



Modus Аналитический портал

Руководство по установке и настройке

Оглавление

Оглавление	2
1 Установка системы, требования для установки.....	3
1.1 Состав и содержание дистрибутивного носителя данных.....	3
1.2 Компоненты Аналитического портала	3
1.3 База данных Аналитического портала.....	4
1.4 Порядок загрузки данных и программ системы «Modus Аналитический портал»..	5
1.4.1 Предварительная настройка портала.....	5
1.4.2 Предварительная настройка базы данных	6
1.4.3 Запуск исполняемого файла	6
1.4.4 Технические настройки для работы «Modus Аналитический портал»	6
2 Лицензирование портала.....	10
3 Провайдеры аутентификации	11
3.1 Общее описание	11
3.1.1 Провайдер аутентификации	11
3.1.2 Конфигурация провайдера аутентификации	12
3.1.3 Параметры конфигурации провайдера аутентификации.....	12
3.1.4 Создание/изменение пользователя	17
3.1.5 Группы для конфигурации провайдера аутентификации.....	18
3.1.6 Установка «Профилей» пользователю	18
3.2 Инструкции и пример настройки	18
3.2.1 Добавление конфигурации провайдеров доступа	18
3.2.2 Пример настройки для Active Directory	19

1 Установка системы, требования для установки

1.1 Состав и содержание дистрибутивного носителя данных

Дистрибутивный носитель данных содержит

- «modusbi.exe» - исполняемый файл, являющийся сервером для Аналитического портала.

Расширение файла зависит от платформы (операционной системы):

- «Windows» – исполняемый файл «modusbi.exe»;
- «Linux» – исполняемый файл «modusbi»;
- «modusbi.json» - файл настройки, который можно использовать для быстрой первичной настройки. Позволяет не изменяя метаданные запустить портал с любыми предварительными настройками;
- «modusbi-*.mbm» - файл инициализации базы данных Аналитического портала;
- «update/modusbi-*.mbu» - файл обновления базы данных Аналитического портала до последней версии.

Примечание.

Если с дистрибутивом поставляются дополнительные файлы, которые не описаны в данном документе, то не стоит их учитывать и тем более выполнять системные команды, которые могут содержаться в файлах.

1.2 Компоненты Аналитического портала

Modus Аналитический портал (АП) является веб-приложением и состоит из трёх частей (см. Рисунок 1):

- **Сервера (Backend)** – основное приложение, выполняющее роль веб-сервера, взаимодействующего с источниками данных и выполняющего пользовательские команды;
- **Клиента (Frontend)** – средство отображения интерфейсов приложения в браузере;
- **Данные и метаданные** – расположенные в БД Аналитического портала необходимые для работы данные, содержащие настройки, команды, списки сущностей для работы приложения.

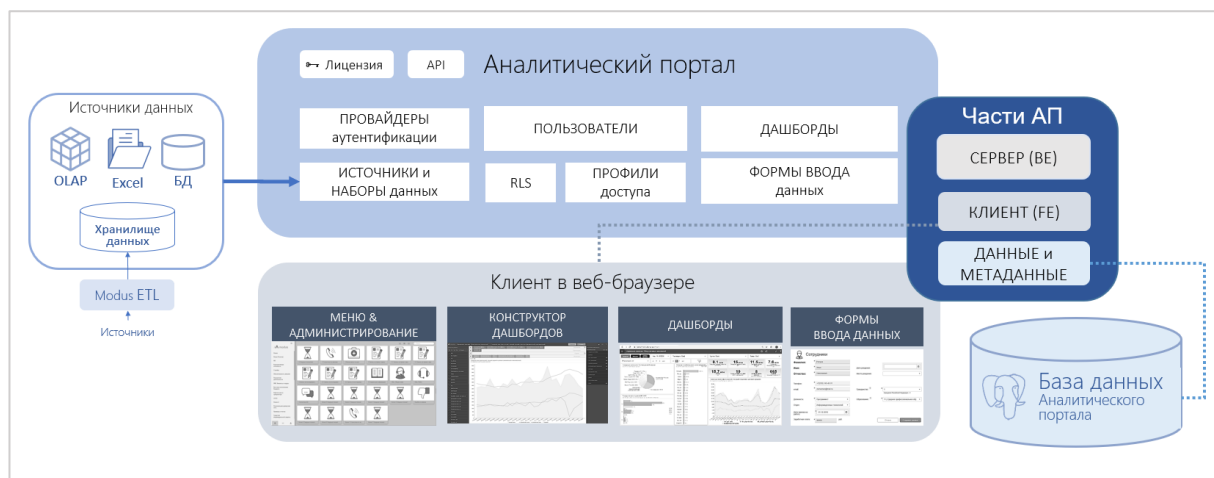


Рисунок 1. Схема компонентов аналитического портала

Схема взаимодействия портала с хранилищем данных и компонентов аналитического портала для отображения аналитических панелей (дашбордов) в веб интерфейсе – см. Рисунок 2.



Рисунок 2. Схема взаимодействия аналитического портала с внешними источниками данных и компонентов портала между собой

Хранилище – база данных, в которой хранятся подготовленные для анализа и визуализации данные.

Набор данных – SQL-запрос к таблицам БД хранилища и описание полей набора данных - наименований, псевдонимов/алиасов, типов данных, иерархий и других свойств.

Конструктор аналитических панелей – предназначен для настройки аналитических панелей (дашбордов).

Дашборды отображаются в веб-браузере и визуализируют данные в форме, удобной для восприятия и анализа.

1.3 База данных Аналитического портала

База данных Аналитического портала содержит данные для работы программного продукта – настройки, команды, описание API, а также данные о пользователях, дашбордах и т.д.

