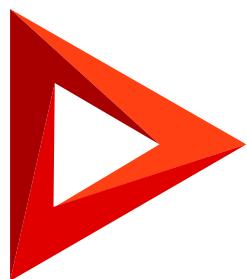


Администрирование

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

Инструменты очистки дискового пространства	10
Возможные причины быстрого роста базы данных	10
Инструменты очистки базы данных Creatio	11
Настроить обработку чатов	12
Добавить очередь чата	13
Настроить действия чата	14
Ограничить количество активных чатов на коммуникационной панели	15
Изменить звук оповещения о новом чате	16
Настроить синхронизацию с LDAP	16
Настроить интеграцию с LDAP	17
Привязать элементы LDAP к пользователям и ролям Creatio	22
Запустить синхронизацию с LDAP	25
Настроить безопасное подключение к почтовому ящику	28
Настроить верификацию для провайдера UniOne	28
Получить записи SPF, DKIM и дополнительный параметр отправки	29
Выполнить настройки в DNS-зоне домена	31
Настроить корректную отправку писем на адреса группы mail.ru	32
Добавить почтовый провайдер IMAP/SMTP	33
Способ 1. Добавить провайдер IMAP/SMTP из вкладки [Email] коммуникационной панели	33
Способ 2. Добавить провайдер IMAP/SMTP из профиля пользователя	37
Лицензировать Creatio	38
Добавить лицензии в приложение	39
Распределить лицензии между пользователями	43
Удалить лицензии в приложении	46
Настроить журнал изменений	47
Способ 1. Настроить логи из раздела [Журнал изменений]	48
Способ 2. Настроить логи из раздела, справочника или детали	50
Настроить Single Sign-On через ADFS	51
Выполнить настройки на стороне ADFS	51
Выполнить настройки на стороне Creatio	59
Безопасная загрузка файлов	68
Выбрать режим проверки файлов	68
Настроить список типов файлов	69
Настроить ограничения для неизвестных типов файлов	70
Настроить исключение веб-сервисов из ограничений загрузки файлов	70
Управление значениями справочника	71

Настроить Microsoft Exchange и Microsoft 365	74
Способ 1. Добавить провайдер из вкладки [Email] коммуникационной панели	74
Способ 2. Добавить провайдер из профиля пользователя	78
Настроить журнал аудита	79
Организационные роли	80
Добавить организационную роль	81
Добавить роль руководителей	82
Добавить пользователей в организационную роль	84
Зарегистрировать приложение Creatio в Google Workspace	86
Шаг 1. Настроить проект Google Cloud Platform	86
Шаг 2. Получить ключи для интеграции Google с внешними приложениями	92
Шаг 3. Ввести ключи Google в Creatio	93
Настроить доступ по операциям	96
Настроить доступ по операциям в объекте раздела	97
Настроить приоритет прав доступа по операциям объекта	100
Настроить доступ по операциям в объекте детали	102
Ускорить обработку сложных запросов к базе данных	104
Шаг 1. Создать реплику базы данных.	105
Шаг 2. Настроить перенаправление тяжелых запросов	105
Настроить интеграцию с Facebook Messenger	106
Шаг 1. Добавить канал Facebook Messenger	106
Шаг 2. Настроить интеграцию Creatio с внешним чат-ботом (опционально)	109
Настроить фильтры Active Directory	109
Формат фильтров	110
Фильтрация пользователей	111
Фильтрация групп	111
Стандартные фильтры пользователей группы Active Directory	111
Настроить фильтры для синхронизации пользователей/групп	112
Настроить персональный почтовый ящик	113
Настроить учетную запись почты преднастроенного провайдера	113
Настроить учетную запись почты на корпоративном домене	114
Настроить верификацию для провайдера Elastic Email	115
Добавить корпоративный домен на страницу настройки email-рассылок	116
Получить SPF- и DKIM-записи	117
Выполнить настройки в DNS-зоне домена	118
Управлять лицензиями пользователей	120
Лицензировать учетную запись пользователя	120
Массово предоставить или отзовать лицензии	121
Просмотреть логи изменений	121

Способ 1. Просмотреть логи записи из журнала изменений	122
Способ 2. Просмотреть логи со страницы записи	124
Настроить Single Sign-On через OneLogin	126
Выполнить настройки на стороне OneLogin	127
Выполнить настройки на стороне Creatio	127
Создать новый справочник	130
Создать справочник в мастере разделов	131
Зарегистрировать справочник на основании существующего объекта	133
Синхронизировать контакты с Microsoft Exchange и Microsoft 365	134
Настроить импорт контактов в Creatio	135
Настроить экспорт контактов из Creatio	135
Синхронизировать контакты с Microsoft Exchange и Microsoft 365	136
Просмотреть и архивировать журнал аудита	136
Открыть журнал аудита	136
Архивировать журнал аудита	137
Синхронизировать контакты и активности с Google	138
Настроить синхронизацию	138
Синхронизировать контакты Creatio с контактами Google	141
Синхронизировать активности Creatio с календарем Google	141
Функциональные роли	142
Добавить функциональную роль	142
Связать функциональные и организационные роли	143
Добавить пользователей в функциональную роль	144
Настроить права доступа на колонки	145
Настроить доступ на колонки объекта	147
Настроить приоритет прав доступа на колонки объекта	149
Рекомендуемые настройки информационной безопасности	151
Внедрить политику паролей организации	152
Время завершения сессии	153
Протокол TLS для Creatio on-site	153
Безопасные конфигурации заголовков для Creatio on-site	153
Ответы на запросы для Creatio on-site	154
Запрет одновременных сеансов для Creatio on-site	154
Настроить интеграцию с Telegram	155
Импортировать новых пользователей и роли из Active Directory	156
Подготовить каталог к интеграции	156
Импортировать новых пользователей из LDAP	156
Настроить общий почтовый ящик	157
Настроить верификацию для провайдера SendGrid	159

Добавить ваш корпоративный домен на страницу настройки email-рассылок	159
Получить ключи настройки для домена	160
Выполнить настройки в DNS-зоне вашего домена	161
Особенности лицензирования Marketing Creatio	162
Определить количество используемых лицензий на активных контактов	164
Очистить логи журнала изменений	166
Настроить Just-In-Time User Provisioning	167
Управление системными настройками	171
Перейти к системным настройкам	172
Изменить системные настройки	173
Предоставить доступ к отдельным системным настройкам	173
Синхронизировать расписание Creatio с календарями Microsoft Exchange и Microsoft 365	174
Настроить импорт активностей в Creatio	175
Настроить экспорт активностей из Creatio	176
Синхронизация активностей с Microsoft Exchange и Microsoft 365	176
Добавить пользователей	176
Добавить пользователя с правами системного администратора	177
Добавить пользователя-сотрудника	179
Добавить новый контакт	179
Создать пользователя	180
Удалить аккаунт Google из Creatio	182
Настроить доступ по записям	182
Настроить доступ на экспорт данных	187
Предоставить удаленный доступ службе поддержки Creatio	188
Настроить безопасный доступ	189
Просмотреть результаты подключения	190
Настроить интеграцию с WhatsApp	191
Шаг 1. Настроить тестовую учетную запись (опционально)	192
Шаг 2. Настроить учетную запись для бизнеса	194
Шаг 3. Добавить канал WhatsApp в Creatio	195
Настроить аутентификацию с LDAP	196
Настроить аутентификацию пользователей через LDAP на .NET Framework	196
Настроить аутентификацию пользователей через LDAP на .NET Core	198
Настроить провайдеры аутентификации	200
Настроить доменную авторизацию	201
Описание системных настроек	203
Автонумерация записей	203
Автообновление возраста	204
Администрирование	205

Бизнес-процессы	208
Блокировка учетной записи пользователя	208
Визирование	208
Глобальный поиск	209
Журнал процессов	210
Заявки	211
Значения по умолчанию	211
Интеграция с внешними ресурсами	213
Конфигурирование	214
Мобильное приложение (Mobile)	216
Настройки раздела Email	216
Обращения	217
Общие	218
Отправка email-сообщений	220
Поиск дублей	221
Подбор продуктов	221
Синхронизация с LDAP	222
Телефония	225
Управление паролями	225
Управление файлами	227
Фильтр нежелательных обращений	228
Финансы	228
Чаты	228
Изменить индивидуальные настройки учетной записи почты	229
Настроить загрузку почты в систему	230
Настроить отправку почты из Creatio	231
Настроить подпись в email-сообщениях	232
Рекомендации по настройке для популярных DNS-провайдеров	232
Настройка SPF	233
Настройка DKIM	234
Настроить OAuth-аутентификацию для Microsoft 365	237
Аутентификация Windows	238
Как работает аутентификация Windows	239
Настроить аутентификацию Windows в IIS	240
Настроить файл Web.config приложения-загрузчика	241
Изменить системного пользователя (Supervisor)	244
Часто задаваемые вопросы о синхронизации пользователей с LDAP	245
Почему в Creatio импортировались не все пользователи из каталога LDAP?	245
Почему в Creatio импортировались не все пользователи Active Directory после синхронизации LDAP?	245

Почему пользователь не может войти под доменной учетной записью после настройки LDAP?	246
Может ли запись пользователя, импортированного из Active Directory, быть привязана к записи определенного контрагента?	246
Почему не импортируются пользователи из группы "Доменные пользователи" ("Domain users")?	246
Что означает ошибка "22021: invalid byte sequence for encoding "UTF8": 0X00" при синхронизации Active Directory с LDAP?	246
Почему возникает ошибка "Cannot insert duplicate key row in object 'dbo.SysAdminUnit' with unique index 'IUSysAdminunitNameDomain'. The duplicate key value is (...)"?	247
Как настроить фильтр LDAP?	247
Импортировать пользователей из Excel	247
Подготовить документ Excel для импорта пользователей	247
Запустить импорт	249
Настроить пароль, роль и выдать лицензии	251
Настроить права доступа на системные операции	252
Назначить пользователю роли	254
Способ 1. Назначить роли со страницы пользователя	254
Способ 2. Назначить роли со страницы ролей	255
Описание системных операций	256
Управление пользователями и ролями	256
Управление пользователями портала	257
Общий доступ к данным	257
Доступ к колонкам, системным операциям	258
Доступ к особым разделам системы	258
Доступ к функциональности поиска дублей	259
Доступ к настройкам интеграций	260
Общие действия в системе	260
Настроить регистрацию лидов из LinkedIn	261
Настроить интеграцию с рекламным аккаунтом LinkedIn	262
Синхронизировать лиды, зарегистрированные до настройки интеграции	266
Отключить лидогенерацию LinkedIn	267
Предоставить лицензии пользователю	268
Делегировать права доступа	269
Делегировать права пользователя другим пользователям и ролям	270
Делегировать права пользователю от других пользователей и ролей	271
Удалить делегированные права доступа	272
Добавить сервис для подключения к online-встречам	273
Разблокировать учетную запись пользователя	274
Внедрить политику паролей организации	274
Время завершения сессии	275
Протокол TLS для Creatio on-site	275

Безопасные конфигурации заголовков для Creatio on-site	275
Ответы на запросы для Creatio on-site	276
Запрет одновременных сеансов для Creatio on-site	277

Инструменты очистки дискового пространства

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

При работе с большими объемами информации важной частью обслуживания базы данных является своевременное удаление устаревших и неактуальных записей. Это позволяет сохранять дисковое пространство на сервере базы данных, увеличивая ее быстродействие.

Возможные причины быстрого роста базы данных

К стремительному росту базы данных могут приводить:

- Некорректно настроенные или избыточные **права доступа на записи**. Например, когда права доступа на запись настроены индивидуально для большого количества пользователей, не объединенных в группы. В этом случае рекомендуем изменить настройки и актуализировать права доступа в приложении. Подробнее: [Управление доступом](#).
- Отсутствие ограничений на **загрузку файлов** в приложение. Файлы могут быть добавлены в приложение сотрудниками, загружены при синхронизации почты или прикреплены к сообщениям на портале самообслуживания. Рекомендуем ограничить размер загружаемых в приложение файлов до 10 Мб. Управлять этим ограничением можно в системной настройке “Максимальный размер загружаемого файла” (код “MaxFileSize”). Также рекомендуем регулярно проверять актуальность загруженных файлов и удалять устаревшие. Для этого в приложении можно настроить бизнес-процесс.
- **Синхронизация всех писем** из почтовых ящиков пользователей. Рекомендуем выбрать для загрузки в приложение только те папки почтового ящика, письма из которых необходимо обработать в приложении. Например, папки “Важные” или “Отмеченные”. Подробнее: [Настроить загрузку почты в систему](#).
- Включение **трассировки процессов** на длительный период. Отладка процессов обычно выполняется на среде разработки или тестовом сайте. В случае, когда необходимо собрать отладочную информацию на продуктивном сайте, рекомендуем отключать трассировку сразу по завершении анализа проблем с выполнением процесса. [Выполнить трассировку параметров процесса](#).
- Некорректная настройка **логики выполнения бизнес-процессов**, из-за которой процесс находится в состоянии “Выполняется” гораздо дольше необходимого. В этом случае в приложении сохраняются все временные файлы, которые имеют отношение к выполнению процесса. Рекомендуем моделировать бизнес-процессы таким образом, чтобы они имели однозначные условия завершения и не оставались в состоянии “Выполняется” дольше нескольких часов. Подробнее: [Просмотреть информацию о выполнении процессов](#).
- Некорректная настройка **чтения данных в бизнес-процессах**. Значения, получаемые в бизнес-процессе при выполнении элемента [Читать данные] хранятся в таблицах с временными данными до завершения выполнения процесса. В случаях, когда для выполнения бизнес-процесса нет необходимости получать значения всех колонок объекта, рекомендуем настраивать точный список значений, которые необходимо вычитать. Это позволит существенно сократить количество

временных данных, хранящихся в приложении. Подробнее: [Элемент процесса \[Читать данные \]](#).

- Избыточное **логирование изменений**. Рекомендуем включать логирование записей только в тех разделах, где необходимо отслеживать динамику смены данных, например, в продуктовом каталоге. Если вы хотите сохранять информацию об изменениях записей, то необходимо регулярно выполнять чистку журнала изменений от неактуальных данных. Подробнее: [Очистить логи журнала изменений](#).
- Некорректная **настройка интеграции внешних сервисов** с приложением Creatio. При отправке запроса к Creatio без заголовка ForceUseSession внешние сервисы вынуждены повторно выполнять аутентификацию. Подробнее: [Аутентификация](#) (документация по разработке).

Инструменты очистки базы данных Creatio

В Creatio для очистки дискового пространства предусмотрены следующие возможности:

- архивация и автоматическая очистка журнала процессов,
- очистка журнала изменений,
- удаление записей в разделах,
- удаление данных в ходе бизнес-процесса.

Автоматическая очистка журнала процессов

В Creatio предусмотрено логирование всех запускаемых процессов. Это позволяет отслеживать узкие места спроектированных схем и оптимизировать их, а также анализировать эффективность работы сотрудников. Чтобы сократить объем используемого пространства, Creatio автоматически архивирует данные о процессах, которым больше 30 дней. Архивные записи сохраняются в системе и доступны для обработки еще 360 дней, после чего они автоматически удаляются. Вы можете управлять сроками архивации данных журнала и хранения архивных записей.

Подробнее: [Архивирование записей журнала процессов](#).

Очистка журнала изменений

Вы можете очищать историю журнала изменений, чтобы избежать хранения устаревших записей в системе. Рекомендуем регулярно очищать записи логов, чтобы в разделе [Журнал изменений] содержалась только актуальная на данный момент информация.

Подробнее: [Очистить логи журнала изменений](#).

Удаление записей в разделах

В разделах приложения могут храниться неактуальные записи. Вы можете удалять такие записи выборочно или массово в любом разделе Creatio. Если у выбранной для удаления записи есть связи в других разделах системы, то Creatio предложит вам просмотреть их и принять решение о необходимости удаления. Вы можете удалить всю информацию или только выбранную запись и оставить все связанные данные.

Подробнее: [Удалить запись](#).

Удаление данных в ходе бизнес-процесса

Вы можете автоматизировать очистку дискового пространства при помощи бизнес-процессов. Элемент процесса [Удалить данные] позволяет удалить из любого объекта системы как одну запись, так и несколько записей, соответствующих определенным условиям. Например, вы можете создать бизнес-процесс, который будет удалять все запланированные активности, которые были отменены. Такой процесс может запускаться:

- **По таймеру**, в определенное время. Такое решение удобно тем, что процесс можно запускать с заданной периодичностью, например, раз в месяц, и во время наименьшей загруженности приложения, например, ночью.
- **При наступлении определенного события**. Такое решение удобно тем, что процесс запускается автоматически и только в том случае, когда в приложении есть данные для удаления.
- **Вручную**. Такое решение удобно тем, что пользователь сможет запустить процесс в любой момент, когда в этом возникнет необходимость.

Подробнее: [Элемент процесса \[Удалить данные \]](#).

Настройте обработку чатов

Для того, чтобы у операторов контакт-центра вашей компании появилась возможность обрабатывать в Creatio сообщения из популярных мессенджеров, необходимо выполнить ряд предварительных настроек. В общем случае порядок настройки чатов выглядит следующим образом:

1. **Добавить и настроить очередь чата.** На этом шаге формируется список операторов, которые будут обрабатывать сообщения чата, настраиваются правила маршрутизации сообщений и таймаут завершения чата.
2. **Настроить действия чата.** На этом шаге настраивается перечень действий, которые оператор может предпринять по итогам общения с клиентом, например, зарегистрировать обращение, создать заказ, отправить информационное письмо.
3. **Ограничить количество активных чатов.** На этом шаге настраивается максимальное количество активных чатов, которые оператор может одновременно видеть на коммуникационной панели.
4. **Изменить звук оповещения** о новом сообщении чата (опционально). На этом шаге вы можете настроить для операторов узнаваемый сигнал о новых сообщениях чата.
5. **Добавить каналы чатов.** Канал чата в Creatio — это источник, из которого в систему будут добавлены сообщения клиентов. Например, публичная страница в Facebook. В Creatio доступны следующие каналы чатов:
 - [Facebook messenger](#);
 - [Telegram](#);
 - [WhatsApp](#).

Каналы, по которым в приложении есть хотя бы один чат, недоступны для удаления. Если данный канал неактуален, деактивируйте его.

Настройки, необходимые для работы с чатами, выполняются в разделе [Настройка чатов] дизайнера системы. Настройка выполняется администратором системы или пользователем, у которого есть права

на системную операцию “Доступ к разделу “Настройка чатов” (код “CanManageChats”).

Рис. 1 — Пример настройки чатов

Чаты

Каналы

Провайдер	Название	Активен	Очередь
Facebook messenger	Наша компания	<input checked="" type="checkbox"/>	Служба поддержки

Очереди чата

Название	Правило маршрутизации	Таймаут для завершения чата, мин.
Все операторы	На всех	2
Служба поддержки	На всех	30

Действия чата

Название	Процесс	Очередь
Создать обращение	Создание обращения из чата	Все операторы

Добавить очередь чата

Для обработки сообщений в чатах необходимо создать и настроить одну или несколько очередей. Очередь чата определяет, какой группе сотрудников будет направлен в работу чат. Количество очередей не зависит от количества каналов и определяется бизнес-целью. Например, для сообщений со страницы бренда можно настроить очередь чата “Служба поддержки”, а для обработки запросов из интернет-магазина — “Продавцы-консультанты”. Очереди для операторов чата создаются в разделе [Настройка чатов] дизайнера системы. Чтобы добавить очередь чата:

- Перейдите в **дизайнер системы** по кнопке
- Откройте раздел [Настройка чатов].
- В области [Очереди чата] нажмите кнопку
- В открывшемся окне заполните параметры новой очереди:
 - [Название] — отразите в названии очереди ее назначение или целевую роль. Например, “1-я линия поддержки”.
 - [Правило маршрутизации] — алгоритм, определяющий, на кого из операторов очереди будет назначен новый чат.

- “**На всех**” — новый чат будет доступен всем операторам, которые назначены в текущей очереди.
 - “**На свободного**” — чаты будут назначаться автоматически на самого свободного оператора в момент распределения. Самым свободным считается оператор, у которого меньше всего чатов в работе на момент распределения. При равном количестве чатов будет направлен на того оператора, который дольше всех не брал новые чаты в работу. Если оператор не берет чат в работу в течение 5 минут, то выполнится перераспределение на следующего оператора, а текущий оператор переходит в статус “Неактивный”. Это время можно изменить в системной настройке “**Таймаут на взятие чата в работу оператором**” (код “OmniChatOperatorAcceptChatTimeout”). Для продолжения работы с чатами оператору необходимо будет поменять статус в коммуникационной панели на “Активный”.
- e. [Таймаут для завершения чата, минут] — максимальное время ожидания с момента последнего исходящего сообщения в чате до его автоматического завершения. По истечению установленного времени данный чат будет автоматически завершен. После завершения чата по таймауту последующие сообщения клиента будут обработаны как новые и распределены на активных операторов. Если значение в поле не установлено, то чаты не будут завершаться автоматически.
- f. На детали [Операторы] нажмите кнопку **+**. В открывшемся окне укажите пользователей или роли, которые будут обрабатывать сообщения в чатах. Например, вы можете использовать организационную роль “Менеджеры колл-центра”. Вы можете добавить в список операторов несколько пользователей или ролей. Также один и тот же пользователь может быть добавлен в операторы нескольких очередей чатов.

Рис. 2 — Пример настройки очереди чата

Служба поддержки

ЗАКРЫТЬ

Название *

Служба поддержки

Правило маршрутизации *

На всех

Таймаут для завершения чата, минут

30

Операторы + :

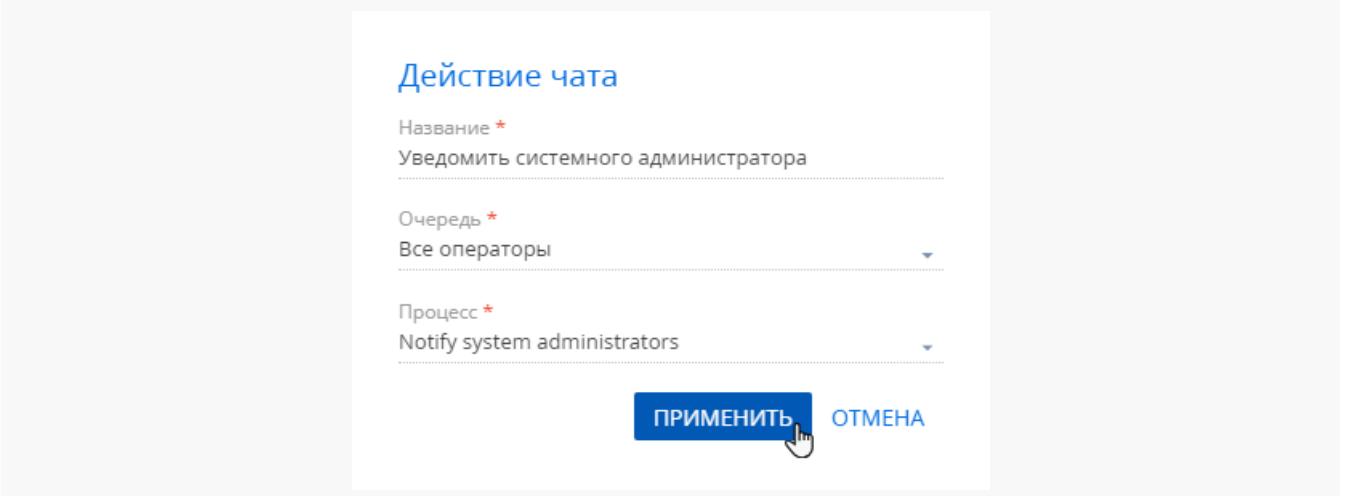
Пользователь/роль
Мирный Евгений
Малянов Дмитрий
Ульяненко Александра
Савченко Ирина

Настройте действия чата

Действия чата позволяют упростить и автоматизировать обработку сообщений. В продуктах Service Creatio преднастроено действие “Создать обращение”, по которому запускается бизнес-процесс “Создание обращения из чата” (CreateCaseFromChat). Вы можете настроить список действий, которые будут доступны оператору при обработке чата, например “Создать заказ”, “Уведомить менеджера об оплате счета” или “Уведомить системного администратора”. Для этого в Creatio должен быть создан процесс, который будет запускаться при работе в чате. Подробнее о создании и настройке процессов читайте в блоке [Настройка процессов \(BPMN\)](#). Когда процесс готов, необходимо сформировать для него действие чата:

1. Перейдите в **дизайнер системы** по кнопке  .
2. Откройте раздел [*Настройка чатов*].
3. В области [*Действия чата*] нажмите кнопку  .
4. В появившейся мини-карточке укажите:
 - a. [*Название*] — заголовок действия, который отобразится для оператора при работе с чатом.
 - b. [*Очередь*] — выберите очередь чата, операторам которой будет доступно данное действие.
 - c. [*Процесс*] — выберите процесс, который будет запускаться по действию чата.
 - d. Нажмите [*Применить*].

Рис. 3 — Пример настройки действия чата



На заметку. В процесс, который запускается по действию чата, передаются входящие параметры “ChatId” и/или “ContactId”, через которые осуществляется привязка процесса к текущему чату. Подробнее читайте в статье [Параметры процесса](#).

