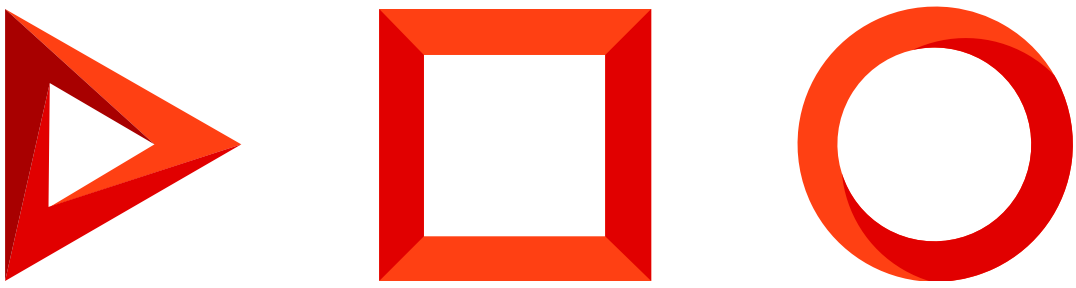
Creatio Academy

Синхронизация пользователей с LDAP

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Настроить синхронизацию с LDAP

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Синхронизация с каталогом LDAP позволяет автоматизировать управление учетными записями пользователей в Creatio. Пользователи, синхронизированные с LDAP, могут использовать свое доменное имя пользователя и пароль для входа в систему.

В системе поддерживаются следующие реализации LDAP: Active Directory и OpenLDAP.

Процедуру синхронизации можно условно разделить на три этапа:

1. Настройка интеграции с LDAP. Выполняется однократно либо при изменении структуры синхронизируемого каталога LDAP. Настройка необходима, чтобы была доступна остальная функциональность по синхронизации с LDAP. Также необходимо настроить фильтрацию пользователей Active Directory для определения параметров синхронизации. Подробнее: Настроить фильтры Active Directory.
2. Привязка элементов (пользователей и элементов организационной структуры) Creatio к соответствующим элементам каталога. Выполняется при добавлении новых пользователей либо организационных ролей. Вы можете привязать уже зарегистрированных пользователей Creatio либо импортировать пользователей из Active Directory.
3. Синхронизация пользователей и элементов организационной структуры Creatio со связанными элементами каталога LDAP. Действие необходимо для обновления данных в соответствии с изменениями, произошедшими в каталоге LDAP с момента предыдущей синхронизации. Выполняется регулярно: автоматически либо по действию [*Синхронизировать с LDAP*] раздела [*Организационные роли*].

> **На заметку.** Каждая организационная роль является элементом организационной структуры и представляет собой организацию или подразделение.

После синхронизации пользователи смогут авторизоваться с помощью LDAP. Подробнее: Настроить аутентификацию с LDAP.

Настроить интеграцию с LDAP

Настройка интеграции с LDAP предусматривает настройку связи элементов каталога LDAP с пользователями и ролями Creatio. Для выполнения настройки необходимо обладать базовыми знаниями структуры каталога LDAP, с которым выполняется интеграция.

В статье приведены примеры настройки LDAP для Active Directory и OpenLDAP.

> **Важно.** В зависимости от особенностей структуры каталогов LDAP, атрибуты элементов LDAP в вашем каталоге могут отличаться от атрибутов, которые приведены в качестве примеров.

1. Откройте дизайнер системы, например, по кнопке .
2. В группе “Импорт и интеграции” перейдите по ссылке “Настройка интеграции с LDAP”. Откроется страница настроек. Выделенные поля нужно обязательно настроить. Для остальных можно использовать значения по умолчанию.

Рис. 1 — Страница настроек интеграции с LDAP для Active Directory

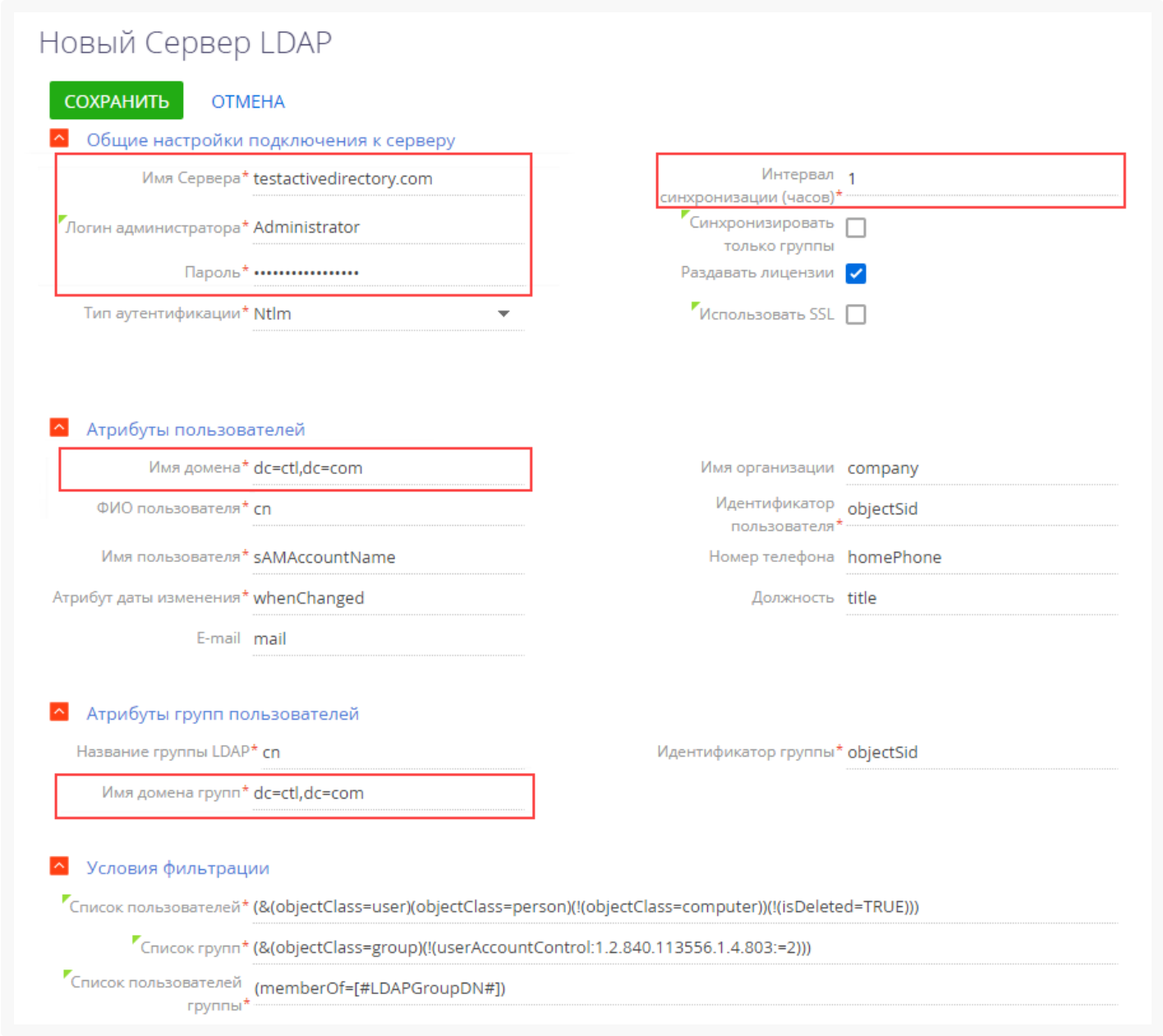
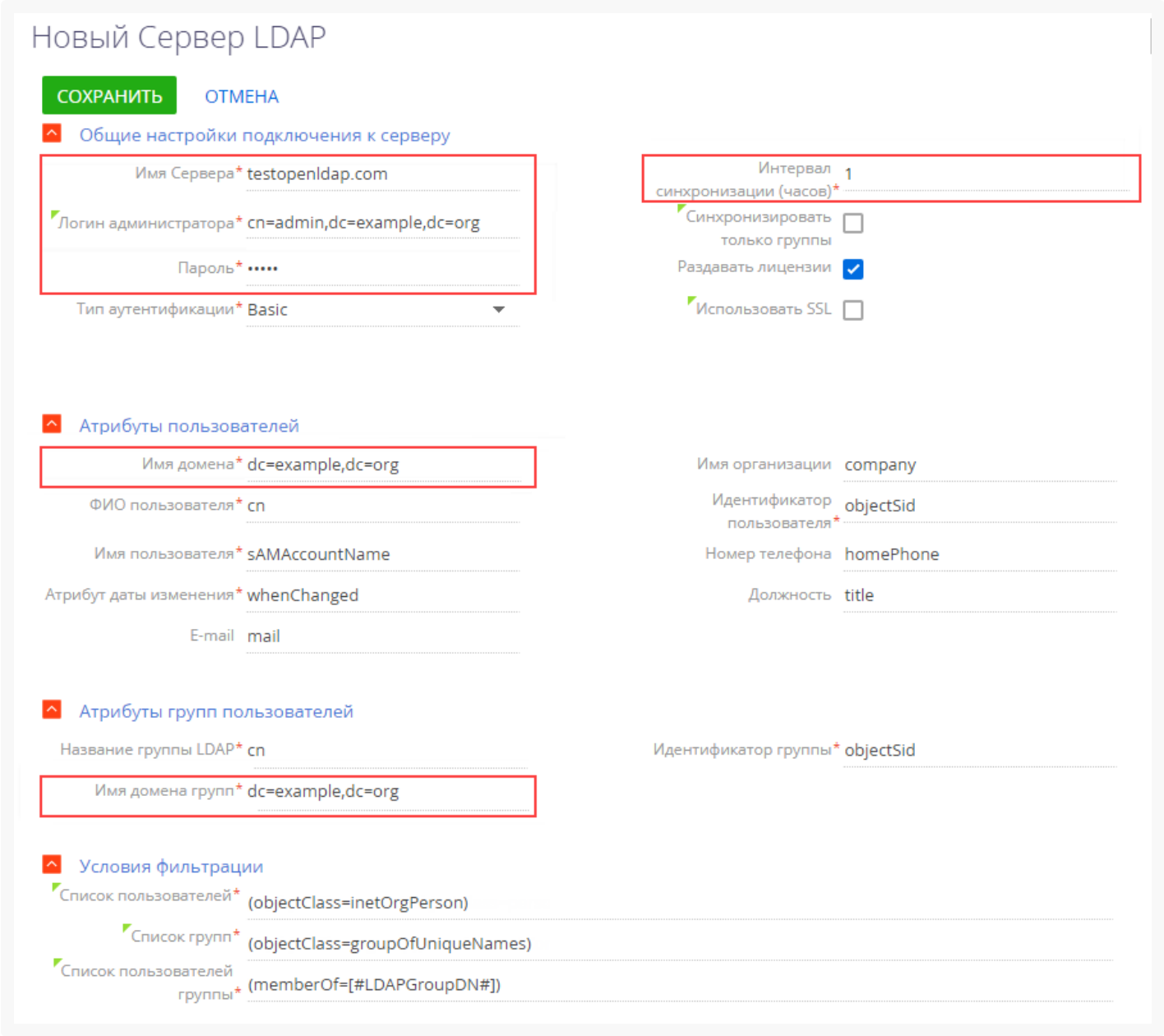


