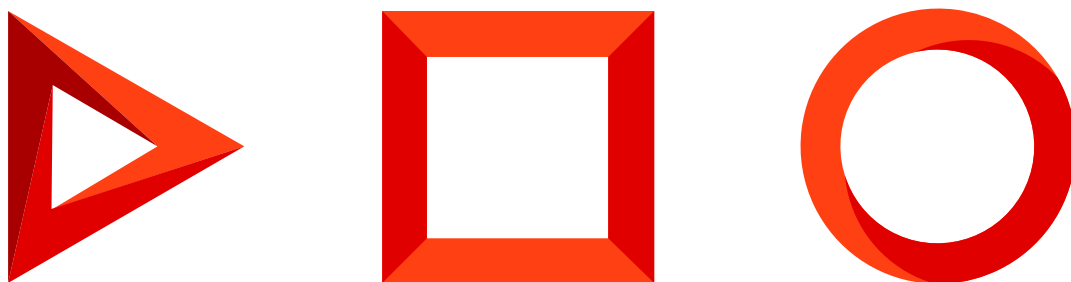


Настройка синхронизации

Настроить синхронизацию 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	4
Настроить интеграцию с LDAP	4
Привязать элементы LDAP к пользователям и ролям Creatio	9
Запустить синхронизацию с LDAP	12

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

Новый Сервер LDAP

СОХРАНИТЬ **ОТМЕНА**

Общие настройки подключения к серверу

Имя Сервера* testactivedirectory.com

Логин администратора* Administrator

Пароль*

Тип аутентификации* Ntlm

Интервал синхронизации (часов)* 1

Синхронизировать только группы ☐

Раздавать лицензии ☒

Использовать SSL ☐

Атрибуты пользователей

Имя домена* dc=cti,dc=com

ФИО пользователя* cn

Имя пользователя* sAMAccountName

Атрибут даты изменения* whenChanged

E-mail mail

Имя организации company

Идентификатор пользователя* objectSid

Номер телефона homePhone

Должность title

Атрибуты групп пользователей

Название группы LDAP* cn

Имя домена групп* dc=cti,dc=com

Идентификатор группы* objectSid

Условия фильтрации

Список пользователей* (&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDeleted=TRUE)))

Список групп* (&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Список пользователей группы* (memberOf=[#LDAPGroupDN#])

Рис. 2 — Страница настроек интеграции с LDAP для OpenLDAP

Новый Сервер LDAP

СОХРАНИТЬ

ОТМЕНА

Общие настройки подключения к серверу

Имя Сервера* testopenldap.com

Логин администратора* cn=admin,dc=example,dc=org

Пароль*

Тип аутентификации* Basic

Интервал
синхронизации (часов)* 1Синхронизировать
только группы ☐Раздавать лицензии ☒Использовать SSL ☐

Атрибуты пользователей

Имя домена* dc=example,dc=org

ФИО пользователя* cn

Имя пользователя* sAMAccountName

Атрибут даты изменения* whenChanged

E-mail mail

Имя организации company

Идентификатор
пользователя* objectSid

Номер телефона homePhone

Должность title

Атрибуты групп пользователей

Название группы LDAP* cn

Имя домена групп* dc=example,dc=org

Идентификатор группы* objectSid

Условия фильтрации

Список пользователей* (objectClass=inetOrgPerson)

Список групп* (objectClass=groupOfUniqueNames)

Список пользователей
группы* (memberOf=[#LDAPGroupDN#])

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.