Ограничить количество активных чатов на коммуникационной панели

Вы можете настроить для операторов ограничение количества активных чатов, которые они могут обрабатывать одновременно. По умолчанию в системе настроено ограничение до 2 чатов. Чтобы его изменить:

- Перейдите в **дизайнер системы** по кнопке  .
- Откройте раздел [Системные настройки].
- Перейдите в системную настройку “**Количество одновременных чатов**” (код “SimultaneousChats”).
- В поле [Значение по умолчанию] укажите необходимое количество чатов, которые оператор сможет обрабатывать одновременно. По умолчанию это 5 чатов. Если у оператора в работе максимально доступное количество чатов, то новые он не увидит, пока не завершит хотя бы один чат. Это ограничение распространяется на все доступные для оператора каналы чатов.
- Нажмите [Сохранить].

Изменить звук оповещения о новом чате

Вы можете заменить стандартный сигнал уведомления о новых сообщениях чата, чтобы операторы легко его идентифицировали. Для этого:

- Перейдите в **дизайнер системы** по кнопке  .
- Откройте раздел [Системные настройки].
- Перейдите в системную настройку “**Звук уведомления о новом чате**” (код “OmniChatNotificationSound”).
- Нажмите [Очистить значение], чтобы удалить стандартный сигнал.
- Нажмите [Выбрать файл] и загрузите файл с вашего компьютера.
- Нажмите [Сохранить].

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:

- [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](#).
- [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.
- [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: [Настройте аутентификацию с LDAP](#).

Настройте 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* testactive directory.com	Интервал 1 синхронизации (часов)*
Логин администратора* Administrator	<input type="checkbox"/> Синхронизировать только группы
Пароль* *****	<input checked="" type="checkbox"/> Раздавать лицензии
Тип аутентификации* Ntlm	<input type="checkbox"/> Использовать SSL

Атрибуты пользователей

Имя домена* dc=ctl,dc=com	Имя организации company
ФИО пользователя* cn	Идентификатор objectSid пользователя*
Имя пользователя* sAMAccountName	Номер телефона homePhone
Атрибут даты изменения* whenChanged	Должность title
E-mail mail	

Атрибуты групп пользователей

Название группы LDAP* cn	Идентификатор группы* objectSid
Имя домена групп* dc=ctl,dc=com	

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* (memberOf=[#LDAPGroupDN#]) группы*

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 1
синхронизации (часов)*Синхронизировать только группыРаздавать 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

Идентификатор группы* objectSid

Имя домена группы* dc=example,dc=org

Условия фильтрации

Список пользователей* (objectClass=inetOrgPerson)

Список групп* (objectClass=groupOfUniqueNames)

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

1. Настроить подключение к серверу

Укажите общие настройки подключения к серверу:

- [Имя сервера] — имя или IP-адрес сервера LDAP.
- [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. Настройте 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".

- [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:

- [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.
- [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.
- [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 OC Linux, и на OC 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.

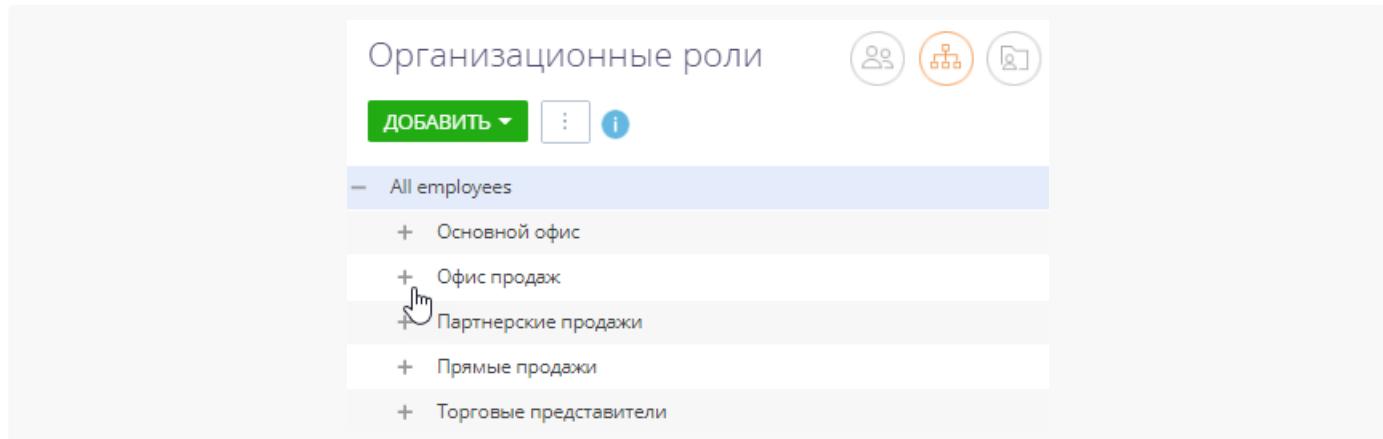
Вы можете перенести в приложение организационную структуру компании и настройки всех ролей из Active Directory после выполнения синхронизации с LDAP.

Настройте синхронизацию организационных ролей Creatio и групп Active Directory

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

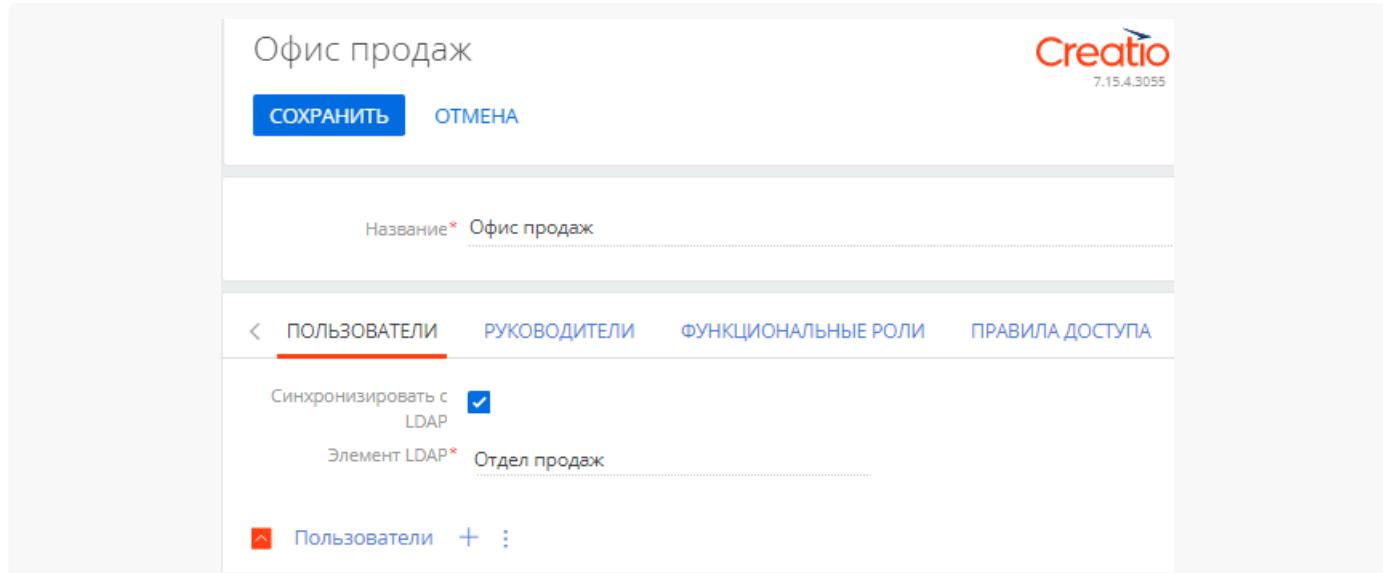
Если нужной роли в дереве групп нет, то нажмите кнопку [Добавить] и выберите “Организацию” или “Подразделение” в зависимости от того, какую роль необходимо добавить. На открывшейся странице укажите название группы.

Рис. 3 — Выбор организационной роли для настройки синхронизации



- 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



- 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

Настройте 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 [Настройте интеграцию с LDAP](#).

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

Рис. 6 — Сохранение заполненной страницы интеграции с LDAP

Новый Сервер LDAP

СОХРАНИТЬ **ОТМЕНА**

Общие настройки подключения к серверу

Имя Сервера* testactive directory.com

Логин администратора* Administrator

Пароль*

Тип аутентификации* NtLM

Интервал 1 синхронизации (часов)*

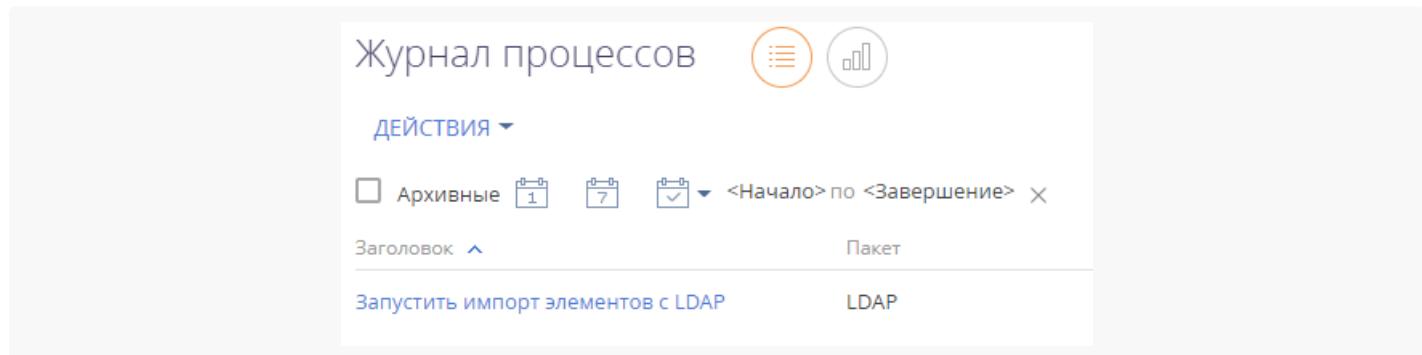
Синхронизировать только группы

Раздавать лицензии

Использовать SSL

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]

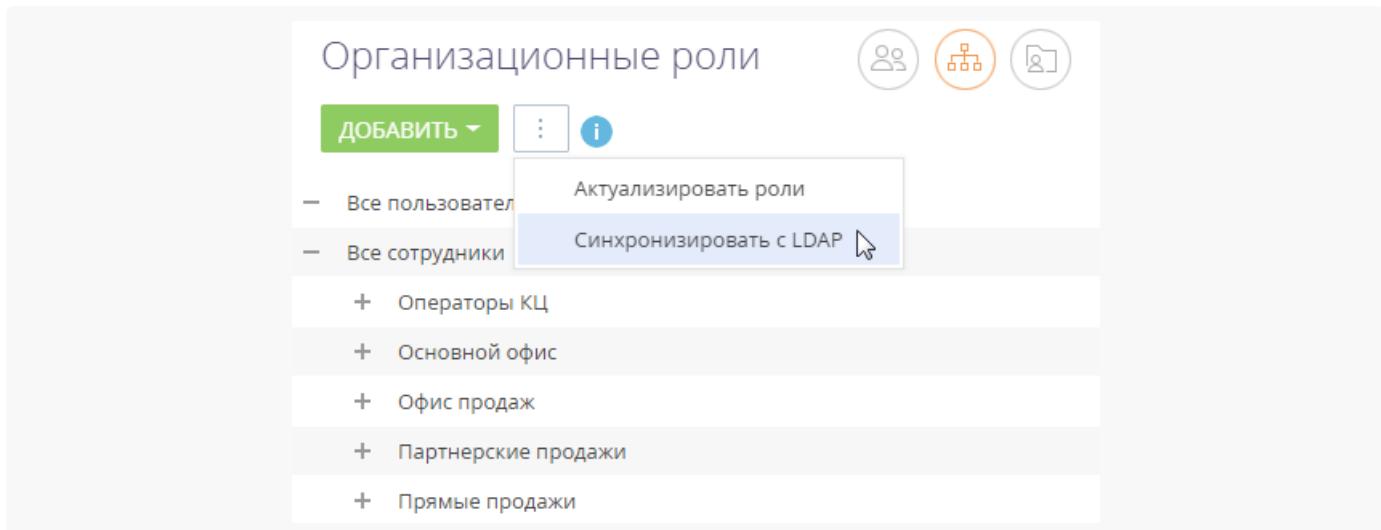
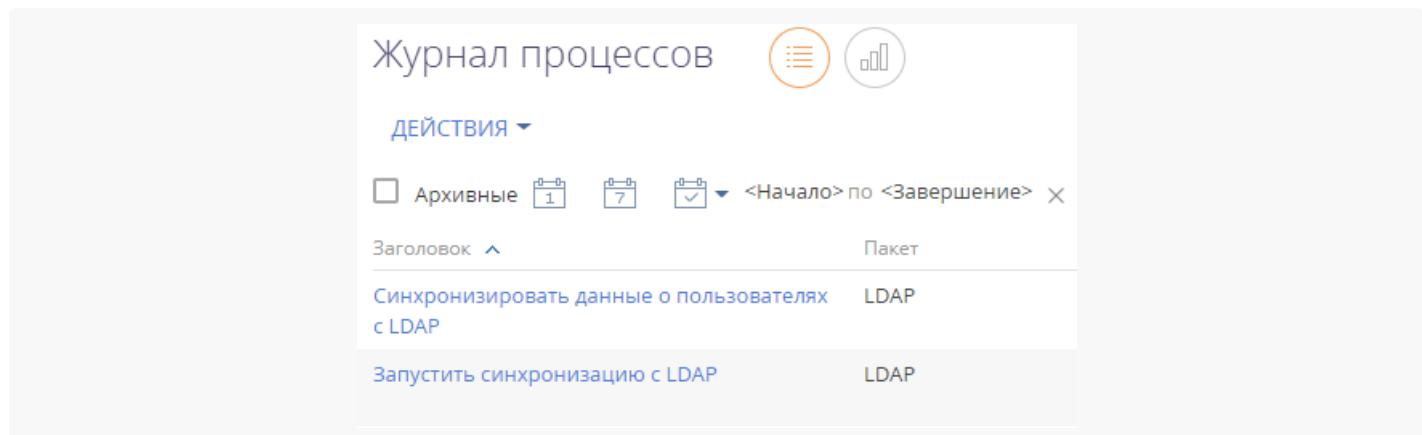


Рис. 9 — Процессы “Запустить синхронизацию с LDAP” и “Синхронизировать данные о пользователях с LDAP”



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 безопасное подключение к почтовому ящику

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Большинство почтовых провайдеров поддерживают двухэтапную аутентификацию и защищенный доступ для внешних приложений по сгенерированному провайдером паролю. Это обеспечивает безопасность вашей учетной записи и хранения персональных данных. При таком способе настройки почтовые провайдеры редко блокируют попытки подключения ящика.

Мы рекомендуем перед добавлением учетной записи в Creatio настроить защищенный доступ для внешних приложений. Настройки выполняются на стороне вашего почтового ящика и различаются в зависимости от используемого провайдера.

Инструкции по настройке пароля для доступа внешних приложений вы найдете в документации вашего почтового провайдера:

- [AOL](#).
- [GMail](#).
- [Yahoo](#).
- [Zoho](#).

После выполнения настроек в вашем почтовом ящике вы получите **пароль для внешних приложений**, который нужно будет ввести в Creatio при добавлении учетной записи почты.

Настроить верификацию для провайдера UniOne

ПРОДУКТЫ: [MARKETING](#)

Если вы планируете отправлять рассылки в Creatio с помощью провайдера UniOne, то верифицируйте ваш email-адрес и корпоративный домен.

В этом случае получатели, которые используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, увидят в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени.

Например, в строке отправителя может отобразиться подобный текст: “UniOne_Ivanov <postman1847554@usndr.com>; on behalf of; UniOne_Ivanov <ivanov.alexej@gmail.com>” либо “UniOne_Ivanov ivanov.alexej@gmail.com с домена usndr.com”.

Провайдер UniOne не позволяет отправлять тестовые письма с помощью бесплатных почтовых служб (например, Gmail, Yahoo! Mail, iCloud и т. д.).

Для использования функциональности рассылок пользователям Creatio on-site необходимо предварительно настроить интеграцию с сервисом массовых рассылок. Подробнее читайте в статье [“Настройка email-рассылок”](#).

Чтобы верифицировать ваши email-адреса и домен, выполните следующие шаги:

1. Получите SPF- и DKIM-записи, а также дополнительный параметр отправки рассылок. [Подробнее >>>](#)
2. Укажите SPF- и DKIM-записи и дополнительный параметр в DNS-зоне вашего домена. [Подробнее >>>](#)

Важно. Один домен может быть верифицирован только для одного приложения Creatio. Если вы используете два разных приложения Creatio, то вы не сможете верифицировать один и тот же домен для обоих.

3. Для корректной отправки писем на адреса группы mail.ru дополнительно настройте сервис Postmaster.mail.ru и Feedbak Loop. [Подробнее >>>](#)

Получить записи SPF, DKIM и дополнительный параметр отправки

Дополнительный параметр необходим для того, чтобы провайдер рассылок дал разрешение на отправку писем. Этот параметр настраивается один раз и действителен всех адресов данного домена. SPF- и DKIM-записи и дополнительный параметр верификации генерируются автоматически в разделе **Email**. Для получения этих записей в разделе **Email** в меню [Действия] выберите **Настройки email-рассылок** ([Рис. 1](#)).

Рис. 1 — Переход на страницу настройки email-рассылок

Настройки email-рассылок

Все необходимые записи будут автоматически сгенерированы в поле **Инструкции по настройке DKIM/SPF** на вкладке **Домены отправителя** ([Рис. 2](#)).

Рис. 2 — Ключи DKIM/SPF для указанного домена

Настройки email-рассылок

ЗАКРЫТЬ

Что я могу для вас сделать? > Creatio 7.16.4.1731

ОБЩИЕ НАСТРОЙКИ ДОМЕНЫ ОТПРАВИТЕЛЯ НАСТРОЙКА ПРОЦЕССА РАЗБОРА ОТКЛИКОВ

Домены отправителя + Обновить

Домен: yourdomain.com Домен верифицирован

☒ Домен yourdomain.com: Инструкции по настройке DKIM/SPF

Для отправки писем от вашего домена, необходимо чтобы системный администратор поменял DNS записи в хостинге вашего домена. Используйте следующие инструкции для настройки. Примеры настроек для наиболее популярных сервисов хостинга можно найти в [Академии](#).

Инструкции отличаются для разных доменов. Для получения инструкции по домену необходимо добавить и выбрать его в списке.

Выберите домен в списке на этой странице.

SPF запись. Добавьте в DNS вашего хостинга первую запись для ключа SPF. Скопируйте и вставьте туда следующий текст:

```
@ TXT v=spf1 include:spf.unisender.com include:spf.unisender.io ~all
@ TXT spf2.0/mfrom,pra include:senderid.unisender.com ~all
```

* В настройках DNS должна быть только 1 SPF запись. Если SPF запись уже существует, добавьте домен из параметра "include" выше в существующую запись. Убедитесь, что он добавлен до любых IP-адресов.

DKIM запись. Создайте в DNS вторую TXT запись для ключа DKIM. Скопируйте и вставьте туда следующий текст:

```
_domainkey TXT c=~_
v=spf1 include:spf.unisender.com include:spf.unisender.io ~all
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDNxiOLfcJKaj0wnIx5LWT Pf/eDovle
c0TX1hL6WEVIIuyNGkh7I+tPTehTjlL4I3emm882FY8cKDceV5cmyiAKgjmUmR2HvJh3V
Xcg0OChnf93QRiiepOLYTIV7itXj/A1iaXK/VPnSwtdmoyNTQjGRe2zyojeKdErPP2MEVnrOwI
DAQAB
```

* В настройках DNS может быть неограниченное количество записей DKIM.

Дополнительные настройки. Создайте в DNS домена новую TXT запись для настройки необходимых функций:

```
@ IN TXT unisender-validate-hash=a00253446bc39f3227905ed9a226262c
```

На заметку. DKIM/SPF настройки отличаются для каждого отдельного домена. Нужно добавить и выбрать каждый домен, чтобы получить разные инструкции. При использовании провайдера UniOne только домены верифицированных email-адресов могут быть добавлены на вкладку [Домены отправителя].

Выполнить настройки в DNS-зоне домена

Чтобы настроить возможность отправки писем, необходимо указать дополнительный параметр отправки в DNS-зоне вашего домена. Чтобы верифицировать почтовый домен при использовании провайдера рассылок UniOne, необходимо добавить записи SPF, DKIM и политику DMARC в DNS-зону настроек почтового домена, иначе не гарантируется высокий уровень репутации домена и доставляемости писем. Если не заполнить хотя бы один из перечисленных параметров, то домен будет считаться недействительным и отправка писем с него выполняться не будет.

Для настройки:

- Укажите дополнительный параметр в DNS-зоне вашего домена.

Скопируйте сгенерированную запись **дополнительного параметра** из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	in TXT	unione-validate-hash=XXXXXXXXXX

В приведенной записи XXXXXXXXXX — это уникальный ключ для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [Домены отправителя].

Если ключ не был сгенерирован, обратитесь в службу поддержки Creatio.

В зависимости от DNS-редактора в поле “Host / Name” DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

- Укажите SPF-записи в DNS-зоне вашего домена.

- Если в DNS-зоне вашего домена еще нет **SPF-записи**, вам нужно ее скопировать из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	TXT	v=spf1 include:spf.unisender.com ~all
@	TXT	spf2.0/mfrom,pra include:senderid.unisender.com ~all

- Если TXT-запись с SPF информацией уже существует, то в конец первой и второй строк этой записи, перед последним оператором (как правило, это **?all**, **~all**, или **-all**), необходимо добавить:

Название	Тип	Значение
Запись SPF1 (первая строка)	TXT	include:spf.unisender.com
Запись SPF2 (вторая строка)	TXT	include:senderid.unisender.com

В зависимости от DNS-редактора в поле "Имя" DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

Важно. UniOne выделяет 24 часа на проверку домена после генерации ключей SPF/DKIM. Если процесс задерживается, свяжитесь со службой поддержки Creatio, чтобы успешно завершить проверку.

- Укажите DKIM-запись в DNS-зоне вашего домена и выполните соответствующую настройку записей DKIM:

Скопируйте сгенерированную запись **DKIM** из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
_domainkey	TXT	o=~
us._domainkey	TXT	k=rsa; p=XXXXXXXXXXXXXXXXXXXXXX

В приведенной записи XXXXXXXXXXXXXXXXXXXX — это уникальный ключ для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [Домены отправителя].

- Настройте DMARC в DNS-зоне вашего домена

Проверка DMARC добавляется только после того, как были добавлены записи SPF и DKIM, и сообщает серверу-получателю, что делать с письмами, отправленными с домена, который не был верифицирован. Для UniOne настройка политики DMARC является необязательной, но рекомендуемой для повышения репутации домена. Чтобы активировать DMARC, добавьте в записи DNS домена правило в виде записи TXT:

Название	Тип	Значение
_dmarc	TXT	v=DMARC1;p=none;

Тег **v** указывает версию протокола, а **p** — способ обработки писем, которые не прошли проверку. Больше информации о протоколе в доступно в статье о [DMARC](#) в Википедии.

Настроить корректную отправку писем на адреса группы mail.ru

При отправке рассылок на адреса группы mail.ru, например, inbox.ru, mail.ua, list.ru, bk.ru и т. д., необходимо выполнить дополнительные настройки:

- Добавить домены, с которых отправляются ваши рассылки, в сервис Postmaster.mail.ru.
- Настроить Feedback Loop (FBL).

На заметку. О механизме получения обратной связи Feedback Loop читайте в статье “[Как и зачем отслеживать отклики “Отправлено в спам”?](#)”.

Отсутствие этих настроек приведет к тому, что в UniOne и Creatio не будут получены отклики почтовой системы на письма, помеченные получателями как спам. Повторная отправка рассылок таким получателям может повлиять на репутацию отправителя и привести к блокировке вашего домена почтовым сервисом.

Для настройки:

1. Зарегистрируйте новый почтовый ящик на Mail.ru и войдите в созданную учетную запись.
2. Перейдите по адресу <https://postmaster.mail.ru/add/>. Используя инструкцию на странице, добавьте домены, с которых вы отправляете рассылки.
3. На странице <https://postmaster.mail.ru/settings/> настройте адреса для получения обратной связи по откликам “Это спам” с помощью механизма Feedback Loop:
 - a. Для каждого вашего домена укажите адрес в формате fbl@ваш_домен. На него будут отправляться письма, на которые жалуются пользователи, в формате Abuse Reporting Format.
 - b. Настройте автоматическое перенаправление писем с этого адреса на адрес fbl@unisender.com для обработки.