Рис. 2 — Страница настроек интеграции с LDAP для OpenLDAP



1. Настроить подключение к серверу

Укажите общие настройки подключения к серверу:

1. [*Имя сервера*] — имя или IP-адрес сервера LDAP.
2. [*Тип аутентификации*] — выбор протокола соединения с LDAP-сервером. Тип аутентификации определяется используемым сервером LDAP, а также требованиями к защищенности аутентификации. Например, выберите тип “Ntlm” для аутентификации “NT LanManager”, поддерживаемой Windows.

> **На заметку.** Если вы выберете тип аутентификации “Kerberos”, то в полях [*Имя сервера*] и [*Центр распределения ключей*] необходимо указать доменное имя (URL-адрес), но не IP-адрес. Сервер приложений Creatio должен быть включен в домен, в котором находится LDAP-сервер и центр распределения ключей.

3. [*Логин администратора*], [*Пароль*] — учетные данные администратора. Если сервер Creatio **установлен на Linux**, то используйте формат “domain\login“.

   На заметку. Убедитесь, что у администратора есть права на чтение информации о пользователях и группах.

4. [*Интервал синхронизации (часов)*] — интервал, по которому будет происходить автоматическая синхронизация пользователей с LDAP. Подробнее: Запустить синхронизацию с LDAP.
5. [*Синхронизировать только группы*] — установка признака автоматически деактивирует в Creatio пользователей, вручную исключенных из синхронизируемых групп в каталоге LDAP и активирует в Creatio пользователей, добавленных вручную в синхронизируемые с приложением LDAP группы.
6. [*Раздавать лицензии*] — установка признака обеспечивает автоматическую выдачу лицензий при синхронизации пользователей по LDAP.
7. [*Использовать SSL*] — установка признака активирует синхронизацию с использованием сертификата SSL. При установке признака укажите в поле [*Имя Сервера*] значение в формате "сервер:порт".
   Значение порта по умолчанию для LDAPS-соединения — "636". Синхронизация по LDAPS поддерживается только в приложении на Windows.
   Значение порта по умолчанию для LDAP-соединения — "389".

   На заметку. Если приложение развернуто в облаке (cloud), то при использовании самоподписанного сертификата необходимо воспользоваться услугой выделенного блока и предоставить сертификат службе технической поддержки Creatio для указания его доверенным.

2. Настроить синхронизацию пользователей

Для настройки синхронизации пользователей укажите атрибуты элементов каталога LDAP, из которых будут импортированы данные о пользователях:

1. Укажите **обязательные** атрибуты:

   a. [*Имя домена*] — уникальное имя элемента организационной структуры LDAP, в который входят синхронизируемые пользователи. При этом для синхронизации будут доступны только те пользователи, которые входят в указанный элемент либо в подчиненные ему элементы, вне зависимости от уровня вложенности. Например, если вы укажете корневой элемент структуры каталога, то для синхронизации будут доступны все пользователи в каталоге.

   b. [*ФИО пользователя*] — атрибут LDAP, который содержит имя и фамилию пользователя LDAP. Значение атрибута используется для автоматического заполнения поля [*ФИО*] страницы контакта при импорте пользователей. Например, ФИО пользователя может содержать атрибут “name” или “cn” (Common Name).

   c. [*Имя пользователя*] — атрибут, который содержит имя пользователя LDAP, используемое для входа в систему. Пользователь, учетная запись которого синхронизирована с LDAP, будет входить в систему под этим именем. Например, “sAMAccountName”.

d. [*Уникальный идентификатор пользователя*] — атрибут, который может быть использован в качестве уникального идентификатора пользователя. Значение указанного атрибута должно быть уникальным для каждого пользователя.

e. [*Атрибут даты изменения*] — атрибут, в который автоматически записывается дата и время последнего изменения элемента LDAP.

Важно. Отсутствие хотя бы одного из вышеперечисленных атрибутов синхронизируемого пользователя приведет к ошибке интеграции с LDAP.

2. При необходимости укажите **дополнительные** атрибуты, из которых будет взята информация для автоматического заполнения страницы контакта пользователя:

a. [*Имя организации*] — атрибут с названием организации, в которой работает пользователь. Используется для заполнения поля [*Контрагент*] страницы контакта. При синхронизации в поле указывается контрагент, название которого полностью соответствует значению указанного атрибута.

b. [*Должность*] — атрибут, который содержит должность пользователя. Используется для заполнения поля [*Должность*] страницы контакта. При синхронизации будет выбрана из справочника должность, название которой полностью соответствует значению указанного атрибута.

На заметку. Организации и должности в системе не создаются автоматически в результате синхронизации, их необходимо создавать вручную.

c. [*Номер телефона*] — атрибут, который содержит номер рабочего телефона пользователя. Используется для заполнения поля [*Рабочий телефон*] страницы контакта.

d. [*E-mail*] — атрибут, который содержит адрес электронной почты пользователя. Используется для заполнения поля [*Email*] страницы контакта.

Важно. Если поля не заполнены, то соответствующие поля страницы контакта не будут автоматически заполняться при импорте пользователей из LDAP.