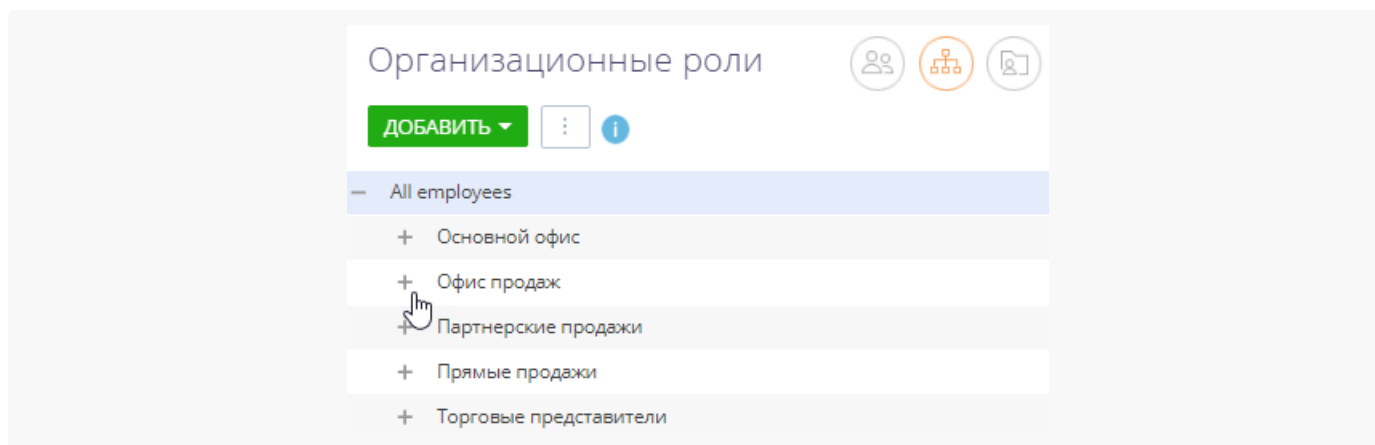
Вы можете перенести в приложение организационную структуру компании и настройки всех ролей из Active Directory после выполнения синхронизации с LDAP.

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).

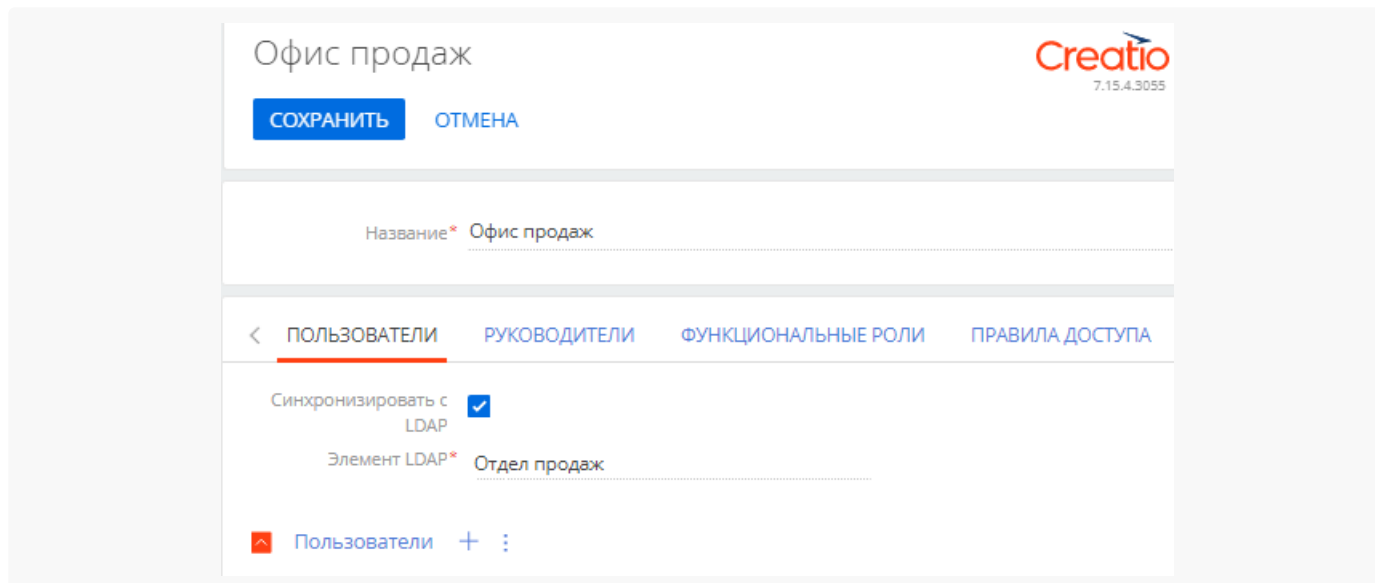
Если нужной роли в дереве групп нет, то нажмите кнопку [*Добавить*] и выберите “Организацию” или “Подразделение” в зависимости от того, какую роль необходимо добавить. На открывшейся странице укажите название группы.

