

Пользователи и доступ

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	6
Настроить интеграцию с LDAP	6
Привязать элементы LDAP к пользователям и ролям Creatio	11
Запустить синхронизацию с LDAP	14
Настроить Single Sign-On через ADFS	17
Выполнить настройки на стороне ADFS	17
Выполнить настройки на стороне Creatio	24
Организационные роли	33
Добавить организационную роль	33
Добавить роль руководителей	34
Добавить пользователей в организационную роль	36
Настроить доступ по операциям	38
Настроить доступ по операциям в объекте раздела	39
Настроить приоритет прав доступа по операциям объекта	42
Настроить доступ по операциям в объекте детали	44
Настроить фильтры Active Directory	46
Формат фильтров	46
Фильтрация пользователей	47
Фильтрация групп	47
Стандартные фильтры пользователей группы Active Directory	48
Настроить фильтры для синхронизации пользователей/групп	48
Настроить Single Sign-On через OneLogin	49
Выполнить настройки на стороне OneLogin	49
Выполнить настройки на стороне Creatio	50
Функциональные роли	53
Добавить функциональную роль	54
Связать функциональные и организационные роли	55
Добавить пользователей в функциональную роль	56
Настроить права доступа на колонки	57
Настроить доступ на колонки объекта	58
Настроить приоритет прав доступа на колонки объекта	61
Импортировать новых пользователей и роли из Active Directory	63
Подготовить каталог к интеграции	63
Импортировать новых пользователей из LDAP	63
Настроить Just-In-Time User Provisioning	64
Добавить пользователей	68

Добавить пользователя с правами системного администратора	69
Добавить пользователя-сотрудника	71
Добавить новый контакт	71
Создать пользователя	72
Настроить доступ по записям	74
Настроить доступ на экспорт данных	78
Настроить аутентификацию с LDAP	80
Настроить аутентификацию пользователей через LDAP на .NET Framework	80
Настроить аутентификацию пользователей через LDAP на .NET Core	82
Настроить провайдеры аутентификации	83
Настроить доменную авторизацию	84
Аутентификация Windows	87
Как работает аутентификация Windows	87
Настроить аутентификацию Windows в IIS	88
Настроить файл Web.config приложения-загрузчика	90
Изменить системного пользователя (Supervisor)	93
Часто задаваемые вопросы о синхронизации пользователей с LDAP	94
Почему в Creatio импортировались не все пользователи из каталога LDAP?	94
Почему в Creatio импортировались не все пользователи Active Directory после синхронизации LDAP?	94
Почему пользователь не может войти под доменной учетной записью после настройки LDAP?	95
Может ли запись пользователя, импортированного из Active Directory, быть привязана к записи определенного контрагента?	95
Почему не импортируются пользователи из группы “Доменные пользователи” (“Domain users”)?	95
Что означает ошибка “22021: invalid byte sequence for encoding “UTF8”: 0X00” при синхронизации Active Directory с LDAP?	95
Почему возникает ошибка “Cannot insert duplicate key row in object 'dbo.SysAdminUnit' with unique index 'IUSysAdminunitNameDomain'. The duplicate key value is (...)”?	96
Как настроить фильтр LDAP?	96
Импортировать пользователей из Excel	96
Подготовить документ Excel для импорта пользователей	96
Запустить импорт	98
Настроить пароль, роль и выдать лицензии	100
Настроить права доступа на системные операции	101
Назначить пользователю роли	103
Способ 1. Назначить роли со страницы пользователя	103
Способ 2. Назначить роли со страницы ролей	104
Описание системных операций	105
Управление пользователями и ролями	105
Управление пользователями портала	106
Общий доступ к данным	106

Доступ к колонкам, системным операциям	107
Доступ к особым разделам системы	107
Доступ к функциональности поиска дублей	108
Доступ к настройкам интеграций	109
Общие действия в системе	109
Предоставить лицензии пользователю	110
Делегировать права доступа	111
Делегировать права пользователя другим пользователям и ролям	112
Делегировать права пользователю от других пользователей и ролей	112
Удалить делегированные права доступа	113
Разблокировать учетную запись пользователя	114
Внедрить политику паролей организации	114
Время завершения сессии	115
Протокол TLS для Creatio on-site	115
Безопасные конфигурации заголовков для Creatio on-site	116
Ответы на запросы для Creatio on-site	117
Запрет одновременных сеансов для Creatio on-site	117

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.

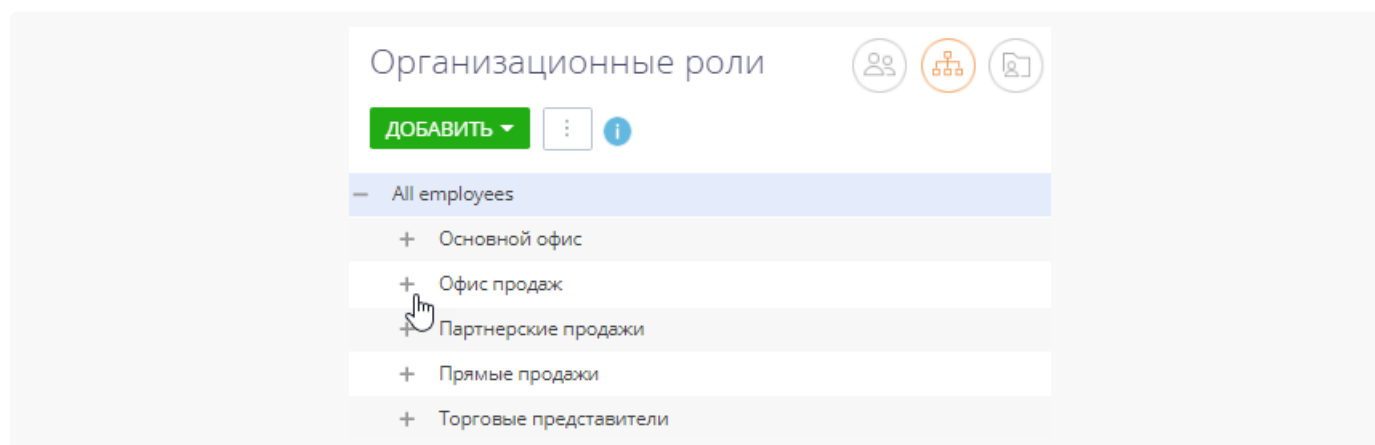
Вы можете перенести в приложение организационную структуру компании и настройки всех ролей из Active Directory после выполнения синхронизации с LDAP.

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).

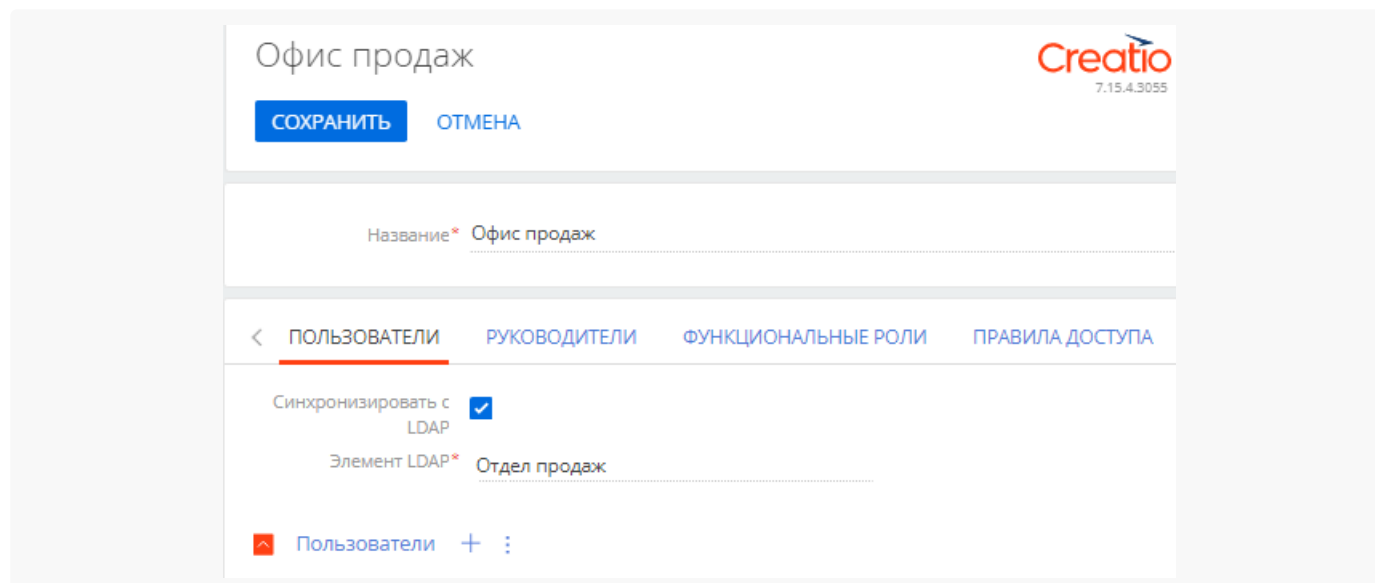
Если нужной роли в дереве групп нет, то нажмите кнопку [*Добавить*] и выберите “Организацию” или “Подразделение” в зависимости от того, какую роль необходимо добавить. На открывшейся странице укажите название группы.

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

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.

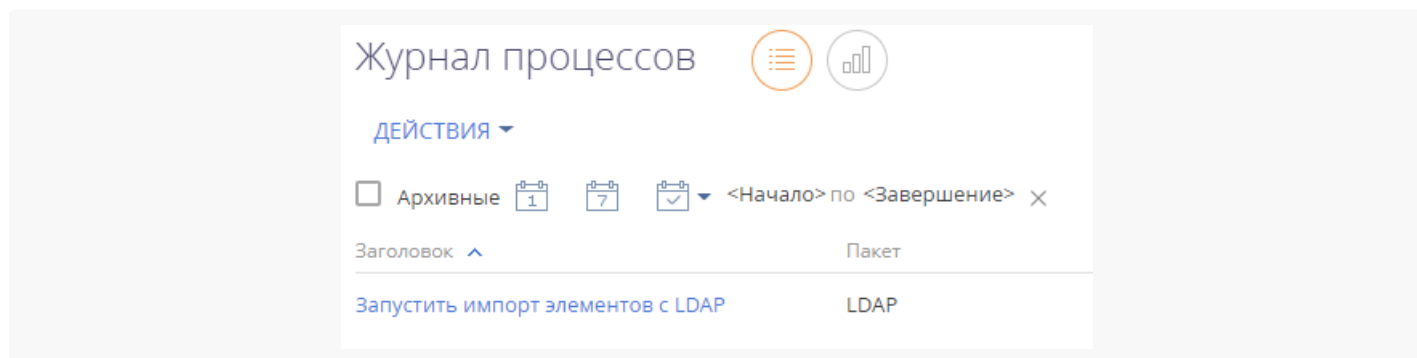
На заметку. Заполнение остальных полей на странице [*Настройка интеграции с LDAP*] описано в блоке [Настроить интеграцию с LDAP](#).

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*]

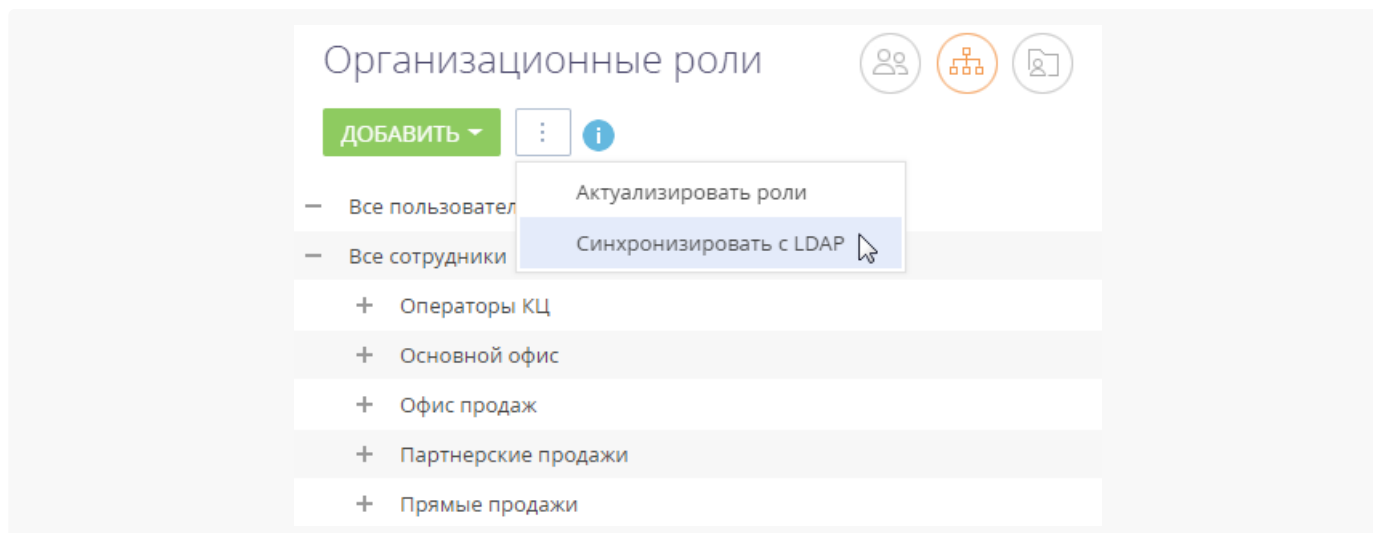
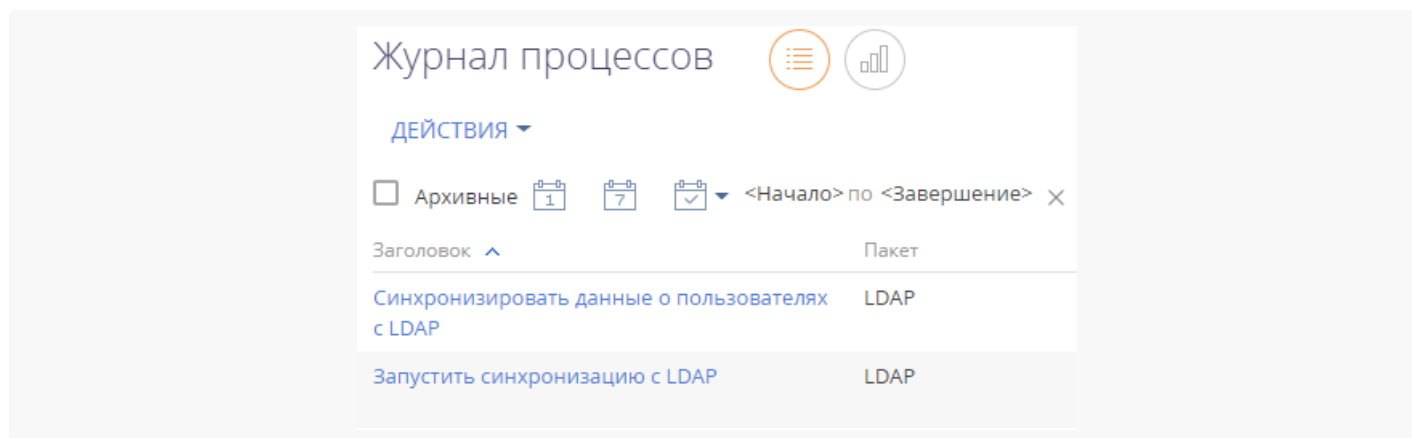


Рис. 9 — Процессы “Запустить синхронизацию с LDAP” и “Синхронизировать данные о пользователях с LDAP”



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 Single Sign-On через ADFS

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

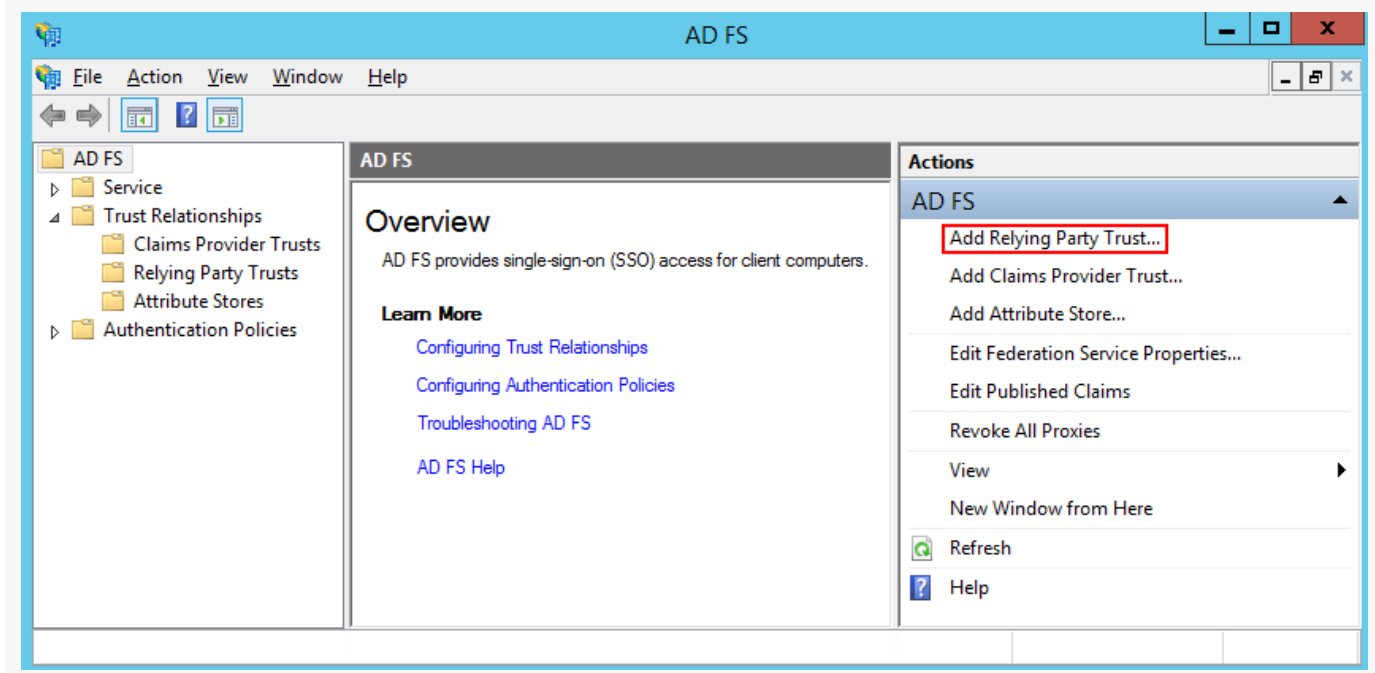
Вы можете настроить интеграцию Creatio с Active Directory Federation Services (ADFS), чтобы с ее помощью управлять возможностью единого входа для всех пользователей системы. Для этого нужно выполнить ряд настроек как на стороне ADFS, так и на стороне Creatio.

Важно. В примере использован адрес сайта Creatio https://site01.creatio.com/Demo_161215/ и адрес сайта сервиса ADFS <http://adfs01.mysite.com/adfs/>. При выполнении настройки замените адреса на соответствующие адреса ваших сайтов.

Выполнить настройки на стороне ADFS

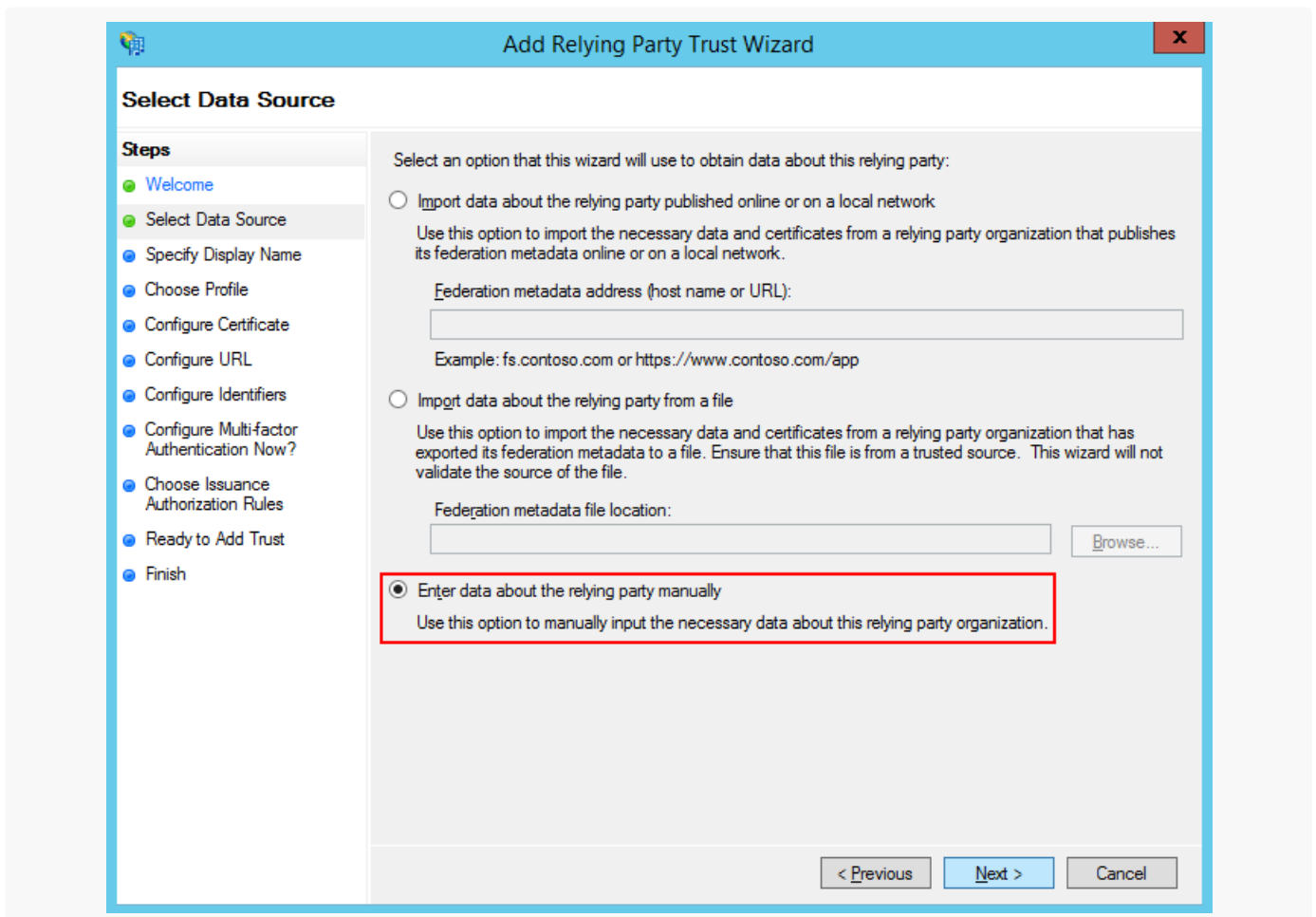
1. Добавьте в ADFS нового поставщика ресурсов (Relying Party Trusts) (Рис. 1).

Рис. 1 — Добавление нового поставщика ресурсов



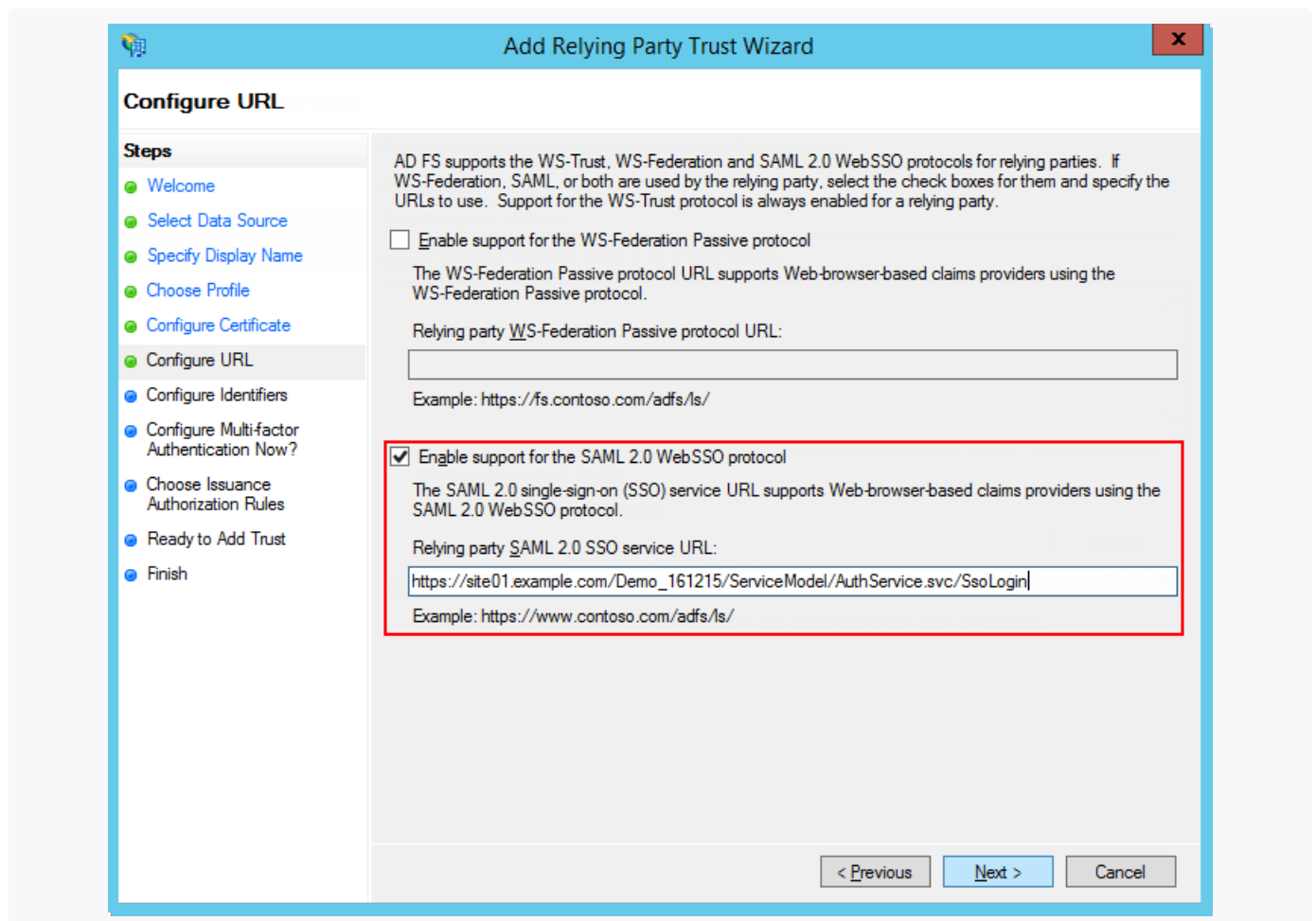
2. Выберите опцию ручного ввода данных ("Enter data about the relying party manually"), как показано на Рис. 2.

Рис. 2 — Выбор опции ручного ввода данных о поставщике ресурсов



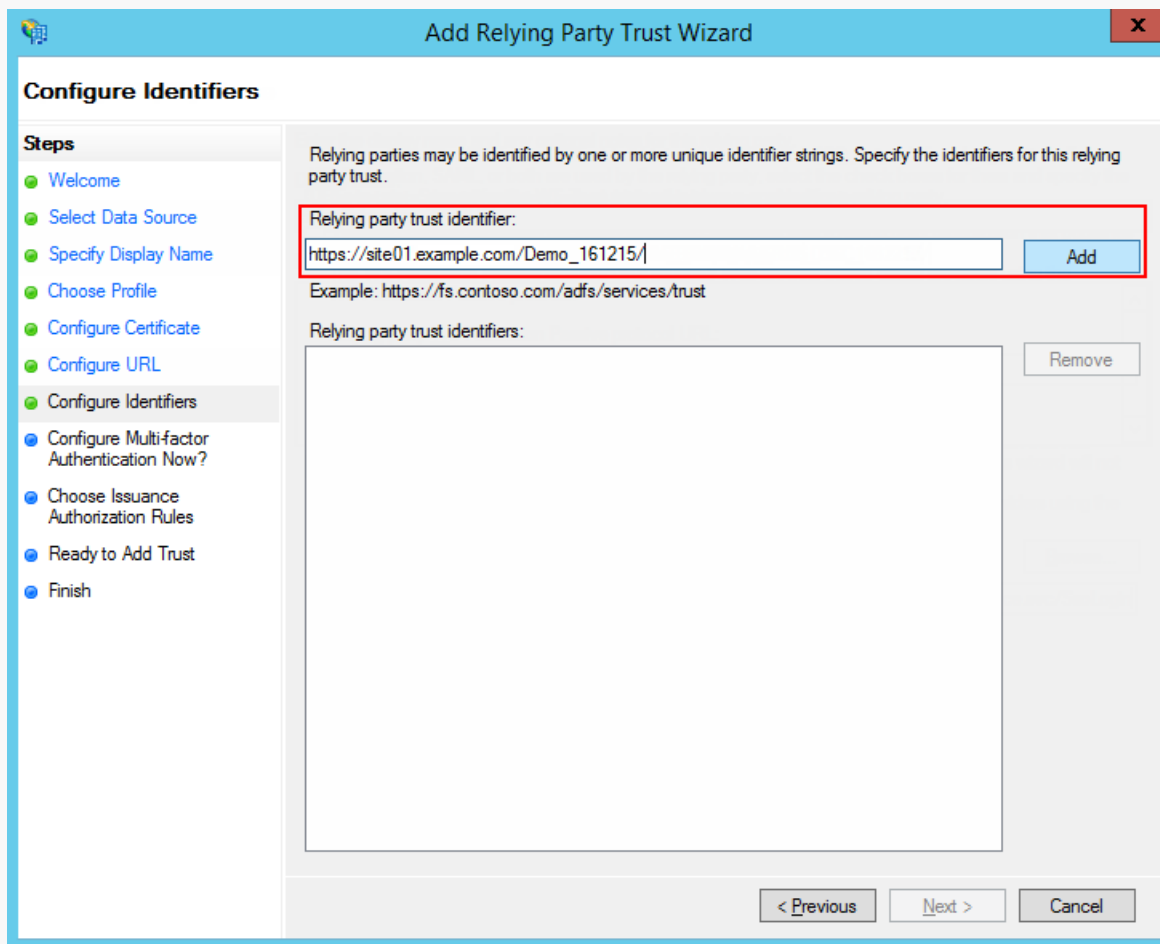
3. В поле [*Отображаемое имя*] (“Display name”) введите название Relying Party. Имя необходимо только для упорядоченного ведения списка доверенных приложений в ADFS.
4. Оставьте профиль “AD FS Profile”, выбранный по умолчанию. Нажмите кнопку [*Далее*] (“Next”).
5. На шаге выбора сертификата нажмите кнопку [*Далее*] (“Next”).
6. Включите поддержку протокола SAML 2.0. Укажите адрес сайта, добавьте к нему “/ServiceModel/AuthService.svc/SsoLogin” (Рис. 3).

Рис. 3 — Включение поддержки протокола SAML 2.0



7. В настройках идентификаторов укажите полный адрес сайта и нажмите кнопку [*Добавить*] (“Add”) как показано на Рис. 4.

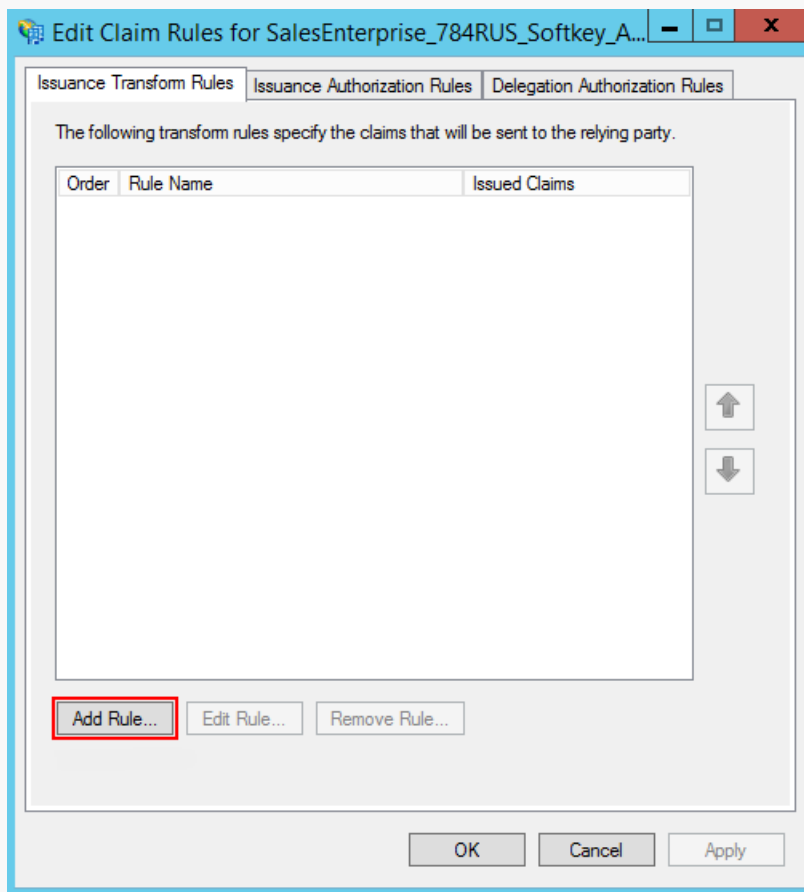
Рис. 4 — Указание идентификатора



Важно. Идентификатор используется при проверке подлинности источника, который запрашивает выполнение аутентификации. URL должен совпадать полностью, включая “/” в конце.

8. Значения остальных параметров настройте в соответствии с требованиями безопасности вашей организации. Для тестового использования эти настройки можно оставить по умолчанию.
9. Нажмите [*Завершить*] (“Finish”). В открывшемся окне по кнопке [*Добавить правило*] (“Add Rule”) добавьте новое правило формирования SAML Assertion в SAML Response (Рис. 5).