3. Настроить синхронизацию групп пользователей LDAP с ролями Creatio

Настройка синхронизации групп обеспечивает возможность привязки групп LDAP к элементам организационной структуры Creatio. Для настройки укажите атрибуты элементов каталога LDAP, из которых будут импортированы данные о группах:

1. [*Название группы LDAP*] — атрибут, который содержит название группы пользователей в LDAP. Например, здесь можно указать атрибут “cn” (“Common Name”).

2. [*Идентификатор группы*] — атрибут, который может быть использован в качестве уникального идентификатора группы. Значение указанного атрибута должно быть уникальным для каждой группы. Например, может быть использован атрибут “objectSid”.

3. [*Имя домена групп*] — уникальное имя элемента организационной структуры LDAP, в который входят синхронизируемые группы. Для синхронизации будут доступны только те группы, которые входят в указанный элемент либо в подчиненные ему элементы независимо от уровня вложенности. Например, если вы укажете корневой элемент структуры каталога, то для синхронизации будут доступны все группы в каталоге.

На заметку. В процессе синхронизации система проверяет пользователей, которые входят в участвующие в синхронизации группы. Если дата, которая хранится в атрибуте даты изменения пользователя LDAP, превышает дату последней синхронизации, то происходит актуализация вхождения этих пользователей в элементы организационной структуры Creatio.

Важно. Отсутствие хотя бы одного из вышеперечисленных атрибутов синхронизируемого пользователя приведет к ошибке интеграции с LDAP.

4. Настроить условия фильтрации

Настройка условий фильтрации позволяет определить, по каким критериям элементы LDAP будут включаться в список синхронизируемых групп и пользователей. Укажите общие настройки подключения к серверу для Active Directory:

1. [*Список пользователей*] — фильтр, по которому из общего списка элементов каталога LDAP будут выбраны только те, которые будут синхронизированы с пользователями Creatio. Фильтр должен выбирать только активные элементы.
2. [*Список групп*] — фильтр, по которому будут выбраны только элементы LDAP для синхронизации с элементами организационной структуры Creatio (организационными ролями). Фильтр должен выбирать только активные элементы.
3. [*Список пользователей группы*] — фильтр для получения списка пользователей, которые входят в группу LDAP. Вхождение пользователя в группу определяется одним или несколькими атрибутами. Например, в большинстве каталогов используется такой атрибут, как “memberOf”. Фильтр (memberOf=[#LDAPGroupDN#]) содержит макрос Creatio и приведет к получению всех объектов (пользователей), которые входят в группу [#LDAPGroupDN#].

На заметку. Каждое логическое выражение необходимо обрамлять скобками (), чтобы фильтр работал корректно и на ОС Linux, и на ОС Windows. Подробнее: Настроить фильтры Active Directory.

Привязать элементы LDAP к пользователям и ролям Creatio

В Creatio существует возможность синхронизации организационных и функциональных ролей пользователей системы с группами Active Directory.

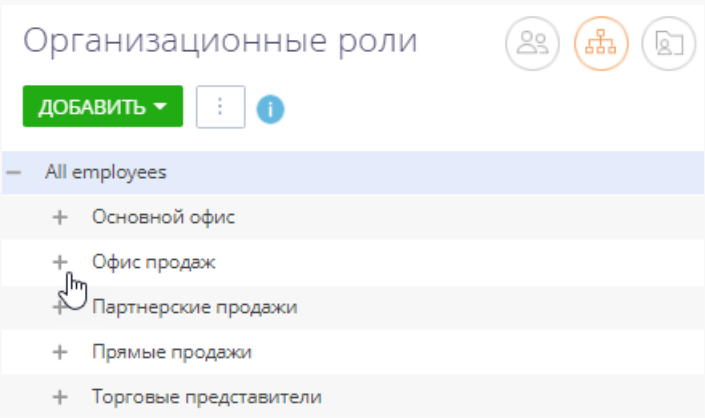
Вы можете перенести в приложение организационную структуру компании и настройки всех ролей из Active Directory после выполнения синхронизации с LDAP.

Настроить синхронизацию организационных ролей Creatio и групп Active Directory

1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Организационные роли”.
3. На открывшейся странице выберите из дерева групп роль, для которой вы хотите настроить синхронизацию (Рис. 3).

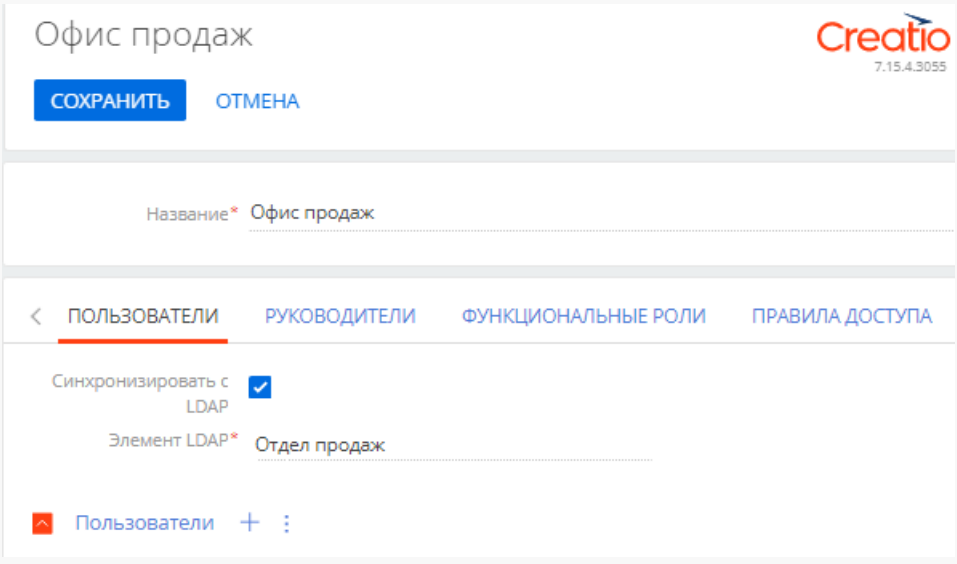
   Если нужной роли в дереве групп нет, то нажмите кнопку [*Добавить*] и выберите “Организацию” или “Подразделение” в зависимости от того, какую роль необходимо добавить. На открывшейся странице укажите название группы.

Рис. 3 — Выбор организационной роли для настройки синхронизации



4. На вкладке [*Пользователи*] установите признак [*Синхронизировать с LDAP*]. В поле [*Элемент LDAP*] выберите группу Active Directory, соответствующую данной организационной роли в Creatio (Рис. 4).

Рис. 4 — Выбор группы Active Directory для настройки синхронизации



5. Если необходимо, то добавьте новых пользователей на детали [*Пользователи*], нажав кнопку .

   Чтобы синхронизировать большое количество пользователей, которые еще не были зарегистрированы в Creatio, рекомендуем импортировать их из каталога LDAP. Подробнее:

Импортировать новых пользователей из Active Directory.

6. Примените настройки по кнопке [*Сохранить*].

В результате при следующей синхронизации будет синхронизироваться и выбранная организационная роль.

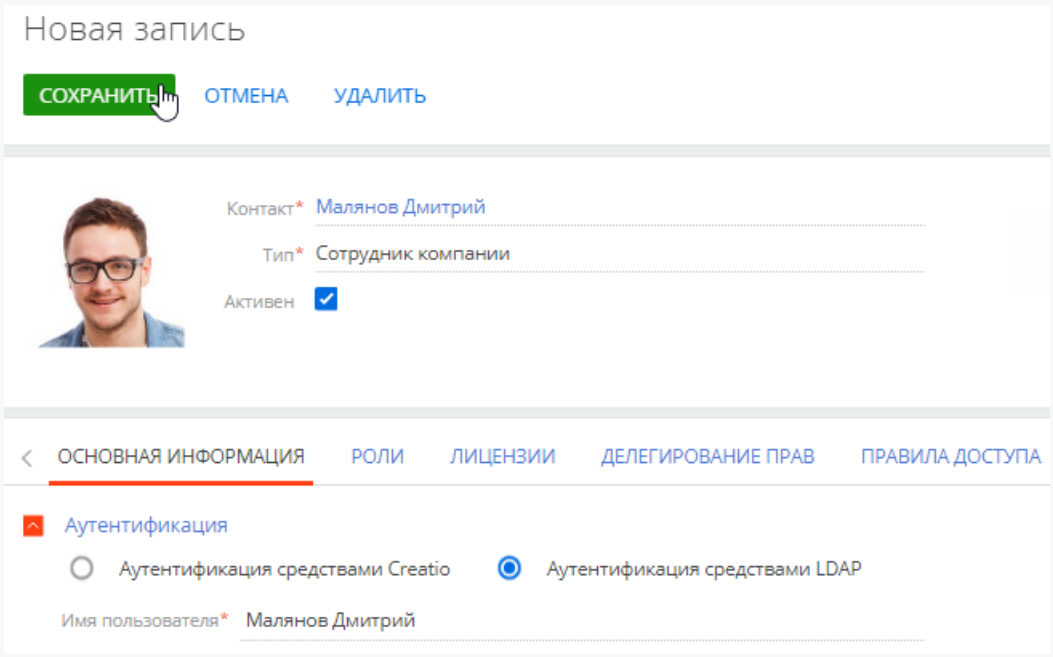
Настроить синхронизацию функциональных ролей Creatio и групп Active Directory

1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Функциональные роли”.
3. Дальнейшие настройки аналогичны **пунктам 3–5** настроек синхронизации организационных ролей Creatio и групп **Active Directory**, описанным выше.