До версии Аналитического портала 3.0 использовалась встраиваемая СУБД – SQLite. Начиная с версии 3.0 база данных портала работает под управлением СУБД PostgreSQL (версии не ниже 10) и требует предварительной установки и настройки администратором. Для установки и настройки СУБД PostgreSQL обратитесь к официальному руководству:

- <https://www.postgresql.org/download/>
- <https://www.postgresql.org/docs/10/runtime-config.html>

Если СУБД PostgreSQL устанавливается впервые и будет использоваться без дополнительного ПО – пуллеров соединений (PgBouncer, Pgpool-II и т.д.), то для корректной работы с Аналитическим порталом в файле конфигурации PostgreSQL необходимо правильно сконфигурировать следующий параметр:

- ▶ *max_connections* - пиковое количество одновременно работающих пользователей (значение рассчитывается в зависимости от мощности сервера, по-умолчанию 100).

Действия по подключению Аналитического портала к Базе данных портала описаны в п.1.4.1. и п. 1.4.2.

1.4 Порядок загрузки данных и программ системы «Modus Аналитический портал»

Скопировать все файлы и папки из дистрибутива на сервер / рабочую станцию / локальную машину, которая будет выступать сервером аналитического портала.

1.4.1 Предварительная настройка портала

Файл `modusbi.json` позволяет запустить портал с предварительными настройками. При этом настройки из файла никуда не сохраняются и не записываются, то есть он нужен только для запуска.

Для подключения к базе данных портала необходимо в файле `modusbi.json` настроить параметры подключения к СУБД PostgreSQL. Для этого в разделе «`metadata`» следует указать следующие настройки:

```
"metadata": {
  "driver": "postgres",
  "datasource": "postgres://<ПОЛЬЗОВАТЕЛЬ_БД>:<ПАРОЛЬ_БД>@<IP-
АДРЕС_PG>:<ПОРТ_PG>/<ИМЯ_БД>?application_name=modusbi&sslmode=disable",
  "maxopenconns": <максимальное количество одновременно открытых соединений, не
больше значения max_connections в PostgreSQL>,
  "maxidleconns" : <максимальное количество открытых (ожидающих) соединений в
пуле>,
  "maxlifetime": <максимальное время жизни соединения в пуле, секунды>
}
```

Пример. Аналитический портал и СУБД PostgreSQL установлены на одном сервере, PostgreSQL слушает стандартный порт 5432, при этом для подключения используется логин `admin`, пароль `pass`, а имя базы данных для портала – `modusbi`. Тогда раздел «`metadata`» файла настроек может быть следующим:

```
"metadata": {
  "driver": "postgres",
  "datasource":
"postgres://admin:pass@localhost:5432/modusbi?application_name=modusbi&sslmode=disable",
  "maxopenconns": 100,
  "maxidleconns" : 20,
  "maxlifetime": 3600
}
```

После запуска портала, в случае необходимости, дальнейшие настройки необходимо осуществлять на странице настроек портала.

Пример. Аналитический портал установлен на сервер-1. Пользователь хочет зайти на портал на сервер-2.

Для этого необходимо:

- Настроить Аналитический портал
Адрес сервера: 0.0.0.0 или 127.0.0.1 или localhost
Порт: 5000
Протокол сервера данных: HTTP
Адрес сервера данных: IP адрес сервера-1
Порт сервера данных: 5000

- Открыть на сервере-2 браузер и перейти по адресу:
IP адрес сервера-1:5000

Для быстрой настройки надо изменить файл `modusbi.json`, как показано ниже, и запустить портал на сервере-1. Затем на сервере-2 в браузере открыть требуемую ссылку. Содержимое файла (подробнее о настройках см. п.1.4.4):

```
{
  "server": {
    "host": "127.0.0.1",
    "port": 5000
  },
  "backend": {
    "protocol": "http",
    "host": "IP адрес сервера-1",
    "port": 5000,
    "base_url": "/v1/api/"
  },
  "frontend": {
    "base_url": "/"
  },
  "form": {
    "base_url": "/fvd"
  }
}
```

1.4.2 Предварительная настройка базы данных

В СУБД PostgreSQL должна быть создана пустая база данных с любой основной схемой (по умолчанию – это *public*).

Для инициализации базы метаданных Аналитического портала необходимо сконфигурировать файл `modusbi.json` согласно п.1.4.1. Затем запустить исполняемый файл `modusbi` с флагом командной строки “-init”. Если всё настроено верно, в файле лога `modusbi.log` появится соответствующее сообщение: *созданы метаданные в '<БД PostgreSQL>'*, необходимо перезапустить сервер.

1.4.3 Запуск исполняемого файла

Далее нужно запустить исполняемый файл `modusbi`.

Для корректной работы Аналитического портала необходимо, чтобы у пользователя, который выполняет запуск исполняемого файла, были права на чтение, изменение, удаление папок и файлов в папке, содержащей файл «`modusbi`».

Во время выполнения файла откроется консоль сервера. **До окончания установки консоль сервера закрывать нельзя.**

После изменения настроек исполняемый файл нужно перезапускать. Для этого нужно закрыть консоль `modusbi` и запустить файл заново.

1.4.4 Технические настройки для работы «Modus Аналитический портал»

Адрес «`http://localhost:5000/`». Логин `admin`, пароль `admin`.

В режиме Администрирования перейдите к разделу «Настройки портала» (Рисунок 3,1).

Описание группы настроек портала - см. **Рисунок 3,2** и **Таблицу 1** - ниже.