Рис. 5 — Добавление правила



На заметку. Данные, которые формируются новым правилом, будут использоваться приложением Creatio для поиска пользователя, актуализации его профиля и ролей.

10. На первом шаге добавления правила оставьте настройку, выбранную по умолчанию, и нажмите кнопку [*Далее*] ("Next"). Установите набор параметров, которые будут получены из данных пользователя (Рис. 6). В указанном примере в SAML Assertion будет передаваться имя ("Name") пользователя и список групп домена, в которые он входит.

Рис. 6 — Установка параметров правила

Add Transform Claim Rule Wizard

X

Configure Rule

Steps

Choose Rule Type

Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)	
	User-Principal-Name	Name ID	⋮
	Token-Groups - Qualified by Doma...	Role	
	E-Mail-Addresses	E-Mail Address	
	Display-Name	Given Name	
▶	User-Principal-Name	Name	

< Previous

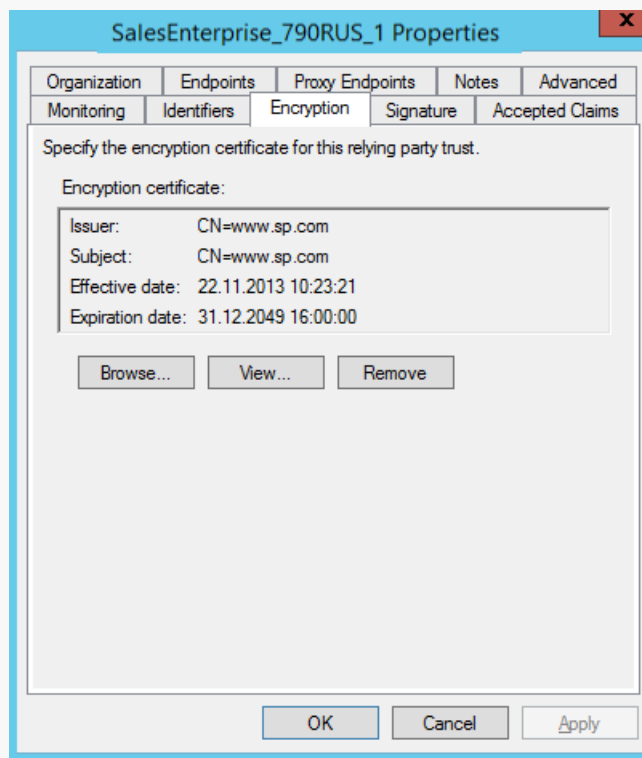
Finish

Cancel

11. Нажмите кнопку [*Сохранить*] (“Save”).
12. Откройте настройки созданного поставщика ресурсов “Trusted Relay” и на вкладке с расширенными настройками (“Advanced”) укажите шифрование SHA-1 согласно алгоритму сертификата сайта.
13. Для настройки шифрования SAML-пакета на вкладке с настройками шифрования (“Encryption”) добавьте публичный ключ сертификата (Рис. 7).

На заметку. Если вы используете Creatio cloud, то публичный ключ сертификата будет предоставлен службой поддержки.

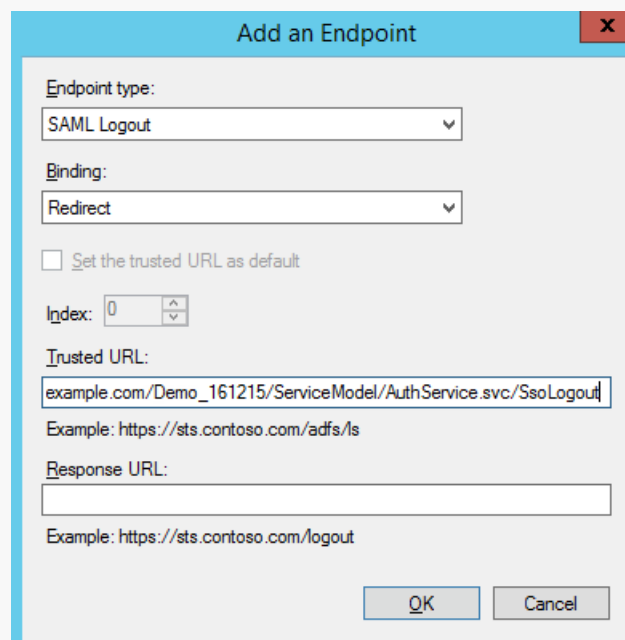
Рис. 7 — Добавление публичного ключа



14. На вкладке [*Конечные точки*] (“Endpoints”) добавьте конечную точку (“Logout endpoint”), и установите такие параметры (Рис. 8):

- **Endpoint type:** SAML Logout.
- **Binding:** Redirect.
- **Trusted URL:** https://site01.creatio.com/Demo_161215/ServiceModel/AuthService.svc/SsoLogout.

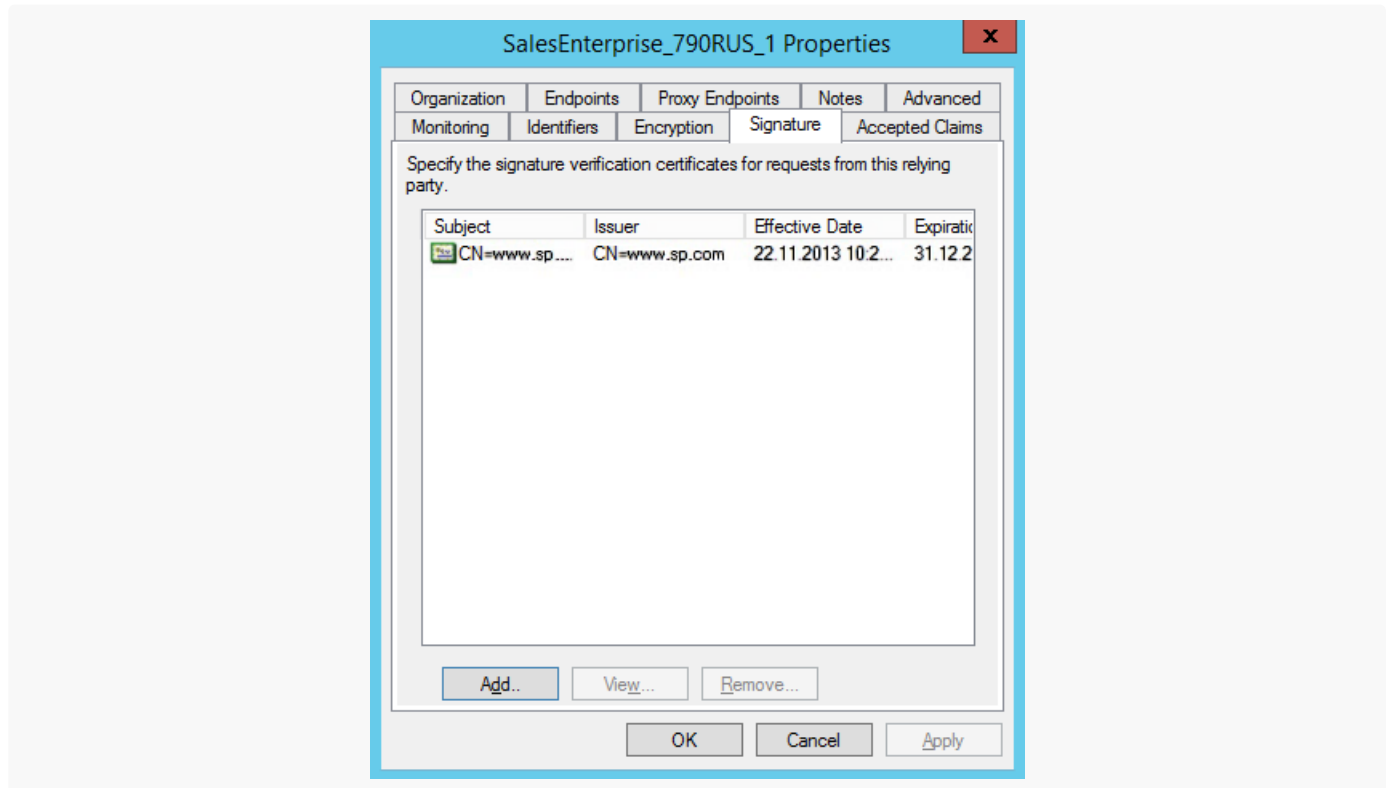
Рис. 8 — Установка параметров конечной точки



15. На вкладке [*Подпись*] (“Signature”) добавьте сертификат для подписывания (“Logout Request”) как

показано на Рис. 9.

Рис. 9 — Добавление сертификата



Важно. Без сертификата не будет работать выход из приложений.

Выполнить настройки на стороне Creatio

Если вы используете **Creatio cloud**, то подготовьте информацию для настройки по инструкции ниже и обратитесь в [службу поддержки Creatio](#) для применения настроек на сайте.

Ниже приведена инструкция по настройке единого входа для пользователей **Creatio on-site**.

Настоятельно рекомендуем предоставить службе поддержки временный доступ к конфигурации Creatio, либо производить эту настройку под руководством службы технической поддержки.

Чтобы выполнить настройку на стороне Creatio, необходимо выполнить следующие настройки в конфигурационных файлах:

1. Внести настройки SAML-провайдера.
2. Настроить параметры SSO-аутентификации в Creatio.
3. Проверить базовые сценарии SSO.
4. Настроить Just-In-Time User Provisioning (JIT).
5. Включить использование SSO по умолчанию.

Настройки для приложения на .NET Framework и приложения на .NET Core имеют ряд различий, которые ниже будут рассмотрены подробнее.

.NET Framework

1. Заполните настройки **SAML-провайдера**, указав данные SAML-провайдера идентификации в **saml.config**.

- a. В параметре Name укажите FQDN вашего сайта.

Важно. Значение параметра ServiceProvider Name должно быть идентично значению Identifier, указанному на стороне провайдера идентификации ADFS. Таким образом выполняется проверка, что SAML Assertion выдан именно для вашего приложения. Для этого удобнее использовать FQDN вашего сайта, например, https://site01.creatio.com/Demo_161215/. Обратите внимание, URL должен совпадать полностью, включая "/" в конце.

- b. В секции Partner Identity Provider укажите настройки со стороны IdP. Эти настройки можно посмотреть в файле метаданных.

- **WantAssertionSigned="false"** — если не будет использоваться сертификат шифрования при обмене SAML Assertion.
- **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Для ADFS, как правило, это: <https://adfs01.mysite.com/adfs/ls>.
- **SingleLogoutServiceUrl** — URL сервиса единого выхода провайдера. Для ADFS, как правило, это: <https://adfs01.mysite.com/adfs/ls>.
- **PartnerCertificateFile** — путь к сертификату безопасности в формате *.cer в файловой системе сервера относительно корня приложения Creatio. Нужно задавать, если WantAssertionSigned="true".
- **SignLogoutRequest="true"** — важно указывать для ADFS, поскольку подписывание LogoutRequest обязательно. Если установлено значение "true", то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.
- **SignLogoutResponse="true"** — важно указывать для ADFS, поскольку подписывание LogoutResponse обязательно. Если установлено значение "true", то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.
- **OverridePendingAuthnRequest="true"** — опция, при включении которой не будет выполняться валидация на соответствие ответа IdP ранее созданным Auth Request.

Пример saml.config для ADFS:

```
<ServiceProvider Name="https://site01.creatio.com/Demo_161215/"
  Description="Example Creatio Service Provider"
  AssertionConsumerServiceUrl="~/ServiceModel/AuthService.svc/SsoLogin"
  LocalCertificateFile="sp.pfx"
  LocalCertificatePassword="password"
/>
<PartnerIdentityProviders>

<!-- ADFS Creatio -->
```

```
<PartnerIdentityProvider Name="http://adfs01.mysite.com/adfs/services/trust"
    OverridePendingAuthnRequest="true"
        Description="MVC Example Identity Provider"
        SignAuthnRequest="false"
        SignLogoutRequest="true"
        SignLogoutResponse="true"
        WantSAMLResponseSigned="false"
        WantAssertionSigned="false"
        WantAssertionEncrypted="false"
        SingleSignOnServiceUrl="https://adfs01.mysite.com/ad
        SingleLogoutServiceUrl="https://adfs01.mysite.com/ad
        PartnerCertificateFile="Certificates\idp.cer"/>
```

Если включен флаг `SignLogoutRequest` или `SignLogoutResponse`, то добавьте в файловую систему, в которой находится приложение Creatio, приватный ключ сертификата шифрования в формате *.pfx. Укажите путь к файлу, а также пароль в файлах конфигурации `saml.config` и убедитесь, что пользователь, под которым запущено приложение, имеет права на чтение файла. Важно, чтобы сертификат был физически добавлен в корневую папку сайта и в папку `Terrasoft.WebApp`.

```
LocalCertificateFile="sp.pfx"
LocalCertificatePassword="password"
```

Рис. 10 — Настройка шифрования SAML-пакета

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
    <ServiceProvider Name="https://site01.creatio.com/Demo_161215/"
        Description="Example Creatio Service Provider"
        AssertionConsumerServiceUrl="~/ServiceModel/AuthService.svc/SsoLogin"
        LocalCertificateFile="sp.pfx"
        LocalCertificatePassword="password"
    />
</PartnerIdentityProviders>
```

2. **Включите использование SSO-провайдера в Creatio.** После указания настроек SAML-провайдера необходимо включить использование SAML SSO в Creatio. Для этого внесите необходимые настройки в **web.config** в корневой папке сайта:

а. Включите использование SSO Auth-провайдеров при выполнении авторизации в Creatio:

- **SsoAuthProvider** — провайдер входа в основное приложение.
- **SSPSsoAuthProvider** — провайдер входа на портал.

Указывать можно оба провайдера или только один, который нужен в конкретном случае.

```
<terrasoft> <authproviderNames="InternalUserPassword,SSPUserPassword,SsoAuthProvider,
```

- d. Укажите, какой из провайдеров идентификации, указанных в `saml.config`, нужно использовать по умолчанию в Service Provider initiated SSO-сценариях. В `web.config` App Loader задайте параметр `PartnerIdP` значением из строки `Issuer URL` в `saml.config`, например:

```
<appSettings>

...

<add key="PartnerIdP" value="http://adfs01.mysite.com/adfs/services/trust"/>

...

</appSettings>
```

3. Проверьте базовый сценарий Identity Provider (IdP) initiated SSO, чтобы убедиться в корректности настроек:

- Переход на страницу доверенных приложений IdP (ссылка по умолчанию: <https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx>).
- Выполнение авторизации.
- Переход на Creatio с результатом авторизации на IdP.

До включения провайдера SSO на стороне Creatio по умолчанию используйте для проверки корректности настроек IdP initiated сценарий. До выполнения проверки убедитесь, что в Creatio содержится активная учетная запись, логин которой совпадает с `Nameld`, передаваемым Identity Provider. В противном случае процесс SSO настройки не будет успешно завершен, поскольку не удастся сопоставить пользователя из домена с пользователем в Creatio. Как только вход через SSO будет выполнен успешно, перейдите к дальнейшим настройкам.

4. Настройте Just-In-Time User Provisioning (JIT). Функциональность Just-In-Time User Provisioning дополняет технологию единого входа. Она позволяет не только создать пользователя при первом входе в приложение, но и при каждом входе обновлять данные на странице контакта данными, полученными от провайдера идентификации. Подробнее читайте в статье [Настроить Just-In-Time User Provisioning](#).

- a. В `web.config` в корневой папке приложения добавьте настройки для JIT.

```
<add name="UseJit" value="true" />
```

Тип пользователя определяется страницей, с которой им был выполнен вход в систему. Если для входа используется сценарий Identity Provider initiated, то необходимо явно указать значение `DefUserType`:

- **General** — обычный пользователь.
- **SSP** — пользователь портала.

d. Настройте сопоставление полей из SAML Assertion с колонками в Creatio в справочнике [Преобразователь SAML атрибута в название поля контакта]. Это необходимо для корректного заполнения полей контакта при создании нового пользователя с помощью Just-In-Time User Provisioning. Если поле пусто или отсутствует в данных провайдера идентификации, оно может быть заполнено значением, указанным в поле [Значение по умолчанию] справочника. При следующем входе пользователя поля контакта, указанные в справочнике, будут заполнены значением, полученным из провайдера, или актуальным значением по умолчанию.

На заметку. Если справочника нет в списке справочников, то его необходимо зарегистрировать.

5. **Включите использование SSO-провайдера по умолчанию** при входе на сайт. Рекомендуем выполнять действие только в случае успешного выполнения предыдущих шагов и проверки корректности работы. После успешного выполнения этого шага будет доступен для использования Service Provider (SP) initiated SSO.

Стандартный сценарий Service Provider (SP) initiated:

- Переход на Creatio, у пользователя нет активной сессии на сайте.
- Переадресация на IdP, выполнение авторизации.
- Переход на Creatio с результатом авторизации из IdP.

Для включения провайдера SSO по умолчанию:

a. Укажите в корневом web.config ресурс по умолчанию NuiLogin.aspx?use_sso=true.

На заметку. Для возможности входа с использованием логина/пароля остается доступной прямая ссылка <https://site01.creatio.com/Login/NuiLogin.aspx?>

Для тестирования работы SSO до включения по умолчанию можно использовать ссылку https://site01.creatio.com/NuiLogin.aspx?use_sso=true

b. Установите отправку к провайдеру идентификации при переходе в корень сайта в корневом web.config:

```
<defaultDocument> <files> <add value="Login/NuiLogin.aspx?use_sso=true" /> </files> </defaultDocument>

<authentication mode="Forms">
  <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true ..." />
</authentication>
```

c. Включите Single Log Out в web.config в папке Terrasoft.WebApp:

```
<add key="UseSlo" value="true" />
```

- d. Укажите в web.config в папке Terrasoft.WebApp ресурс для перенаправления при истечении активной сессии:

```
<authentication mode="Forms">
  <forms loginUrl="~/../Login/NullLogin.aspx?use_sso=true..."
</authentication>
```

- e. Для использования технологии единого входа в мобильном приложении установите признак [Значение по умолчанию] в системной настройке “Использовать SSO в мобильном приложении” (код “MobileUseSSO”).

.Net Core

1. **Заполните настройки SAML-провайдера**, указав данные SAML-провайдера идентификации в **saml.json**.

- a. В параметре Name укажите FQDN вашего сайта.

Важно. Значение параметра ServiceProvider Name должно быть идентично значению Identifier, указанному на стороне провайдера идентификации ADFS. Таким образом выполняется проверка, что SAML Assertion выдан именно для вашего приложения. Для этого удобнее использовать FQDN вашего сайта, например, https://site01.creatio.com/Demo_161215/. Обратите внимание, URL должен совпадать полностью, включая “/” в конце.

- b. В секции Partner Identity Provider укажите настройки со стороны IdP. Эти настройки можно посмотреть в файле метаданных.

- **WantAssertionSigned** — укажите “false”, если не будет использоваться сертификат шифрования при обмене SAML Assertion.

```
"WantLogoutRequestSigned":false
```

- **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Для ADFS, как правило, это: <https://adfs01.mysite.com/adfs/ls>.

```
"SingleSignOnServiceUrl":"https://adfs01.mysite.com/adfs/ls"
```

- **SingleLogoutServiceUrl** — URL сервиса единого выхода провайдера. Для ADFS, как правило, это: <https://adfs01.mysite.com/adfs/ls>.

```
"SingleLogoutServiceUrl":"https://adfs01.mysite.com/adfs/ls"
```

- **PartnerCertificates** — путь к сертификату безопасности в формате *.cer в файловой системе сервера относительно корня приложения Creatio. Нужно задавать, если

WantAssertionSigned="true".

```
"PartnerCertificates":[
  {
    "FileName":"adfs_sandbox.cer"
  }
]
```

- **SignLogoutRequest** – укажите “true” для ADFS, поскольку подписывание LogoutRequest обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.

```
"SignLogoutRequest":true
```

- **SignLogoutResponse** — укажите “true” для ADFS, поскольку подписывание LogoutResponse обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.

```
"SignLogoutResponse":true
```

2. Если включен флаг SignLogoutRequest или SignLogoutResponse, то добавьте в файловую систему, в которой находится приложение Creatio, приватный ключ сертификата шифрования в формате *.pfx. Укажите путь к файлу, а также пароль в файле конфигурации saml.json, и убедитесь, что пользователь, под которым запущено приложение, имеет права на чтение файла. Важно, чтобы сертификат был физически добавлен в корневую папку сайта и в папку Terrasoft.WebApp.

```
"...""LocalCertificates":[
  {
    "FileName":"sp.pfx",
    "Password":"password"}
]"..."
```

3. **Включите использование SSO-провайдера в Creatio.** После указания настроек SAML-провайдера необходимо включить использование SAML SSO в Creatio. Для этого внесите необходимые настройки в **Terrasoft.WebHost.dll.config** в корневой папке сайта:

- a. Включите использование SSO Auth-провайдеров при выполнении авторизации в Creatio:

- **SsoAuthProvider** — провайдер входа в основное приложение.
- **SSPSsoAuthProvider** — провайдер входа на портал.
Указывать можно оба провайдера или только один, который нужен в конкретном случае.

```
"..."
```

```
<auth providerNames=""LdapProvider,InternalUserPassword,SSPUserPassword,SsoAuthProvid
```

```
..."
```

- d. Укажите, какой из провайдеров идентификации, указанных в `saml.json`, нужно использовать по умолчанию в Service Provider initiated SSO-сценариях. В **Terrasoft.WebHost.dll.config** задайте параметр `PartnerIdP` значением из строки `Issuer URL` в `saml.json`, например:

```
"..."PartnerName":"http://adfs.sandbox.local/adfs/services/trust",
..."
```

4. Проверьте базовый сценарий Identity Provider (IdP) initiated SSO, чтобы убедиться в корректности настроек:

- Переход на страницу доверенных приложений IdP (ссылка по умолчанию: <https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx>).
- Выполнение авторизации.
- Переход на Creatio с результатом авторизации на IdP.

До включения провайдера SSO на стороне Creatio по умолчанию используйте для проверки корректности настроек IdP initiated сценарий. До выполнения проверки убедитесь, что в Creatio содержится активная учетная запись, логин которой совпадает с `Nameld`, передаваемым Identity Provider. В противном случае процесс SSO настройки не будет успешно завершен, поскольку не удастся сопоставить пользователя из домена с пользователем в Creatio. Как только вход через SSO будет выполнен успешно, перейдите к дальнейшим настройкам.

5. Настройте Just-In-Time User Provisioning (JIT). Функциональность Just-In-Time User Provisioning дополняет технологию единого входа. Она позволяет не только создать пользователя при первом входе в приложение, но и при каждом входе обновлять данные на странице контакта данными, полученными от провайдера идентификации. Подробнее читайте в статье [Настроить Just-In-Time User Provisioning](#).

- a. В **Terrasoft.WebHost.dll.config** в корневой папке приложения добавьте настройки для JIT (включается для пользователей системы в настройках `SsoAuthProvider` и для пользователей портала в настройках `SSPSsoAuthProvider`):

```
...
<provider name="SsoAuthProvider" type="Terrasoft.Authentication.Core.SSO.BaseSsoAuthProvider,
Terrasoft.Authentication">
  <parameters>
    <add name="UserType" value="General" />
    <add name="UseJit" value="true" />
  </parameters>
</provider>
<provider name="SSPSsoAuthProvider"
type="Terrasoft.Authentication.Core.SSO.BaseSsoAuthProvider, Terrasoft.Authentication">
  <parameters>
    <add name="UserType" value="SSP" />
    <add name="UseJit" value="true" />
```

```
</parameters>
```

```
...
```

Тип пользователя определяется страницей, с которой им был выполнен вход в систему. Если для входа используется сценарий Identity Provider initiated, то необходимо явно указать значение DefUserType:

- **General** — обычный пользователь.
- **SSP** — пользователь портала.

- Настройте сопоставление полей из SAML Assertion с колонками в Creatio в справочнике [Преобразователь SAML атрибута в название поля контакта]. Это необходимо для корректного заполнения полей контакта при создании нового пользователя с помощью Just-In-Time User Provisioning. Если поле пусто или отсутствует в данных провайдера идентификации, оно может быть заполнено значением, указанным в поле [Значение по умолчанию] справочника. При следующем входе пользователя поля контакта, указанные в справочнике, будут заполнены значением, полученным из провайдера, или актуальным значением по умолчанию.

На заметку. Если справочника нет в списке справочников, то его необходимо зарегистрировать.

- Включите использование SSO-провайдера по умолчанию** при входе на сайт. Рекомендуем выполнять действие только в случае успешного выполнения предыдущих шагов и проверки корректности работы. После успешного выполнения этого шага будет доступен для использования Service Provider (SP) initiated SSO.

Стандартный сценарий Service Provider (SP) initiated:

- Переход на Creatio, у пользователя нет активной сессии на сайте.
- Переадресация на IdP, выполнение авторизации.
- Переход на Creatio с результатом авторизации из IdP.

Для включения провайдера SSO по умолчанию:

- Укажите в файле saml.json UseSsoByDefault": "true".

На заметку. Для возможности входа с использованием логина/пароля остается доступной прямая ссылка <https://site01.creatio.com/Login/NuiLogin.aspx?>

Для тестирования работы SSO до включения по умолчанию можно использовать ссылку https://site01.creatio.com/NuiLogin.aspx?use_sso=true

- Установите отправку к провайдеру идентификации при переходе в корень сайта в **Terrasoft.WebHost.dll.config**:

```
<defaultDocument> <files> <add value="Login/NuiLogin.aspx?use_sso=true" /> </files> </de

<authentication mode="Forms">
    <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true ...
```



```
</authentication>
```

- c. Включите Single Log Out в **Terrasoft.WebHost.dll.config**:

```
<add key="UseSlo" value="true" />
```

- d. Укажите в **Terrasoft.WebHost.dll.config** ресурс для перенаправления при истечении активной сессии:

```
<authentication mode="Forms">
  <forms loginUrl="~/../Login/NuiLogin.aspx?use_sso=true..." />
</authentication>
```

- e. Для использования технологии единого входа в мобильном приложении установите признак [*Значение по умолчанию*] в системной настройке “Использовать SSO в мобильном приложении” (код “MobileUseSSO”).

Организационные роли

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**


Организационные роли — это часть организационной структуры компании, некая организация или подразделение, например, “Отдел продаж основного офиса” или “HR-отдел регионального офиса”. Каждой организационной роли можно назначить права доступа, которые будут применены ко всем ее пользователям. Организационные роли также автоматически наследуют права доступа от своих родительских организационных ролей. Подробнее: [Пользователи и роли](#) (статья онлайн-курса).

Для управления организационными ролями нажмите  → “**Организационные роли**”.

В разделе доступна древовидная организационная структура компании, сформированная из организационных ролей, а также информация по выбранной организационной роли.

На заметку. По умолчанию доступ к разделу есть только у администраторов системы. Для работы с этим разделом пользователям необходимо иметь разрешение на выполнение системной операции “Управление списком пользователей” (“CanManageUsers”).

Добавить организационную роль

1. Нажмите  → “**Организационные роли**”.
2. В списке организационных ролей **выберите родительскую роль**. Например, создадим роль для регионального офиса.
3. Нажмите [*Добавить*] и **укажите тип роли** (“Организация” или “Подразделение”). Например, создадим подразделение “Отдел маркетинга” для регионального офиса.

4. Введите **название** новой роли. Название организационной роли должно быть уникальным.
5. Откройте вкладку [*Функциональные роли*] и добавьте функциональные роли, которые получают права доступа создаваемой организационной роли, например, “Менеджеры по маркетингу”, “Копирайтеры” и т. д.

Данный шаг не является обязательным.

На заметку. Установить связи между организационными и функциональными ролями можно также на странице функциональной роли. Подробнее: [Связать функциональные и организационные роли](#).


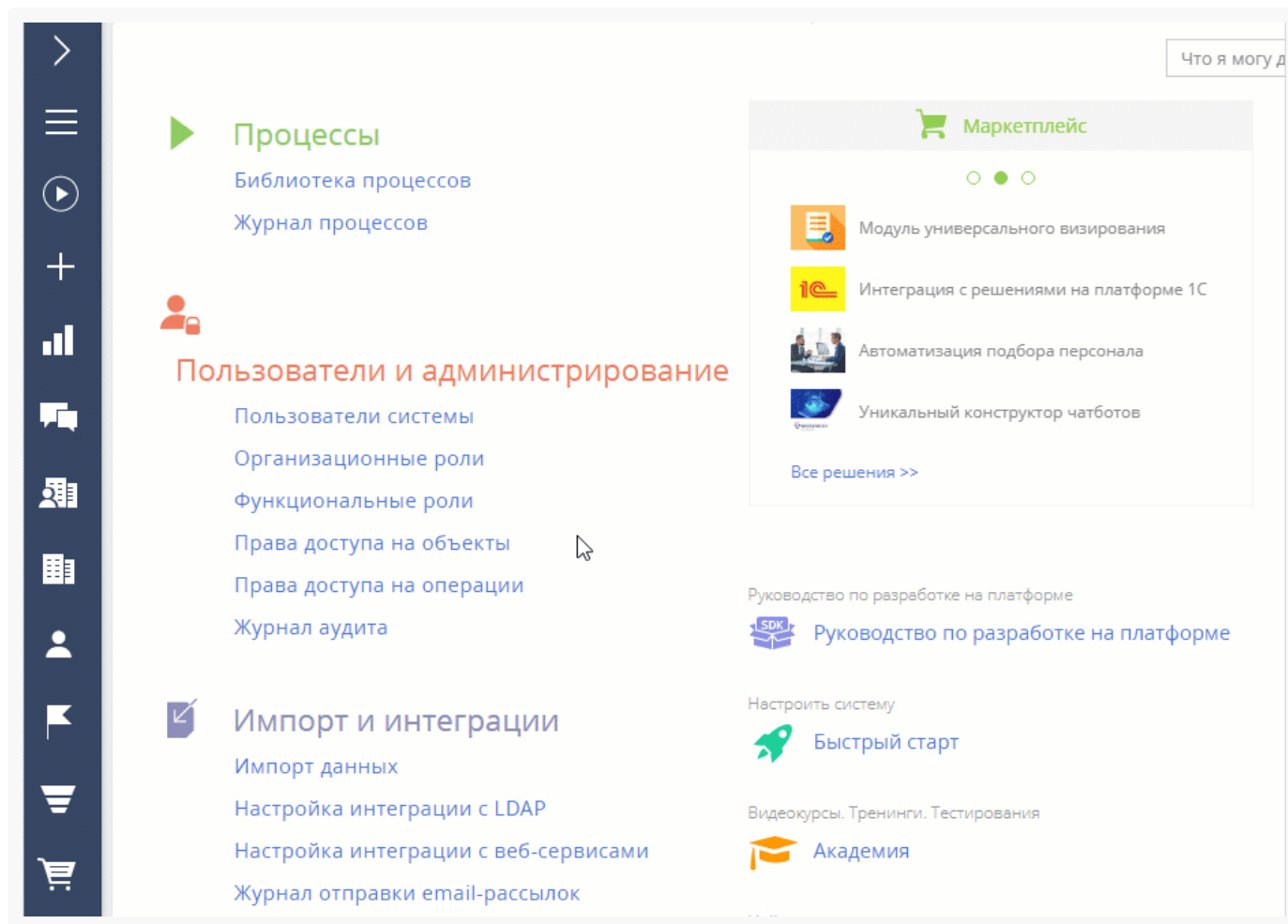
6. Чтобы изменения вступили в силу, закройте страницу и нажмите  → [*Актуализировать роли*] (Рис. 1).

Рис. 1 — Добавление организационной роли



В результате в Creatio будет добавлена новая организационная роль. Ей автоматически будут предоставлены те же права доступа, что и родительской организационной роли.

Добавить роль руководителей

Вы можете настроить особые права доступа для управленческого персонала, добавив роль

“**Руководители**” в существующую организационную роль. Роль руководителей существует в системе как самостоятельная организационная роль и может иметь собственные права доступа, но она не отображается в древовидном списке организационных ролей.

Роль руководителей автоматически наследует все права доступа роли подчиненных.

Чтобы добавить роль руководителей:


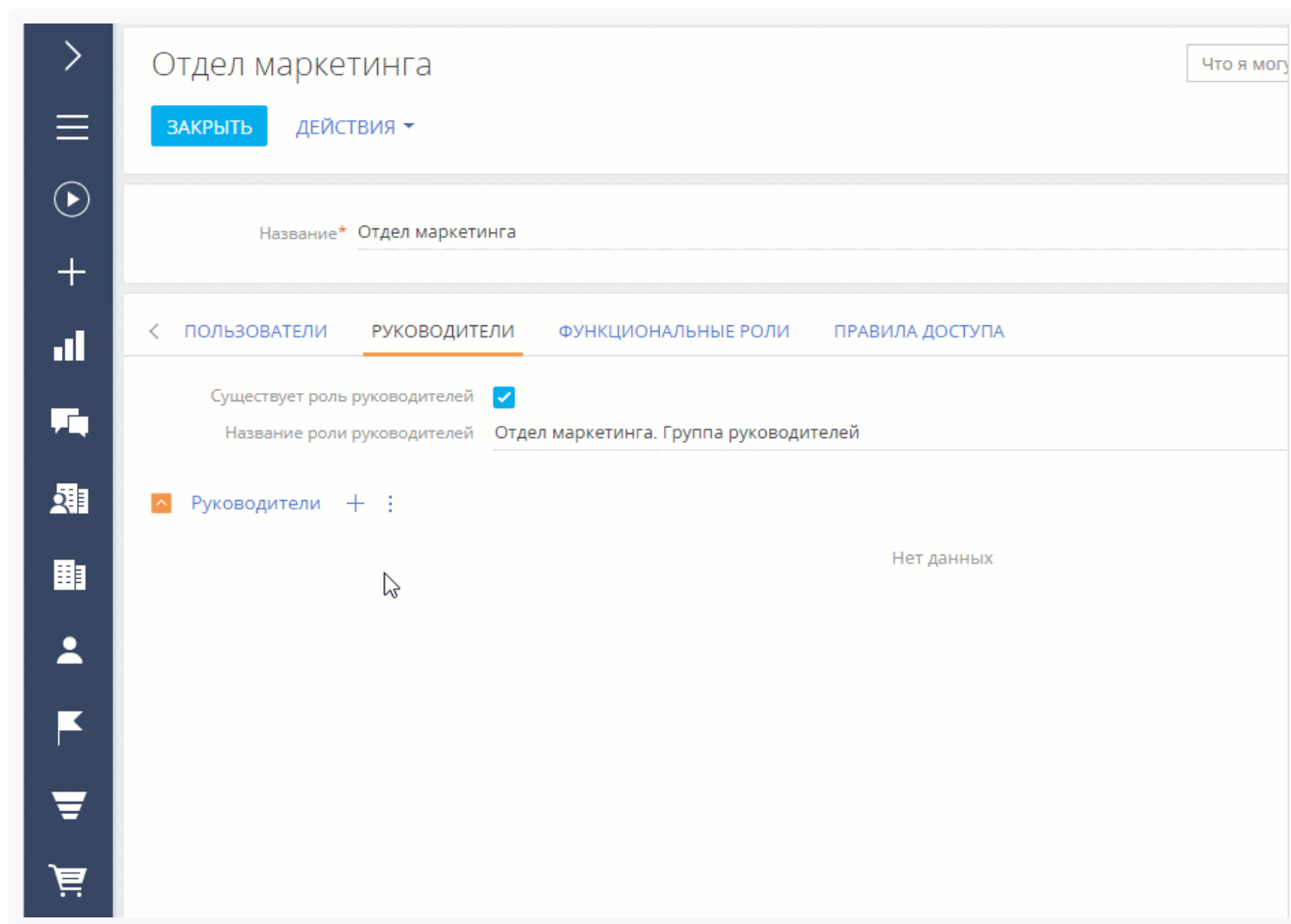
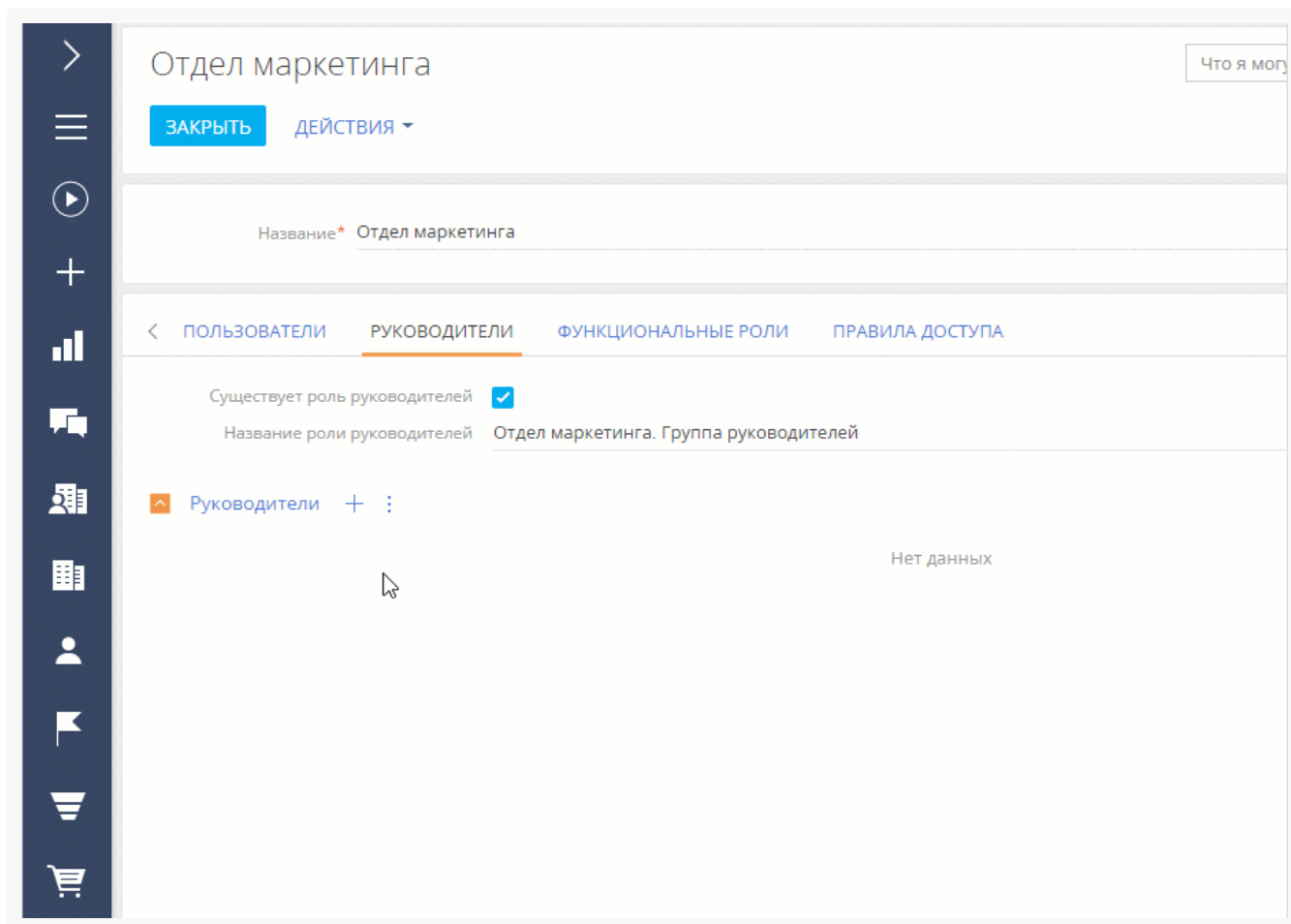
1. Нажмите  → “**Организационные роли**”.
2. В списке организационных ролей выберите организацию или подразделение, для которых нужно назначить роль руководителя. Например, создадим руководителей для роли “Отдел маркетинга” в основном офисе.
3. На вкладке [*Руководители*] установите признак [*Существует роль руководителей*].
4. В поле [*Название роли руководителей*] укажите название роли (Рис. 2).

Рис. 2 — Создание роли руководителя для организационной роли “Отдел маркетинга”



5. На вкладке [*Руководители*]:
 - a. **Если пользователь уже создан** в системе, то нажмите **+** и выберите [*Добавить существующего*]. Во всплывающем окне выберите нужных пользователей (Рис. 3).
 - b. **Если пользователь еще не создан** в системе, то нажмите **+** и выберите [*Добавить нового*]. Вам нужно будет заполнить страницу нового пользователя.

Рис. 3 — Включение пользователя в роль руководителя



В результате новая роль руководителя будет добавлена в организационную роль. Пользователи, которые входят в роль руководителей, получают все права доступа этой роли, включая права, унаследованные от организационной роли подчиненных (в текущем примере — роль “Отдел маркетинга”).

В некоторых случаях руководители могут наследовать избыточные права подчиненных. Например, если какому-либо сотруднику были предоставлены расширенные права доступа для выполнения рабочих задач. Чтобы избежать наследования излишних прав доступа руководителями, вы можете ограничить автоматическое делегирование прав доступа для определенных ролей.

Для этого добавьте нужные организационные или функциональные роли в [справочник](#) “Роли пользователей, не наследуемые руководителями”. По умолчанию в справочник добавлена роль “System administrators”.

Подробнее: [Настроить доступ по операциям](#), [Настроить доступ по записям](#), [Настроить права доступа на колонки](#), [Настроить права доступа на системные операции](#).

Добавить пользователей в организационную роль

Существует несколько способов добавить пользователей в организационную роль:

- Добавить существующих пользователей (выбрать из списка пользователей).
- Создать и добавить нового пользователя (нужно будет заполнить страницу нового пользователя).

- Импортировать пользователей LDAP.

Важно. Импортировать пользователей LDAP можно только в том случае, если настроена интеграция системы с LDAP. Подробнее: [Настроить синхронизацию с LDAP](#).

Все пользователи, которые входят в организационную роль, наследуют настроенные для нее права доступа.

Чтобы добавить пользователей в организационную роль:




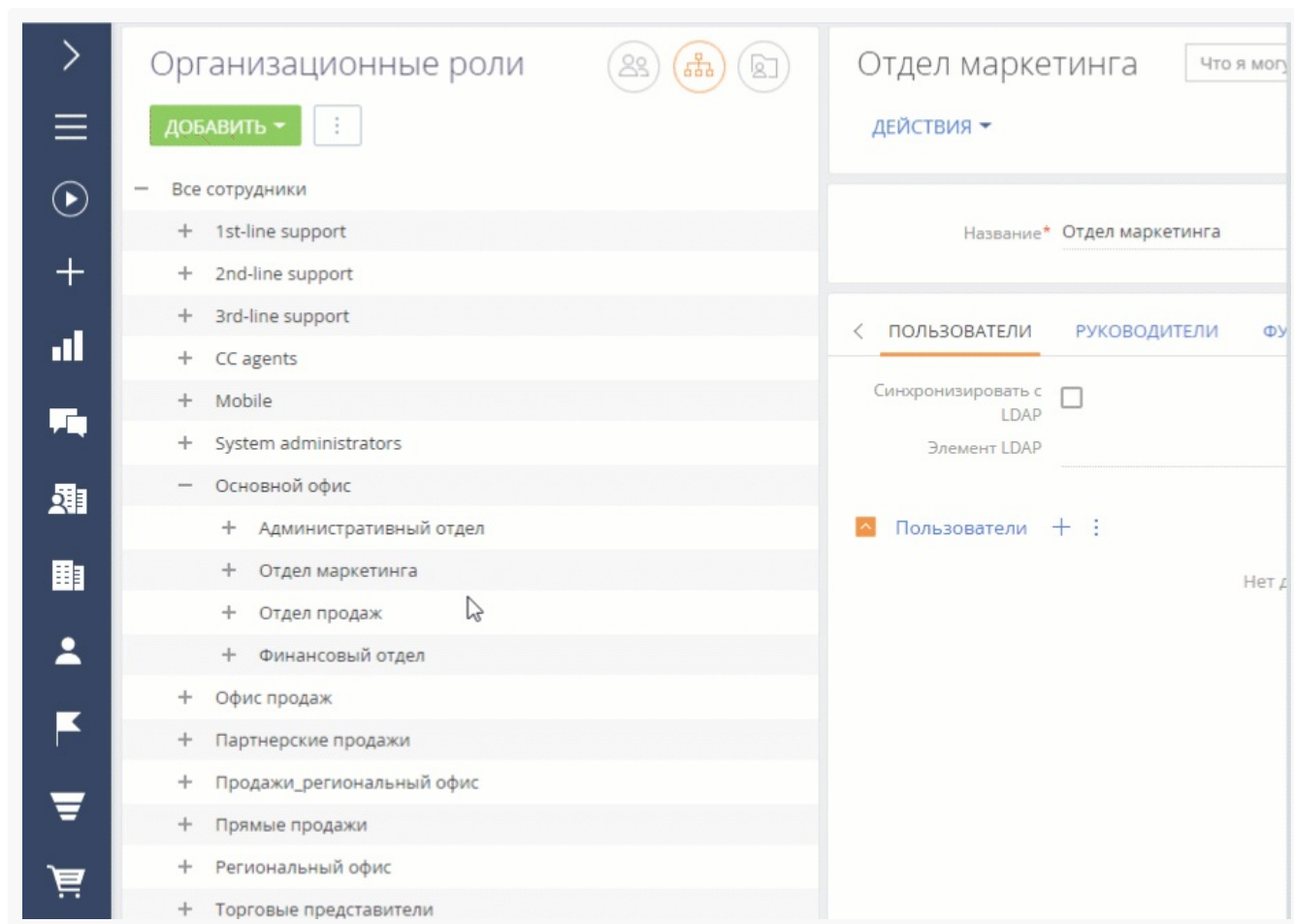
1. Нажмите  → “Организационные роли”.
2. В древовидной структуре ролей **выберите роль**, для которой нужно добавить пользователей.
3. На вкладке [Пользователи]:
 - a. **Если пользователь уже создан** в системе, то нажмите  и выберите [*Добавить существующего*]. Выберите нужных пользователей (Рис. 4).
 - b. **Если пользователь еще не создан** в системе, то нажмите  и выберите [*Добавить нового*]. Заполните страницу нового пользователя.

Рис. 4 — Добавление пользователей в организационную роль



В результате выбранные пользователи будут добавлены в организационную роль. Пользователи получат

все права доступа своей организационной роли.

Подробнее: [Настроить доступ по операциям](#), [Настроить доступ по записям](#), [Настроить права доступа на колонки](#), [Настроить права доступа на системные операции](#).

Настроить доступ по операциям

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

В этой статье рассмотрена настройка прав **доступа к бизнес-данным**. Доступ к бизнес-данным подразумевает выполнение CRUD-операций с данными (создание, чтение, редактирование и удаление) и выполняется через настройку прав доступа к соответствующим объектам системы.

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты Creatio в онлайн-курсе [Управление пользователями и ролями. Права доступа](#).

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Ниже будет рассмотрена настройка прав на выполнение операций с данными, содержащимися в двух разных объектах системы — в разделе и на детали.
- **По записям.** Подробнее: [Настроить доступ по записям](#).
- **По колонкам.** Подробнее: [Настроить права доступа на колонки](#).

Доступ к действиям системы предоставляется с помощью системных операций. Операции в объекте не следует путать с системными операциями. Настройки прав доступа к действиям системы выполняются в разделе [*Доступ к операциям*] дизайнера системы. Подробнее: [Настроить права доступа на системные операции](#).

На заметку. Существует четыре системные операции, которые отменяют любые другие настройки прав на объект: “Просмотр любых данных” (код “CanSelectEverything”), “Добавление любых данных” (код “CanInsertEverything”), “Изменение любых данных” (код “CanUpdateEverything”) и “Удаление любых данных” (код “CanDeleteEverything”). Пользователь с доступом к этим операциям получит права независимо от настроек в разделе [*Доступ к объектам*].

По умолчанию в приложении настроены права:

- Для организационной роли “**All employees**” (“Все сотрудники”) предоставляется доступ на операции чтения, создания, редактирования и удаления записей всех объектов. Пользователи, входящие в роль “All employees”, будут иметь права на указанные операции, даже если доступ по операциям не используется и переключатель выключен.
- Для организационной роли “**All portal users**” (“Все пользователи портала”) запрещен доступ на выполнение любых операций с записями системы. Чтобы пользователи, входящие в роль “All portal users”, могли видеть на портале свои записи и данные своей организации, необходимо настроить в разделах, доступных на портале, права доступа по операциям.
- Для организационной роли “**System administrators**” (“Системные администраторы”) настроен доступ на системные операции “Добавление любых данных”, “Чтение любых данных”, “Изменение любых данных”, “Удаление любых данных”, имеющие более высокий приоритет, чем настройки, заданные в разделе [*Права доступа на объекты*].

Настроить доступ по операциям в объекте раздела


Пример. Выполним настройку прав доступа к разделу [*Продажи*].

У менеджеров по продажам должны быть все права на записи раздела, кроме удаления.

У их руководителей должен быть неограниченный доступ к записям.

У одного из сотрудников с ролью “Секретари” должна быть возможность просматривать записи раздела, а для остальных секретарей раздел [*Продажи*] должен быть скрыт.

Важно. Если удалить роль “All employees” из области настройки доступа по операциям, а затем выключить переключатель “Использовать доступ по операциям” и применить изменения, то пользователи не смогут видеть записи объекта.

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке “**Права доступа на объекты**”.

Обратите внимание, признаки в колонках [*Доступ по операциям ограничен*], [*Доступ по записям ограничен*] и [*Доступ к колонкам ограничен*] в реестре объектов не редактируются. Они устанавливаются автоматически в зависимости от того, какой тип администрирования доступа (по операциям, по записям, по колонкам) используется для каждого объекта. Если ни один из типов доступа к объекту не ограничен (не установлен ни один из признаков), то все пользователи имеют полный доступ к объекту и имеют право на создание, чтение, редактирование и удаление данных объекта.

2. Выберите необходимый объект из списка или с помощью строки поиска. Например, чтобы настроить права доступа к разделу [*Продажи*], установите фильтр “Разделы” и выберите объект “Продажа”. Кликните по его заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Продажи*] (Рис. 1).

На заметку. Подробнее о выборе объекта читайте в статье [Права доступа на объекты](#) (онлайн-курс).

Рис. 1 — Выбор объекта раздела и переход на страницу настройки прав доступа

Права доступа на объекты

ЗАКРЫТЬ

ДЕЙСТВИЯ

☰ Все объекты

🔍 Поиск

Заголовок	Название	Доступ по операциям ограничен	Доступ по записям ограничен	Доступ по колонкам ограничен
"Правило поиска дублей" в группе	DuplicatesRuleInFolder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
"Правило поиска дублей" в тегах	DuplicatesRuleInTag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmail in campaign view	VwBulkEmailInCampaign	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailInProgress	BulkEmailInProgress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailRecipientMacro	BulkEmailRecipientMacro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailRecipientReplica	BulkEmailRecipientReplica	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Business processes in sections	ProcessInModules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ContactFolder in campaign view	VwFolderInCampaign	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по операциям” (Рис. 2).

Рис. 2 — Включение администрирования по операциям

Права доступа на объект Продажа

ПРИМЕНИТЬ ОТМЕНА ДЕЙСТВИЯ ▼

Заголовок
Продажа

Название
Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

☒ Использовать доступ по операциям ⓘ

Добавьте роли или пользователей, чтобы предоставить им доступ к данным объекта

+ Добавить

☐ Использовать доступ по записям ⓘ

☐ Использовать доступ по колонкам ⓘ

4. По кнопке [*Добавить*] добавьте роли и пользователей, для которых необходимо настроить права доступа. Используйте строку поиска, а также вкладки [*Организационные роли*], [*Функциональные роли*] и [*Пользователи*], чтобы быстро найти нужную роль или пользователя в списке окна выбора. В нашем примере это:
 - a. роль "All employees" (Все сотрудники) — добавляется автоматически;
 - b. организационная роль "Менеджеры по продажам";
 - c. организационная роль "Менеджеры по продажам. Группа руководителей";
 - d. организационная роль "Секретари";
 - e. определенный пользователь с ролью "Секретари" (Рис. 3), например, Ульяновенко Александра.

Рис. 3 — Добавление ролей и пользователей для предоставления им доступа к разделу

Права доступа на объект Продажа

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▼

Заголовок
Продажа

Название
Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

Использовать доступ по операциям ⓘ

Использовать доступ по записям ⓘ

Использовать доступ по колонкам ⓘ


5. По умолчанию для каждой добавленной роли или пользователя устанавливается доступ на просмотр, создание, редактирование и удаление данных объекта. Откорректируйте уровень доступа в соответствии с необходимостью:
 - a. Для роли **“Все сотрудники”** оставьте признак только в колонке [Чтение], а признаки в колонках [Создание], [Редактирование] и [Удаление] снимите. В итоге все сотрудники компании смогут просматривать записи раздела [Продажи], но не смогут их добавлять, вносить изменения и удалять.
 - b. Для роли **“Менеджеры по продажам”** оставьте признаки в колонках [Создание], [Чтение] и [Редактирование], а признак в колонке [Удаление] снимите. В итоге сотрудники отдела продаж смогут просматривать, добавлять и редактировать записи раздела, но не будут иметь возможности их удалять.
 - c. Оставьте признаки в колонках [Создание], [Чтение], [Редактирование] и [Удаление] для роли **“Менеджеры по продажам. Группа руководителей”**. Так руководитель менеджеров по продажам получит право на просмотр, добавление, изменение и удаление записей раздела [Продажи].
 - d. Для роли **“Секретари”** снимите признаки в колонках [Создание], [Чтение], [Редактирование] и [Удаление]. В итоге для секретарей компании раздел [Продажи] будет скрыт.
 - e. Для **определенного пользователя**, который входит в роль “Секретари” (в нашем примере это Ульяновко Александра) оставьте признак в колонке [Чтение]. Так пользователь Ульяновко Александра получит право на просмотр записей раздела [Продажи].

После выполнения настроек рядом с некоторыми правами доступа могут отображаться значки ⓘ . Это означает, что некоторые настройки противоречат друг другу и для корректной работы прав доступа необходимо настроить их приоритет.

Настроить приоритет прав доступа по операциям

© 2022 Terrasoft. Все права защищены.

объекта

Возможны случаи, когда настроенные для некоторых ролей уровни доступа противоречат друг другу, т. к. роли пересекаются. Например, роли “Менеджеры по продажам”, “Менеджеры по продажам. Группа руководителей” и “Секретари” входят в роль “Все сотрудники”. А для одного из секретарей настроены права доступа, которые отличаются от прав, настроенных для всех секретарей. О необходимости настроить приоритеты свидетельствует значок  рядом с противоречащим правом доступа.


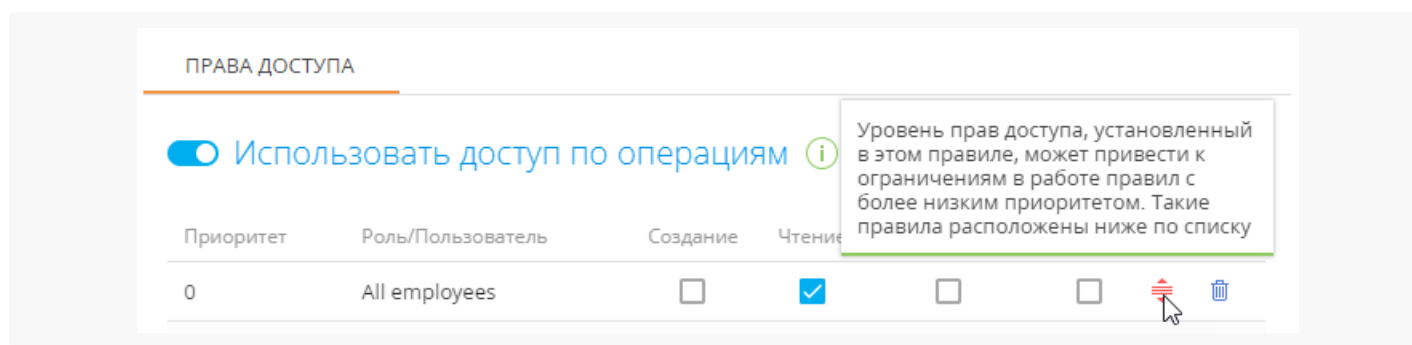
Чем выше в списке правило, тем выше его приоритет. Наиболее приоритетному правилу соответствует значение “0” в колонке [*Приоритет*]. Чем ниже в списке расположено правило и чем больше число в колонке [*Приоритет*], тем ниже приоритет этого правила. Значок , который может отображаться рядом с некоторыми из правил, обозначает, что некоторые из настроенных правил пересекаются. Необходимо понизить или повысить приоритет одного правила, чтобы корректно работало другое (Рис. 4).

Рис. 4 — Предупреждение о необходимости откорректировать приоритет прав доступа



При настройке приоритетов прав доступа **руководствуйтесь следующими правилами:**

- Например, мы хотим запретить всем пользователям доступ к записям раздела [*Продажи*], но менеджерам по продажам (они также входят в роль “Все пользователи”) необходимо дать все права, кроме удаления записей. Для этого расположим роль “Менеджеры по продажам” выше, а роль “Все пользователи” — ниже.
- Если пользователь входит в несколько ролей, для которых настраиваются права доступа, то для него будет применен уровень доступа той роли, которая расположена **выше** в списке. Если определенной роли, за исключением одного или нескольких пользователей, необходимо запретить доступ к какой-либо операции, то расположите такую роль **ниже**, а пользователей, которым надо предоставить доступ — выше. Так, если мы запрещаем доступ к разделу [*Продажи*] для всех секретарей, но предоставляем право просмотра данных одному из них, то роль “Секретари” должна быть расположена ниже того сотрудника, который должен иметь доступ к разделу.
- Пользователи или роли, которые **не добавлены** в область настройки доступа по операциям, не получают доступа к операциям и не участвуют при определении приоритетов прав.

Настроим приоритет прав доступа для приведенного выше примера. Для изменения порядка отображения правил захватите правило курсором мыши и перетащите на нужное место (Рис. 5):

1. Организационную роль с максимальным уровнем доступа (в нашем примере это “Менеджеры по продажам. Группа руководителей”) расположите сверху списка.
2. Далее расположите роль “Менеджеры по продажам”.
3. Роль “All employees” и пользователь Ульяненко Александра, который входит в роль “Секретари”,

имеют одинаковый уровень доступа. Поэтому расположите их под ролью “Менеджеры по продажам” в любом порядке.

4. У роли “Секретари” не должно быть доступа к разделу [*Продажи*], поэтому расположите ее внизу списка.
5. Сохраните настройки по кнопке [*Применить*] в верхнем левом углу страницы.

Рис. 5 — Настройка приоритета прав доступа

Права доступа на объект Продажа

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок
Продажа

Название
Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

Использовать доступ по операциям ⓘ

Приоритет	Роль/Пользователь	Создание	Чтение	Редактирование	Удаление
0	Менеджеры по продажам. Группа руководителей	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Менеджеры по продажам	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	All employees	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Ульяненко Александра	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Секретари	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

+ Добавить

В результате выполненных настроек:

- У пользователей с ролью “**Менеджеры по продажам**” будет доступ к разделу [*Продажи*] с возможностью создавать и редактировать записи раздела. Удалять записи менеджеры по продажам не смогут.
- У **руководителей менеджеров по продажам** будет полный доступ к разделу с возможностью удаления записей.
- **Все сотрудники компании** смогут просматривать записи раздела, но не смогут их создавать, редактировать и удалять.
- Для всех **секретарей** компании, кроме Ульяненко Александры, раздел [*Продажи*] будет скрыт.
- Секретарь **Ульяненко Александра** сможет перейти в раздел и просмотреть записи.

Настроить доступ по операциям в объекте детали

Пример. Выполним настройку доступа к детали [*Файлы и ссылки*] раздела [*Договоры*]. Пользователи с ролью “Менеджеры по продажам” должны иметь полный доступ к записям на детали.

Остальным пользователям необходимо разрешить только просмотр содержащихся на детали файлов и ссылок и запретить их редактирование и удаление.


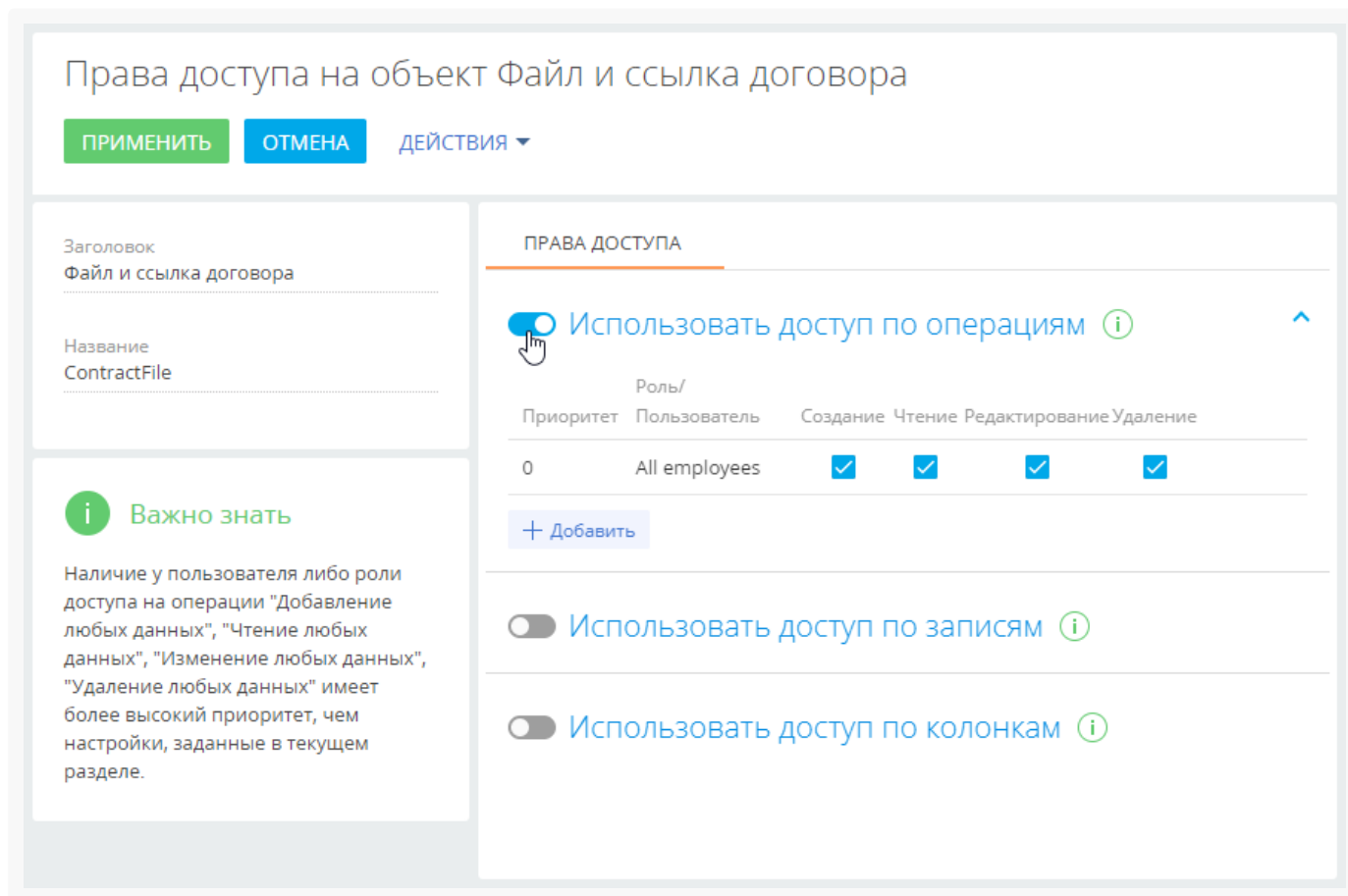

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке **“Права доступа на объекты”**.
2. Установите фильтр “Все объекты”.
3. Найдите объект “Файл и ссылка договора” с помощью строки поиска.
4. Кликните по заголовку или названию найденного объекта.
5. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по операциям” (Рис. 6).

Рис. 6 — Включение администрирования по операциям



6. По кнопке [*Добавить*] добавьте роли и пользователей, для которых необходимо настроить права доступа. Используйте строку поиска, чтобы быстро найти нужную роль или пользователя в списке. В нашем примере это:
 - a. роль “All employees” (Все сотрудники) — добавляется автоматически;
 - b. роль “Менеджеры по продажам”.
7. По умолчанию для каждой добавленной роли или пользователя устанавливаются права на просмотр, создание, редактирование и удаление данных объекта. Откорректируйте уровень прав доступа в соответствии с необходимостью.

- a. Для роли **“Менеджеры по продажам”** оставьте признаки в колонках [*Создание*], [*Чтение*], [*Редактирование*] и [*Удаление*]. Так сотрудники отдела продаж смогут просматривать, добавлять, изменять и удалять данные на детали [*Файлы и ссылки*].
 - b. Для роли **“Все сотрудники”** оставьте признак только в колонке [*Чтение*], а признаки в колонках [*Создание*], [*Редактирование*] и [*Удаление*] снимите. Так все сотрудники смогут только просматривать содержимое детали [*Файлы и ссылки*] договора, но не смогут его добавлять, редактировать и удалять.
8. При необходимости настройте приоритеты прав доступа для указанных ролей. Настройка может потребоваться, если уровни доступа противоречат друг другу, т. к. роли пересекаются. Например, роль “Менеджеры по продажам” входит в роль “Все сотрудники”. О необходимости настроить приоритеты свидетельствует значок  рядом с противоречащим правом доступа.

В результате выполненных настроек:

- У пользователей с ролью **“Менеджеры по продажам”** будет полный доступ к детали [*Файлы и ссылки*] договора с возможностью просматривать, создавать, редактировать и удалять содержимое детали.
- **Все сотрудники компании** смогут просматривать содержимое детали [*Файлы и ссылки*] договора, но не смогут их создавать, редактировать и удалять.

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*))
```

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.

Настроить Single Sign-On через OneLogin

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Вы можете использовать портал OneLogin в качестве единой точки входа для всех сервисов, которые используются в вашей компании, включая Creatio. Для этого нужно выполнить ряд настроек как на стороне OneLogin, так и на стороне Creatio.

Важно. В примере настройки использован адрес сайта Creatio `https://site01.creatio.com/` и `"appid"` как `id` приложения на OneLogin. При выполнении настройки замените эти значения на адрес вашего сайта и `id` соответствующего приложения на OneLogin.

Выполнить настройки на стороне OneLogin

1. Войдите в OneLogin под учетной записью администратора.
2. Нажмите [*Приложения*] ("Apps") и выберите [*Добавить приложения*] ("Add Apps"). В строке поиска введите "Creatio" и выберите приложение Creatio.
3. Если необходимо, то измените значение в поле [*Отображаемое имя*] ("Display name"), измените иконки приложения или снимите признак [*Доступно на портале*] ("Visible in portal"). Эти настройки влияют на отображение сайта для пользователей на сайте OneLogin.

4. Нажмите [*Сохранить*] ("Save").
5. После сохранения перейдите на вкладку [*Конфигурация*] ("Configuration") и в поле [*Сайт Creatio*] ("Creatio site") введите доменное имя вашего сайта, например, site01 (Рис. 1).

Рис. 1 — Страница конфигурации сайта

The screenshot shows the 'Configuration' tab in the Creatio interface. Under the 'Application Details' section, there is a field labeled 'creatio site' with the value 'site01' entered. Below this field, a note states: 'Enter only your personal domain name. For example "name" if your site URL is https://name.creatio.com'. At the top right, there are buttons for 'MORE ACTIONS' and 'SAVE'.