Связать учетные записи пользователей Creatio и пользователей LDAP

1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Организационные роли” либо “Функциональные роли” в зависимости от того, для пользователей каких групп вы хотите настроить синхронизацию.
3. На открывшейся странице выберите роль, в которую входит нужный пользователь.
4. Перейдите на вкладку [*Пользователи*], выберите строку, содержащую данные нужного пользователя, и с помощью двойного клика откройте его страницу.
5. На вкладке [*Основная информация*] выберите опцию [*Аутентификация средствами LDAP*].
6. В поле [*Имя пользователя*] выберите необходимого пользователя LDAP.
7. Примените настройки по кнопке [*Сохранить*] (Рис. 5).

Рис. 5 — Привязка пользователя



В результате выбранный пользователь Creatio будет связан с пользователем LDAP и сможет входить в систему, используя имя пользователя и пароль, которые хранятся в каталоге LDAP (например, имя и пароль доменного пользователя).

В процессе синхронизации изменения, которые произошли с пользователями и группами LDAP, переносятся на связанные с ними учетные записи пользователей и элементы организационной структуры Creatio.

Запустить синхронизацию с LDAP

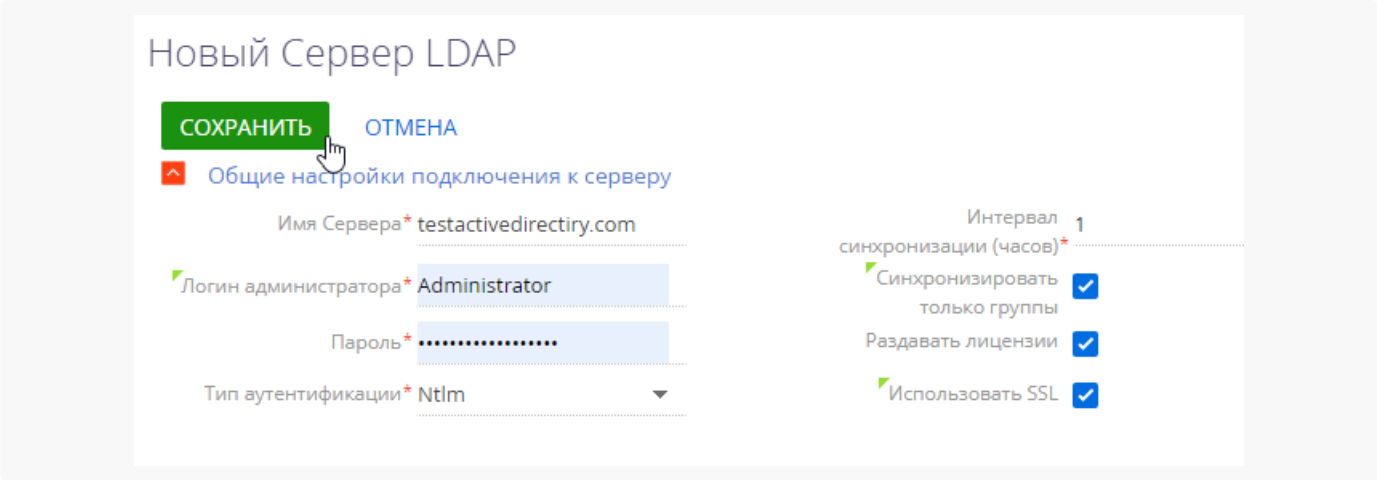
Настроить автоматическую синхронизацию

1. Откройте дизайнер системы, например, по кнопке в правом верхнем углу приложения.
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка интеграции с LDAP”.
3. На открывшейся странице заполните поле [*Интервал синхронизации (часов)*]. Автоматическая синхронизация пользователей с LDAP будет выполняться с указанным интервалом.

> **На заметку.** Заполнение остальных полей на странице [*Настройка интеграции с LDAP*] описано в блоке Настроить интеграцию с LDAP.

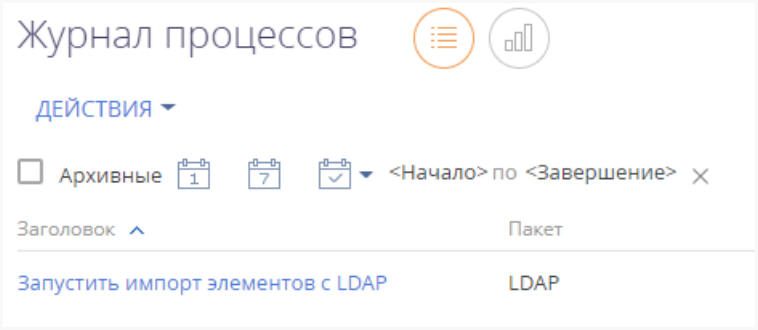
4. Нажмите кнопку [*Сохранить*] (Рис. 6).

Рис. 6 — Сохранение заполненной страницы интеграции с LDAP



После сохранения страницы интеграции с LDAP автоматически запустится синхронизация. При этом будет запущен процесс “Запустить импорт элементов с LDAP” (Рис. 7).

Рис. 7 — Процесс “Запустить импорт элементов с LDAP”



Запустить синхронизацию вручную

1. Откройте дизайнер системы, например, по кнопке в правом верхнем углу приложения.
2. В группе “Пользователи и администрирование” кликните по ссылке “Организационные роли”.
3. В меню действий раздела выберите действие [*Синхронизировать с LDAP*] (Рис. 8). При этом запустится процесс “Запустить синхронизацию с LDAP”, который в свою очередь вызывает процесс “Синхронизировать данные о пользователях с LDAP” (Рис. 9).

Рис. 8 — Действие [*Синхронизировать с LDAP*]