Администрирование → Настройки портала

3 Сохранить настройки 4 Перезагрузка

modus

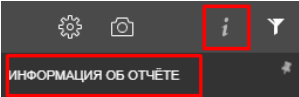
- Источники
- Наборы данных
- Загрузка из Excel
- Настройки RLS
- Роли RLS
- Отчеты
- Компоненты
- Фасеты
- Профили доступа к отчётам
- Профили наборов данных
- Профили экспорта
- Настройки провайдеров
- Лицензия
- Пользователи
- Настройки портала** 1

Адрес сервера	server.host 0.0.0.0	2
Порт	server.port 5000	
Корневой каталог приложения на сервере	frontend_base_url /	
Наименование (заголовок окна)	frontend.title Modus BI: Аналитический портал	
Версия frontend портала	2.4.20	
Источник дат обновления	ETL_НаборДанных ✕	
Поле фильтра	НаборДанных	
Поле значения	ДатаАктуальности	
Протокол сервера данных	SSL	
Адрес сервера данных	backend.host dev.modusbi.ru	
Порт сервера данных	backend.port 443	
Путь к API данных	backend_base_url /v1/api/	
Ключ SSL	Выберите файл Файл не выбран	
Сертификат SSL	Выберите файл Файл не выбран	
Заголовок сервисного режима	backend.serviceMode.title Сервис временно недоступен.	
Сообщение сервисного режима	backend.serviceMode.message Портал находится на сервисном обслуживании. Попробуйте обновить страницу через некоторое время.	
Заголовок при недоступности сервиса	backend.offlineMode.title Сервис недоступен.	
Сообщение при недоступности сервиса	backend.offlineMode.message Портал недоступен. Попробуйте зайти позже.	
Максимальное число получаемых записей данных	dataset.count 5000	
Шаблон Excel по умолчанию	Выберите файл Файл не выбран	
Корневой каталог приложения Форм Ввода Данных	form_base_url /fvd	
Фасеты. Источник таблиц	Фасеты. Список таблиц (md_table_list) ✕	
Фасеты. Источник полей	Фасеты. Список фасетов (md_facet_lis) ✕	
Фасеты. Источник значений	Фасеты. Список значений фасетов (mc) ✕	

Обновить Frontend Импортировать обновление Загрузить лицензию

Рисунок 3. Настройки портала

Таблица 1. Описание настроек портала

Пункт настройки	Описание
<p>Адрес сервера server.host</p>	<p>Строка, содержащая сетевой адрес, по которому сервер(Backend) будет принимать клиентские подключения. Запись 0.0.0.0 позволяет задействовать все адреса IPv4.</p> <ul style="list-style-type: none"> По умолчанию равно «localhost». <p>Адрес «http://localhost:5000/», логин admin, пароль admin. Пример: {«client»: {«baseURL»: «/»}, «server»: {«protocol»: «HTTP», «host»: «localhost», «port»: «5000»}}</p>
<p>Порт server.port</p>	<p>Строка, содержащая TCP-порт, открываемый сервером(Backend) Аналитического портала.</p> <ul style="list-style-type: none"> По умолчанию равно «5000».
<p>Корневой каталог приложения на сервере frontend.base_url</p>	<p>Строка, содержащая название аналитического портала.</p> <ul style="list-style-type: none"> По умолчанию равно «/». <p>Пример 1: Доменное имя, используемое для сайтов компании в «www.mysite.com». {«client»: {«baseURL»: «/»}, «server»: {«protocol»: «HTTP», «host»: «localhost», «port»: «5000»}} Аналитический портал доступен по адресу «http://www.mysite.com/».</p> <p>Пример 2: Доменное имя, используемое для сайтов компании в «www.mysite.com/bi-portal». {«client»: {«baseURL»: «bi-portal/»}, «server»: {«protocol»: «HTTP», «host»: «localhost», «port»: «5000»}} Аналитический портал доступен по адресу «http://www.mysite.com/bi-portal/»</p>
<p>Наименование (заголовок окна) Frontend.title</p>	<p>Заголовок окна для пользователя</p>
<p>Версия Frontend портала</p>	<p>Версия Frontend портала. В списке отображаются доступные для настройки версии</p> <div data-bbox="646 1339 863 1379" style="border: 1px solid #ccc; padding: 2px;"> 1.2.13 </div> <ul style="list-style-type: none"> По умолчанию устанавливается максимально доступная версия FE-портала.
<p>Источник дат обновления</p>	<p>Настройка / подключение информации по датам обновления источников данных, отображаемая в описании отчета.</p>  <p>Для настройки источника необходимо подключить источник с необходимой информацией (например, таблица). Связать поля фильтр и значения, где фильтр – поле с наименованием источника данных, значение – дата последнего обновления данных в источнике.</p> <div data-bbox="639 1832 1410 1995" style="border: 1px solid #ccc; padding: 5px;"> <p>Источник дат обновления ETL_НаборДанных</p> <p>Поле фильтра НаборДанных</p> <p>Поле значения ДатаАктуально</p> </div> <ul style="list-style-type: none"> По умолчанию источник не указан <p>Подробнее см. Руководство пользователя, Приложение А</p>