Выполнить настройки на стороне Creatio

Если вы используете **Creatio cloud**, то подготовьте информацию для настройки по инструкции ниже и обратитесь в [службу поддержки Creatio](#) для применения настроек на сайте.

Ниже приведена инструкция по настройке единого входа для пользователей **on-site**. Настоятельно рекомендуем предоставить службе поддержки временный доступ к конфигурации Creatio, либо производить эту настройку под руководством службы технической поддержки.

Чтобы выполнить настройку на стороне Creatio, необходимо выполнить следующие настройки в конфигурационных файлах:

1. Внести настройки SAML-провайдера.
2. Настроить параметры SSO-аутентификации в Creatio.
3. Проверить базовые сценарии SSO.
4. Настроить Just-In-Time User Provisioning (JIT).
5. Включить использование SSO по умолчанию.

Рассмотрим эти пункты подробнее:

1. **Заполните настройки SAML-провайдера**, указав данные SAML-провайдера идентификации в `saml.config`.
 - a. В параметре Name укажите FQDN вашего сайта.

Важно. Значение параметра ServiceProvider Name должно быть идентично значению Identifier, указанному на стороне провайдера идентификации ADFS. Таким образом выполняется проверка, что SAML Assertion выдан именно для вашего приложения. Для этого удобнее использовать FQDN вашего сайта, например, `https://site01.creatio.com/Demo_161215/`.

Обратите внимание, URL должен совпадать полностью, включая "/" в конце.

- b. В секции Partner Identity Provider укажите настройки со стороны IdP. Эти настройки можно посмотреть в файле метаданных.

- **WantAssertionSigned** — укажите "false", если не будет использоваться сертификат шифрования при обмене SALM Assertion.

```
WantAssertionSigned="false"
```

- **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Можно взять из строки SAML 2.0 Endpoint (HTTP) на странице trusted приложения.

```
SingleSignOnServiceUrl="https://ts-dev.onelogin.com/trust/saml2/http-post/sso/appid"
```

- **SingleLogoutServiceUrl** — URL сервиса единого выхода провайдера. Можно взять из строки SLO Endpoint (HTTP) на странице trusted приложения.

```
SingleLogoutServiceUrl="https://ts-dev.onelogin.com/trust/saml2/http-redirect/slo/appid"
```

2. **Включите использование SSO-провайдера в Creatio.** Для этого внесите необходимые настройки в web.config в корневой папке сайта:

- a. Включите использование SSO Auth-провайдеров при выполнении авторизации в Creatio:

- **SsoAuthProvider** — провайдер входа в основное приложение.
- **SSPSsoAuthProvider** — провайдер входа на портал.
Указывать можно оба провайдера или только один, который нужен в конкретном случае.

```
<terrasoft>
<auth providerNames="InternalUserPassword,SSPUserPassword,SsoAuthProvider,SSPSsoAuthProv
<providers>
```

- d. Укажите, какой из провайдеров идентификации, указанных в saml.config, нужно использовать по умолчанию в Service Provider initiated SSO-сценариях. В web.config App Loader задайте параметр PartnerIdP значением из строки Issuer URL в saml.config, например:

```
<appSettings> ... <add key="PartnerIdP" value="https://app.onelogin.com/saml/metadata/appid">
```

- e. Установите использование SSO-провайдера по умолчанию при входе на сайт. Для этого укажите в web.config App Loader ресурс по умолчанию Login/NuiLogin.aspx?use_sso=true.

На заметку. Для возможности входа с использованием логина/пароля остается доступной прямая ссылка <https://site01.creatio.com/Login/NuiLogin.aspx?>. Для тестирования работы SSO

до включения по умолчанию можно использовать ссылку
https://site01.creatio.com/NuiLogin.aspx?use_sso=true.

- f. Установите отправку к провайдеру идентификации при переходе в корень сайта:

```
<defaultDocument> <files> <add value="Login/NuiLogin.aspx?use_sso=true" /> </files> </defaultDocument>
```

- g. Установите отправку к провайдеру идентификации при отсутствии сессии пользователя:

```
<authentication mode="Forms">
  <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true" protection="All" timeout="60" name=".LoginFormsAuthentication" />
</authentication>
```

3. Проверьте базовый сценарий Identity Provider (IdP) initiated SSO, чтобы убедиться в корректности настроек:

- Переход на страницу доверенных приложений IdP (ссылка по умолчанию:
<https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx>).
- Выполнение авторизации.
- Переход на Creatio с результатом авторизации на IdP.
 До включения провайдера SSO на стороне Creatio по умолчанию используйте для проверки корректности настроек IdP initiated сценарий. До выполнения проверки убедитесь, что в Creatio содержится активная учетная запись, логин которой совпадает с NameId, передаваемым Identity Provider. В противном случае процесс SSO настройки не будет успешно завершен, поскольку не удастся сопоставить пользователя из домена с пользователем в Creatio. Как только вход через SSO будет выполнен успешно, перейдите к дальнейшим настройкам.

4. Настройте Just-In-Time User Provisioning (JIT). Функциональность Just-In-Time User Provisioning дополняет технологию единого входа. Она позволяет не только создать пользователя при первом входе в приложение, но и при каждом входе обновлять данные на странице контакта данными, полученными от провайдера идентификации. Подробнее читайте в статье [Настроить Just-In-Time User Provisioning](#).

- a. В web.config в корневой папке приложения добавьте настройки для JIT:

```
<add name="UseJit" value="true" />
```

Тип пользователя определяется страницей, с которой им был выполнен вход в систему. Если для входа используется сценарий **IdP initiated**, то необходимо явно указать значение DefUserType:

- General — обычный пользователь;
- SSP — пользователь портала.

- d. Настройте сопоставление полей из SAML Assertion с колонками в Creatio в справочнике [Преобразователь SAML атрибута в название поля контакта]. Это необходимо для корректного

заполнения полей контакта при создании нового пользователя с помощью Just-In-Time User Provisioning. Если поле пусто или отсутствует в данных провайдера идентификации, то оно может быть заполнено значением, указанным в поле[*Значение по умолчанию*] справочника. При следующем входе пользователя поля контакта, указанные в справочнике, будут заполнены значением, полученным из провайдера, или актуальным значением по умолчанию.

На заметку. Если справочника нет в списке справочников, то его необходимо зарегистрировать.

5. **Включите использование SSO-провайдера по умолчанию** при входе на сайт. Рекомендуем выполнять действие только в случае успешного выполнения предыдущих шагов и проверки корректности работы. После успешного выполнения этого шага будет доступен для использования Service Provider (SP) initiated SSO. Стандартный сценарий Service Provider (SP) initiated:

- a. Переход на Creatio, у пользователя нет активной сессии на сайте.
- b. Переадресация на IdP, выполнение авторизации.
- c. Переадресация Переход на Creatio с результатом авторизации из IdP.

Для включения провайдера SSO по умолчанию:

- a. Включите Single Log Out в web.config в папке Terrasoft.WebApp:


```
<add key="UseSlo" value="true" />
```

- b. Для использования технологии единого входа в мобильном приложении установите признак [*Значение по умолчанию*] в системной настройке “Использовать SSO в мобильном приложении” (код “MobileUseSSO”).

Функциональные роли

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Функциональная роль отражает должность, которую сотрудник занимает в компании, например, роль “Менеджеры по продажам”. Подробнее: [Пользователи и роли](#) (статья онлайн-курса).

Для управления такими должностями нажмите  —> “**Функциональные роли**”.

В разделе доступна древовидная структура функциональных ролей компании, а также информация по выбранной функциональной роли.

На заметку. По умолчанию доступ к разделу есть только у администраторов системы. Для работы с этим разделом пользователям необходимо иметь разрешение на выполнение системной операции “Управление списком пользователей” (“CanManageUsers”).


Используйте функциональные роли для настройки одинаковых прав доступа для всех сотрудников, которые занимают определенную должность, независимо от того, в каком подразделении компании они

работают. Например, для руководителей, работающих в основном и региональном офисах компании. Для этого:

1. **Создайте функциональные роли** в системе.
2. **Включите в функциональную роль организационные роли**, которые должны в нее входить.
3. **Настройте права доступа** для добавленной функциональной роли. Подробнее: [Настроить доступ по операциям](#), [Настроить доступ по записям](#), [Настроить права доступа на колонки](#), [Настроить доступ по операциям](#).

Добавить функциональную роль

Для добавления функциональной роли:

1. Нажмите  —> **“Функциональные роли”**.
2. Нажмите кнопку [*Добавить*]. В открывшемся окне введите название роли.

На заметку. Название функциональной роли должно быть уникальным.


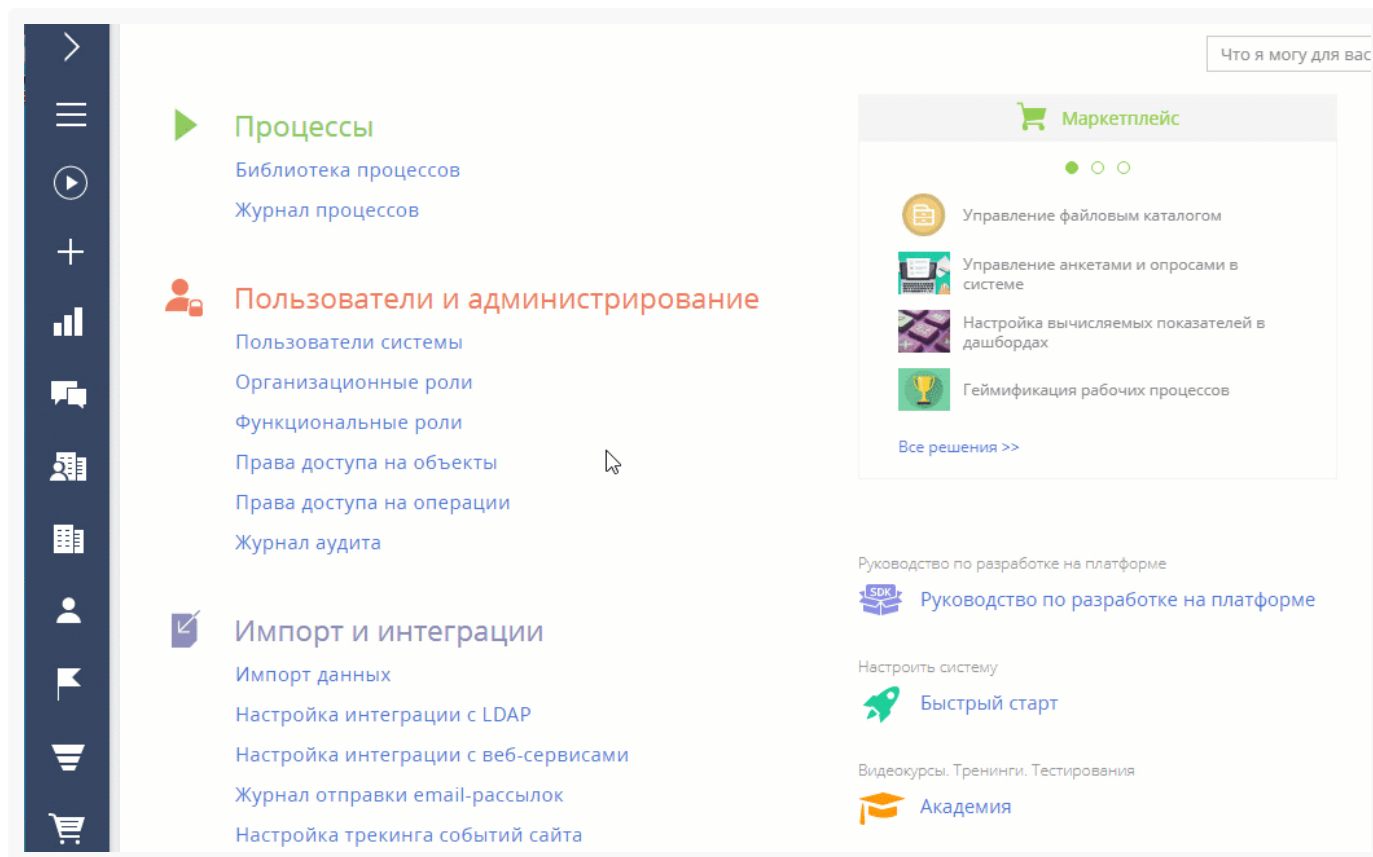
3. Нажмите [**Сохранить**].
4. Чтобы изменения вступили в силу, нажмите  —> [**Актуализировать роли**] ([Рис. 1](#)).

Рис. 1 — Добавление функциональной роли



В результате в Creatio будет добавлена новая функциональная роль.

Связать функциональные и организационные роли

Функциональная роль может включать в себя ряд организационных ролей. Например, вы можете связать функциональную роль “Менеджеры” с организационными ролями “Главный офис. Группа руководителей” и “Региональный офис. Группа руководителей”.

Для того чтобы связать функциональную роль с организационными ролями:




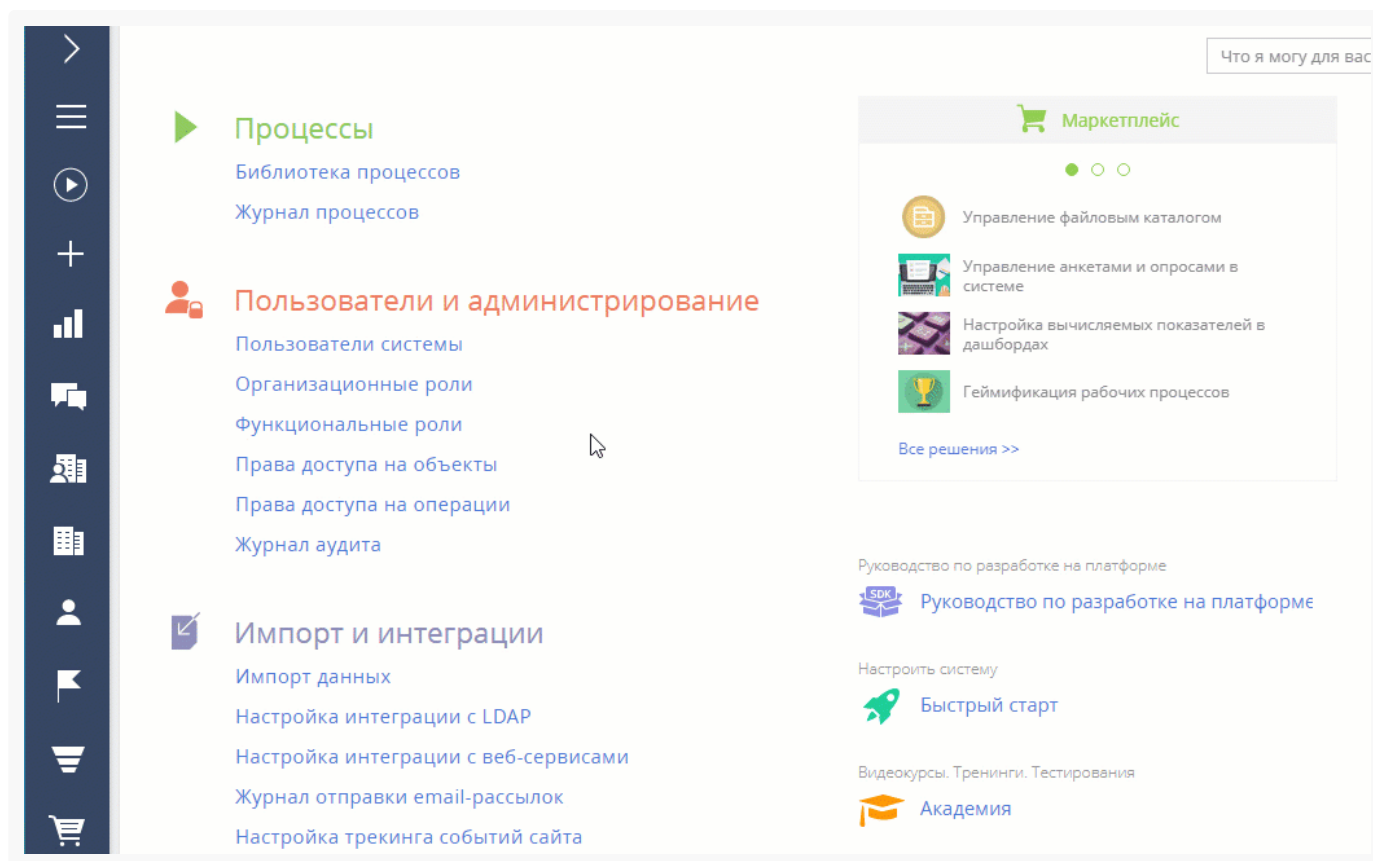
1. Нажмите  —> “**Функциональные роли**”.
2. В списке функциональных ролей **выберите нужную функциональную роль**. Справа откроется страница выбранной роли.
3. На вкладке [**Организационные роли**] нажмите  и **добавьте организационные роли**, которые должны входить в данную функциональную роль. Например, в функциональную роль “Руководство” включите роли “Основной офис. Группа руководителей” и “Региональный офис. Группа руководителей”.
4. Чтобы изменения вступили в силу, закройте страницу и нажмите  —> [**Актуализировать роли**] ([Рис. 2](#)).

Рис. 2 — Связь функциональной и организационных ролей



В результате функциональная роль “Менеджеры” будет связана с организационными ролями “Главный офис. Группа руководителей” и “Региональный офис. Группа руководителей”. Все права доступа связанных организационных ролей будут предоставлены пользователям, входящим в функциональную роль “Менеджеры”.

Добавить пользователей в функциональную роль

Существует несколько способов добавить пользователей в функциональную роль:

- Добавить существующих пользователей (выбрать из списка пользователей).
- Создать и добавить нового пользователя (нужно будет заполнить страницу нового пользователя).
- Импортировать пользователей LDAP. [Подробнее >>>](#)

Важно. Импортировать пользователей LDAP можно только в том случае, если настроена интеграция системы с LDAP. Подробнее: [Настройка интеграции с LDAP](#).

Чтобы добавить пользователей в функциональную роль:


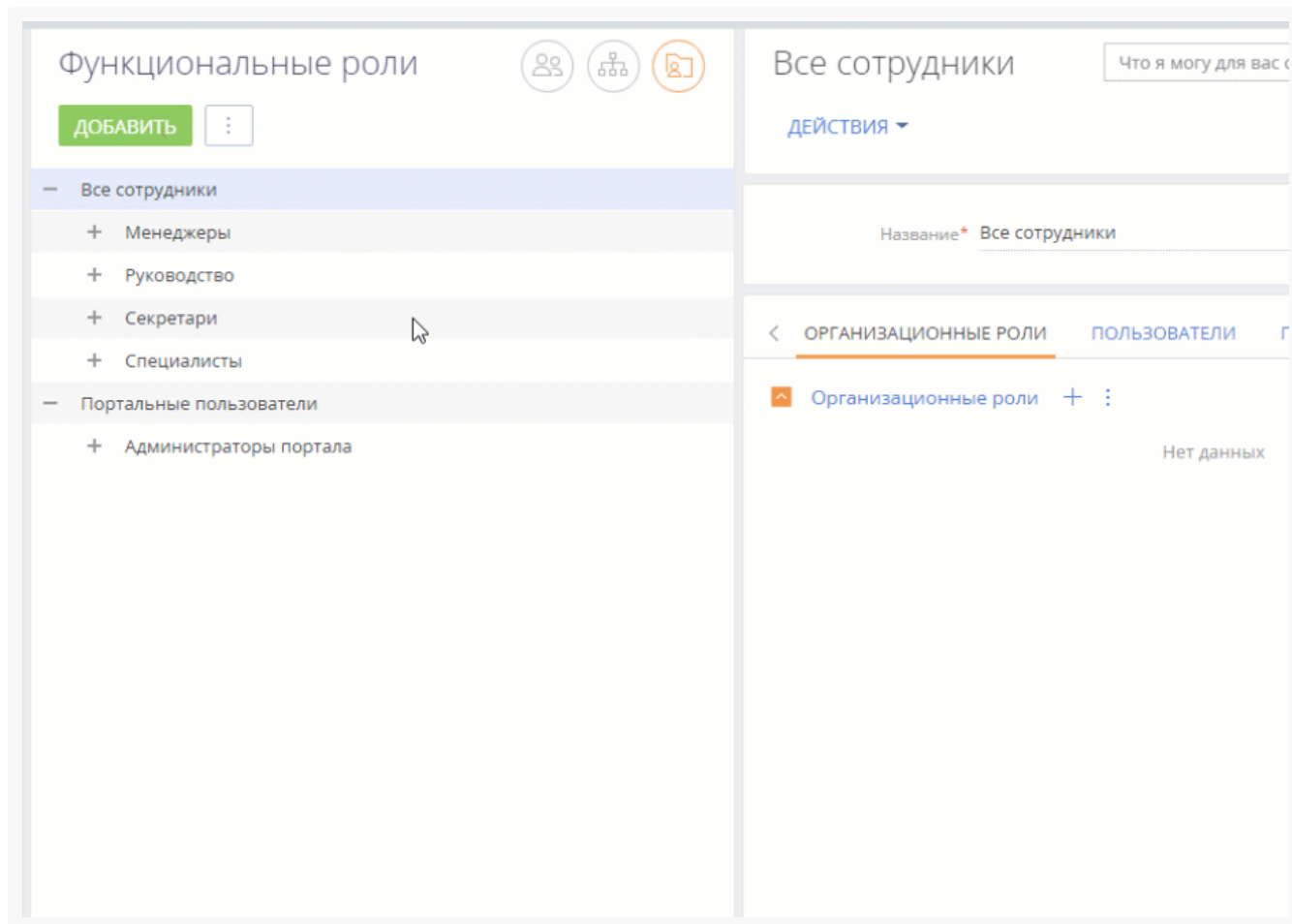
1. Нажмите  —> “**Функциональные роли**”.
2. В списке функциональных ролей **выберите нужную организацию или подразделение**.
3. На вкладке [**Пользователи**]:
 - a. **Если пользователь уже создан** в системе, то нажмите **+** и выберите [**Добавить существующего**]. Выберите нужных пользователей ([Рис. 3](#)).
 - b. **Если пользователь еще не создан** в системе, то нажмите **+** и выберите [**Добавить нового**]. Заполните страницу нового пользователя.

Рис. 3 — Добавление пользователей в функциональную роль



В результате новые или существующие пользователи будут добавлены в функциональную роль. Кроме того, они унаследуют все права доступа, настроенные для этой роли.

Подробнее: [Настроить доступ по операциям](#), [Настроить доступ по записям](#), [Настроить права доступа на колонки](#), [Настроить доступ по операциям](#).

Настроить права доступа на колонки

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Подробнее: [Настроить доступ по операциям](#).
- **По записям.** Подробнее: [Настроить доступ по записям](#).
- **По колонкам.** Настройка прав доступа на уровне чтения, редактирования и удаления **отдельных колонок** выбранного объекта будет рассмотрена в данной статье.

Колонки объектов отображаются в виде полей на страницах и в реестрах разделов и деталей.

Использование доступа по колонкам позволяет ограничить права на чтение и редактирование значений в отдельных полях объекта для отдельных пользователей или ролей. Например, вы можете ограничить право на просмотр данных в поле [*Годовой оборот*] для роли "Секретари", а остальным сотрудникам

компании оставить доступ к полю. При этом для пользователей, у которых нет права на чтение данных в поле [*Годовой оборот*], поле останется видимым, но его значение отображаться не будет (Рис. 1).

Рис. 1 — Пример отображения поля [*Годовой оборот*], когда настроен запрет на доступ к нему

The screenshot shows a user interface for a company profile. At the top, there are four tabs: 'ОСНОВНАЯ ИНФОРМАЦИЯ' (Basic Information), 'КОНТАКТЫ И СТРУКТУРА' (Contacts and Structure), 'ОБСЛУЖИВАНИЕ' (Service), and 'ХРОНОЛОГИЯ' (Chronology). The 'ОСНОВНАЯ ИНФОРМАЦИЯ' tab is active. Below the tabs, the company name 'АльфаБизнес' (AlfaBusiness) is displayed with a code '34'. Under the 'Категоризация' (Categorization) section, 'Количество сотрудников' (Number of employees) is '501-1000' and 'Форма собственности' (Ownership form) is 'АО'. The 'Годовой оборот' (Annual turnover) field is highlighted with a red box, indicating it is redacted. Below this, the 'Средства связи' (Contact methods) section shows the website 'www.alfabizness.com', a fax number '+7 495 277 01 98', and two phone numbers: '+7 495 277 01 96' and '+7 495 384 02 18'.

При использовании доступа по колонкам для определенных ролей и пользователей более приоритетными являются настроенные для них [права доступа по операциям](#). Например, если у пользователя нет права на операцию чтения данных объекта, то для такого пользователя объект будет скрыт полностью.

Доступ к колонкам, не добавленным на деталь, и к колонкам на детали, для которых не указаны права доступа, определяется настройками прав доступа по операциям.

Если в объект, для которого уже используется администрирование по колонкам, добавляется новая колонка, то право на чтение такой колонки выдается автоматически всем пользователям.

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты в Creatio в онлайн-курсе [Управление пользователями и ролями. Права доступа](#).

Важно. Перед настройкой прав доступа на колонки объекта убедитесь, что у пользователя есть доступ на те операции в объекте, которые соответствуют необходимым правам доступа по колонкам. Обратите внимание, если доступ к объекту не администрируется по операциям, то всем пользователям по умолчанию предоставляется право на операции создания, чтения, редактирования и удаления данных объекта. Подробнее: [Настроить доступ по операциям](#).

Настроить доступ на колонки объекта

Рассмотрим, как предоставить или ограничить права групп пользователей на просмотр и редактирование данных, содержащихся в определенном поле записи раздела.

Пример. Выполним настройку прав доступа к полю [*Годовой оборот*] на странице контрагента. Все сотрудники компании, кроме секретарей, должны иметь возможность просматривать значение

поля [*Годовой оборот*], а менеджеры по продажам — просматривать и редактировать значение поля.

Для секретарей значение этого поля должно быть скрыто.


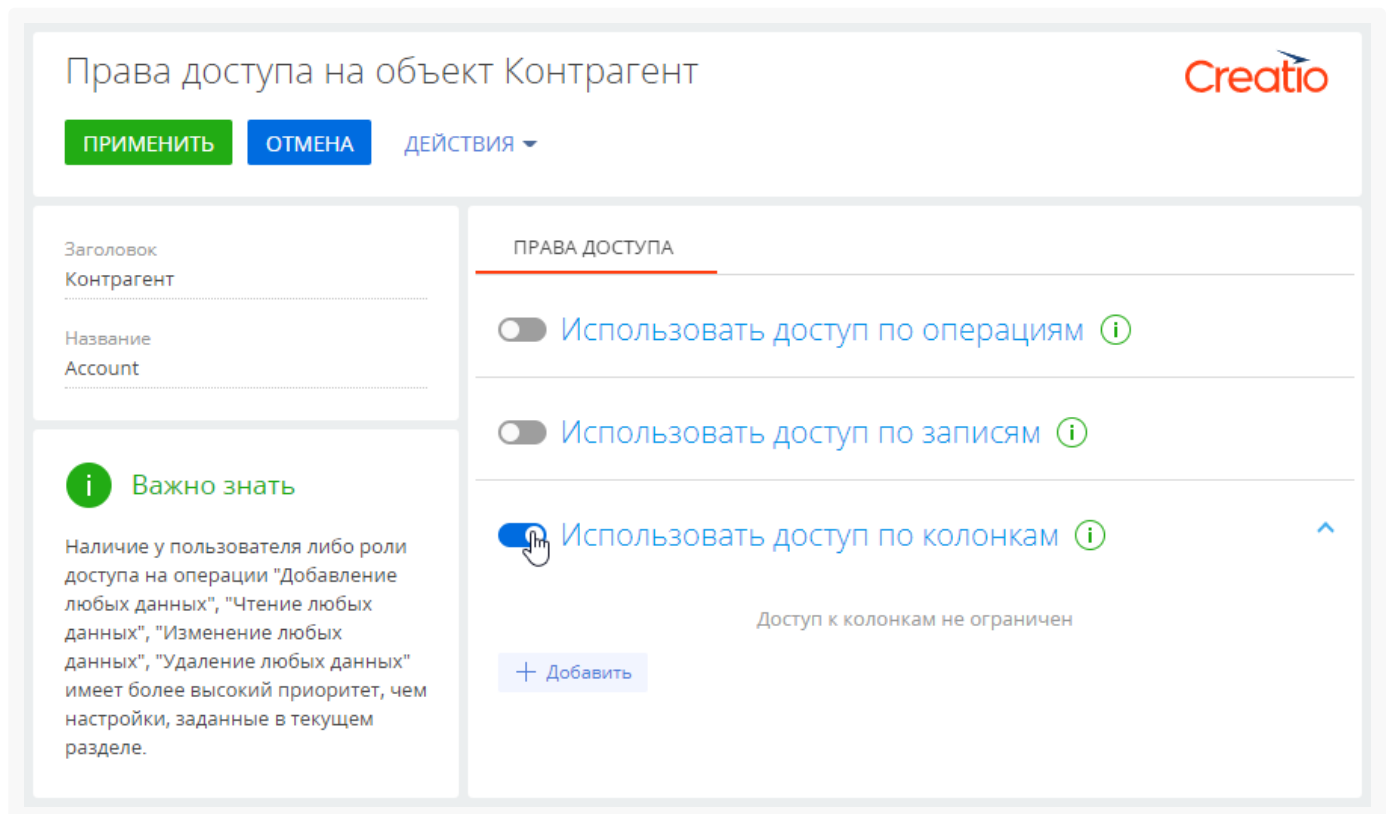
1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке **“Права доступа на объекты”**.
2. Выберите необходимый объект из списка или с помощью строки поиска. Так, чтобы настроить права доступа к полю [*Годовой оборот*] контрагента, установите фильтр “Разделы” и выберите объект “Контрагент”. Кликните по его заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Контрагенты*].
3. Убедитесь, что у пользователей или ролей, для которых вы хотите настроить доступ по колонкам, уже есть доступ на операции в объекте — объект не администрируется по операциям, либо пользователи и роли имеют доступ на соответствующие операции на уровне объекта.
4. Включите ограничение доступа по колонкам с помощью переключателя “Использовать доступ по колонкам” (Рис. 2).

Рис. 2 — Включение администрирования по колонкам

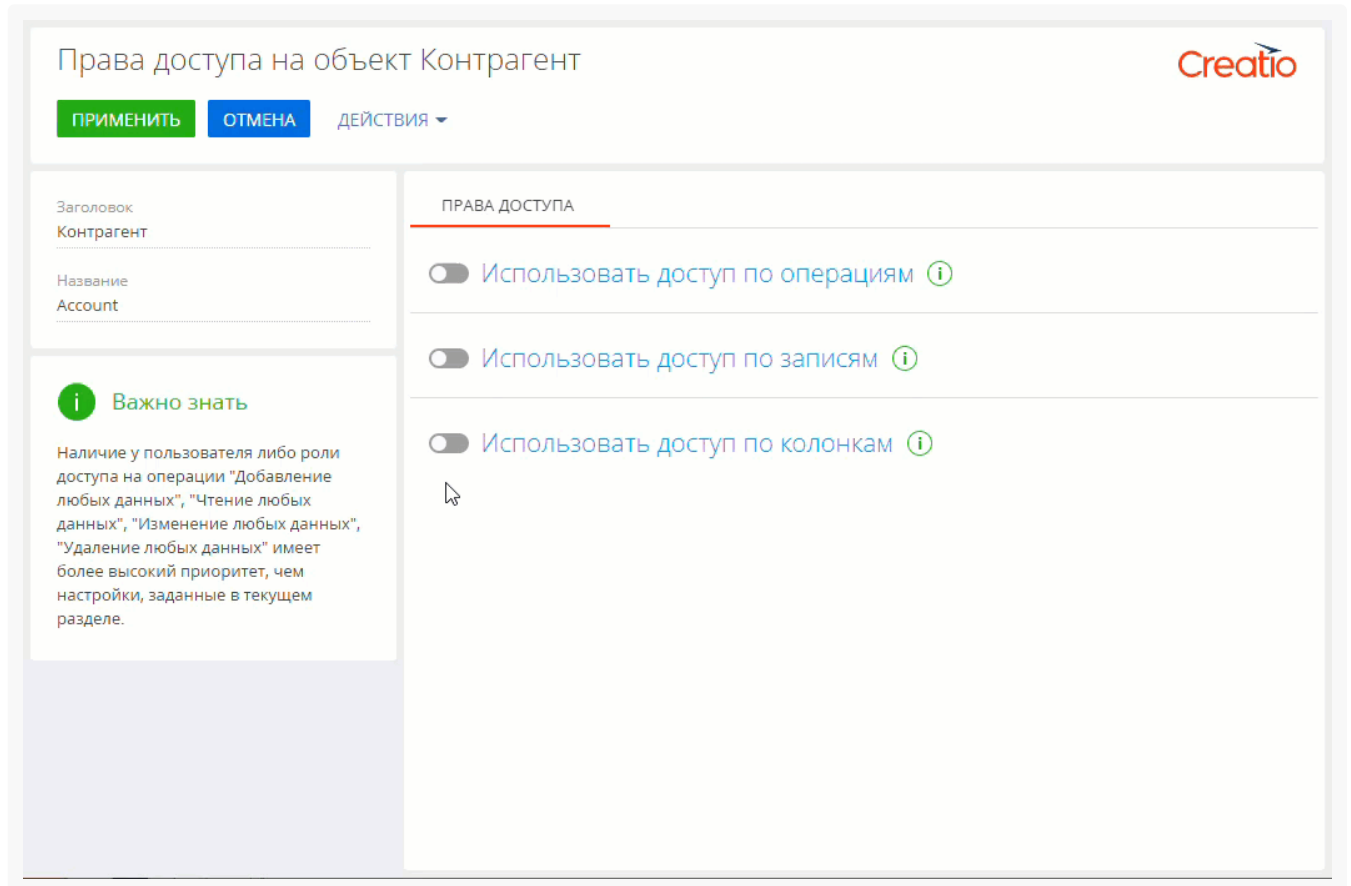


5. По кнопке [*Добавить*] выберите и добавьте колонку объекта, доступ к которой необходимо ограничить. Например, для ограничения доступа к полю [*Годовой оборот*] введите его название в строку поиска и нажмите [*Выбрать*]. Выбранная колонка отобразится в области настройки прав доступа слева. Справа можно добавить роли и пользователей и установить для них уровень прав доступа (Рис. 3). При необходимости добавьте и другие колонки, на которые нужно ограничить доступ. Переключайтесь между колонками в списке, чтобы настроить права доступа для каждой из них.

