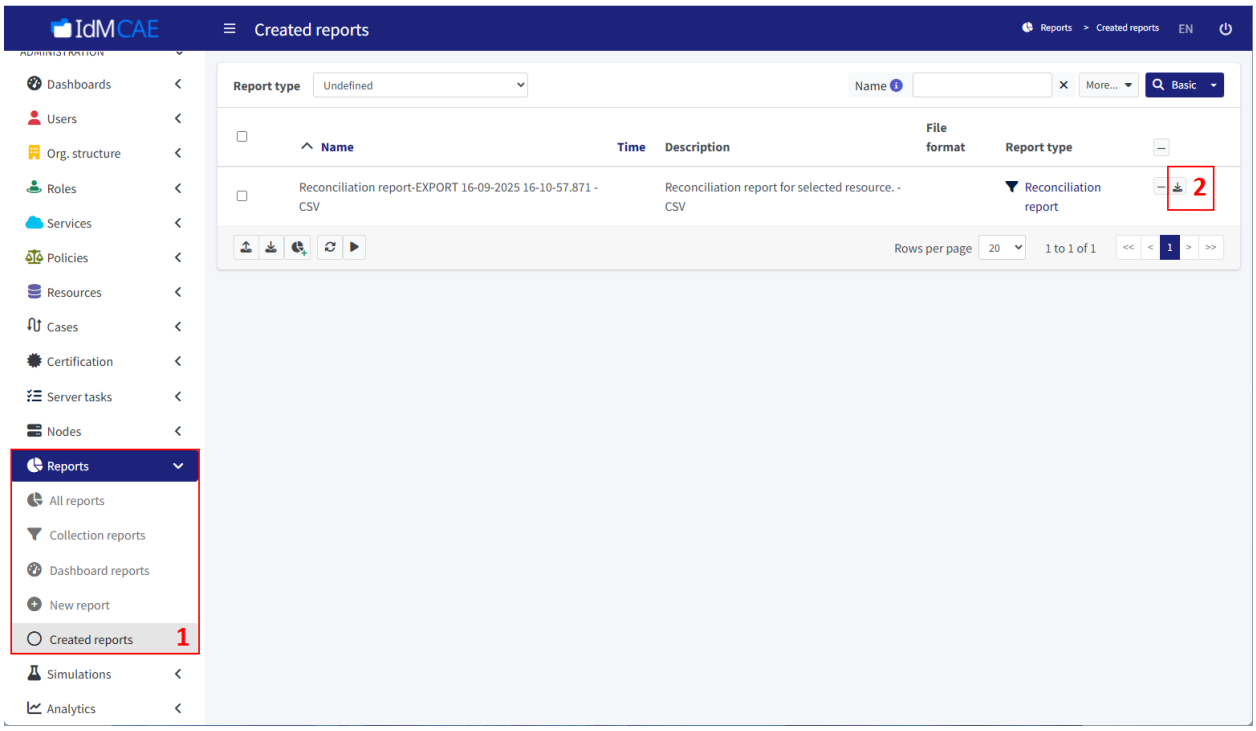


Рисунок 189 – Просмотр отчёта

7.2. Компонент Workflow Management

7.2.1. Веб-интерфейс компонента Workflow Management

7.2.1.1. Общее описание

Компонент Workflow Management состоит из трёх ключевых разделов (рисунок 190):

- Admin;
- Cockpit;
- Tasklist.

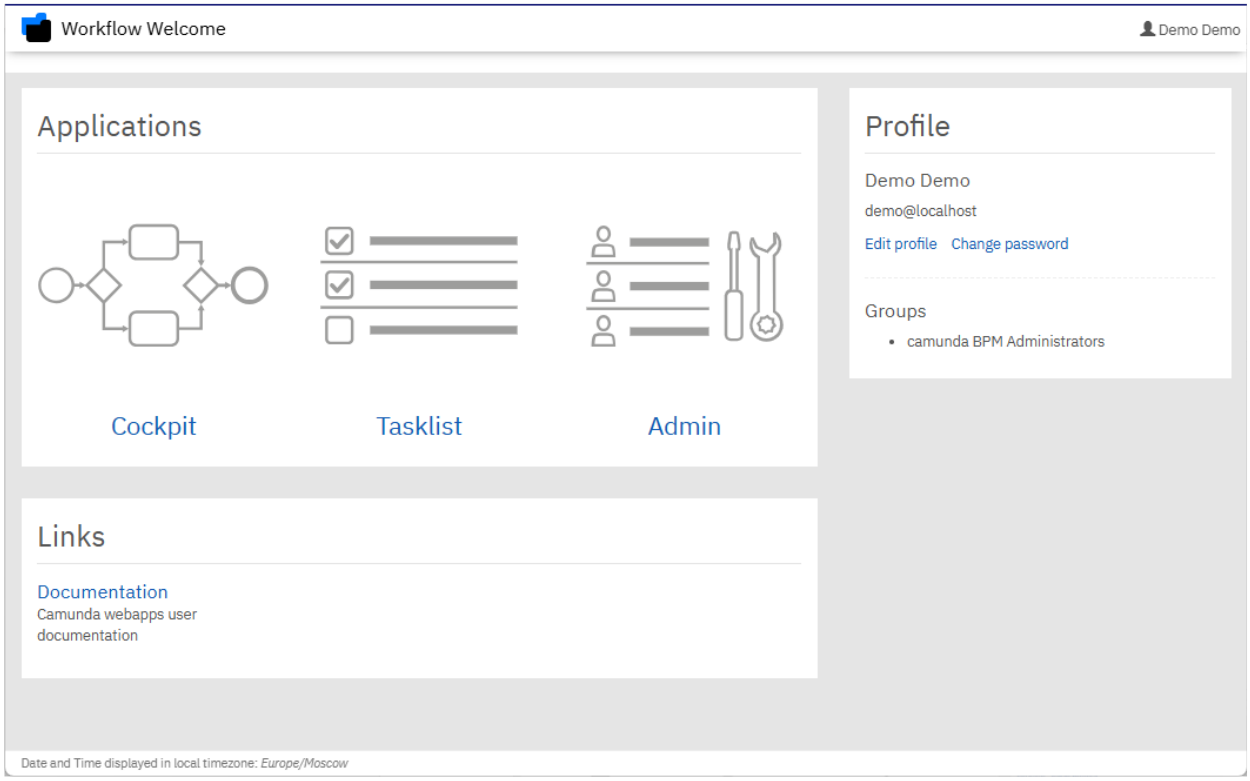


Рисунок 190 – Приветственное окно

Раздел **Admin** предназначен для управления пользователями, группами и правами доступа. Он представляет из себя инструмент администрирования, который предоставляет возможность конфигурирования. Данный раздел позволяет пользователю, в зависимости от его прав доступа, просматривать и взаимодействовать со следующими подразделами:

- **Users**: подраздел позволяет просматривать и управлять пользователями внутри компонента Workflow Management. Предоставляется возможность создания новых пользователей, изменения существующих и просмотра списка пользователей. Также существует возможность просмотра собственного профиля и изменения персональной информации;

- **Groups**: подраздел позволяет просматривать и управлять группами внутри компонента Workflow Management. Предоставляется возможность создания новых групп, изменения существующих и просмотра полного списка всех групп. Также существует возможность назначения групп для пользователей;
- **Tenants**: подраздел позволяет управлять тенантами;
- **Authorizations**: подраздел позволяет просматривать настроенные права доступа для групп и пользователей в компоненте Workflow Management, а также настраивать эти права доступа. Подробнее про содержащиеся в подразделе категории настройки прав доступа см. в Приложении 2;
- **System**: раздел предоставляет пользователю возможность просматривать системную информацию о компоненте Workflow Management, включая состояние движка компонента, ключевую информацию о подключённой БД и версии компонента, а также метрики исполнения моделей процессов.

Раздел **Cockpit** предназначен для просмотра и управления существующими моделями процессов. Данный раздел позволяет пользователю просматривать запущенные экземпляры моделей процессов, модели этих процессов, открытые инциденты, возникшие в ходе работы компонента, а также активные пользовательские

задачи. Данный раздел является инструментом администрирования, который предоставляет возможность взаимодействия с процессами в компоненте Workflow Management. Раздел Cockpit позволяет пользователю, в зависимости от его прав доступа, просматривать и взаимодействовать со следующими подразделами:

- **Processes**: подраздел позволяет пользователю просматривать полный список моделей процессов, развёрнутых в компоненте Workflow Management, а также список активных экземпляров этих моделей процессов. Пользователь может просматривать схемы этих моделей, включать и отключать исполнение этих моделей, запускать экземпляры моделей и взаимодействовать с их контекстом;
- **Human Tasks**: подраздел содержит необходимую для пользователя информацию о существующих пользовательских задачах (сколько из них назначено на пользователя/группу, общее количество активных задач).
- **Deployments**: подраздел позволяет пользователям просматривать список выполненных развёртываний моделей процессов и ресурсов, связанных с ними.

7.2.1.2. Навигация в разделах компонента Workflow Management

Навигация в разделах **Admin** и **Cockpit** идентична и заключается в выборе нужного пункта либо в верхнем меню (1, рисунок 191, 192), либо в центральном окне (2, рисунок 191, 192).

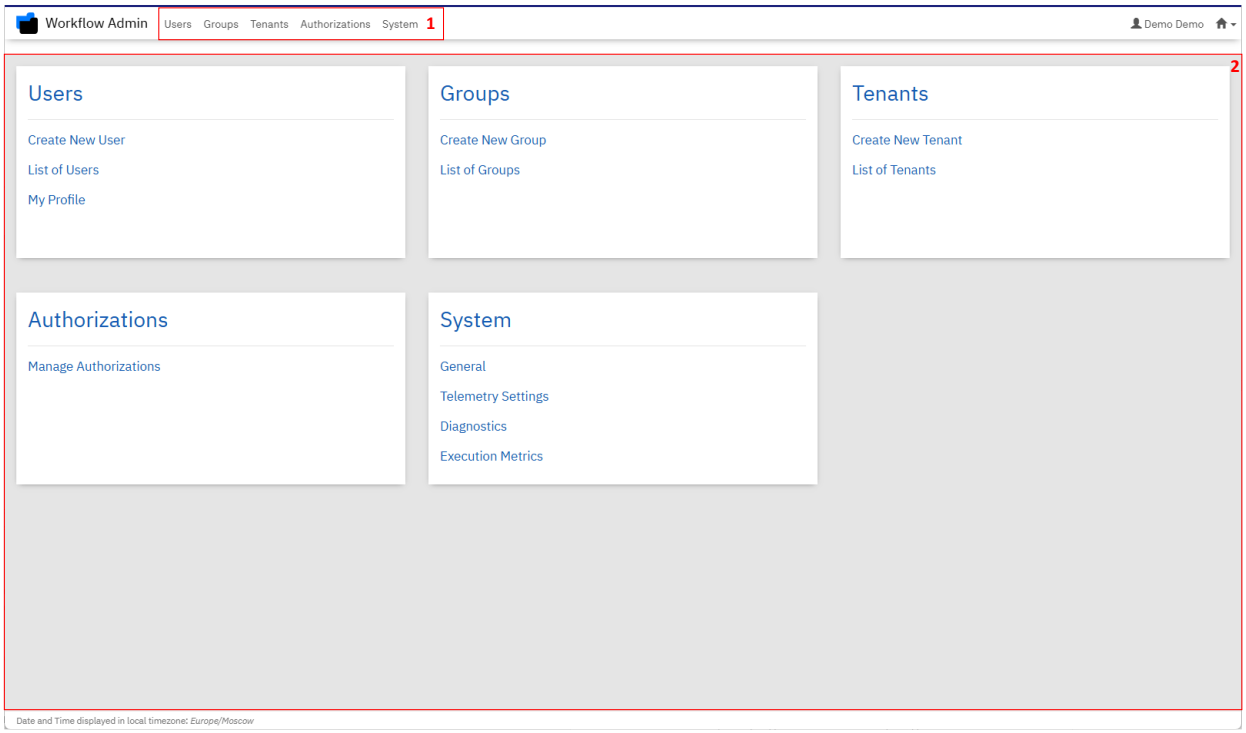


Рисунок 191 – Навигация в разделе Admin

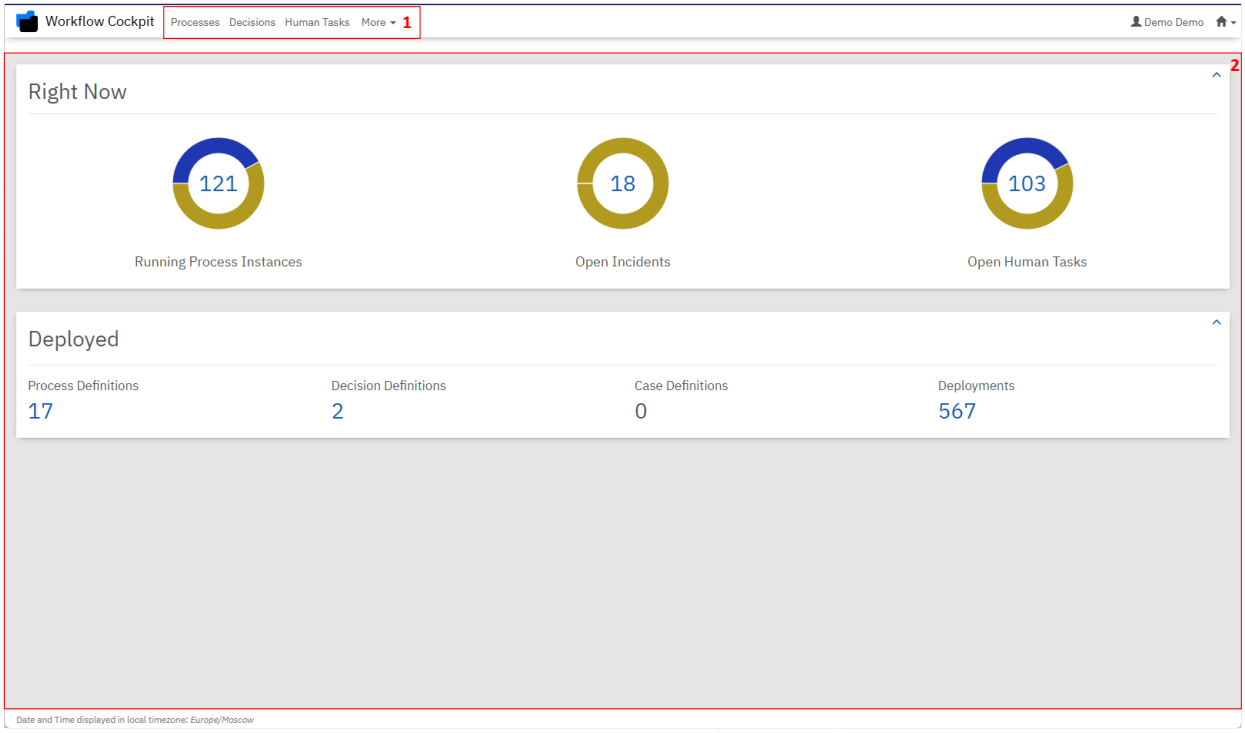


Рисунок 192 – Навигация в разделе Cockpit

7.2.1.3. Вход в веб-интерфейс компонента Workflow Management

Для входа в веб-интерфейс в компонент Workflow Management IDM CAE выполните следующие шаги:

1. В адресной строке браузера введите адрес https://<host>/workflow/app/welcome, где host – адрес сервера, на котором установлен компонент Workflow Management IDM CAE. После перехода по ссылке отобразится окно аутентификации (рисунок 193).
2. В поле **Username** (1, рисунок 193) введите имя пользователя, в поле **Password** – пароль (2, рисунок 193).
3. Нажмите на **Log in** (3, рисунок 193).
    a. В случае правильно введённых данных отобразится приветственное окно (рисунок 194).
    b. В случае неправильно введённых данных будет выведена ошибка в правом нижнем углу окна (рисунок 195). Повторите попытку входа.

Рисунок 193 – Окно аутентификации компонента Workflow Management

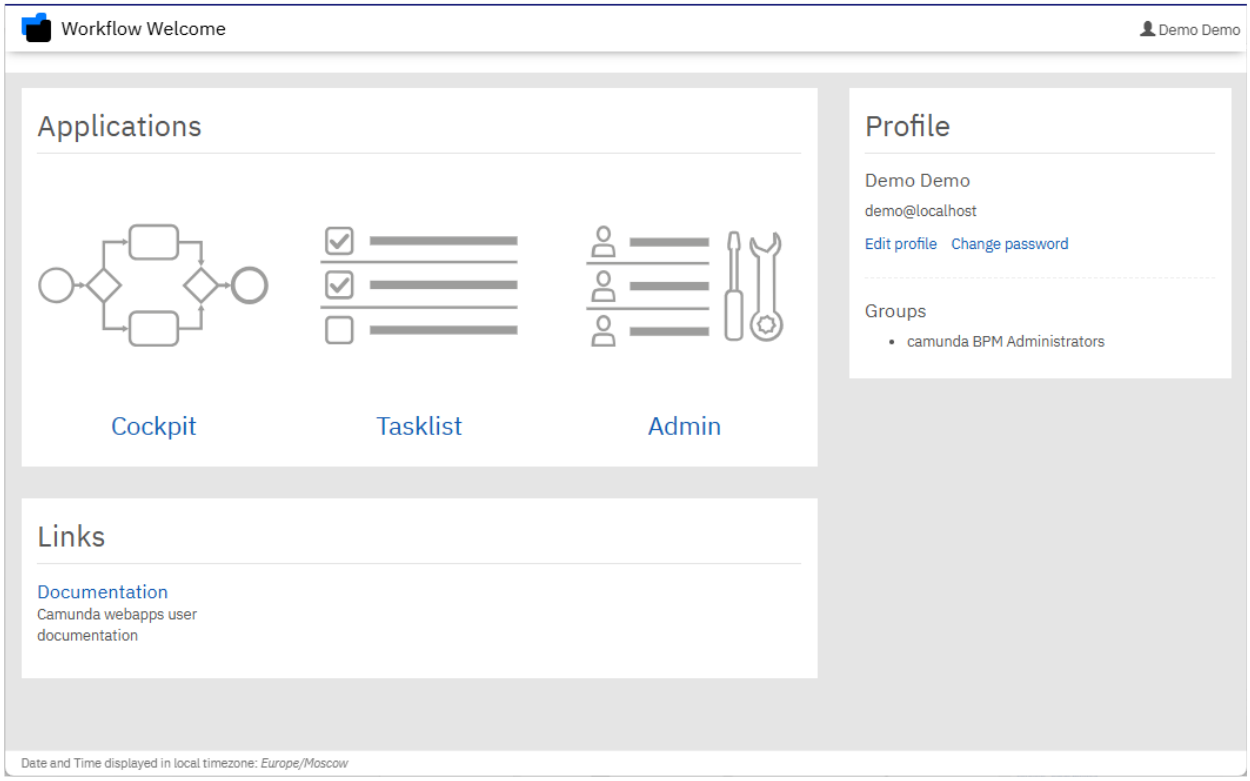


Рисунок 194 – Приветственное окно

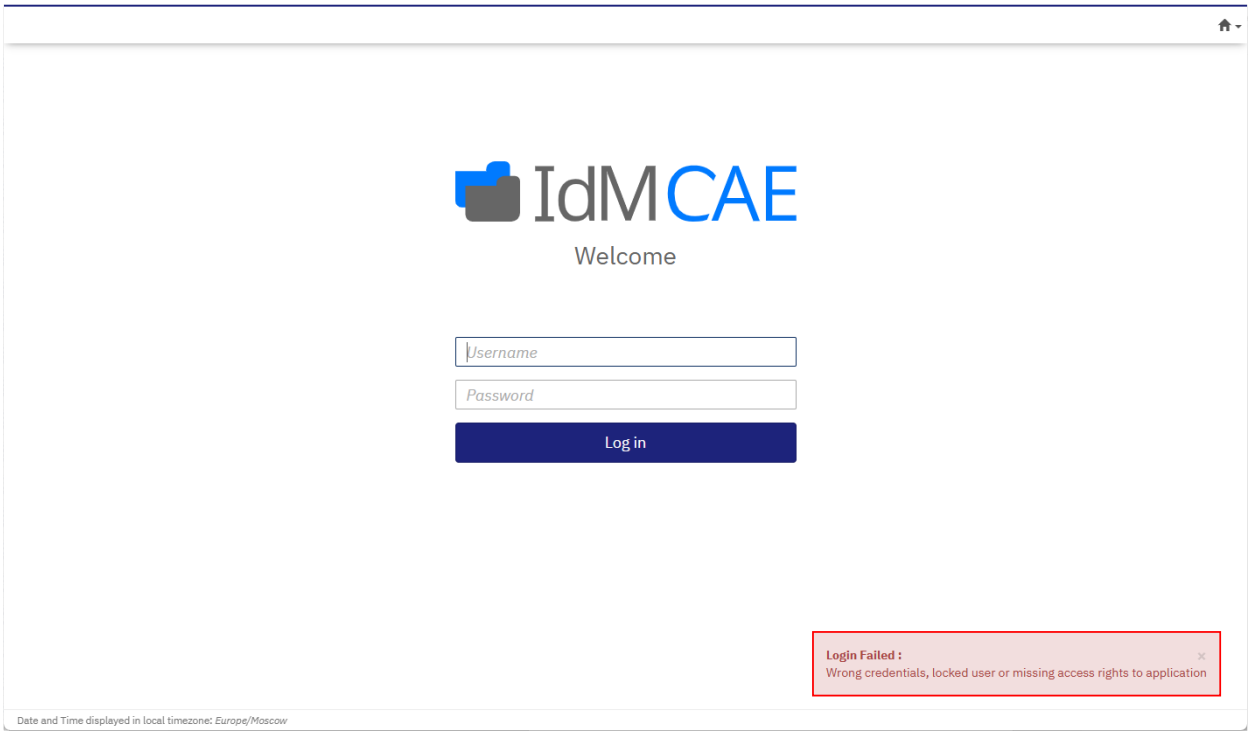


Рисунок 195 – Ошибка при попытке аутентификации

В приветственном окне можно выбрать нужный раздел (**Cockpit** / **Tasklist** / **Admin**). Также возможен вход сразу в нужный раздел из окна аутентификации, для этого перед вводом имени

пользователя и пароля в правом верхнем углу нажмите на  и в выпадающем списке выберите нужный раздел (с помощью  можно переключаться между разделами из любого окна компонента Workflow Management). Для перехода в приветственное окно из любого окна компонента Workflow Management нажмите на  в правом верхнем углу окна и выберите **My profile** (рисунок 196).

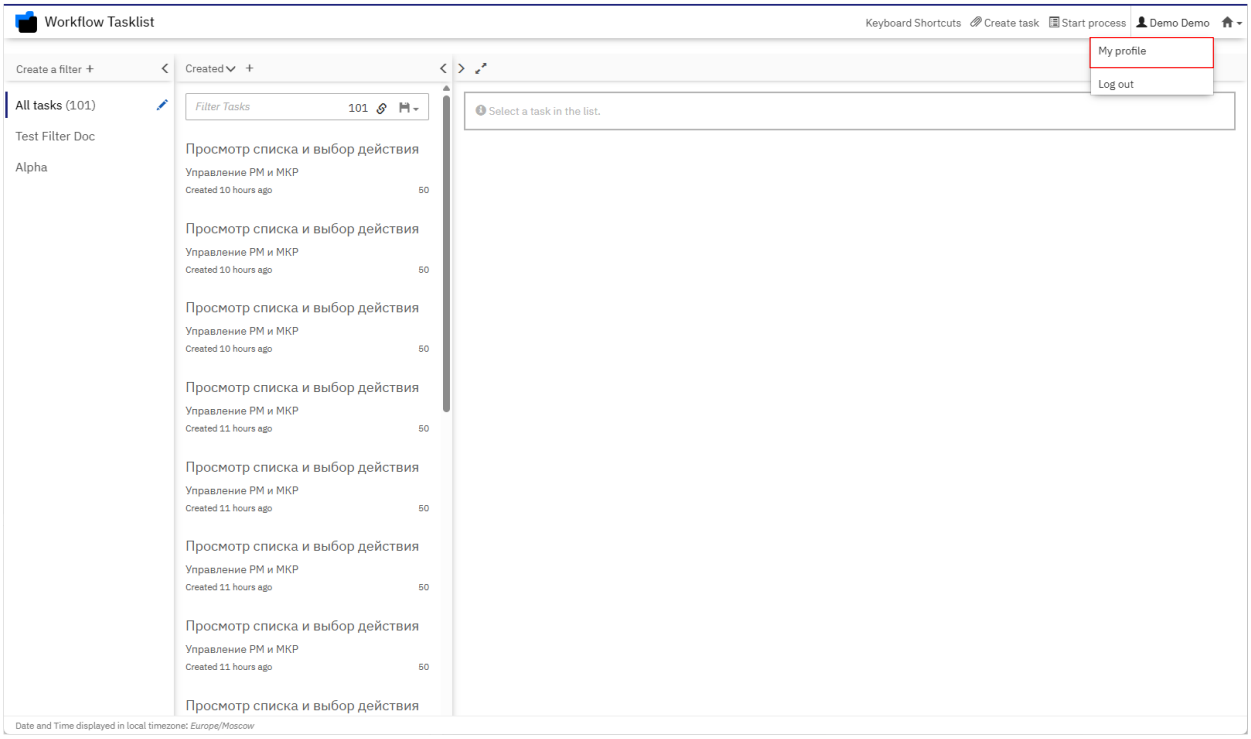


Рисунок 196 – Переход в приветственное окно

7.2.2. Управление УЗ пользователей

7.2.2.1. Создание УЗ пользователя

В компоненте Workflow Management нельзя создавать УЗ пользователей только для этого компонента, такая функциональность предусмотрена только для Camunda 7. Информация об УЗ пользователей может поступать через LDAP.

Для создания УЗ локального пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Users** (1, рисунок 197) нажмите на **Add user** (2, рисунок 197).

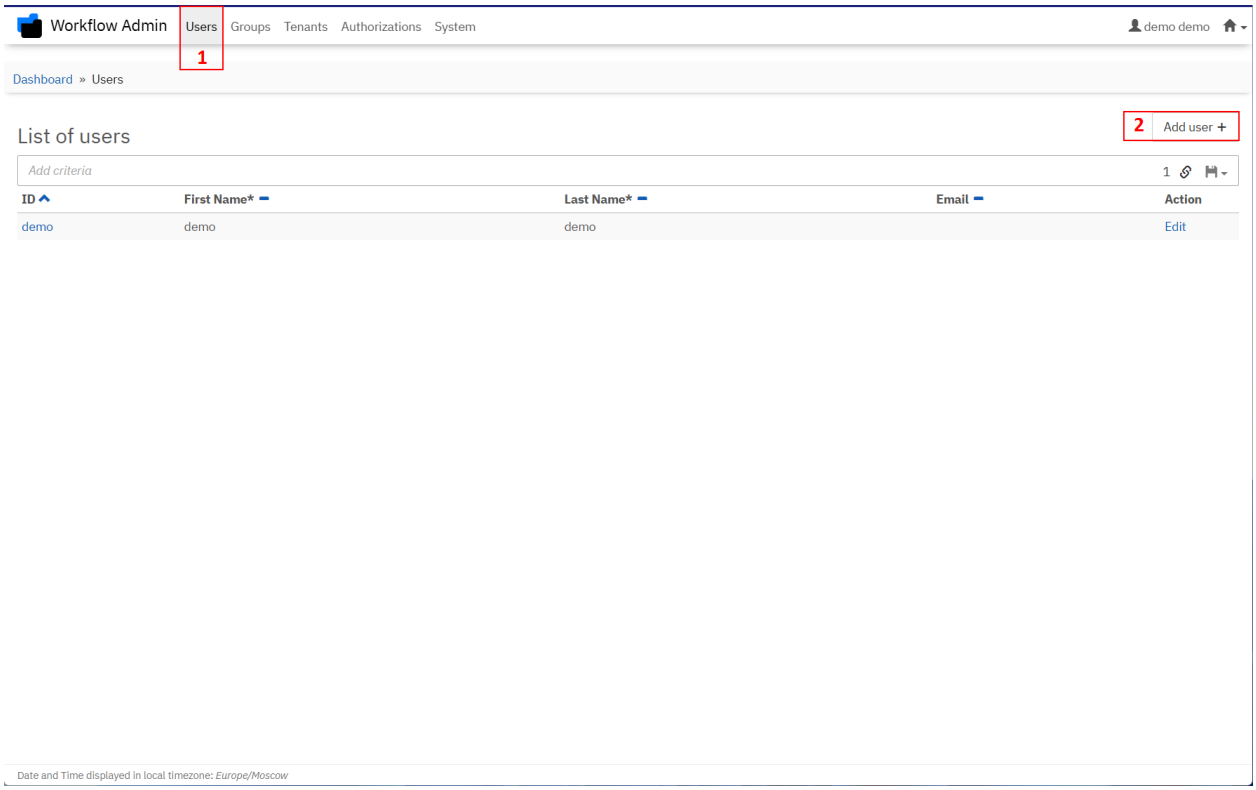


Рисунок 197 – Переход к добавлению УЗ пользователя

3. Заполните поля в разделах **User Account** и **User Profile**, обязательны к заполнению только поля, помеченные *****. Нажмите на **Create new user** (рисунок 198). Убедитесь в создании УЗ пользователя, дождавшись соответствующего сообщения в правом нижнем углу окна (рисунок 199).