Пункт настройки	Описание
Протокол сервера данных	Строка, содержащая наименование протокола, который будет использовать Аналитический портал. <ul style="list-style-type: none"> По умолчанию равно «HTTP». Допустимые значения: «HTTP», «SSL».
Адрес сервера данных backend.host	Строка, содержащая сетевой адрес для обращений клиентского приложения(Frontend) к серверу(Backend) Аналитического портала
Порт сервера данных backend.port	Строка, содержащая порт, по которому будут выполняться обращения клиентского приложения(Frontend) к серверу(Backend) Аналитического портала. <ul style="list-style-type: none"> По умолчанию равно «5000».
Путь к API данных backend.base_url	Строка, содержащая название, используемое для доступа к ресурсам аналитического портала. <ul style="list-style-type: none"> По умолчанию равно «/v1/api/».
Ключ SSL	Строка, содержащая полный локальный путь к файлу, содержащему ключ для сертификата для работы аналитического портала по протоколу «HTTPS». <ul style="list-style-type: none"> По умолчанию равно «». Используется только при значении настройки «protocol» равной «HTTPS».
Сертификат SSL	Строка, содержащая полный локальный путь к файлу, содержащему сертификат для работы аналитического портала по протоколу «HTTPS». <ul style="list-style-type: none"> По умолчанию равно «». Используется только при значении настройки «protocol» равной «HTTPS».
Заголовок сервисного режима Backend.serviceMode.title	Строка заголовка для информационного сообщения портала во время сервисного режима. <ul style="list-style-type: none"> По умолчанию «Сервис временно недоступен»
Сообщение сервисного режима Backend.serviceMode.message	Строка для информационного сообщения пользователям портала во время сервисного режима. <ul style="list-style-type: none"> По умолчанию «Портал находится на сервисном обслуживании. Попробуйте обновить страницу через некоторое время.»
Заголовок при недоступности сервиса Backend.offlineMode.title	Строка заголовка для информационного сообщения портала во время сервисного режима. <ul style="list-style-type: none"> По умолчанию «Сервис недоступен.»
Сообщение при недоступности сервиса Backend.offlineMode.message	Строка для информационного сообщения пользователям портала во время сервисного режима. <ul style="list-style-type: none"> По умолчанию «Портал недоступен. Попробуйте зайти позже.»
Максимальное число получаемых записей данных Dateset.count	Число, используемое по умолчанию для ограничения количества строк набора данных при отображении в отчете. Ограничение количества строк устанавливается для сокращения времени отображения отчетов на портале. При необходимости это число можно увеличить или уменьшить. <ul style="list-style-type: none"> По умолчанию 5000

Пункт настройки	Описание
Шаблон Excel по умолчанию	Настраиваемый общий шаблон для выгрузки данных с портала в Excel. <input type="button" value="Выберите файл"/> Файл не выбран
Корневой каталог приложения Форм Ввода Данных form.base_url	Строка, содержащая название, используемое для доступа к ресурсам Форм Ввода Данных аналитического портала. <ul style="list-style-type: none"> По умолчанию равно «//fvd».
Фасеты Источник таблиц Источник полей Источник значений	“Фасеты” содержат статистику по полям таблиц хранилища данных. Возможно указать имена таблиц, полей и значений по которым будет работать интерфейс Администрирование\[Фасеты]. Обычно таблицы фасетов создаются, заполняются и обновляются, при использовании соответствующего функционала Modus ETL.

Внесите изменения в настройки и сохраните их по кнопке [Сохранить настройки] - см. Рисунок 3,3.

Для применения настроек воспользуйтесь кнопкой [Перезагрузка] в правом верхнем углу окна настроек - см. Рисунок 3,4.

2 Лицензирование портала

С релиза 2.4.0 портал поставляется в виде демо-версии с триальным ключом со следующими ограничениями:

- по сроку использования - 30 дней с момента первого запуска,
- количеству пользователей - 5,
- количеству дашбордов - 5.

Для работы с коммерческой версией портала необходимо установить и активировать электронный ключ, «привязанный» к оборудованию и содержащий лицензию Аналитического портала.

Установка ключа производится в 2 этапа:

На 1ом этапе формируется запрос на лицензию, который должен быть направлен вендору.

На 2ом этапе устанавливается присланный ответ.

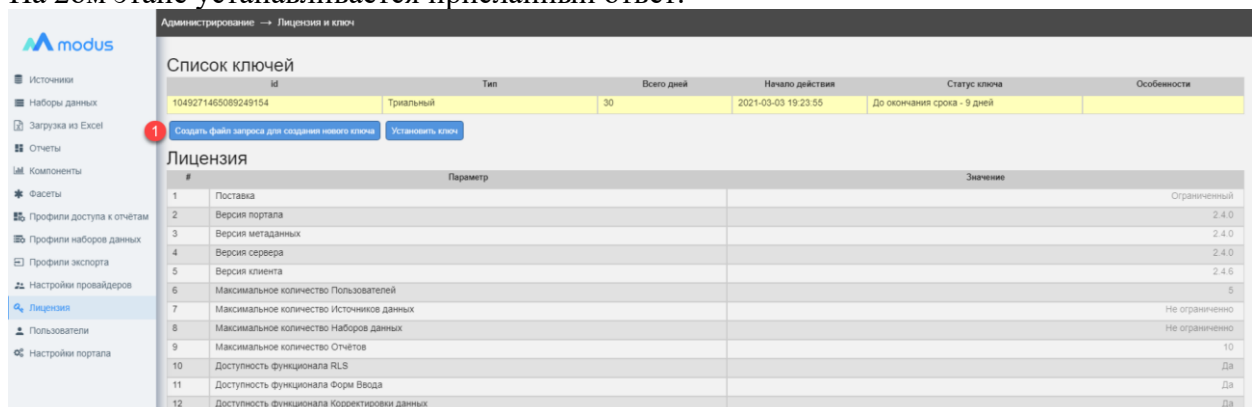


Рисунок 4 Раздел "Лицензии"

Этап 1. Формирование запроса

1. В режиме Администрирования перейдите к разделу «Лицензия» и нажмите на кн[Создать файл запроса для создания нового ключа]. Введите присланный ранее пин-код и ИНН организации.
2. Сохраните файл запроса вида *.mbc
3. Направьте сформированный файл запроса по электронной почте на адрес 112@modusbi.ru

Этап 2. Установка ключа

4. После получения файла-ответа снова зайдите на Аналитический портал, перейдите в раздел Администрирование\Лицензии и нажмите на кн[Установить ключ]
5. Выберите полученный файл-ответ формата *.mbv.
6. Перезагрузите Аналитический портал
7. После перезагрузки будет доступен функционал портала в рамках, заданных лицензией. Параметры лицензии будут отображены в таблице [Лицензии], а активный ключ будет выделен желтым цветом в [Списке ключей].