6. По кнопке [*Добавить*] в правой части области настройки добавьте все роли и пользователей, для которых нужно настроить доступ к выбранной колонке. Используйте строку поиска и вкладки [*Организационные роли*], [*Функциональные роли*] и [*Пользователи*], чтобы быстро найти нужную роль или пользователя (Рис. 3). В нашем примере это:


- роль “All employees” (Все сотрудники) — добавляется автоматически;
- организационная роль “Менеджеры по продажам”;
- организационная роль “Секретари”.

Рис. 3 — Добавление ролей и пользователей для настройки доступа к полю [*Годовой оборот*] контрагента



По умолчанию для каждой добавленной роли или пользователя устанавливается доступ на чтение и редактирование значения выбранного поля объекта. Откорректируйте уровень прав доступа в соответствии с необходимостью. Например:

- Для организационной роли “**All employees**” (Все сотрудники) измените уровень прав на “Чтение разрешено”. В итоге все сотрудники компании смогут видеть значение в поле [*Годовой оборот*] контрагента, но не смогут его отредактировать.
- Для роли “**Менеджеры по продажам**” оставьте уровень доступа “Чтение и редактирование разрешено”. Так сотрудники отдела продаж смогут видеть и редактировать значения в поле [*Годовой оборот*] контрагента.
- Для роли “**Секретари**” установите уровень прав “Чтение и редактирование запрещено”. В итоге для секретарей компании значение поля [*Годовой оборот*] будет скрыто.

После выполнения настроек рядом с некоторыми правами доступа могут отображаться значки  .

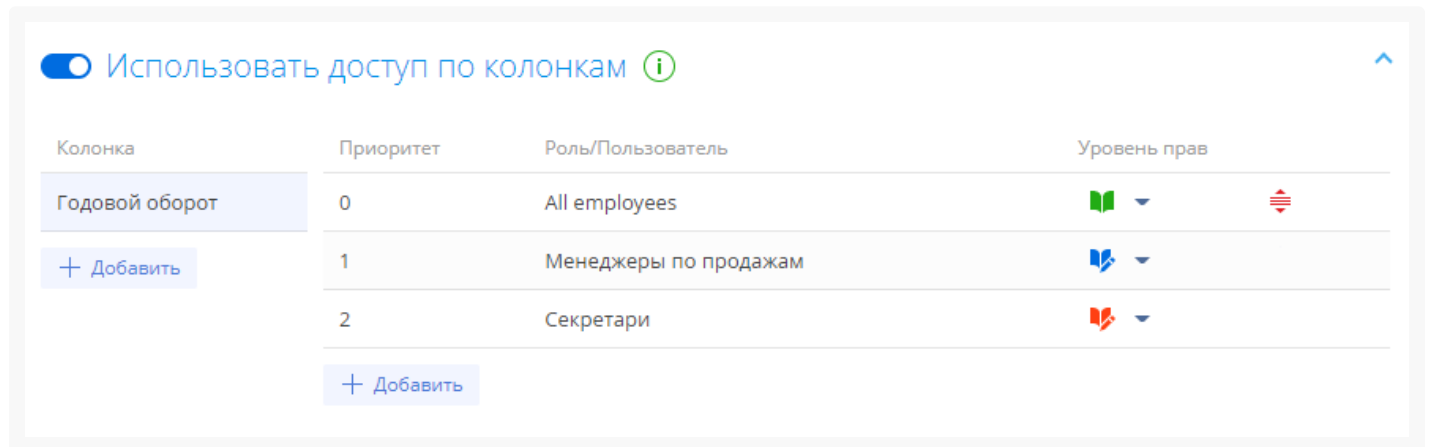
Это означает, что некоторые настройки противоречат друг другу и возможно, потребуется настроить приоритет для корректной работы прав доступа.


Настроить приоритет прав доступа на колонки объекта

Возможны случаи, когда настроенные для некоторых ролей или пользователей уровни доступа противоречат друг другу, т. к. роли пересекаются.

Например, роли “Менеджеры по продажам”, и “Секретари” входят в роль “Все сотрудники”. При этом уровень прав доступа для менеджеров по продажам выше, чем уровень прав для всех сотрудников (Рис. 4).

Рис. 4 — Пример противоречия между уровнями прав доступа




Чем выше в списке правило, тем выше его приоритет. Наиболее приоритетному правилу соответствует значение “0” в колонке [*Приоритет*]. Чем ниже в списке расположено правило и чем больше число в колонке [*Приоритет*], тем ниже приоритет этого правила. Значок , который может отображаться рядом с некоторыми из правил, обозначает, что некоторые из настроенных правил пересекаются и возможно, необходимо понизить или повысить приоритет одного правила, чтобы корректно работало другое.

При настройке приоритетов прав доступа по колонкам **руководствуйтесь следующими правилами:**

- Самыми приоритетными являются ограничения по операциям, используемые для данного объекта.
- Если пользователь входит в несколько ролей, для которых настраиваются права доступа, то для него будет применен уровень доступа той роли, которая расположена выше в списке.

Например, мы хотим запретить всем сотрудникам редактировать поле, но менеджерам по продажам оставить возможность чтения и редактирования. Для этого расположим роль “Менеджеры по продажам” выше, а роль “All employees” (Все сотрудники) — ниже.

- Если роль, для которой необходимо полностью запретить доступ к колонке, входит в роль с более высоким уровнем доступа, то выше расположите роль, для которой ограничиваете доступ, а родительскую роль — ниже.

Так, если мы запрещаем чтение и редактирование поля для всех секретарей, то роль “Секретари” должна быть расположена выше роли “All employees” (Все сотрудники), у которых есть только право на чтение колонки. При этом рядом с уровнем прав, установленным для секретарей, отображается значок .

На заметку. В данном случае настройка приоритета не требуется, т. к. противоречие между правами доступа для роли “Секретари” и роли “All employees” (Все сотрудники), в которую входит роль “Секретари”, состоит в том, что секретари не смогут просматривать значение колонки, что и было необходимо настроить.

- Права доступа для пользователей или ролей, которые не добавлены в область настройки доступа по колонкам, соответствуют правам доступа по операциям, которые для них настроены.

Настроим приоритет прав доступа для приведенного выше примера. Для изменения порядка отображения правил захватите правило курсором мыши и перетащите на нужное место (Рис. 5):

- Организационную роль с максимальным уровнем доступа (в нашем примере это “Менеджеры по продажам”) расположите вверху списка.
- Далее расположите роль “Секретари”, для которой значение поля [*Годовой доход*] должно быть скрыто.
- Роль “All employees” (Все сотрудники) расположите внизу списка.
- Сохраните настройки по кнопке [*Применить*] в верхнем левом углу страницы.

Рис. 5 — Пример настройки приоритета прав доступа по колонкам

Права доступа на объект Контрагент

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок

Контрагент

Название

Account

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

Использовать доступ по операциям ⓘ

Приоритет	Роль/Пользователь	Создание	Чтение	Редактирование	Удаление
0	All employees	✓	✓	✓	✓

+ Добавить

Использовать доступ по записям ⓘ

Использовать доступ по колонкам ⓘ

Колонка	Приоритет	Роль/Пользователь	Уровень прав
Годовой оборот	0	Менеджеры по продажам	🔵 ▾
	1	Секретари	🔴 ▾ 🔒
	2	All employees	🟢 ▾

+ Добавить

В результате выполненных настроек:

- У пользователей с ролью “**Менеджеры по продажам**” будет возможность просматривать и редактировать значение в поле [*Годовой оборот*] контрагента.
- Для всех **секретарей** значение в поле [*Годовой оборот*] контрагента будет скрыто.
- **Все сотрудники компании** смогут видеть значение в поле [*Годовой оборот*], но не смогут его редактировать.

Подробнее: [Пользователи и права доступа](#) (онлайн-курс).

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.

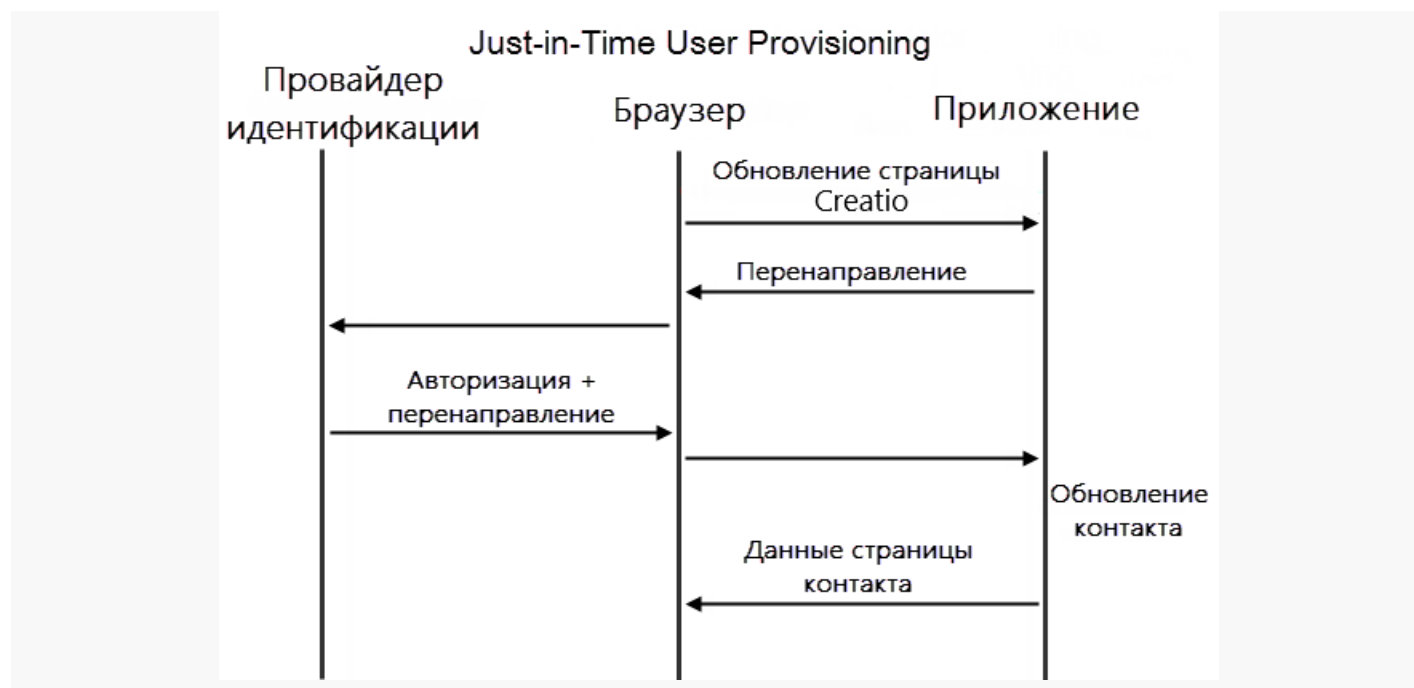
На заметку. При связывании пользователя LDAP с учетной записью пользователя Creatio происходит автоматическое лицензирование последней, если установлен соответствующий признак. Подробнее: [Настроить подключение к серверу](#).

Настроить Just-In-Time User Provisioning

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Функциональность Just-In-Time User Provisioning (JIT UP) избавляет от необходимости создания учетных записей для каждого отдельного сервиса и поддержания актуальности базы пользователей вручную. JIT UP дополняет технологию единого входа, позволяя снизить количество операций по администрированию учетных записей и персональных данных в записи контактов. При каждом входе пользователя с помощью технологии единого входа данные на странице контакта обновляются данными, полученными от провайдера идентификации ([Рис. 1](#)). Если у пользователя нет учетной записи в Creatio, то она может быть создана при первом входе.

Рис. 1 — Схема обновления данных при использовании Just-in-Time User Provisioning



На заметку. Обновление контакта данными от провайдера идентификации включает в себя обновление данных контакта на странице записи и принадлежности к группам контактов в Creatio.

Включить использование JIT UP вы можете при настройке интеграции с провайдером идентификации. Подробнее читайте в статьях [“Настроить Single Sign-On через ADFS”](#) и [“Настроить Single Sign-On через OneLogin”](#).

Для того чтобы указать, какие поля записи контакта необходимо заполнять данными из домена, необходимо настроить сопоставление полей из SAML Assertion с колонками Creatio. Настройка сопоставления выполняется в SAML Assertion провайдера идентификации и в справочнике [*Соответствие полей SAML полям контакта*] в Creatio.

Для выполнения настройки необходима настроенная учетная запись в провайдере идентификации ([Рис. 2](#)), в которой есть необходимые для Creatio данные.

Рис. 2 — Поля учетной записи в провайдере идентификации OneLogin

← John Best

MORE ACTIONS

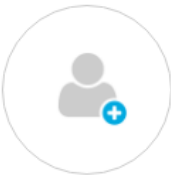
SAVE USER

User Info

Authentication

Applications

Activity



Active

☒

First Name *

John

Last Name *

Best

Email

john.best.business@gmail.com

Username

John Best

Phone Number

+44205549222

Manager

Choose a manager

Company

Our company

Department

IT Service

Title

Manager

Custom Fields

Show Custom Fields

Directory Details

Show Directory Details

Для настройки параметров заполнения полей выполните следующие действия:

На заметку. Для проверки корректности параметров рекомендуем использовать дополнение [SAML Decoder](#) в браузере Google Chrome.

1. Проверьте, что все нужные поля передаются в Creatio. Например, для заполнения профиля пользователя John Best необходимо настроить передачу полей [*Company*], [*Department*], [*Email*], [*First Name*], [*Last Name*], [*Phone*] ([Рис. 3](#)).

Рис. 3 — Параметры приложения в провайдере идентификации OneLogin

MORE ACTIONS

SAVE

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users

bpmonline Field	Value	Add parameter
Company	Company	custom parameter
NameID	Email	
department	Department	
email	Email	
first name	First Name	
last name	Last Name	
phone number	Phone	
role	- No default -	
username	AD user name	

2. Проверьте, что на стороне Creatio для каждого необходимого поля заданы корректные правила получения значений и обновления колонок. Правила настраиваются в справочнике [*Соответствие полей SAML полям контакта*]. Для каждого поля, полученного из провайдера идентификации, необходимо указать колонку в Creatio. Например, для заполнения профиля контакта John Best укажите колонки [*Department*], [*Account*], [*Phone*], [*Email*], [*Given name*], [*Surname*] ([Рис. 4](#)).

На заметку. В качестве колонок контакта необходимо указывать названия колонок в базе данных Creatio.

Рис. 4 — Настройка справочника SAML

Преобразователь SAML атрибута в название поля контакта

 Фильтр ▼

Название SAML атрибута	Название колонки контакта	Значение колонки по умолчанию
type	Type	Сотрудник
department	Department	
Company	Account	
phone number	Phone	
email	Email	
first name	Given Name	
last name	Surname	
Company	Account	

3. Поле, которое отсутствует в данных провайдера идентификации, может быть заполнено значением, указанным в поле [*Значение колонки по умолчанию*] справочника [*Соответствие полей SAML полям контакта*]. Например, провайдер идентификации OneLogin не содержит поле [*Тип контакта*] и не передает его при входе пользователя. Для заполнения этого поля задайте в справочнике правило и укажите в нем значение по умолчанию “Сотрудник” ([Рис. 4](#)). В этом случае у созданных контактов в поле [*Тип*] всегда будет указано значение “Сотрудник”.
4. При необходимости, для провайдера идентификации OneLogin можно добавить пользовательские параметры и поместить в них макросы. Подробнее о работе с макросами читайте в [документации OneLogin](#).

Добавить пользователей

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для управления пользователями в Creatio используется раздел [*Пользователи системы*]. Настройки пользователя определяют, какие задачи пользователь может выполнять, какие данные может видеть и как с этими данными взаимодействовать.

На заметку. По умолчанию доступ к разделу есть только у администраторов системы.

Для перехода в раздел нажмите  — > “Пользователи системы”.

Добавить пользователя с правами системного администратора

В системе доступна организационная роль “**Системные администраторы**” (“System administrators”), члены которой по умолчанию имеют полный доступ ко всем данным. Он достигается за счет доступа к следующим системным операциям:

- “Добавление любых данных” (код “CanInsertEverything”);
- “Удаление любых данных” (код “CanDeleteEverything”);
- “Изменение любых данных” (код “CanUpdateEverything”);
- “Просмотр любых данных” (код “CanSelectEverything”).

Подробнее: [Описание системных операций](#).

Для создания нового пользователя с правами системного администратора:

1. В разделе [*Контакты*] **добавьте контакт** для нового пользователя или убедитесь, что соответствующий контакт уже существует. Подробнее: [Добавить новый контакт](#).
2. В разделе [*Пользователи системы*] добавьте нового пользователя, указав контакт в профиле пользователя. Подробнее: [Добавить нового пользователя](#).
3. Включите пользователя в роль “Системные администраторы” (System administrators).

Важно. Доступ к этим операциям отменяет любые ограничения доступа на объекты, которые могут быть у пользователя. Например, если пользователь имеет доступ к операции “Просмотр любых данных”, то он сможет просматривать данные всех объектов, даже если доступ к операциям чтения в таких объектах был ограничен.

Существует несколько способов назначить пользователю роль системного администратора:

- Со страницы пользователя.
- Со страницы ролей.

Способ 1. Назначить роль системного администратора со страницы пользователя



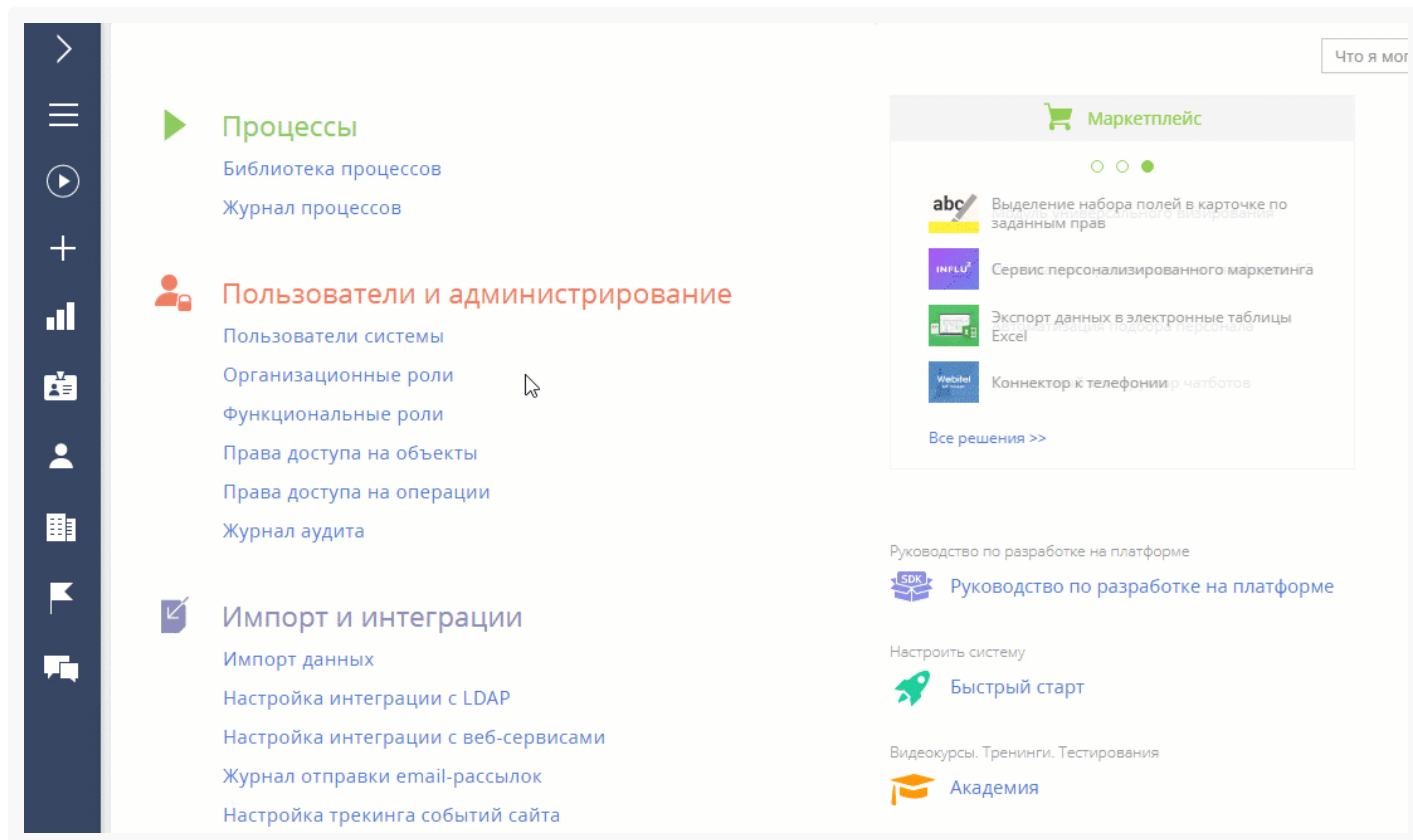
1. Нажмите  — > Дизайнер системы — > “Пользователи системы”.
2. Откройте страницу пользователя — > вкладка [*Роли*].
3. На детали [*Организационные роли*] нажмите  и укажите роль “Системные администраторы” (Рис. 1).

Рис. 1 — Назначение роли системного администратора со страницы пользователя



В результате пользователь будет добавлен с ролью системного администратора и получит полный доступ ко всем данным.

Способ 2. Включить пользователя в роль системного администратора с помощью раздела [Организационные роли]




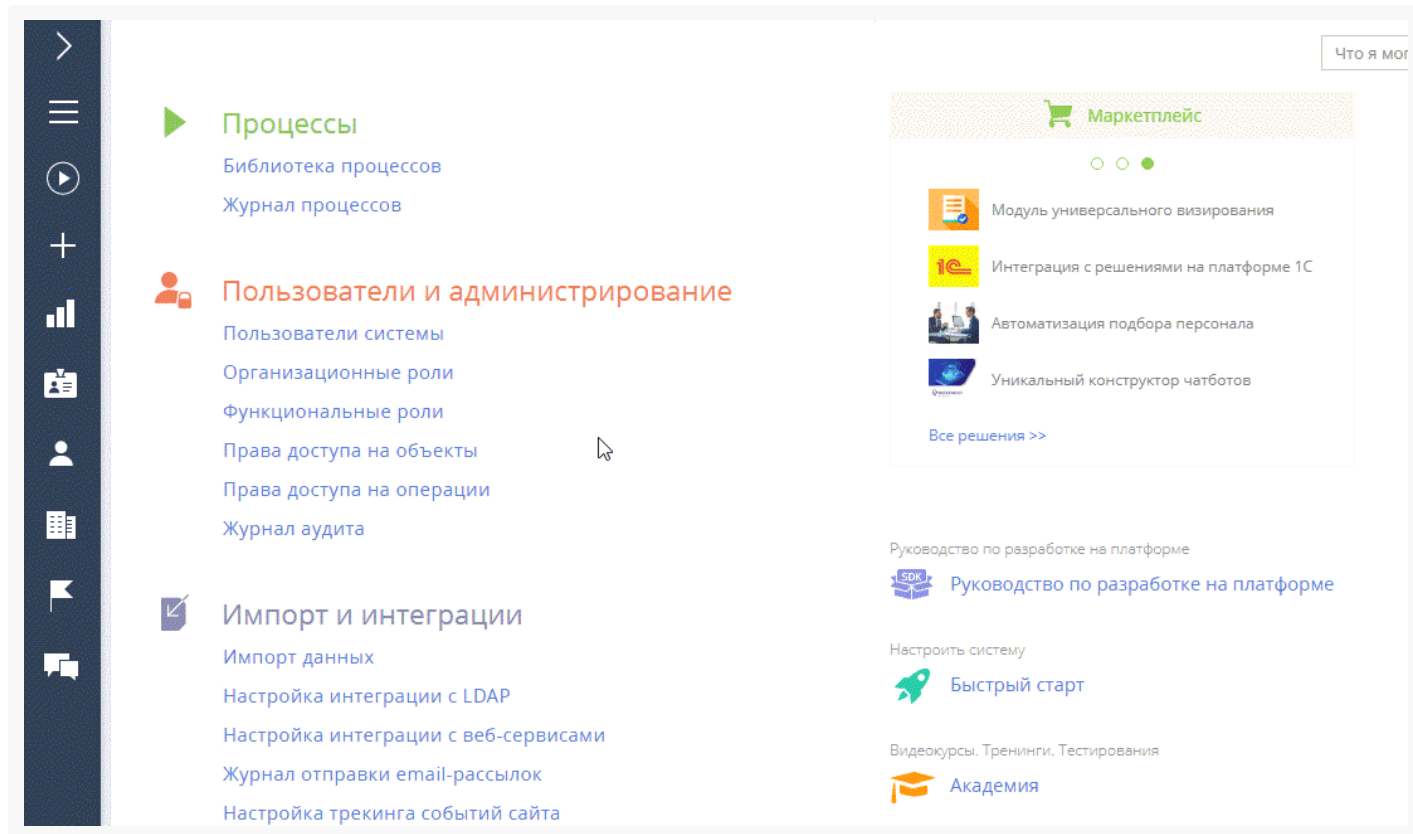
1. Нажмите  — > “Организационные роли”.
2. В списке организационных ролей, представленном в виде древовидной иерархической структуры, выберите роль “Системные администраторы”. Справа от списка ролей откроется страница выбранной роли.
3. На вкладке [*Пользователи*]:
 - a. **Если пользователь уже создан** в системе, то нажмите  и выберите [*Добавить существующего*]. Во всплывающем окне выберите соответствующего пользователя (Рис. 2).
 - b. **Если пользователь еще не создан** в системе, то нажмите  и выберите [*Добавить нового*]. После этого необходимо будет заполнить страницу нового пользователя.

Рис. 2 — Включение пользователя в роль системного администратора с помощью раздела [*Организационные роли*]



В результате пользователь будет добавлен с ролью системного администратора и получит полный доступ ко всем данным.

Добавить пользователя-сотрудника

Для создания нового пользователя:

1. В разделе [*Контакты*] **добавьте контакт** для нового пользователя или убедитесь, что соответствующий контакт уже существует. Подробнее: [Добавить новый контакт](#).
2. В разделе [*Пользователи системы*] **добавьте нового пользователя**, указав контакт в профиле пользователя. Подробнее: [Создать пользователя](#).
3. **Назначьте пользователю роль**, если это необходимо. Подробнее: [Назначить пользователю роли](#).
4. **Предоставьте пользователю лицензии**. Подробнее: [Предоставить лицензии пользователю](#).


Добавить новый контакт

1. Раздел [*Контакты*] — > [*Добавить контакт*].
2. Заполните страницу контакта и нажмите кнопку [*Сохранить*] (Рис. 3).

Рис. 3 — Добавление нового контакта

<div> <div>Контракты</div> <div> <div></div> <div></div> </div> <div> <div>ДОБАВИТЬ КОНТАКТ</div> <div>ДЕЙСТВИЯ</div> </div> </div>			
<div> <div>Фильтры/группы</div> <div>Тег</div> </div>			
ФИО	Контрагент	Должность	Email
Ткачевская Юлия Петровна	Омега-Тур	Директор	yulia.tkachevska@omega.com
Золотов Ярослав Викторович	Аксиома	Руководитель отдела	yaroslav.zolotov@gmail.com
Сладов Вадим Степанович	Призма плюс	Директор	v-slador@gmail.com
Шевченко Виталий	Our company	Руководитель отдела	v-shevchenko@gmail.com
Соколов Виталий Петрович	Бальвия-фарм	Руководитель отдела	vitaliy.sokolov@gmail.com
Омелин Виталий	Астра-оптимум	Маркетолог	vit.omelin@gmail.com
Ткаченко Виктория	Our company	Специалист	viktoriya_tkachenko@gmail.com
Петров Василий	Our company	Специалист	vas.petrov@yahoo.com
Жаврук Виталий	Астра-оптимум	Руководитель отдела	v.zhavruk@gmail.com
Уварова Ираида Олеговна	Лира	Специалист	UvarovalraidaOlegovna@gmail.com
Усилова Анастасия Павеловна	Камелия	Специалист	UsilovaAnastasiiaPavelovna@gmail.com
Умелов Михаил Петрович	Аксиома	Специалист	umelov@gmail.com
Турова Лилия Тимофеевна	Our company	Специалист	TurovaLilyiaTimofeevna@gmail.com
Трошин Виталий	ПК - Стайл	Разработчик	troshinv@pcstyle.com
Трощинский Владислав Викторович	Бальвия-фарм	Директор по продажам	TroshchinskiiVladislavVictorovich@gmail.com
Трофимова Ольга	Our company	Специалист	TrofimovaOlga@gmail.com
Тополь Анастасия Петровна	Софт-Плюс	Специалист	TopolAnastasiiaPetrovna@bigmir.net
Тюлепова Александра Романовна	Атриус	Специалист	TiulepovaAlexandraRomanovna@yahoo.com

В результате в системе будет создан новый контакт, для которого можно создать пользователя.

На заметку. Вы также можете пропустить этот шаг и создать контакт позже, непосредственно при добавлении нового пользователя. Заполняя поле [*Контакт*] на странице пользователя, нажмите , в открывшемся окне нажмите кнопку [*Добавить*] и заполните страницу контакта. После сохранения страницы вы вернетесь на страницу пользователя, где поле [*Контакт*] будет заполнено созданным контактом.

Создать пользователя


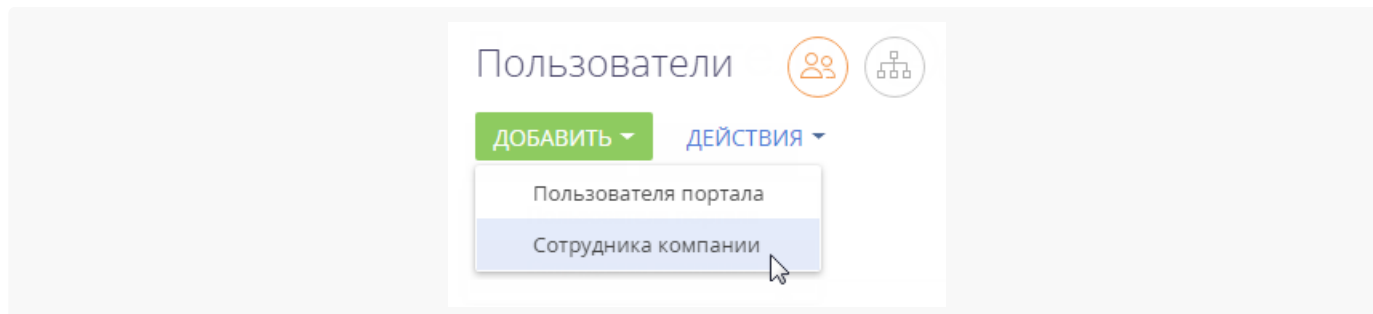
1. Нажмите  —> “Пользователи системы”.
2. Нажмите [*Добавить*] —> [*Сотрудника компании*] (Рис. 4).

Рис. 4 — Выбор типа пользователя



На заметку. После сохранения записи вы сможете изменить тип пользователя (“Сотрудник компании” или “Пользователь портала”), повторно открыв его страницу.

3. На открывшейся странице заполните следующие поля:

- a. [*Контакт*] — выберите пользователя из раздела [*Контакты*].
- b. [*Тип*] — система заполнит поле автоматически после выбора типа пользователя в предыдущем шаге. Возможные значения поля — “Сотрудник компании” или “Пользователь портала”.
- c. [*Активен*] — признак будет автоматически отмечен для активных пользователей. Чтобы деактивировать пользователя, снимите данный признак.
- d. [*Культура*] — поле отображает информацию о языке приложения для текущего пользователя. Значение поля указывается автоматически, изменить язык можно в профиле пользователя.

На заметку. Поле [*Культура*] показывает активные языки. Чтобы выбрать другие языки, сначала активируйте их в разделе [*Языки*] дизайнера системы. Подробнее: [Мультязычие](#).

- e. [*Домашняя страница*] — укажите страницу раздела, которая будет открываться автоматически при входе пользователя в систему. Если вы оставите поле незаполненным, то пользователь будет перенаправлен в главное меню, а при последующих входах — на последнюю открытую страницу во время предыдущего сеанса.
- f. [*Формат даты и времени*] — укажите формат, выбрав необходимый из выпадающего списка. Вы можете оставить поле незаполненным, и пользователь сможет указать эти данные позднее в своем профиле.

4. На детали [*Аутентификация*] заполните следующие поля:

- a. [*Имя пользователя*] — укажите логин пользователя, под которым он будет входить в систему. Поле является обязательным для заполнения.
- b. [*Email*] — укажите email-адрес пользователя, который он сможет использовать для входа в систему вместо логина. Если вы заполните это поле, то данный пользователь сможет войти в систему как по имени, так и по email-адресу.
- c. [*Пароль*], [*Подтверждение пароля*] — укажите пароль пользователя, с помощью которого он будет входить в систему. Поля являются обязательными для заполнения.
- d. Дата окончания действия пароля — не редактируемое поле, отображает дату истечения срока действия пароля. Дата определяется на основании поля [*Значение по умолчанию*] системной настройки “Срок действия пароля, дни” (код “MaxPasswordAge”). Значение поля системной настройки по умолчанию — “0”, в этом случае пароль действует бессрочно, поле [*Срок действия*

пароля] на странице пользователя остается пустым и заблокированным.