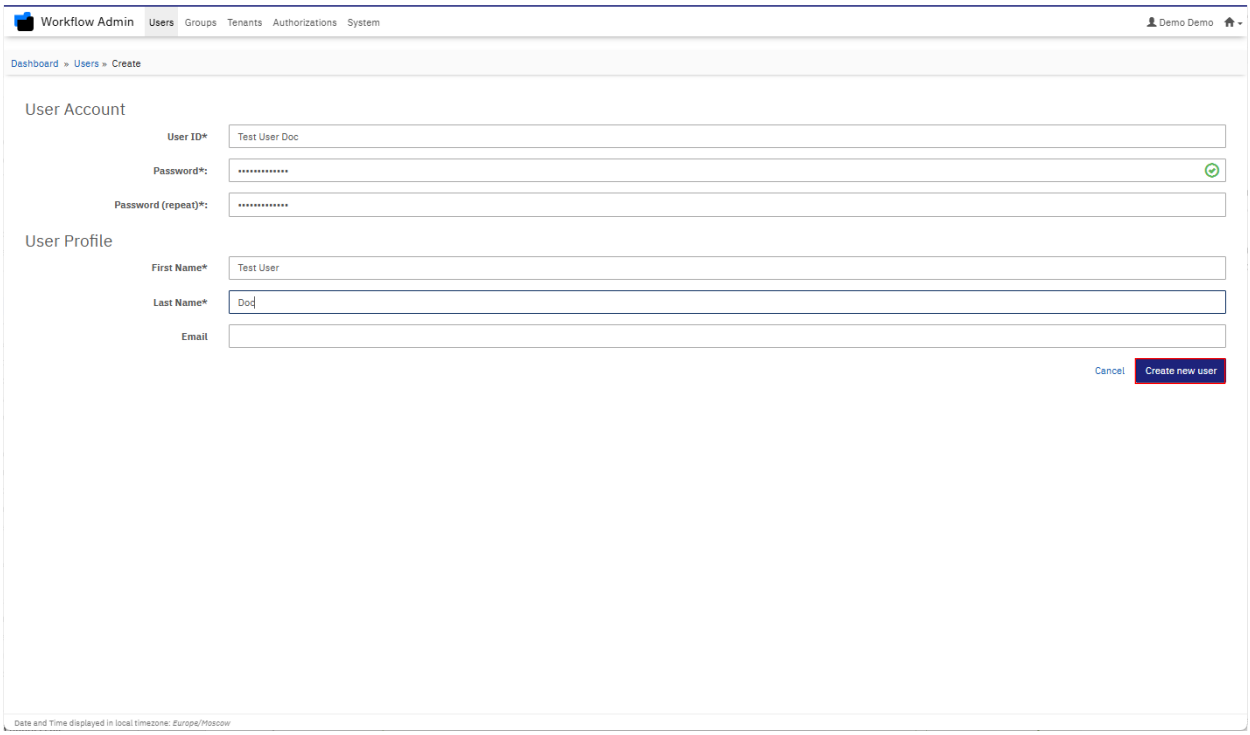


Рисунок 198 – Создание УЗ пользователя

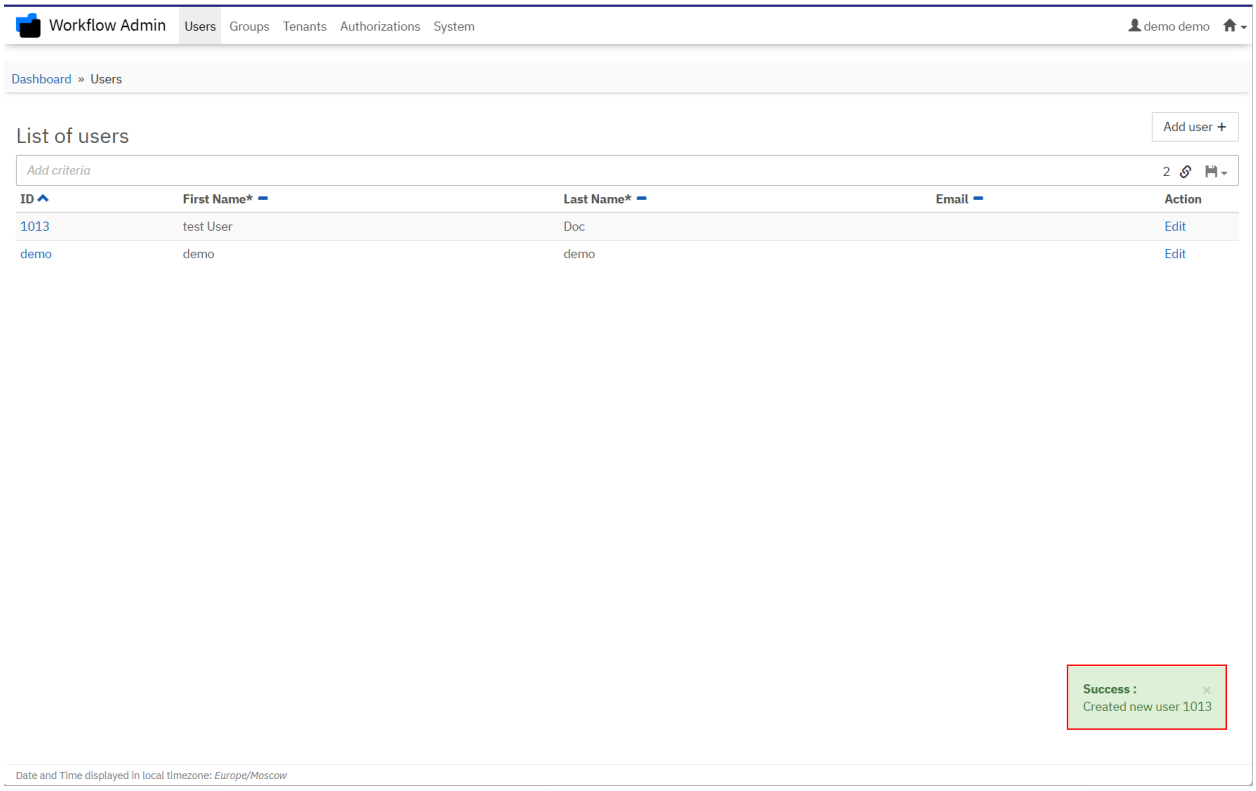


Рисунок 199 – Сообщение об успешном создании УЗ пользователя

7.2.2.2. Изменение УЗ пользователя

Под изменением УЗ пользователя компонента Workflow Management подразумевается редактирование УЗ пользователя Camunda 7.

Для редактирования УЗ пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Users** (1, рисунок 200) в общем списке выберите УЗ пользователя, нажав на его **ID** либо на **Edit** в правом столбце (2, рисунок 200).

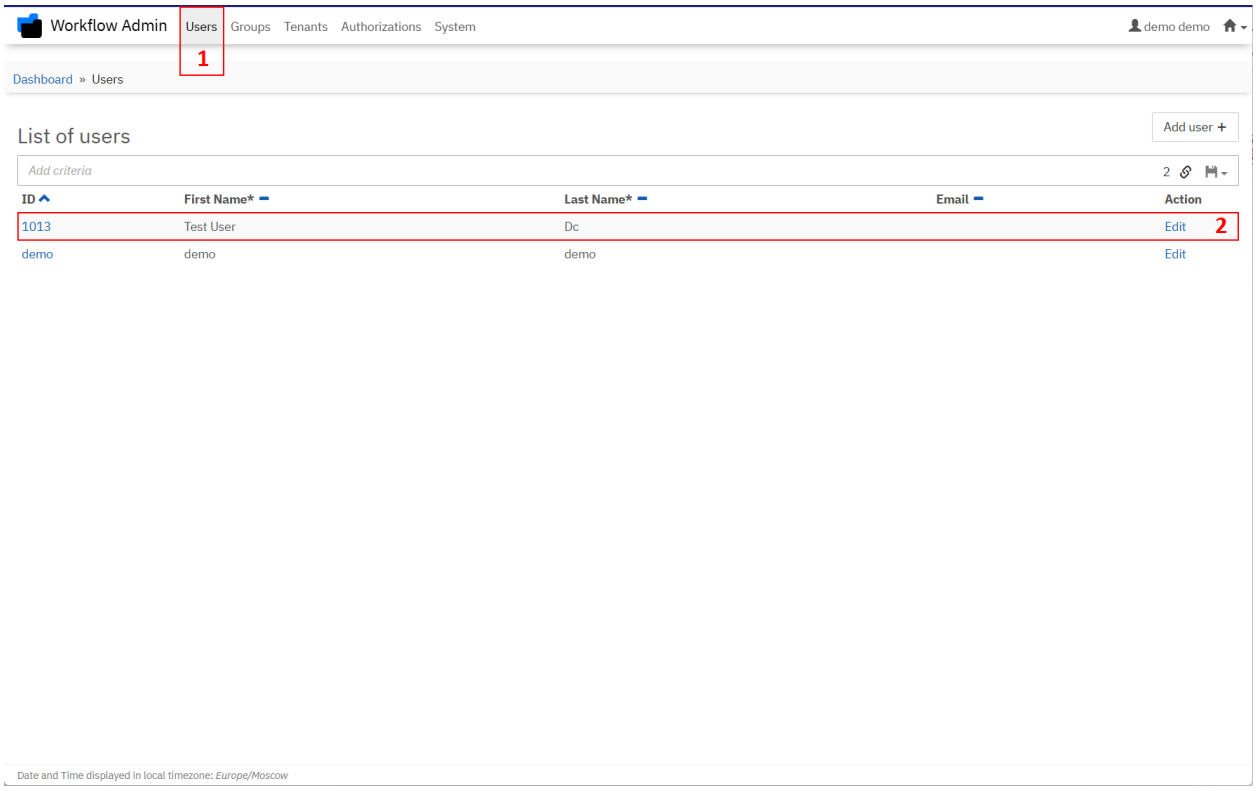


Рисунок 200 – Выбор УЗ пользователя

3. Отредактируйте поля на нужной вкладке (1, рисунок 201). Нажмите на **Update Profile** (2, рисунок 201). Убедитесь, что данные УЗ обновились, дождавшись соответствующего сообщения в правом нижнем углу окна (3, рисунок 201).

   Предусмотрено четыре вкладки для изменения:

   a. **Profile** – содержит поля с именем и адресом почтового ящика пользователя;
   b. **Account** – позволяет управлять УЗ пользователя. Содержит поля настройки аутентификации (смены пароля от УЗ), а также кнопки для удаления (**Delete User**) и разблокировки УЗ (**Unlock User**);
   c. **Groups** – позволяет управлять группами, в которые включена УЗ;
   d. **Tenants** – позволяет управлять доступом к тенантам.

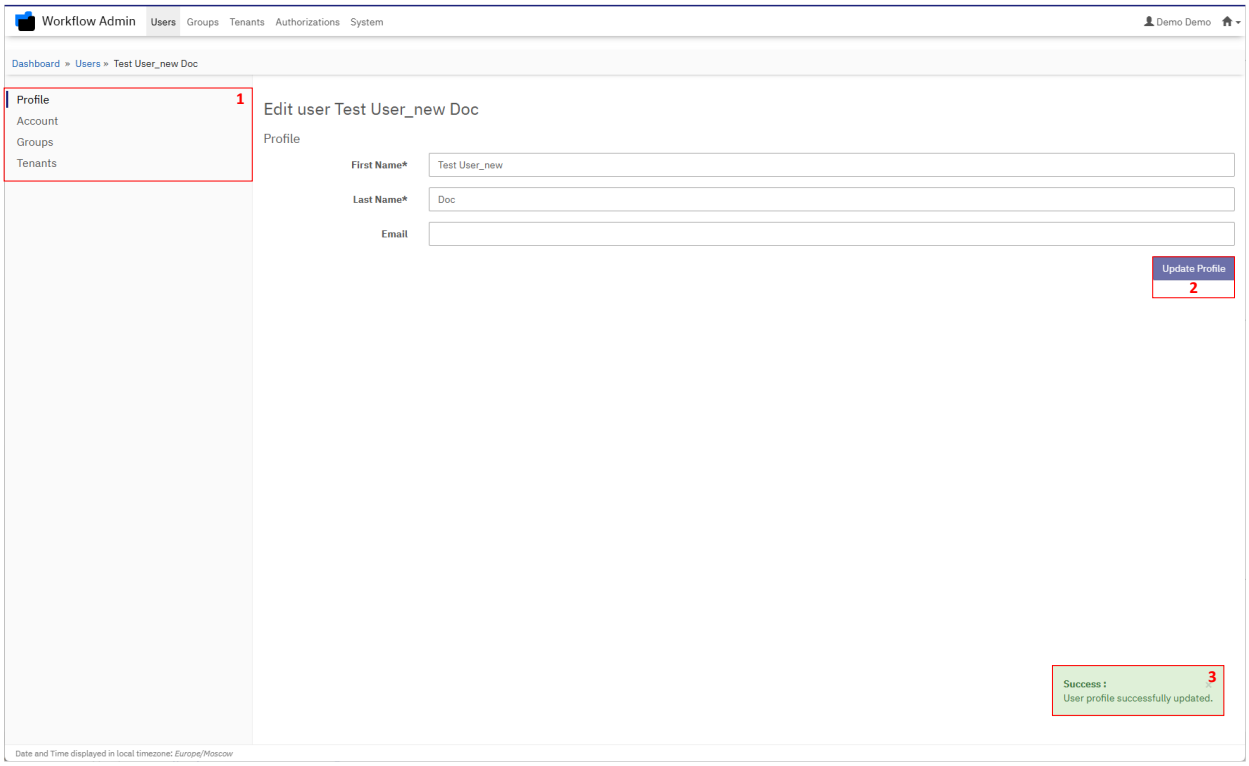


Рисунок 201 – Изменение УЗ пользователя

7.2.2.3. Удаление УЗ пользователя

Для удаления УЗ пользователя выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Users** (1, рисунок 202) в общем списке выберите УЗ пользователя, нажав на его **ID** либо на **Edit** в правом столбце (2, рисунок 202).

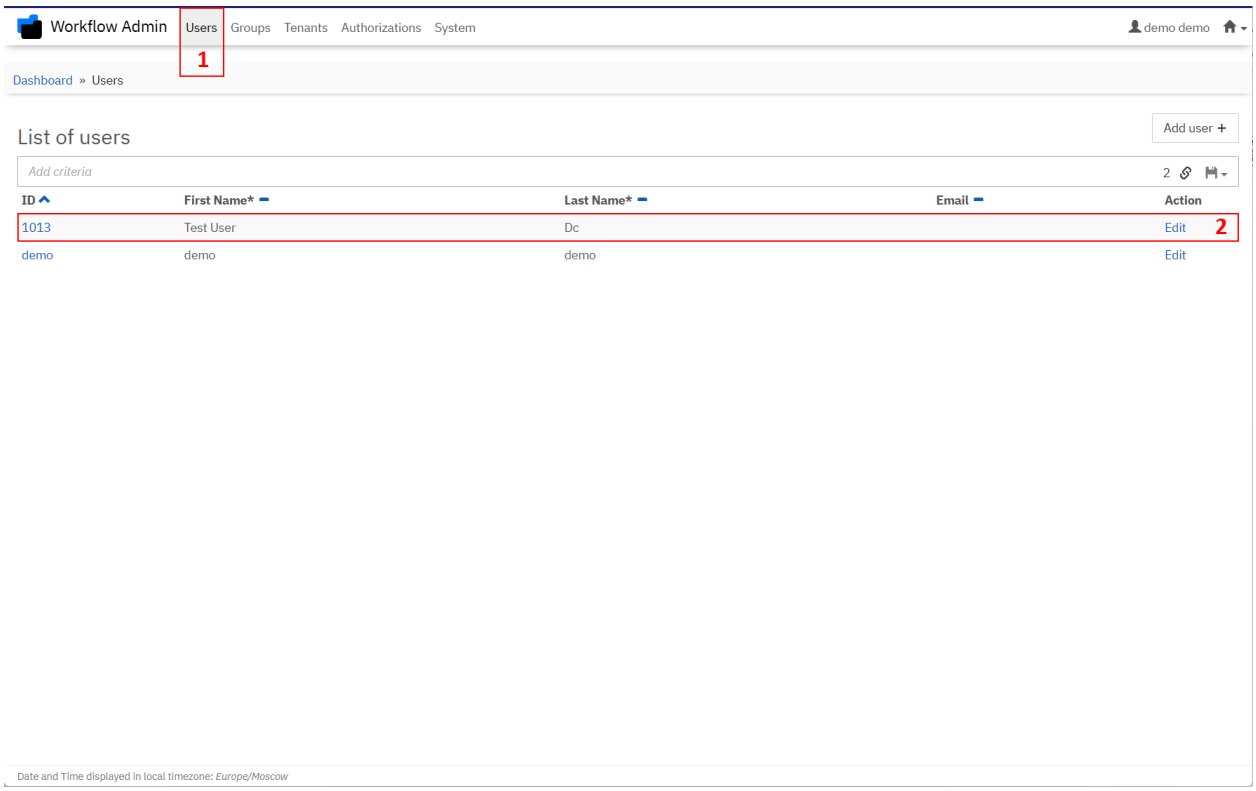


Рисунок 202 – Выбор УЗ пользователя

3. Перейдите на вкладку **Account** (1, рисунок 203) и нажмите на **Delete User** (2, рисунок 203). В всплывающем окне подтвердите удаление, нажав на **Proceed**. Убедитесь в удалении УЗ пользователя, дождавшись соответствующего сообщения в правом нижнем углу окна (рисунок 204).

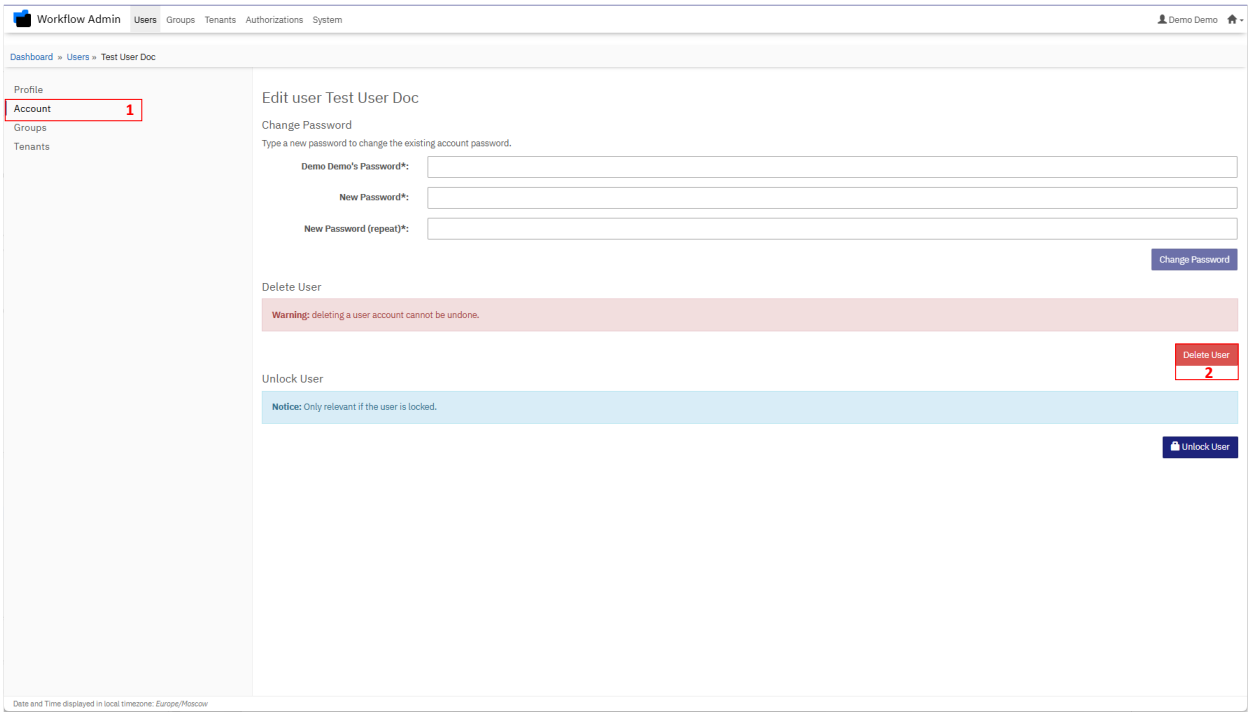


Рисунок 203 – Удаление УЗ пользователя

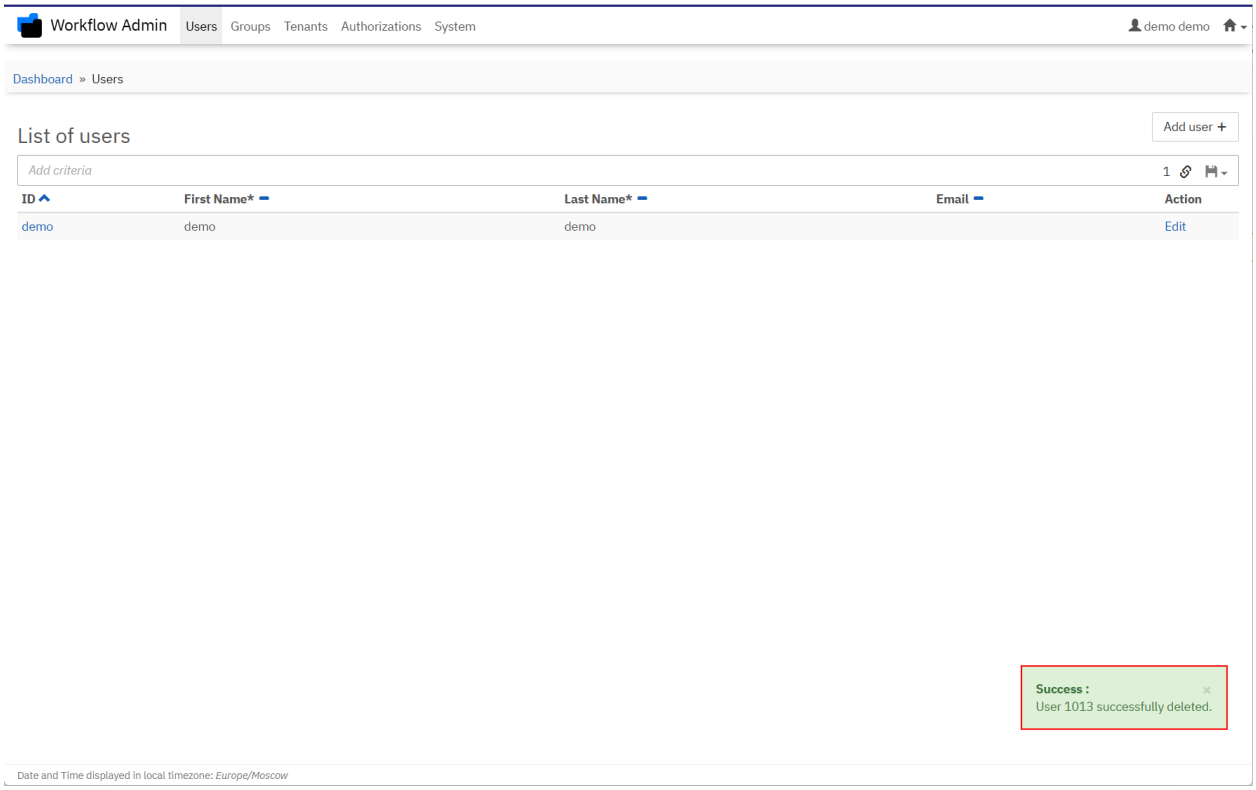


Рисунок 204 – Сообщение об успешном удалении УЗ пользователя

7.2.2.4. Назначение УЗ пользователя группы

Для назначения УЗ пользователя группы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Users** (1; рисунок 205) выберите нужную УЗ пользователя (2; рисунок 205).

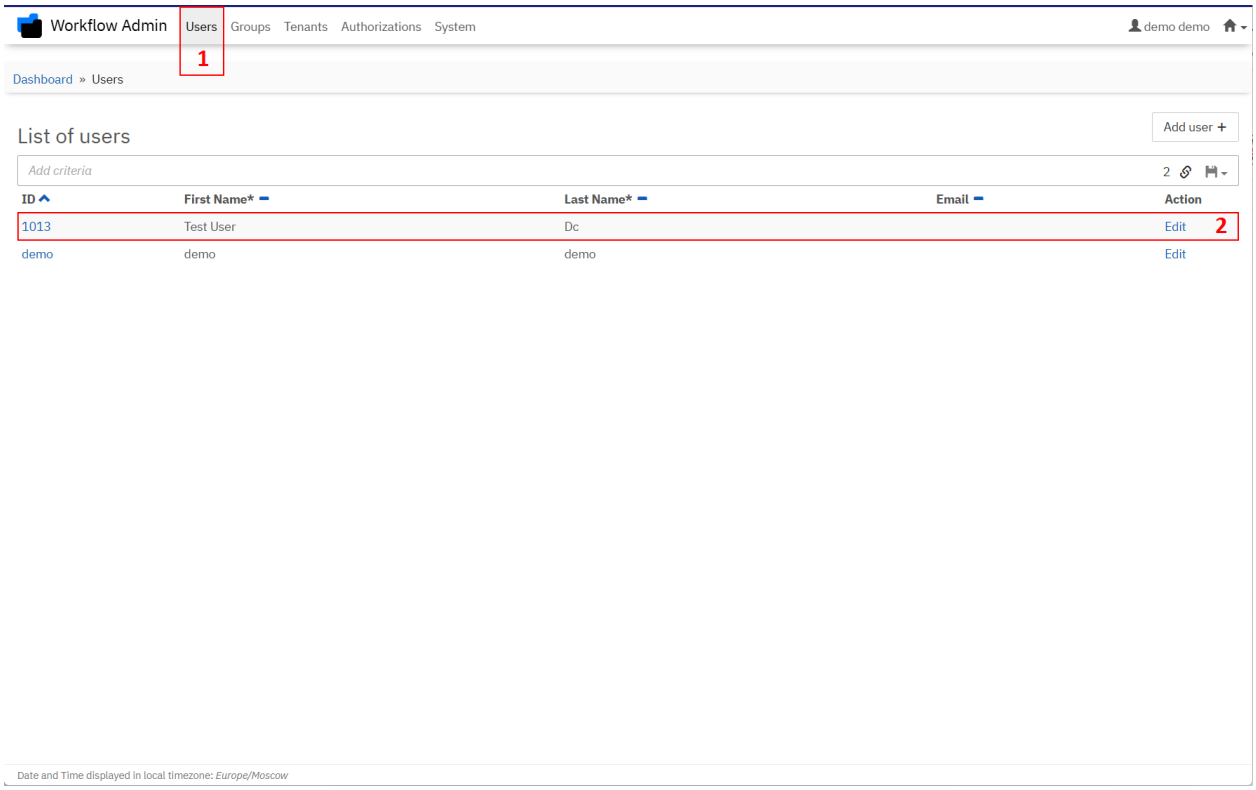


Рисунок 205 – Выбор УЗ пользователя

3. Перейдите в **Groups** (1; рисунок 206). Нажмите на **Add to a group** (2; рисунок 206).

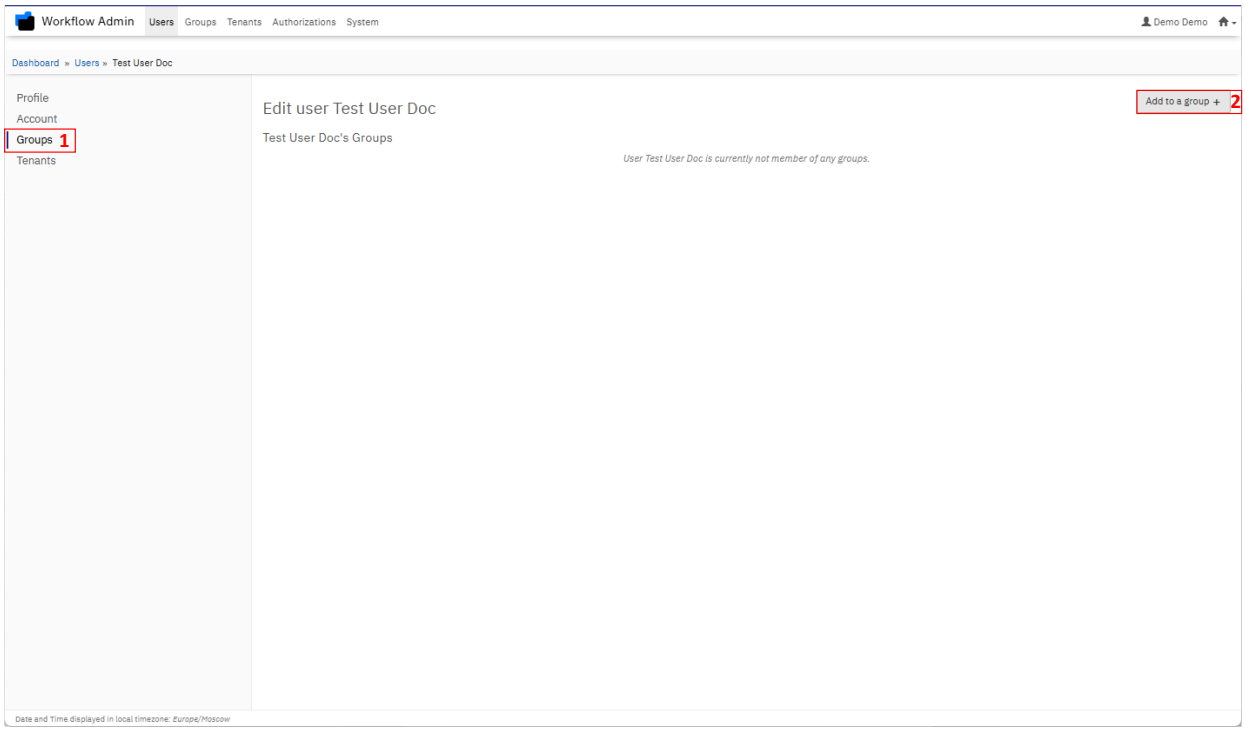


Рисунок 206 – Переход к назначению группы УЗ пользователя

4. В появившемся окне **Select Groups** отметьте флагами назначаемые УЗ пользователя группы (1; рисунок 207) и нажмите на **Add Groups** (2; рисунок 207). Убедитесь в назначении группы; дождавшись соответствующего сообщения (рисунок 208).