Добавить почтовый провайдер IMAP/SMTP

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

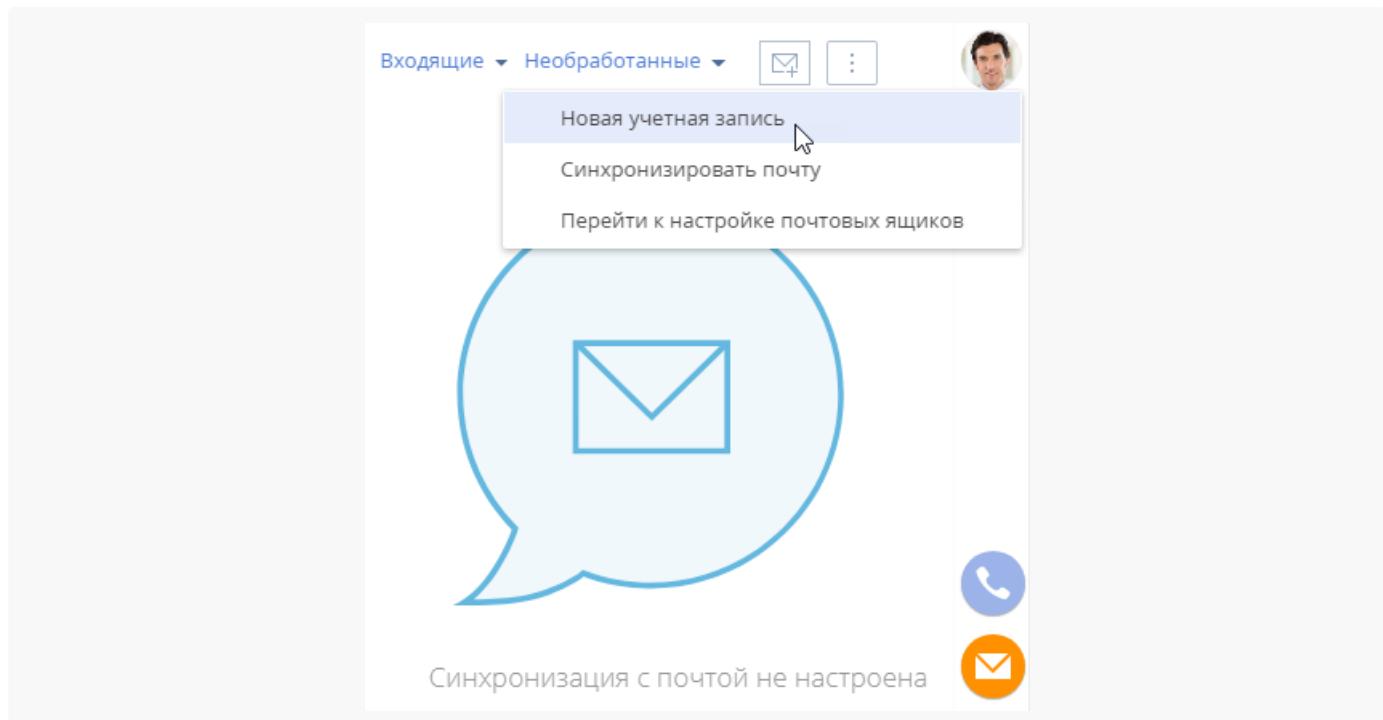
Добавить почтовый провайдер IMAP/SMTP можно несколькими способами.

Способ 1. Добавить провайдер IMAP/SMTP из вкладки [Email] коммуникационной панели

На заметку. Для добавления новой учетной записи вы также можете в меню кнопки  выбрать [Перейти к настройке почтовых ящиков] и на открывшейся странице нажать кнопку [Добавить].

1. Откройте коммуникационную панель и перейдите на вкладку [Email] по кнопке .
2. Нажмите  и выберите действие [Новая учетная запись] ([Рис. 1](#)).

Рис. 1— Добавление новой учетной записи



3. В открывшемся окне введите электронный адрес и нажмите кнопку [Далее].
4. Нажмите кнопку **Добавить провайдер**.

На заметку. Для автоматического распознавания почтового провайдера по доменному имени добавьте домены нового провайдера в справочник [Домены почтовых провайдеров]. В результате при настройке учетной записи почты пользователям не придется указывать почтового провайдера вручную.

5. На открывшейся странице нажмите кнопку [Добавить] ([Рис. 2](#)).

Рис. 2— Добавление почтового провайдера

Настройки почтового ящика

ПОЧТОВЫЕ СЕРВИСЫ

Почтовый сервис	Тип
GMail	IMAP
AOL mail	IMAP
Zoho	IMAP
Office 365	Exchange
Yahoo	IMAP
Mail.ru	IMAP
Yandex.ru	IMAP

ДОБАВИТЬ

6. На открывшейся странице выберите тип почтового сервиса — IMAP.
7. Введите два обязательных параметра: адрес сервера входящей почты (IMAP) в формате `imap@domain.com` и адрес сервера исходящей почты (SMTP) в формате `smtp@domain.com` ([Рис. 3](#)).

Рис. 3— Настройки почтового провайдера IMAP/SMTP

Добавить сервис

ПРИМЕНЕНИЕ **ОТМЕНА**

Настройки сервиса

Тип почтового сервиса
IMAP

Сервер входящей почты (IMAP)

Настройки почтового сервиса, необходимые для получения почты. Укажите адрес и порт почтового сервера, а также выберите параметры безопасности передачи данных

Адрес сервера *
imap@domain.com

Порт
993

Безопасность
SSL/TLS

Сервер исходящей почты (SMTP)

Настройки почтового сервиса, необходимые для отправки почты. Укажите адрес и порт почтового сервера, а также выберите параметры безопасности передачи данных

Адрес сервера *
smtp@domain.com

Порт
465

Безопасность
SSL/TLS

Дополнительные настройки

8. Другие настройки почтового сервиса IMAP/SMTP будут заполнены автоматически. Вы можете их поменять, выбрав в каждом поле нужный вариант из выпадающего списка, чтобы настроить порт почтового сервера, а также параметры безопасности передачи данных.

Для настройки порта сервера входящей почты:

- Выберите “**143**”, если вы хотите использовать порт без шифрования.
- Выберите “**993**”, если вы хотите использовать порт для безопасного соединения.

Для настройки параметров безопасности сервера входящей почты:

- a. Выберите “**SSL/TLS**”, чтобы использовать стандартный протокол защиты данных.
- b. Выберите “**STARTTLS**”, если вы хотите использовать расширение обычного протокола.
- c. Выберите “**Нет**”, если вы хотите отключить настройки защиты данных входящей почты.

Для настройки порта сервера исходящей почты:

- a. Выберите “**587**”, если вы хотите использовать порт без шифрования.
- b. Выберите “**455**”, если вы хотите использовать порт для безопасного соединения.

Для настройки параметров безопасности сервера исходящей почты:

- a. Выберите “**SSL/TLS**”, чтобы использовать стандартный протокол защиты данных.
- b. Выберите “**Нет**”, если вы хотите отключить настройки защиты данных исходящей почты.

9. Заполните дополнительные настройки.

Для настройки формата логина:

- a. Выберите [*Формировать имя вручную*], если пользователь должен самостоятельно ввести email-адрес и имя пользователя.
- b. Выберите [*Использовать email*], если в качестве логина должен использоваться полный email-адрес, например, example@google.com.
- c. Выберите [*Использовать имя почтового ящика*], если в качестве логина должна использоваться часть email-адреса до символа “@”. Например, для email-адреса “example@google.com” логином будет “example”.

Для настройки метода аутентификации:

- a. Выберите “**Basic**” для базовой аутентификации с использованием имени пользователя и пароля, закодированных с помощью Base64.
- b. Выберите “**OAuth 2.0**”, если хотите предоставить сервису ограниченный доступ к защищенным ресурсам пользователя без необходимости передачи логина и пароля. Заполните обязательные поля [*Идентификатор приложения (клиент)*] и [*Секрет клиента*]. [*Идентификатор приложения (клиент)*] выдается сервером авторизации почтового сервиса. В документации и API идентификатор приложения может называться Product ID (идентификатор продукта). [*Секрет клиента*] — секретный ключ, предоставленный сервером авторизации. В документации и API секретный ключ может также называться Product key (ключ продукта).

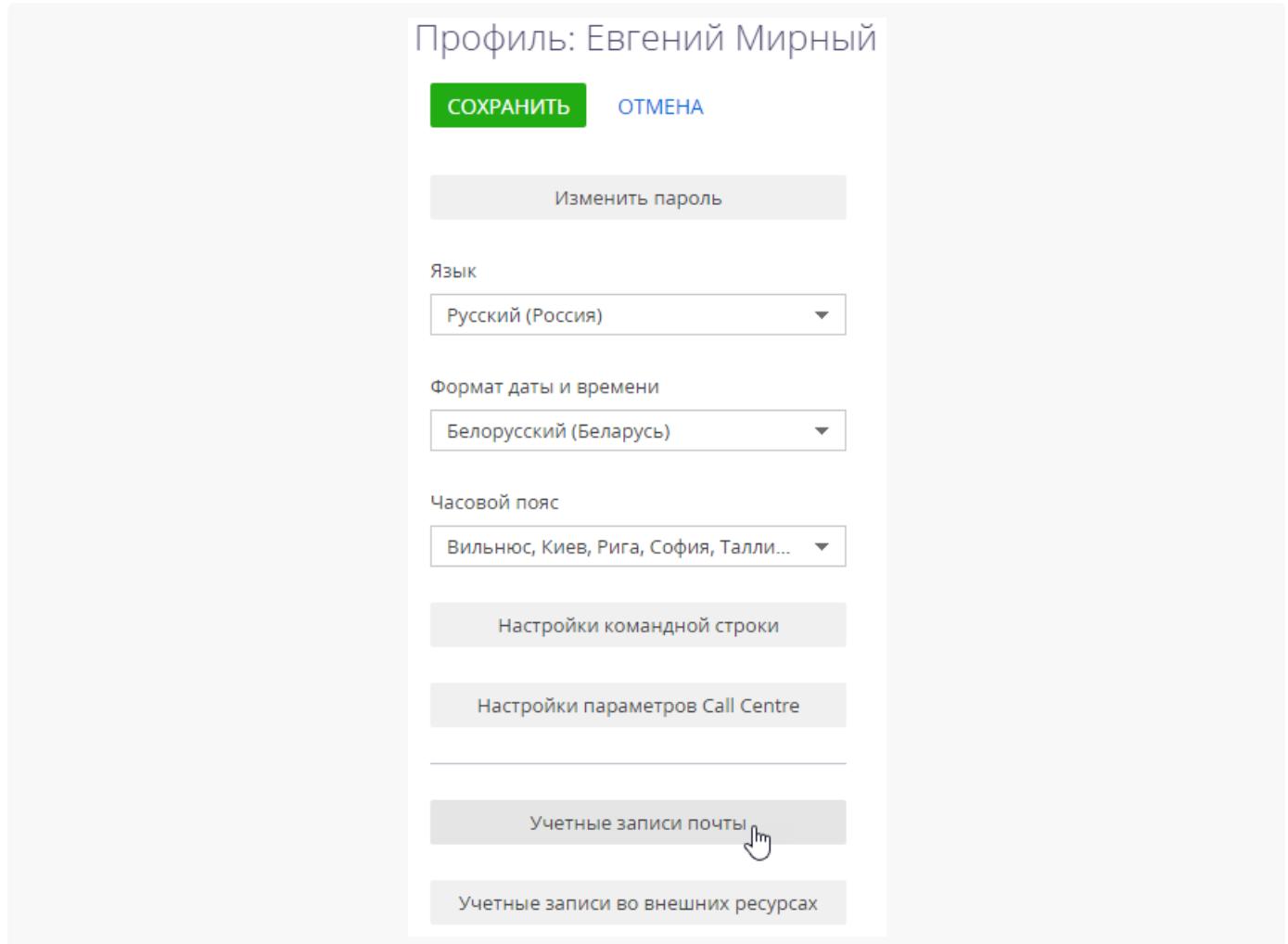
10. Сохраните изменения по кнопке [*Применить*].

В результате пользователи системы смогут использовать почтовые ящики данного провайдера для отправки и получения email-сообщений.

Способ 2. Добавить провайдер IMAP/SMTP из профиля пользователя

1. Откройте страницу профиля пользователя, например, кликнув по ссылке [*Профиль*] на главной странице приложения.
2. Кликните по полю [*Учетные записи почты*] ([Рис. 1](#)).

Рис. 1— Учетные записи почты



3. В открывшемся окне нажмите кнопку [Добавить].
4. Для завершения настройки **выполните шаги 3-10**, описанные выше в **Способе 1**.

На заметку. Чтобы удалить почтовый сервис, сначала нужно удалить все почтовые ящики, которые с ним работают.

Лицензировать Creatio

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Доступ к функциональности Creatio получают только лицензированные пользователи.

Этапы лицензирования в Creatio:

1. Лицензирование приложения. [Подробнее >>>](#)
2. Распределение существующих лицензий между учетными записями пользователей. [Подробнее >>>](#)

Эти операции выполняются в разделе [*Менеджер лицензий*] (Рис. 1).

Рис. 1 — Раздел [*Менеджер лицензий*]

The screenshot shows the 'Менеджер лицензий' (License Manager) page. At the top left is a 'ЗАКРЫТЬ' (Close) button. To its right is a 'ДЕЙСТВИЯ' (Actions) dropdown menu with options: 'Запросить' (Request), 'Загрузить' (Import), and 'Удалить' (Delete). Below the menu is a search bar with the placeholder 'Поиск' (Search). The main area contains a table with the following columns: Название (Name), Тип (Type), Дата начала (Start Date), Дата (End Date), Статус (Status), and Всего (Total). The table lists ten entries, all of which are 'Активна' (Active) and have a value of '5' in the 'Всего' column.

Название	Тип	Дата начала	Дата	Статус	Всего
receivables management for creatio cloud	Серверная	06.04.2021	31.08.2021	Активна	5
automatic data import from excel file for creatio cloud	Серверная	24.02.2021	31.08.2021	Активна	5
zabbix connector for creatio cloud	Серверная	19.02.2021	31.08.2021	Активна	5
no-code reports for creatio cloud	Именная	10.02.2021	31.08.2021	Активна	5
printable forms filtering for creatio cloud	Серверная	04.02.2021	31.08.2021	Активна	5
advertising creatio enterprise cloud	Именная	27.01.2021	31.08.2021	Активна	5
colored activities by tags for creatio cloud	Серверная	30.12.2020	31.08.2021	Активна	5
control visits for creatio cloud	Именная	11.12.2020	31.08.2021	Активна	5
auto-generating print forms for creatio cloud	Серверная	27.11.2020	31.08.2021	Активна	5
mango office sms for creatio cloud	Серверная	04.11.2020	31.08.2021	Активна	5

Если истек срок действия лицензий, то при попытке входа в систему пользователя, который включен в организационную роль “Системные администраторы”, менеджер лицензий откроется автоматически.

На заметку. Чтобы просматривать, раздавать и отзывать лицензии, у вас должны быть настроены права доступа на выполнение системной операции “Управление лицензиями пользователей” (код “CanManageLicUsers”). Подробнее: [Настроить права доступа на системные операции](#).

Добавить лицензии в приложение

Процедура лицензирования программного обеспечения одинакова для всех типов лицензий, использующихся в Creatio.

При покупке лицензий, продлении действия существующих лицензий и обновлении on-site приложения Creatio:

1. Сформируйте запрос на лицензии и отправьте его в службу технической поддержки.
2. Загрузите в систему файл, полученный в ответ.

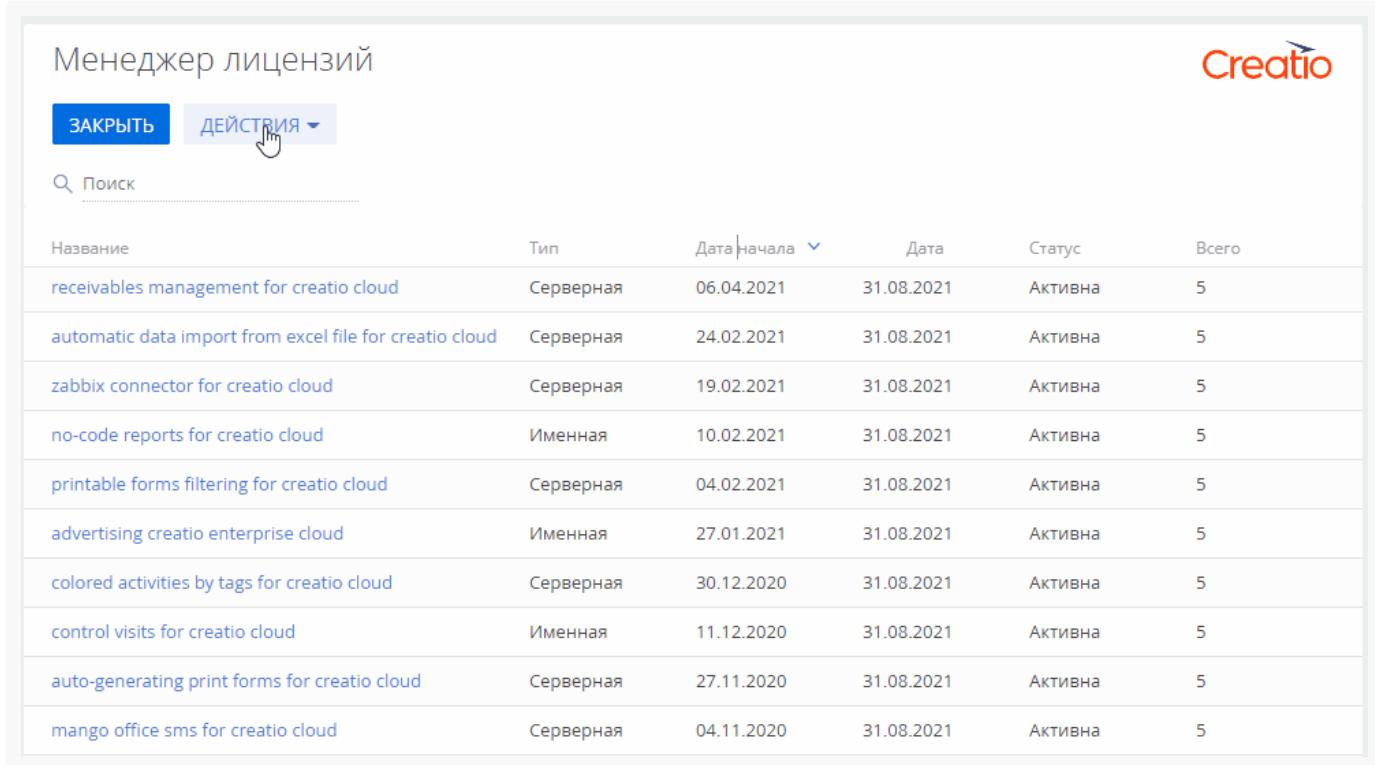
Начиная с версии 7.17.4 данную процедуру необходимо выполнять также и при обновлении on-site приложения Creatio на новую версию.

Сформировать запрос на получение лицензий

1. Перейдите в дизайнер системы по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
3. Нажмите [Действия] —> [Запросить].
4. Введите идентификатор компании для запроса лицензий. Идентификатор предоставляется при покупке. Вы также можете запросить его в службе поддержки Creatio.
5. Нажмите кнопку [Сформировать запрос] (Рис. 2).

В результате будет создан и загружен файл запроса лицензий в формате *.tlr.

Рис. 2 — Запрос на получение лицензий



Название	Тип	Дата начала	Дата	Статус	Всего
receivables management for creatio cloud	Серверная	06.04.2021	31.08.2021	Активна	5
automatic data import from excel file for creatio cloud	Серверная	24.02.2021	31.08.2021	Активна	5
zabbix connector for creatio cloud	Серверная	19.02.2021	31.08.2021	Активна	5
no-code reports for creatio cloud	Именная	10.02.2021	31.08.2021	Активна	5
printable forms filtering for creatio cloud	Серверная	04.02.2021	31.08.2021	Активна	5
advertising creatio enterprise cloud	Именная	27.01.2021	31.08.2021	Активна	5
colored activities by tags for creatio cloud	Серверная	30.12.2020	31.08.2021	Активна	5
control visits for creatio cloud	Именная	11.12.2020	31.08.2021	Активна	5
auto-generating print forms for creatio cloud	Серверная	27.11.2020	31.08.2021	Активна	5
mango office sms for creatio cloud	Серверная	04.11.2020	31.08.2021	Активна	5

6. Для версий 7.17.4 и выше: в поле [Версия лицензии] укажите версию, на которую планируется обновление.
7. Отправьте файл запроса лицензий в службу технической поддержки Creatio. В ответ вам будет отправлен файл с данными о приобретенных лицензиях.

Запросить лицензии также можно в разделе [Пользователи системы] по действию [Запросить лицензии] (Рис. 3).

Рис. 3 — Запрос на получение лицензий

Имя пользователя	Активен	Должность	Рабочий телефон	ФИО
Шевченко Виталий	Да	Руководитель отдела	5537	Шевченко Виталий
Портальный пользователь 1	Да	Директор	+7 495 277 07 70	Елисеев Андрей Николаевич
Тарасов Олег	Да	Директор	+7 495 780 80 80	Тарасов Олег Константинович
Administrator	Да			Administrator
N.Sem	Да	Руководитель отдела	+7 915 496 24 50	Швец Ирина
SysPortalConnection	Да			SysPortalConnection
Омелин Виталий	Да		5316	Омелин Виталий
Наринская Виктория	Да	Руководитель отдела	+7 495 738 16 95	Наринская Виктория
Петров Василий	Да	Специалист	4618	Петров Василий
Федоров Артем	Да	Специалист	5270	Федоров Артем
Тириллов Сергей Петрович	Да	Директор по продажам	+7 499 550 43 42	Тириллов Сергей

Загрузить лицензии в приложение

- Сохраните на жестком диске файл лицензионного ключа, полученный от службы технической поддержки.
- Перейдите в дизайнер системы по кнопке
- В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
- Нажмите [Действия] —> [Загрузить] (Рис. 4).

Рис. 4 — Загрузка файла с лицензионным ключом в Creatio

Менеджер лицензий

ДЕЙСТВИЯ

Название	Тип	Дата начала	Дата	Статус	Всего
Advanced schedule for creatio server cloud	Серверная	18.09.2019	31.08.2021	Активна	5
Chat2Desk connector cloud subscription	Именная	26.02.2018	31.08.2021	Активна	5
File manager for creatio server cloud subscription	Серверная	11.12.2019	31.08.2021	Активна	5
File manager for creatio user cloud subscription	Именная	16.11.2018	31.08.2021	Активна	5
SMS-mailing for creatio cloud	Серверная	20.02.2019	31.08.2021	Активна	5
a4f dadata connector for creatio cloud	Серверная	28.09.2018	31.08.2021	Активна	5
account verification for creatio cloud	Серверная	25.10.2018	31.08.2021	Активна	5
additional details in product selection page for creati...	Серверная	05.08.2019	31.08.2021	Активна	5
adobe sign connector for creatio cloud	Серверная	17.11.2017	31.08.2021	Активна	5
advanced fields patterns for creatio cloud	Серверная	07.07.2020	31.08.2021	Активна	5

5. Укажите путь к сохраненному файлу.

Запросить лицензии также можно в разделе [Пользователи системы] по действию [Загрузить лицензии] (Рис. 5).

Рис. 5 — Загрузка файла с лицензионным ключом в Creatio

Пользователи

ДЕЙСТВИЯ

- Выбрать несколько записей
- Выбрать все
- Выдать лицензии
- Отозвать лицензии
- Загрузить лицензии**
- Запросить лицензии
- Экспорт в Excel
- Актуализировать роли

В результате новые лицензии будут загружены в систему. При этом может увеличиться общее количество лицензий, а также будут продлены сроки действия лицензий.

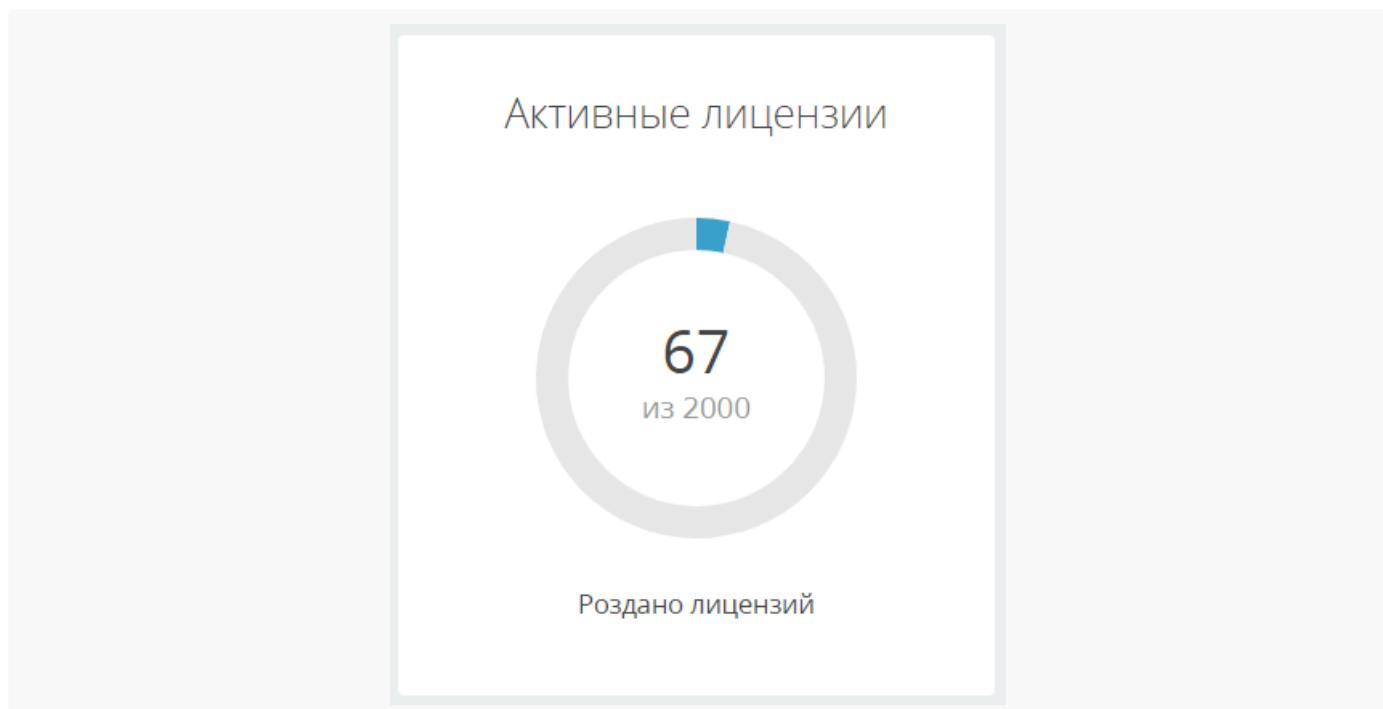
Распределить лицензии между пользователями

Чтобы пользователь мог войти в систему, необходимо выполнить лицензирование его учетной записи. Администратор системы может в любое время перераспределить существующие лицензии. Количество активных и доступных лицензий отображается на странице лицензирования продукта и зависит от типа лицензии (Рис. 6 и 7).