- е. [*Сбросить пароль*] — установите этот признак, если вы хотите, чтобы пользователь изменил свой пароль при входе в систему. Если признак установлен, то система уведомит пользователя о том, что срок действия пароля истек и запросит изменение пароля при следующей попытке входа.

На заметку. Если вы используете аутентификацию средствами LDAP, то установите признак [*Аутентификация средствами LDAP*] и в поле [*Имя пользователя*] укажите имя пользователя из справочника LDAP. Справочник этого поля содержит перечень пользователей LDAP, которые еще не синхронизированы с системой. Подробнее: [Настроить синхронизацию с LDAP](#).

5. Сохраните страницу.

В результате новый пользователь будет добавлен в Creatio.

Настроить доступ по записям

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Подробнее: [Настроить доступ по операциям](#).
- **По колонкам.** Подробнее: [Настроить права доступа на колонки](#).
- **По записям.** Настройка прав доступа на уровне чтения, редактирования и удаления **отдельных записей** выбранного объекта будет рассмотрена в данной статье.

Администратор системы может управлять правами на чтение, обновление или удаление **отдельных записей**, а также возможностями делегирования этих прав.

Распределение прав доступа по записям включается переключателем “Использовать доступ по записи” в разделе [*Права доступа на объекты*] дизайнера системы и зависит от авторства записи. Если автор записи входит в роль, которая указана в столбце “Автор записи”, то система раздает права роли-получателю, указанной в столбце “Получатель прав”. Если роль-получатель является подчиненной, то роль ее руководителей наследует все полученные права доступа.

По умолчанию максимальные права на управление записью имеют:

- **Системные администраторы**, которым дан доступ на системные операции “Добавление любых данных”, “Чтение любых данных”, “Изменение любых данных”, “Удаление любых данных”. Эти настройки имеют более высокий приоритет, чем настройки, заданные в разделе [*Права доступа на объекты*].
- **Автор записи и роль руководителей автора** с возможностью делегирования прав другим пользователям.
- **Ответственный за запись и роль руководителей ответственного** с возможностью делегирования прав другим пользователям.

Подробнее: [Настроить права доступа на запись](#).

На заметку. Если для объекта отключено администрирование прав доступа по записям, то записи будут доступны всем пользователям, у которых есть [доступ по операциям](#) в объекте.

Если администрирование по записям включено, но права доступа не настроены, то записи будут доступны только их автору, роли руководителей автора, ответственному по записи, роли руководителей ответственного, а также системным администраторам.

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты Creatio в онлайн-курсе [Управление пользователями и ролями. Права доступа](#).


Пример. Выполним настройку прав доступа для записей раздела [*Продажи*].

Если записи созданы менеджерами по продажам, то все сотрудники, входящие в эту роль, должны иметь возможность их просматривать (с делегированием), а также редактировать, но не иметь возможности удалять.

Если записи созданы руководителями менеджеров по продажам, то менеджеры должны иметь доступ на их чтение и редактирование, но без делегирования, а руководители должны иметь полный доступ с правом делегирования.

В нашем примере авторами записей и получателями прав будут сотрудники, входящие в роли “Менеджеры по продажам” и “Менеджеры по продажам. Группа руководителей”.

На заметку. Если для обеспечения отказоустойчивости в вашем приложении используется балансировщик нагрузки, то настройку необходимо выполнить на одном экземпляре приложения, после чего перенести на другие. Аналогичным образом выполняется установка приложений Marketplace, пакетов с пользовательской кастомизацией и другие настройки, требующие компиляции. Подробнее: [Установить приложение Marketplace на среду с балансировщиком](#).

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке “**Права доступа на объекты**”.
2. Например, чтобы настроить права доступа к разделу [*Продажи*], установите фильтр “Разделы” и выберите объект “Продажа”. Кликните по его заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Продажи*] (Рис. 1).

Подробнее: [Права доступа на объекты](#).

Рис. 1 — Выбор объекта раздела и переход на страницу настройки прав доступа

Права доступа на объекты Creatio

ЗАКРЫТЬ **ДЕЙСТВИЯ** ▾

■ Все объекты ▾ 🔍 Поиск

Заголовок	Название	Доступ по операциям ограничен	Доступ по записям ограничен	Доступ по колонкам ограничен
"Правило поиска дублей" в группе	DuplicatesRuleInFolder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
"Правило поиска дублей" в тегах	DuplicatesRuleInTag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(Устаревший)Раздел SSP	Portal_SysModule	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bulk email throttling queue	EmailThrottlingQueue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmail in campaign view	VwBulkEmailInCampaign	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailInProgress	BulkEmailInProgress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailQueue	BulkEmailQueue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailQueueOp	BulkEmailQueueOp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailRecipientMacro	BulkEmailRecipientMacro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CampaignParticipantInfo	CampaignParticipantInfo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CampaignParticipantOpInfo (операционная таблица)	CampaignParticipantOpInfo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по записям” (Рис. 2).

Рис. 2 — Включение администрирования по записям

Права доступа на объект Продажа Creatio

ЗАКРЫТЬ **ДЕЙСТВИЯ** ▾

Заголовок
Продажа

Название
Opportunity

Важно знать
Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

☐ Использовать доступ по операциям ⓘ

☒ **Использовать доступ по записям** ⓘ

Раздача прав в зависимости от автора записи ⓘ

Отсутствуют правила раздачи прав в зависимости от автора

[+ Добавить](#)

☐ Использовать доступ по колонкам ⓘ

4. По кнопке [*Добавить*] откроется окно, в котором необходимо указать пользователя или роль, на чьи записи будут раздаваться права доступа, а также пользователя или роль, которая получит эти права. Используйте строку поиска, чтобы быстро найти нужную роль или пользователя в списке. В нашем примере нужно добавить три записи (Рис. 3).

Рис. 3 — Пример добавления ролей для настройки прав доступа

Права доступа на объект Продажа

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок

Продажа

Название

Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

Использовать доступ по операциям ⓘ

Использовать доступ по записям ⓘ

Раздача прав в зависимости от автора записи ⓘ

Автор записи	Получатель прав	Чтение	Редактирование	Удаление
Менеджеры по продажам	Менеджеры по продажам			
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам			

+ Добавить

Использовать доступ по колонкам ⓘ

5. По умолчанию права доступа для получателей не установлены. Чтобы определить уровни доступа, для каждого из получателей в колонке, соответствующей праву (чтение, редактирование или удаление) нажмите кнопку ▾ и выберите “Разрешено” или “Разрешено с делегированием” . В нашем примере устанавливаются следующие права (Рис. 4):

Рис. 4 — Пример настройки прав доступа по записям

Использовать доступ по записям ⓘ


Раздача прав в зависимости от автора записи ⓘ

Автор записи	Получатель прав	Чтение	Редактирование	Удаление
Менеджеры по продажам	Менеджеры по продажам			
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам			
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам. Группа руководителей			

+ Добавить

- Чтобы сотрудники отдела продаж могли просматривать записи, созданные их коллегами, делегировать это право другим пользователям, вносить в записи изменения, но не могли их удалять, для роли “**Менеджеры по продажам**” установите признак “Разрешено с делегированием” в колонке [Чтение] и признак “Разрешено” в колонке [Редактирование].
- Чтобы сотрудники отдела продаж могли просматривать записи, созданные их руководителями, вносить в записи изменения, но не могли их удалять, для роли “**Менеджеры по продажам**”

установите признак “Разрешено”  в колонках [Чтение] и [Редактирование].

- с. Чтобы руководители менеджеров по продажам имели право на просмотр, изменение и удаление записей раздела [Продажи], созданных их коллегами, а также возможность делегировать эти права другим пользователям, установите признак “Разрешено с делегированием”  для роли **“Менеджеры по продажам. Группа руководителей”** в колонках [Чтение], [Редактирование] и [Удаление] для записей, авторы которых входят в роль “Менеджеры по продажам. Группа руководителей”.

На заметку. В отличие от прав доступа по операциям, для прав доступа по записям порядок добавления не влияет на приоритет.

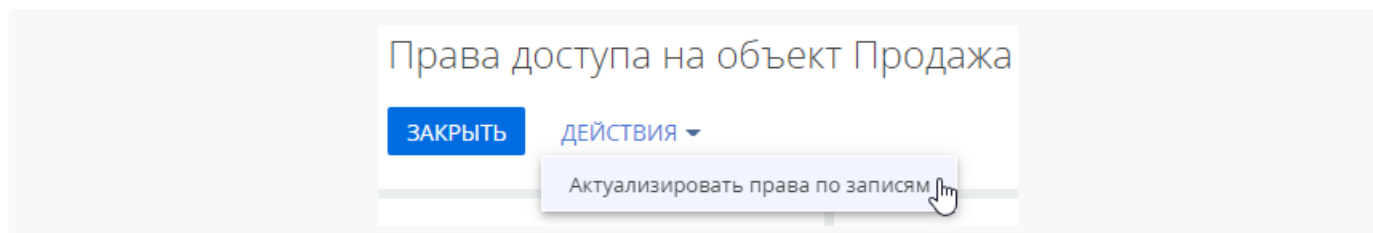
6. Чтобы сохранить настроенные права доступа, нажмите кнопку [Применить].

Важно. Если права доступа настроены в разделе, в котором уже есть записи, то необходимо выполнить актуализацию прав доступа. Иначе настроенные права доступа будут применяться только к новым записям раздела.

Актуализация прав доступа — это ресурсоемкая процедура. В зависимости от количества записей в разделе, а также ролей и пользователей, для которых она выполняется, актуализация может занять от 3 минут и более и повлиять на производительность системы. Чтобы этого избежать, рекомендуем выполнять актуализацию прав доступа во время наименьшей нагрузки на систему.

Чтобы применить новые права доступа к существующим записям раздела, откройте страницу настройки прав доступа к объекту и в меню [Действия] выберите пункт “Актуализировать права по записям” (Рис. 5).

Рис. 5 — Запуск актуализации прав по записям раздела



В результате актуализации прав записи будут удалены все права, установленные настройками по умолчанию, и созданы новые. Права, которые были [добавлены пользователем вручную](#) на странице настройки прав определенной записи или [настроены в рамках бизнес-процесса](#), при актуализации прав не удаляются.

На заметку. Для одной роли может существовать несколько записей прав. Например, это могут быть права, созданные в результате выполнения действия [Актуализировать права по записям] и полученные в ходе выполнения бизнес-процесса, или добавленные пользователем вручную и полученные в ходе выполнения бизнес-процесса.

Настроить доступ на экспорт данных

настроить доступ на экспорт данных

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Вы можете предоставить доступ ролям и отдельным пользователям на экспорт реестра как для отдельных объектов, так и для всех разделов системы.

Права на экспорт реестра являются разновидностью прав [доступа на объекты](#) приложения. Вы можете предоставить некоторым ролям и пользователям, например, руководству компании, неограниченный доступ на экспорт данных. Для этого необходимо предоставить им права на выполнение системной операции [системной операции](#) “Экспорт реестра” (код “CanExportGrid”). Для конфиденциальной и чувствительной информации рекомендуем настраивать права на экспорт для отдельных объектов. Например, предоставить руководителям финансового департамента право экспортировать счета.

Пример. Необходимо настроить для роли “Руководители финансового отдела” доступ к экспорту только реестра счетов.



1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Права доступа на объекты”.
3. В списке объектов системы найдите необходимый вам объект раздела, справочника или детали. Установите фильтр “Разделы” и выберите объект “Счет”.
4. Кликните по заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Счета*].
5. На открывшейся странице перейдите на вкладку [*Расширенные действия*].
6. Нажмите кнопку [*Добавить*] и в открывшемся окне укажите роль или пользователя, которым необходимо предоставить доступ к экспорту реестра.
 - a. В поле [*Роль/Пользователь*] нажмите , выберите нужную организационную, функциональную роль или пользователя, а затем подтвердите действие по кнопке [*Выбрать*].
 - b. В поле [*Выбрать операцию*] укажите “Export”.
 - c. Подтвердите действие по кнопке [*Добавить*].
7. При необходимости повторите шаг 6 для добавления прав на экспорт другим пользователям и ролям.
8. Для сохранения настроек нажмите кнопку [*Применить*] (Рис. 1).

Рис. 1 — Пример настройки прав на экспорт реестра

Права доступа на объект Счет

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок

Счет

Название

Invoice

Важно знать

Наличие у пользователя либо роли доступа на операции "Экспорт реестра" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

РАСШИРЕННЫЕ ДЕЙСТВИЯ

Дополнительные разрешения ⓘ

Роль/Пользователь	Операция ▴
Руководители финансового отдела	Export
+ Добавить	

В результате сотрудники, входящие в роль “Руководители финансового отдела”, смогут выполнять экспорт только реестра раздела [Счета]. Экспорт остальных реестров системы для них будет недоступен.

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="(&(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="(&(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="(&(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 порталных 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 порталные 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="(&(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 порталых пользователей в секции "SspLdapProvider":

```
<provider name="SSPLdapProvider" type="Terrasoft.WebApp.Loader.Authentication.SSPUserPassword"
<parameters>
  <add name="ServerPath" value="ldapsrvr.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>:

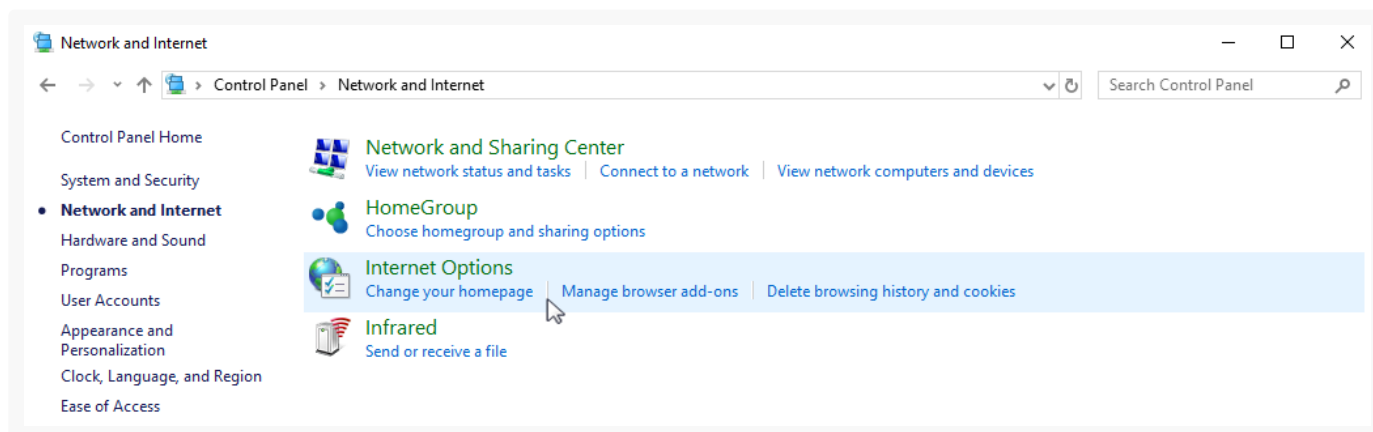
```
<appSettings> <add key="UsePathThroughAuthentication" value="true" /> ... </appSettings>
```

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:

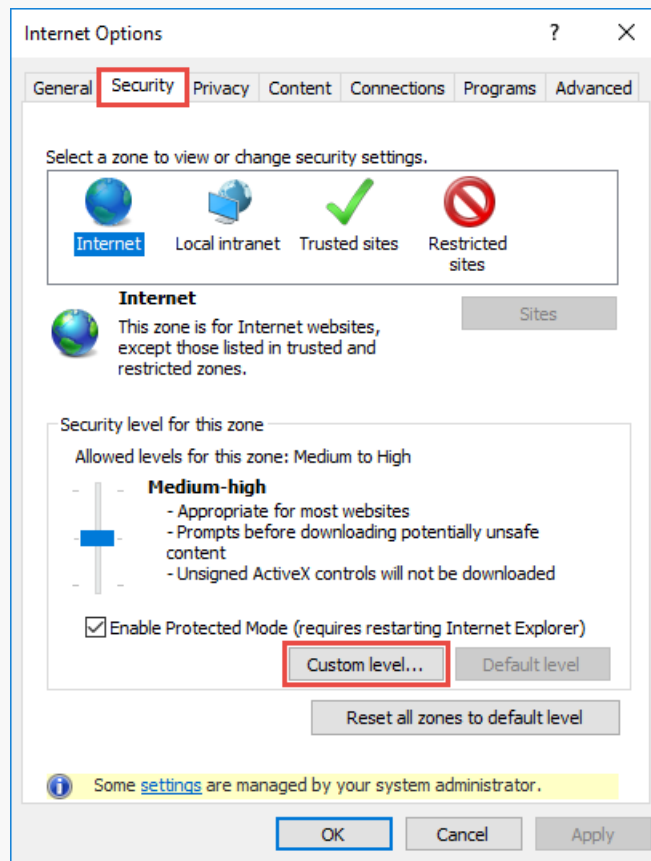
1. В меню “Пуск” (“Start”) → “Параметры” (“Settings”) → “Control Panel” (“Панель управления”) → “Сеть и Интернет” (“Network and Internet”) выберите пункт “Свойства обозревателя” (“Internet options”) (Рис. 1).

Рис. 1 — Настройка свойств обозревателя



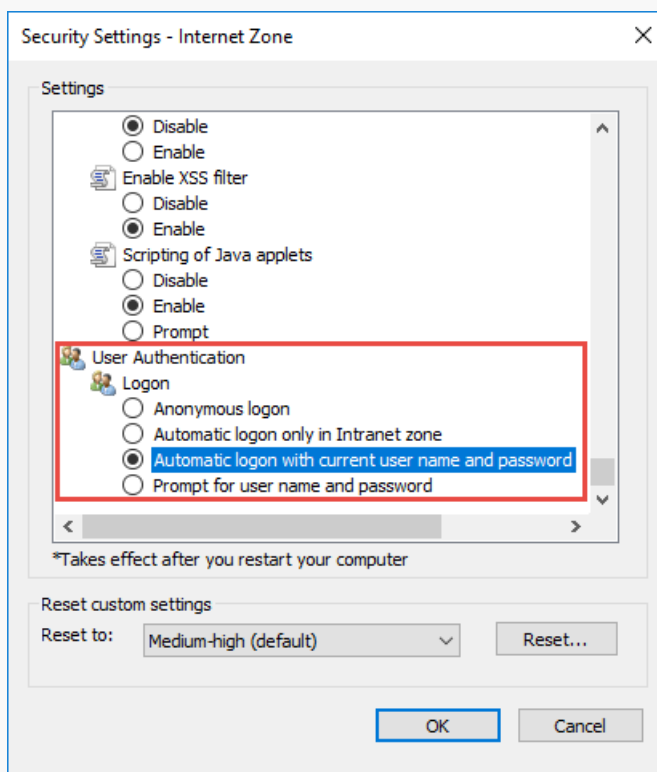
2. В открывшемся окне перейдите на вкладку “Безопасность” (“Security”) и по кнопке “Другой” (“Custom level”) перейдите к настройкам безопасности (Рис. 2).

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.

Аутентификация Windows

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Как работает аутентификация Windows

Аутентификации Windows (NTLM) и LDAP могут работать независимо друг от друга. Аутентификация Windows требует ввода учетных данных пользователя в окне авторизации браузера. А аутентификация LDAP использует проверку пароля пользователя на сервере Active Directory. Аутентификации Windows (NTLM) и LDAP работают вместе, когда пользователь нажимает ссылку “Войти под доменным пользователем”, и его аккаунт синхронизирован с LDAP.

На заметку. Аутентификация Windows доступна только для on-site приложений в связи с особенностями cloud-архитектуры.

При попытке пользователя войти в систему, используя доменные учетные данные, выполняется следующий алгоритм аутентификации:

1. Выполняется проверка авторизации пользователя в домене.
2. Имя и пароль текущего доменного пользователя считываются из cookie-файла, если эти данные записаны в cookie. В противном случае отображается браузерное окно ввода учетных данных.

Дальнейшие шаги зависят от того, синхронизирован ли пользователь с каталогом LDAP.

1. Если пользователь не синхронизирован с LDAP:

- Выполняется проверка подлинности пользователя путем сравнения логина и пароля, записанных в cookie-файл, с учетными данными соответствующей записи Creatio. Таким образом, для возможности Windows-аутентификации пользователя, не синхронизированного с LDAP, необходимо, чтобы при регистрации данного пользователя в Creatio были указаны те же логин и пароль, которые используются им в домене.
- Если по результатам проверки данные совпадают и учетная запись пользователя [лицензирована](#), осуществляется авторизация в приложении.
- Если пользователь синхронизирован с LDAP:
- Браузер посылает запрос в службу Active Directory для проверки подлинности пользователя.
- Запрос возвращает учетные данные текущего доменного пользователя, которые сравниваются с логином и паролем, записанными в cookie-файл.
- Если данные совпадают и учетная запись пользователя [лицензирована](#), то осуществляется авторизация в приложении.

На заметку. Проверка подлинности выполняется как среди пользователей основного приложения, так и среди пользователей портала самообслуживания. Порядок проверки настраивается в файле Web.config приложения-загрузчика. Подробнее: [Настроить файл Web.config приложения-загрузчика](#).

Для использования функциональности аутентификации Windows по протоколу NTLM необходимо зарегистрировать пользователей в системе вручную или импортировать из LDAP и предоставить им лицензии. Также необходимо, чтобы у пользователей в настройках браузера была разрешена запись локальных данных в cookie-файлы.

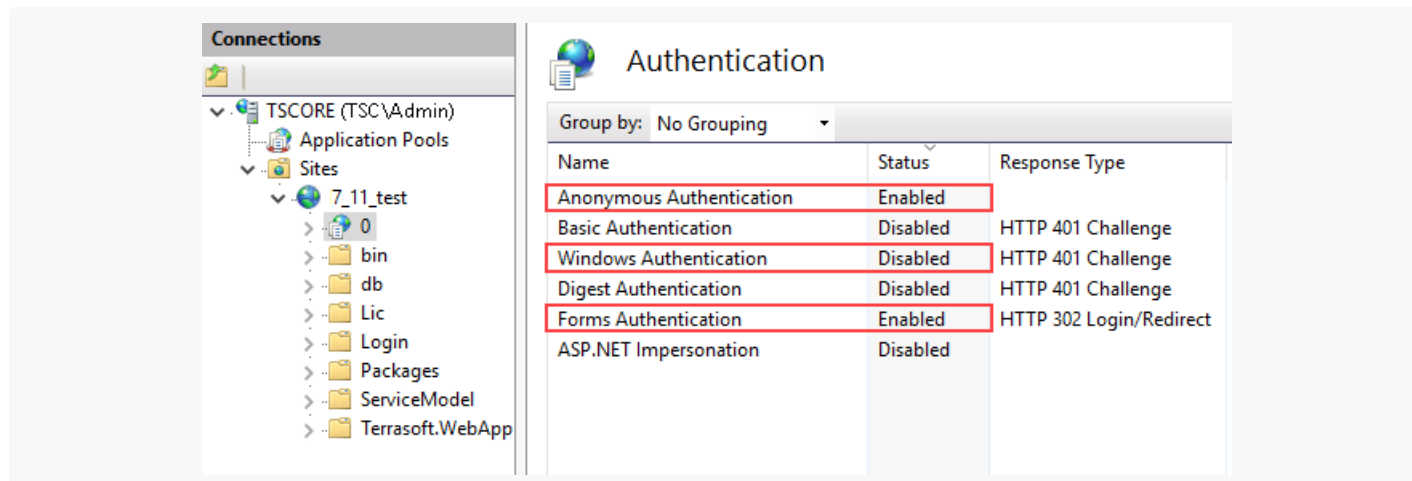
Настройка выполняется на сервере, где развернуто приложение, и включает в себя:

- Настройку сервера IIS, которая активирует аутентификацию по протоколу NTLM. Подробнее: [Настроить аутентификацию Windows в IIS](#).
- Настройку файла Web.config приложения-загрузчика, которая определяет провайдеров аутентификации и порядок проверки наличия пользователей среди зарегистрированных в Creatio. Подробнее: [Настроить файл Web.config приложения-загрузчика](#).

Настроить аутентификацию Windows в IIS

Для приложения-загрузчика и веб-приложения включите анонимную аутентификацию и аутентификацию форм (Рис. 1).

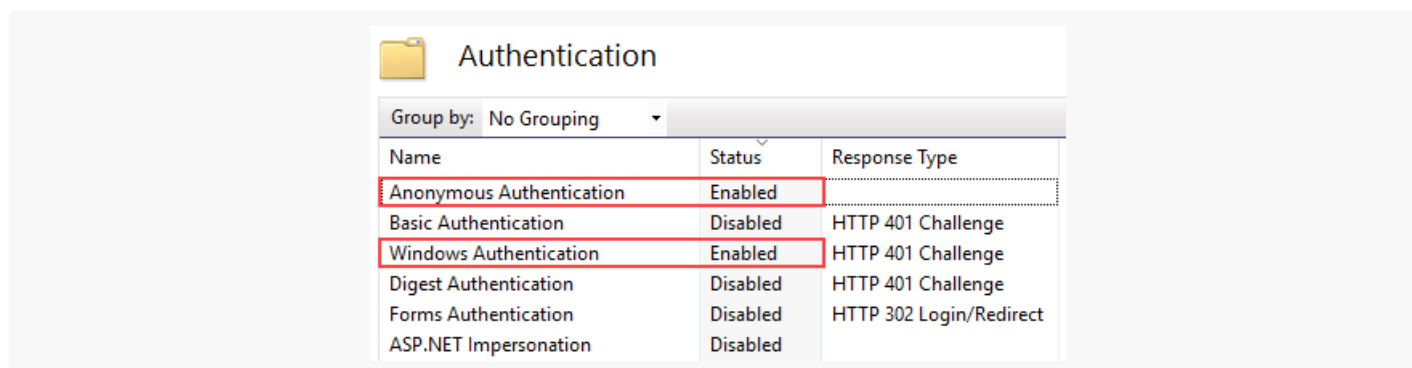
Рис. 1 — Настройки для приложения-загрузчика в настройках IIS



На заметку. Обратите внимание, что необходимо выключить настройку “Windows Authentication”, которая в IIS включена по умолчанию.

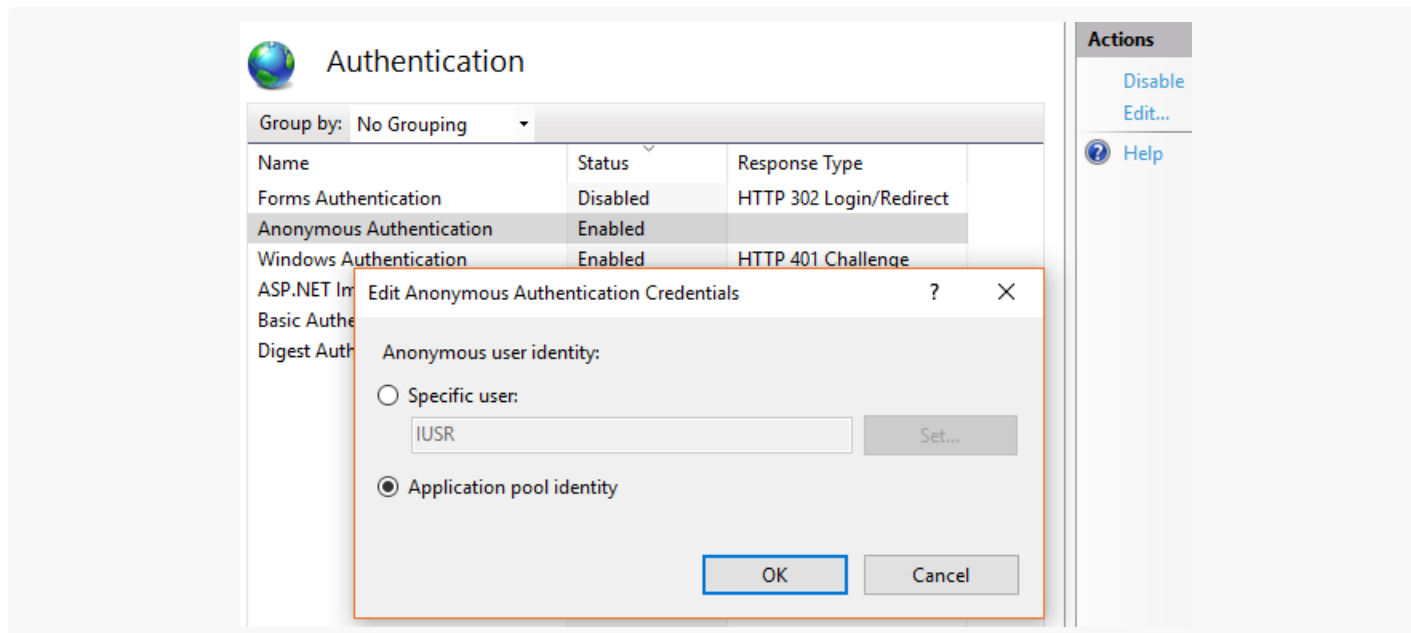
Для директории Login внутри приложения-загрузчика отключите аутентификацию форм и включите анонимную аутентификацию и аутентификацию Windows (Рис. 2).

Рис. 2 — Настройки для директории Login



Обратите внимание, что анонимная аутентификация приложения-загрузчика и рабочих приложений должна выполняться под пользователем Application Pool Identity. Для этого перейдите в окно редактирования данных входа настроек Authentication по кнопке [*Edit*] в боковом меню [*Actions*] менеджера IIS, и выберите пользователя “Application Pool Identity” (Рис. 3).

Рис. 3 — Указание пользователя для анонимной аутентификации в настройках IIS



На заметку. Подробнее о настройке аутентификации Windows читайте в [справочной документации Microsoft](#).

Настроить файл Web.config приложения-загрузчика

[*InternalUserPassword*] — провайдер, указанный в файле Web.config по умолчанию. Если вы хотите предоставить возможность аутентификации по NTLM-протоколу только пользователям, которые не синхронизированы с LDAP, 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*].

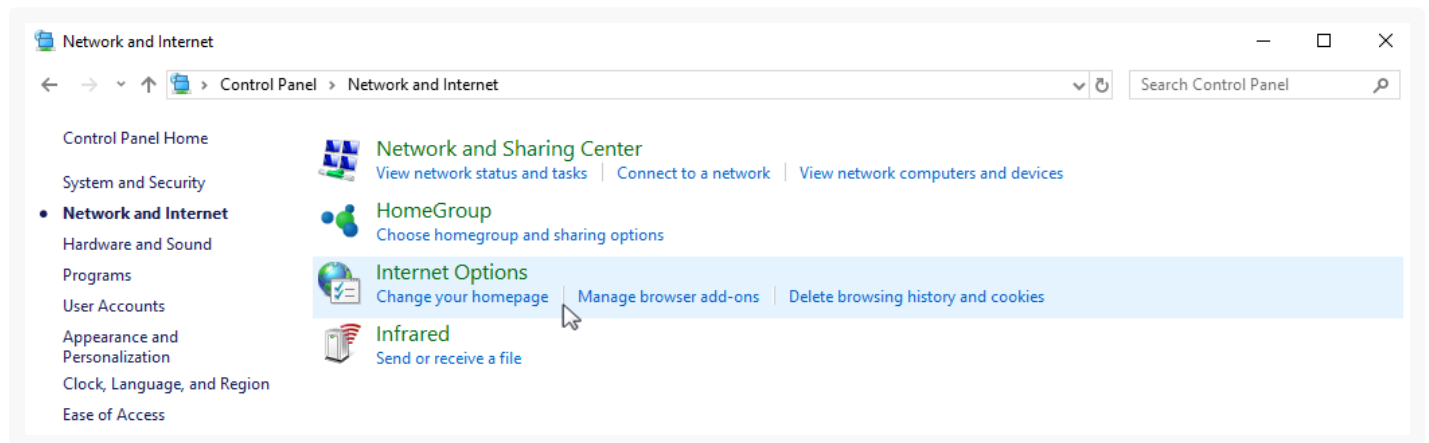
Для отображения страницы входа в систему с доступной ссылкой [*Войти под доменным пользователем*] укажите значение “false” для параметра [*UsePathThroughAuthentication*]. При этом сквозная аутентификация будет выполняться лишь при переходе на главную страницу приложения. Чтобы отобразить страницу входа,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

В меню “Start” → “Settings” → “Control Panel” → “Network and Internet” выберите пункт “Internet options” (Рис. 4).

Рис. 4 — Настройка свойств обозревателя



1. Откройте для редактирования файл Web.config приложения-загрузчика.
2. Укажите в файле провайдеры аутентификации Windows:

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

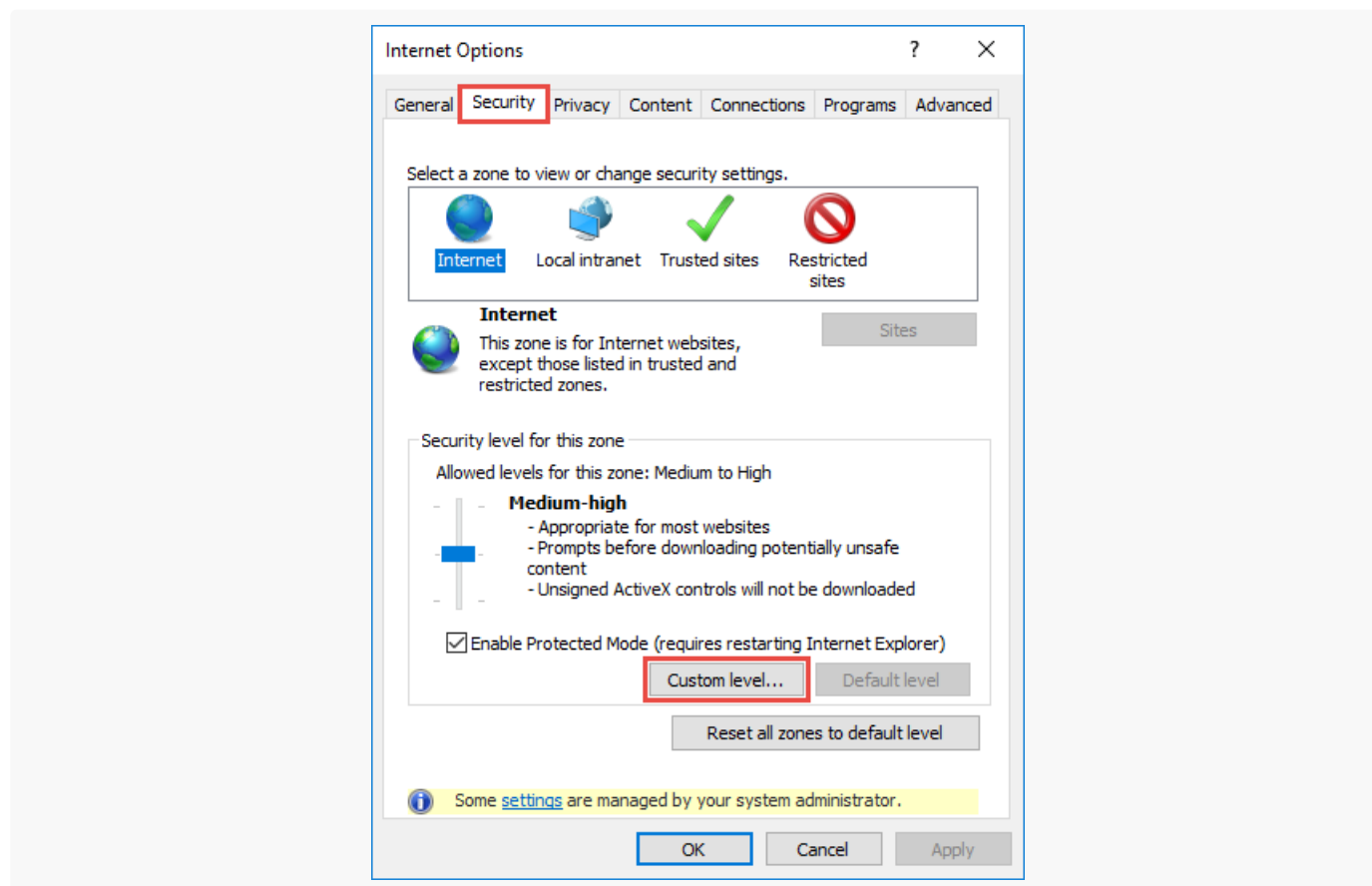
3. Если вы хотите активировать сквозную аутентификацию, чтобы пользователь имел возможность авторизоваться в Creatio, минуя страницу входа, укажите значение “true” для параметра [*UsePathThroughAuthentication*] элемента <appSettings>:

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

4. В открывшемся окне перейдите на вкладку “Security” и по кнопке “Custom level” перейдите к

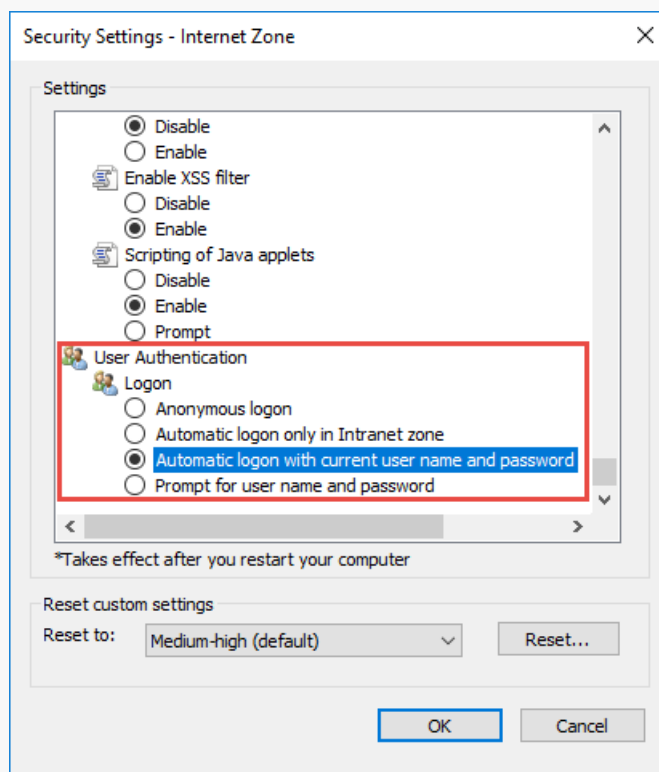
настройкам безопасности (Рис. 5).

Рис. 5 — Настройки безопасности



5. В группе настроек “User Authentication” выберите способ авторизации “Automatic logon with current user name and password” (Рис. 6).

Рис. 6 — Выбор способа авторизации



6. Нажмите “OK”.

В результате пользователи, которые уже прошли аутентификацию в домене, смогут войти в Creatio по ссылке “Войти как доменный пользователь”, и им не придется повторно вводить учетные данные домена каждый раз для получения доступа к Creatio.

Изменить системного пользователя (Supervisor)

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для корректной работы системы обязательным условием является наличие пользователя, который используется для выполнения системных операций. Системный пользователь — это пользователь, который:

- имеет максимум прав;
- имеет полный пакет лицензий;
- указан в системной настройке “**Пользователь для выполнения системных операций**”.

По умолчанию в системе таким пользователем является Supervisor.

На заметку. Если у вас в системе нет пользователя с именем Supervisor, то убедитесь, что у пользователя, указанного в системной настройке “Пользователь для выполнения системных операций” есть полный пакет лицензий и максимальные права.

В отличие от системных администраторов, системный пользователь может быть только один.

Важно. Вы можете переименовывать или переназначить системного пользователя, но его нельзя удалять, а также лишать прав и лицензий — это приведет к сбоям в работе системы.

Системный пользователь необходим не только для администрирования и настройки системы, но также для обеспечения корректности работы системных операций. Например, от имени системного пользователя выполняются индексация данных для глобального поиска, сохранение изменений в мастере разделов и мастере деталей, отправки рассылок. Если системный пользователь был удален или лишен прав и лицензий, то в функциональности Creatio могут возникнуть сбои. Для смены системного пользователя:

1. Передайте **максимальный пакет лицензий** от текущего системного пользователя будущему.
2. Укажите для будущего системного пользователя роль, которой в системе розданы **максимальные права**, например, “Системные администраторы”.
3. Укажите в системной настройке “**Пользователь для выполнения системных операций**” нового пользователя.

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=TRL
```