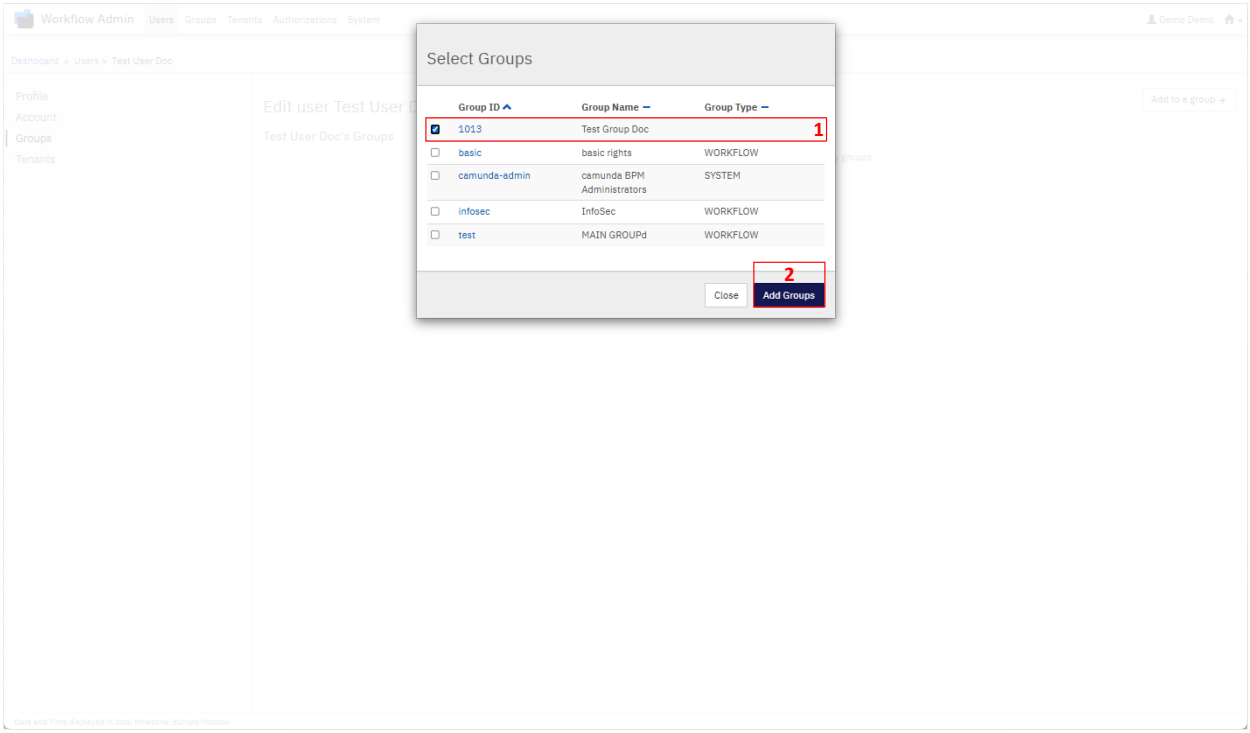


Рисунок 207 – Выбор группы

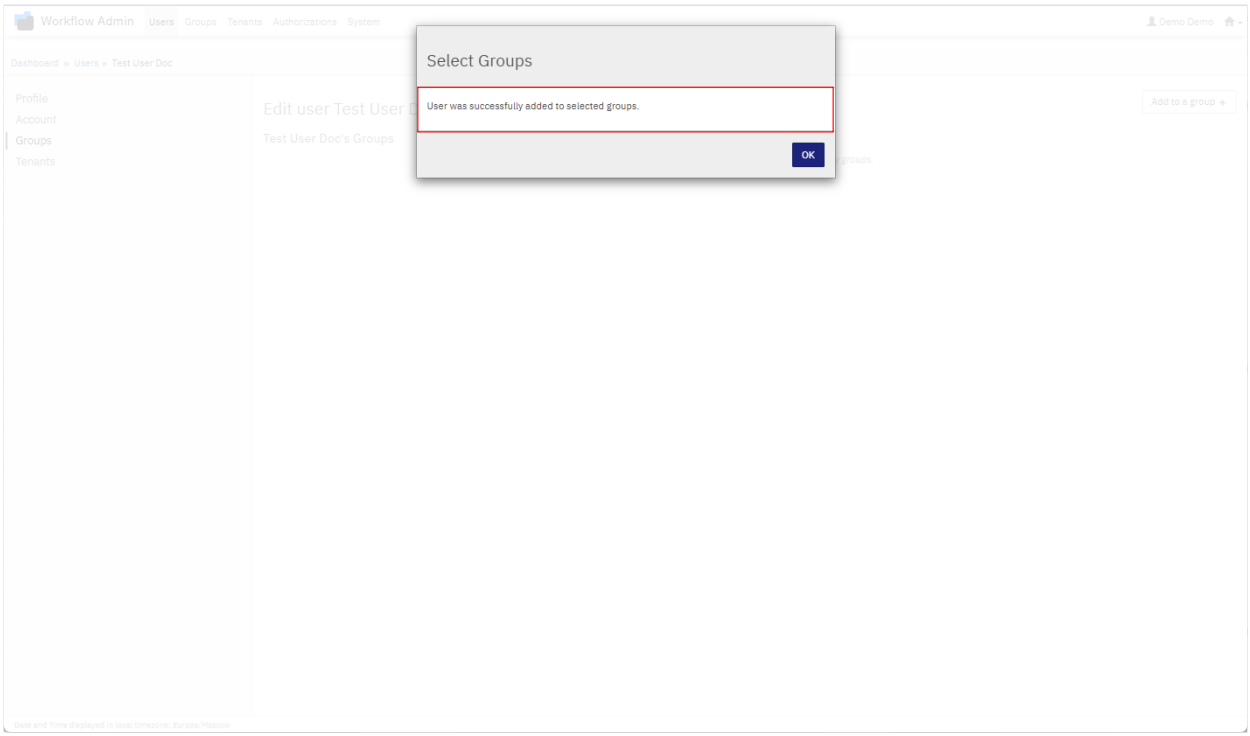


Рисунок 208 – Сообщение о назначении УЗ пользователя группы

7.2.3. Управление правами доступа

7.2.3.1. Предоставление прав доступа

Для предоставления прав доступа к категориям выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Authorization** (рисунок 209).

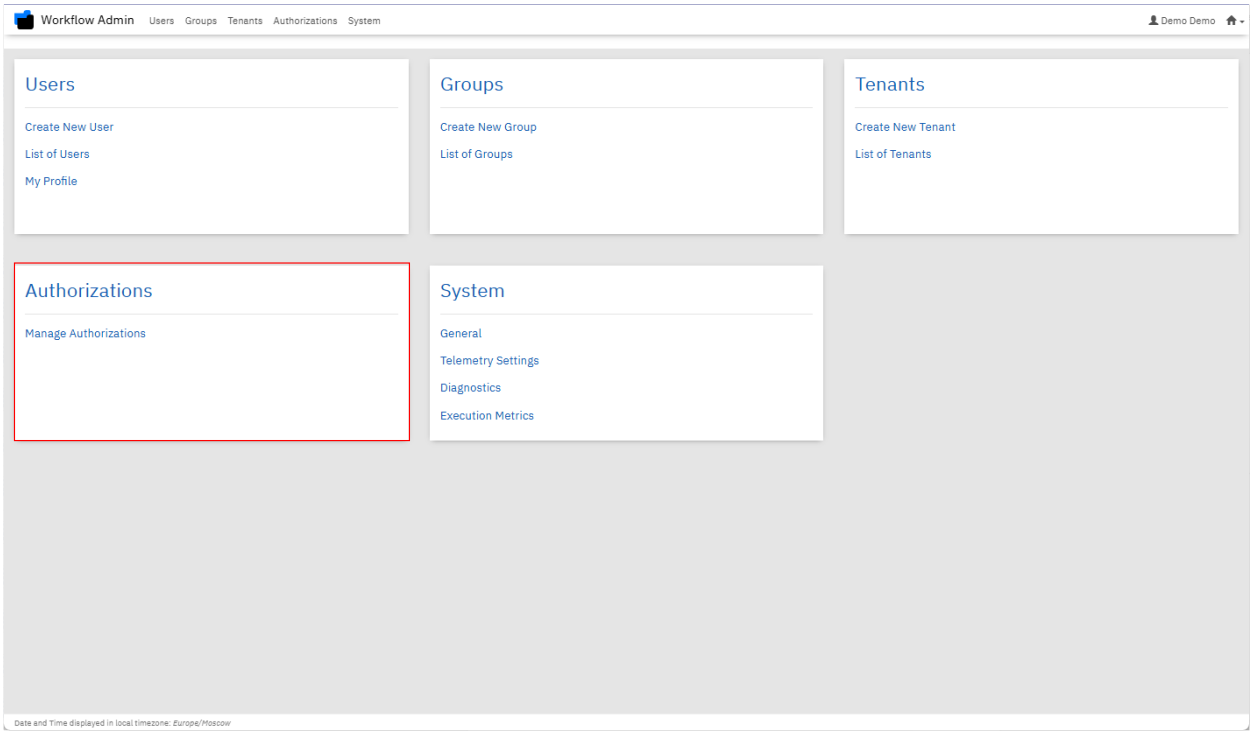


Рисунок 209 – Переход к Authorization

3. Выберите нужную категорию (1; рисунок 210). Нажмите на **Create new authorizations** (2; рисунок 210).

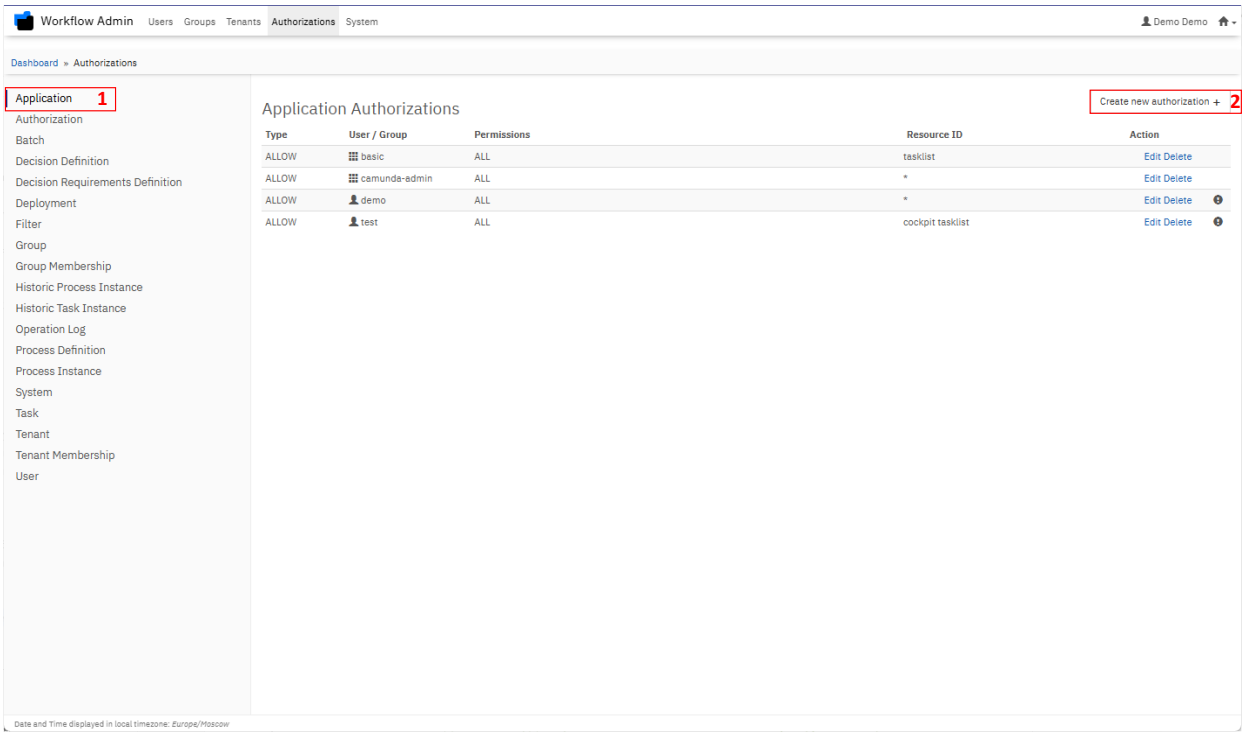


Рисунок 210 – Настройка прав доступа к категориям

4. Введите ID группы в столбец **User/Group** (1; рисунок 211).

Подсказка: для переключения режима ввода ID (пользователя/группы) нажмите на  /  (2; рисунок 211).

5. Введите необходимые значения в столбец **Resource ID** (3; рисунок 211). Для сохранения нажмите на  (4; рисунок 211). При необходимости измените набор прав доступа; для этого нажмите на  (5; рисунок 211) и укажите нужные права с помощью флагов.

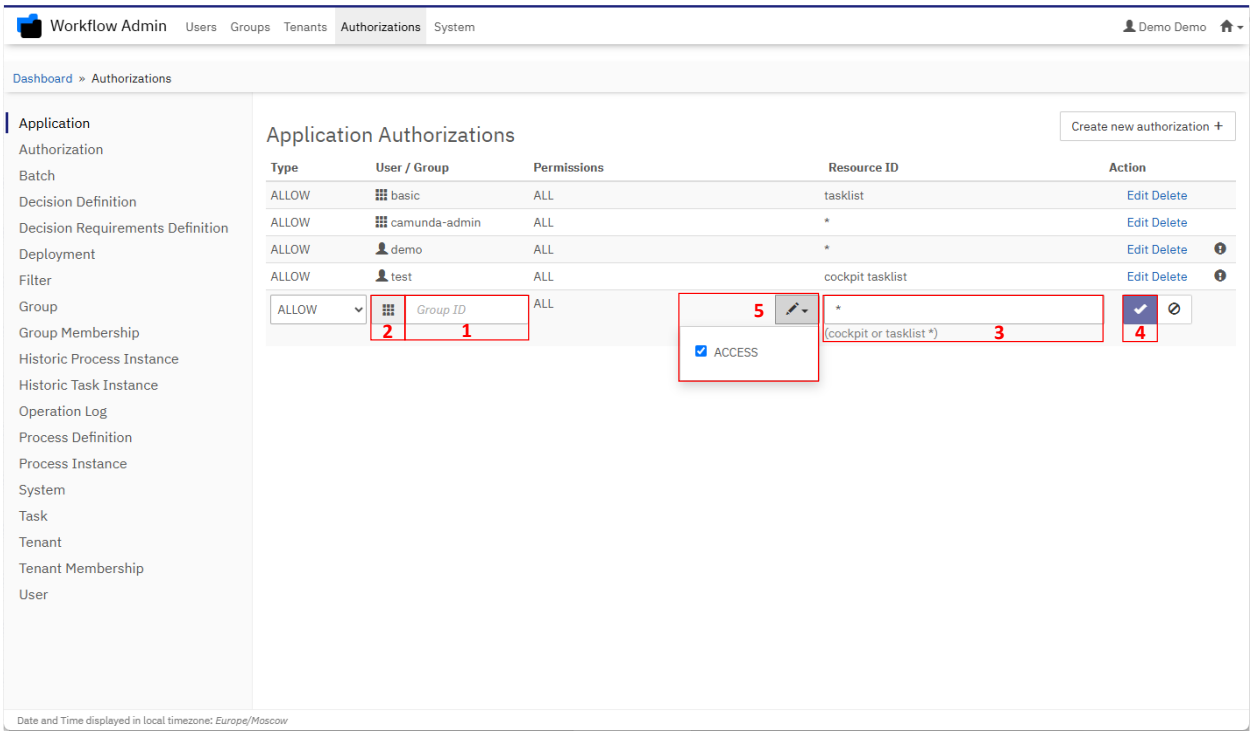


Рисунок 211 – Предоставление прав доступа

7.2.3.2. Изменение прав доступа

Для изменения прав доступа выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Authorization** (рисунок 212).

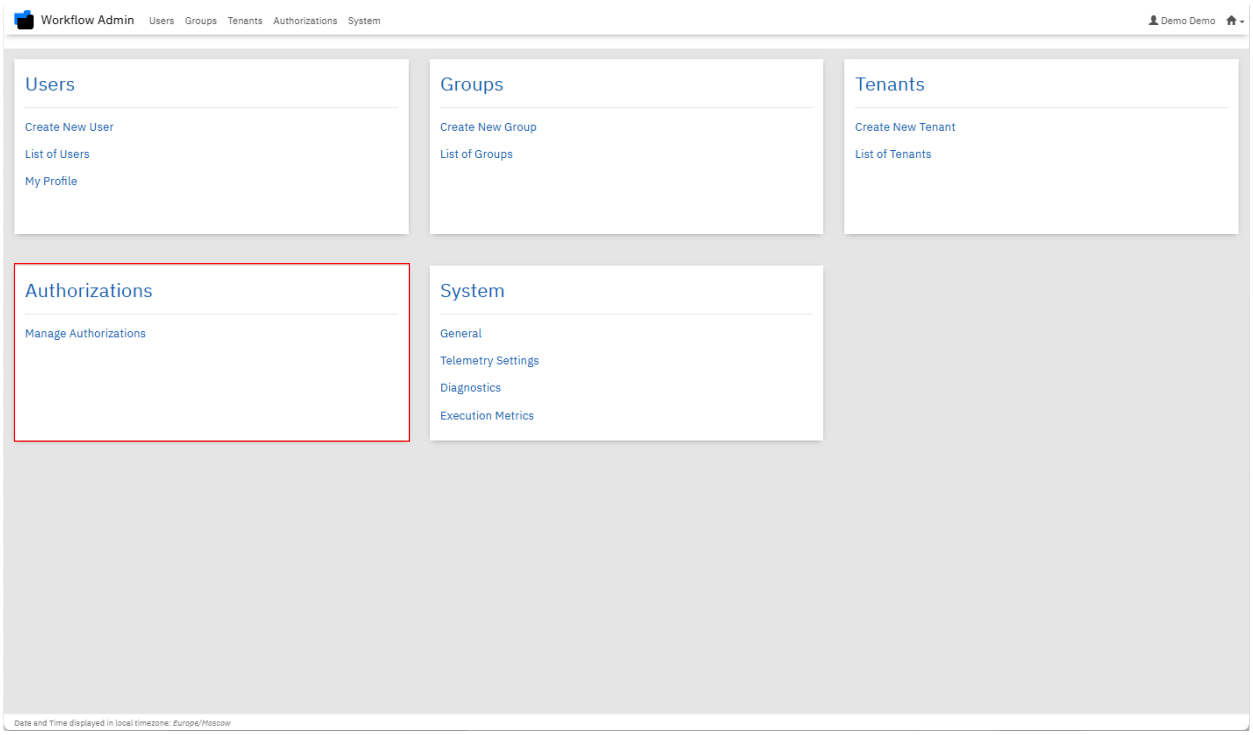


Рисунок 212 – Переход к Authorization

3. Выберите нужную категорию (1; рисунок 213). Нажмите на **Edit** справа от пользователя / группы (2; рисунок 213).

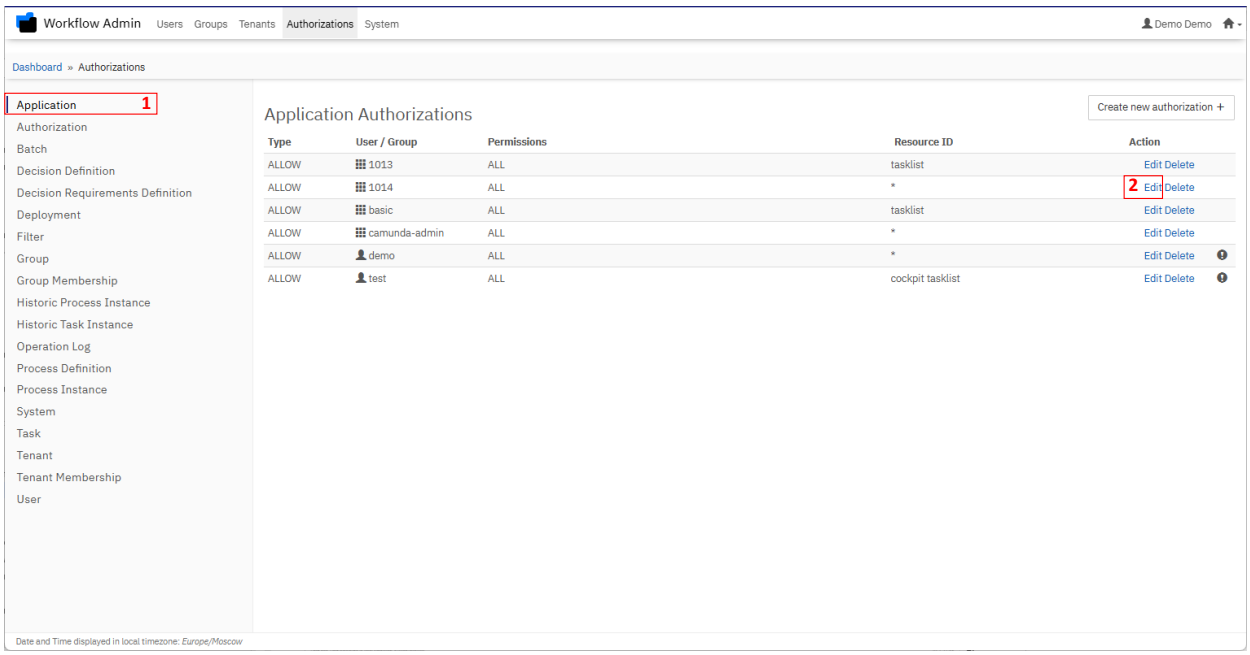


Рисунок 213 – Переход к изменению прав доступа

4. Отредактируйте нужные поля (**User / Group, Permissions, Resource ID**) и для сохранения нажмите на  (рисунок 214).

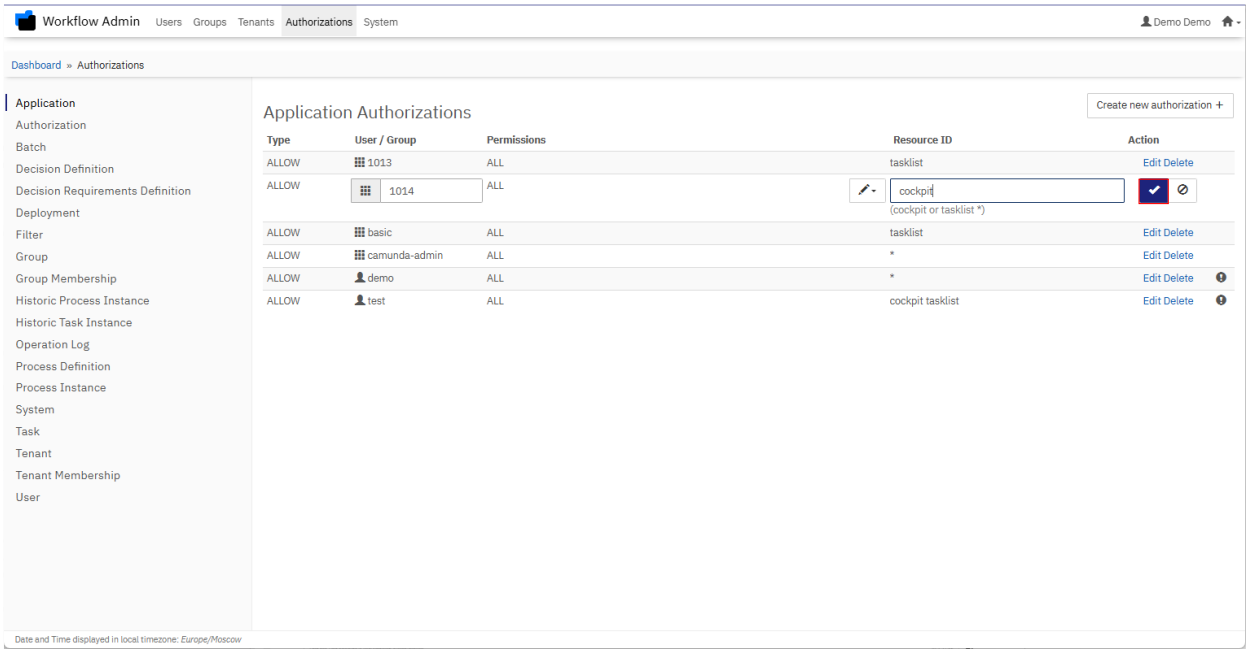


Рисунок 214 – Изменение прав доступа

7.2.3.3. Отзыв прав доступа

Под отзывом прав доступа подразумевается удаление информации о доступе пользователя / группы к категории.

Для изменения прав доступа выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Authorization** (рисунок 215).

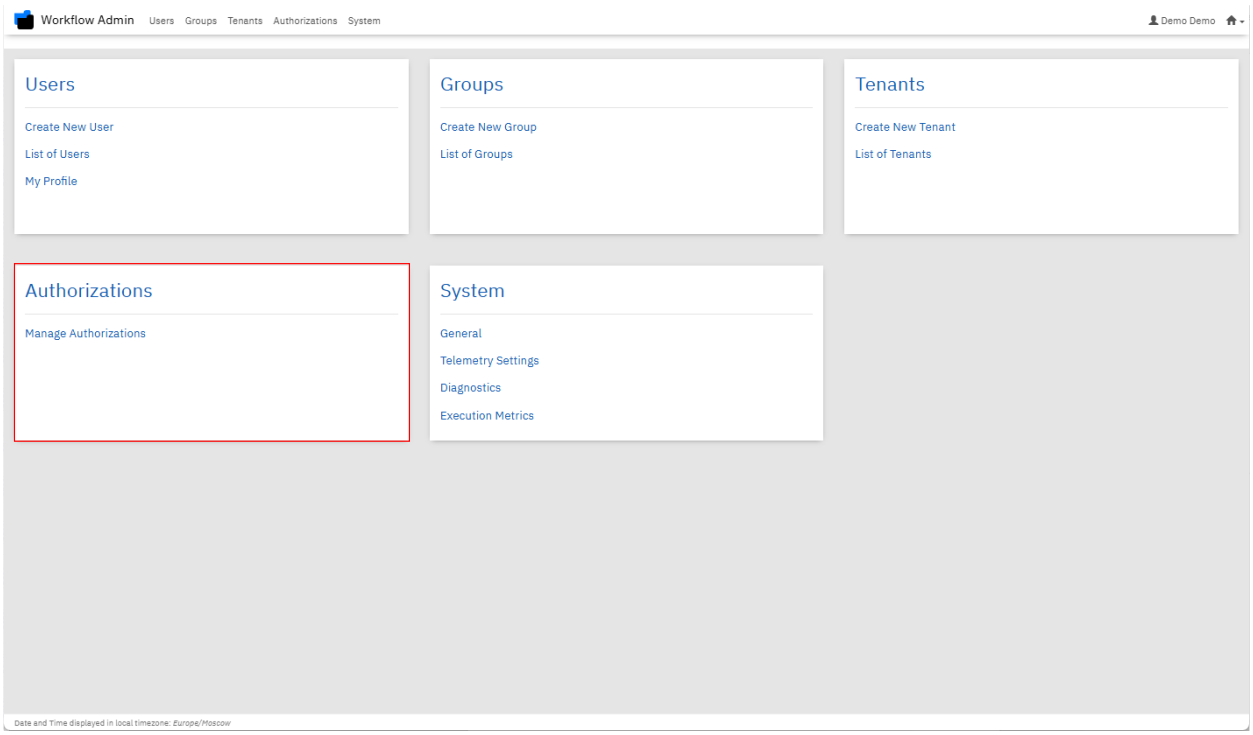


Рисунок 215 – Переход к Authorization

3. Выберите нужную категорию (1; рисунок 216). Нажмите на **Delete** справа от пользователя / группы (2; рисунок 216). В всплывающем окне подтвердите отзыв прав доступа, нажав на **Delete**. Убедитесь в отзыве прав доступа, дождавшись соответствующего сообщения (рисунок 217).