В Creatio используются следующие типы лицензий:

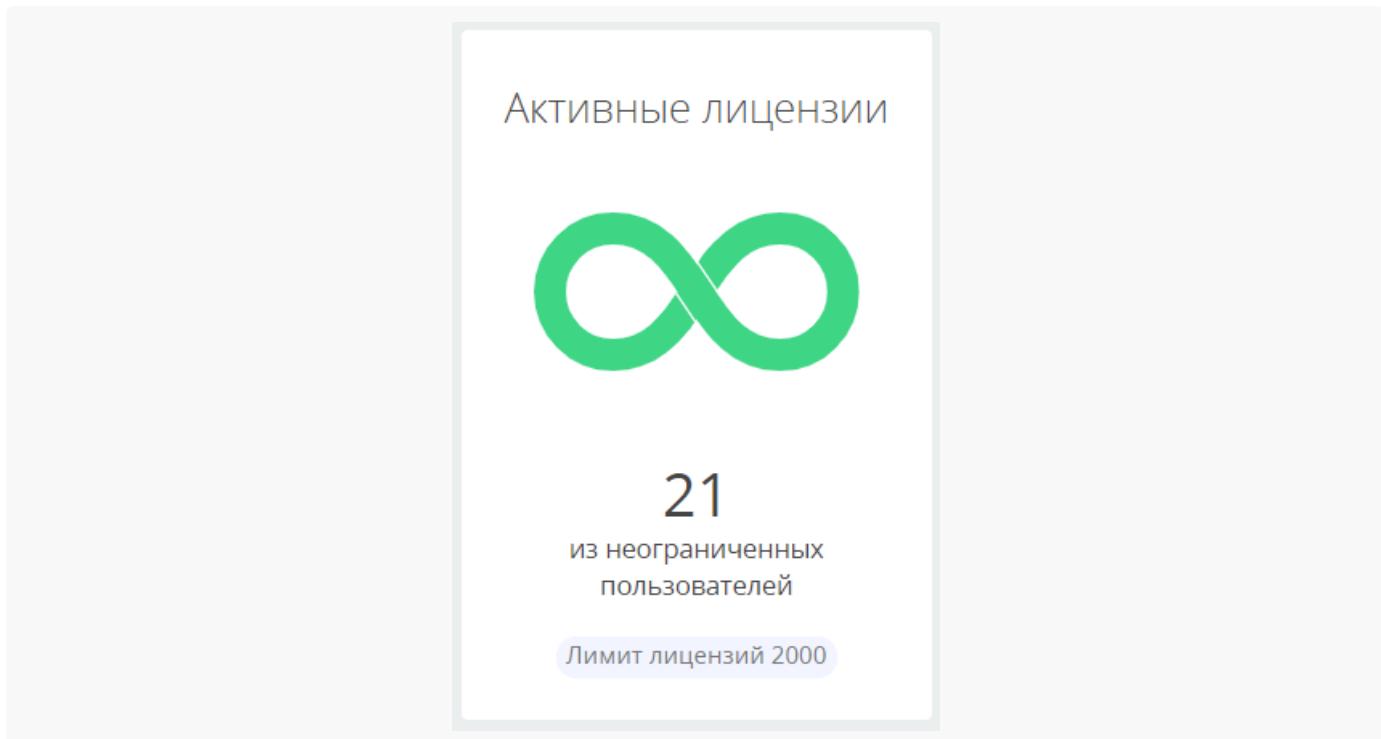
- **Именные лицензии** предоставляют доступ к продукту для конкретных пользователей. Эти лицензии привязываются к учетным записям. При распределении именных лицензий необходимо учитывать, что количество предоставленных лицензий не может превышать количество приобретенных лицензий.

Рис. 6 — Количество именных лицензий



- **Серверные лицензии** предоставляют доступ к дополнительной функциональности системы, например, к функциональности телефонии. В отличие от именной лицензии, серверную лицензию можно привязать к неограниченному количеству учетных записей.

Рис. 7 — Количество серверных лицензий



Распределить лицензии можно в разделах [*Менеджер лицензий*] или [*Пользователи системы*]. Если необходимо лицензировать сразу несколько учетных записей пользователей, то используйте раздел [*Менеджер лицензий*]:

1. Перейдите в дизайнер системы по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
3. Выберите лицензию из списка. Чтобы быстро найти нужный продукт по названию, используйте форму поиска и сортировку реестра по колонкам.
4. Кликните по названию продукта.

Откроется страница лицензирования продукта. Здесь вы можете увидеть тип лицензии, дату ее начала и завершения, статус, количество доступных лицензий, а также распределить существующие лицензии между пользователями.

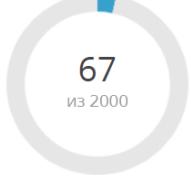
5. Нажмите кнопку [*Добавить*] и выберите пользователей, которым вы хотите выдать лицензии (Рис. 8).

Рис. 8 — Добавление пользователей в менеджере лицензий

Продукт sales creatio enterprise edition on-site

[ЗАКРЫТЬ](#)

Активные лицензии



67
из 2000

Роздано лицензий

Лицензии

Название	Тип	Дата начала	Дата завершения	Статус	Всего
sales creatio enterprise edition on-site	Именная	09.05.2016	31.12.2021	Активна	2 000

Пользователи с лицензией

Поиск

<input type="checkbox"/> Пользователь	Email	Должность
<input type="checkbox"/> Жаврук Виталий Алексеевич	v.zhavruk@gmail.com	Специалист
<input type="checkbox"/> Елисеев Андрей Николаевич	a.eliseev@alfabizness.com	Специалист
<input type="checkbox"/> Варенская Ольга Константиновна	olga.ravenskaya@gmail.com	Специалист
<input type="checkbox"/> Валевский Андрей Георгиевич	a_vakevsky@gmail.com	Специалист
<input type="checkbox"/> Авдоров Сергей Валентинович	s.avdorov@yahoo.com	Специалист

[+ Добавить](#)

Обратите внимание, что число указанных пользователей не должно быть больше количества лицензий. Количество доступных/использованных лицензий можно отслеживать на круговой диаграмме в левой части экрана (Рис. 8).

При необходимости вы можете отзывать лицензии, чтобы затем перераспределить их другим пользователям.

- Чтобы отозвать лицензии, выберите пользователей из списка и нажмите кнопку [Отозвать лицензии] (Рис. 9).

Рис. 9 — Отзыв лицензий

Лицензии

Название ^	Тип	Дата начала	Дата завершения	Статус	Всего
sales creatio enterprise edition on-site	Именная	09.05.2016	31.12.2021	Активна	2 000

Пользователи с лицензией

Поиск

<input checked="" type="checkbox"/> Пользователь ^	Email	Должность
<input checked="" type="checkbox"/> Жаврук Виталий Алексеевич	v.zhavruk@gmail.com	Специалист
<input type="checkbox"/> Елисеев Андрей Николаевич	a.eliseev@alfabizness.com	Специалист
<input checked="" type="checkbox"/> Варенская Ольга Константиновна	olga.ravenskaya@gmail.com	Специалист
<input type="checkbox"/> Валевский Андрей Георгиевич	a_vakevsky@gmail.com	Специалист
<input type="checkbox"/> Авдоров Сергей Валентинович	s.avdorov@yahoo.com	Специалист

[+ Добавить](#) [Удалить](#) [Отозвать лицензии \(2\)](#)

Вы также можете навести курсор на строку с именем пользователя, у которого вы хотите отозвать лицензию, и нажать кнопку  (Рис. 10).

Рис. 10 — Отзыв лицензий

Пользователи с лицензией

Поиск

<input type="checkbox"/> Пользователь ^	Email	Должность	Удалить
<input type="checkbox"/> Жаврук Виталий Алексеевич	v.zhavruk@gmail.com	Специалист	
<input type="checkbox"/> Елисеев Андрей Николаевич	a.eliseev@alfabizness.com	Специалист	
<input type="checkbox"/> Варенская Ольга Константиновна	olga.ravenskaya@gmail.com	Специалист	
<input type="checkbox"/> Валевский Андрей Георгиевич	a_vakevsky@gmail.com	Специалист	
<input type="checkbox"/> Авдоров Сергей Валентинович	s.avdorov@yahoo.com	Специалист	

7. Сохраните изменения по кнопке [Применить].
8. Аналогичным образом распределите лицензии на другие приобретенные продукты.
9. Закройте окно менеджера лицензий.

В результате для выбранных учетных записей будут предоставлены либо отозваны лицензии Creatio.

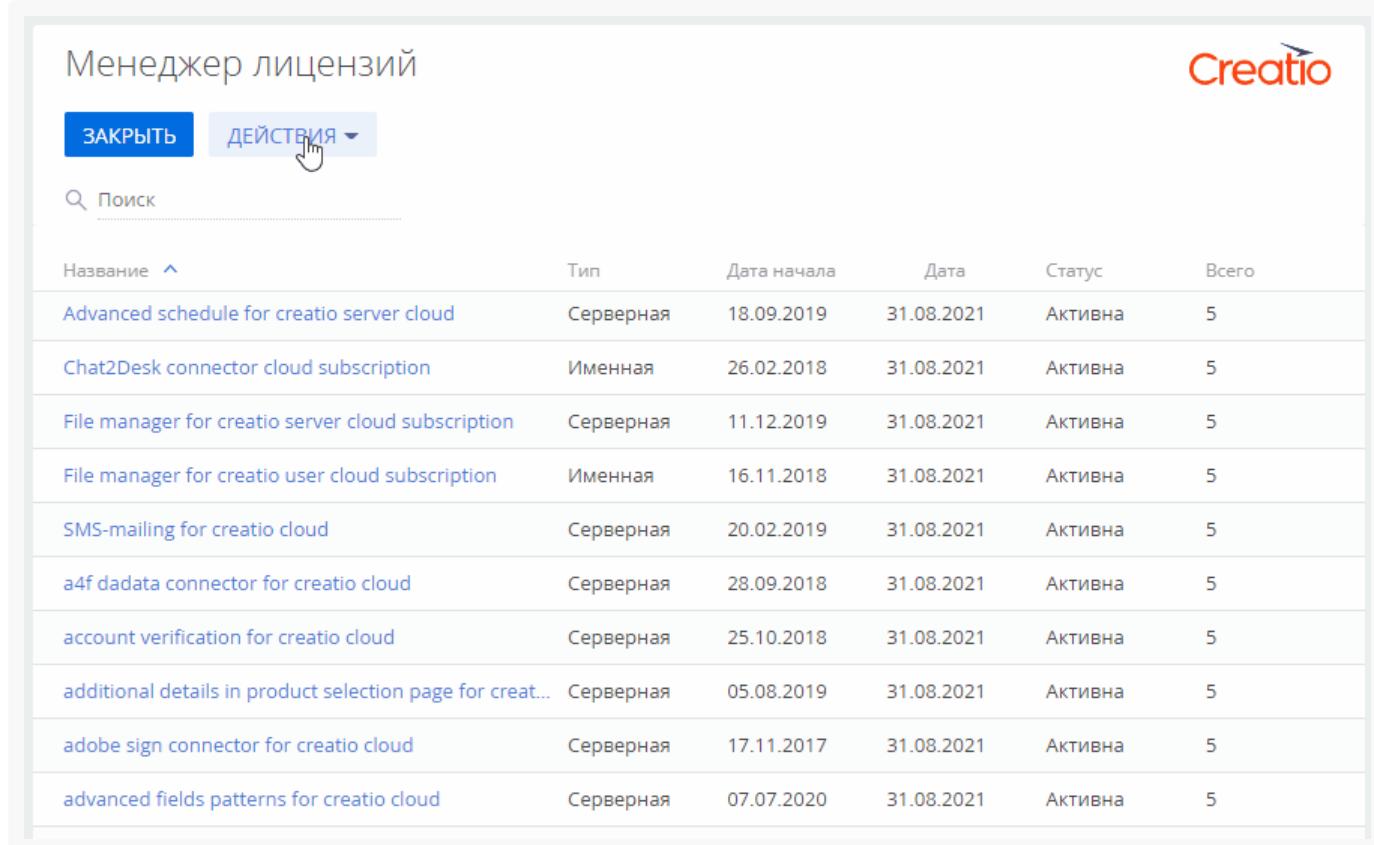
Удалить лицензии в приложении

Есть случаи, когда необходимо удалить лицензии (например, при переводе приложения в демо-режим).

Чтобы **удалить лицензии в приложении**:

- Перейдите в дизайнер системы по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
- Нажмите [Действия] —> [Удалить] (Рис. 11).

Рис. 11 — Удалить лицензии



Название	Тип	Дата начала	Дата	Статус	Всего
Advanced schedule for creatio server cloud	Серверная	18.09.2019	31.08.2021	Активна	5
Chat2Desk connector cloud subscription	Именная	26.02.2018	31.08.2021	Активна	5
File manager for creatio server cloud subscription	Серверная	11.12.2019	31.08.2021	Активна	5
File manager for creatio user cloud subscription	Именная	16.11.2018	31.08.2021	Активна	5
SMS-mailing for creatio cloud	Серверная	20.02.2019	31.08.2021	Активна	5
a4f dadata connector for creatio cloud	Серверная	28.09.2018	31.08.2021	Активна	5
account verification for creatio cloud	Серверная	25.10.2018	31.08.2021	Активна	5
additional details in product selection page for creat...	Серверная	05.08.2019	31.08.2021	Активна	5
adobe sign connector for creatio cloud	Серверная	17.11.2017	31.08.2021	Активна	5
advanced fields patterns for creatio cloud	Серверная	07.07.2020	31.08.2021	Активна	5

В результате будут удалены все лицензии.

Настроить журнал изменений

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Журнал изменений используется для логирования бизнес-данных, например, чтобы отслеживать изменения цены продукта или остатка по счетам.

Для логирования системных событий, системных настроек и системных данных используется **журнал аудита**. Подробнее: [Настроить журнал аудита](#).

По умолчанию логирование журнала изменений отключено. Чтобы изменения логировались, выполните настройки, описанные в данной статье.

Настройка логирования осуществляется как в разделе [Журнал изменений], так и в любом другом разделе, справочнике или детали Creatio.

Пример. Необходимо отслеживать изменения телефонных номеров и email-адресов контактов, которые используются для идентификации клиентов.

Эта задача решается настройкой логов изменений для email-адреса, мобильного и рабочего телефонных номеров в профиле контакта.

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](#).

Способ 1. Настроить логи из раздела [Журнал изменений]

На заметку. Рекомендуем настраивать логи только тех колонок, изменения значений которых необходимо отслеживать. При объемной базе данных логирование большого количества объектов и колонок может повлиять на производительность системы.

1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Журнал изменений”.

На заметку. Для работы с разделом [Журнал изменений] у вас должны быть настроены права доступа на выполнение системной операции “Доступ к разделу “Журнал изменений” (код “CanManageChangeLog”). Подробнее: [Права доступа на системные операции](#).

3. В списке объектов системы найдите необходимый вам объект раздела, справочника или детали. В нашем примере — установите фильтр “Разделы” (Рис. 1).

Рис. 1 — Установка фильтра для выбора логируемых объектов системы

Журнал изменений

ЗАКРЫТЬ ДЕЙСТВИЯ ▾

	Название	Логируется
Все объекты	DuplicatesRuleInFolder	<input type="checkbox"/>
Разделы	DuplicatesRuleInTag	<input type="checkbox"/>
Справочники	VwBulkEmailInCampaign	<input type="checkbox"/>
"Правило поиска дублей" в тегах	BulkEmailInProgress	<input type="checkbox"/>
BulkEmail in campaign view	BulkEmailRecipientMacro	<input type="checkbox"/>
BulkEmailRecipientReplica	BulkEmailRecipientReplica	<input type="checkbox"/>
Business processes in sections	ProcessInModules	<input type="checkbox"/>
ContactFolder in campaign view	VwFolderInCampaign	<input type="checkbox"/>
DCAttribute	DCAttribute	<input type="checkbox"/>

- Выберите раздел из списка или найдите его с помощью строки поиска (Рис. 2). Кликните по названию нужного объекта системы. В нашем примере — по объекту “Контакт”.

Рис. 2 — Поиск раздела для настройки логов

Журнал изменений

ЗАКРЫТЬ ДЕЙСТВИЯ ▾

Разделы ▾ Контакт ×

Заголовок ^

Контакт 

- На открывшейся странице включите логирование, перетащив ползунок вправо.

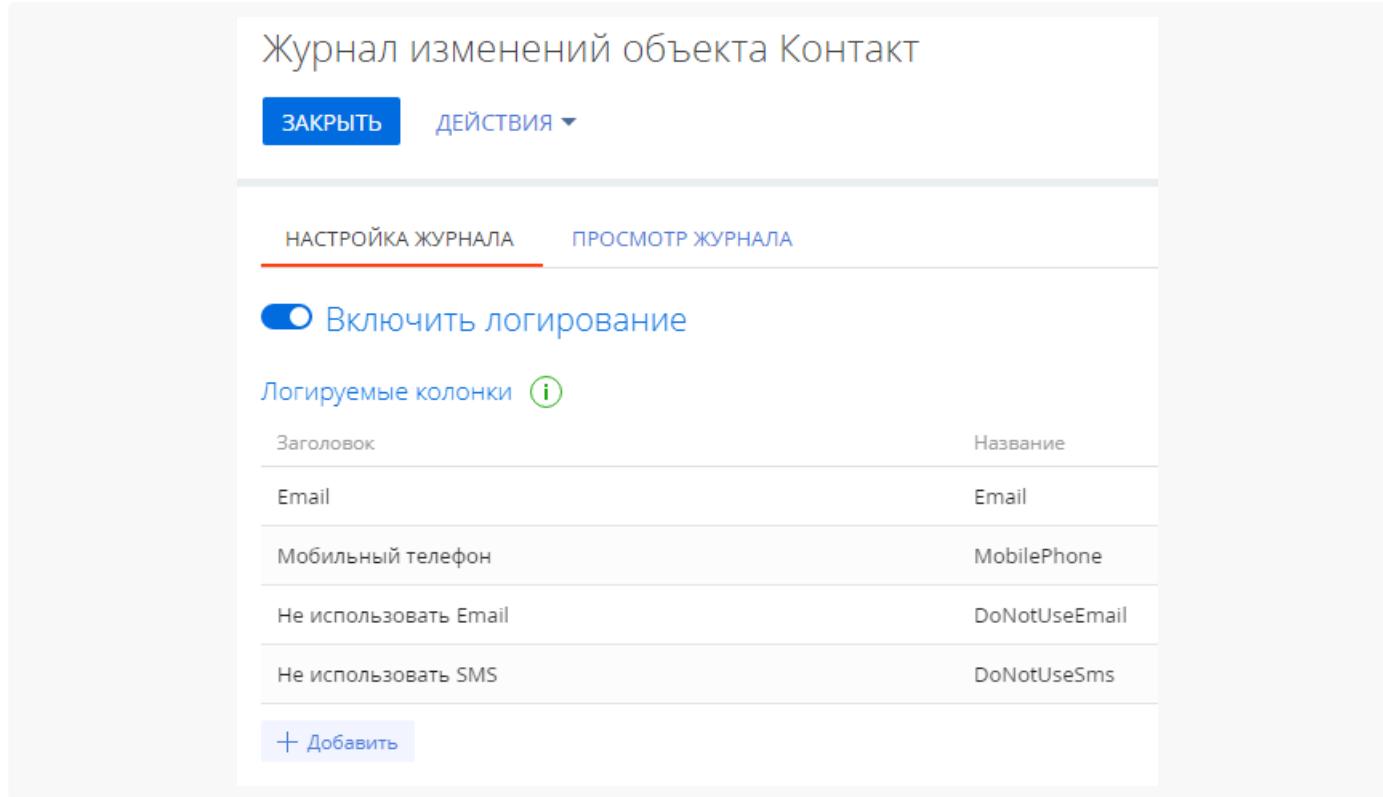
На заметку. Если вы сохраните изменения на этом этапе, то логироваться будет создание, изменение и удаление записей.

- Настройте список колонок, которые будут логироваться при изменении записи. В нашем случае это колонки [Email], [Мобильный телефон], [Рабочий телефон] (Рис. 3).

Чтобы добавить новую колонку, нажмите кнопку [Добавить]. Чтобы удалить добавленную ранее

колонку, наведите курсор на строку, содержащую название этой колонки, и нажмите кнопку .

Рис. 3 — Настройка логирования колонок



- Чтобы сохранить настройки фильтрации, нажмите кнопку [Применить].

После сохранения настроек Creatio начнет отслеживать изменения и фиксировать их в журнале изменений.

Способ 2. Настроить логи из раздела, справочника или детали

- Перейдите в нужный раздел, справочник или на деталь. В нашем примере — в раздел [Контакты].
- Нажмите [Действия] —> [Настроить журнал изменений] (Рис. 4).

Рис. 4 — Переход к настройке журнала изменений из раздела [Контакты]

The screenshot shows the 'Контакты' (Contacts) module in the Creatio application. At the top, there are navigation icons: a grid, a bar chart, and a search bar. Below the header, there's a green button labeled 'Добавить контакт' (Add contact). On the left, a list of contacts is displayed with their names, company logos, and roles. On the right, a 'Действия' (Actions) dropdown menu is open, listing various options like 'Синхронизировать контакты' (Sync contacts), 'Выбрать несколько записей' (Select multiple records), and 'Настроить журнал изменений' (Configure Change Log), which is highlighted with a blue background.

На заметку. Если у вас не отображается действие [Настроить журнал изменений], проверьте настройку прав доступа на выполнение системной операции “Доступ к разделу “Журнал изменений” (код “CanManageChangeLog”). Подробнее: [Права доступа на системные операции](#).

В результате выполнения действия вы перейдете к настройке логов журнала изменений раздела [Контакты]. Для завершения настройки **выполните шаги 5-7**, описанные в **Способе 1**.

Настроить Single Sign-On через ADFS

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

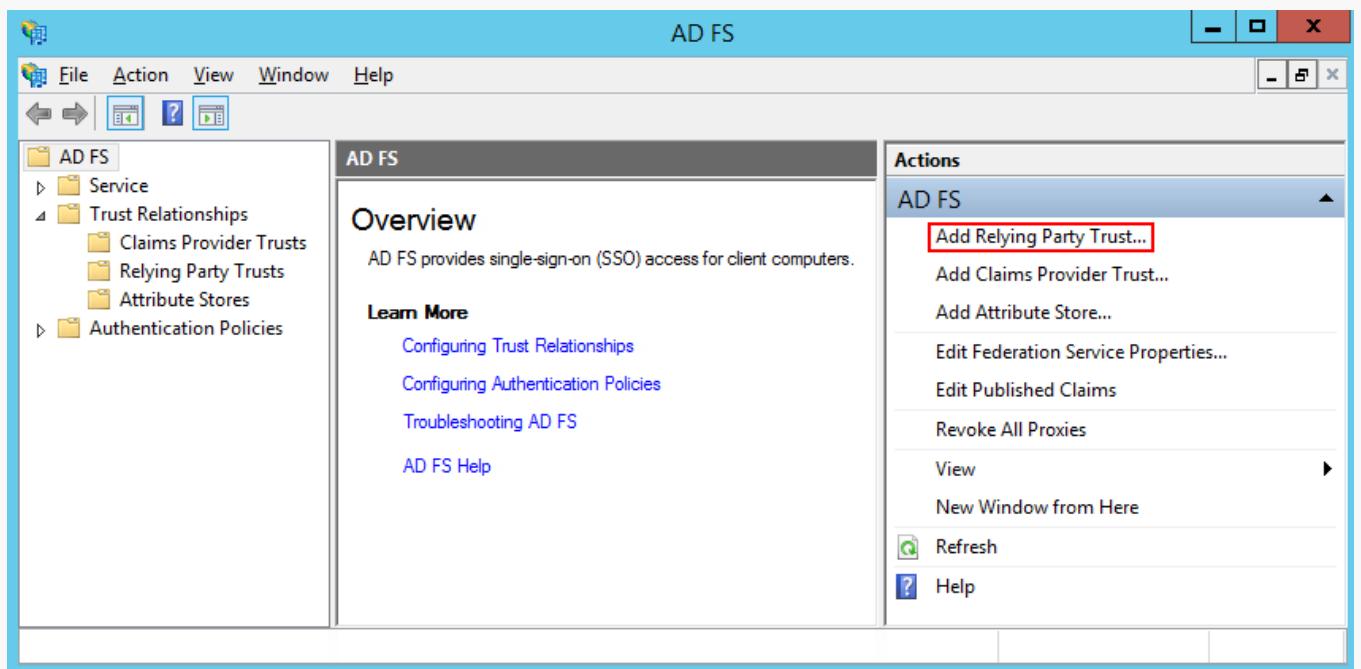
Вы можете настроить интеграцию Creatio с Active Directory Federation Services (ADFS), чтобы с ее помощью управлять возможностью единого входа для всех пользователей системы. Для этого нужно выполнить ряд настроек как на стороне ADFS, так и на стороне Creatio.