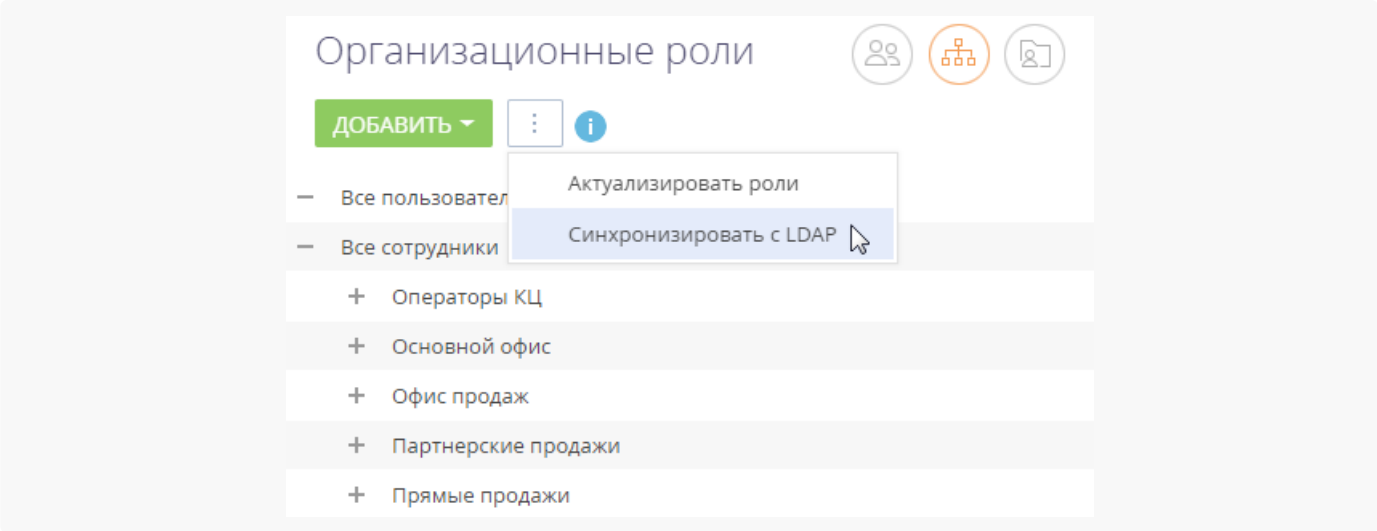
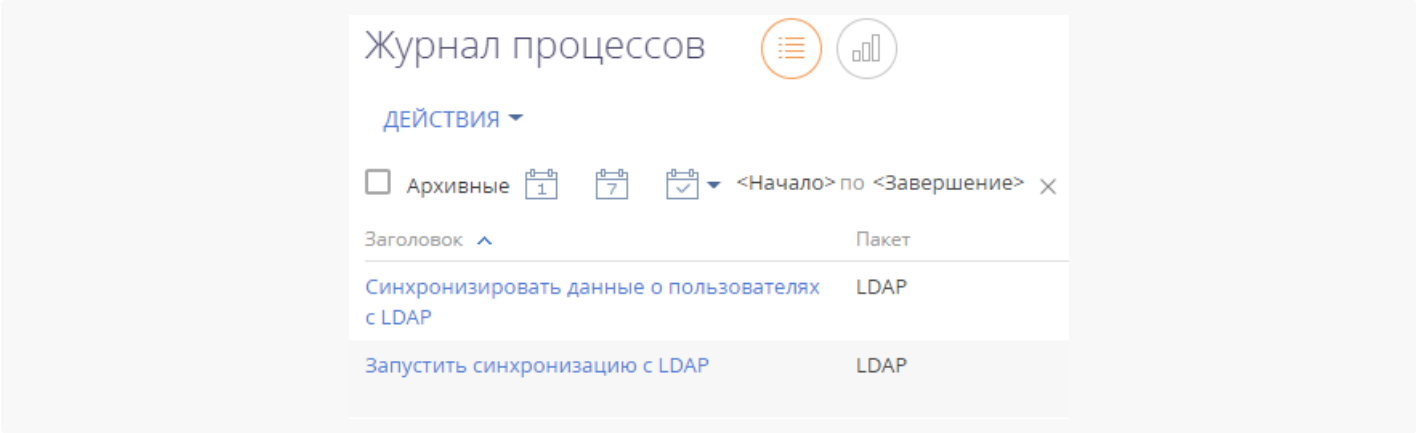


Рис. 9 — Процессы “Запустить синхронизацию с LDAP” и “Синхронизировать данные о пользователях с LDAP”



После завершения процесса синхронизации будет отображено информационное сообщение.

На заметку. Если при синхронизации с каталогом LDAP количество пользователей превысит количество доступных лицензий, то администраторы системы получат уведомление на коммуникационной панели и детальную информацию в email-сообщении.

Результаты синхронизации

- Если пользователь LDAP более не входит в список активных пользователей, то на странице синхронизируемого с ним пользователя Creatio будет снят признак [*Активен*], и он не сможет залогиниться.
- Если ранее неактивный пользователь LDAP был активирован, то на странице синхронизируемого с ним пользователя Creatio будет установлен признак [*Активен*].
- Если пользователь LDAP либо группа пользователей LDAP были переименованы, то будут переименованы и синхронизированные с ними пользователь/роль Creatio.
- В случае установки признака в поле [*Синхронизировать только группы*] при исключении пользователя LDAP из группы LDAP, связанной с элементом организационной структуры Creatio,

синхронизируемый с ним пользователь Creatio будет деактивирован и исключен из соответствующего элемента организационной структуры Creatio.

- В случае установки признака в поле [*Синхронизировать только группы*] при добавлении пользователя в группу LDAP, связанную с элементом организационной структуры Creatio, связанный с ним пользователь Creatio будет добавлен в соответствующий элемент структуры и активирован.
- Если в синхронизируемый элемент LDAP были включены новые пользователи, ранее не синхронизированные с Creatio, то пользователи будут импортированы в Creatio.
- Если в Creatio есть пользователи (не импортированные из LDAP) с именами, совпадающими с именами пользователей в LDAP, то их синхронизация не выполняется.
- Если синхронизированный пользователь LDAP был удален из группы, связанной с элементом организационной структуры Creatio, то соответствующий пользователь останется активным в Creatio, но не сможет залогиниться.
- Всем синхронизированным пользователям будут предоставлены лицензии, если установлен соответствующий признак. Подробнее: Настроить подключение к серверу.

Настроить фильтры Active Directory

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Правильная настройка фильтров Active Directory обеспечит необходимые параметры для синхронизации пользователей, групп и пользователей определенной группы.

Формат фильтров

В общем случае фильтры Active Directory имеют следующий формат:

```
(<оператор><фильтр1><фильтр2>)
```

В котором <фильтр1> имеет вид:

```
(<атрибут><оператор><значение>)
```

Вы можете использовать необходимое количество операторов и фильтров при настройке фильтрации. Для создания и настройки фильтров используются следующие операторы:

`=` — Логическое равенство.

`~=` — Приблизительное равенство.

`=>` — Больше или равно.

`<=` — Меньше или равно.

`&` — “И”.

`|` — “Или”.

`!` — “Не”.

Значения представляют фактические значения атрибутов Active Directory. Они не чувствительны к регистру и не заключаются в кавычки. Кроме того, возможно использование символа подстановки “*”, например, для получения всех элементов в виде: `(objectClass=*)`.

Каждое логическое выражение необходимо обрамлять скобками, чтобы фильтр работал корректно и на ОС Linux, и на ОС Windows.

Пример корректно настроенного фильтра

```
(&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(|(cn=szgroup)(cn=CoreCC*)
```

Пример некорректно настроенного фильтра

```
(&(objectClass=group)(!userAccountControl:1.2.840.113556.1.4.803:=2)(|(cn=szgroup)(cn=CoreCC*)(c
```

Фильтрация пользователей

Если в вашей компании используется служба каталогов Active Directory, то рекомендуем воспользоваться стандартным фильтром для синхронизации активных пользователей:

```
(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDeleted=TRUE)))
```

В этой функции:

`&` — Оператор “И” для всех фильтров.

`objectClass=user` — Выбор в массиве всех элементов “user”.

`objectClass=person` — Выбор в массиве всех элементов “person”.

`!(objectClass=computer)` — Исключить все элементы “computer”.

`!(isDeleted=TRUE)` — Объекты не удалены.

Фильтрация групп

Чтобы синхронизировать пользователей Active Directory с организационной структурой Creatio, необходимо настроить фильтрацию групп. Как и в случае с синхронизацией пользователей, воспользуйтесь стандартным фильтром для синхронизации групп всех активных пользователей:

```
(&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

В этой функции:

`&` — Оператор “И” для всех фильтров.

`objectClass=group` — Выбор в массиве всех элементов групп.

`userAccountControl` — Флаги контроля учетных записей, числовое обозначение.

`:1.2.840.113556.1.4.803:` — Побитовое “И” в формате LDAP.

`2` — флаг “ACCOUNTDISABLE”.

Таким образом, фильтр `(!(userAccountControl:1.2.840.113556.1.4.803:=2))` исключает отключенные (неактивные) аккаунты. Подробнее читайте на сайте поддержки Microsoft.

Стандартные фильтры пользователей группы Active Directory

Кроме фильтрации пользователей и организационной структуры, дополнительно нужно получить список пользователей, которые входят в группу Active Directory и, соответственно, в LDAP. Стандартный фильтр, который находит весь список пользователей в группе, имеет вид:

```
(memberOf=[#LDAPGroupDN#])
```

В этой функции:

`memberOf` — стандартный атрибут объекта Active Directory, определяет имя группы, к которой принадлежит данный объект;

`#LDAPGroupDN#` — макрос Creatio для получения списка пользователей группы с уникальным именем (т.н. Distinguished Name).

Макросы не являются стандартом LDAP и используются только для формирования запроса на выборку объектов. В зависимости от настроек AD, можно использовать следующие параметры:

`#LDAPGroupName#` — название группы, указанной в поле [*Название группы LDAP*] в настройках интеграции с LDAP.

`#LDAPGroupIdentity#` — уникальный идентификатор группы, указанный в поле [*Идентификатор группы*].

Настроить фильтры для синхронизации пользователей/групп

В зависимости от потребностей, вы можете самостоятельно настроить фильтры для синхронизации пользователей и групп.

> **Пример.** Необходимо различать сотрудников с одинаковыми ФИО после синхронизации с Active Directory.

Чтобы решить задачу, нужно дополнить фильтр синхронизации пользователей. При поиске объектов по

умолчанию используется атрибут cn (Common Name). Он обязателен для корректной работы Creatio, так как связан с полем [*ФИО пользователя*]. В условия фильтрации можно также включить атрибут “displayName”, который будет отличаться для разных пользователей. То есть, необходимо синхронизировать пользователей с атрибутом “displayName”. Для этого:

1. Откройте настройки синхронизации с LDAP.
2. Перед стандартным фильтром списка пользователей добавьте условие “атрибут displayName заполнен”. Фильтр будет выглядеть следующим образом:

   ```
   (displayName=*)(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDeleted=
   ```

3. Добавьте булеву функцию «И» для одновременного выполнения условий фильтрации:

   ```
   (&(displayName=*)(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDelete
   ```

4. Замените стандартный фильтр в поле [*Список пользователей*] полученным фильтром.
5. Сохраните настройки и запустите синхронизацию с LDAP.

Импортировать новых пользователей и роли из Active Directory

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Если вы используете Active Directory, то вы можете импортировать пользователей из каталогов в Creatio посредством синхронизации с LDAP. Синхронизация позволит скопировать пользователей и роли из Active Directory в Creatio.

Подготовить каталог к интеграции

Перед добавлением пользователей посредством синхронизации с LDAP подготовьте каталог к интеграции:

1. Убедитесь, что пользователи входят в группы Active Directory, которые будут синхронизированы с Creatio. Пользователи Active Directory (AD), не принадлежащие ни к одной группе пользователей AD, не будут импортированы. В Creatio импортируется только организационная структура, представленная группами пользователей AD.
2. Настройте интеграцию с LDAP. После того как вы нажмете [*Сохранить*] на странице настройки интеграции с LDAP, Creatio уведомит вас о запуске бизнес-процесса, в фоновом режиме выполняющего импорт пользователей и ролей из LDAP.

Импортировать новых пользователей из LDAP

1. Перейдите в дизайнер системы, например, по кнопке  .

2. В блоке “Пользователи и администрирование” перейдите по ссылке “Организационные роли” либо “Функциональные роли” в зависимости от того, в какие группы вы хотите импортировать пользователей.
   Вы также можете создать новую роль для группы пользователей AD в организационной структуре Creatio. Для этого:

   a. Выберите родительскую роль (например, “Все сотрудники” для добавления пользователей или “Все пользователи портала” для добавления пользователей портала) —> [*Добавить*] —> [*Организацию*].

   b. Укажите название для новой роли. Название может совпадать с названием группы в AD или же отличаться от него.

3. В дереве ролей выберите элемент, в который будут импортироваться пользователи LDAP.
4. На вкладке [*Пользователи*] установите признак [*Синхронизировать с LDAP*]. В поле [*Элемент LDAP*] выберите группу Active Directory, соответствующую данной организационной роли в Creatio.
5. Нажмите [*Сохранить*].
6. Запустите синхронизацию по действию [*Синхронизировать с LDAP*] в меню действий раздела. После завершения синхронизации в выбранную организационную или функциональную группу импортируются все пользователи из группы на сервере LDAP.

На заметку. Если синхронизация LDAP была выполнена с ошибкой, то вы можете определить ее причину, проверив экземпляры бизнес-процесса “Синхронизировать данные о пользователях с LDAP” в разделе [*Журнал процессов*].

В результате для выбранных пользователей LDAP будут созданы контакты и связанные с ними учетные записи пользователей Creatio. Новые учетные записи будут автоматически помещены в выбранный элемент организационной структуры. При этом поля на страницах контактов импортированных пользователей автоматически заполняются значениями атрибутов элементов LDAP, указанными при настройке синхронизации.

Важно. В списке пользователей LDAP отображаются все пользователи, независимо от того, включены они в элемент LDAP, связанный с элементом организационной структуры, или нет.

При синхронизации с LDAP будут синхронизированы только те пользователи, которые входят в элемент LDAP, связанный с элементом организационной структуры.

На заметку. При связывании пользователя LDAP с учетной записью пользователя Creatio происходит автоматическое лицензирование последней, если установлен сответствующий признак. Подробнее: Настроить подключение к серверу.

Настроить аутентификацию с LDAP

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Настроить аутентификацию пользователей через LDAP на .NET Framework

Для включения возможности авторизации пользователей с помощью LDAP внесите изменения в файл Web.config в корневой папке приложения. Настройки для Active Directory и OpenLDAP имеют некоторые различия.

1. Укажите “Ldap” и “SspLdapProvider” в списке доступных провайдеров авторизации. Шаг выполняется одинаково для Active Directory и OpenLDAP:

```
<terrasoft>
<auth providerNames="InternalUserPassword,Ldap,SSPLdapProvider" autoLoginProviderNames="" def
<providers>
```

Важно. Необходимо соблюдать регистр согласно примеру. Также обратите внимание, что названия провайдеров должны быть приведены через запятую и без пробелов.

2. Укажите IP или адрес сервера, а также параметры домена для пользователей в секции “Ldap”. Параметры для Active Directory и OpenLDAP различаются.

Для Active Directory

```
<provider name="Ldap" type="Terrasoft.WebApp.Loader.Authentication.Ldap.LdapProvider, Terraso
<parameters>
...
    <add name="ServerPath" value="testactivedirectory.com" />
    <add name="AuthType" value="Ntlm" />
    <add name="DistinguishedName" value="dc=tscrm,dc=com" />
    <add name="UseLoginUserLDAPEntryDN" value="false" />
    <!--<add name="SearchPattern"
    value="(&amp;(objectCategory=person)(objectClass=user)
    (!(userAccountControl:1.2.840.113556.1.4.803:=2))
    memberOf=CN=SVNUsers,OU=groups,OU=Terrasoft,DC=tscrm,DC=com))" />-->
    <add name="SearchPattern"
    value="(&amp;(sAMAccountName={0})(objectClass=person))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

Для OpenLDAP

```
<provider name="Ldap" type="Terrasoft.WebApp.Loader.Authentication.Ldap.LdapProvider, Terraso
<parameters>
...
```

```
    <add name="ServerPath" value="testopenldap.com" />
    <add name="AuthType" value="Basic" />
    <add name="DistinguishedName" value="dc=example,dc=org" />
    <add name="UseLoginUserLDAPEntryDN" value="true" />
    <add name="SearchPattern"
    value="(&amp;(uid={0})(objectClass=inetOrgPerson))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

- **ServerPath** — доменное имя (URL-адрес) LDAP сервера, но не IP-адрес.
- **KeyDistributionCenter** — доменное имя (URL-адрес), но не IP-адрес.

На заметку. Если вы выберете тип аутентификации “Kerberos”, то сервер приложений Creatio должен быть включен в домен, в котором находится LDAP-сервер и центр распределения ключей.

3. Укажите IP или адрес сервера, а также параметры домена для портальных пользователей в секции “SspLdapProvider”. Шаг выполняется одинаково для Active Directory и OpenLDAP:

```
<provider name="SSPLdapProvider" type="Terrasoft.WebApp.Loader.Authentication.SSPUserPassword
<parameters>
...
     <add name="ServerPath" value="ldapserver.domain.com" />
...
     <add name="DistinguishedName" value="dc=domain, dc=com" />
...
</parameters>
```

4. Сохраните изменения в файле Web.config.
5. **Шаг только для настройки OpenLDAP**: перед синхронизацией с OpenLDAP-сервером укажите в файле Web.config в Terrasoft.WebApp значение для “UseLoginUserLDAPEntryDN”.