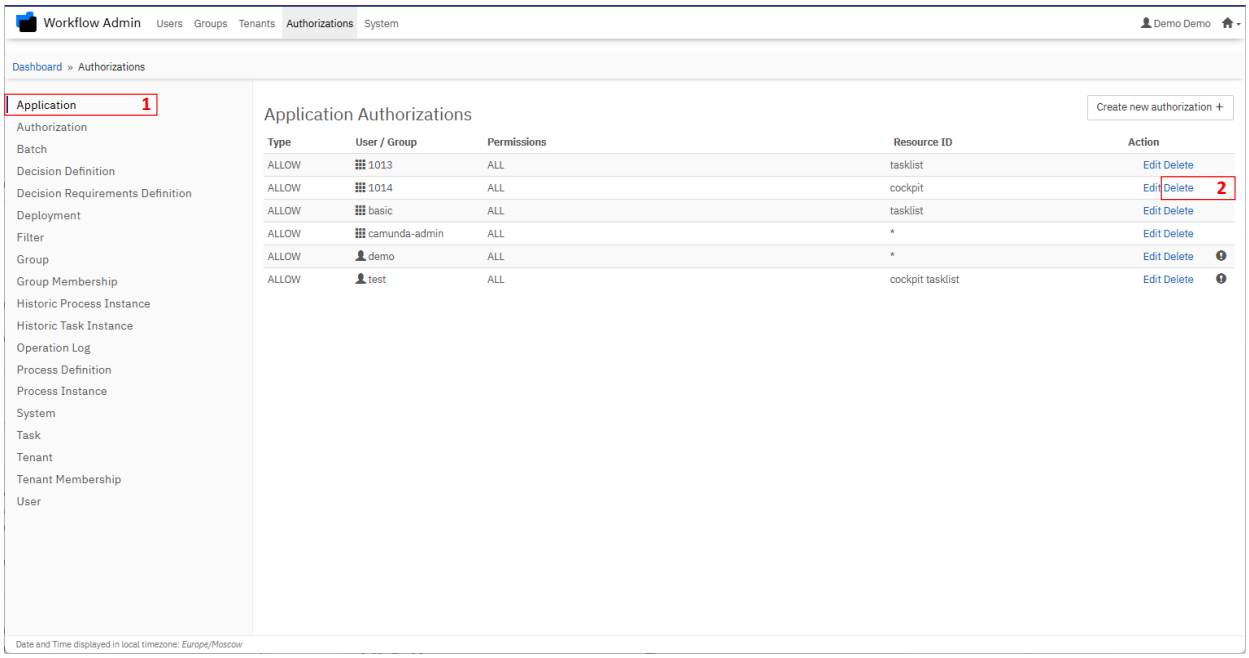


Рисунок 216 – Переход к отзыву прав доступа

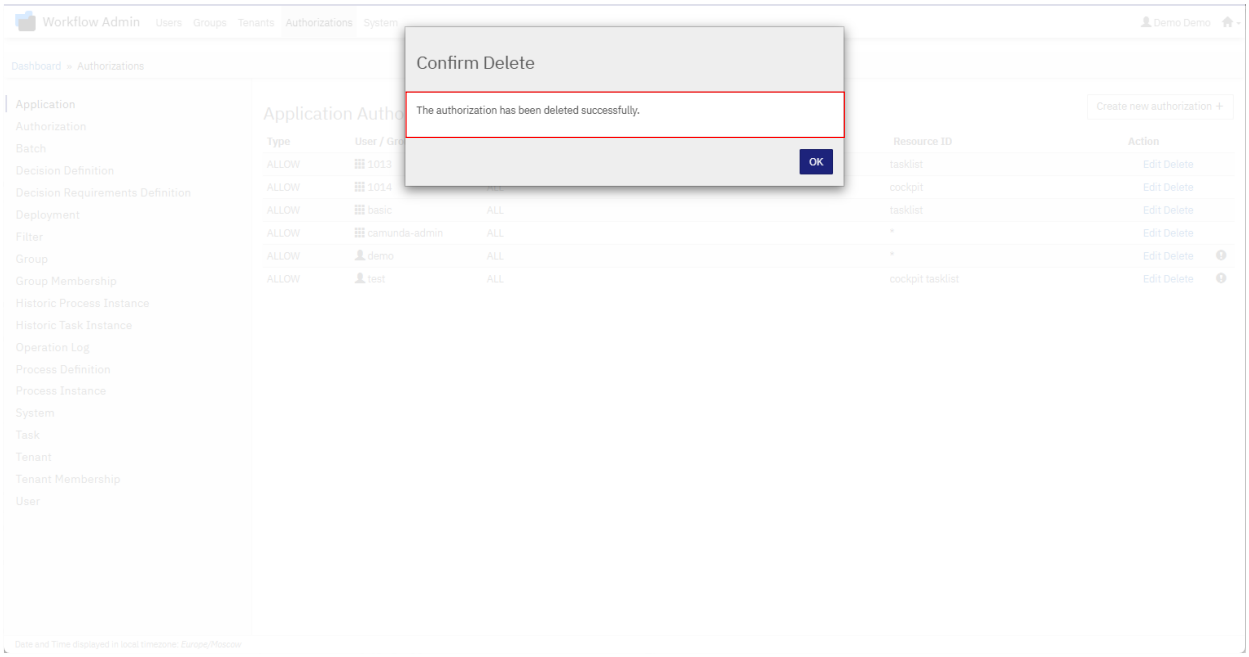


Рисунок 217 – Сообщение об успешном отзыве прав доступа

7.2.4. Управление группами

7.2.4.1. Создание группы

Для создания группы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Groups** (1; рисунок 218) нажмите на **Create new group** (2; рисунок 218).

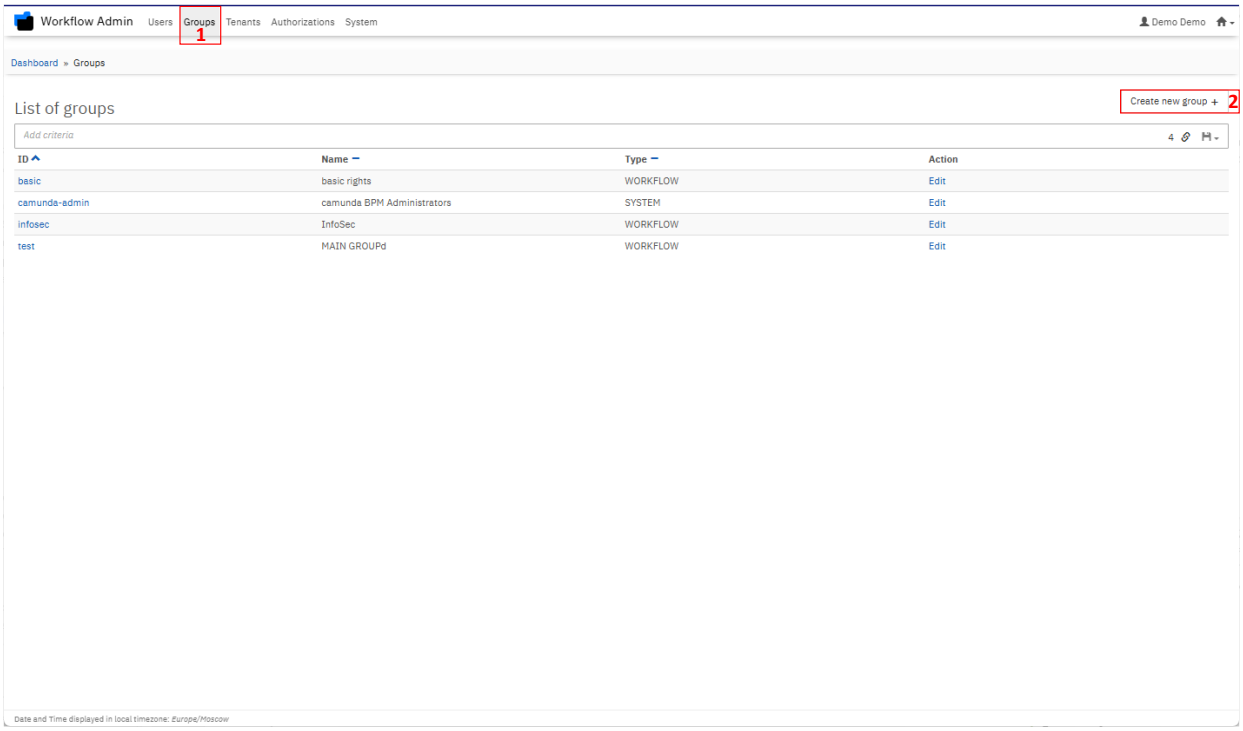


Рисунок 218 – Переход к созданию группы

3. Заполните поля в разделе **Create new group**; обязательны к заполнению только поля; помеченные *****. Нажмите на **Create new group** (рисунок 219). Убедитесь в создании группы; дождавшись соответствующего сообщения в правом нижнем углу окна (рисунок 220).

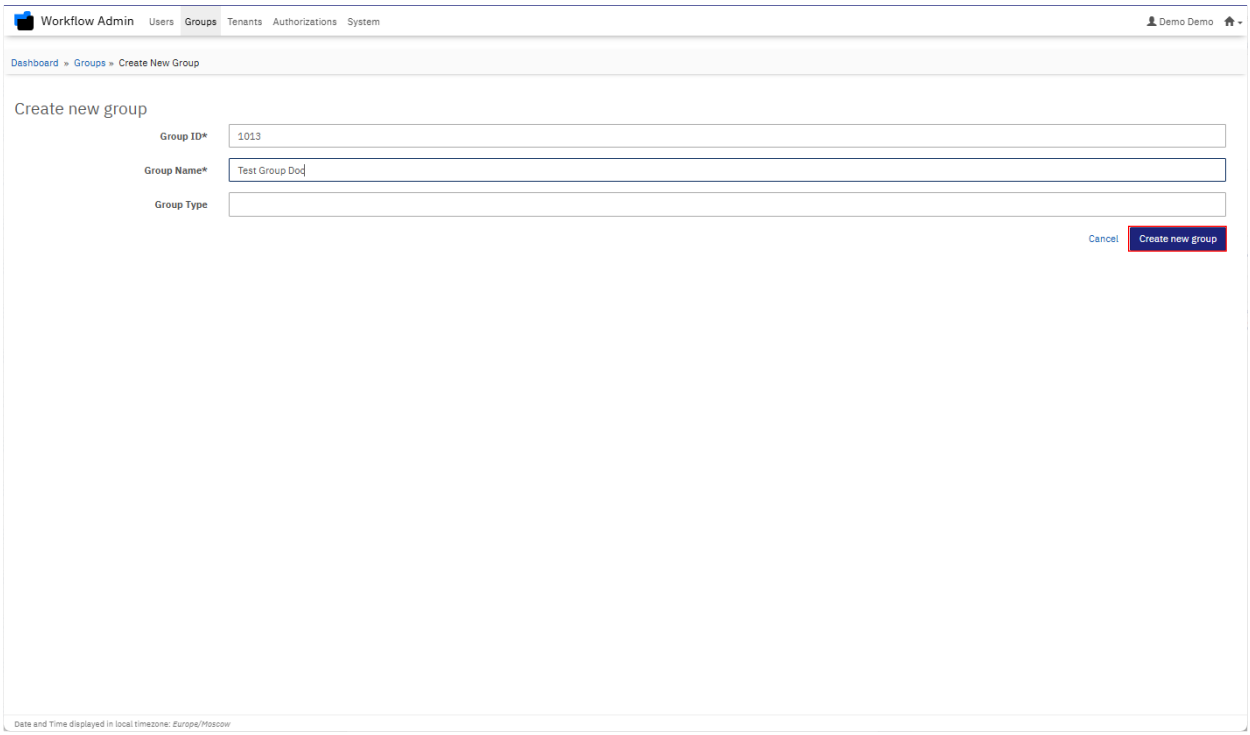


Рисунок 219 – Создание группы

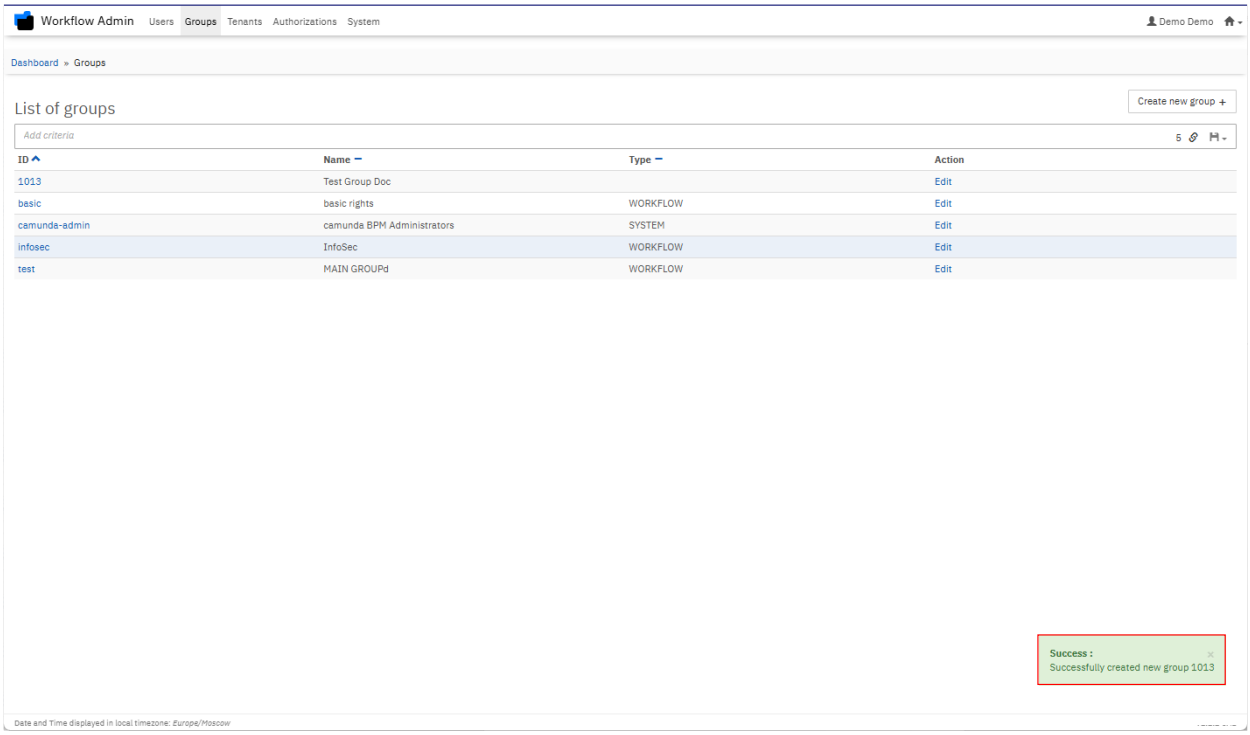


Рисунок 220 – Сообщение об успешном создании группы

7.2.4.2. Изменение группы

Для изменения группы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Groups** (1, рисунок 221) в общем списке выберите группу, нажав на её **ID** либо на **Edit** в правом столбце (2, рисунок 221).

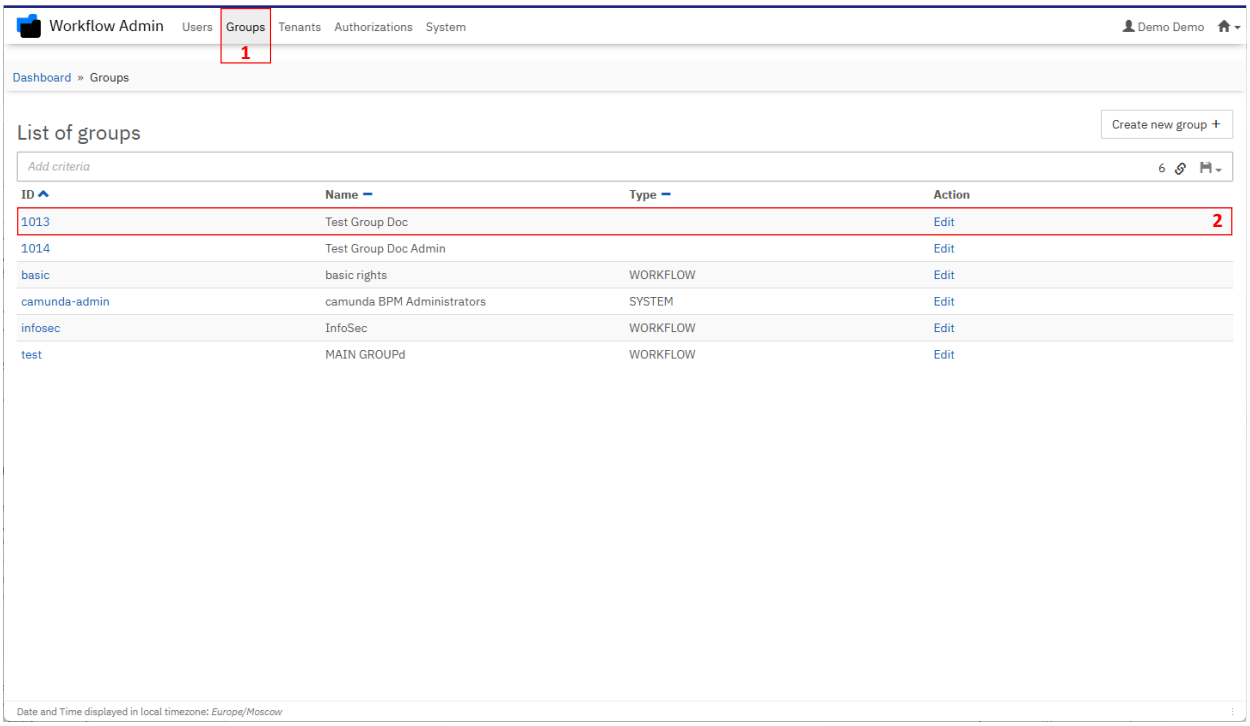


Рисунок 221 – Выбор группы

3. Отредактируйте поля на нужной вкладке (1, рисунок 222). Нажмите на **Update Profile** (2, рисунок 222). Убедитесь, что данные УЗ обновились, дождавшись соответствующего сообщения в правом нижнем углу окна (3, рисунок 222).

   Предусмотрено три вкладки для изменения:

a. **Information** – содержит поля с основной информацией о наименовании и типе группы. Также содержит кнопку для удаления группы **Delete Group**;
b. **Tenants** – позволяет управлять доступом к тенантам;
c. **Users** – позволяет включать / исключать УЗ пользователей в / из группы.

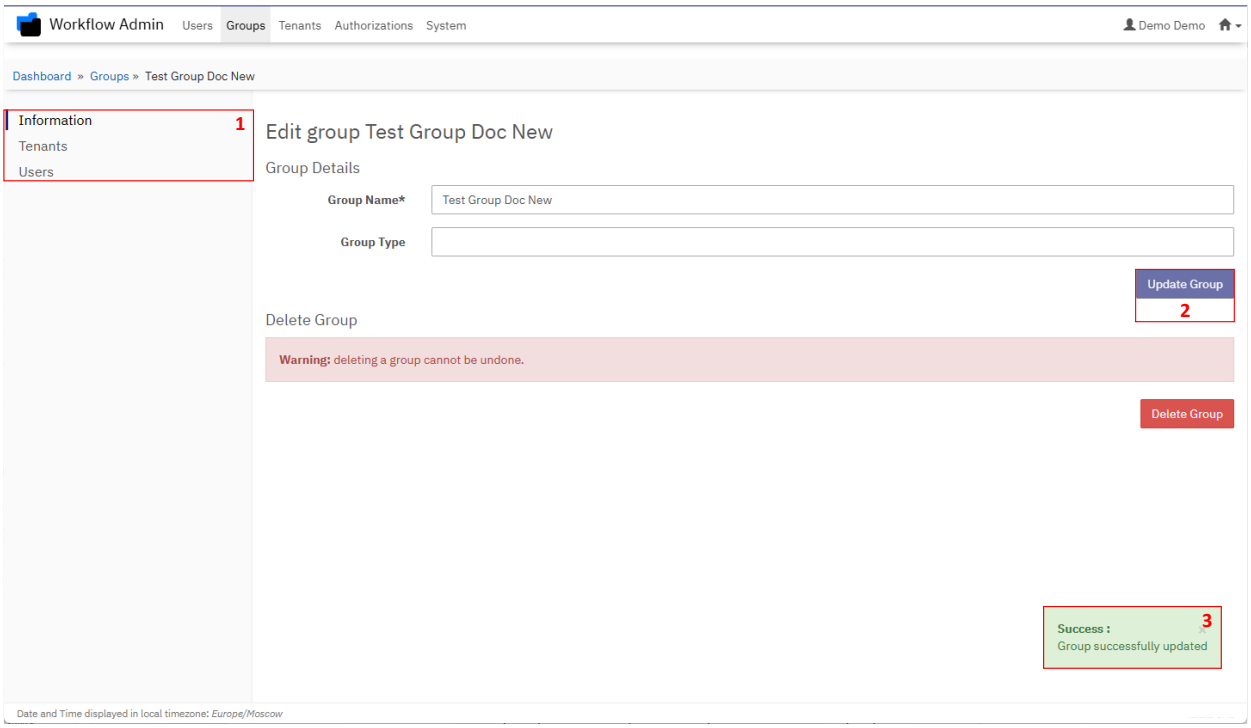


Рисунок 222 – Изменение группы

7.2.4.3. Удаление группы

Для удаления группы выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **Groups** (1, рисунок 223) в общем списке выберите группу, нажав на её **ID** либо на **Edit** в правом столбце (2, рисунок 223).

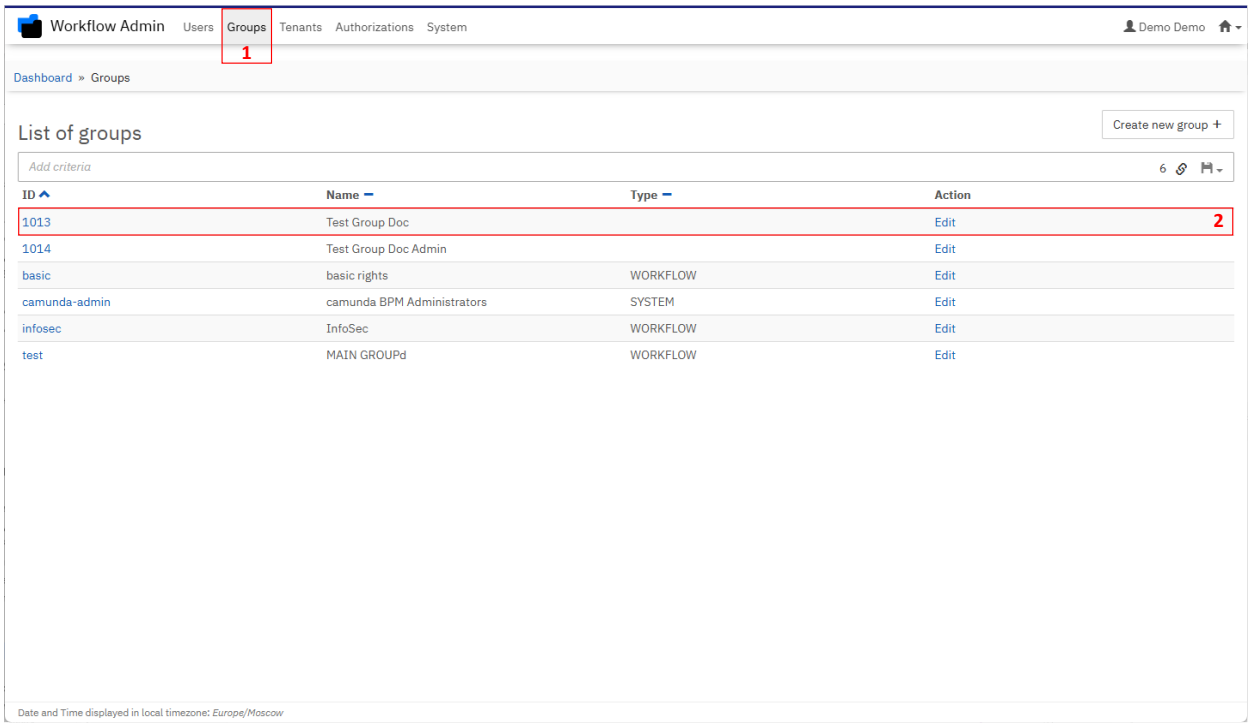


Рисунок 223 – Выбор группы

3. Перейдите на вкладку **Information** (1, рисунок 224) и нажмите на **Delete Group** (2, рисунок 224). В всплывающем окне подтвердите удаление, нажав на **Proceed**. Убедитесь в удалении группы, дождавшись соответствующего сообщения в правом нижнем углу окна (рисунок 225).

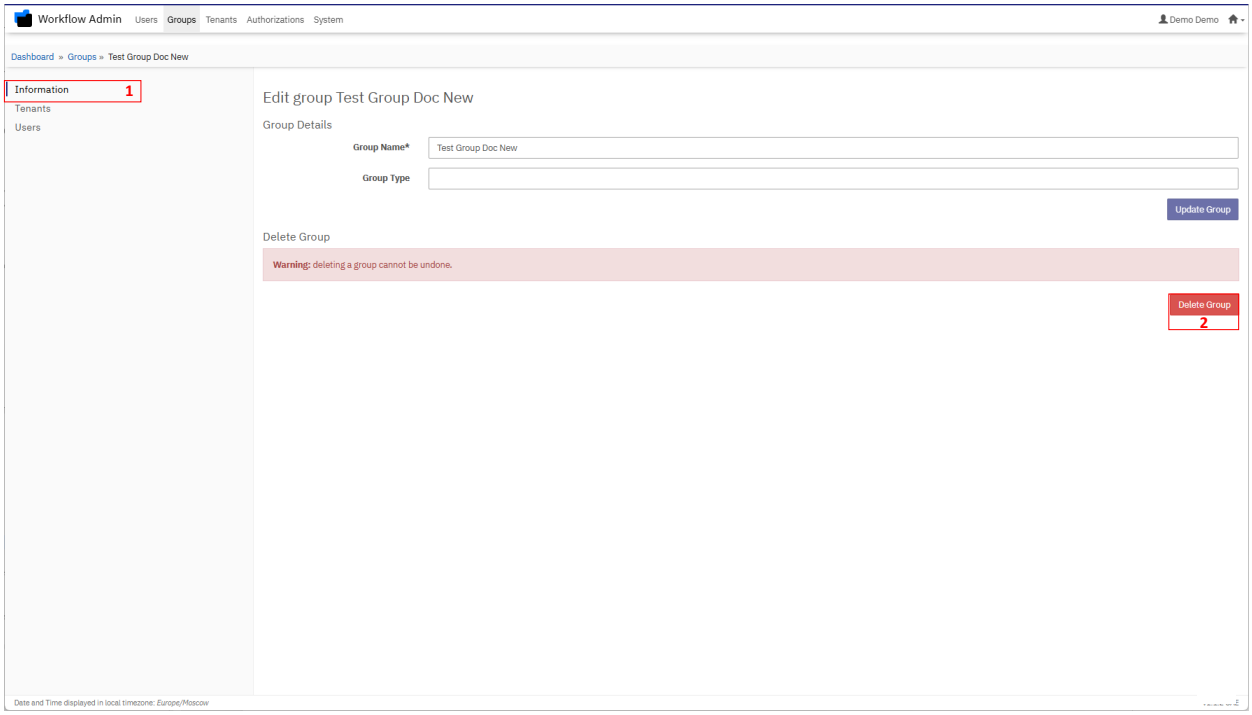


Рисунок 224 – Удаление группы

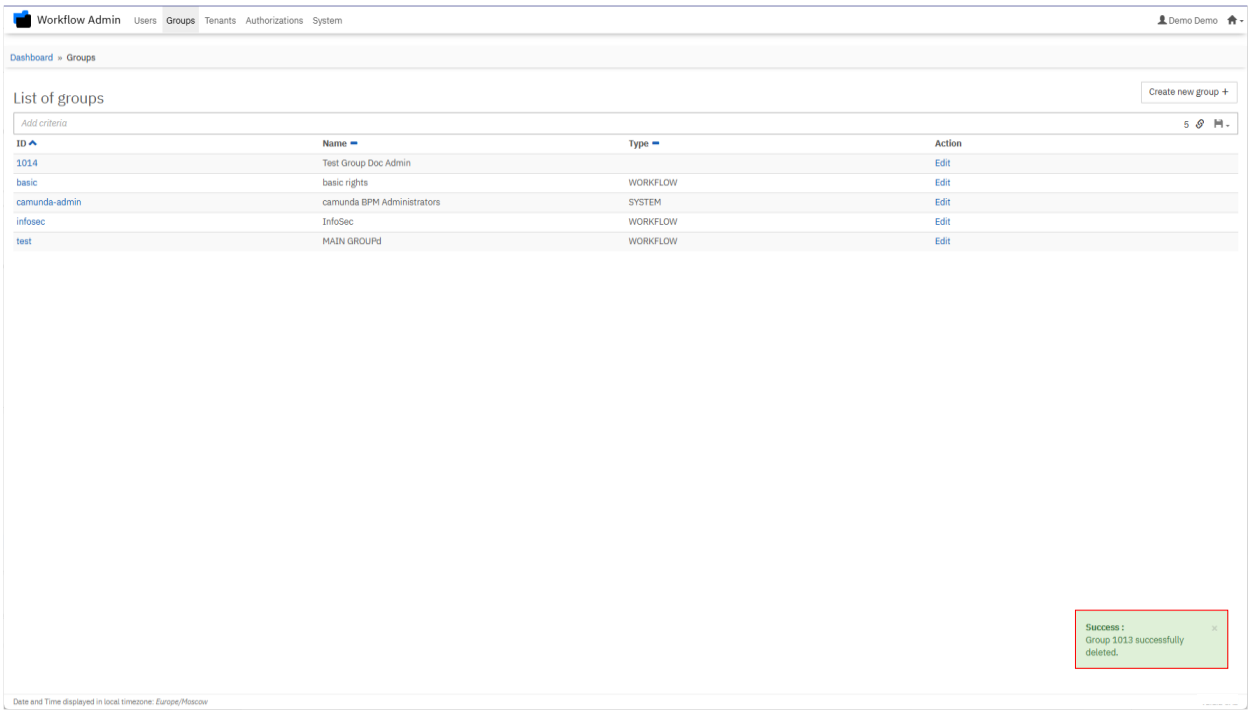


Рисунок 225 – Сообщение об успешном удалении группы

7.2.5. Управление моделями процессов

7.2.5.1. Добавление модели процесса

Для добавления новой модели процесса вручную загрузите BPMN-файл в папку configuration/resources на всех нодах компонента Workflow Management и перезапустите службу на этих серверах с помощью команды

```
systemctl restart camunda
```

7.2.5.2. Изменение модели процесса

Для изменения модели процесса либо вручную измените исходный код BPMN-файла этой модели, либо воспользуйтесь внешними инструментами (например, Camunda Modeler), с помощью которого измените модель, обновите файл на всех серверах, где хранится данная модель и перезапустите службу на этих серверах с помощью команды

```
systemctl restart camunda
```

7.2.5.3. Удаление модели процесса

Для удаления модели процесса вручную удалите или переместите в другую папку BPMN-файл с описанием процесса из папки configuration/resources и перезапустите службу на серверах с помощью команды

```
systemctl restart camunda
```

7.2.5.4. Приостановка модели процесса

Для приостановки модели процесса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Cockpit** (подробнее см. в разделе 7.2.1.3).