Администрирование → Лицензия и ключ

Список ключей

id	Тип	Всего дней	Начало действия	Статус ключа	Особенности
763699190570702837	Стандартный	Не ограничено		Не ограничено	
1049271465089249154	Триальный	30	2021-03-03 19:23:55	До окончания срока - 9 дней	

Создать файл запроса для создания нового ключа | Установить ключ 2

Лицензия

#	Параметр	Значение
1	Поставка	Стандартный
2	Версия портала	2.4.0
3	Версия метаданных	2.4.0
4	Версия сервера	2.4.0
5	Версия клиента	2.4.6
6	Максимальное количество Пользователей	7
7	Максимальное количество Источников данных	Не ограничено
8	Максимальное количество Наборов данных	Не ограничено
9	Максимальное количество Отчётов	Не ограничено
10	Доступность функционала RLS	Да
11	Доступность функционала Форм Ввода	Да
12	Доступность функционала Корректировки данных	Да

Рисунок 5 Установка полученного файла

3 Провайдеры аутентификации

3.1 Общее описание

Для обеспечения возможности входа пользователя на аналитический портал (АП) посредством разных методов идентификации и аутентификации, спроектированы и разработаны провайдеры аутентификации.

3.1.1 Провайдер аутентификации

Провайдер аутентификации (ПА) – это некоторый внутренний/внешний метод/сервис, который может выполнить **идентификацию** и последующую **аутентификацию** пользователя, результатом работы которого будет как минимум информация об учётных данных пользователя и маркер доступа с периодом действия (**токен**).

Пока период действия маркера доступа не истёк, пользователь автоматически входит на АП.

На основе текущей реализации вариантов входа на АП созданы следующие **провайдеры аутентификации**:

1. **Password** – провайдер использующий имя пользователя для идентификации и пароль для аутентификации.

2. **LDAP for Active Directory** – провайдер передающий имя пользователя и пароль в службу каталогов «**Active Directory**» посредством протокола «**LDAP**».
3. **SAML** – провайдер выполняющий создание подписанного «XML – документа» по стандарту «**SAML**», который используется для идентификации системы и передающий созданный документ внешней системе для выполнения аутентификации пользователя.
4. **OAuth2.0 Client Credentials** – провайдер аутентификации выполняющий авторизацию посредством стандарта авторизации «**OAuth 2.0**», с использованием типа предоставления учётных данных «**Client Credentials**», который используется для конфиденциальных клиентов, которые запрашивают доступ к своим ресурсам или ресурсам, заранее согласованным с сервером авторизации.
5. **OAuth2.0 Authorization Code** – провайдер аутентификации выполняющий авторизацию посредством стандарта авторизации «**OAuth 2.0**», с использованием типа предоставления учётных данных «**Authorization code**», который в основном используется для «**Web-сервисов**», которые выполняют перенаправление запроса на сервер авторизации и обрабатывают ответ.

3.1.2 Конфигурация провайдера аутентификации

Так как для одного **провайдера аутентификации** могут быть разные настройки, то совокупность уникальных **настроек и провайдера аутентификации** объединены понятием **конфигурация провайдера аутентификации**.

Таким образом получается, что администратор АП может управлять методом **идентификации и аутентификации** на АП посредством создания/изменения **конфигураций провайдера аутентификации**.

3.1.3 Параметры конфигурации провайдера аутентификации

Параметры конфигурации провайдера состоят из двух частей **постоянных** параметров и **динамического** набора полей, который определяется схемой провайдера аутентификации. Постоянные параметры конфигурации:

- 1) **Провайдер** аутентификации/авторизации – выбирается при добавлении конфигурации и не может быть изменён.
- 2) **Тип хеширования** – алгоритм который используется для обработки пароля пользователя, выбирается при добавлении конфигурации и не может быть изменён.
- 3) **Имя** конфигурации – уникальное внутреннее название для конфигурации.
- 4) **Отображаемое наименование** – уникальное название конфигурации, которое отображается пользователю.
- 5) **Администратор доступа** – пользователь, от имени которого выполняются автоматические операции после успешной обработки ответа от службы/сервиса идентификации/аутентификации.
- 6) **Иконка** – графическое изображение которое выводится на форме Входа/Выхода пользователя.

- 7) **Встроенный** – признак, который устанавливается разработчиками и не может быть изменён, характеризует **конфигурацию провайдера аутентификации**, встроенную в АП, которая используется всегда при отсутствии других конфигураций.
- 8) **По умолчанию** – признак, указывающий на конфигурацию, которая используется для идентификации/аутентификации пользователя, если пользователь не существует в списке пользователей АП или создан без указания конфигурации провайдера.
- 9) **Показывать форму** – признак указывает на необходимость отображения формы Входа.

Для каждого **провайдера аутентификации** набор **динамических** полей определяют разработчики на основе схемы.

Для следующих провайдеров аутентификации на текущий момент определены следующие наборы **динамических** полей:

1) **Password:**

1. Необходимо ввести имя пользователя – требует ввода имени пользователя на форме Входа.
2. Необходимо ввести пароль – требует ввода пароля на форме Входа.

2) **LDAP for Active Directory:**

1. Необходимо ввести имя пользователя – требует ввода имени пользователя на форме Входа.
2. Необходимо ввести пароль – требует ввода пароля на форме Входа.
3. адрес (**host**) – обязательное поле, содержит IP-адрес или DNS-имя сервера LDAP.
4. порт – (**port**) – не обязательное поле, содержит порт, который прослушивается службой LDAP на «адрес».

По умолчанию 0.