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](#).

Импортировать пользователей из Excel

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Вы можете быстро добавить пользователей в Creatio, просто импортировав их из файла Excel. Подробнее: [Импорт данных из Excel](#).

При импорте вам необходимо указать объект под названием “Объект администрирования”, который соответствует таблице базы данных “SysAdminUnit”. В этом объекте содержится организационная структура компании: пользователи, организационные и функциональные роли.

Чтобы импортировать пользователей из Excel:

1. **Подготовьте файл для импорта**, заполнив все обязательные колонки. Подробнее: [Подготовить документ Excel для импорта пользователей](#).
2. Загрузите файл и **импортируйте пользователей** в систему. Подробнее: [Запустить импорт](#).
3. **Настройте пользователей**: назначьте роли, укажите пароли и доступные лицензии. Подробнее: [Настроить пароль, роль и выдать лицензии](#).

Подготовить документ Excel для импорта пользователей

Создайте документ в формате *.xlsx. В файле обязательно должны быть колонки “Название” и “Тип”, в которых указаны логины и тип. Остальные колонки опциональны для заполнения.

Название колонки	Значение колонки в файле Excel
Название	<p>Логин пользователя, под которым он будет входить в систему.</p> <p>Колонка обязательна для заполнения.</p>
Тип	<p>Укажите “4” для того, чтобы импортировать записи как пользователей.</p> <p>Колонка определяет тип импортируемой административной единицы — роли или пользователи. Различные типы административных единиц системы хранятся в объекте “Тип объекта администрирования” (SysAdminUnitType). Ниже вы найдете возможные значения этой таблицы.</p> <p>Колонка обязательна для заполнения.</p>
Контакт	<p>ФИО контакта пользователя. ФИО в колонке “Контакт” в файле Excel должны полностью соответствовать ФИО этих контактов в системе, иначе при импорте система создаст новый контакт.</p> <p>Колонка не обязательна для заполнения. Если колонка не заполнена, то система создаст новые контакты, используя логин пользователя (колонка “Имя”) как ФИО контакта.</p>
Активен	<p>Возможные варианты:</p> <ul style="list-style-type: none"> • “0” — для деактивированных пользователей. • “1” — для активных пользователей. <p>Колонка не обязательна для заполнения. По умолчанию все пользователи активны.</p>
Культура	<p>Код языка (например, “ru-RU” для русского языка приложения). Подробнее: Мультиязычие.</p> <p>Колонка не обязательна для заполнения. По умолчанию используется русский язык.</p>
Тип пользователя	<p>Тип пользователя определяет базовый набор прав доступа, которые он получит (пользователь портала или сотрудник компании).</p> <ul style="list-style-type: none"> • “0” — для сотрудников компании. • “1” — для пользователей портала. <p>Колонка не обязательна для заполнения. По умолчанию все пользователи импортируются как сотрудники компании.</p>

Значения для объекта “Тип объекта администрирования” (SysAdminUnitType) приведены в таблице ниже.

Тип административной единицы	Значение в колонке “Тип”	Значение в колонке “Тип соединения”
Организация	0	0
Подразделение	1	0
Руководитель	2	0
Пользователь	4	0
Пользователь портала	4	1
Функциональная роль	6	0

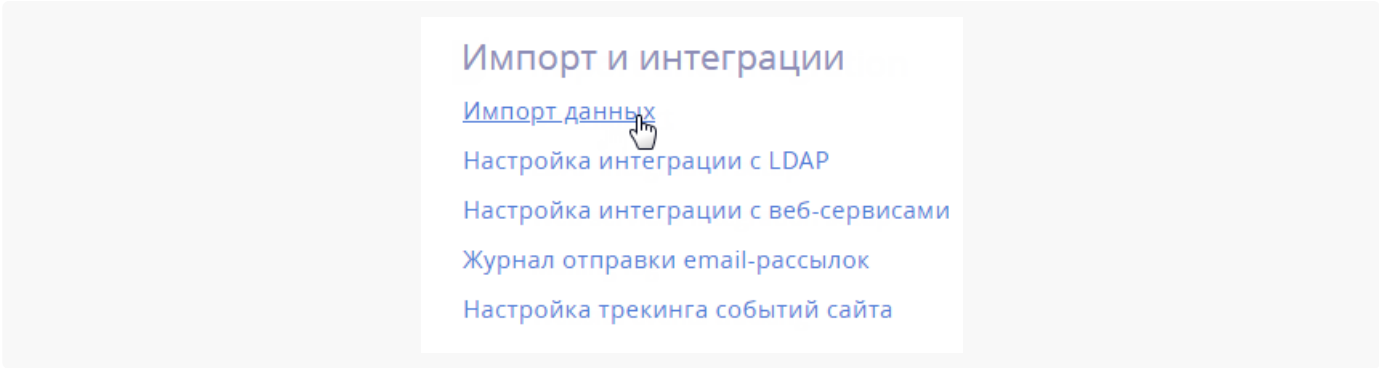
Подробнее: [Подготовить файл импорта.](#)

Запустить импорт

Чтобы импортировать пользователей из Excel:

- 1. Нажмите  —> “Импорт данных” (Рис. 1).

Рис. 1 — Переход к функциональности [Импорт данных]




- 2. **Добавьте ваш файл Excel для импорта:** перетащите его на открывшуюся страницу “Загрузка данных” или нажмите [*Выбрать файл*] и укажите его на вашем компьютере.
- 3. Нажмите [*Другое*] и выберите “**Объект администрирования**” как объект, куда будут загружены данные (Рис. 2). Нажмите [*Далее*].

Рис. 2 — Выбор объекта для импорта

Загрузка данных: Загрузка файла


ЗАКРЫТЬ НАЗАД ДАЛЕЕ

Вы выбрали файл




importing_users.xlsx X

Куда вы хотите загрузить данные?



КОНТАКТ



КОНТРАГЕНТ

ОБЪЕКТ
АДМИНИСТРИРОВАНИЯ

ДАЛЕЕ


4. Укажите **соответствия колонок** файла Excel с колонками (полями) выбранного объекта Creatio (Рис. 3). Нажмите [*Далее*].

Рис. 3 — Соответствие колонок

Загрузка данных: Настройка колонок

ЗАКРЫТЬ НАЗАД ДАЛЕЕ

Укажите соответствие колонок в файле Excel



Excel

Название	✓	Название
Тип	✓	Тип
Контакт	✓	Контакт
Активен	✓	Активен
Культура	✓	Культура

ДАЛЕЕ

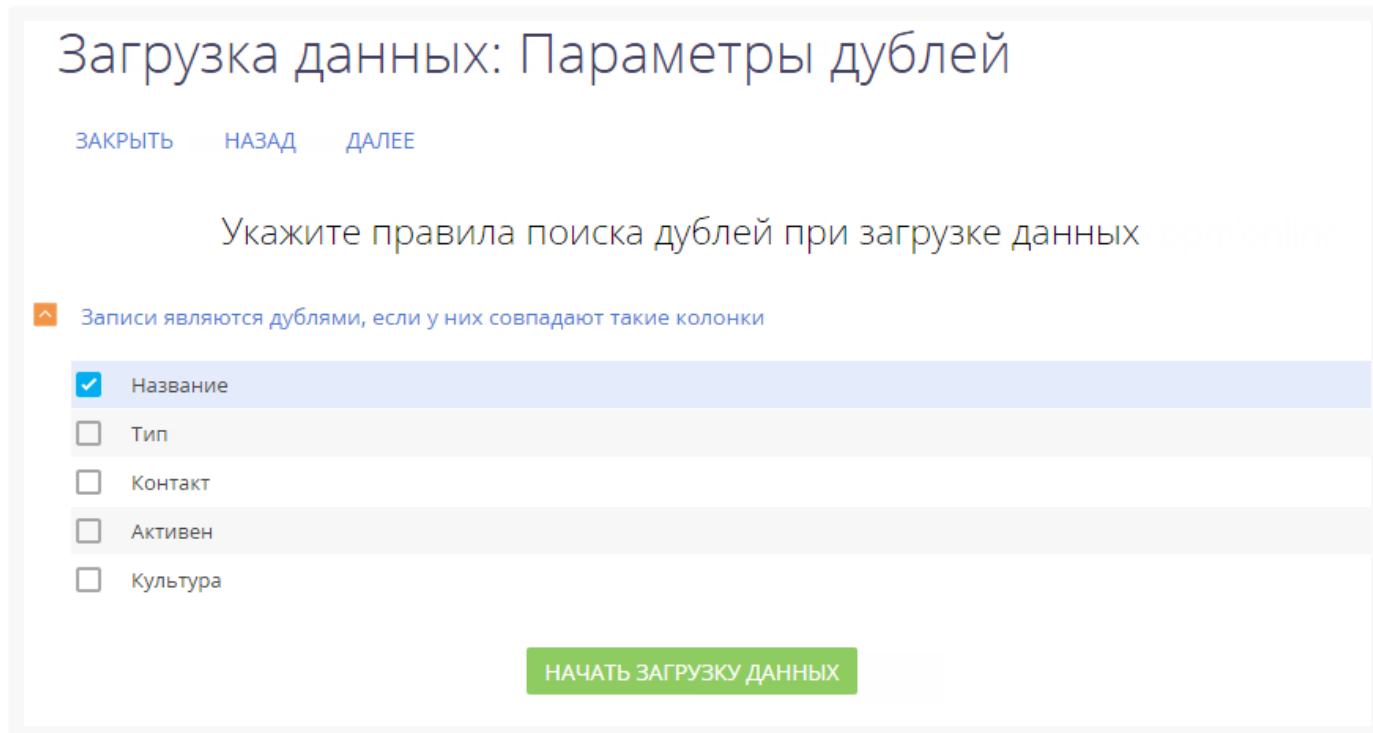
5. Укажите условия, по которым будет выполняться поиск дублей записей. Данные этих колонок должны быть уникальны для каждой импортируемой записи (Рис. 4).

Если при проверке в системе будет найдена запись, у которой значения в выбранных колонках

совпадут со значениями в файле импорта, то эта запись будет обновлена. Если соответствия не найдется, то в систему будет добавлена новая запись.

Например, при выборе колонки “Название” если пользователь с таким именем есть в базе данных, то система обновит существующую запись. Если такого имени нет, то будет создана новая запись.

Рис. 4 — Правила поиска дублей при загрузке данных



6. Нажмите кнопку [*Начать загрузку данных*].

На заметку. Процесс настройки колонок и правил поиска дублей подробнее описан в статье [Выполнить импорт клиентской базы](#).

По завершении импорта вы получите сообщение в центре уведомлений.

В результате записи отобразятся в реестре пользователей системы. Обратите внимание, что у этих пользователей не настроены роли, лицензии и пароли. Эти данные нужно заполнить вручную.

Настроить пароль, роль и выдать лицензии

По завершении импорта нужно вручную выполнить следующие действия для каждого проимпортированного пользователя:

1. **Установите пароль** для входа пользователя в систему на вкладке [*Основная информация*].

На заметку. Пользователи смогут изменить пароли при первом входе в систему. Подробнее: [Создать пользователя](#).

2. **Выберите роль** (например, “Все сотрудники”) на вкладке [*Роли*]. Подробнее: [Назначить](#)

[пользователю роли.](#)

3. Раздайте лицензии на вкладке [*Лицензии*]. Подробнее: [Предоставить лицензии пользователю.](#)

Настроить права доступа на системные операции

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

В этой статье рассмотрена настройка прав **доступа к действиям системы**. Примеры таких действий: импорт и экспорт данных, создание бизнес-процессов, настройка рабочих мест, изменение содержимого справочников, конфигурирование системы и т. д.

Действия системы не относятся к конкретному объекту и права на них не могут настраиваться на уровне операций чтения, редактирования и удаления данных в объекте. Для настройки прав доступа к действиям системы используются **системные операции**. Они имеют два уровня доступа: у пользователя либо роли есть право на выполнение системной операции, или его нет. Например, если вы разрешите роли “Все сотрудники компании” выполнять операцию “Экспорт реестра” (код “Export list records”), то все без исключения пользователи смогут экспортировать данные реестра раздела в Excel.

Управление доступом к системным операциям доступно в дизайнера системы, по ссылке **“Права доступа на операции”**. Работа с группами в реестре системных операций не предусмотрена, но вы можете воспользоваться [стандартным](#) или [расширенным](#) фильтром.


Доступ к бизнес-данным подразумевает выполнение CRUD-операций с данными (создание, чтение, редактирование и удаление) и выполняется через настройку прав доступа к соответствующим объектам системы. Подробнее читайте в статье [Настроить доступ по операциям](#).

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты в Creatio в онлайн-курсе [Управление пользователями и ролями. Права доступа](#).

Обратите внимание, что право на выполнение системной операции не отменяет других прав доступа. Например, пользователи смогут экспортировать только те данные, к которым у них есть доступ.

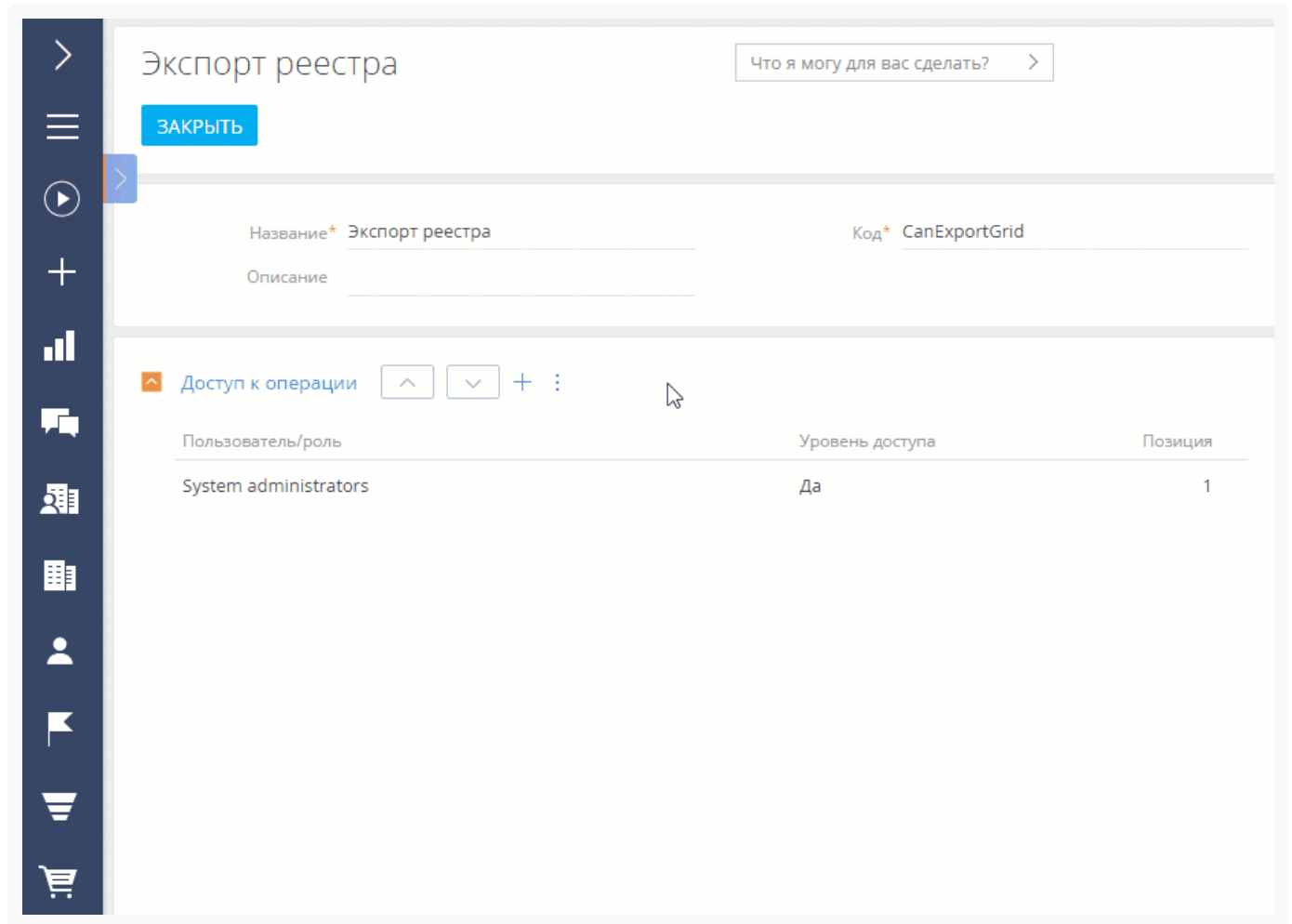
По умолчанию доступ к основным системным операциям есть только у администраторов системы. Вы можете настроить права доступа к системным операциям для определенных пользователей или групп пользователей.

Пример. Дать доступ на экспорт реестра для руководителей менеджеров по продажам.

1. Нажмите  —> Дизайнер системы —> **“Права доступа на операции”**.
2. Установите фильтр “Название = Экспорт реестра” (или “Код = CanExportGrid”). **Кликните по заголовку** системной операции или выделите ее в реестре и нажмите кнопку [*Открыть*].
3. На детали [*Доступ к операции*] нажмите кнопку **+** —> **укажите получателя прав**. В нашем примере это роль “Менеджеры по продажам. Группа руководителей”. Запись появится на детали со значением “Да” в колонке “Уровень доступа”. В результате пользователи, входящие в роль “Менеджеры по продажам. Группа руководителей” получают доступ к системной операции [*Экспорт*

реестра] ([Рис. 1](#)).

Рис. 1 — Добавление прав доступа на системную операцию



На заметку. Чтобы запретить доступ, установите в колонке [*Уровень доступа*] значение “Нет”. Для этого выберите пользователя или роль в списке. Значение в колонке “Уровень доступа” отобразится в виде признака. Снимите признак, чтобы запретить доступ для выбранного пользователя или роли. Сохраните запись.

Когда вы настраиваете ограничения на доступ к системной операции для определенных пользователей или ролей, возможны случаи, что уровни доступа противоречат друг другу, т. к. роли пересекаются. Настройте приоритетность прав доступа на операцию, чтобы для всех ролей они обрабатывали корректно. Для этого воспользуйтесь кнопками и на детали [*Доступ к операции*]. Если пользователь будет входить в несколько ролей, добавленных на деталь, то для него будут применен уровень доступа той роли, которая расположена выше в списке. Например, если вы хотели бы запретить всем пользователям, кроме руководителей менеджеров по продажам, экспорт реестра, расположите роль “Все сотрудники компании” ниже, а роль “Менеджеры по продажам. Группа руководителей” — выше.

На заметку. Пользователи или роли, которые не добавлены на деталь, не получают права доступа

к операции. При этом они не участвуют в определении приоритетов прав.

Назначить пользователю роли

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Роли — это группы пользователей в системе. Вы можете назначить пользователям организационные и функциональные роли. Более подробную информацию об этом вы найдете в модульном курсе [Управление пользователями и ролями. Права доступа](#).

Назначенные роли дают пользователю доступ к соответствующим [объектам](#) данных и системным операциям. Вы можете назначить пользователю одну или несколько ролей.

НА ЗАМЕТКУ. По умолчанию новым пользователям с типом “Сотрудник компании” назначается организационная роль “Все сотрудники” (All employees).

Существует несколько способов назначить пользователю роль:

- Со страницы пользователя.
- Со страницы ролей.

Способ 1. Назначить роли со страницы пользователя


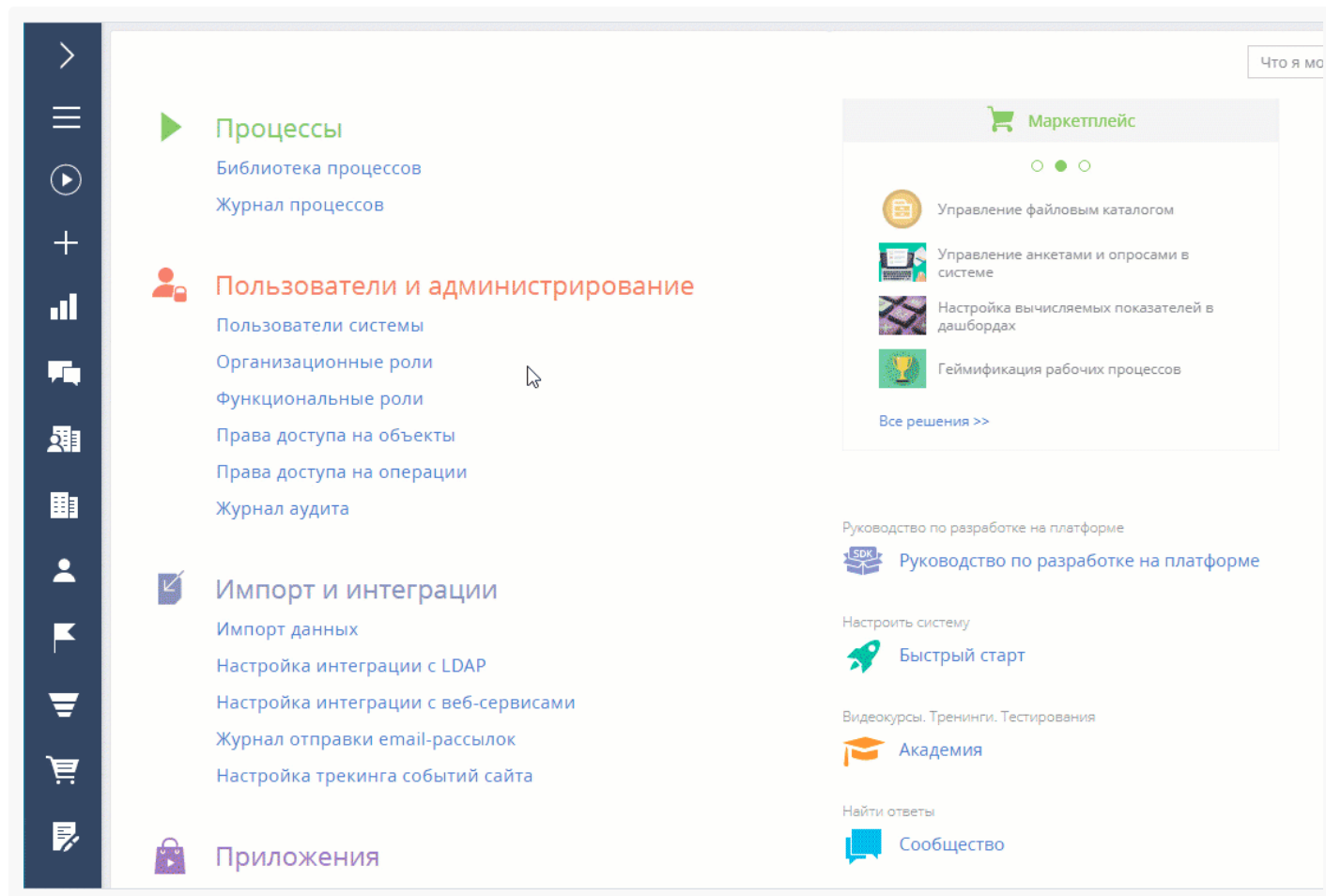
1. Нажмите  —> Дизайнер системы —> “**Пользователи системы**”.
2. Откройте страницу пользователя —> вкладка [**Роли**].
3. На детали [**Организационные роли**] нажмите + и выберите роли из организационной структуры компании.
4. На детали [**Функциональные роли**] нажмите + и укажите функциональную роль пользователя. Функциональные роли обычно базируются на должности пользователя ([Рис. 1](#)).

Рис. 1— Назначение ролей со страницы пользователя



В результате пользователь получит все права доступа, которые дают назначенные роли.

Способ 2. Назначить роли со страницы ролей



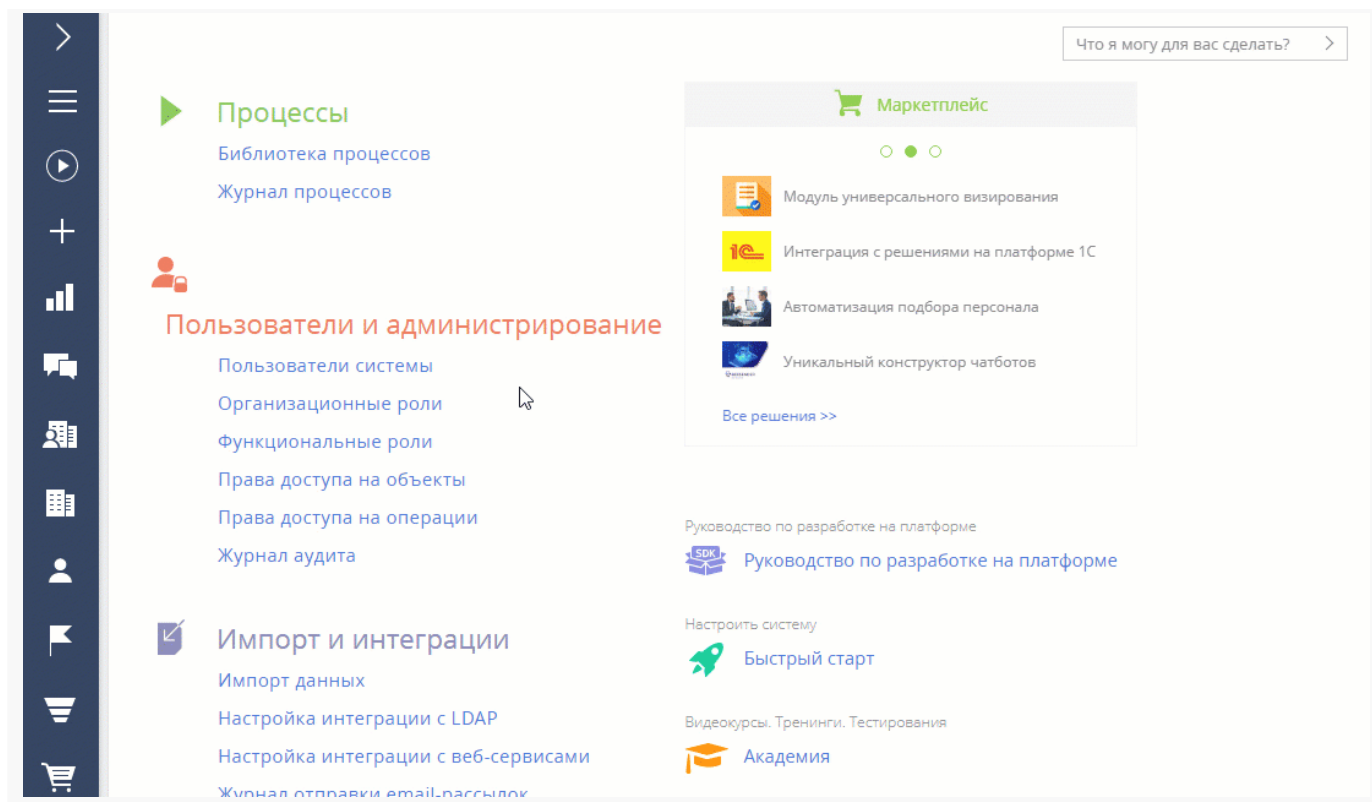
1. Нажмите  —> **“Организационные роли”**.
2. В древовидной структуре ролей **выберите роль**, для которой нужно добавить пользователей. Справа откроется страница выбранной роли.
3. На вкладке [**Пользователи**]:
 - a. **Если пользователь уже создан** в системе, то нажмите **+** и выберите [**Добавить существующего**]. Выберите соответствующего пользователя ([Рис. 2](#)).
 - b. **Если пользователь еще не создан** в системе, то нажмите **+** и выберите [**Добавить нового**]. Заполните страницу нового пользователя.
4. Чтобы назначить пользователю функциональную роль, переключитесь на представление [**Функциональные роли**], нажав , затем **выберите соответствующую функциональную роль**.
5. Повторите шаг 3 ([Рис. 2](#)).