2. Выберите **Processes** (1, рисунок 226) и нужную модель процесса (2, рисунок 226).

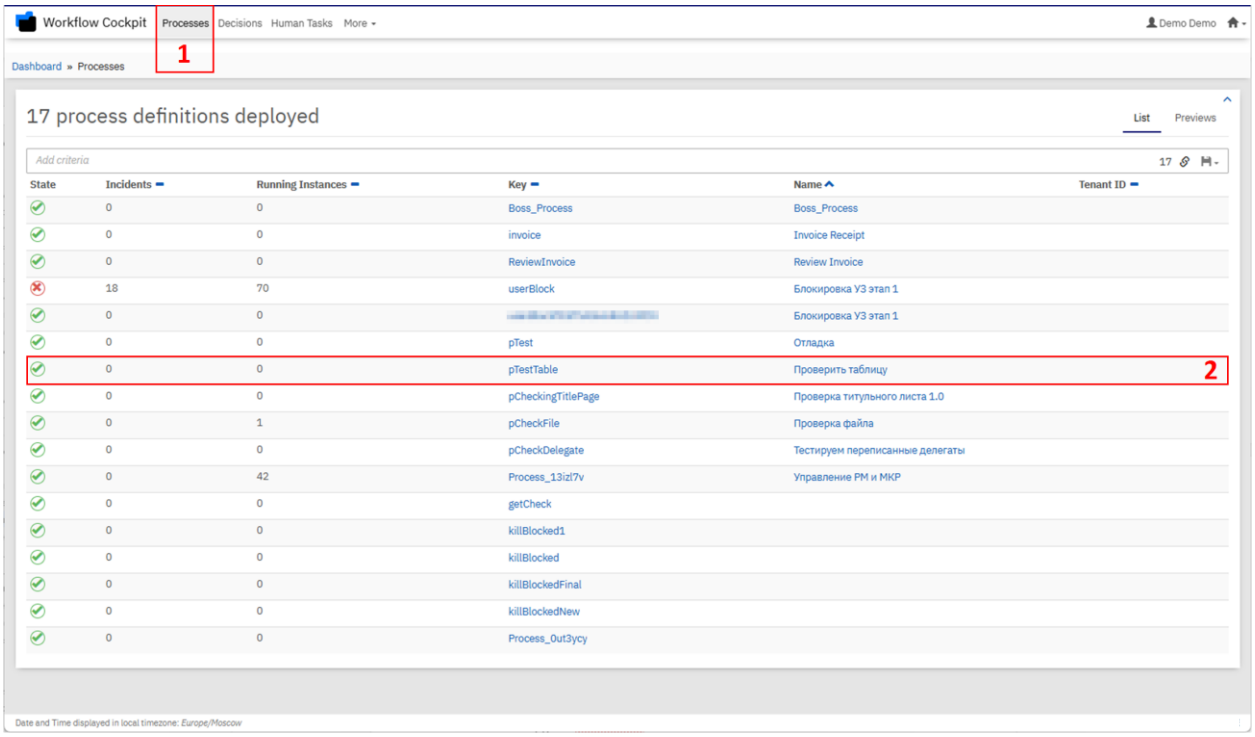


Рисунок 226 – Выбор модели процесса

3. Нажмите на  (рисунок 227). Далее в всплывающем окне нажмите на **Suspend** (рисунок 228) и убедитесь в появления сообщения о приостановке модели процесса (рисунок 229).

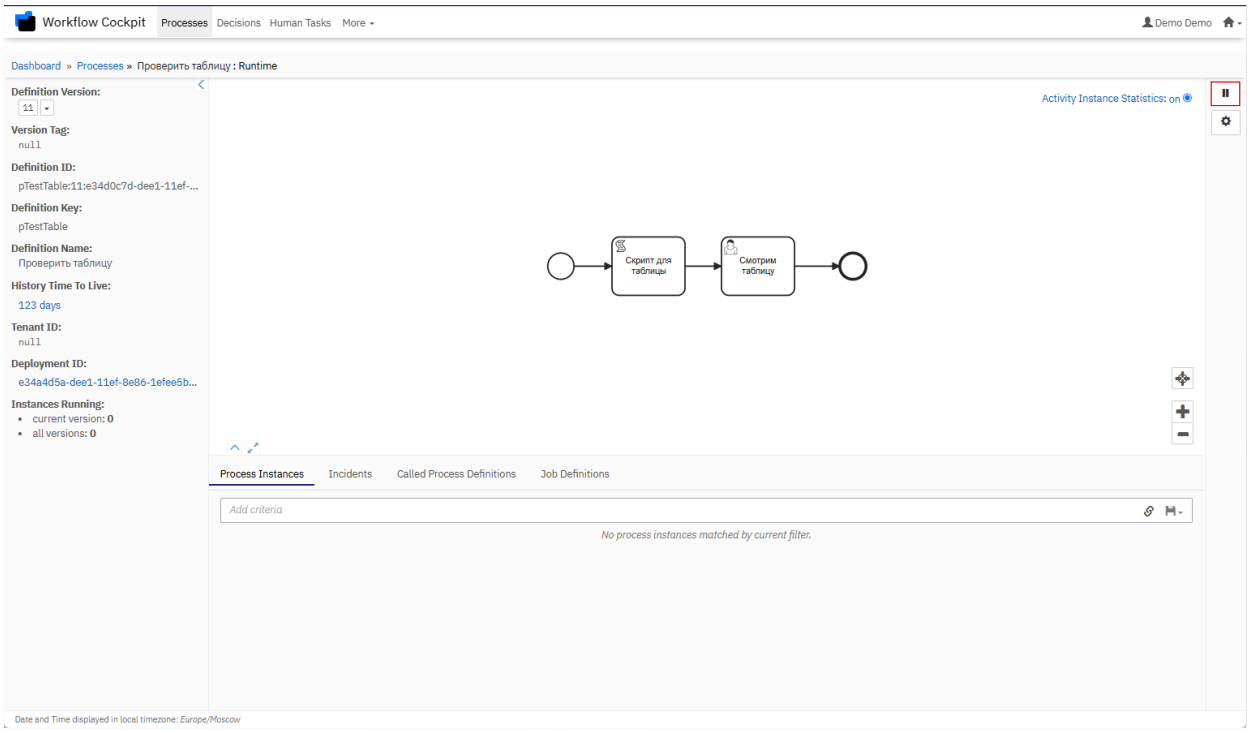


Рисунок 227 – Инициализация приостановки модели процесса

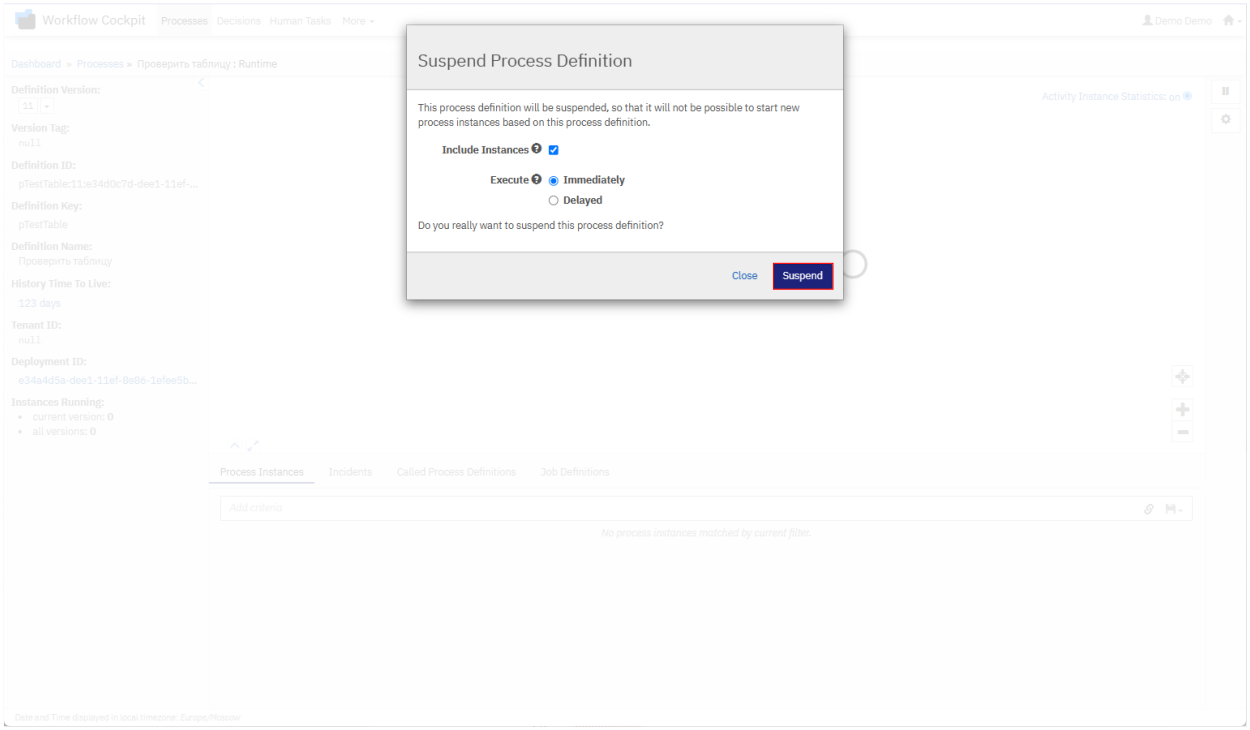


Рисунок 228 – Подтверждение приостановки модели процесса

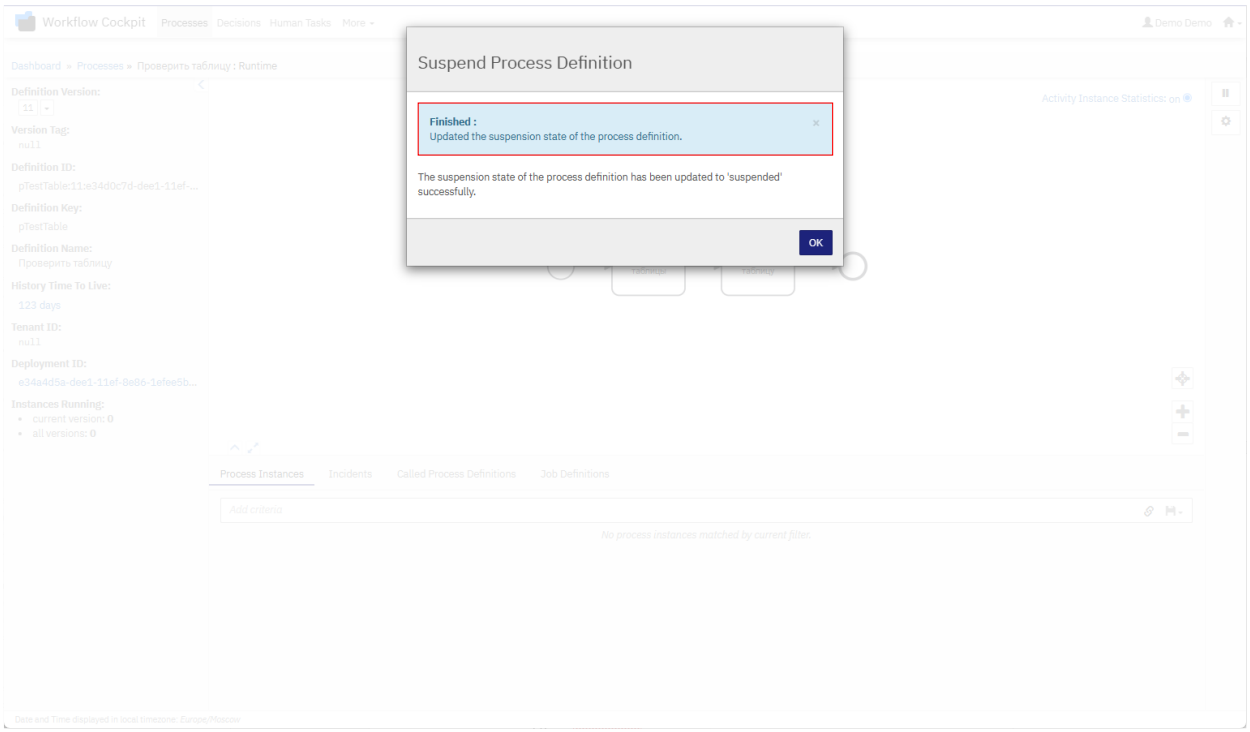


Рисунок 229 – Сообщение об успешной приостановке модели процесса

7.2.5.5. Возобновление модели процесса

Для приостановки модели процесса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Cockpit** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Processes** (1, рисунок 230) и нужную приостановленную модель процесса (2, рисунок 230).

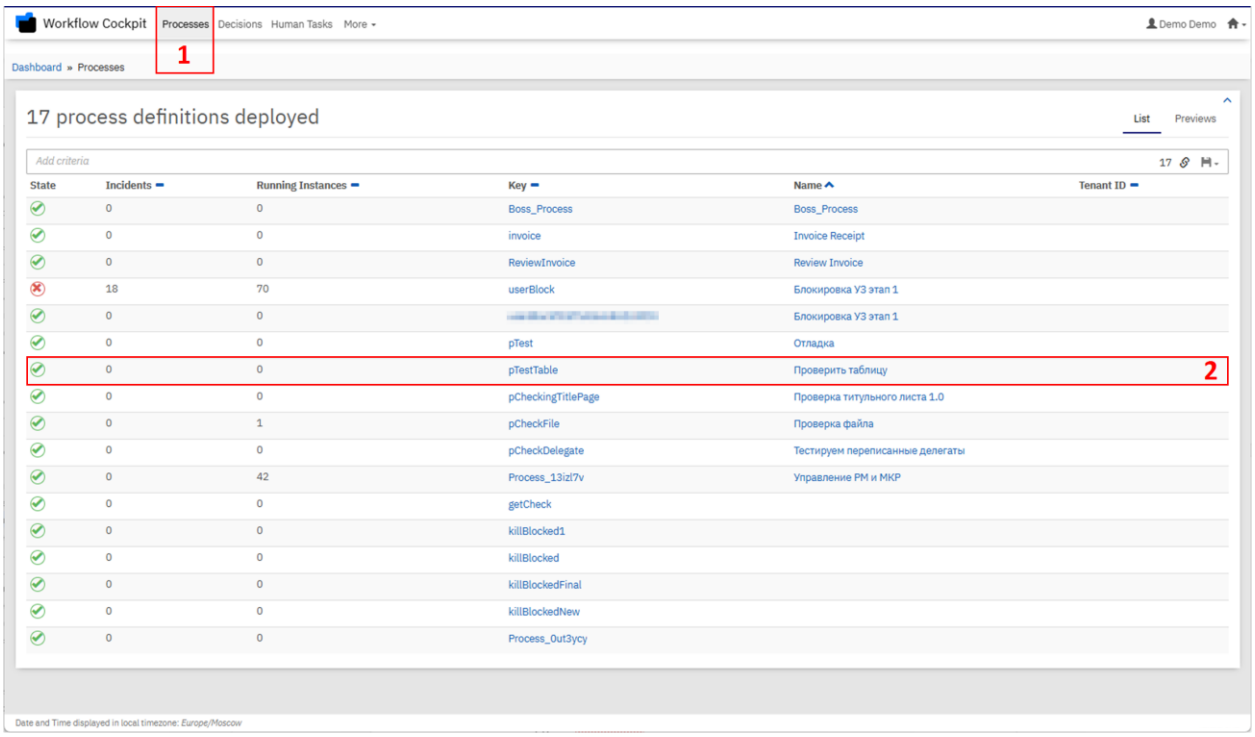


Рисунок 230 – Выбор модели процесса

3. Нажмите на  (рисунок 231). Далее в всплывающем окне нажмите на **Activate** (рисунок 232) и убедитесь в появления сообщения о возобновлении модели процесса (рисунок 233).

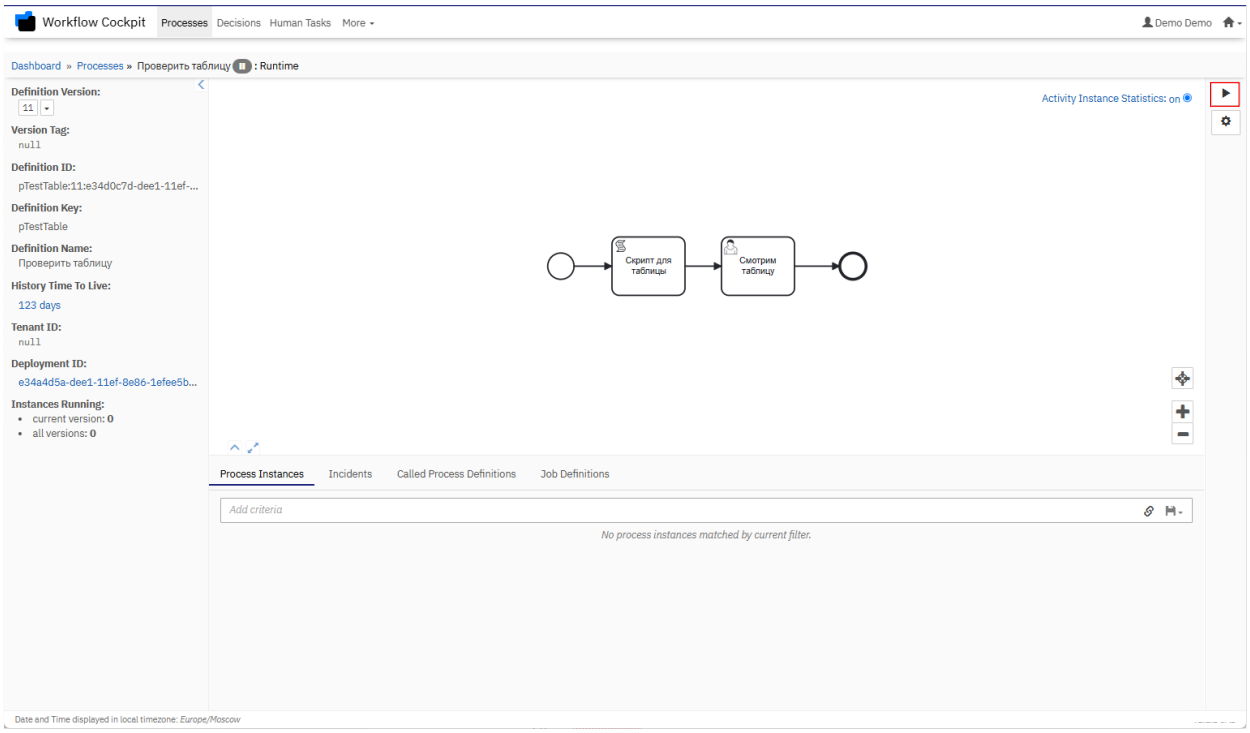


Рисунок 231 – Инициализация возобновления модели процесса

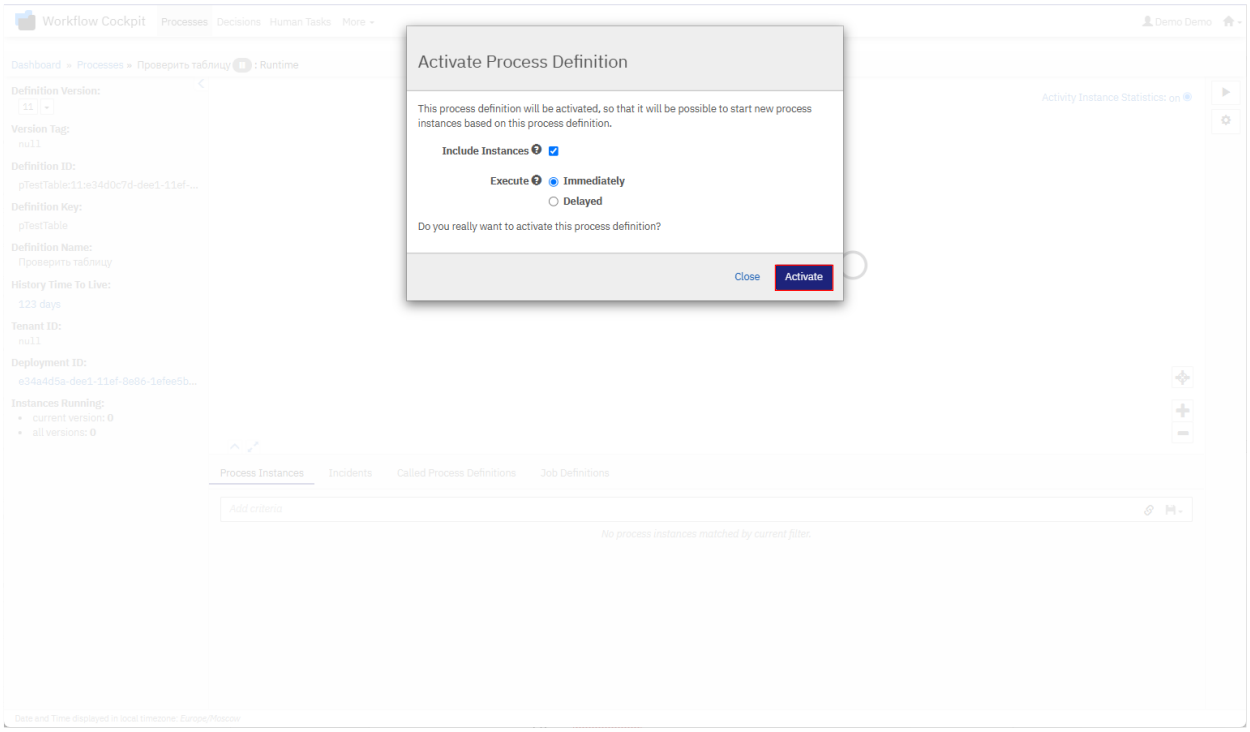


Рисунок 232 – Подтверждение возобновления модели процесса

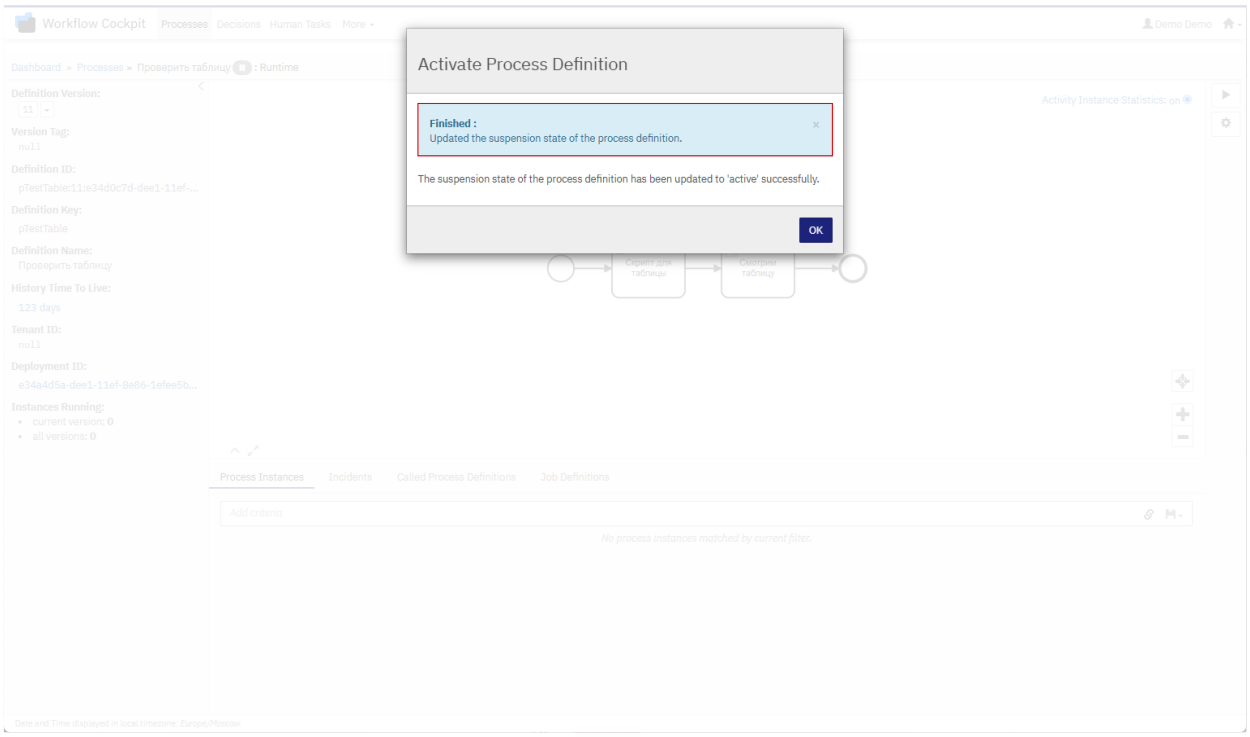


Рисунок 233 – Сообщение об успешном возобновлении модели процесса

7.2.6. Управление экземплярами моделей процессов

7.2.6.1. Запуск экземпляра модели процесса через REST API

Для запуска экземпляра модели процесса с помощью REST API (POST-запроса) выполните следующие шаги:

1. Подключитесь к серверу приложений компонента Workflow Management.
2. Отправьте POST-запрос следующего вида:

```
curl -u <логин ТУЗ к camunda>:<пароль ТУЗ к camunda> -X POST https://<хост camunda>:<порт camunda>/engine-rest/process-definition/key/<ключ модели запускаемого процесса>/start -H "Content-Type: application/json" -d '{"variables": {"<имя переменной>": {"value": "<значение переменной>", "type": "<тип данных переменной>", "valueInfo": {}}}}'
```

В теле запроса перечислите все переменные, передаваемые в запускаемый процесс. Результатом успешного запуска будет HTTP код 200.

7.2.6.2. Запуск экземпляра модели процесса через веб-интерфейс

Описание шагов для запуска экземпляра модели процесса через веб-интерфейс представлено в Руководстве пользователя для модуля Base.

7.2.6.3. Приостановка исполняемого экземпляра модели процесса

Для приостановки исполняемого экземпляра модели процесса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Cockpit** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Processes** (1, рисунок 234) и нужную модель процесса (2, рисунок 234).

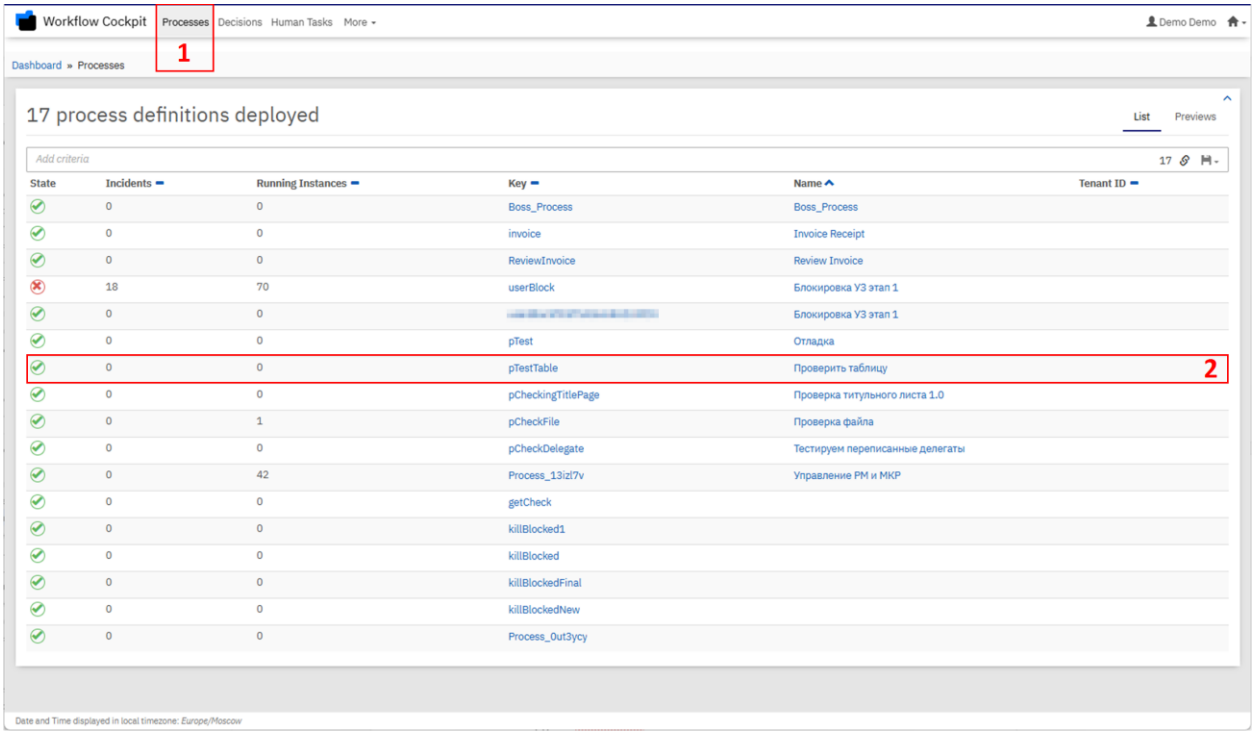


Рисунок 234 – Выбор модели процесса

3. На вкладке **Process Instances** выберите нужный исполняемый экземпляр модели процесса (рисунок 235).