Если равен 0, то используется стандартный порт "389" для не защищённого соединения или порт "636" для защищённого соединения (параметры указываются ниже).

5. база поиска (**base_dn**) - обязательное поле, содержит уникальное имя базы поиска (DN), состоящее из одного или нескольких относительных уникальных имён (RDN).
Пример: «dc=example,dc=com».
6. база поиска с пользователем (**bind_dn**) – не обязательное поле, содержащее уникальное имя базы поиска, содержащее клиента/пользователя.
Пример: «cn=username,dc=example,dc=com»
7. пароль пользователя (**bind_pass**) – не обязательный если не указан «база поиска с пользователем», содержит пароль клиента/пользователя, указанного в «база поиска с пользователем».
8. не использовать шифрование TLS (**skip_tls**) – не обязательное поле, по умолчанию значение «Да», не использовать шифрование TLS при выполнении запросов.
9. использовать шифрование SSL (**use_ssl**) - не обязательное поле, по умолчанию значение «Нет», использовать шифрование SSL при выполнении запросов (параметры указываются ниже).
10. SSL-сертификат (**ssl_cert**) - не обязательное поле, путь и наименование файла, содержащего SSL-сертификат, используется если «использовать шифрование SSL» установлено в «Да».

11. SSL-ключ (**ssl_key**) - не обязательное поле, путь и наименование файла, содержащего SSL-ключ, используется если «использовать шифрование SSL» установлено в «Да».
12. название сервера из SSL-сертификата (**server_name**) – не обязательное поле, содержащее название сервера, указанное в SSL сертификате (Server Name Indication), используется если «использовать шифрование SSL» установлено в «Да».
13. NetBIOS имя сервера (**server_netbios**) – обязательное поле, содержит NetBIOS имя сервера, используется если «использовать имя пользователя (UPN) в интернет стиле» установлено в «Нет».
14. пропускать проверку безопасности при использовании SSL (**insecure_skip_verify**) – не обязательное поле, по умолчанию установлено в «Да», пропускать проверку безопасности при использовании "SSL".
15. использовать имя пользователя (UPN) в интернет стиле (**user_principal_name**) - не обязательное поле, по умолчанию установлено в «Да», использовать имя входа пользователя (UPN) в интернет стиле.

Пример: username@example.com

3) SAML:

1. Поставщик учётных записей: **Файла метаданных** – обязательное поле, содержит наименование и полный путь к файлу, содержащему метаданных поставщика идентификации/аутентификации.
Пример: «metadata.xml»
2. Поставщик сервиса: **Адрес сервера портала** – обязательное поле, содержит адрес сервера портала.
Пример: «https://dev.modusbi.ru/v1/api»
3. Поставщик сервиса: **Использовать самозаверенный сертификат** – не обязательное поле, если значение установлено в «Да», то автоматически создаётся сертификат и ключ для доменного имени используемого в адресе сервера портала.
4. Поставщик сервиса: **Файла сертификата** - обязательное поле, если сервер портала использует протокол «HTTPS» и значение «Поставщик сервиса: Использовать самозаверенный сертификат» установлено в «Нет», содержит наименование и полный путь к файлу, содержащему сертификат, созданный для доменного имени, используемого в адресе АП.
Пример: «domain.cert»
5. Поставщик сервиса: **Файла ключа для сертификата** - обязательное поле, если сервер портала использует протокол «HTTPS» и значение «Поставщик сервиса: Использовать самозаверенный сертификат» установлено в «Нет», содержит наименование и полный путь к файлу, содержащему ключ для сертификата созданный для доменного имени, используемого в адресе АП.
Пример: «domain.key»
6. Поставщик сервиса: **Создавать пользователя** – не обязательное поле, если установлено в «Да», то после получения ответа от «Поставщик учётных записей» об успешной идентификации/аутентификации, создаётся новый пользователь в АП с данными полученными из ответа.

7. Поставщик сервиса: **Устанавливать Профили** – не обязательное поле, если установлено в «Да», то после получения ответа от «Поставщик учётных записей» об успешной идентификации/аутентификации, пользователю устанавливаются «Профили» с использованием «Групп для конфигурации провайдера аутентификации».
8. Поставщик учётных записей: **способ передачи для Входа (SingleSignOnService)** – определяет значение атрибута «Binding» «XML-тэга» «SingleSignOnService», который необходимо использовать в файле настроек, указанного в пункте «1». Если значение настройки не указано, то используется первая запись «XML-тэга» «SingleSignOnService» из файла настроек, указанного в пункте «1». Допустимые поддерживаемые значения:
 - 1) «urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST» - значение по умолчанию.
 - 2) «urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect».
9. Поставщик учётных записей: **способ передачи для Выхода (SingleLogoutService)** – определяет значение атрибута «Binding» «XML-тэга» «SingleLogoutService», который необходимо использовать в файле настроек, указанного в пункте «1». Если значение настройки не указано, то используется первая запись «XML-тэга» «SingleLogoutService» из файла настроек, указанного в пункте «1». Допустимые поддерживаемые значения:
 - 3) «urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST» - значение по умолчанию.
 - 4) «urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect».
10. Поставщик сервиса: **Формат идентификатора пользователя (NameIDFormat)** – задаёт значение «XML-тэга» из которого необходимо получать формат представления идентификатора пользователя. В соответствии с документацией (<http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>, §2.4.2), поддерживаются следующие значения:
 - 1) «urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified» - используется как значение по умолчанию.
 - 2) «urn:oasis:names:tc:SAML:2.0:nameid-format:persistent».
 - 3) «urn:oasis:names:tc:SAML:2.0:nameid-format:transient».
 - 4) «urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress».
 - 5) «urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName».
11. Поставщик сервиса: **Подписать запрос аутентификации** – определяет необходимость использования шифрования отправляемых данных.
12. Поставщик сервиса: **Проверить действительность сертификата шифрования** – перед тем как подписывается запрос аутентификации выполняется проверка срока годности сертификата, используемого для шифрования.
13. Поставщик сервиса: **Не проверять подпись** – при обработке ответа от поставщика учётных записей не выполняется проверка подписи перед расшифровкой.
14. Поставщик сервиса: **Разрешить отсутствие атрибутов** – если в результате обработки ответа от поставщика учётных записей не будут найдены некоторые атрибуты в «XML-тэгах», то не возвращать ошибку обработки.
15. Поставщик сервиса: **Проверить данные подтверждения субъекта** – при обработке ответа от поставщика учётных записей проверяются атрибуты «XML-тэга» «urn:oasis:names:tc:SAML:2.0:assertion Subject».