Рис. 2 — Назначение ролей через страницы соответствующих ролей



В результате пользователю будут назначены выбранные роли и предоставлены соответствующие права.

Описание системных операций

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Ниже представлено описание системных операций, доступом к которым вы можете управлять.

Управление пользователями и ролями

Системная операция	Описание
Управление списком пользователей Код "CanManageUsers"	Право добавлять, изменять и удалять учетные записи пользователей в разделах управления ролями и пользователями дизайнера системы.
Управление лицензиями пользователей Код "CanManageLicUsers"	Право доступа к разделу [Менеджер лицензий]. Пользователи, обладающие этим правом, могут войти в систему и перераспределить лицензии даже в случае блокировки системы в связи с превышением количества лицензий.
Изменение делегируемых прав Код "CanChangeAdminUnitGrantedRight"	Возможность делегировать права доступа одним пользователям другим при помощи детали [Делегирование прав доступа] на странице пользователя.

Управление пользователями портала

Системная операция	Описание
Возможность управлять пользователями портала Код "CanAdministratePortalUsers"	Право добавлять, изменять и удалять учетные записи пользователей портала в разделах управления ролями и пользователями дизайнера системы.
Доступ к модулю настройки главной страницы портала Код "CanManagePortalMainPage"	Право настраивать главную страницу портала .

Общий доступ к данным

Операции общего доступа к данным относятся ко всем записям во всех объектах. Как правило, общий доступ к данным предоставляется **администратору системы**.

Важно. Действие прав доступа, предоставленных данными операциями, не может быть ограничено никакими специфическими правами доступа к записям, операциям либо колонкам объектов: если такие ограничения существуют, то они не будут приниматься во внимание. Например, если пользователь имеет доступ к операции [*Просмотр любых данных*], то он сможет просматривать данные всех объектов, даже если доступ к операциям чтения в таких объектах ограничен.

Системная операция	Описание
Просмотр любых данных Код "CanSelectEverything"	Право просматривать все записи во всех объектах.
Добавление любых данных Код "CanInsertEverything"	Право добавлять записи в любые объекты системы.
Изменение любых данных Код "CanUpdateEverything"	Право редактировать любые записи во всех объектах системы.
Удаление любых данных Код "CanDeleteEverything"	Возможность удалять любые записи из любых объектов системы.

Доступ к колонкам, системным операциям

Системная операция	Описание
Изменение прав на системные операции Код "CanChangeAdminOperationGrantee"	Право предоставления доступа к системным операциям . Данная операция также включает в себя право регистрации дополнительных системных операций.

Доступ к особым разделам системы

Системная операция	Описание
Доступ к рабочему месту “Администрирование” Код “CanManageAdministration”	Право доступа к разделам [Права доступа на объекты] и [Права доступа на операции]. Требуется для управления записями sysAdminUnit. Доступ к конкретным операциям администрирования должен быть предоставлен отдельно.
Доступ к разделу “Дизайн процессов” Код “CanManageProcessDesign”	Право доступа к дизайнеру процессов , а также возможность добавлять и редактировать бизнес-процессы.
Доступ к разделу “Журнал изменений” Код “CanManageChangeLog”	Право доступа к разделу [Журнал изменений].
Доступ к разделу “Системные настройки” Код “CanManageSysSettings”	Право доступа к разделу [Системные настройки].
Доступ к разделу “Справочники” Код “CanManageLookups”	Право доступа к разделу [Справочники].
Доступ к разделу “Конфигурация” Код “CanManageSolution”	Право доступа к разделу [Управление конфигурацией] дизайнера системы.
Просмотр раздела “Журнал аудита” Код “CanViewSysOperationAudit”	Право на просмотр содержимого раздела [Журнал аудита].
Управление разделом “Журнал аудита” Код “CanManageSysOperationAudit”	Право на просмотр содержимого раздела [Журнал аудита], а также на выполнение действия архивирования журнала.

Доступ к функциональности поиска дублей

Системная операция	Описание
Поиск дублей Код "CanSearchDuplicates"	Право выполнять поиск дублирующихся записей в разделах, для которых настроены правила поиска дублей .
Обработка дублей Код "CanMergeDuplicates"	Право на выполнение слияния дублей на странице результатов массового поиска дублей, а также во всех разделах и справочниках.
Доступ к правилам поиска дублей Код "CanManageDuplicatesRules"	Право создавать и редактировать правила поиска дублей.

Доступ к настройкам интеграций

Системная операция	Описание
Доступ к OData Код "CanUseODataService"	Право доступа к интеграции с внешними ресурсами по протоколу OData.

Общие действия в системе

Системная операция	Описание
Настройка списка почтовых провайдеров Код "CanManageMailServers"	Право формировать список email-серверов, используемых для отправки и получения писем.
Настройка синхронизации с общими почтовыми ящиками Код "CanManageSharedMailboxes"	Право управлять доступом к почтовым ящикам, для которых был установлен признак [Общий].
Изменение прав на запись Код "CanChangeEntitySchemaRecordRight"	Право устанавливать доступ по записям в объектах. Для того чтобы доступ по записям объекта работал, переключатель [<i>Использовать доступ по операциям</i>] в том же объекте должен быть включен.
Не учитывать проверку доступа по IP-адресу Код "SuppressIPRestriction"	Для пользователя, который имеет доступ к данной операции, при попытке входа в систему будут игнорироваться ограничения по IP-адресу.
Экспорт реестра	Право сохранения данных реестра в файл

Код "CanExportGrid" Системная операция	Описание формата *.xlsx. Если у пользователя нет права на данную операцию, то действие [Экспорт в Excel] в разделах и в меню блоков итогов "Список" неактивно.
Возможность запускать бизнес-процессы Код "CanRunBusinessProcesses"	Право запускать выполнение любых бизнес-процессов в системе. По умолчанию права на эту системную операцию предоставлены всем пользователям.
Отмена выполнения процесса Код "CanCancelProcess"	Право отменять выполнение запущенного бизнес-процесса в журнале процессов.
Доступ к настройке рабочих мест Код "CanManageWorkplaceSettings"	Право на создание и настройку рабочих мест : управление перечнем разделов, которые доступны в боковой панели.
Доступ к комментариям Код "CanEditOrDeleteComment"	Право редактировать и удалять комментарии к сообщениям в ленте.
Права на удаление сообщений и комментариев Код "CanDeleteAllMessageComment"	Право удалять сообщения и комментарии, оставленные другими пользователями в разделе [<i>Лента</i>], вкладке [<i>Лента</i>] панели уведомлений, а также на вкладке [<i>Лента</i>] страниц просмотра и редактирования разделов системы. Пользователи могут редактировать и удалять собственные сообщения и комментарии, не обладая доступом к данной системной операции.

Предоставить лицензии пользователю

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Каждому новому пользователю системы нужно выдать лицензию. Только лицензированные пользователи могут войти в систему и имеют доступ к ее функциональности. Например, если пользователю не выдана лицензия продукта Creatio marketing, то он не сможет пользоваться специфической функциональностью продукта, такой как разделы [*Email*] и [*Кампании*]. По умолчанию распределение лицензий между пользователями выполняют системные администраторы.

Важно. Для лицензирования учетной записи в системе должны быть доступны лицензии, которые не были назначены другим пользователям.

Чтобы предоставить пользователю лицензию:


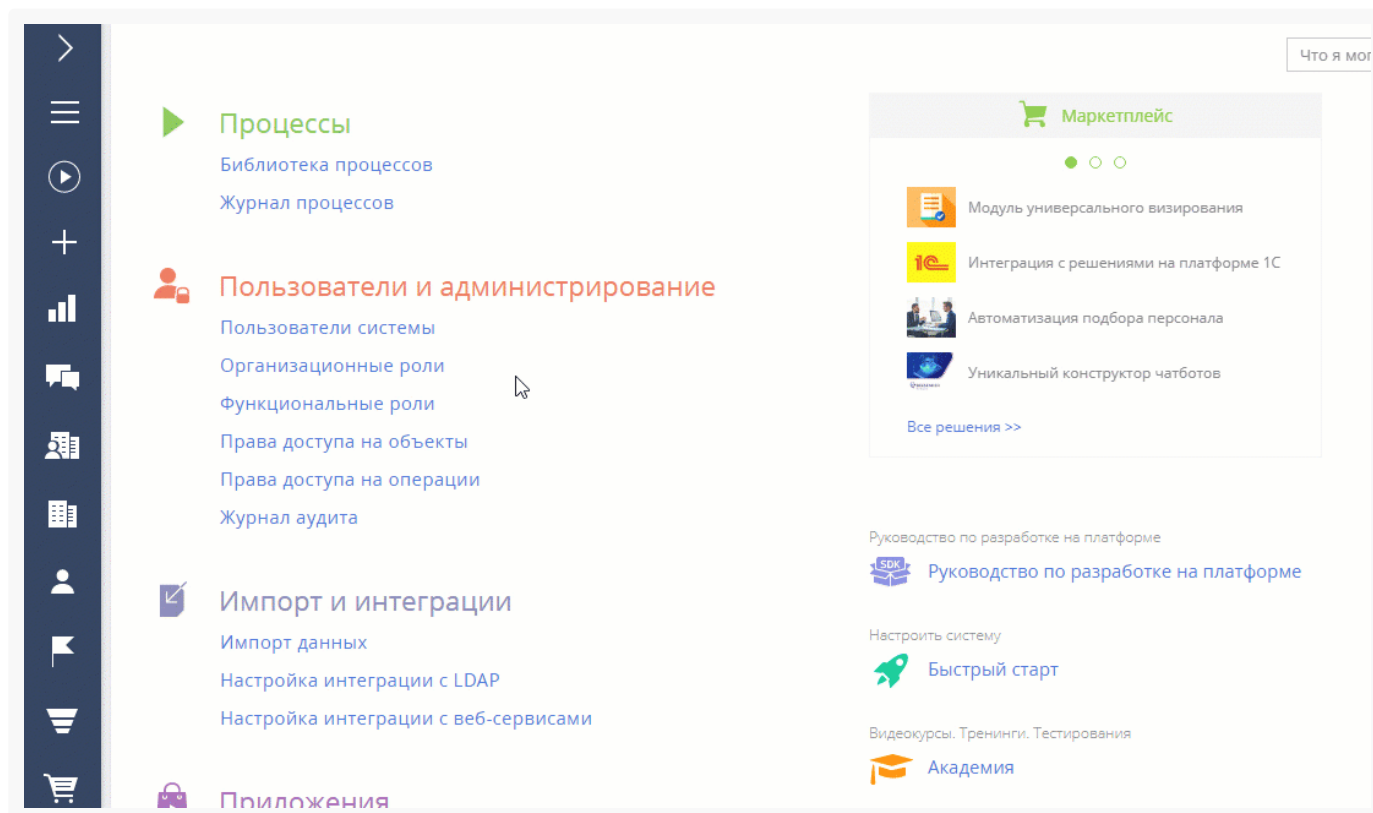
1. Нажмите  —> “**Пользователи системы**”.
2. Откройте страницу пользователя —> вкладка [**Лицензии**].
3. Установите признак напротив той лицензии, которую необходимо предоставить пользователю ([Рис. 1](#)).

Рис. 1 — Предоставление пользователю лицензии



В результате пользователю будет предоставлена лицензия на выбранный продукт.

На заметку. Если в приложении нет доступных лицензий, то запросите их у службы поддержки и загрузите систему. Подробнее читайте в статье [Лицензировать Creatio](#).

Делегировать права доступа

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)


Делегирование прав доступа позволяет передать все права доступа одного сотрудника другому на ограниченный период времени. Это полезно, например, когда сотрудник находится вне офиса или иным образом недоступен, и кто-то должен взять на себя его обязанности. Можно делегировать права отдельных пользователей или ролей любому количеству других пользователей или ролей.

Для делегирования прав у пользователя должен быть доступ к системным операциям “**Управление списком пользователей**” (код CanManageUsers) и “**Изменение делегируемых прав**” (код

CanChangeAdminUnitGrantedRight).

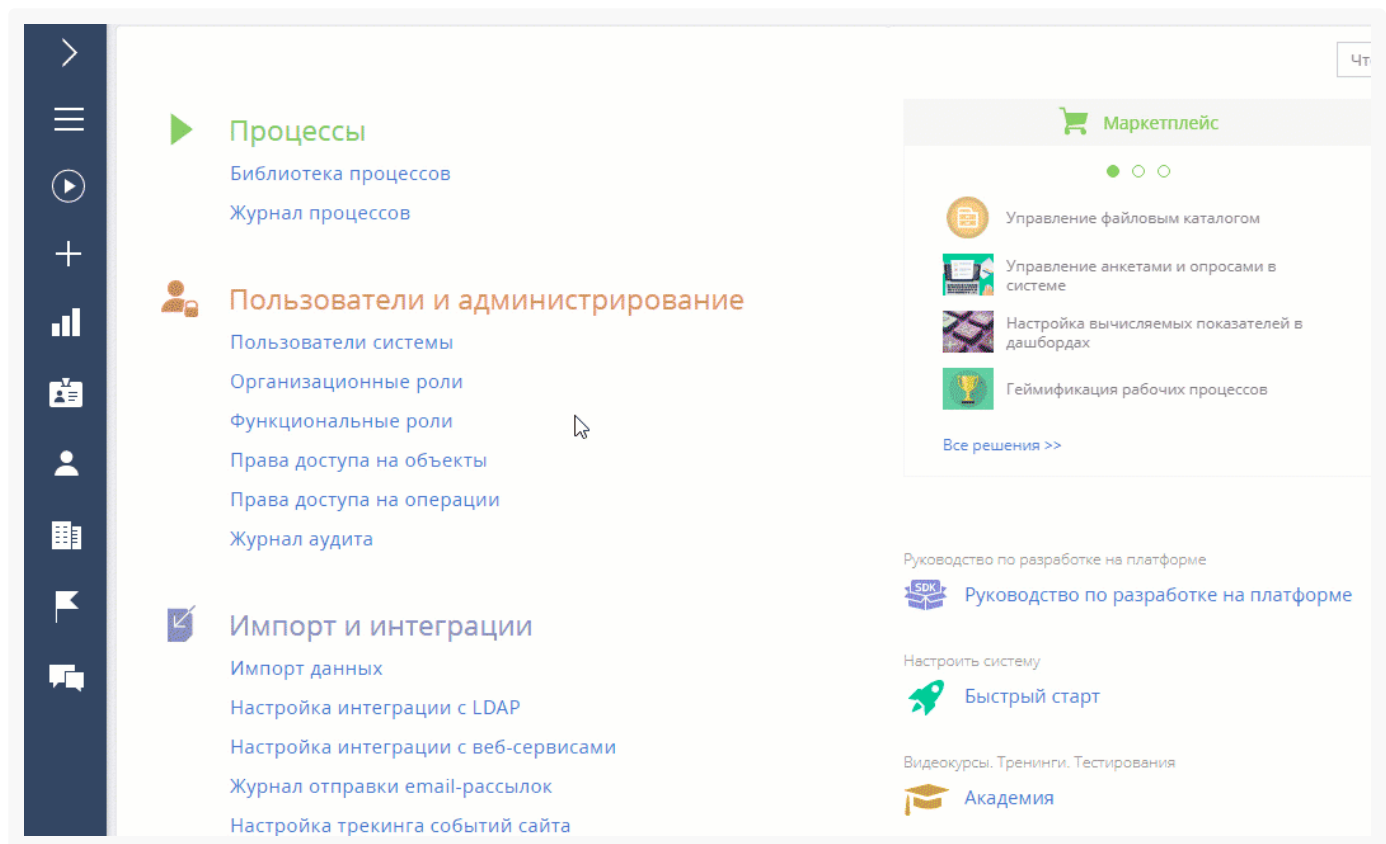
Делегировать права пользователя другим пользователям и ролям

Для того, чтобы делегировать права другому пользователю или группе пользователей:

1. Нажмите  —> “**Пользователи системы**”.
2. Откройте страницу пользователя, **чьи права вы хотите делегировать**.
3. Откройте вкладку [**Делегирование прав**] —> кнопка [**Делегировать права**].
4. В открывшемся окне выберите пользователя или группу пользователей, **которые получают права**, например организационная роль “Отдел продаж”.
5. Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Заккрыть**] на странице пользователя.
6. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].

В результате на детали [**Делегирование прав доступа**] пользователи и роли, которые получили права, отображаются в колонке [**Получает права**], а пользователь, чьи права были делегированы, отображается в колонке [**Раздает права**] ([Рис. 1](#)).


Рис. 1 — Делегирование прав сотрудника другому сотруднику или группе



Делегировать права пользователю от других

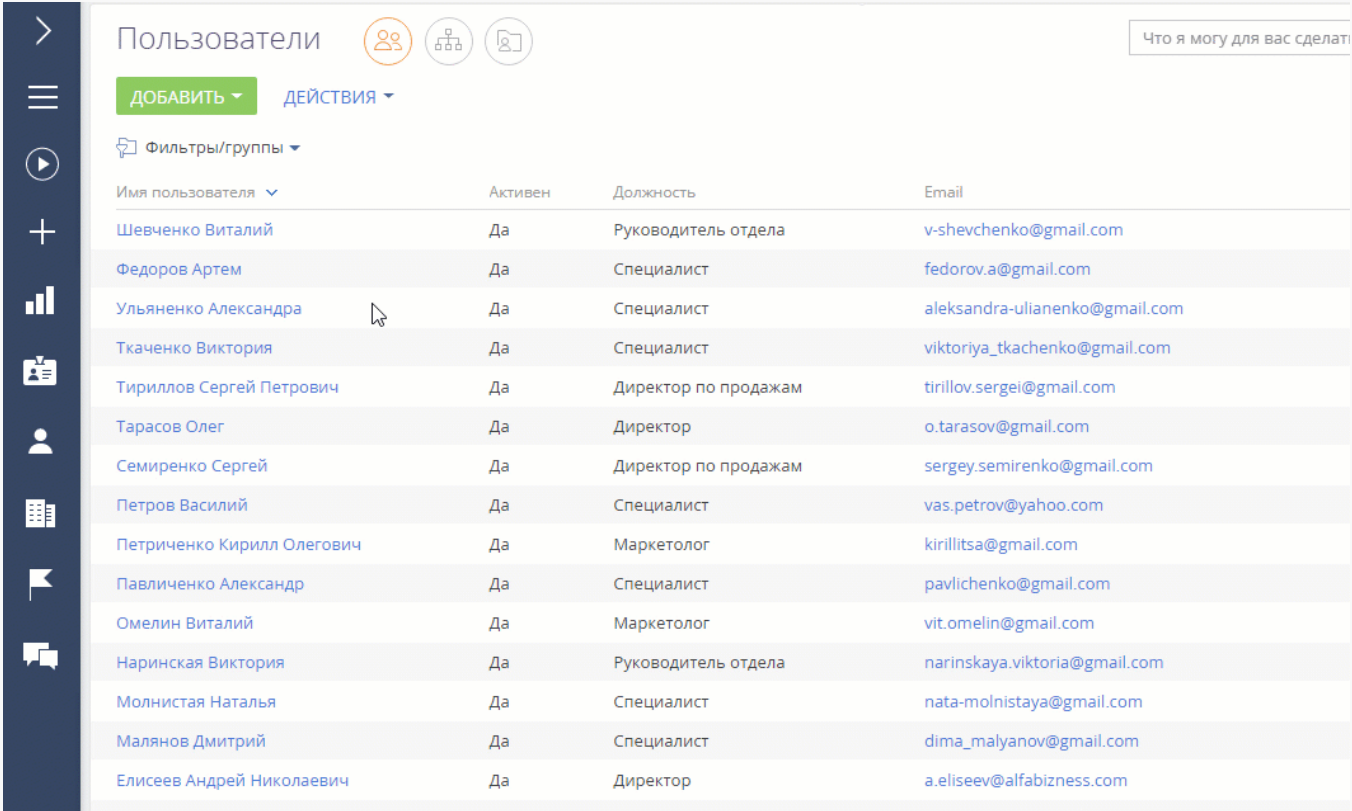
пользователей и ролей

Чтобы передать пользователю права от других пользователей и ролей:

1. Нажмите  —> **“Пользователи системы”**.
2. Откройте страницу пользователя, **который получит права**.
3. Откройте вкладку [**Делегирование прав**] —> кнопка [**Получить права**].
4. В открывшемся окне выберите пользователя или группу пользователей, **чьи права необходимо делегировать**, например организационная роль “Отдел продаж”.
5. Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Заккрыть**] на странице пользователя.
6. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].


В результате имя пользователя, который получил права, появится на детали [**Делегирование прав доступа**] в колонке [**Получает права**], а организационная роль, чьи права были делегированы, появится в колонке [**Раздает права**] ([Рис. 2](#)).

Рис. 2 — Делегирование прав пользователю от других пользователей и ролей



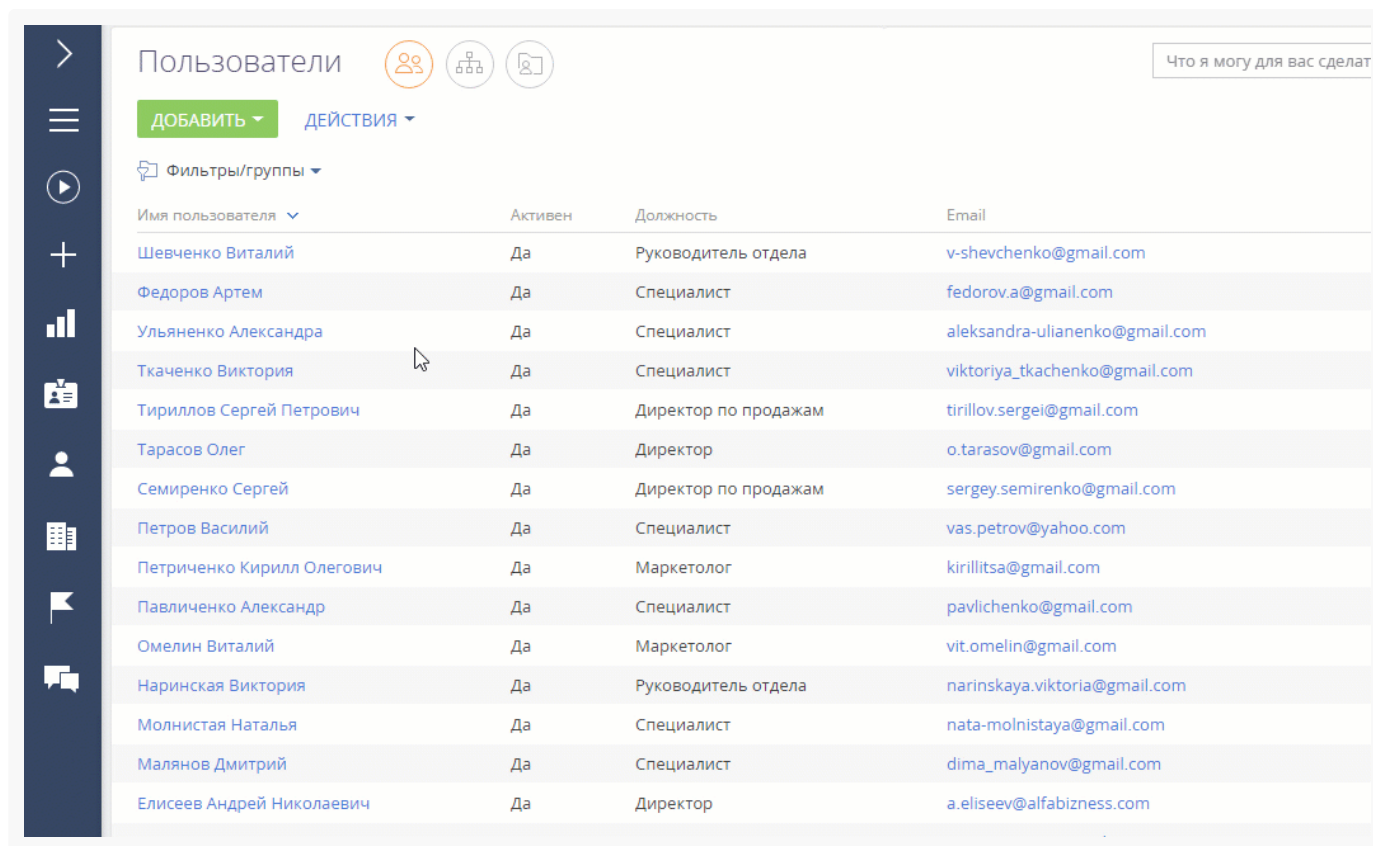
Имя пользователя	Активен	Должность	Email
Шевченко Виталий	Да	Руководитель отдела	v-shevchenko@gmail.com
Федоров Артем	Да	Специалист	fedorov.a@gmail.com
Ульяненко Александра	Да	Специалист	aleksandra-ulianenko@gmail.com
Ткаченко Виктория	Да	Специалист	viktoriya_tkachenko@gmail.com
Тириллов Сергей Петрович	Да	Директор по продажам	tirillov.sergei@gmail.com
Тарасов Олег	Да	Директор	o.tarasov@gmail.com
Семиренко Сергей	Да	Директор по продажам	sergey.semirenko@gmail.com
Петров Василий	Да	Специалист	vas.petrov@yahoo.com
Петриченко Кирилл Олегович	Да	Маркетолог	kirillitsa@gmail.com
Павличенко Александр	Да	Специалист	pavlichenko@gmail.com
Омелин Виталий	Да	Маркетолог	vit.omelin@gmail.com
Наринская Виктория	Да	Руководитель отдела	narinskaya.viktoria@gmail.com
Молнистая Наталья	Да	Специалист	nata-molnistaya@gmail.com
Малянов Дмитрий	Да	Специалист	dima_malyanov@gmail.com
Елисеев Андрей Николаевич	Да	Директор	a.eliseev@alfabizness.com

Удалить делегированные права доступа

1. Нажмите  —> **“Пользователи системы”**.
2. Откройте страницу пользователя, **делегированные права которого вы хотите удалить**.
3. Откройте вкладку [**Делегирование прав**], **отметьте запись**, которую вам необходимо удалить.

4. Нажмите **:** —> “Удалить” ([Рис. 3](#)). **Закройте страницу пользователя.**
5. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].

Рис. 3 — Удаление делегированных прав



Имя пользователя	Активен	Должность	Email
Шевченко Виталий	Да	Руководитель отдела	v-shevchenko@gmail.com
Федоров Артем	Да	Специалист	fedorov.a@gmail.com
Ульяненко Александра	Да	Специалист	aleksandra-ulianenko@gmail.com
Ткаченко Виктория	Да	Специалист	viktoriya_tkachenko@gmail.com
Тириллов Сергей Петрович	Да	Директор по продажам	tirillov.sergei@gmail.com
Тарасов Олег	Да	Директор	o.tarasov@gmail.com
Семиренко Сергей	Да	Директор по продажам	sergey.semirenko@gmail.com
Петров Василий	Да	Специалист	vas.petrov@yahoo.com
Петриченко Кирилл Олегович	Да	Маркетолог	kirillitsa@gmail.com
Павличенко Александр	Да	Специалист	pavlichenko@gmail.com
Омелин Виталий	Да	Маркетолог	vit.omelin@gmail.com
Наринская Виктория	Да	Руководитель отдела	narinskaya.viktoria@gmail.com
Молнистая Наталья	Да	Специалист	nata-molnistaya@gmail.com
Малянов Дмитрий	Да	Специалист	dima_malyanov@gmail.com
Елисеев Андрей Николаевич	Да	Директор	a.eliseev@alfabizness.com

В результате делегированные права доступа удаляются, у пользователя останутся только те права, которые были у него изначально.

Разблокировать учетную запись пользователя

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Статья содержит лучшие практики настроек информационной безопасности Creatio.

Внедрить политику паролей организации

Убедитесь в том, что настройки логина и пароля соответствуют политике безопасности компании. Вы можете использовать рекомендованные значения, если в политике не определены точные требования.

Длина пароля. Рекомендуем использовать пароли, состоящие из 8 и более символов. Установить сложность пароля вы можете в [системных настройках](#):

- “Сложность пароля: Минимальная длина” (код “MinPasswordLength”);
- “Сложность пароля: Минимальное количество символов нижнего регистра” (код “MinPasswordLowercaseCharCount”);
- “Сложность пароля Минимальное количество символов верхнего регистра” (код “MinPasswordUppercaseCharCount”);
- “Сложность пароля Минимальное количество цифр” (код “MinPasswordNumericCharCount”);
- “Сложность пароля Минимальное количество специальных символов” (код “MinPasswordSpecialCharCount”).

История паролей. Creatio сравнивает предыдущий пароль пользователя с новым, чтобы убедиться, что они не совпадают. Количество предыдущих паролей, которые необходимо сравнивать с новым, вы можете указать в системной настройке “Количество анализируемых паролей” (код “PasswordHistoryRecordCount”).

Количество попыток входа до предупреждающего сообщения и время блокировки пользователя. Рекомендуем установить 5 попыток входа до предупреждающего сообщения и 15 минут в качестве времени блокировки пользователя. Вы можете отрегулировать поведение блокировки в следующих системных настройках:

- “Количество попыток входа” (код “LoginAttemptCount”) — допустимое количество неудачных попыток ввода логина или пароля.
- “Количество попыток входа до предупреждающего сообщения” (код “LoginAttemptCount”) — порядковый номер неудачной попытки ввода логина или пароля, после которого отобразится сообщение о возможности дальнейшей блокировки учетной записи пользователя.
- “Время блокировки пользователя” (код “UserLockoutDuration”) — время блокировки (в минутах) учетной записи пользователя после указанного количества неудачных попыток ввода логина или пароля.

Подробнее: [Разблокировать учетную запись пользователя](#).

Сообщения о неверном пароле и блокировке при попытке входа. Рекомендуем отображать сообщение с общей информацией без уточнения конкретной проблемы. Для этого убедитесь, что в значениях по умолчанию следующих системных настроек снят признак:

- “Отображать информацию о блокировке учетной записи при входе” (код “DisplayAccountLockoutMessageAtLogin”);
- “Отображать информацию о неверном пароле при входе” (код “DisplayIncorrectPasswordMessageAtLogin”).

Время завершения сессии

Задайте интервал в минутах, по истечении которого сессия будет закрыта, в системной настройке “Таймаут сеанса пользователя” (код “UserSessionTimeout”). Значение по умолчанию: “60”.

Протокол TLS для Creatio on-site

В Creatio реализована поддержка протокола TLS 1.2. Устаревшие версии протокола TLS 1.0 и 1.1 делают систему безопасности уязвимой.

Безопасные конфигурации заголовков для Creatio on-site

Примите необходимые меры для того, чтобы современные браузеры не поддавались уязвимостям, которые можно предотвратить. Для этого включите следующие заголовки, которые соответствуют [OWASP Secure Headers Project](#) (открытый проект обеспечения безопасности веб-приложений):

HTTP Strict Transport Security (HSTS). Включите заголовок `Strict-Transport-Security` и установите значение хранения параметра в памяти браузера, соответствующее одному году:

```
Strict-Transport-Security: max-age=3153600
```

Защита от кликджекинга (clickjacking). Включите заголовок `X-Frame-Options` и разрешите встраивание веб-страниц только на тех же адресах, что и у вашего приложения Creatio:

```
X-Frame-Options: sameorigin
```

Защита от атак межсайтового скриптинга (XSS). Включите заголовок `X-Frame-Options` и установите блокировку попыток XSS-атак:

```
X-XSS-Protection: 1; mode=block
```

Защита от MIME-сниффинга. Включите заголовок `X-Content-Type-Options` и установите режим “nosniff”. Этот режим предотвращает попытку браузера переопределить тип контента ресурса, если он отличается от объявленного типа контента:

```
X-Content-Type-Options: nosniff
```

Политика реферера (referrer policy). Включите заголовок `Referrer-Policy` и установите значение “origin-when-cross-origin”. Заголовок определяет, какой объем информации о реферере (отправленной с заголовком “Referer”) будет включен в запросы:

```
Referrer-Policy: origin-when-cross-origin
```

Безопасность контента. Включите заголовок `Content Security Policy` и настройте его следующим образом:

```
Content-Security-Policy: default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'; script-src
```

Ответы на запросы для Creatio on-site

Ограничьте количество и тип информации, доступной в ответах на запросы. Для этого измените файл [Web.config file](#) в корневом каталоге Creatio следующим образом:

Отключите `X-Powered-By`.

```
<system.webServer> <httpProtocol> <customHeaders> <remove name="X-Powered-By" /> </customHeaders>
```

Отключите `X-AspNet-Version`.

```
<httpRuntime enableVersionHeader="false" />
```

Отключите `Server Header` (доступно для IIS версии 10 и выше).

```
<system.webServer> <security> <requestFiltering removeServerHeader ="true" /> </security> </syst
```

Запрет одновременных сеансов для Creatio on-site

Начиная с версии Creatio 7.13.3, вы можете запретить несколько одновременных входов в систему под одним пользователем. Creatio автоматически закроет старую сессию на другом устройстве, если пользователь откроет новую. Чтобы включить ограничение сессии, установите для параметра web.config **Feature-AllowOnlyOneSessionPerUser** значение "true":

```
<add key="Feature-AllowOnlyOneSessionPerUser" value="true" />
```

Функциональность доступна в режиме бета-тестирования. Не поддерживаются следующие функции:

- мобильное приложение;
- сквозная аутентификация Windows (UsePathThroughAuthentication);
- SSO (SAML);

Кроме того, для каждой интеграции необходима отдельная учетная запись Creatio, которая не используется пользователями.