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

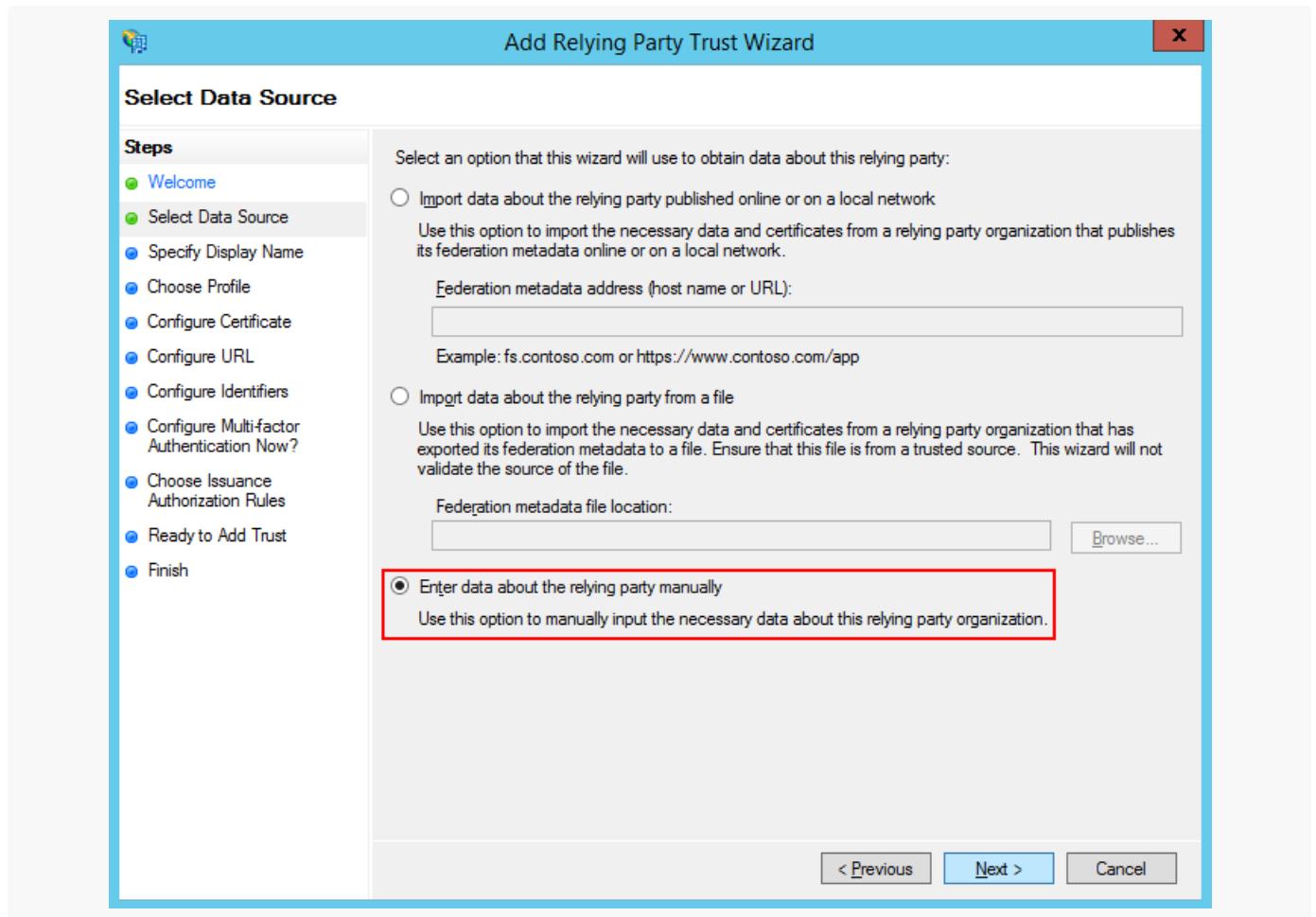
1. Добавьте в ADFS нового поставщика ресурсов (Relying Party Trusts) (Рис. 1).

Рис. 1 — Добавление нового поставщика ресурсов



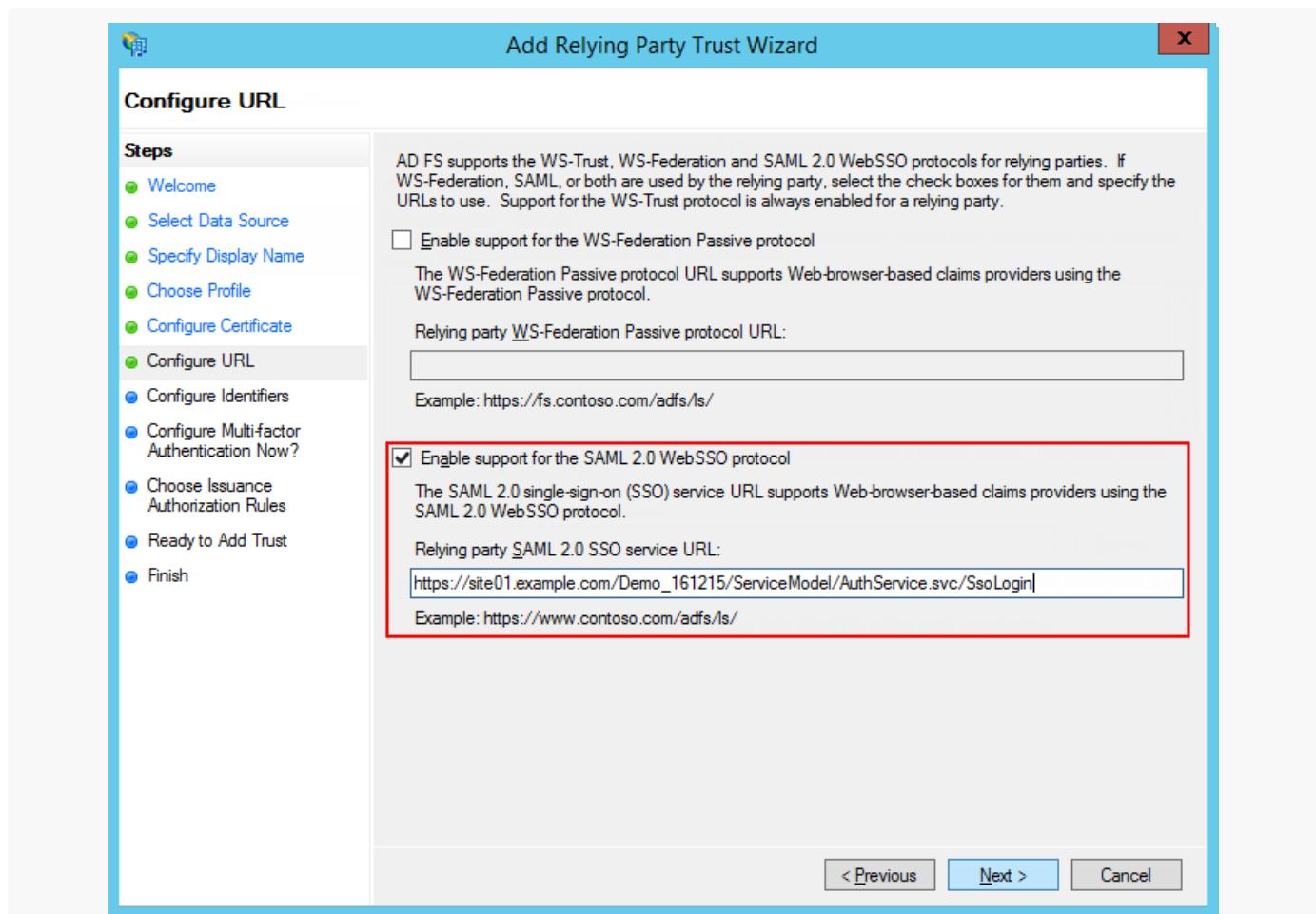
2. Выберите опцию ручного ввода данных ("Enter data about the relying party manually"), как показано на Рис. 2.

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



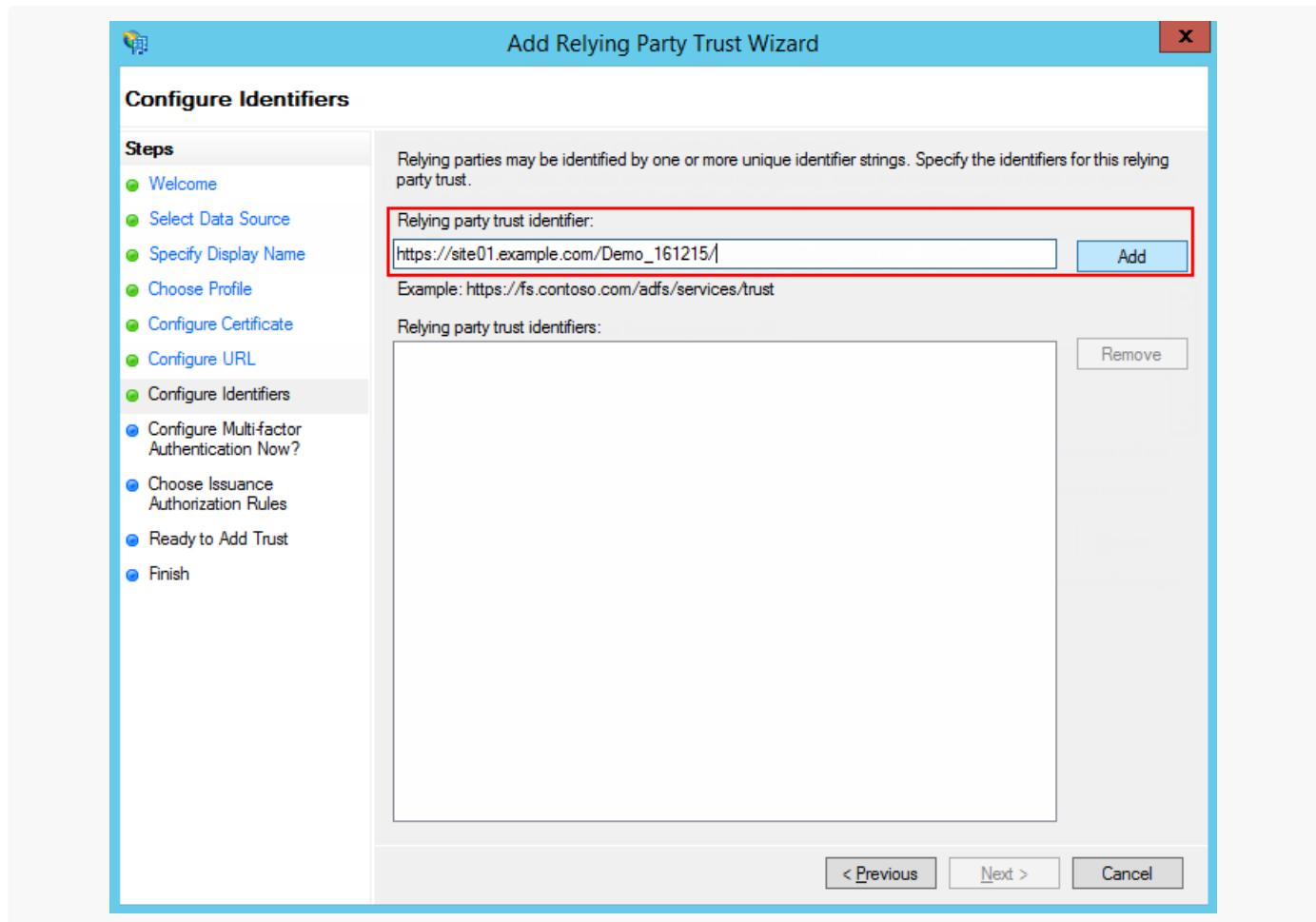
3. В поле [Отображаемое имя] ("Display name") введите название Relying Party. Имя необходимо только для упорядоченного ведения списка доверенных приложений в ADFS.
4. Оставьте профиль "AD FS Profile", выбранный по умолчанию. Нажмите кнопку [Далее] ("Next").
5. На шаге выбора сертификата нажмите кнопку [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.

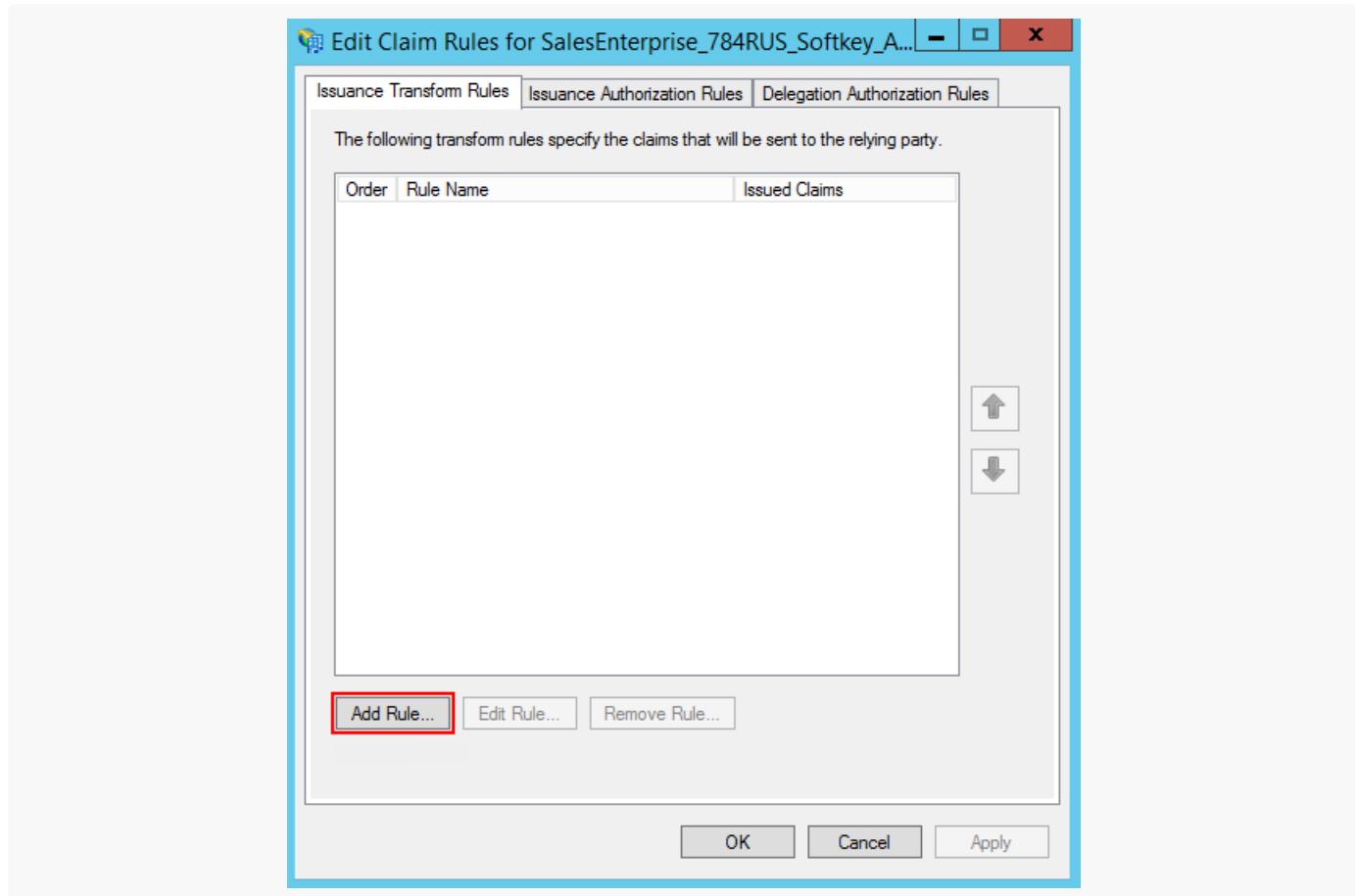
Рис. 4 — Указание идентификатора



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).

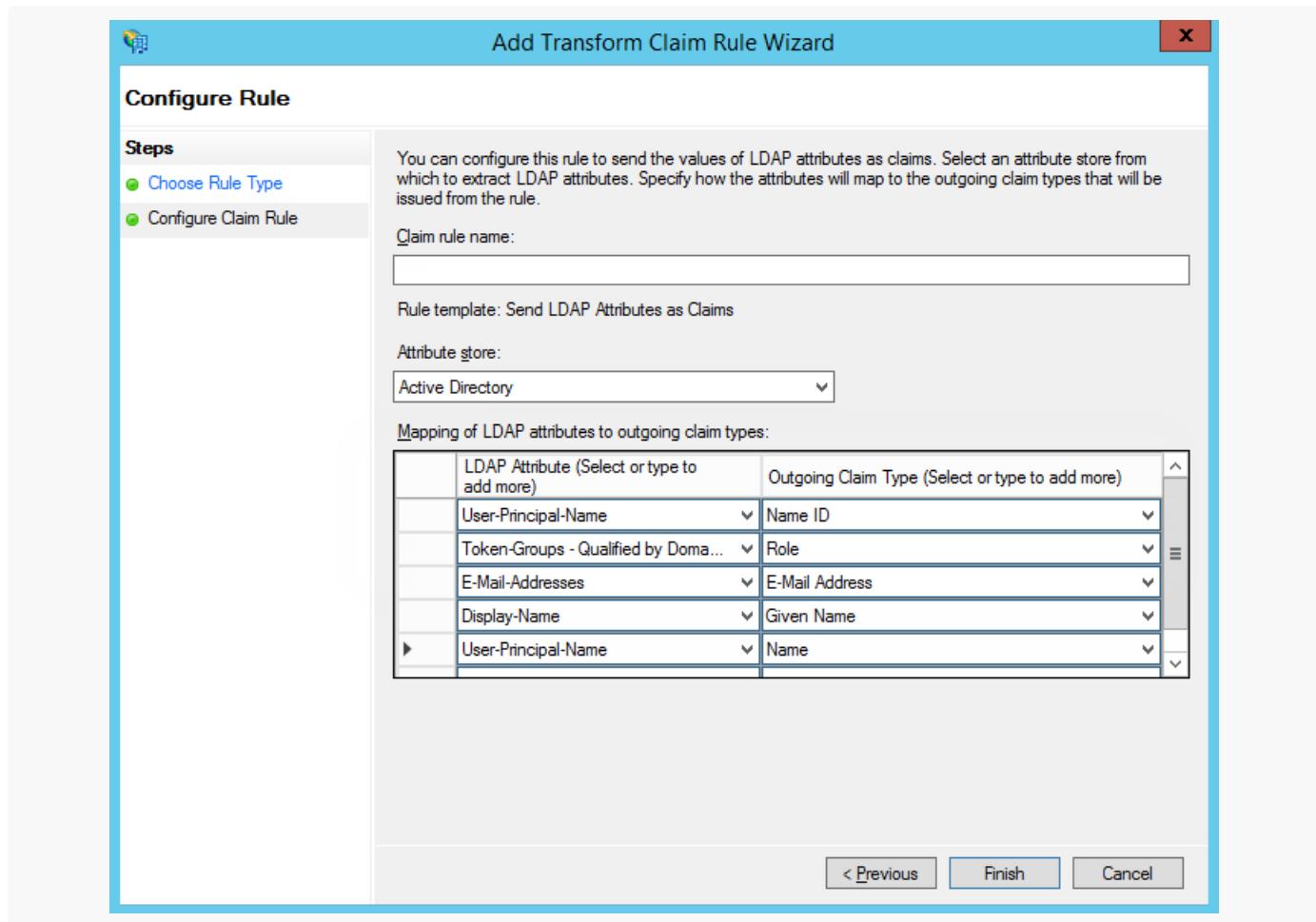
Рис. 5 — Добавление правила



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



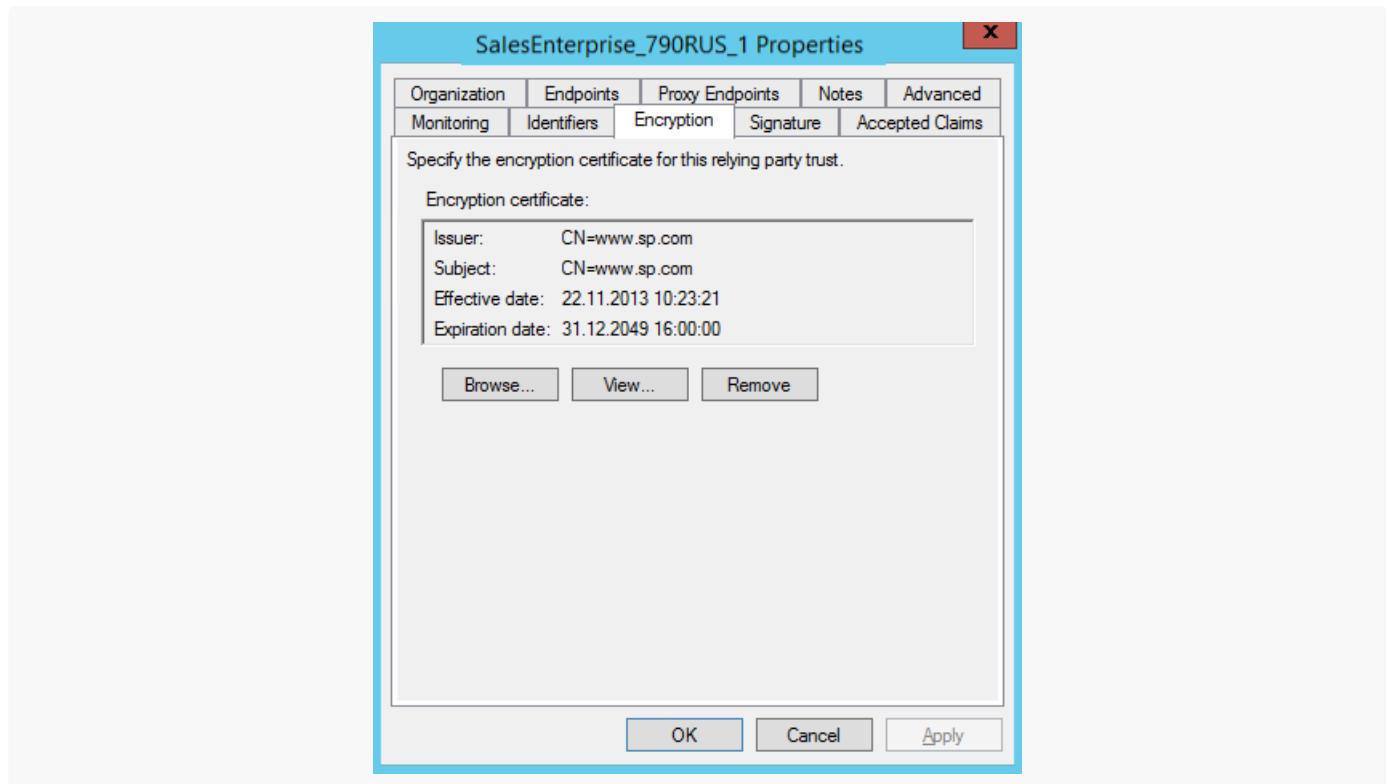
11. Нажмите кнопку [Сохранить] ("Save").

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.

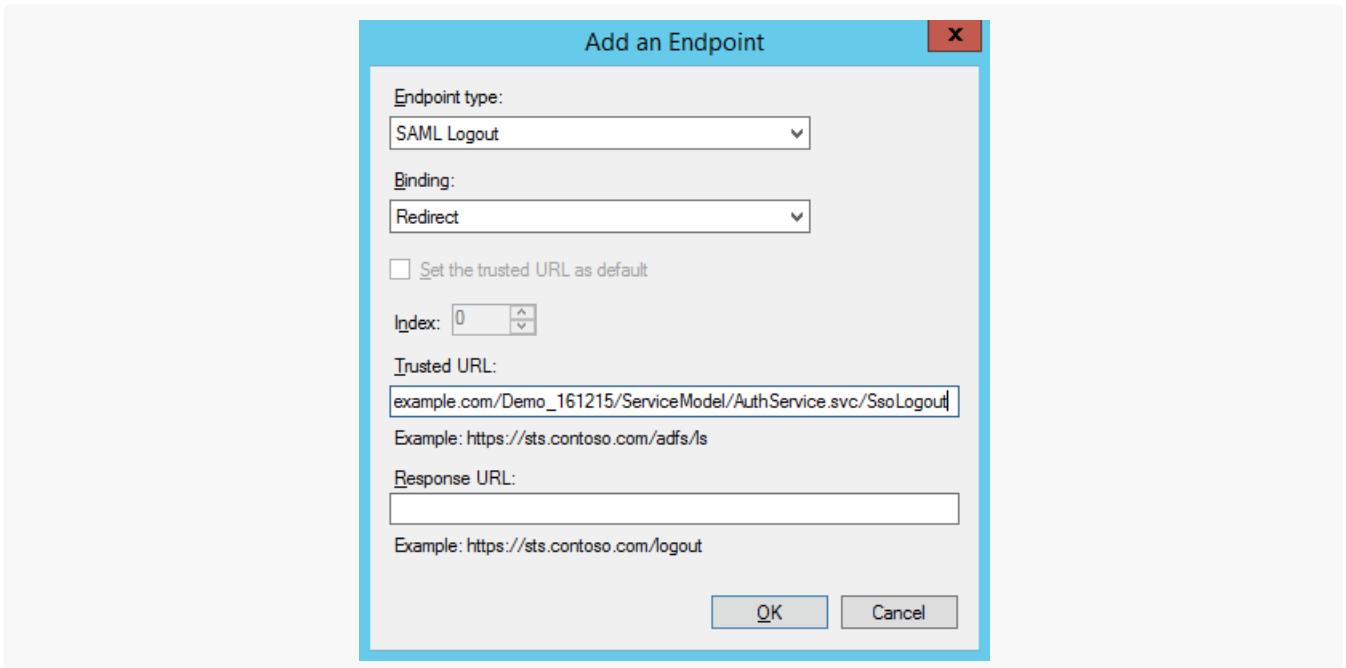
Рис. 7 — Добавление публичного ключа



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.