6) OAuth2.0 Client Credentials:

1. **Необходимо ввести имя пользователя** – требует ввода имени пользователя на форме Входа.
2. **Необходимо ввести пароль** – требует ввода пароля на форме Входа.
3. **Идентификатор приложения** – строковое значение, полученное при регистрации на сервере авторизации («**client id**»).
4. **Код приложения** – строковое значение, полученное при регистрации на сервере авторизации («**client secret**»).
5. **Адрес сервера авторизации** – интернет адрес сервера авторизации.
6. **Адрес получения маркера доступа** – интернет адрес куда необходимо отправлять запросы на получение маркера доступа.
7. **Адрес получения данных пользователя** – интернет адрес куда необходимо отправлять запросы с полученным маркером доступа, чтобы получить данные пользователя.
8. **Получать области пользователя** (разделённые пробелом) – строка, содержащая значения, описывающие данные пользователя на стороне сервера авторизации и используемые при создании и обновлении пользователя после успешной аутентификации в АП, по умолчанию равно «**openid name email groups roles**».
9. **Области для установки профилей** (разделённые пробелом) – строка, содержащая значения, описывающие данные пользователя на стороне сервера авторизации и используемые для установки профилей после успешной аутентификации в АП, посредством «**Групп конфигурации провайдера аутентификации**», по умолчанию равно «**groups roles**».
10. **Создавать пользователя** – не обязательное поле, если установлено в «**Да**», то после успешной авторизации на сервере авторизации, создаётся новый пользователь в АП с данными полученными из ответа.
11. **Устанавливать Профили** – не обязательное поле, если установлено в «**Да**», то после успешной авторизации на сервере авторизации, пользователю устанавливаются «**Профили**» с использованием «**Групп для конфигурации провайдера аутентификации**».

7) OAuth2.0 Authorization Code:

1. **Необходимо ввести имя пользователя** – требует ввода имени пользователя на форме Входа.
2. **Необходимо ввести пароль** – требует ввода пароля на форме Входа.
3. **Идентификатор приложения** – строковое значение, полученное при регистрации на сервере авторизации («**client id**»).
4. **Код приложения** – строковое значение, полученное при регистрации на сервере авторизации («**client secret**»).

5. **Адрес сервера портала** (<https://demo.modusbi.ru>) – адрес сервера Аналитического портала на который, будет выполнено перенаправление с сервера авторизации. **Не путать** с адресом портала, так как по умолчанию адрес сервера портала, содержит адрес портала и суффикс «**/v1/api/**» (значение настройки «**Путь к API данных**»).
6. **Адрес сервера авторизации** – интернет адрес сервера авторизации.
7. **Адрес получения маркера доступа** – интернет адрес куда необходимо отправлять запросы на получение маркера доступа.
8. **Адрес получения данных пользователя** – интернет адрес куда необходимо отправлять запросы с полученным маркером доступа, чтобы получить данные пользователя.
9. **Получать области пользователя** (разделённые пробелом) – строка, содержащая значения, описывающие данные пользователя на стороне сервера авторизации и использующиеся при создании и обновлении пользователя после успешной аутентификации в АП, по умолчанию равно «**openid name email groups roles**».
10. **Области для установки профилей** (разделённые пробелом) – строка, содержащая значения, описывающие данные пользователя на стороне сервера авторизации и использующиеся для установки профилей после успешной аутентификации в АП, посредством «**Групп конфигурации провайдера аутентификации**», по умолчанию равно «**groups roles**».
11. **Создавать пользователя** – не обязательное поле, если установлено в «**Да**», то после успешной авторизации на сервере авторизации, создаётся новый пользователь в АП с данными полученными из ответа.
12. **Устанавливать Профили** – не обязательное поле, если установлено в «**Да**», то после успешной авторизации на сервере авторизации, пользователю устанавливаются «**Профили**» с использованием «**Групп для конфигурации провайдера аутентификации**».

3.1.4 Создание/изменение пользователя

Так как в результате **идентификации** и **аутентификации** пользователя может возникнуть необходимость **создания/изменения учётных данных** для пользователя в АП, а также назначение доступа пользователя к разным частям АП посредством назначения «**Профилей**», то для каждой **конфигурации провайдера аутентификации** возможно:

- 1) Указание необходимости создания пользователя после успешной идентификации и аутентификации.
- 2) Назначение пользователю «**Профилей**» (любых типов) на основании полученного «**Списка доступа**» в результате идентификации и аутентификации в **провайдере аутентификации**.

3.1.5 Группы для конфигурации провайдера аутентификации

Для корректного назначения «Профилей» пользователю необходимо, что бы с каждым возможным элементом «Списка доступа» были установлены связи с одним или несколькими существующими «Профилями».

Таким образом для каждой **конфигурации провайдера аутентификации** можно создать свой уникальный «Список доступа», который называется «Группы конфигурации».

Каждый элемент «Группы конфигурации» может быть связан с одним или несколькими существующими «Профилями».