```
<appSettings>
...
    <add key="UseLoginUserLDAPEntryDN" value="true" />
```

Без данной настройки пользователи будут синхронизироваться без значений в поле [*LDAPEntryDN*] таблицы [*SysAdminUnit*], что приведет к проблемам с авторизацией.

Настроить аутентификацию пользователей через LDAP на

.NET Core

Для включения возможности авторизации пользователей с помощью LDAP внесите изменения в файл Terrasoft.WebHost.dll.config в корневой папке приложения. Настройки для Active Directory и OpenLDAP одинаковы.

1. Укажите “Ldap” в списке доступных провайдеров авторизации. Чтобы портальные пользователи могли войти в систему, добавьте провайдер “SspLdapProvider”:

```
<terrasoft>
<auth providerNames="InternalUserPassword,Ldap,SspLdapProvider" autoLoginProviderNames="" def
<providers>
```

Важно. Необходимо соблюдать регистр согласно примеру. Также обратите внимание, что названия провайдеров должны быть приведены через запятую и без пробелов.

2. Укажите настройки провайдера аутентификации “Ldap”:

```
<provider name="LdapProvider" type="Terrasoft.Authentication.Core.Ldap.NetStandardLdapProvide
<parameters>
    <add name="ServerPath" value="testldap.com" />
    <add name="DistinguishedName" value="dc=ctl,dc=com" />
    <add name="UseLoginUserLDAPEntryDN" value="false" />
    <add name="SearchPattern" value="(&amp;(sAMAccountName={0})(objectClass=person))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
    <!--При использовании LDAPS-->
    <add name="SecureSocketLayer" value="false" />
    <add name="CertificateFileName" value="" />
</parameters></provider>
```

- **ServerPath** — доменное имя (URL-адрес) LDAP сервера, но не IP-адрес.
- **KeyDistributionCenter** — доменное имя (URL-адрес), но не IP-адрес.

На заметку. Если вы выберете тип аутентификации “Kerberos”, то сервер приложений Creatio должен быть включен в домен, в котором находится LDAP-сервер и центр распределения ключей.

Чтобы использовать **защищенный протокол LDAPS**, в настройках провайдера аутентификации укажите следующие параметры:

- **SecureSocketLayer** — флаг для использования LDAPS.
- **CertificateFileName** — имя сгенерированного SSL-сертификата для валидации LDAPS-

подключения. Данный сертификат должен находиться в корне приложения. Этот параметр обязательный для заполнения при SecureSocketLayer=true, например:

```
<add name="CertificateFileName" value="ldap_certificate_example.cer" />
<add name="SecureSocketLayer" value="true" />
```

3. Укажите IP или адрес сервера, а также параметры домена для портальных пользователей в секции “SspLdapProvider”:

```
<provider name="SSPLdapProvider" type="Terrasoft.WebApp.Loader.Authentication.SSPUserPassword
<parameters>
    <add name="ServerPath" value="ldapserver.domain.com" />
...
    <add name="DistinguishedName" value="dc=domain, dc=com" />
…
</parameters>
```

4. Сохраните изменения в файле Terrasoft.WebHost.dll.config.

Настроить провайдеры аутентификации

Настройка провайдеров аутентификации осуществляется одинаково для приложений на **.NET Framework** и **.NET Core**. Настройки вносятся в следующих файлах, которые находятся в корневой директории приложения:

- **Web.config** для приложения на **.NET Framework**.
- **Terrasoft.WebHost.dll.config** для приложения на **.NET Core**.

Для настройки откройте файл в текстовом редакторе и укажите провайдеров аутентификации:

```
auth providerNames="InternalUserPassword,SSPLdapProvider,Ldap" autoLoginProviderNames="NtlmUser,
```

- **InternalUserPassword** — провайдер, указанный по умолчанию. Если вы хотите предоставить возможность аутентификации по NTLM-протоколу только пользователям, которые не синхронизированы с LDAP, то не указывайте для параметра [*providerNames*] дополнительные значения.
- **Ldap** — добавьте к значениям параметра [*providerNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям приложения, которые синхронизированы с LDAP.
- **SSPLdapProvider** — добавьте к значениям параметра [*providerNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям портала самообслуживания, которые синхронизированы с LDAP.
- **NtlmUser** — добавьте к значениям параметра [*autoLoginProviderNames*] данный провайдер, чтобы

предоставить возможность аутентификации по NTLM-протоколу пользователям приложения, независимо от того, синхронизированы ли они с LDAP и какой тип аутентификации установлен для данных пользователей в Creatio.

- **SSPNtlmUser** — добавьте к значениям параметра [*autoLoginProviderNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям портала самообслуживания, независимо от того, синхронизированы ли они с LDAP и какой тип аутентификации установлен для данных пользователей в Creatio.
- Порядок записи провайдеров параметра [*autoLoginProviderNames*] определяет, в каком порядке выполняется проверка наличия пользователя системы среди пользователей приложения (NtlmUser) или среди пользователей портала (SSPNtlmUser). Например, чтобы проверка осуществлялась в первую очередь среди пользователей основного приложения, укажите провайдер **NtlmUser** первым в списке значений параметра [*autoLoginProviderNames*].

Важно. Вы можете указать в качестве значения параметра [*autoLoginProviderNames*] провайдер **SSPNtlmUser**, только если указан дополнительно провайдер **NtlmUser**. Существует возможность использовать отдельно только провайдер **NtlmUser**.

Настроить доменную авторизацию

Если вы хотите активировать **сквозную аутентификацию**, чтобы пользователь имел возможность авторизоваться в Creatio, минуя страницу входа, то укажите значение “true” для параметра [*UsePathThroughAuthentication*] элемента <appSettings>:

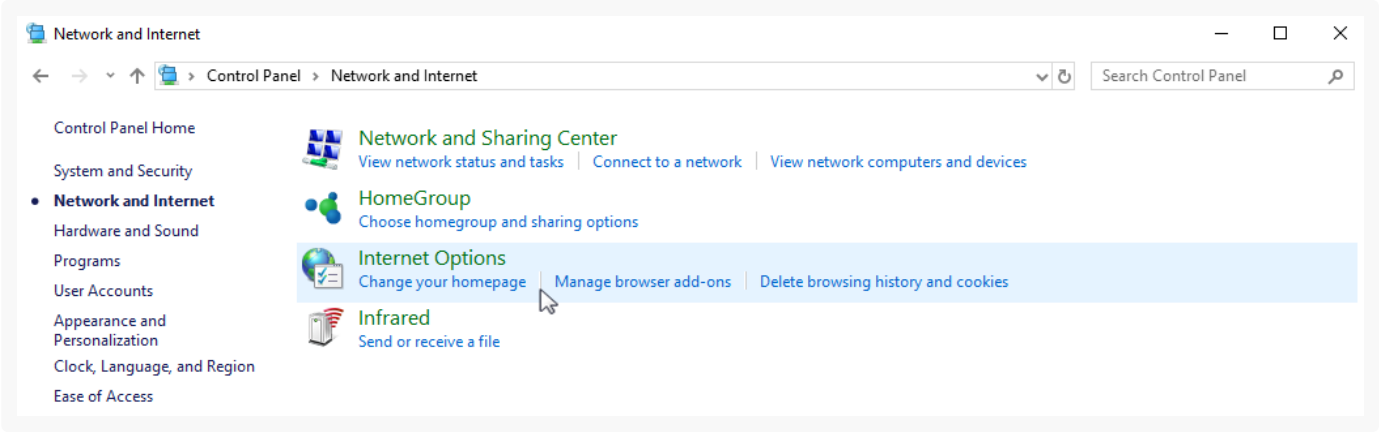
```
<appSettings> <add key="UsePathThroughAuthentication" value="true" /> ... </appSettings>
```

Для **отображения страницы входа** в систему с доступной ссылкой [*Войти под доменным пользователем*] укажите значение “false” для параметра [*UsePathThroughAuthentication*]. При этом сквозная аутентификация будет выполняться лишь при переходе на главную страницу приложения. Чтобы отобразить страницу входа, добавьте запись /Login/NuiLogin.aspx к адресу сайта.

Если после выполнения описанных действий при первой попытке входа в систему отображается окно доменной авторизации, то необходимо дополнительно настроить свойства обозревателя Windows. Чтобы в дальнейшем окно доменной авторизации не отображалось:

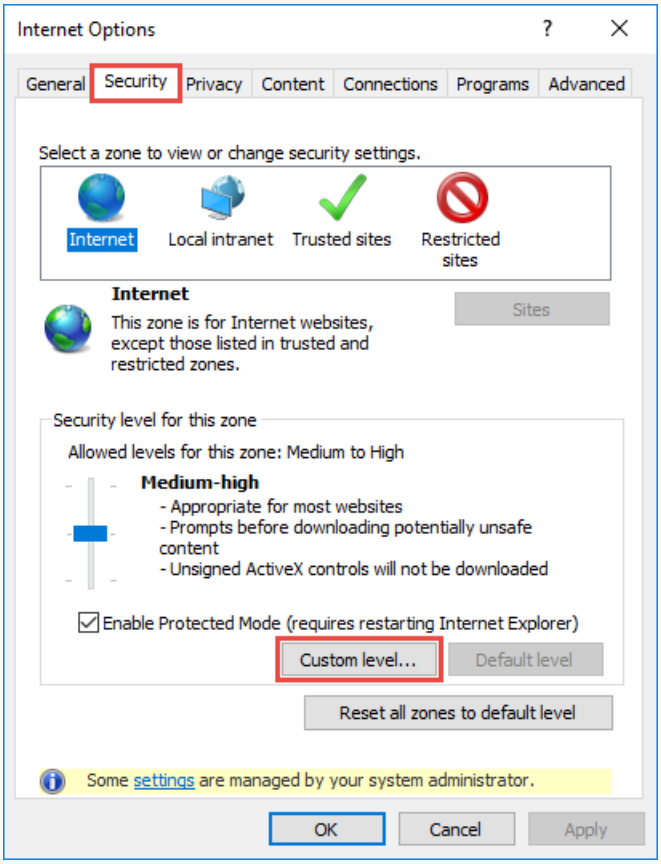
1. В меню “Пуск” (“Start”) → “Параметры” (“Settings”) → “Control Panel” (“Панель управления”) → “Сеть и Интернет” (“Network and Internet”) выберите пункт “Свойства обозревателя” (“Internet options”) (Рис. 1).

Рис. 1 — Настройка свойств обозревателя



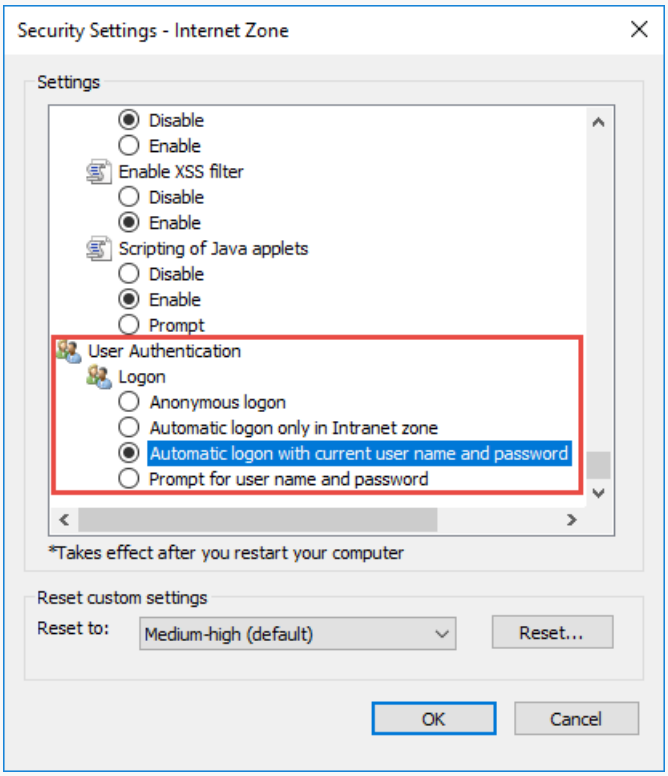
2. В открывшемся окне перейдите на вкладку “Безопасность” (“Security”) и по кнопке “Другой” (“Custom level”) перейдите к настройкам безопасности (Рис. 2).

Рис. 2 — Настройки безопасности



3. В группе настроек “Проверка подлинности пользователя” (“User Authentication”) выберите способ авторизации “Автоматический вход с текущим именем пользователя и паролем” (“Automatic logon with current user name and password”) (Рис. 3).

Рис. 3 — Выбор способа авторизации



4. Нажмите “OK”.

В результате выполненных настроек окно доменной авторизации не будет отображаться при входе в систему.

Часто задаваемые вопросы о синхронизации пользователей с LDAP

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Почему в Creatio импортировались не все пользователи из каталога LDAP?

Это может быть обусловлено рядом причин:

- У пользователей каталога при совпадении значения атрибута “ФИО пользователя” совпадают или отсутствуют значения атрибутов “Email” и “Номер телефона”. Creatio автоматически проверяет дубли значений атрибутов “Имя пользователя”, “Email” и “Номер телефона” при синхронизации с каталогом LDAP.
- Дата, указанная в системной настройке “Максимальная дата изменения элемента LDAP” (код “LDAPEntryMaxModifiedOn”), является более поздней, чем дата в пользовательском атрибуте LDAP “whenChanged”. Creatio импортирует пользователя только в том случае, если дата, указанная в системной настройке “Максимальная дата изменения элемента LDAP”, раньше даты, указанной в пользовательском атрибуте LDAP “whenChanged”.

Почему в Creatio импортировались не все пользователи Active Directory после синхронизации LDAP?

Размер страницы Active Directory может быть меньше, чем количество пользователей. Поскольку Creatio не поддерживает постраничную вычитку при синхронизации пользователей из LDAP, то при указании размера страницы меньше, чем общее количество записей, будет обработана только первая страница. Для решения этой проблемы увеличьте значение “MaxPageSize” в Active Directory таким образом, чтобы все пользователи попали на страницу.

Почему пользователь не может войти под доменной учетной записью после настройки LDAP?

Если приложение Creatio развернуто **on-site**, то отредактируйте файл конфигурации Web.config, который размещен в корневом каталоге сайта. Укажите провайдеры аутентификации в параметре “auth providerNames”:

```
auth providerNames = "InternalUserPassword,Ldap,SSPLdapProvider"
```

После внесения изменений перезапустите синхронизацию с LDAP.

Если приложение развернуто в облаке (**cloud**), то обратитесь в службу поддержки Creatio.

Может ли запись пользователя, импортированного из Active Directory, быть привязана к записи определенного контрагента?

- Если значение атрибута пользователя “Имя организации” совпадает с названием контрагента в Creatio, то Creatio автоматически привяжет импортированного пользователя к записи данного контрагента.
- Если название контрагента, указанное в качестве значения атрибута “Имя организации”, не совпадает с названием какого-либо контрагента в Creatio, то Creatio автоматически привяжет запись импортированного пользователя к записи контрагента “Наша компания”.

Почему не импортируются пользователи из группы “Доменные пользователи” (“Domain users”)?

Группа “Domain users” является первичной группой (“primary group”) для всех пользователей. Атрибут “memberOf“ не отображается в первичных группах. Для импорта таких пользователей добавьте их в другую группу, которая не является первичной.

Что означает ошибка “22021: invalid byte sequence for encoding "UTF8": 0X00” при синхронизации Active Directory

с LDAP?

Данная ошибка возникает в приложениях, развернутых с базой данных PostgreSQL, если в импортированных данных есть системные группы, которые поддерживались в версиях до Windows 2000. Для решения проблемы исключите эти системные группы из синхронизации и измените фильтр групп на следующий:

```
(&(objectClass=group)(!userAccountControl:1.2.840.113556.1.4.803:=2)(!isCriticalSystemObject=TRU
```

Почему возникает ошибка “Cannot insert duplicate key row in object 'dbo.SysAdminUnit' with unique index 'IUSysAdminunitNameDomain'. The duplicate key value is (...)”?

Данная ошибка возникает при синхронизации с LDAP, если пользователь ранее был внесен в систему вручную, а не импортирован из LDAP.

Как настроить фильтр LDAP?

Вы можете получить подробную информацию о настройке LDAP-фильтров в руководстве Internet Engineering Task Force Lightweight Directory Access Protocol (LDAP): Строковое представление поисковых фильтров (перевод статьи Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters).

Также вы можете найти полезную информацию в документации Microsoft Active Directory: Использование LDAP-фильтров.