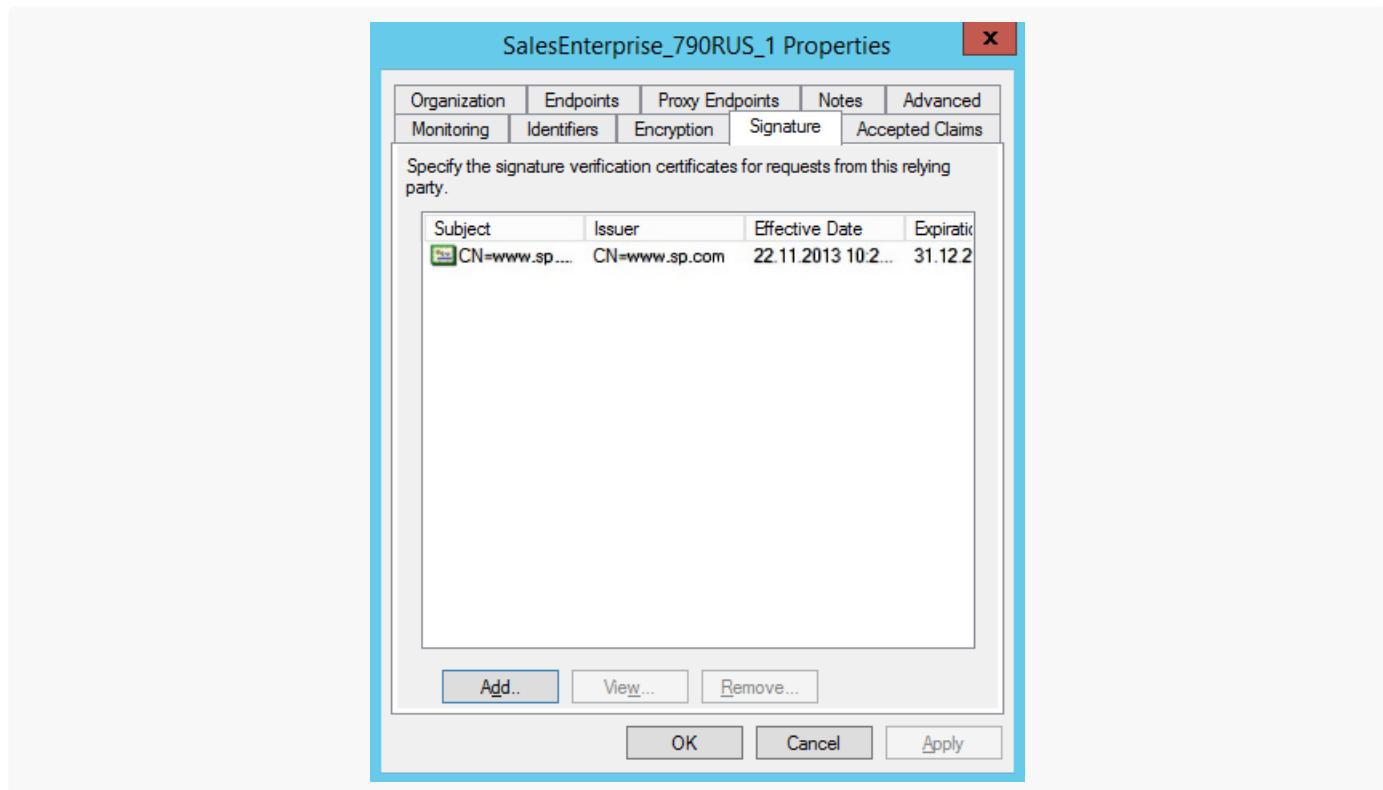
Рис. 8 — Установка параметров конечной точки



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

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

- 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.

- 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/adfs/ls"
    SingleLogoutServiceUrl="https://adfs01.mysite.com/adfs/ls"
    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:

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> <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 [Настройте 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\](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" ...>
    </forms>
</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/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”).