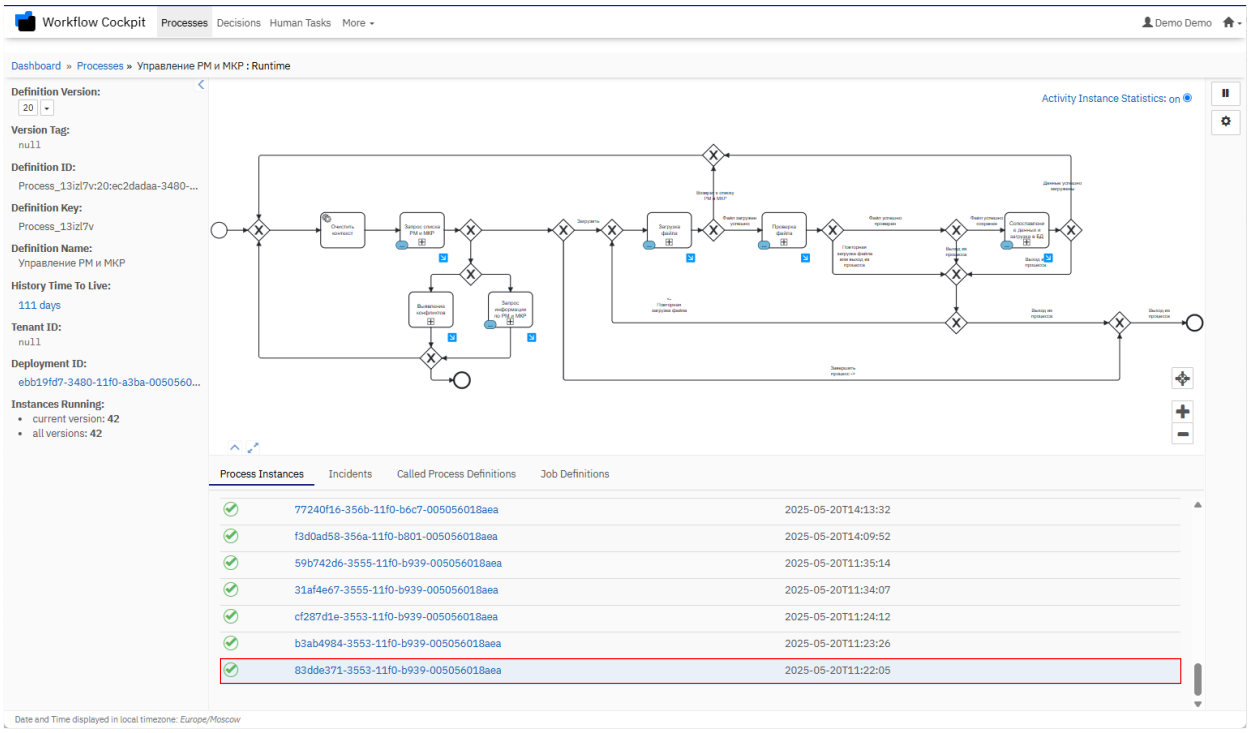


Рисунок 235 – Выбор исполняемого экземпляра модели процесса

4. Нажмите на  (рисунок 236). Далее в всплывающем окне нажмите на **Suspend** (рисунок 237) и убедитесь в появления сообщения о приостановке исполняемого экземпляра модели процесса (рисунок 238).

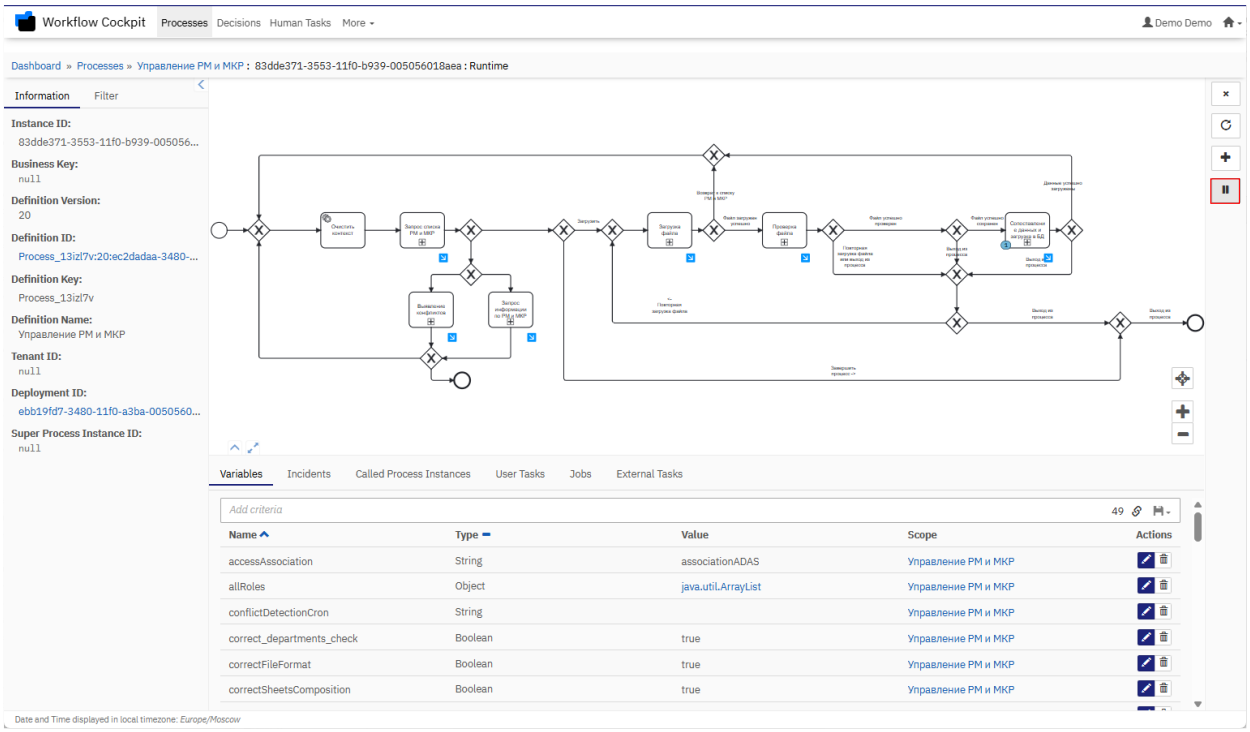


Рисунок 236 – Инициализация приостановки исполняемого экземпляра модели процесса

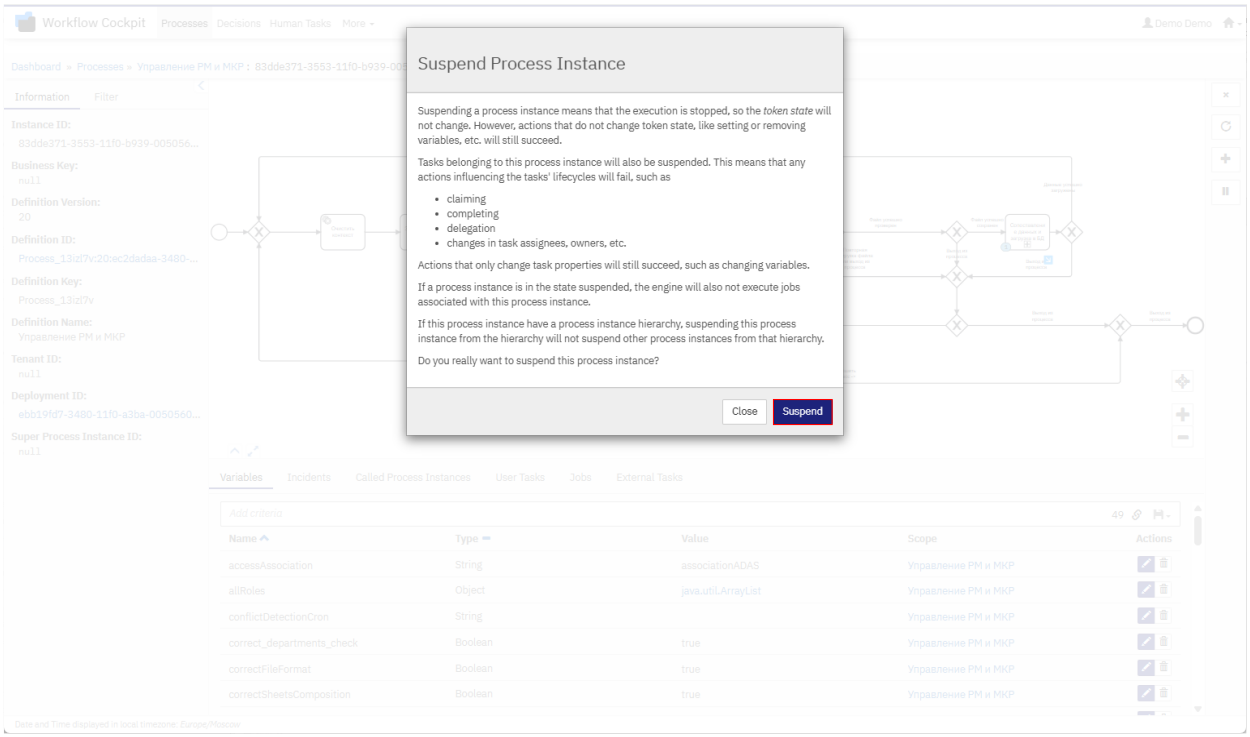


Рисунок 237 – Подтверждение приостановки исполняемого экземпляра модели процесса

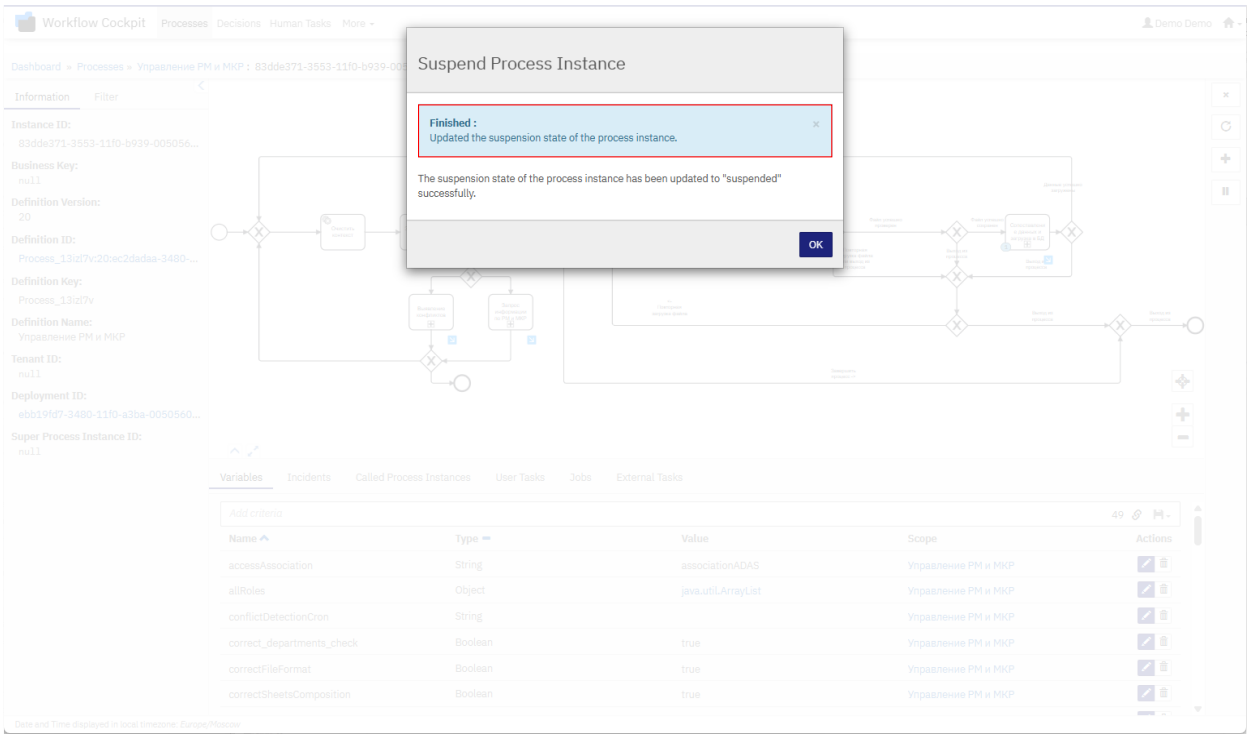


Рисунок 238 – Сообщение об успешной приостановке исполняемого экземпляра модели процесса

7.2.6.4. Возобновление приостановленного экземпляра модели процесса

Для возобновления приостановленного экземпляра модели процесса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Cockpit** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Processes** (1, рисунок 239) и нужную модель процесса (2, рисунок 239).

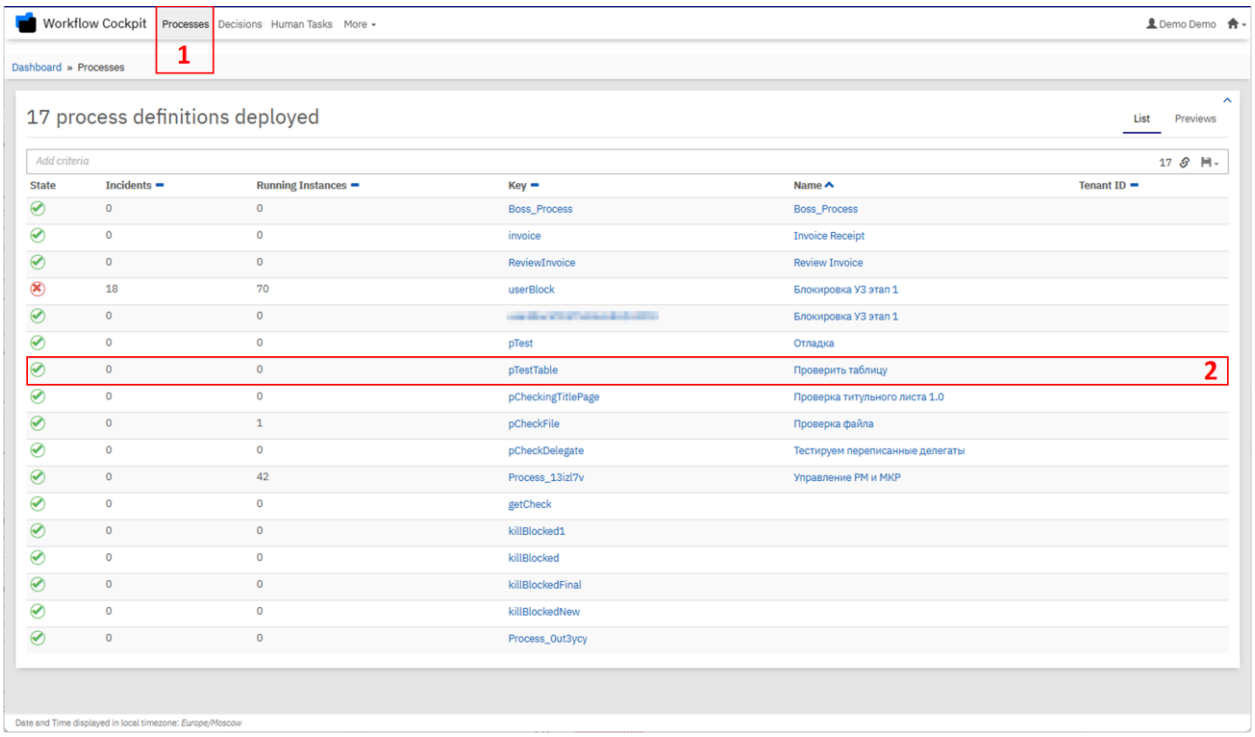


Рисунок 239 – Выбор модели процесса

3. На вкладке **Process Instances** выберите нужный приостановленной экземпляр модели процесса (рисунок 240).

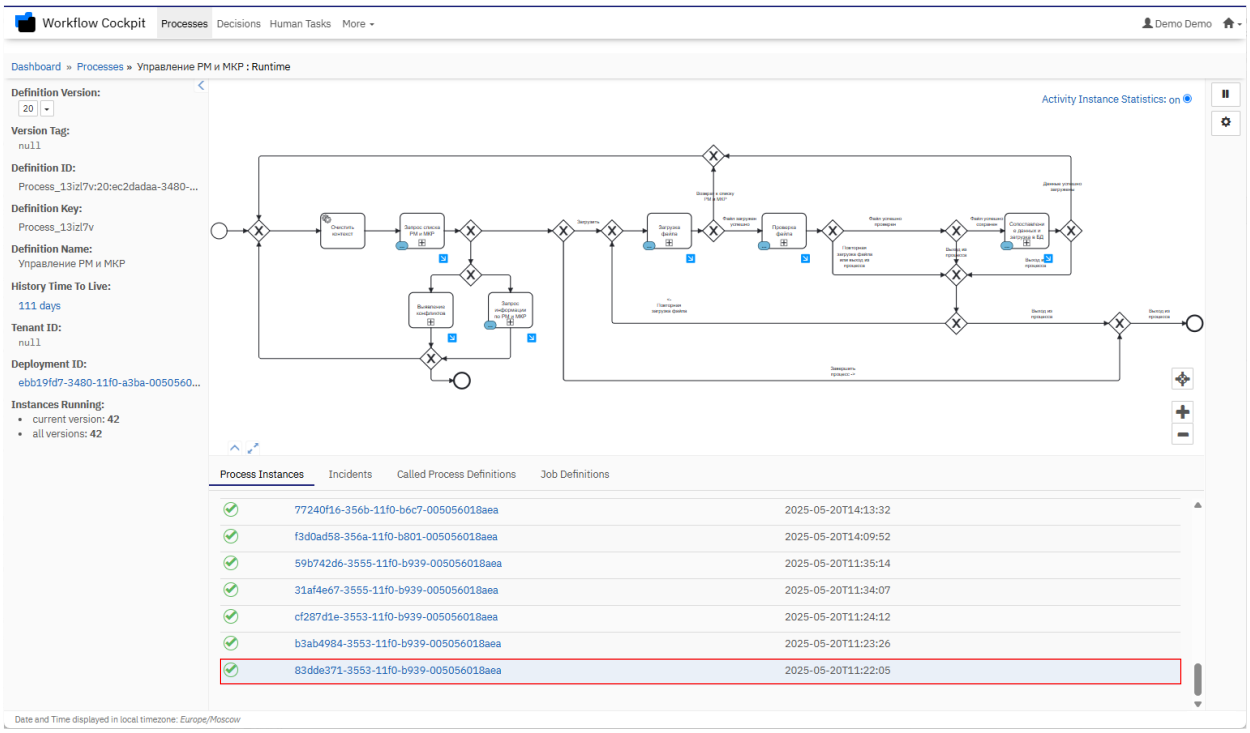


Рисунок 240 – Выбор приостановленного экземпляра модели процесса

4. Нажмите на  (рисунок 241). Далее в всплывающем окне нажмите на **Activate** (рисунок 242) и убедитесь в появления сообщения о возобновлении приостановленного экземпляра модели процесса (рисунок 243).

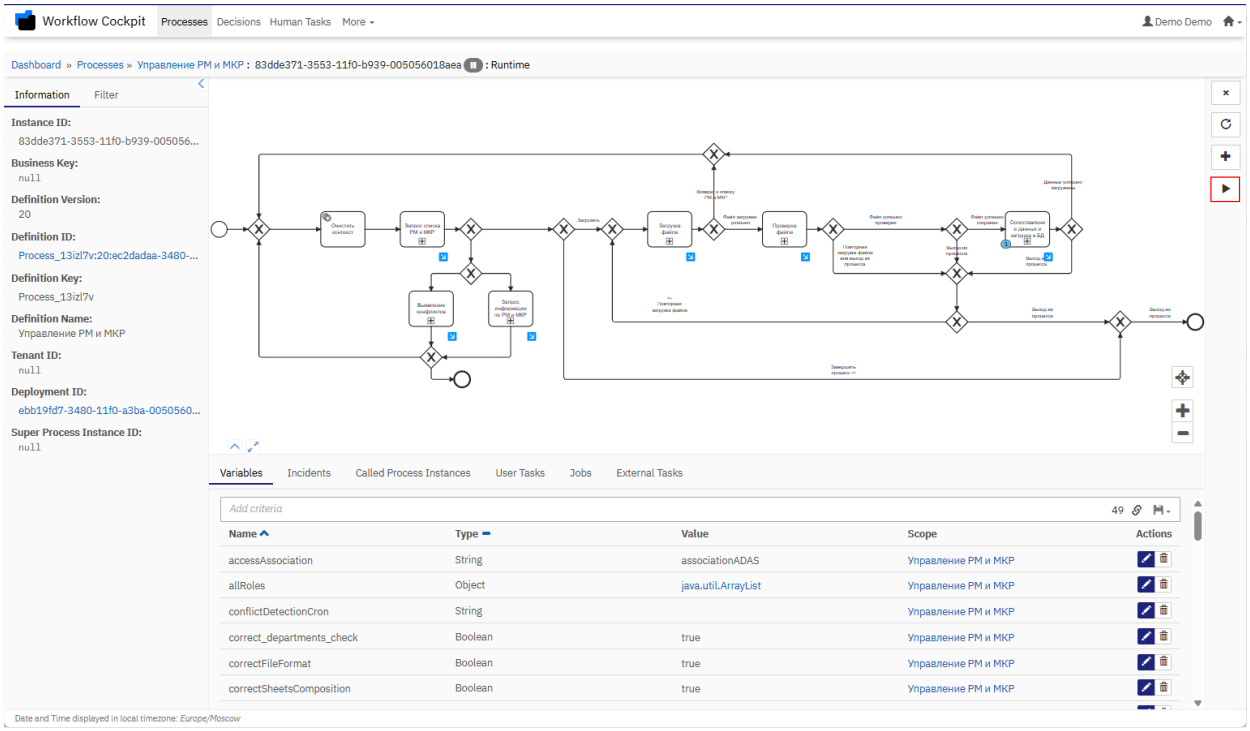


Рисунок 241 – Инициализация возобновления приостановленного экземпляра модели процесса

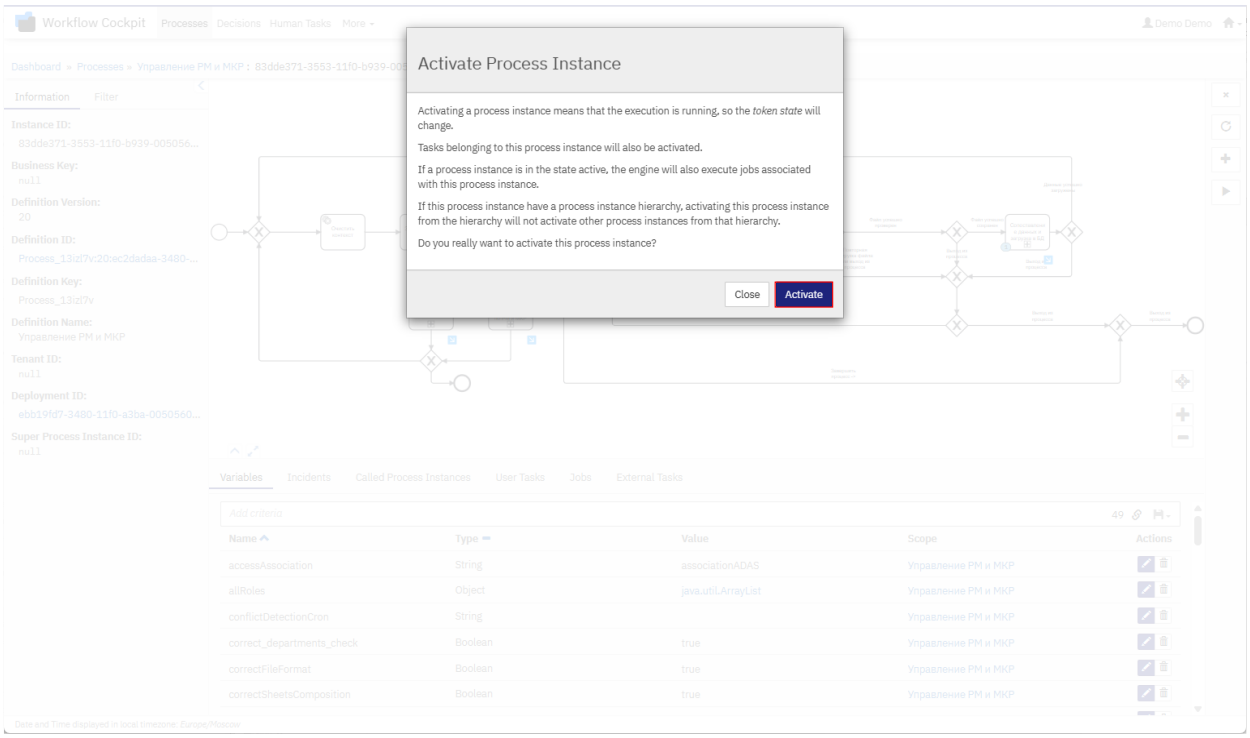


Рисунок 242 – Подтверждение возобновления приостановленного экземпляра модели процесса

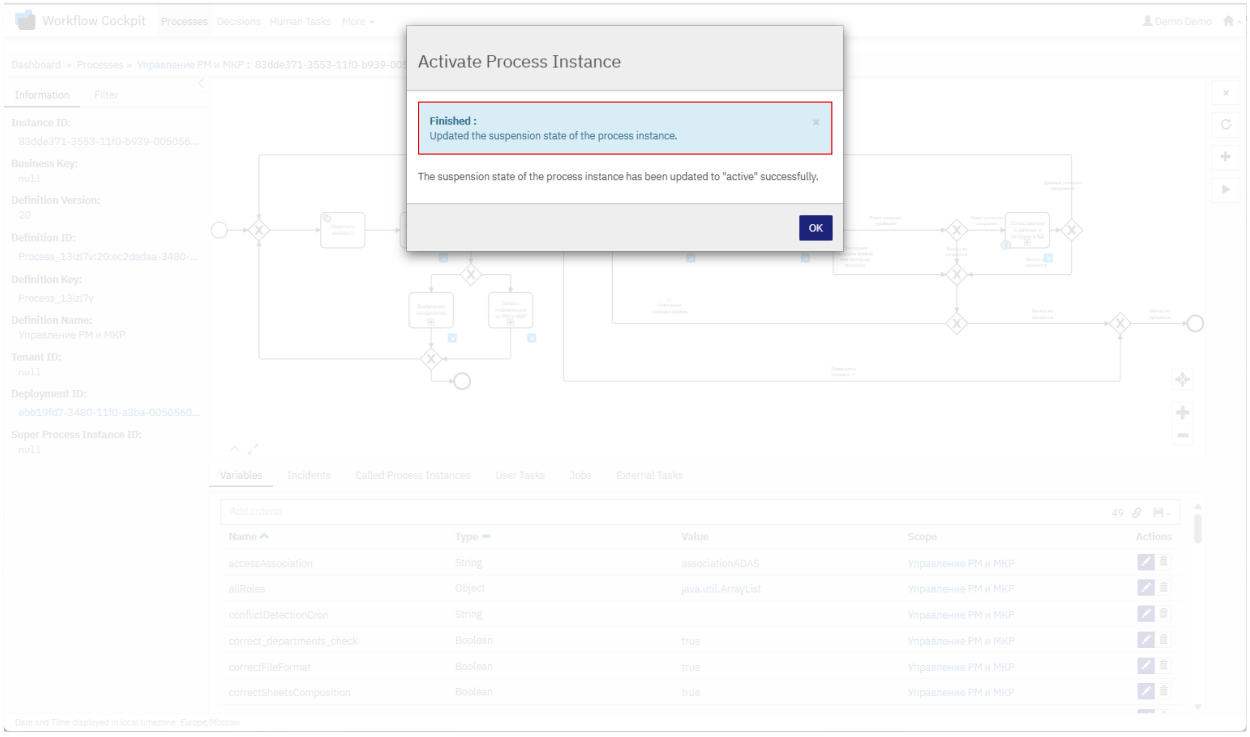


Рисунок 243 – Сообщение об успешном возобновлении приостановленного экземпляра модели процесса

7.2.6.5. Полная остановка и удаление исполняемого экземпляра модели процесса

Для полной остановки и удаления исполняемого экземпляра модели процесса выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Cockpit** (подробнее см. в разделе 7.2.1.3).
2. Выберите **Processes** (1, рисунок 244) и нужную модель процесса (2, рисунок 244).