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

Новая запись

СОХРАНИТЬ ОТМЕНА УДАЛИТЬ

Контакт* Маянов Дмитрий

Тип* Сотрудник компании

Активен ☒

< ОСНОВНАЯ ИНФОРМАЦИЯ РОЛИ ЛИЦЕНЗИИ ДЕЛЕГИРОВАНИЕ ПРАВ ПРАВИЛА ДОСТУПА

Аутентификация

☐ Аутентификация средствами Creatio ☒ Аутентификация средствами LDAP


Имя пользователя* Маянов Дмитрий

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.

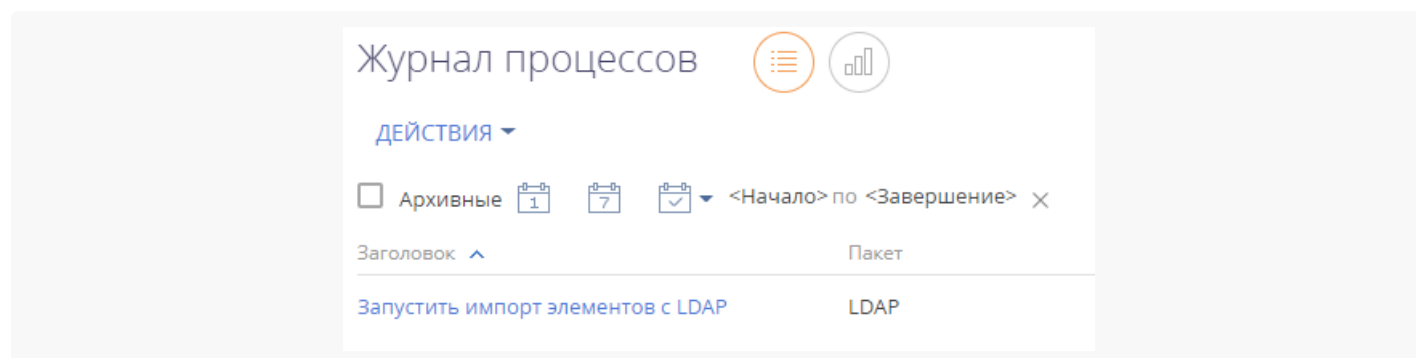
На заметку. Заполнение остальных полей на странице [*Настройка интеграции с LDAP*] описано в блоке [Настроить интеграцию с LDAP](#).

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*]