.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 [Настройте 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 SSPSSsoAuthProvider):

```
...
<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.

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.

6. **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 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?use_sso=true

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 **TerrasoftWebHost.dll.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 **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”).

Безопасная загрузка файлов

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для повышения безопасности работы в Creatio вы можете настроить ограничения форматов загружаемых в приложение сторонних файлов. Ограничения на загрузку файлов действуют как для пользователей, так и для интеграций, например, внешних веб-сервисов.

При настроенных ограничениях Creatio проверяет формат файлов, которые загружаются на деталь [*Файлы и ссылки*]. В случае соответствия настройкам файл будет успешно загружен. В другом случае файл загружен не будет, а пользователь получит уведомление, что загрузка данного файла запрещена настройками безопасности. Для файлов, загруженных в систему до включения ограничений, настройки не применяются.

Ограничения действуют только на загрузку файлов в Creatio, скачивать файлы могут все пользователи, имеющие к ним доступ.

В системе предусмотрены следующие способы ограничения загрузки файлов:

- Ограничения для файлов **определенных типов** — вы можете настроить список **разрешенных расширений** или список **запрещенных расширений** файлов. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов определенных типов.
- Ограничения для файлов **неизвестных типов**. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов, у которых не указано расширение и невозможно определить тип по содержимому.

Выбрать режим проверки файлов

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку “**Режим проверки файлов**” (код “FileSecurityMode”).
4. В поле [**Значение по умолчанию**] выберите необходимый тип ограничения:
 - “**Проверка файлов отключена**” — чтобы отменить все ограничения на загрузку файлов в приложение.
 - “**Список запрещенных расширений**” — чтобы запретить загрузку в приложение файлов определенных типов.
 - “**Список разрешенных расширений**” — чтобы разрешить загрузку в приложение только файлов определенных типов.
5. **Сохраните** изменения.

Настроить список типов файлов

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку
 - “**Список разрешенных расширений файлов**” (код “FileExtensionsAllowList”), чтобы настроить список разрешенных к загрузке типов файлов. По умолчанию в настройке приведены наиболее часто используемые типы файлов.
 - “**Список запрещенных расширений файлов**” (код “FileExtensionsDenyList”), чтобы настроить список запрещенных к загрузке типов файлов. По умолчанию в настройке приведены типы файлов, которые могут являться вредоносными.
4. В поле [**Значение по умолчанию**] через запятую без пробела укажите **расширения файлов** ([Рис. 1](#)) и проверьте корректность ввода.

Рис. 1 — Пример заполнения системной настройки “Список разрешенных расширений файлов”

The screenshot shows the 'Список разрешенных расширений файлов' (List of allowed file extensions) configuration screen. On the left is a vertical toolbar with icons for various system functions. The main area has a header 'Список разрешенных расширений файлов' and a 'ЗАКРЫТЬ' (Close) button. Below the header are fields for 'Название*' (Name*) and 'Тип*' (Type*), both set to 'Список разрешенных расширений файлов'. There's also a 'Код*' (Code*) field set to 'FileExtensionsAllowList'. A 'Кэшируется?' (Caches?) checkbox is checked. A note says 'Сохранять значение для текущего пользователя' (Save value for current user). Below these are sections for 'Первичное наполнение:' (Initial fill:) and 'Описание:' (Description:), which list various file types and formats. On the right side of the interface, there are several circular icons for communication and notifications.

5. Сохраните изменения.

Настроить ограничения для неизвестных типов файлов

Creatio определяет типы загружаемых файлов по их расширению. В случае если расширение не указано, система определяет тип файла на основании его содержимого. По умолчанию в систему разрешено загружать файлы неизвестных типов. Запрет загрузки таких файлов повысит безопасность работы в приложении, но в этом случае обязательно потребуется настроить список разрешенных или запрещенных расширений.

Чтобы **запретить загрузку** в Creatio файлов неизвестных типов:

1. Перейдите в **дизайнер системы** по кнопке
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку **“Разрешить работу с неизвестными типами файлов”** (код “AllowFilesWithUnknownType”).
4. Снимите признак [**Значение по умолчанию**].
5. **Сохраните** изменения.

Настроить исключение веб-сервисов из ограничений загрузки файлов

Ограничение загрузки файлов применяется для всех используемых в системе веб-сервисов, включая те, которые были добавлены в процессе кастомизации системы, в проектных решениях и приложениях Marketplace. Чтобы веб-сервисы могли добавлять в Creatio файлы тех типов, которые не разрешены пользователям, их необходимо **добавить в список исключений**. Для этого:

1. Перейдите в **дизайнер системы** по кнопке
2. Перейдите в раздел [**Справочники**].

3. Откройте справочник [**Список исключений из проверки безопасности файлов**].
4. Нажмите [**Добавить**].
5. В поле [**Название**] укажите **URI** веб-сервиса, который необходимо добавить в исключения. Запись сохраняется автоматически.
 - Пример для приложений на **.NET Framework**: /0/rest/[Название пользовательского сервиса]/[Конечная точка пользовательского сервиса], без указания [Адреса приложения].
 - Пример для приложений на **.NET CORE**: /rest/[Название пользовательского сервиса]/[Конечная точка пользовательского сервиса], без указания [Адреса приложения].
6. **Повторите** для всех веб-сервисов, которым необходимо разрешить загрузку файлов в приложение.

Управление значениями справочника

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Большинство выпадающих списков в Creatio используют значения из справочников. Также существует особый справочный тип полей при заполнении которых пользователь сможет выбрать запись из объекта Creatio. Объекты, в которых хранятся возможные значения для определенного поля, называются справочниками.

Вы можете управлять значениями, доступными в выпадающих списках и справочных полях, используя для этого записи соответствующих справочников. Например, после создания в мастере разделов нового справочного поля необходимо заполнить значения соответствующего справочника в разделе [**Справочники**].

Важно. Для настройки справочников требуется доступ к системной операции “Доступ к разделу “Справочники” (CanManageLookups). Кроме того, если объект справочника управляет операциями, записями или колонками, пользователю необходимы соответствующие права, чтобы получить возможность управлять записями этого объекта.

Чтобы перейти к **списку справочников**, откройте раздел [**Справочники**] из рабочего места [**Студия**] или из дизайнера системы.

Рис. 1— Переход к разделу [**Справочники**] из рабочего места [**Студия**]

Контакты

Добавить контакт Действия

Фильтры/группы Тег

Имя Леонидович	Должность Руководитель отдела	Мобильный телефон +7 915 255 85 87
Контрагент Технокомплект		
Кирдин Анатолий Александрович	Рабочий телефон +7 915 178-45-36	
Контрагент Вектор	Email a.kirdin@rondo.net	
Кирдин Анатолий Александрович	Должность Руководитель отдела	Рабочий телефон +7 495 461 44 45
Контрагент Рондо		Мобильный телефон +7 915 178 45 36
Комаров Александр Андреевич	Должность Директор	Рабочий телефон +7 495 640 05 05
Контрагент Астра-оптимум	Email a.komarov@aksioma.com	Мобильный телефон +7 903 672 98 10

Рис. 2— Переход к разделу [Справочники] из дизайнера системы

Контакты

Добавить контакт Действия

Фильтры/группы Тег

Контрагент Аксиома	Email s.avdorov@yahoo.com	Мобильный телефон +7 905 726 46 29
Валевский Андрей Георгиевич	Должность Руководитель отдела	Рабочий телефон +7 495 780 80 93
Контрагент Вектор	Email a_valevsky@gmail.com	
Елисеев Андрей Николаевич	Должность Директор	Рабочий телефон +7 495 277 07 70
Контрагент Альфабизнес	Email a.eliseev@alfabizness.co m	Мобильный телефон +7 915 260 01 95
Жаврук Виталий	Должность Руководитель отдела	Рабочий телефон +7 495 233 55 36
Контрагент Астра-оптимум	Email v.zhavruk@gmail.com	Мобильный телефон +7 905 893 11 04
Захарцев Александр	Должность	Рабочий телефон

Раздел [Справочники] содержит список зарегистрированных справочников. Регистрация справочника в разделе [Справочники] позволяет пользователям управлять наполнением (записями) и свойствами справочника. Справочник может существовать и без регистрации в разделе [Справочники], однако, если объект такого справочника не используется как раздел или деталь, то отредактировать его наполнение и свойства будет невозможно.

Чтобы управлять записями определенного справочника, необходимо сначала найти его в списке справочников. Обычно названия объектов справочников отражают имена справочных полей, значения которых они хранят. Например, справочник, в котором хранятся значения поля [Категория] раздела [Активности], называется “Категории активностей”.

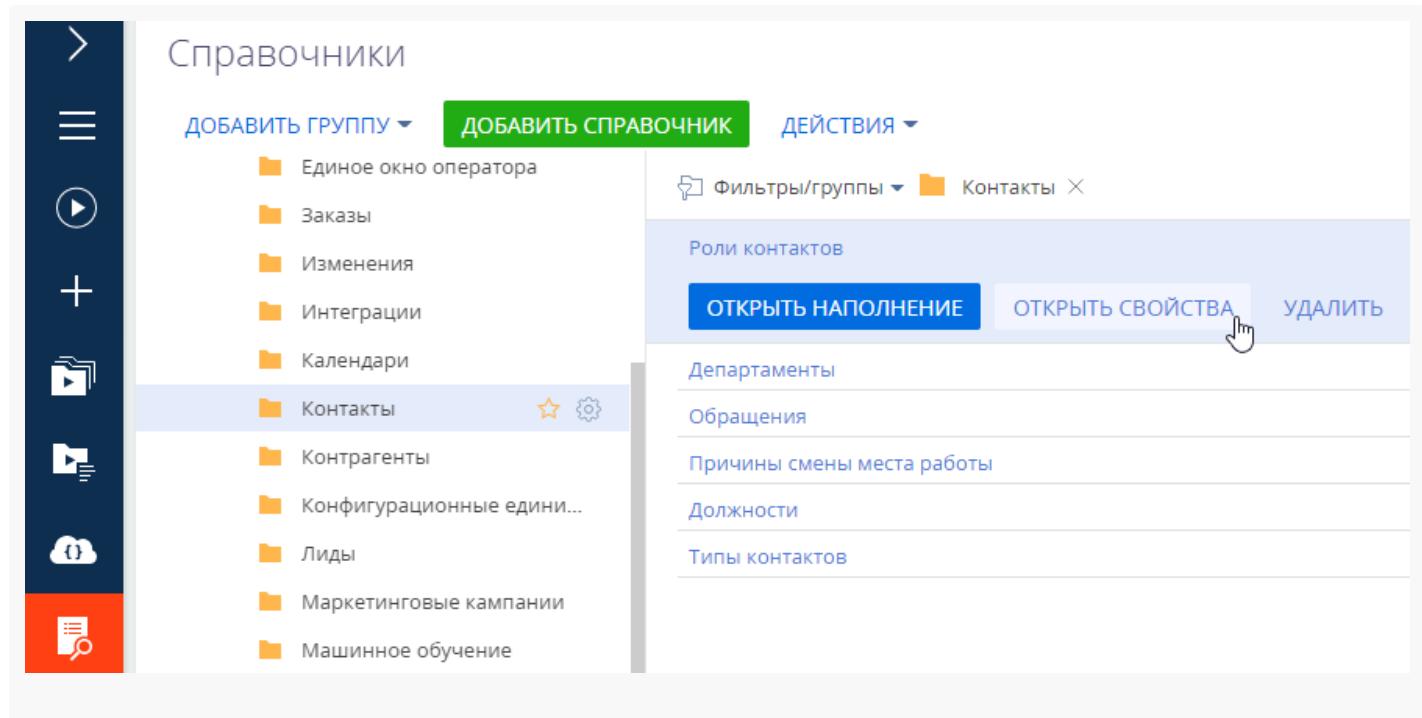
На заметку. Вы можете проверить имя объекта справочника, изменив соответствующее справочное поле в мастере разделов. Подробнее работа с полями описана в статье “[Настроить поля страницы](#)”.

Используйте стандартные [фильтры](#) и [группы](#), чтобы **найти нужный справочник**. Если вы не можете найти нужный справочник в разделе [Справочники], то, возможно, объект справочника еще не зарегистрирован в разделе. Подробнее о регистрации справочников читайте в статье “[Создать новый справочник](#)”.

Чтобы **управлять записями справочника**, выберите нужный справочник в реестре и нажмите кнопку [Открыть наполнение]. Большинство справочников используют стандартный редактируемый список, в который можно добавлять записи, редактировать или удалять их. Обратите внимание, что прежде чем управлять содержимым колонок реестра, их необходимо добавить. Некоторые справочники могут иметь специальные страницы, предназначенные для редактирования записей.

Чтобы **изменить название справочника, объект или страницу реестра**, нажмите кнопку [Открыть свойства].

Рис. 3— Открытие справочника для редактирования свойств



Чтобы **удалить справочник** из раздела [Справочники], нажмите кнопку [Удалить]. Удаление справочника из раздела [Справочники] не удаляет соответствующий объект справочника и никак не влияет на работу справочных полей. Удаленный справочник всегда можно вновь добавить в раздел [Справочники].

Настроить Microsoft Exchange и Microsoft 365

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для настройки параметров соединения с почтовыми провайдерами пользователь должен обладать правом на выполнение системной операции “Доступ к рабочему месту “Администрирование”” (код “CanManageAdministration”). Подробно назначение и использование системных операций описаны в статье [Права доступа на системные операции](#).

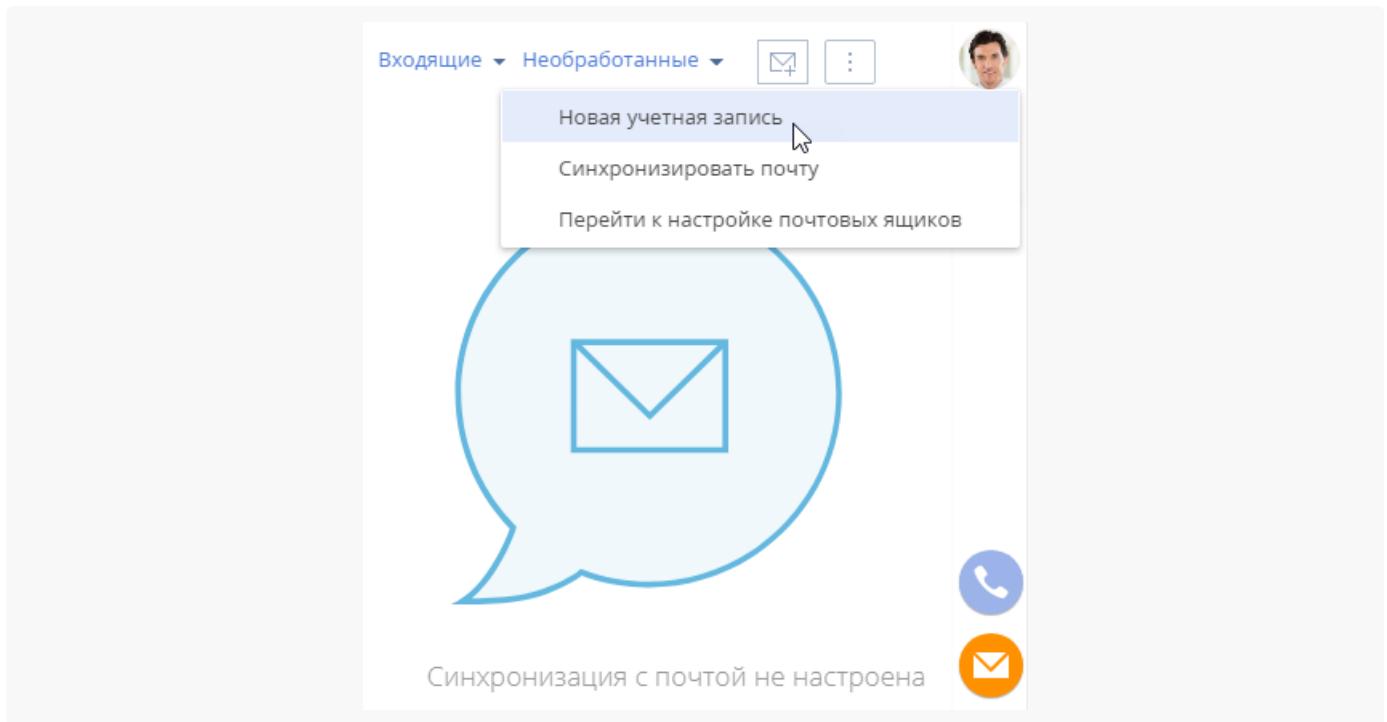
На заметку. Перед тем, как перейти к настройке почтового провайдера, необходимо настроить сервис синхронизации [Exchange Listener](#).

Добавить почтовый провайдер можно несколькими способами.

Способ 1. Добавить провайдер из вкладки [Email] коммуникационной панели

1. Откройте коммуникационную панель и перейдите на вкладку [Email] по кнопке .
2. Нажмите  и выберите действие [Новая учетная запись] (Рис. 1).

Рис. 1 — Добавление новой учетной записи



На заметку. Для добавления новой учетной записи вы также можете в меню кнопки выбрать [Перейти к настройке почтовых ящиков] и на открывшейся странице нажать кнопку [Добавить].

3. В открывшемся окне введите электронный адрес и нажмите кнопку [Далее].
4. Нажмите кнопку [Добавить провайдер].

На заметку. Для автоматического распознавания почтового провайдера по доменному имени добавьте домены нового провайдера в справочник [Домены почтовых провайдеров]. В результате при настройке учетной записи почты пользователям не придется указывать почтового провайдера вручную.

5. На открывшейся странице нажмите кнопку [Добавить] (Рис. 2).

Рис. 2 — Добавление почтового провайдера

Настройки почтового ящика

ПОЧТОВЫЕ СЕРВИСЫ

Почтовый сервис	Тип
GMail	IMAP
AOL mail	IMAP
Zoho	IMAP
Office 365	Exchange
Yahoo	IMAP

ДОБАВИТЬ

6. На открывшейся странице выберите тип почтового сервиса — Exchange.
7. Заполните обязательное поле [Адрес почтового сервиса] в формате example.exchange.com (Рис. 3).

Рис. 3 — Адрес почтового сервиса

Добавить сервис

ПРИМЕНЬТЬ **ОТМЕНА**

Настройки сервиса

Тип почтового сервиса
Exchange

Адрес почтового сервиса *
example.exchange.com

Дополнительные настройки

8. Также вы можете заполнить дополнительные настройки, чтобы установить опции загрузки и отправки писем, формат логина, метод аутентификации (Рис. 4).

На заметку. Чтобы настроить OAuth-авторизацию без использования пароля для учетных записей почтового сервиса Microsoft 365, предварительно должно быть зарегистрировано OAuth-приложение. Подробнее читайте в статье [Настройте OAuth-автентификацию для Microsoft 365](#).

Рис. 4 — Дополнительные настройки почтового сервиса

Добавить сервис

ПРИМЕНЕНИТЬ ОТМЕНА

Настройки сервиса

Тип почтового сервиса
Exchange

Адрес почтового сервиса *

example.exchange.com

Дополнительные настройки

Загружать электронные письма

Отправлять электронные письма

Формат логина
Использовать email

Название сервиса *

example.exchange.com

Метод аутентификации
OAuth 2.0

Идентификатор приложения (клиент) *

269d98e4922fb3895e9ae2108cbb5064

Секрет клиента *

.....

a. Для настройки загрузки и отправки писем:

Установите признак [Загружать электронные письма] и/или [Отправлять электронные письма].

Необходимо выбрать минимум один пункт.

b. Для настройки формата логина:

- Выберите [Формировать имя вручную], если пользователь должен самостоятельно ввести email-адрес и имя пользователя.
- Выберите [Использовать email], если в качестве логина должен использоваться полный email-адрес, например, example@google.com.
- Выберите [Использовать имя почтового ящика], если в качестве логина должна использоваться часть email-адреса до символа "@". Например, для email-адреса "example@google.com" логином будет "example".

f. Для настройки метода аутентификации:

- Выберите "Basic" для базовой аутентификации с использованием имени пользователя и пароля, закодированных с помощью Base64.

- Выберите “OAuth 2.0”, если хотите предоставить сервису ограниченный доступ к защищенным ресурсам пользователя без необходимости передачи логина и пароля. Заполните обязательные поля [Идентификатор приложения (клиент)] и [Секрет клиента].

[Идентификатор приложения (клиент)] выдается сервером авторизации Microsoft. В документации и API идентификатор приложения может называться Product ID (идентификатор продукта).

[Секрет клиента] — секретный ключ, предоставленный сервером авторизации. В документации и API секретный ключ может также называться Product key (ключ продукта).

9. Сохраните изменения по кнопке [Применить].

В результате пользователи системы смогут использовать добавленный почтовый провайдер для получения и отправки email-сообщений.

Способ 2. Добавить провайдер из профиля пользователя

- Откройте страницу профиля пользователя, например, кликнув по ссылке [Профиль] на главной странице приложения.
- Кликните по полю [Учетные записи почты] (Рис. 1).

Рис. 1 — Учетные записи почты

Профиль: Евгений Мирный

СОХРАНИТЬ **ОТМЕНА**

Изменить пароль

Язык
Русский (Россия)

Формат даты и времени
Белорусский (Беларусь)

Часовой пояс
Вильнюс, Киев, Рига, София, Талли...

Настройки командной строки

Настройки параметров Call Centre

Учетные записи почты 

Учетные записи во внешних ресурсах

3. В открывшемся окне нажмите кнопку [Добавить].

Для завершения настройки **выполните шаги 3-9**, описанные выше в **Способе 1**.

На заметку. Чтобы удалить почтовый сервис, сначала нужно удалить все почтовые ящики, которые с ним работают.

Настроить журнал аудита

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Журнал аудита используется для логирования системных настроек, событий и данных. В нем регистрируются события, связанные с изменением структуры ролей пользователей, распределением прав доступа, изменением значений системных настроек, авторизацией пользователей в системе и т. д.

Для логирования бизнес-данных, например, отслеживания изменения цены продукта или остатка по счетам, используется **журнал изменений**. Подробнее: [Настроить журнал изменений](#).

На заметку. Для просмотра журнала аудита требуется доступ к системной операции “Просмотр раздела “Журнал аудита” (код “CanViewSysOperationAudit”). Для просмотра и выполнения

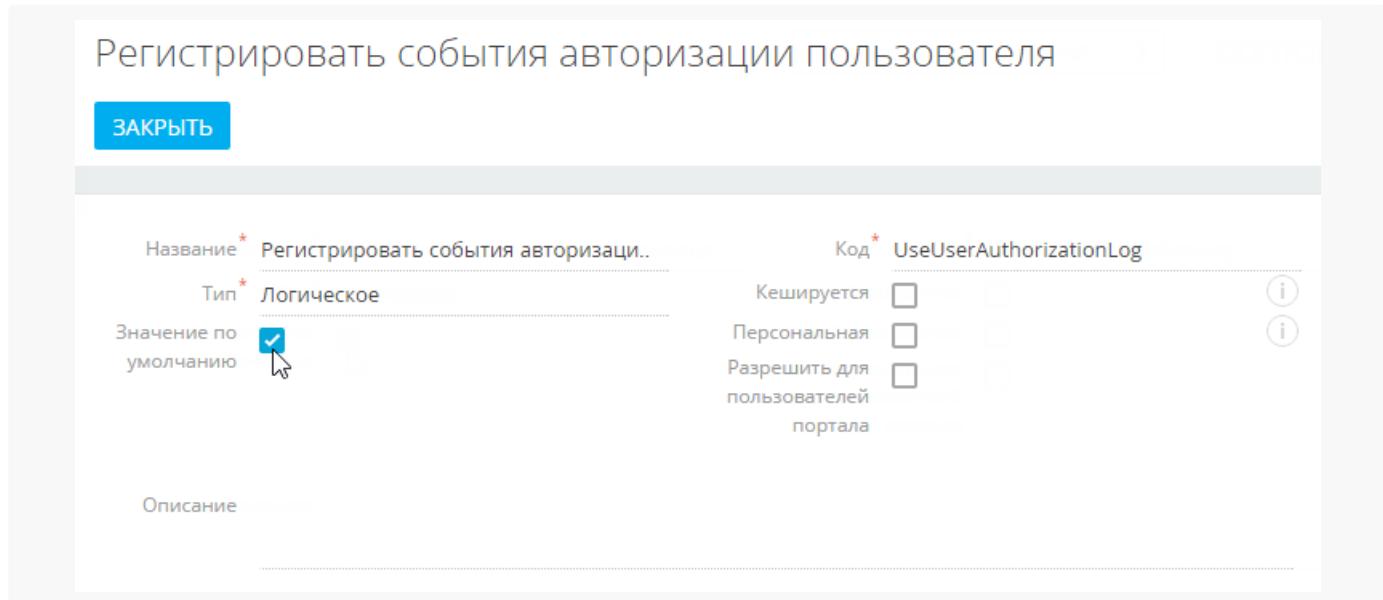
архивации записей требуется доступ к системной операции “Управление разделом “Журнал аудита” (код “CanManageSysOperationAudit”). Подробнее: [Права доступа на системные операции](#).

По умолчанию логирование журнала аудита отключено. Чтобы изменения логировались, выполните настройки, описанные в данной статье.

Для включения и настройки журнала аудита с помощью системных настроек:

1. Откройте дизайнер системы нажатием кнопки  в правом верхнем углу приложения.
2. В блоке “Настройка системы” перейдите по ссылке “Системные настройки”.