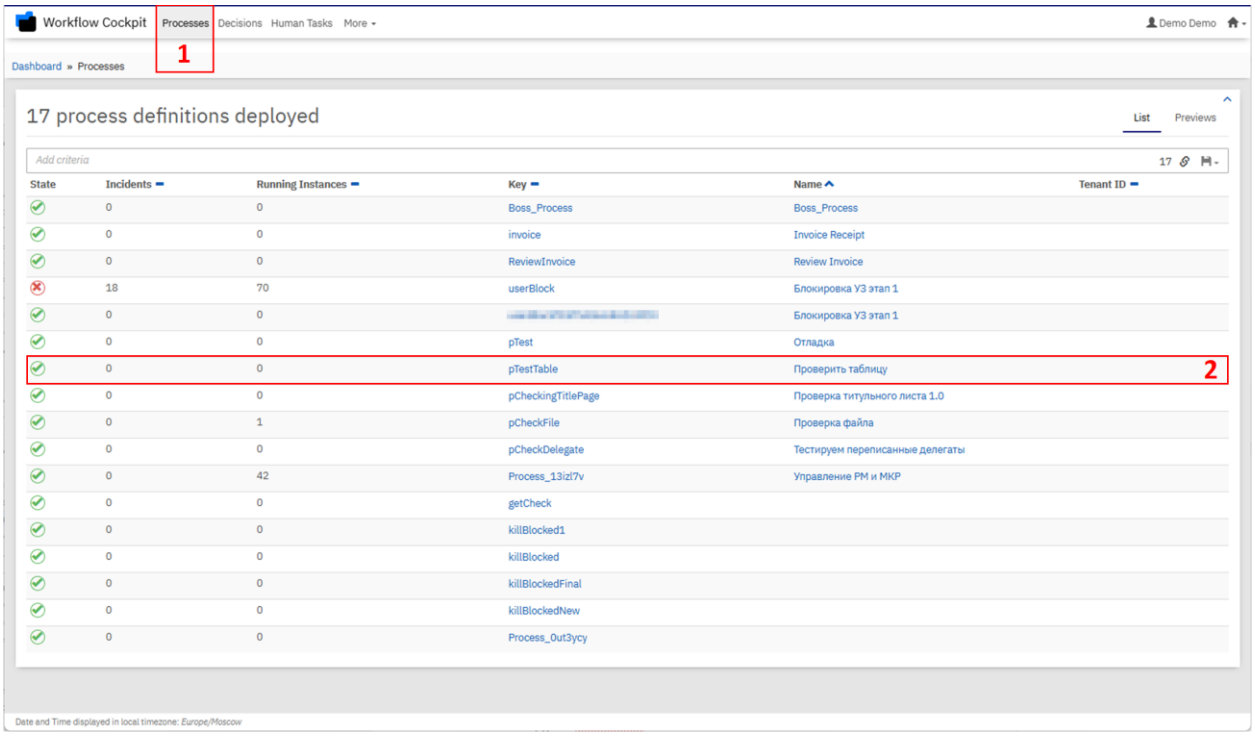


Рисунок 244 – Выбор модели процесса

3. На вкладке **Process Instances** выберите нужный исполняемый экземпляр модели процесса (рисунок 245).

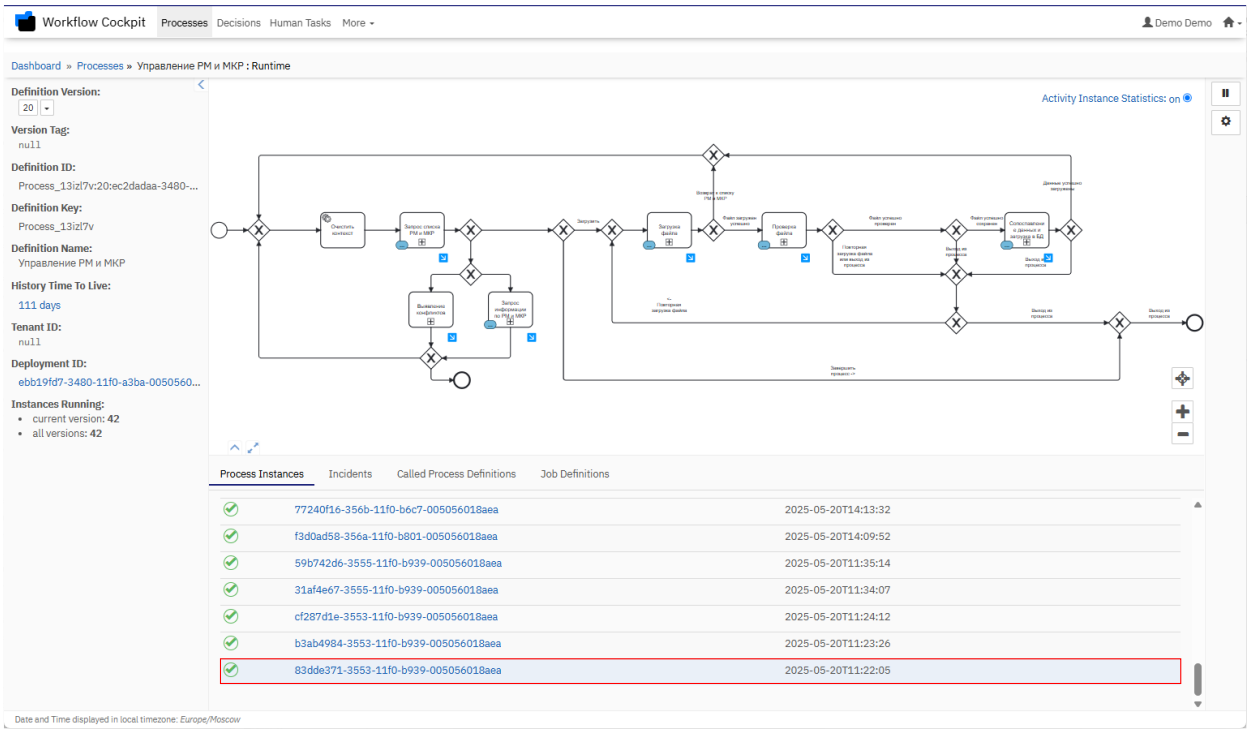


Рисунок 245 – Выбор исполняемого экземпляра модели процесса

4. Нажмите на  (рисунок 246). Далее в всплывающем окне нажмите на **Delete Process Instance** (рисунок 247) и убедитесь в появления сообщения об удалении исполняемого экземпляра модели процесса (рисунок 248).

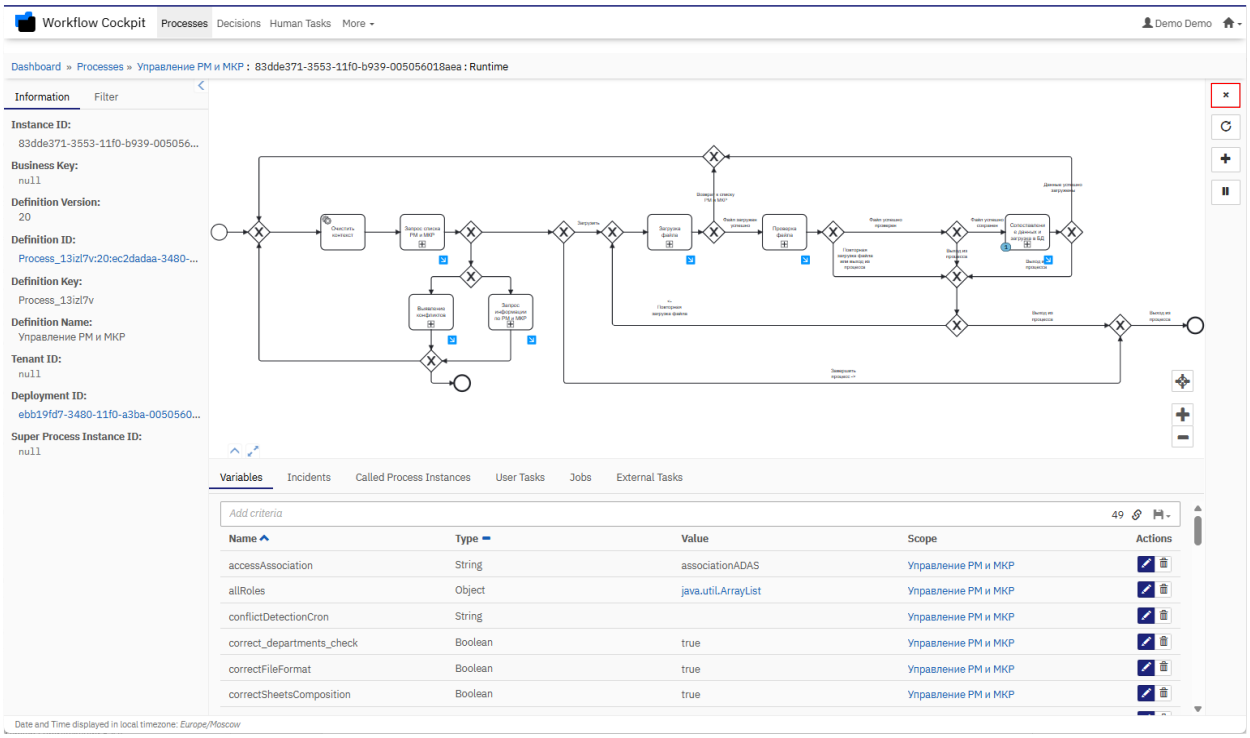


Рисунок 246 – Инициализация удаления исполняемого экземпляра модели процесса

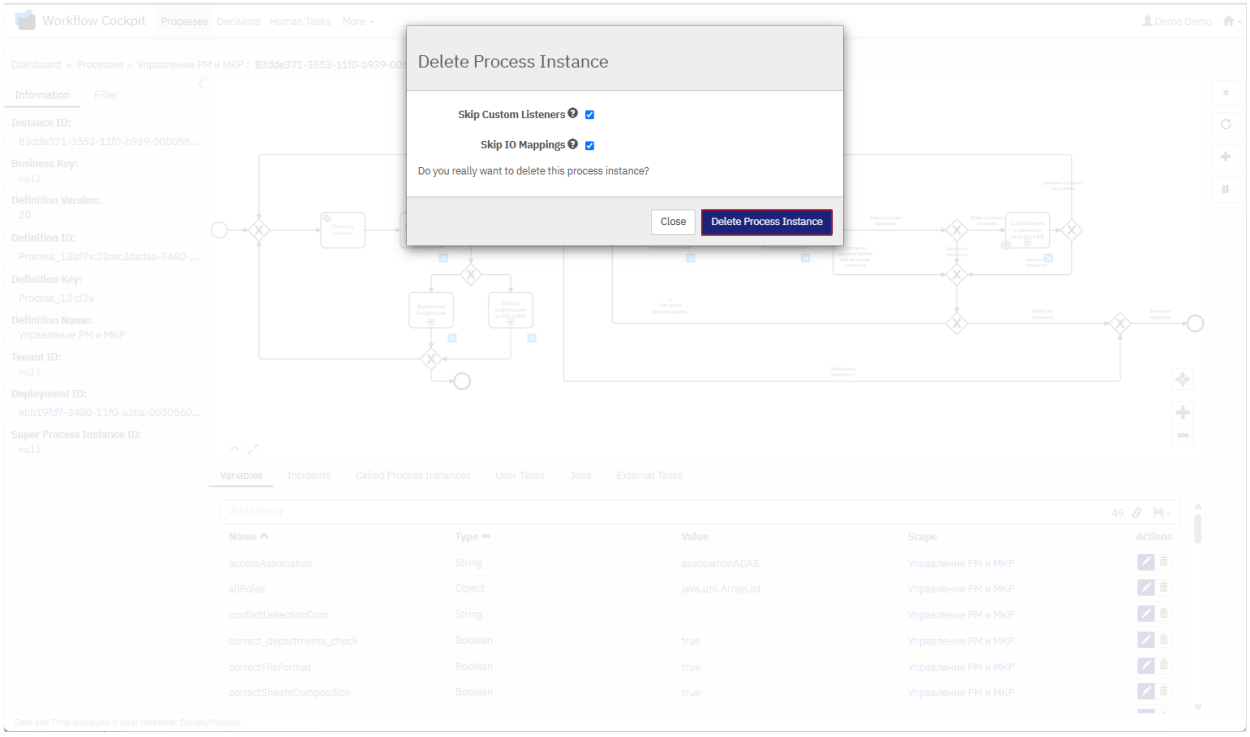


Рисунок 247 – Подтверждение удаления исполняемого экземпляра модели процесса

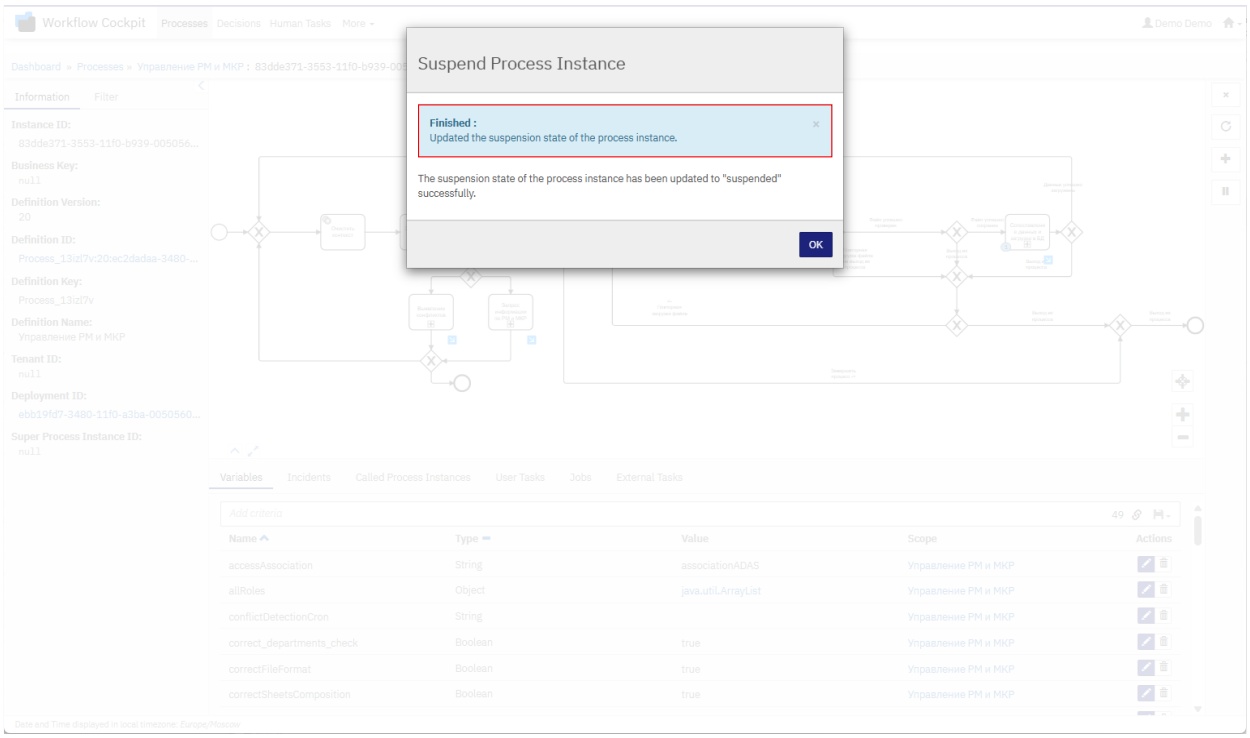


Рисунок 248 – Сообщение об успешном удалении исполняемого экземпляра модели процесса

7.2.6.6. Просмотр расширенной истории исполнения экземпляров модели процесса

Просмотр полной истории исполнения экземпляров моделей процессов осуществляется через подключения к серверу БД компонента Workflow Management. Сама история хранится в таблице **act_hi_procinst**. Она содержит записи о когда-либо созданных экземплярах моделей процессов, включая: от какой модели они произошли, время начала их исполнения, время конца их исполнения, время их удаления, общее время их существования, назначенного пользователя и их статус.

Для просмотра расширенной истории исполнения экземпляров модели процессов выполните следующие шаги:

1. Подключитесь к мастер-ноде серверов БД компонента Workflow Management.

2. Войдите в оболочку командной строки компонента PostgreSQL:

```
psql --host=<host> -U postgres -d camunda -W
```

3. Получите расширенную историю исполнения экземпляров моделей процессов, выполнив следующий SQL запрос:

```
SELECT * FROM act_hi_procinst limit 500;
```

Для получения расширенной истории исполнения экземпляров моделей процессов для конкретной модели процесса выполните следующий SQL запрос:

```
SELECT * FROM act_hi_procinst where proc_def_key_='<key модели процесса>' limit 500;
```

Пример истории исполнения экземпляров моделей процессов представлен на рисунке 249.

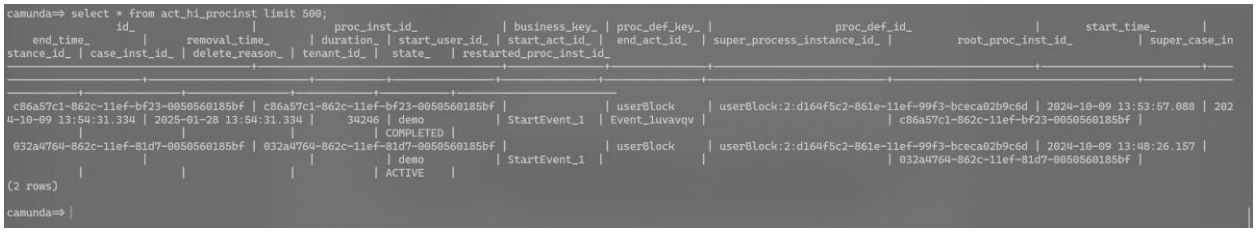


Рисунок 249 – Пример истории исполнения экземпляров моделей процессов

7.2.7. Управление пользовательскими задачами

Управление пользовательскими задачами описано в Руководстве пользователя для модуля Base.

8. МОНИТОРИНГ СОСТОЯНИЯ КОМПОНЕНТОВ

8.1. Просмотр состояния компонента Provisioning Management

Просмотреть работоспособность службы можно командой:

```
systemctl status idmcae-pm.service
```

Результат должен содержать строку

```
Active: active (running)
```

8.2. Просмотр состояния компонента Workflow Management

Просмотреть различные метрики компонента Workflow Management можно через веб-интерфейс.

8.2.1. Просмотр метрик исполнения процессов и принятия решений

На странице просмотра метрик исполнения процессов и принятия решений доступна соответствующая статистика за последние 12 месяцев как в виде гистограммы, так и в виде таблицы.

Для просмотра метрик исполнения процессов и принятия решений выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **System** (1, рисунок 250) нажмите на **Execution Metrics** (2, рисунок 250).

Описание используемых обозначений представлено ниже:

- **PI** – общее количество исполненных экземпляров моделей процессов;

- **DI** – общее количество исполненных экземпляров моделей принятия решений;
- **TU** – общее количество созданных пользовательских задач.

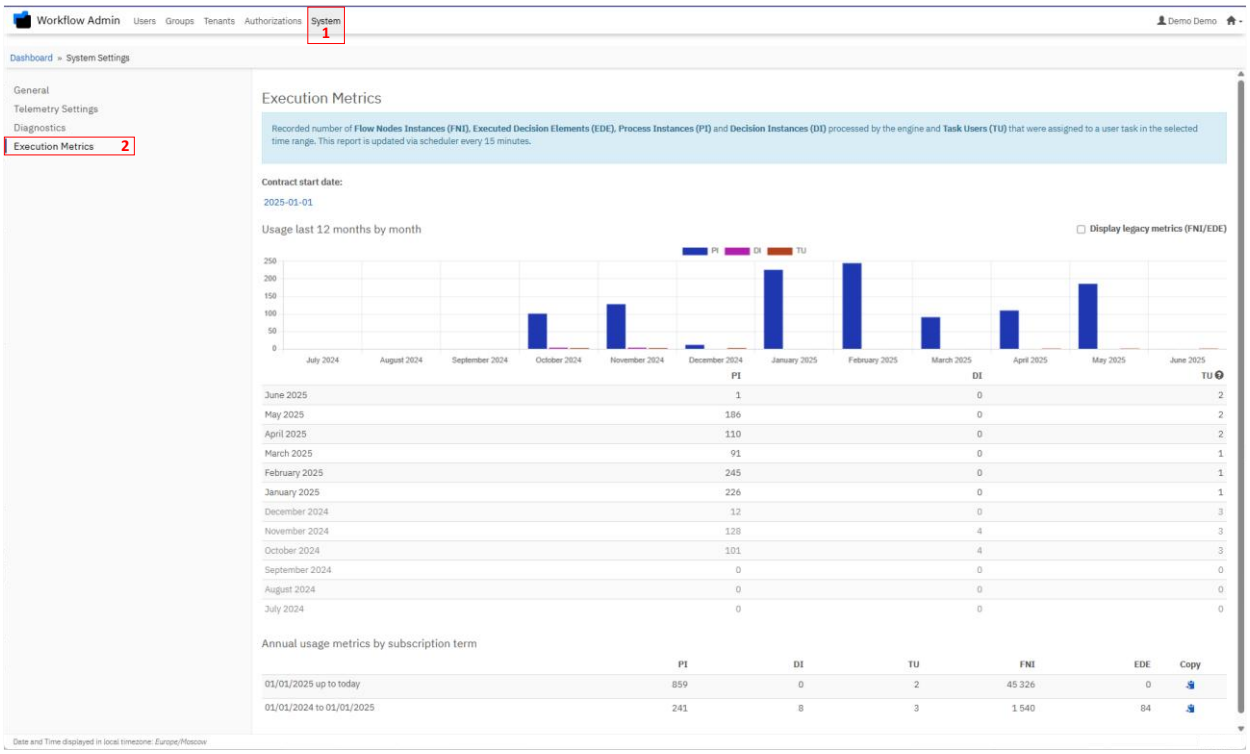


Рисунок 250 – Метрики исполнения процессов и принятия решений

8.2.2. Просмотр состояния движка

Для просмотра состояния движка выполните следующие шаги:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **System** (1, рисунок 251) нажмите на **General** (2, рисунок 251).

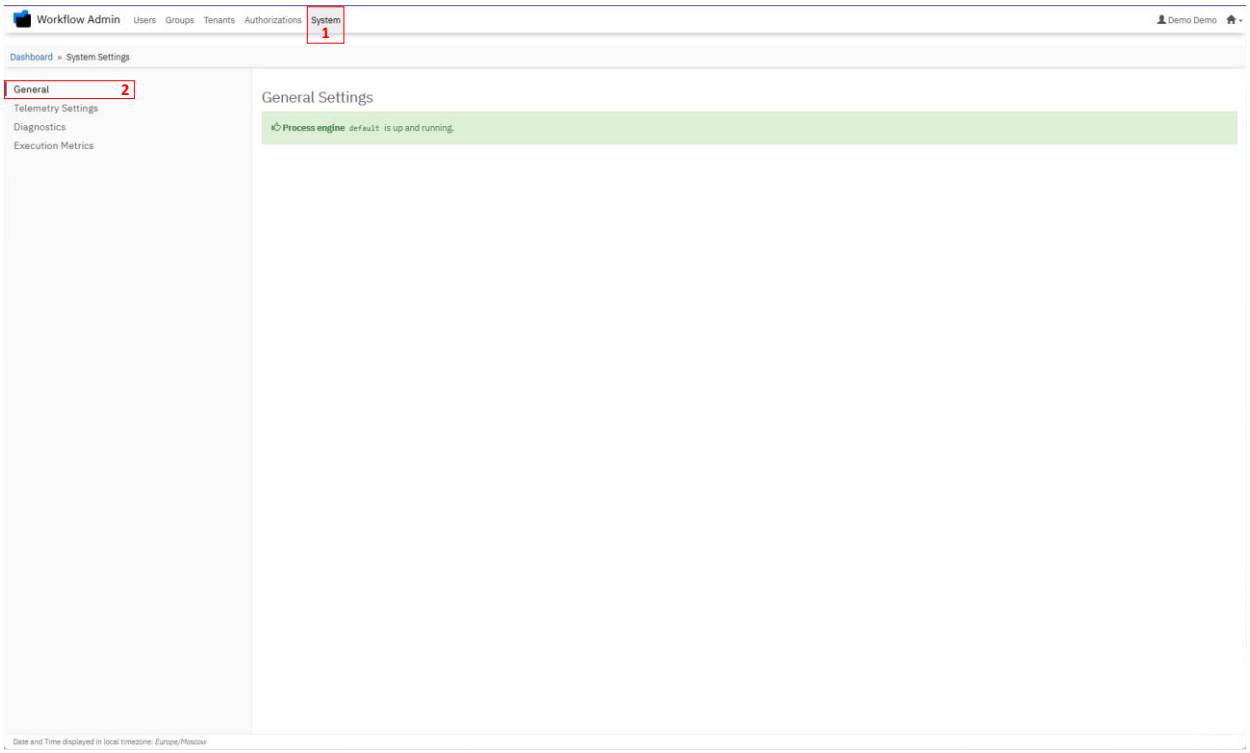


Рисунок 251 – Состояние движка

8.2.3. Просмотр диагностических данных

На странице просмотра диагностических данных представлена следующая информация:

- используемый сервер БД и его версия. Параметр *database* в JSON-описании диагностических данных;
- версия сборки компонента Workflow Management. Параметр *product - version* в JSON-описании диагностических данных;
- используемая версия JDK. Параметр *jdk - version* в JSON-описании диагностических данных;
- используемые внутренние интеграции. Параметр *camunda-integration* в JSON- описании диагностических данных;

- дополнительные метрики, не отображаемые в разделе 8.2.1.

Для просмотра диагностических данных выполните следующие действия:

1. Войдите в веб-интерфейс компонента Workflow Management и выберите раздел **Admin** (подробнее см. в разделе 7.2.1.3).
2. На вкладке **System** (1, рисунок 252) нажмите на **Diagnostics** (2, рисунок 252).

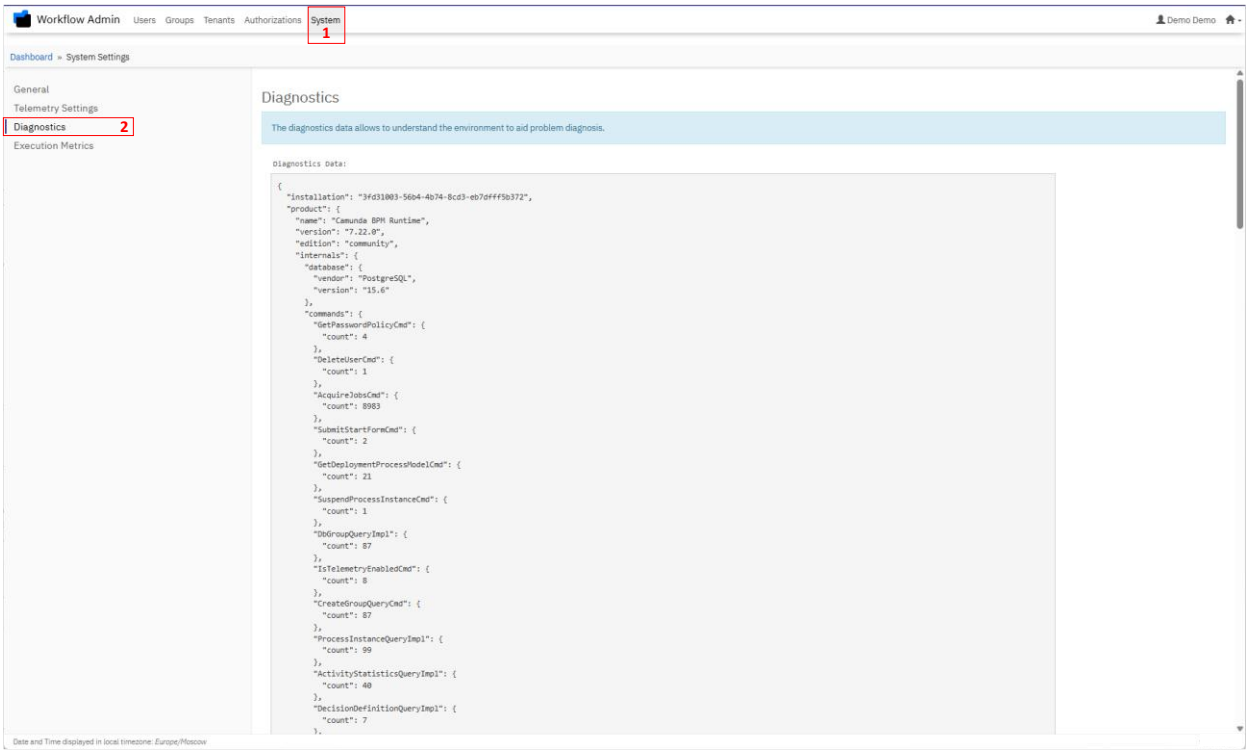


Рисунок 252 – Диагностические данные

8.2.4. Просмотр дополнительных метрик

Бóльшая часть метрик недоступна для просмотра в пользовательском интерфрейсе. Вместо этого администратору необходимо выполнить ручное подключение к БД компонента Workflow

Management путём подключения к мастер-ноде кластера БД. Сами метрики хранятся в следующих таблицах:

- *act_ru_meter_log*: содержит более подробную информацию о метриках из раздела 8.2.3;
- *act_ru_task_meter_log*: содержит более подробную информацию о пользовательских задачах.