3.1.6 Установка «Профилей» пользователю

Для обеспечения корректного текущего доступа пользователя к частям АП, установка «Профилей» на основании связи с «Группами конфигурации» выполняется каждый раз после успешной **идентификации и аутентификации** пользователя в **провайдере аутентификации**, посредством **удаления** установленных «Профилей» кроме профиля с типом «Личный» и назначения новых «Профилей» на основании «Группами конфигурации».

3.2 Инструкции и пример настройки

3.2.1 Добавление конфигурации провайдеров доступа

- 1) Зайти на портал с правами Администратора.

Перейти в меню Администрирование (см. Рисунок 6 , 1), Настройки провайдеров (2) и нажать кн[Добавить конфигурацию] (3):

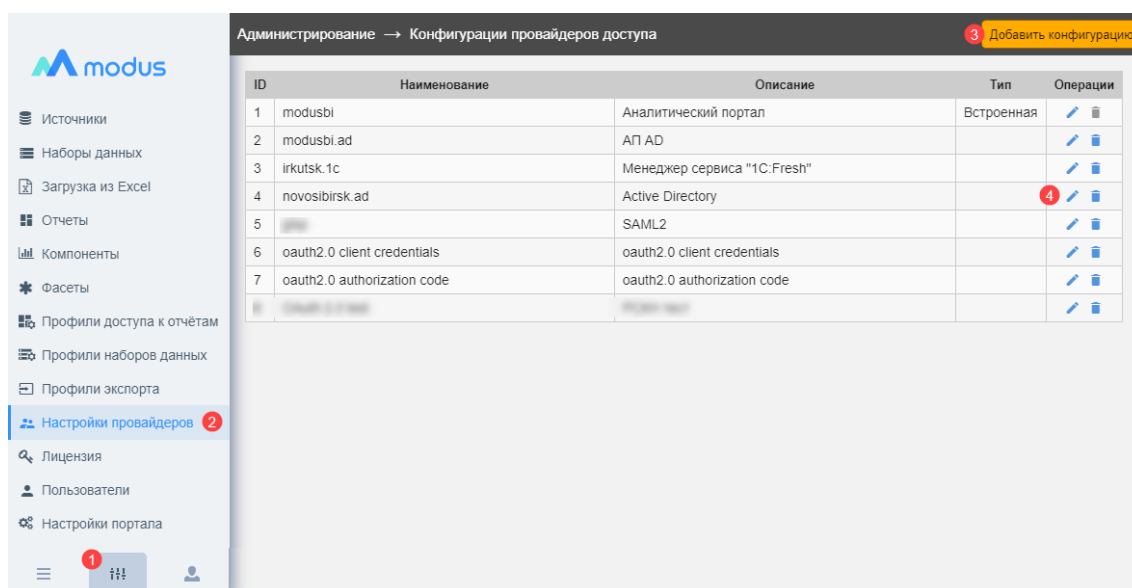



Рисунок 6. Настройки провайдеров аутентификации. Форма списка

- 2) Заполнить поля «Имя» (см.Рисунок 7, 1), «Отображаемое наименование» (2).
Выбрать провайдера авторизации(3), тип хэширования (4) и нажать кн[Создать].

Рисунок 7. Добавление новой конфигурации

- 3) Перейти в редактирование конфигурации по кнопке  - см. Рисунок 6 , 1.
- 4) При необходимости - изменить «Имя» (см.Рисунок 8, 1) и «Отображаемое наименование» (2), установить опции и (3), выбрать иконку (4), выбрать администратора доступа (5). Заполнить поля (6) – поля меняются в зависимости от выбранного провайдера авторизации:

Поле	Значение
Необходимо ввести имя пользователя	Вкл. <input checked="" type="checkbox"/>
Необходимо ввести пароль	Вкл. <input checked="" type="checkbox"/>

Рисунок 8. Форма редактирования провайдера аутентификации

3.2.2 Пример настройки для Active Directory

- 1) Добавляем конфигурацию с параметрами:

Добавление новой конфигурации

Имя
AD

Отображаемое наименование
AD

Выбрать провайдера авторизации
LDAP for Active Directory

Выбрать тип хеширования
Skip hashing


- 2) Заполняем настройки (подробное описание параметров в п. 3.1.3 (2)) конфигурации - поля «Адрес», «База поиска» и выбираем иконку для конфигурации:

Редактирование конфигурации

Имя
AD

Отображаемое наименование
AD

Конфигурация по умолчанию
 Показывать форму авторизации

Иконка 

Администратор доступа

Поле	Значение
Необходимо ввести имя пользователя	Вкл. <input checked="" type="checkbox"/>
Необходимо ввести пароль	Вкл. <input checked="" type="checkbox"/>
адрес	192.168.0.21
порт	Введите значение port
база поиска	dc=corp,dc=handy-soft,dc=com
база поиска с пользователем	Введите значение bind_dn

- 3) Создаем пользователя. Имя пользователя (UPN) по умолчанию в интернет стиле, также указываем конфигурацию:


Редактирование пользователя

Конфигурация: AD Группы доступа: **не назначены**

Фамилия: 1 Имя: 1 Отчество: Введите отчество

Организация: Введите название организации Подразделение: Введите наименование Должность: Укажите должность

E-mail: Введите e-mail Телефон: Введите номер

Логин: p.petrov@corp.handy-soft.com Пароль: Заполните чтобы сменить пароль 


Роль пользователя: Состояние: Права доступа: Ссылка на ФВД:

Профили наборов данных: [Только СВОИ наборы данных](#)


- 4) Проверяем доступ на портал указывая Логин, Пароль и нажимая на иконку созданной конфигурации:

Логин
p.petrov@corp.handy-soft.com

Пароль
.....

 Войти

Другие способы авторизации

 AD