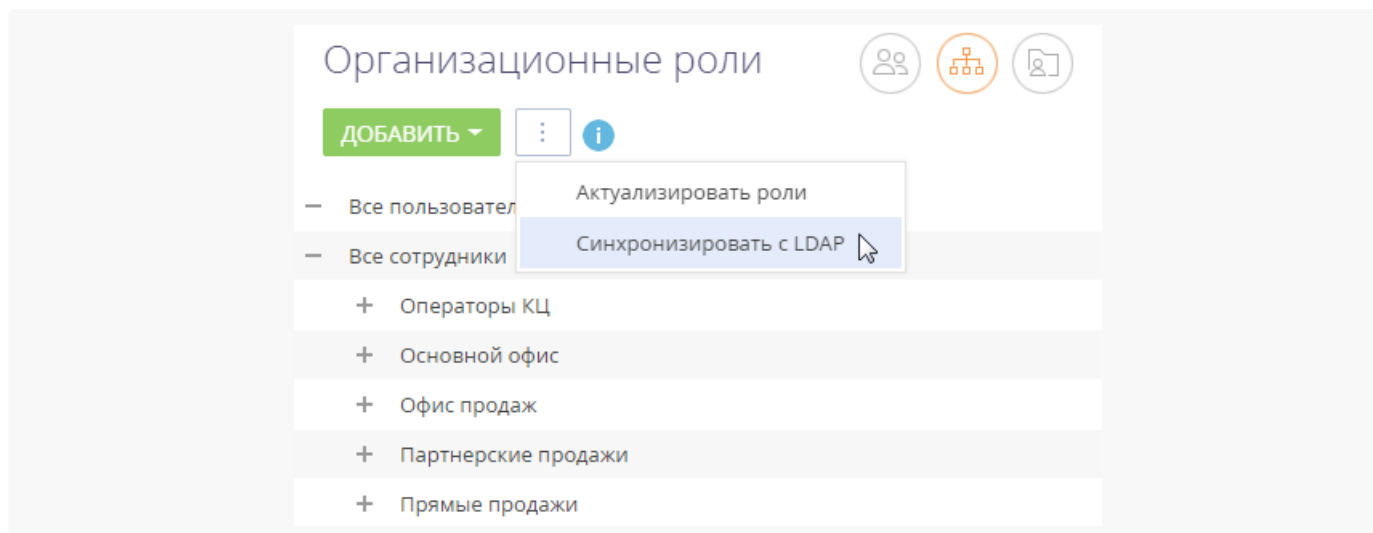
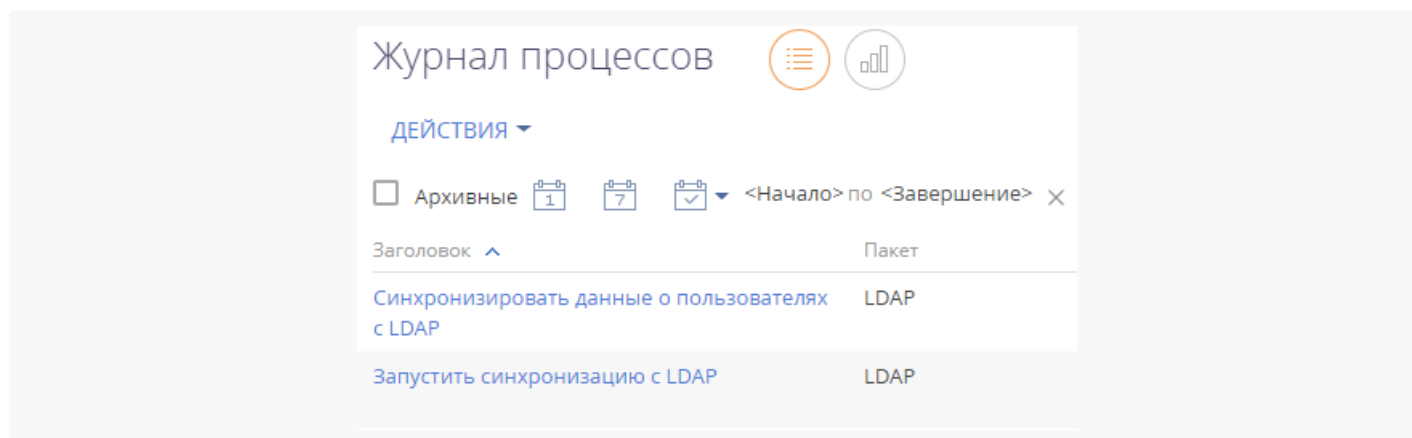


Рис. 9 — Процессы “Запустить синхронизацию с LDAP” и “Синхронизировать данные о пользователях с LDAP”



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](#).