Для получения необходимых метрик выполните следующие шаги:

1. Подключитесь к мастер-ноде серверов БД.
2. Войдите в оболочку командной строки компонента PostgreSQL:

```
psql --host=<host> -U postgres -d camunda -W
```

3. Получите необходимые метрики, выполнив следующий SQL запрос:

```
SELECT * FROM <наименование таблицы с метриками> limit 500;
```

9. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ И КОНФИГУРАЦИОННЫХ ФАЙЛОВ

9.1. Создание резервной копии

Для создания резервной копии выполните команду

```
pg_dump [connection-option][parameter][db_name]> [catalog_for_backup_postgres_database]
```

где:

- `connection-option` – параметры подключения к БД. Их можно выбрать из нескольких вариантов:
  - `-d [db_name]` или `--dbname=[db_name]` – имя БД;
  - `-h [server_name]` или `--host=[server_ name]` – имя сервера;
  - `-p [port]` или `--port=[port]` – порт для подключения;
  - `-U [username]` или `--username=[username]` – имя пользователя;
- `parameter` – параметры создания резервной копии;
- `db_name` – имя БД;
- `catalog_for_backup_postgres_database` – путь к каталогу, в который нужно сохранить дамп.

9.2. Восстановление из резервной копии

Для восстановления БД из бэкапа войдите на лидер-узел кластера patroni и на нём выполните команду

```
pg_restore [connection-option] [parameter] [dump_name]
```

где:

- `connection-option` – параметры подключения к БД. Их можно выбрать из нескольких вариантов:
  - `-h [server_name]` или `--host=[server_ name]` – имя сервера,
  - `-p [port]` или `--port=[port]` – порт для подключения,
  - `-U [username]` или `--username=[username]` – имя пользователя,
  - `-w` или `--no-password` – отключить запрос пароля,
  - `-W` или `--password` – включить запрос пароля,
  - `--role=[username]` – задать имя роли пользователя;
- `parameter` – параметры создания резервной копии;
- `dump_name` – имя дампа БД.

10. СПРАВОЧНАЯ ИНФОРМАЦИЯ

10.1. Просмотр и расположение конфигурационных файлов

Информация о конфигурационных файлах компонентов модуля Base с их описанием и назначением представлена в таблице 8.

Таблица 8 – Информация о конфигурационных файлах

№	Компонент	Имя файла, включая путь	Описание, включая назначение файла
1.	Provisioning Management	/opt/idmcae/base/var/config.yml	Конфигурационный файл компонента, содержащий параметры подключения к репозиторию и вторичные настройки
2.	Workflow Management	/opt/idmcae/workflow/configuration/production.yml	

10.2. Расположение и назначение журналов

Информация о расположении и назначении журналов компонентов модуля Base с их описанием и назначением представлена в таблице 9.

Таблица 9 – Информация о журналах

№	Компонент	Имя файла, включая путь	Описание, включая назначение файла
1.	Provisioning Management	opt/idmcae/base/var/logs/*.log	Журнал событий
2.	Workflow Management	• /var/log/messages • /opt/idmcae/workflow/ logs/*.log	

11. ДИАГНОСТИКА И РЕШЕНИЕ ПРОБЛЕМ

11.1. Сообщения об ошибках и результаты операций

Каждая выполняемая в компоненте Provisioning Management операция записывает важные моменты во время обработки в результат операции. Результаты операции являются иерархической структурой (рисунок 253). Если сообщение верхнего уровня не предоставляет информацию о проблеме, необходимо проверять вложенные операции до тех пор, пока не будет найдена первопричина проблемы.

Рисунок 253 – Иерархическая структура сообщений об ошибках

Каждый результат операции имеет свой статус. Возможные статусы с их описанием представлены в таблице 10.

Таблица 10 – Статусы операций

№	Статус	Описание
1.	SUCCESS	Операция завершена успешно, ошибки отсутствуют
2.	WARNING	Операция завершена, но есть предупреждения
3.	PARTIAL_ERROR	Некоторые части операции завершились успешно, другие части операции привели к ошибке. Однако операция не была остановлена, и её выполнение продолжилось, несмотря на ошибки. Частичная ошибка часто указывается в том случае, когда модификация пользователя проходит успешно, но модификация УЗ не удаётся
4.	FATAL_ERROR	Операция была прервана из-за ошибки, которая не позволила завершить операцию
5.	HANDLED_ERROR	Операция завершена. Во время выполнения операции произошла ошибка. Однако ошибка была устранена, и IDM CAE смогла компенсировать её последствия. Результаты должны быть эквивалентны успешному выполнению операции
6.	NOT_APPLICABLE	Операция не была начата, поскольку она не применима к входным данным
7.	IN_PROGRESS	Операция находится в процессе выполнения. Этот статус характерен для фоновых операций. Также может использоваться для операций, ожидающих внешнего события, например, операций утверждения или повторных попыток выполнения операции.
8.	UNKNOWN	Статус операции неизвестен. Этот код состояния может возникнуть при особых обстоятельствах. Например, если из-за ошибки в IDM CAE или коннекторе операция находится в неопределенном состоянии или если возникла непредвиденная ошибка и не была обработана должным образом

11.2. Логирование

Логирование предоставляет информацию обо всех важных событиях, происходящих в IDM CAE.

По умолчанию в логи записывается небольшое количество информации. IDM CAE позволяет перенастроить систему протоколирования так, чтобы она фиксировала больше подробностей. Протоколирование может быть глубоким и содержать тонкие детали операций в IDM CAE.

В домашнем каталоге IDM CAE находится подкаталог *logs*, в котором находятся файлы логов IDM CAE. Обычно их несколько:

- *midpoint.log* – основной лог-файл. В него записываются почти все сообщения логов IDM CAE;
- *midpoint.out* – файл, в который записывается стандартный вывод процессов IDM CAE. Обычно он содержит небольшое количество событий, происходящих до запуска и после остановки.

Если в одном лог-файле накапливается слишком много данных, он переименовывается, а старые файлы удаляются. В противном случае лог-файлы заполнят все доступное дисковое пространство.

Сообщения логов имеют структурированный формат (рисунок 254). Описание полей логов IDM CAE приведено в таблице 11.

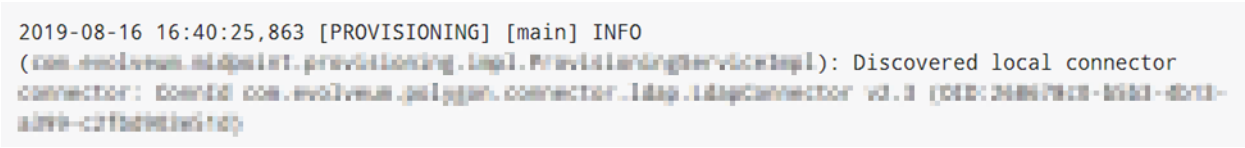


Рисунок 254 – Пример сообщения логов

Таблица 11 – Виды полей логов IDM CAE

№	Поле	Описание	Пример
1.	Timestamp	Временная метка момента, в который было сгенерировано сообщение	2019-08-16 16:40:25,863
2.	Component name	Имя элемента, в котором возникло сообщение	[PROVISIONING]
3.	Thread name	Имя потока, в котором возникло сообщение	[main]
4.	Log level	Уровень логирования	INFO

№	Поле	Описание	Пример
5.	Logger name	Обычно это имя пакета или полное имя класса, породившего сообщение. Могут существовать специализированные регистраторы с особыми именами	(...):
6.	Message	Содержание сообщения лог-файла. Обычно это однострочное сообщение, но могут встречаться и многострочные	Discovered local connector...

Поскольку IDM CAE использует параллельную обработку, имя потока может быть использовано для отсеивания сообщений, относящихся к одной операции. При необходимости формат логов может быть настроен.

Управление гранулярностью протоколирования может осуществляться на двух уровнях:

- **уровень логов**: определяет степень подробностей, которые записываются в логи. Уровень *Информация (INFO)* будет регистрировать только важные события. На уровне *Отслеживание (TRACE)* будет регистрироваться информация, в первую очередь необходимая для разработчиков. Это позволяет контролировать глубину протоколирования;
- **уровень пакета**: определяет то, какие компоненты IDM CAE будут записывать в логи свои сообщения. Установка уровня логов для конкретного пакета также позволяет вести логи для всех подпакетов и классов. Это позволяет контролировать широту протоколирования.

Настройка протоколирования представляет собой комбинацию уровней пакета и логов. Таким образом можно получить подробное протоколирование от одного пакета, а протоколирование других пакетов оставить на грубом уровне.

Каждый уровень имеет точное определение количества предоставляемых подробностей (таблица 12).

Таблица 12 – Уровни логов IDM CAE

№	Уровень	Обстоятельства	Описание
1.	FATAL	Критические ошибки, сбой или прекращение работы IDM CAE	IDM CAE больше не может работать
2.	ERROR	Ошибка, серьезно влияющая на работу IDM CAE, но позволяющая ей восстановиться	Обычно вызвана ошибками в данных, ошибками сети и т. д. Требуется ручное вмешательство администратора.
3.	WARNING	Подозрительная ситуация. IDM CAE может работать нормально, но может существовать скрытая или временная проблема, или признак будущей ошибки	Важные сообщения, которые не должны возникать в хорошо сконфигурированных и настроенных системах. Немедленные действия обычно не требуются
4.	INFO	Важные изменения в состоянии IDM CAE, запуск / остановка важных системных задач и т. д.	Эти события обычно происходят практически во всех работающих системах
5.	DEBUG	Сообщения об исполнении, изменениях состояния, об оценке выражений и аналогичные сообщения для администратора	Этот уровень журнала предназначен для администраторов для отладки конфигурации. Предоставляет сообщения, которые могут быть использованы для поиска проблем с конфигурацией
6.	TRACE	Тонкие сообщения о деталях выполнения	Этот уровень журнала предоставляет много данных и подробностей. Позволяет разработчикам находить ошибки в производственных системах. Предоставляет администраторам ценную информацию при устранении сложных проблем.

Уровни логов IDM CAE организованы в виде иерархии. Если для конкретного пакета установлен уровень *Отладка (DEBUG)*, он

также будет регистрировать все сообщения с более высокими уровнями. Обычно при поиске ошибки начинают с уровня логов *Отладка*.

Имена пакетов протоколирования напрямую заимствованы из пакетов и классов Java. Имена пакетов могут быть использованы для управления протоколированием отдельных частей IDM CAE (таблица 13).

Таблица 13 – Виды пакетов протоколирования

№	Часть IDM CAE	Имя пакета	Описание
1.	GUI	com.evolveum.midpoint.gui com.evolveum.midpoint.web	Веб- интерфейс, управляет взаимодействием с пользователем
2.	Model	com.evolveum.midpoint.model	Реализует большую часть логики IDM CAE (обработка пользователей, RBAC, организационная структура, политики и т. д.)
3.	Provisioning	com.evolveum.midpoint.provisioning	Связь с целевыми ИС. Отвечает за связь с коннекторами, управление теневыми объектами, управление живой синхронизацией, ручными коннекторами, повторами операций, управление ресурсами и коннекторами и т. д.
4.	ConnId	org.identityconnectors. framework	Фреймворк коннекторов ConnId. Отвечает за запуск коннекторов и передачу операций коннекторам
5.	Repository	com.evolveum.midpoint. repo	Хранит объекты IDM CAE в базе данных. Управляет задачами, обработкой авторизации, оценкой выражений и т. д.
6.	Schema	com.evolveum.midpoint.schema	Определение модели данных IDM CAE и различных утилит
7.	Prism	com.evolveum.midpoint.prism	Библиотека, осуществляющая разбор и хранение объектов в форматах представления данных (XML / JSON / YAML)

При настройке протоколирования рекомендуется действовать следующим образом:

1. Включите уровень *Отладка (DEBUG)* для всей части IDM CAE. Журнал данных не должен быть слишком подробным.
2. Изучите лог-файл и выясните, в каком месте возникает отслеживаемое событие. Обратите внимание на имена пакетов, используемых в сообщениях;
3. Установите уровень *Отслеживание (TRACE)* только для тех пакетов или классов, в которых содержится информация об отслеживаемом событии.
4. По желанию отключите пакеты, которые отображают слишком много данных, установив для них уровень логов *Информация (INFO)*.

Установка уровня логов *Отладка (DEBUG)* на *clockwork*, *projector* или *change executor* подходит для диагностики проблем, связанных с сопоставлениями и назначениями.

Логи операций *ConnId* подходят для диагностики проблем, связанных с коннекторами.

11.3. Аудит

Назначение механизма аудита – фиксация всех операций в IDM CAE для целей отчётности.

Механизм аудита записывает все операции в структурированном виде. Аудиторский след можно просмотреть, чтобы убедиться в правильности выполнения операции. Кроме того, в журнал аудита

записываются результаты выполнения операции. Таким образом, аудит может быть быстрым и эффективным способом получения представления об операции в целом.

Аудит может использоваться при изучении массовых операций, например, результатов синхронизации или сверки. Задачи, в которых выполняются эти операции, дают представление о результатах, например, о количестве ошибок. Однако, структура данных задачи не может содержать детали каждой операции. Существуют записи аудита для каждой из этих операций.

Обычно журнал аудита используется для получения обзора ежедневных операций. Например, записи аудита могут предоставлять данные о том, сколько операций было обработано за прошедший день, какие операции были неудачными за последние несколько часов и т.д. Для отображения такой информации существует специальный тип отчёта.

Данные аудита могут также записываться в файлы логов. Это не рекомендуется делать при производственном развёртывании. В этом случае велика вероятность переполнения логов и даже раскрытия конфиденциальных данных. Однако, направление записей аудита в системные логи может создать преимущества. Например, в случае использования подробного отладочного журнала записи аудита будут содержать краткое описание операции и е результат в том же журнале с подробностями. Это облегчает анализ лог-файлов.

Пример сообщения журнала аудита приведён на рисунке 255.

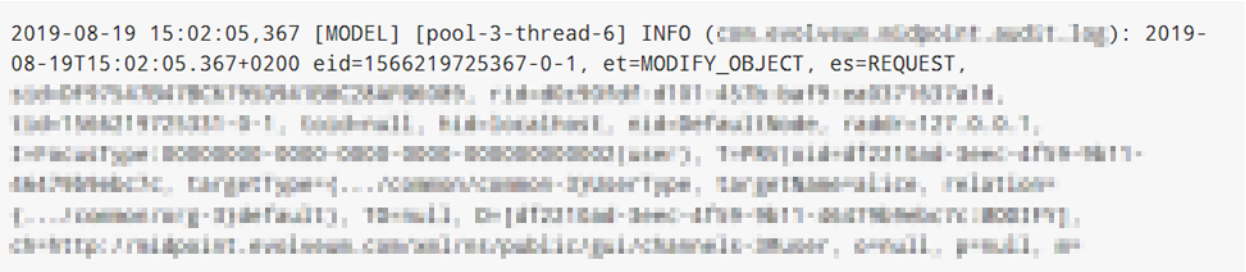


Рисунок 255 – Пример сообщения журнала аудита

12. ОБРАЩЕНИЕ В ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ

Раздел содержит требования к содержимому обращения и его оформлению.

12.1. Порядок подачи обращений в службу технической поддержки

Обращения в службу поддержки компании «ООО «Кросстех Солюшнс Групп» (Вендор) в гарантийных случаях необходимо производить через электронную почту support@ct-sg.ru.

12.2. Требование к содержанию обращения

При подаче обращения через портал технической поддержки для ускорения предоставления решения по обращению необходимо максимально подробно заполнить все поля и приложить файлы с необходимой информацией (логи, скриншоты, другие файлы).

Требования к оформлению обращений:

1. Одно обращение описывает одну проблему, возникшую в процессе работы системы.
2. Наименование обращения кратко описывает имеющуюся проблему.
3. Указан приоритет устранения проблемы:

- критичный - существование дефекта приводит к масштабным последствиям катастрофического характера, например: потеря данных, раскрытие конфиденциальной информации;

- средний - существование дефекта слабо влияет на типичные сценарии работы пользователей, и/или существует обходной путь достижения цели, например: диалоговое окно не закрывается автоматически после нажатия **OK**/**Cancel**;
- низкий - существование дефекта редко обнаруживается незначительным процентом пользователей и (почти) не влияет на их работу, например: опечатка в глубоко вложенном пункте меню настроек.

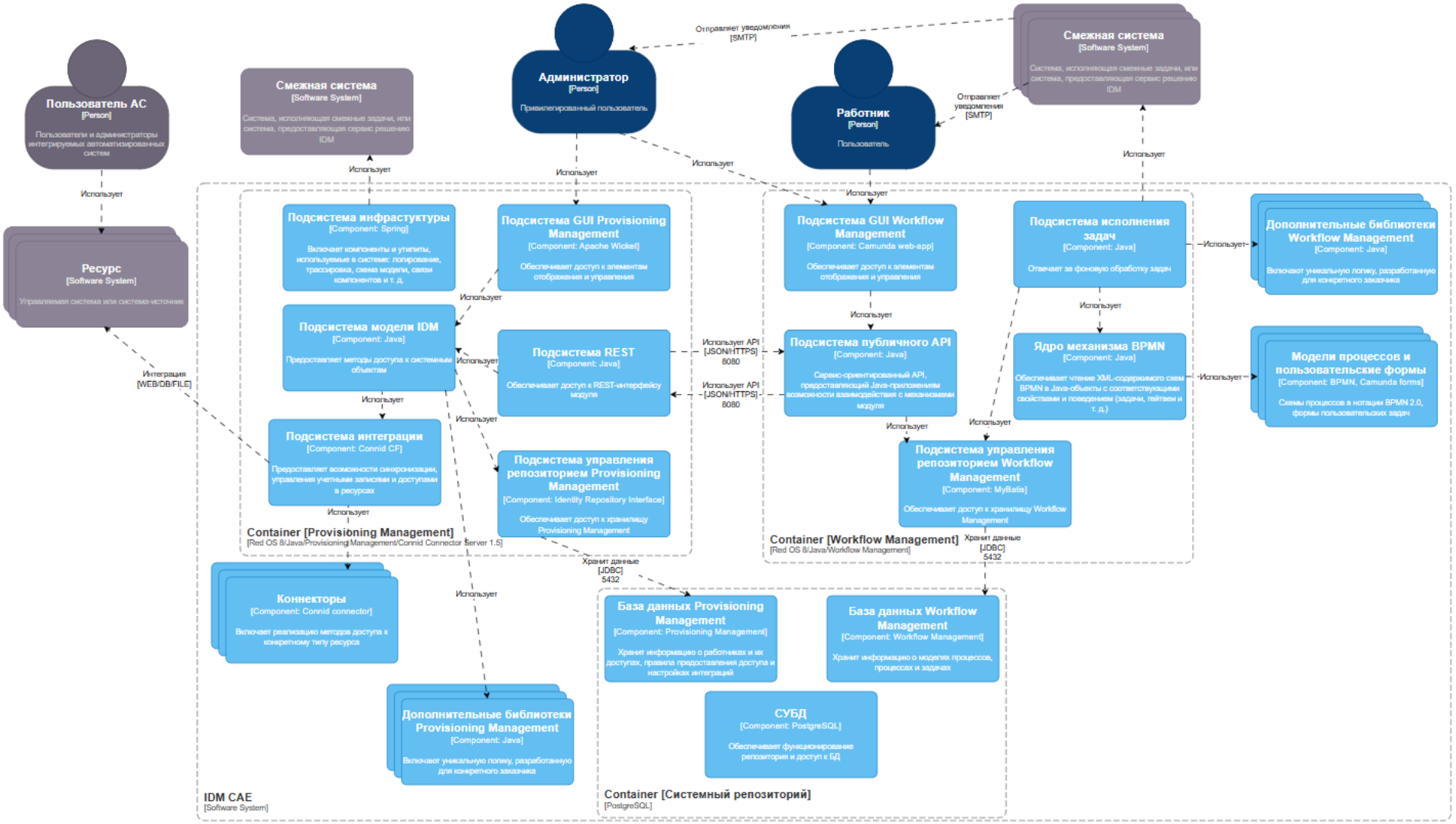
4. Описание проблемы подробное и содержит следующие пункты:

- окружение - версия операционной системы и ее разрядность, версия продукта, дополнительные параметры (браузеры и их версии или приложения и их версии);
- шаги воспроизведения - алгоритм в форме пошаговой инструкции воспроизведения ошибки, где одно действие указано как один шаг;
- ожидаемый результат - описание того, как система должна работать после выполнения шагов, указанных выше;
- фактический результат - описание того, как система работает после воспроизведения вышеуказанной последовательности шагов;

- вложенные файлы - дополнительная информация: скриншоты, текстовые файлы, логи, видео выполняемых действий.

5. Дополнительные параметры: предусловие, постусловие, дополнения.

ПРИЛОЖЕНИЕ 1. АРХИТЕКТУРНАЯ СХЕМА МОДУЛЯ BASE



ПРИЛОЖЕНИЕ 2. КАТЕГОРИИ НАСТРОЙКИ ПРАВ ДОСТУПА КОМПОНЕНТА WORKFLOW MANAGEMENT

Компонент Workflow Management предоставляет возможности для ограничения прав доступа к различным разделам компонента. Подраздел *Authorizations* содержит 19 категорий, для которых можно настроить определенные правила как для групп, так и для пользователей напрямую:

- *Application*: позволяет настроить разграничение доступа к разделам *Tasklist*, *Admin* и *Cockpit*;
- *Authorization*: позволяет настроить разграничение доступа к разделу *Authorization*, в котором настраиваются разграничения прав доступа;
- *Batch*: позволяет настроить разграничение доступа к Batch-операциям, необходимым для множественной выгрузки процессов с целью их асинхронного неблокирующего исполнения;
- *Decision Definition*: позволяет настроить разграничение доступа к подразделу *Decisions* в разделе *Cockpit*;
- *Decision Requirements Definition*: позволяет настроить разграничение доступа к параметру *Decision Requirements Definitio* в категории *Decision Definition*;
- *Deployment*: позволяет настроить разграничение доступа к возможностям развёртывания моделей процессов;
- *Filter*: позволяет настроить разграничение доступа к управлению и использованию поисковых фильтров;

- *Group*: позволяет настроить разграничение доступа к управлению группами;
- *Group Membership*: позволяет настроить разграничение доступа к управлению участниками групп;
- *Historic Process Instance*: позволяет настроить разграничение доступа к просмотру истории исполнения экземпляров моделей процессов;
- *Historic Task Instance*: позволяет настроить разграничение доступа к просмотру истории исполнения пользовательских задач;
- *Operation Log*: позволяет настроить разграничение доступа к просмотру лога операций;
- *Process Definition*: позволяет настроить разграничение доступа к управлению моделями процессов;
- *Process Instance*: позволяет настроить разграничение доступа к управлению исполняемыми экземплярами моделей процессов;
- *System*: позволяет настроить разграничение доступа к системным метрикам компонента;
- *Task*: позволяет настроить разграничение доступа к управлению пользовательскими задачами;
- *Tenant*: позволяет настроить разграничение доступа к управлению локальными тенантами;
- *Tenant Membership*: позволяет настроить разграничение доступа к управлению участниками локальных тенантов;

- *User*: позволяет настроить разграничение доступа к управлению пользователями.

ПРИЛОЖЕНИЕ 3. КОД НАСТРОЙКИ АССОЦИАЦИЙ ДЛЯ РОЛЕЙ

```
            <association>
                <ref>GOK group membership to App Role</ref>
                <inbound>
                    <strength>normal</strength>
                    <channel>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#rec-
onciliation</channel>
                    <expression>
                        <assignmentTargetSearch>
                            <targetType>RoleType</targetType>
                            <filter>
                                <q:equal>
                                    <q:path>identifier</q:path>
                                    <expression>
                                        <script>
                                            <code>
                                               import com.evolveum.midpoint.xml.ns._public.com-
mon.common_3.*


                                                for (a in focus.assignment) {
                                                   _targetType    =    basic.stringify(a.getTar-
getRef().type)
                                                   log.info(_targetType)
                                                   if     (_targetType     ==     "{http://mid-
point.evolveum.com/xml/ns/public/common/common-3}RoleType") {
                                                      log.info("ROLE TYPE! " + _targetType)
                                                      role_oid    =    basic.stringify(a.getTar-
getRef().oid)
                                                      log.info("Role OID! "+ role_oid)
                                                      role = midpoint.getObject(RoleType.class,
role_oid)
                                                      log.info(role.toString())

                                                      for (i in role.inducement) {
                                                         _rtargetType  =  basic.stringify(i.get-
TargetRef().type)
                                                         log.info(_rtargetType)
                                                            if  (_rtargetType  ==  "{http://mid-
point.evolveum.com/xml/ns/public/common/common-3}RoleType") {
                                                            log.info("ROLE TYPE INDUCEMENT! " +
_targetType)
                                                            irole_oid  =  basic.stringify(i.get-
TargetRef().oid)
                                                            log.info("Getting irole from oid =
" + irole_oid)
                                                            irole            =            mid-
point.getObject(RoleType.class, irole_oid)
                                                            log.info("Got    irole    =    "    +
basic.stringify(irole))
```

```
                                                    log.info("Irole identifier = " +
irole.getIdentifier())
                                                    log.info("Irole name = " +
irole.getName())
                                                    irole_real_oid = irole.getIdenti-
fier()

                                                    log.info("IROLE_REAL_OID = " +
irole_real_oid + " permission_uid = " + basic.getAttributeValue(entitlement, 'permission_uid'))

                                                    if (basic.getAttributeValue(enti-
tlement, 'permission_uid') == irole_real_oid) {
                                                       log.info("irole == permis-
sion_uid")
                                                       return "99999999-9999-9999-9999-
999999999999"
                                                    }
                                                 }
                                              }
                                           }
                                           else if (_targetType == "{http://mid-
point.evolveum.com/xml/ns/public/common/common-3}OrgType") {
                                              log.info("ORG TYPE! " + _targetType)
                                              org_oid = basic.stringify(a.getTar-
getRef().oid)
                                              log.info("Org OID! "+ org_oid)
                                              org = midpoint.getObject(OrgType.class,
org_oid)
                                              log.info(org.toString())

                                              for (i in org.inducement) {
                                                 _targetType = basic.stringify(i.get-
TargetRef().type)
                                                 log.info(_targetType)
                                                 if (_targetType == "{http://mid-
point.evolveum.com/xml/ns/public/common/common-3}RoleType") {
                                                    log.info("ROLE TYPE! " + _target-
Type)
                                                    role_oid = basic.stringify(i.get-
TargetRef().oid)
                                                    log.info("Role OID! "+ role_oid)
                                                    role = mid-
point.getObject(RoleType.class, role_oid)
                                                    log.info(role.toString())

                                                    for (ir in role.inducement) {
                                                       _rtargetType =
basic.stringify(ir.getTargetRef().type)
                                                       log.info(_rtargetType)
                                                          if (_rtargetType ==
"{http://midpoint.evolveum.com/xml/ns/public/common/common-3}RoleType") {
                                                             log.info("ROLE TYPE INDUCE-
MENT! " + _targetType)
```

```
                                                                    irole_oid                   =
basic.stringify(ir.getTargetRef().oid)
                                                                    log.info("Getting irole from
oid = " + irole_oid)
                                                                    irole         =         mid-
point.getObject(RoleType.class, irole_oid)
                                                                    log.info("Got  irole  =  "  +
basic.stringify(irole))
                                                                    log.info("Irole identifier =
" + irole.getIdentifier())
                                                                    log.info("Irole  name  =  "  +
irole.getName())
                                                                    irole_real_oid              =
irole.getIdentifier()

                                                                    log.info("IROLE_REAL_OID  =  "
+ irole_real_oid + " permission_uid = " + basic.getAttributeValue(entitlement, 'permission_uid'))

                                                                    if              (basic.getAt-
tributeValue(entitlement, 'permission_uid') == irole_real_oid) {
                                                                       log.info("irole == permis-
sion_uid")
                                                                       return     "99999999-9999-
9999-9999-999999999999"
                                                                    }
                                                                 }
                                                              }
                                                           }
                                                        }
                                                     }
                                                  }

                                                  return     basic.getAttributeValue(entitlement,
'permission_uid')
                                               </code>
                                            </script>
                                         </expression>
                                      </q:equal>
                                   </filter>
                                </assignmentTargetSearch>
                             </expression>
                             <target>
                                <path>assignment</path>
                             </target>
                          </inbound>
                          <kind>entitlement</kind>
                          <intent>Group Intent</intent>
                          <direction>objectToSubject</direction>
                          <associationAttribute>ri:members</associationAttribute>
                          <valueAttribute>icfs:uid</valueAttribute>
                          <shortcutAssociationAttribute>memberOf</shortcutAssociationAttribute>
                          <shortcutValueAttribute>icfs:uid</shortcutValueAttribute>
                          <explicitReferentialIntegrity>false</explicitReferentialIntegrity>
```

```
        </association>
```