3. В списке групп откройте группу “Администрирование” и выберите подгруппу “Журнал аудита”. Здесь содержатся все настройки, которые отвечают за логирование событий в Creatio. Каждому типу логируемого события соответствует системная настройка, которая включает или отключает его. Подробнее о системных настройках журнала аудита читайте в статье: [Описание системных настроек](#).
4. Для включения настройки откройте ее и установите признак [Значение по умолчанию]. Например, установите признак для настройки [Регистрировать события авторизации пользователя], (Рис. 1) если необходимо логировать выполняемые пользователями вход в систему и выход из нее.

Рис. 1 — Включение системной настройки журнала аудита



После отключения системной настройки журнала аудита может потребоваться перезагрузка Redis, чтобы изменения вступили в силу.

На заметку. Если журнал аудита включен на уровне конфигурационных файлов системы, то значения системных настроек игнорируются.

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

- Нажмите  → “**Организационные роли**”.
 - В списке организационных ролей **выберите родительскую роль**. Например, создадим роль для регионального офиса.
 - Нажмите [**Добавить**] и **укажите тип роли** (“Организация” или “Подразделение”). Например, создадим подразделение “Отдел маркетинга” для регионального офиса.
 - Ведите **название** новой роли. Название организационной роли должно быть уникальным.
 - Откройте вкладку [**Функциональные роли**] и добавьте функциональные роли, которые получат 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](#).

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

Рис. 1 — Добавление организационной роли

Процессы

- Библиотека процессов
- Журнал процессов

Пользователи и администрирование

- Пользователи системы
- Организационные роли
- Функциональные роли
- Права доступа на объекты
- Права доступа на операции
- Журнал аудита

Импорт и интеграции

- Импорт данных
- Настройка интеграции с LDAP
- Настройка интеграции с веб-сервисами
- Журнал отправки email-рассылок

Маркетплейс

- Модуль универсального визирования
- Интеграция с решениями на платформе 1С
- Автоматизация подбора персонала
- Уникальный конструктор чатботов

[Все решения >>](#)

Руководство по разработке на платформе [SDK](#)

Настроить систему [Быстрый старт](#)

Видеокурсы. Тренинги. Тестирования [Академия](#)

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:

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

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

5. На вкладке [Руководители]:

- Если пользователь уже создан** в системе, то нажмите **+** и выберите [**Добавить существующего**]. Во всплывающем окне выберите нужных пользователей (Рис. 3).
- 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, получат 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

The screenshot shows the Terrasoft application interface for managing organizational roles. On the left, there's a vertical sidebar with various icons. The main area is titled 'Организационные роли' (Organizational roles). A tree view on the left lists organizational units: 'Все сотрудники' (All employees) and 'Основной офис' (Main office), which further branches into 'Административный отдел' (Administrative department), 'Отдел маркетинга' (Marketing department), 'Отдел продаж' (Sales department), 'Финансовый отдел' (Financial department), 'Офис продаж' (Sales office), 'Партнерские продажи' (Partnership sales), 'Продажи_региональный офис' (Regional sales office), 'Прямые продажи' (Direct sales), 'Региональный офис' (Regional office), and 'Торговые представители' (Sales representatives). The 'Marketing department' node is currently selected. To the right, a detailed view of the 'Marketing department' role is shown. It has a title 'Название* Отдел маркетинга'. Below it, there are tabs for 'ПОЛЬЗОВАТЕЛИ' (Users), 'РУКОВОДИТЕЛИ' (Managers), and 'ФУНКЦИИ' (Functions). Under the 'ПОЛЬЗОВАТЕЛИ' tab, there's a section for 'Синхронизировать с LDAP' (Sync with LDAP) with a checkbox and a link 'Элемент LDAP'. Below this, there's a button 'Пользователи + :'. The overall interface is clean and modern, typical of a business management application.

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](#).

Зарегистрировать приложение Creatio в Google Workspace

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Google Workspace — это набор облачных сервисов, который позволяет администраторам Creatio интегрировать доменное имя вашего приложения с Gmail и предоставить пользователям возможность синхронизировать корпоративную почту и календари Google с Creatio.

Регистрация приложения в Workspace происходит в несколько этапов:

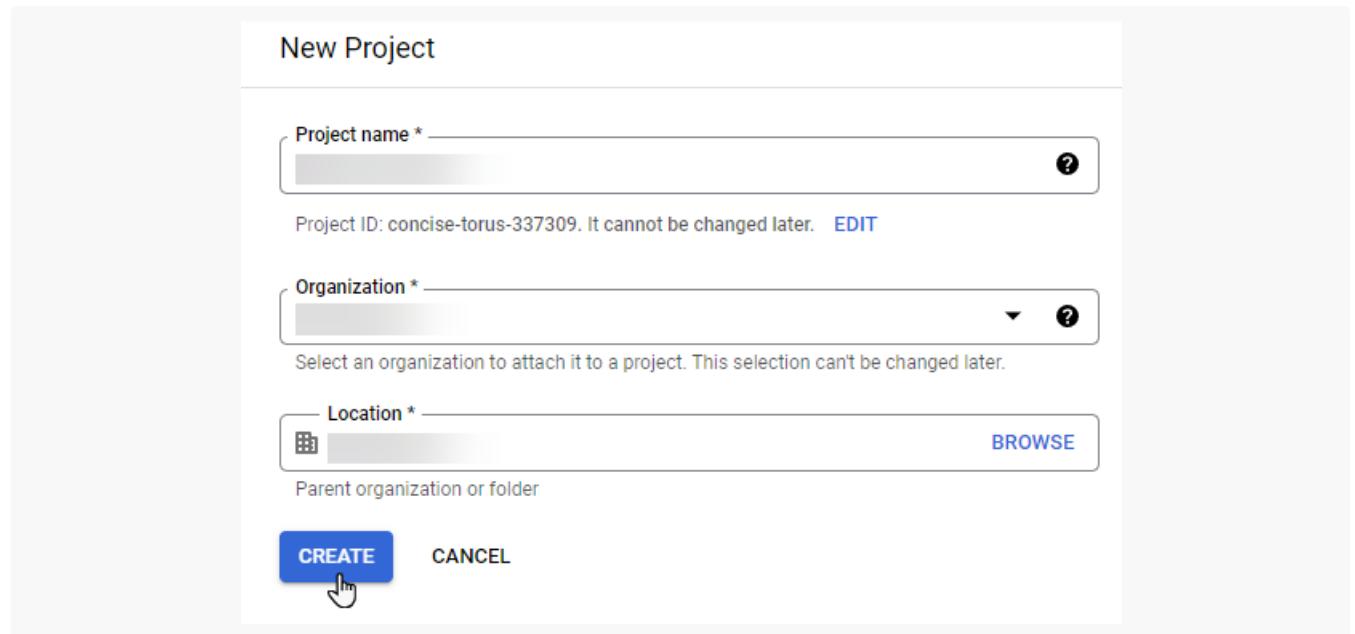
1. Необходимо зарегистрировать и настроить проект Google Cloud Platform, открыть доступ к API, сгенерировать ключи для Creatio (“Client ID” и “Client Secret”).
2. Полученные ключи “Client ID” и “Client Secret” необходимо ввести в Creatio в настройках синхронизации календарей и настройке почтового сервиса.

Шаг 1. Настроить проект Google Cloud Platform

Чтобы настроить проект Google:

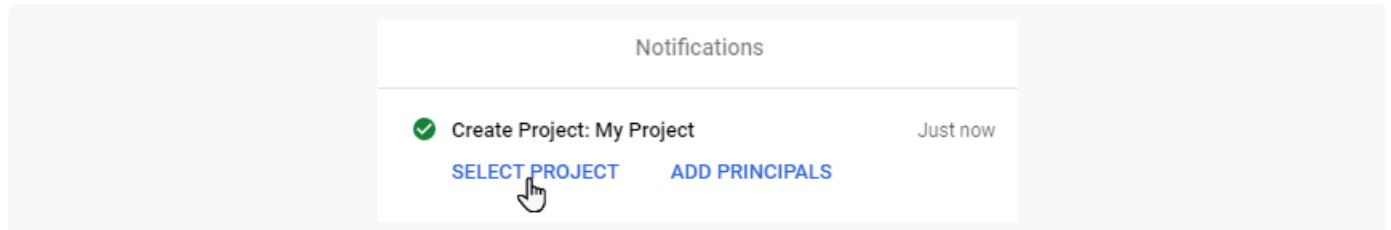
1. Откройте страницу <https://console.cloud.google.com/cloud-resource-manager>.
2. Авторизуйтесь как администратор Workspace.
3. Для регистрации приложения Creatio в Google Workspace необходим проект Google Cloud Platform. Если вы хотите создать новый проект, то переходите к пункту 4. Если вы хотите использовать созданный ранее проект, то пропустите пункты 4-5 и сразу переходите к пункту 6.
4. Чтобы создать новый проект, выполните следующие действия:
 - a. Нажмите кнопку [*Create Project*].
 - b. Заполните поля:
 - [*Project name*] — укажите произвольное имя проекта. Например, “Creatio OAuth”.
 - [*Organization*] — укажите название предприятия, чтобы проект был закреплен в Google Cloud за вашей компанией, а не за сотрудником, создавшим учетную запись, либо выберите “No organization”. После сохранения проекта значение поля нельзя будет изменить.
 - [*Location*] — укажите папку, в которой будет размещен ваш проект. Данное поле заполнится автоматически, если вы указали организацию в предыдущем поле. Если в предыдущем поле вы выбрали “No organization”, то необходимо выбрать папку, в которой будет расположен новый проект в данной учетной записи.
 - c. Нажмите кнопку [*Create*] (Рис. 1).

Рис. 1 — Создание проекта



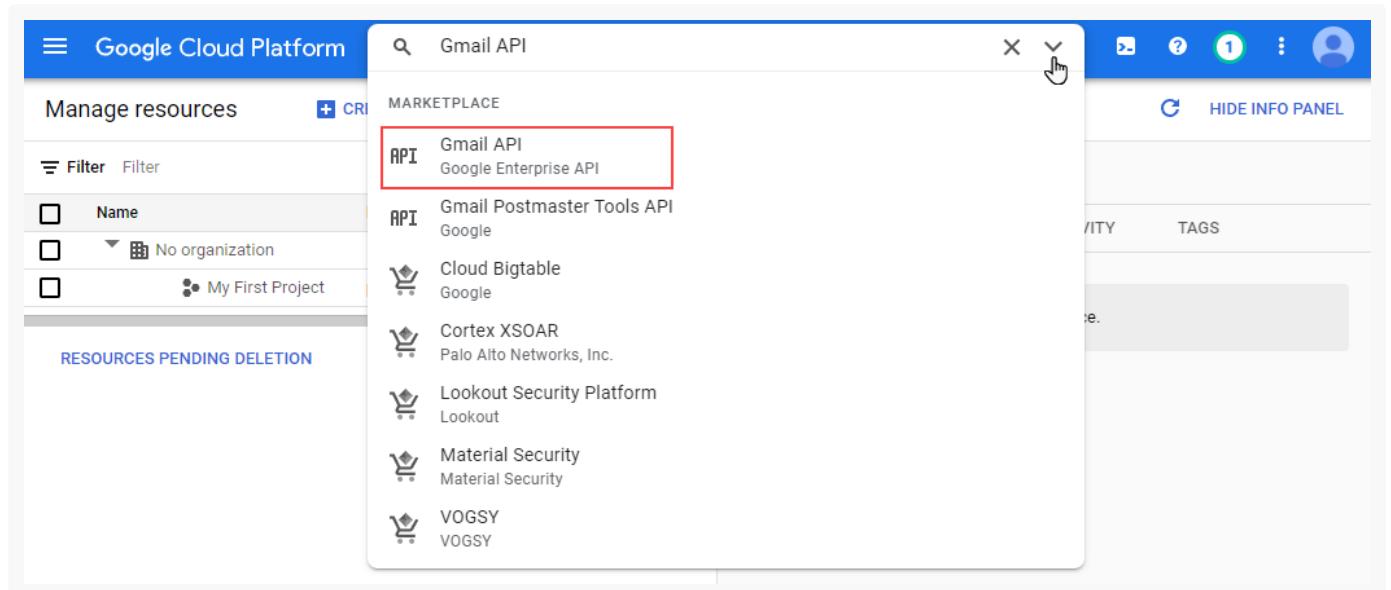
5. Чтобы продолжить настройку созданного проекта, во всплывающем окне выберите проект с помощью кнопки [Select Project] (Рис. 2).

Рис. 2 — Выбор проекта



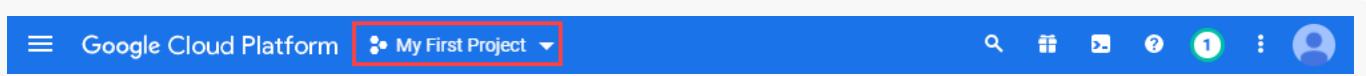
6. В выбранном проекте разрешите использовать те API, которые используются Creatio. При помощи строки поиска найдите Gmail API (Рис. 3).

Рис. 3 — Переход к Gmail API



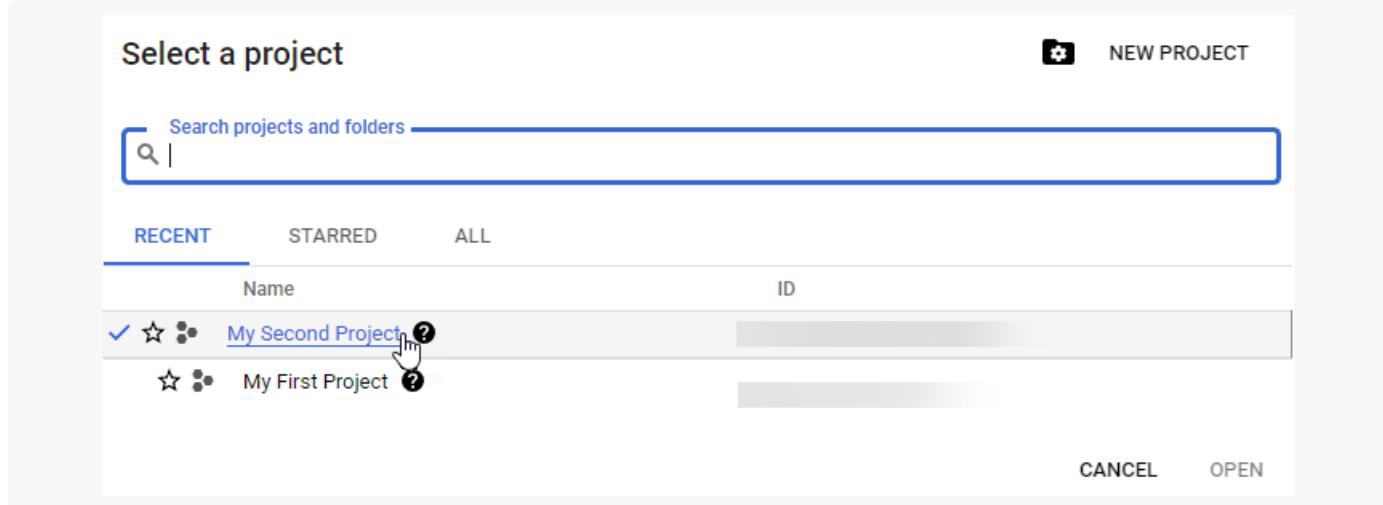
7. Перейдите на страницу Gmail API. Убедитесь, что выбран необходимый вам проект. Название активного проекта отобразится в верхней панели открывшейся страницы (Рис. 4).

Рис. 4 — Отображение активного проекта



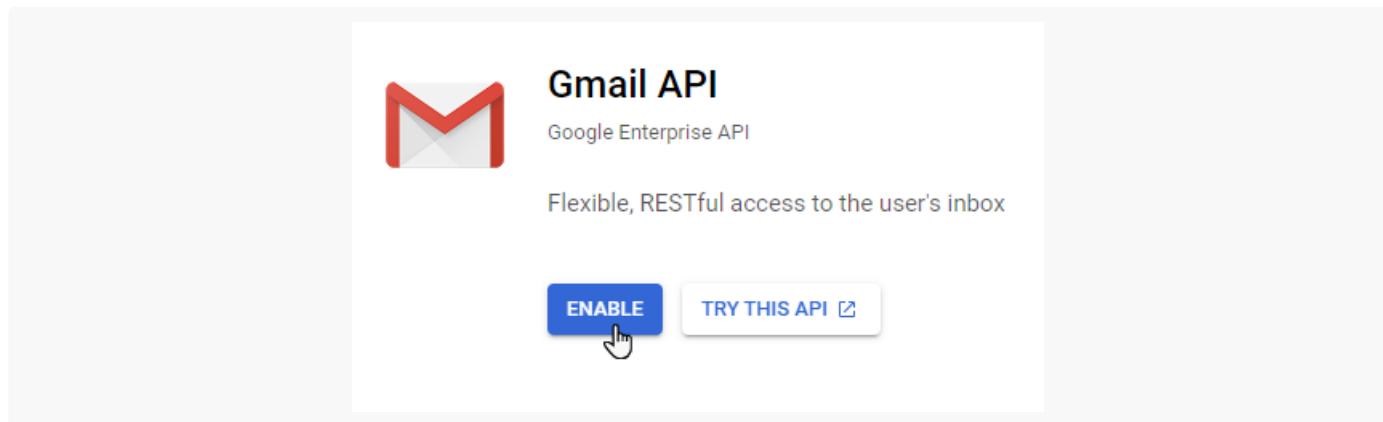
Чтобы изменить активный проект, необходимо нажать на название в верхней панели и во всплывающем окне выбрать необходимый проект (Рис. 5).

Рис. 5 — Выбор активного проекта



8. Для включения Gmail API нажмите кнопку [*Enable*] (Рис. 6).

Рис. 6 — Включение Gmail API



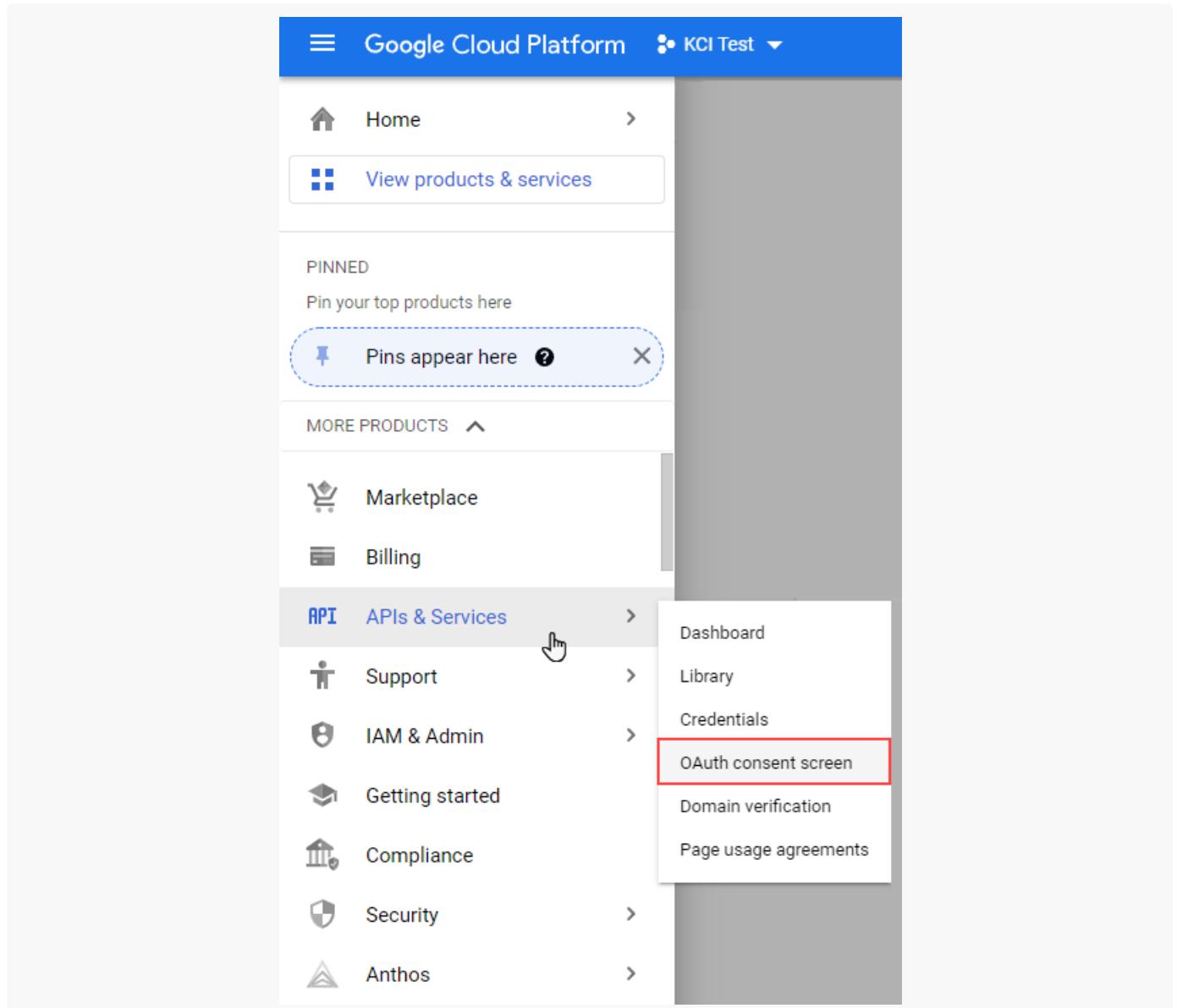
В результате добавленный API отобразится в списке доступных на панели управления (Рис. 7).

Рис. 7 — Список доступных API проекта

Name	↓ Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Gmail API				

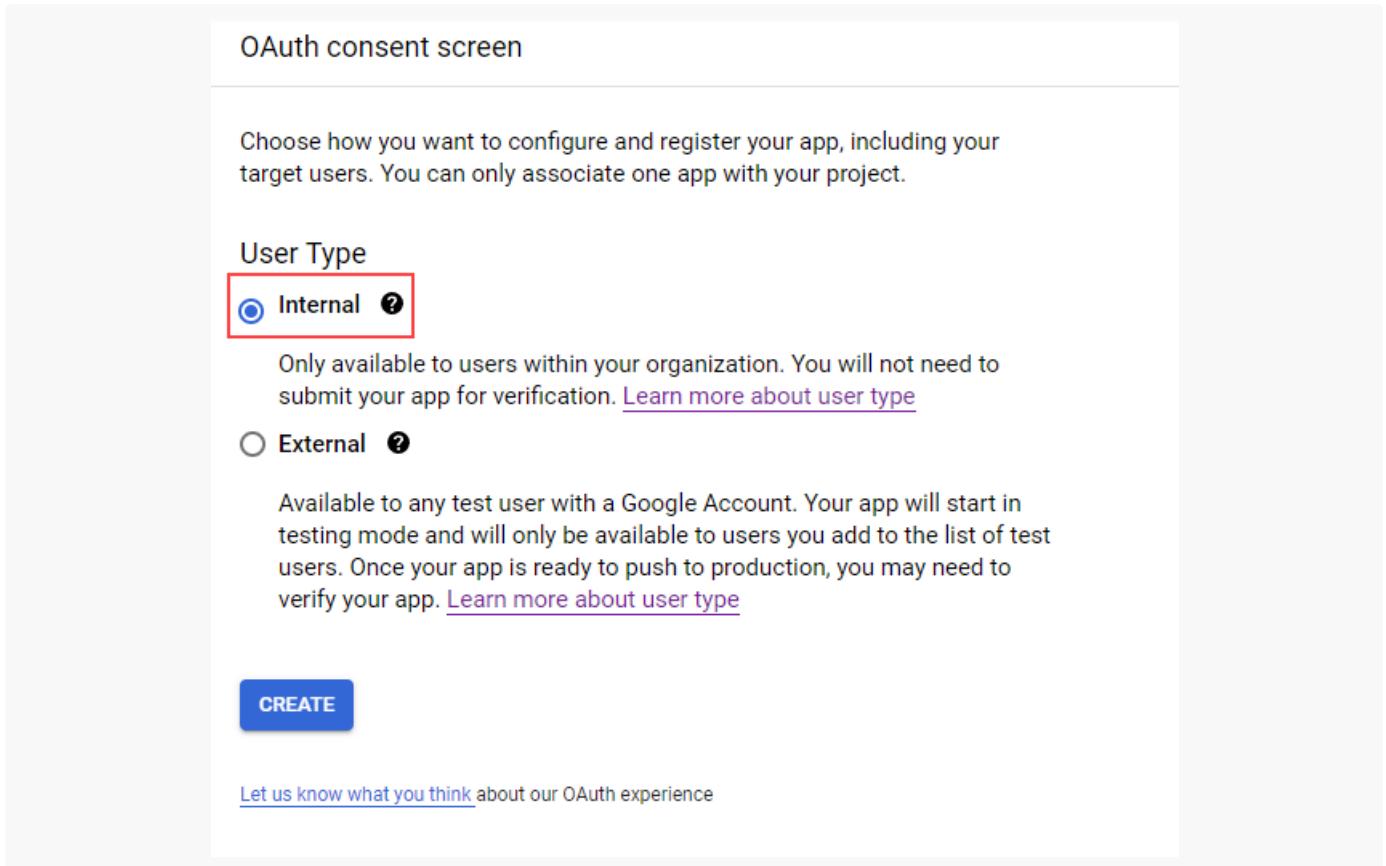
9. Повторите пункты 5–7 инструкции для активации Contacts API и Calendar API.
10. Для того, чтобы указать тип, название и параметры приложения, откройте навигационное меню кнопкой  в левом верхнем углу страницы настроек, выберите [APIs&Services] → [OAuth consent screen] (Рис. 8).

Рис. 8 — Переход на страницу Auth consent screen



11. Для настройки доступа к сервисам Google только для пользователей из вашей компании укажите тип приложения [Internal] (Рис. 9).

Рис. 9 — Выбор типа приложения



12. Заполните параметры доменов:

- [*App name*] — название продукта, которое будет показано пользователям при авторизации приложения Creatio для использования учетной записи Google. Например, "Creatio".
- [*User support email*] — email-адрес администратора Workspace или вашей службы поддержки.
- [*Authorized domains*] — домен вашего приложения Creatio. Для приложений, развернутых в **Creatio Cloud** укажите "creatio.com". Для приложений, развернутых **on-site**, укажите ваш индивидуальный домен.
- [*Developer contact information*] — почтовый адрес администратора Workspace.

13. Перейдите к настройке прав доступа по кнопке [*Add or remove scopes*] (Рис. 10).

Рис. 10 — Переход к странице управления правами доступа

The screenshot shows the 'Edit app registration' interface. At the top, there are three tabs: 'OAuth consent screen' (with a checkmark), 'Scopes' (which is selected and highlighted in blue), and 'Summary'. Below the tabs, a descriptive text states: 'Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account.' A link 'Learn more' is provided. At the bottom of this section is a blue button labeled 'ADD OR REMOVE SCOPES', which is also enclosed in a red rectangular box.

14. Настройте права доступа для пользователей вашего домена. Для этого отметьте в открывшемся списке все строки, в столбце [API] которых указано "Gmail API" (Рис. 11), кроме тех, у которых в столбце [Scopes] указаны права только на чтение и вид строки: .../*.readonly.

Выполните аналогичные действия для строк, в столбце [API] которых указано "Contacts API" и "Calendar API".

Рис. 11 — Пример настройки прав доступа

The screenshot displays a table titled 'Scopes' with a 'Filter' input field at the top left. The table has four columns: 'API' (with an upward arrow icon), 'Scope', 'User-facing description', and a question mark icon at the top right. The rows are as follows:

API ↑	Scope	User-facing description
<input type="checkbox"/>	Cloud Trace API	.../auth/trace.readonly Read Trace data for a project or application
<input type="checkbox"/>	Cloud Trace API	.../auth/trace.append Write Trace data for a project or application
<input checked="" type="checkbox"/>	Gmail API https://mail.google.com/	Read, compose, send, and permanently delete all your email from Gmail
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.modify	Read, compose, and send emails from your Gmail account
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.compose	Manage drafts and send emails
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.addons.current.action.compose	Manage drafts and send emails when you interact with the add-on
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.addons.current.message.action	View your email messages when you interact with the add-on
<input type="checkbox"/>	Gmail API .../auth/gmail.readonly	View your email messages and settings
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.metadata	View your email message metadata such as labels and headers, but not the email body
<input checked="" type="checkbox"/>	Gmail API .../auth/gmail.insert	Add emails into your Gmail mailbox

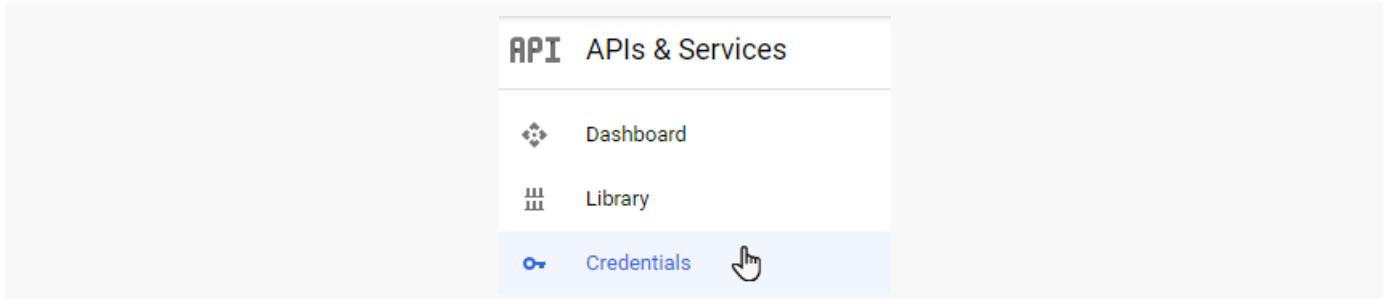
At the bottom, there are pagination controls: 'Rows per page: 10 ▾ 21 – 30 of 39 < >'.

15. Сохраните внесенные изменения по кнопке [Save and continue].

Шаг 2. Получить ключи для интеграции Google с внешними приложениями

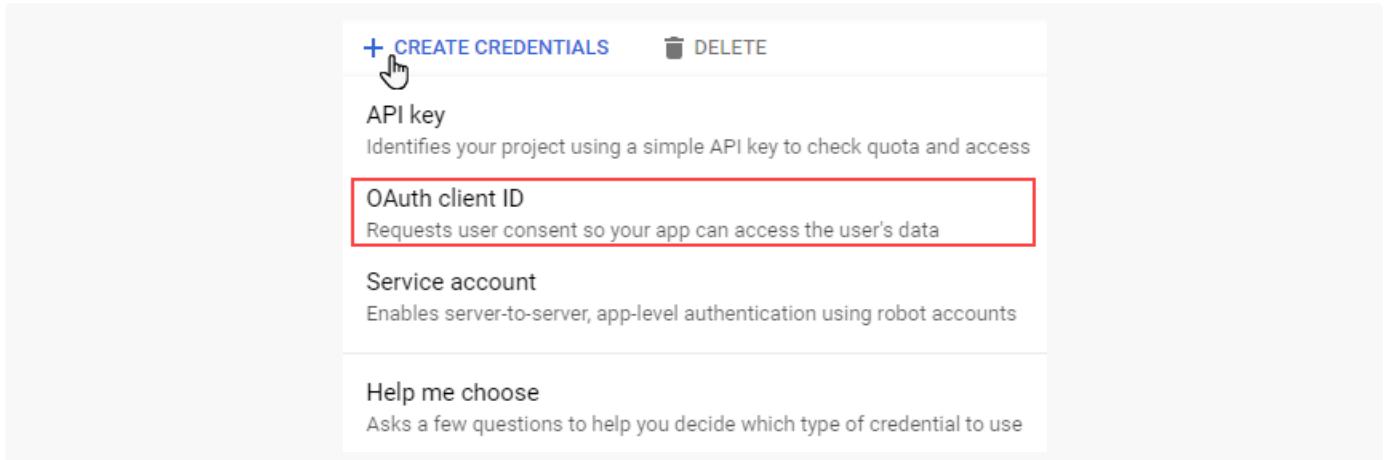
- Перейдите на страницу учетных данных. Для этого в боковом меню выберите [*Credentials*] (Рис. 12).

Рис. 12 — Переход на страницу [Учетные данные]



- Чтобы создать идентификатор клиента OAuth 2.0 нажмите кнопку [*Create Credentials*] и выберите в появившемся меню OAuth client ID (Рис. 11).

Рис. 13 — Выбор OAuth client ID



- Для создания идентификатора клиента OAuth 2.0, заполните обязательные параметры (Рис. 10):

- [*Application type*] — "Web application".
- [*Name*] — произвольное название клиента OAuth 2.0.
- [*Authorized JavaScript origins*] — полный URL-адрес вашего приложения Creatio. Для приложений, развернутых в **Creatio Cloud** укажите адрес с доменом "creatio.com". Например, "https://050651-studio.creatio.com". Для приложений, развернутых **on-site**, укажите адрес с вашим индивидуальным доменом.
- [*Developer contact information*] — ссылки на ваше приложение в следующих форматах:

Для Creatio **версий 7.17.0 и ниже**:

https://адрес_вашего_сайта/0/Page.aspx?Id=3b22f0ff-034a-48da-8758-a0660e5a26ff
https://адрес_вашего_сайта/0/rest/GoogleOAuthAuthenticator/ProcessAuthenticationCode

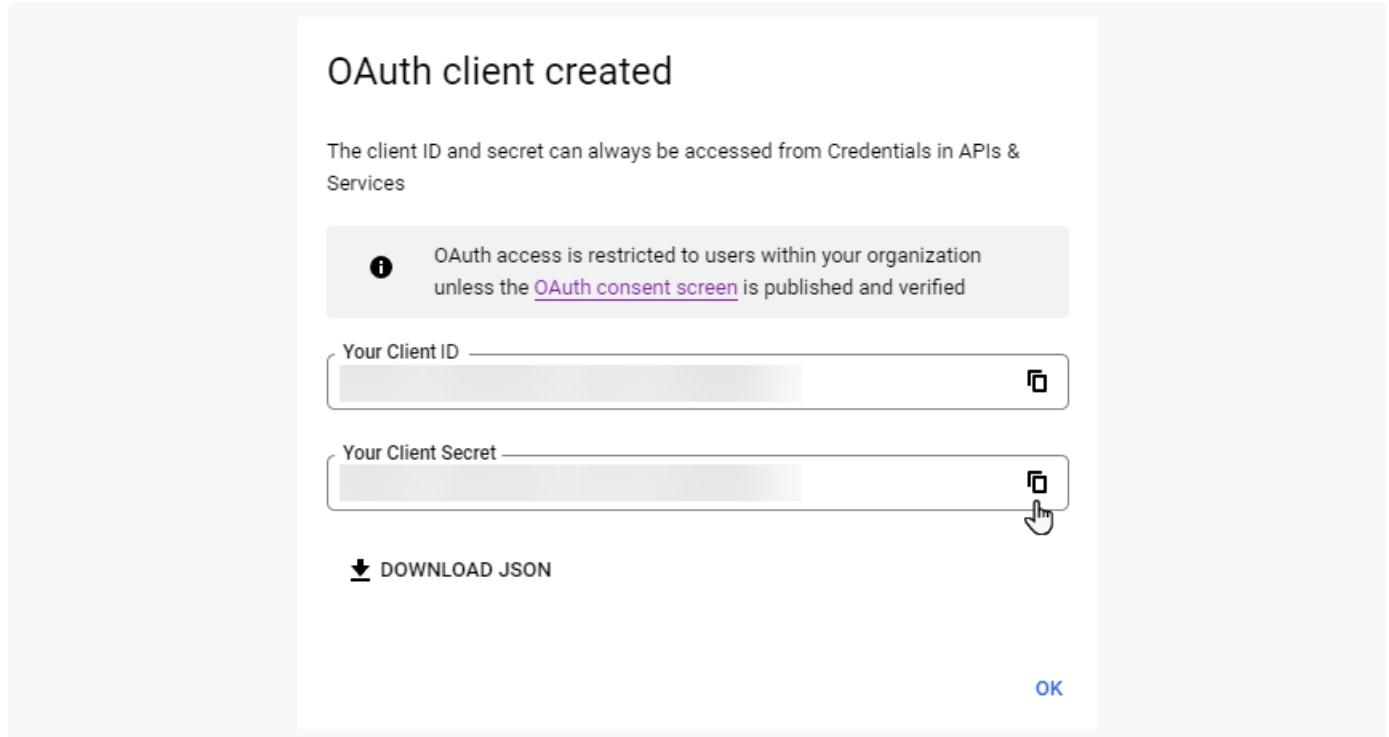
Для Creatio **версий 7.17.1 и выше**:

https://адрес_вашего_сайта/0/LegacySocialAccountAuthPage.aspx?Id=3b22f0ff-034a-48da-8758-a0660e5a26ff
https://адрес_вашего_сайта/0/rest/GoogleOAuthAuthenticator/ProcessAuthenticationCode

На заметку. Обратите внимание, что при обновлении до версии Creatio 7.17.1 и выше необходимо указать новые адреса перенаправления [*Authorized redirect URIs*] в существующем идентификаторе клиента OAuth 2.0, либо создать новый идентификатор клиента с новыми адресами и использовать его клиентский и секретный ключи для интеграции с аккаунтом Creatio.

4. Скопируйте и сохраните локально полученные идентификатор клиента (Client ID) и секретный ключ клиента (Client Secret) (Рис. 14).

Рис. 14 — Ключи Google



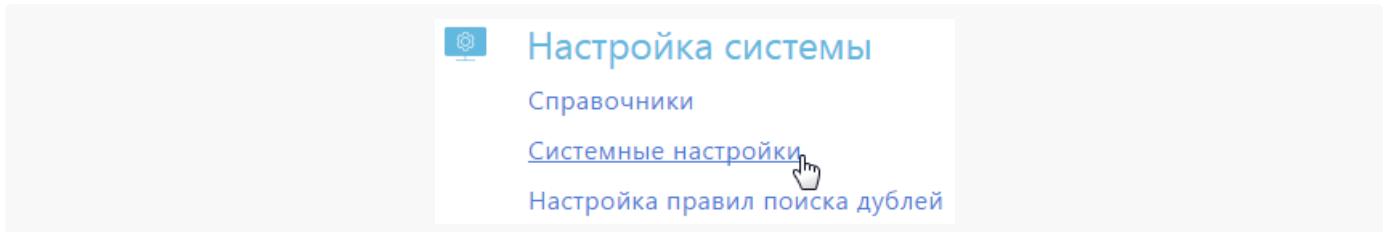
Шаг 3. Ввести ключи Google в Creatio

Ввести ключи Google для синхронизации с контактами и календарем

Полученные коды “Идентификатор клиента” (“Client ID”) и “Секретный ключ клиента” (“Client Secret”) необходимо ввести в Creatio в качестве значений системных настроек “Ключ для доступа к сервисам Google” и “Секретный ключ для доступа к сервисам Google” соответственно. Для этого:

1. Откройте приложение Creatio.
2. Откройте дизайнер системы, например по кнопке  .
3. В блоке [*Настройка системы*] перейдите по ссылке [*Системные настройки*] (Рис. 15).

Рис. 15 — Раздел [*Системные настройки*]



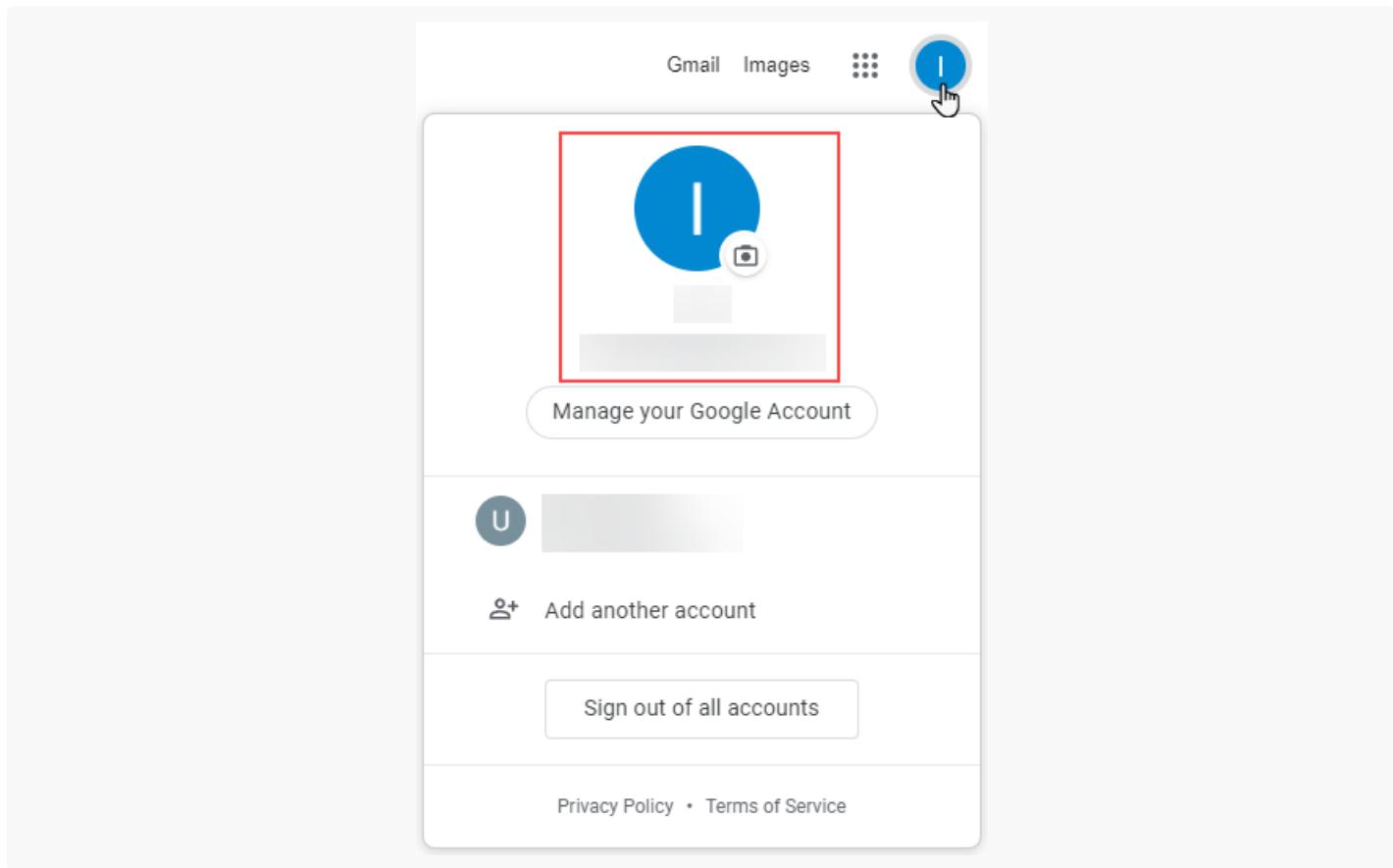
4. В реестре системных настроек выберите настройку “Ключ для доступа к сервисам Google” и нажмите кнопку [Открыть].
5. На странице системной настройки в поле [Значение по умолчанию] введите код “Ваш идентификатор клиента”, полученный при регистрации Creatio в Google (доступен в поле [Your Client ID] сообщения Google API), и сохраните изменения.
6. В реестре системных настроек выберите настройку “Секретный ключ для доступа к сервисам Google” и нажмите кнопку [Открыть].
7. На странице системной настройки в поле [Значение по умолчанию] введите код “Ваш секретный ключ клиента”, полученный при регистрации Creatio в Google (доступен в поле [Your Client Secret] сообщения Google API), и сохраните изменения.
8. В реестре системных настроек выберите настройку [Использовать общее приложение Google] и нажмите кнопку [Открыть] и убедитесь, что признак [Значение по умолчанию] **неактивен**.

В результате вы сможете настроить [синхронизацию задач в системе с календарем Google](#).

Ввести ключи Google для синхронизации с почтой

Поскольку при внесении данных в Google Workspace был выбран внутренний тип приложения (Internal), то при добавлении нового почтового ящика либо настройке синхронизации с почтой в Creatio, необходимо убедиться в том, что вы вошли в учетную запись Google как **пользователь авторизованного домена** и эта учетная запись является приоритетной в данный момент. Для этого перейдите по адресу: <https://www.google.com/> и убедитесь, что учетная запись с авторизованным доменом в адресе почты находится в приоритете (Рис. 16)

Рис. 16 — Приоритет учетной записи в Google



Полученные коды “Идентификатор клиента” (“Client ID”) и “Секретный ключ клиента” (“Client Secret”) необходимо ввести в Creatio при настройке для провайдера Gmail защищенного подключения OAuth 2.0. Для этого:

1. Откройте приложение Creatio.
2. Откройте дизайнер системы, например по кнопке .
3. В блоке [Настройка системы] перейдите по ссылке [Справочники].
4. Откройте наполнение справочника [Список почтовых провайдеров].
5. Перейдите к настройкам провайдера Gmail.
6. В области [Дополнительные настройки] укажите метод аутентификации OAuth 2.0, чтобы предоставить почтовому сервису ограниченный доступ к защищенным ресурсам пользователя без необходимости передачи логина и пароля.
7. В обязательных полях [Идентификатор приложения (клиент)] и [Секрет клиента] укажите полученные ранее коды “Идентификатор клиента” (“Client ID”) и “Секретный ключ клиента” (“Client Secret”) соответственно (Рис. 15).

Рис. 17 — Настройка OAuth 2.0 для Gmail

GMail

ПРИМЕНЕНИЕ **ОТМЕНА**

Адрес сервера *
imap.gmail.com

Порт
993

Безопасность
SSL/TLS

Сервер исходящей почты (SMTP)

Настройки почтового сервиса, необходимые для отправки почты. Укажите адрес и порт почтового сервера, а также выберите параметры безопасности передачи данных

Адрес сервера *
smtp.gmail.com

Порт
465

Безопасность
SSL/TLS

[Дополнительные настройки](#)

Формат логина
Использовать имя почтового ящика

Название сервиса *
GMail

Метод аутентификации
OAuth 2.0

Идентификатор приложения (клиент) *
Client ID
.....

8. Сохраните настройки почтового провайдера.

После регистрации вашего приложения в Google Workspace пользователи смогут настроить синхронизацию почтовых ящиков и календарей Google со своими учетными записями Creatio.

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.

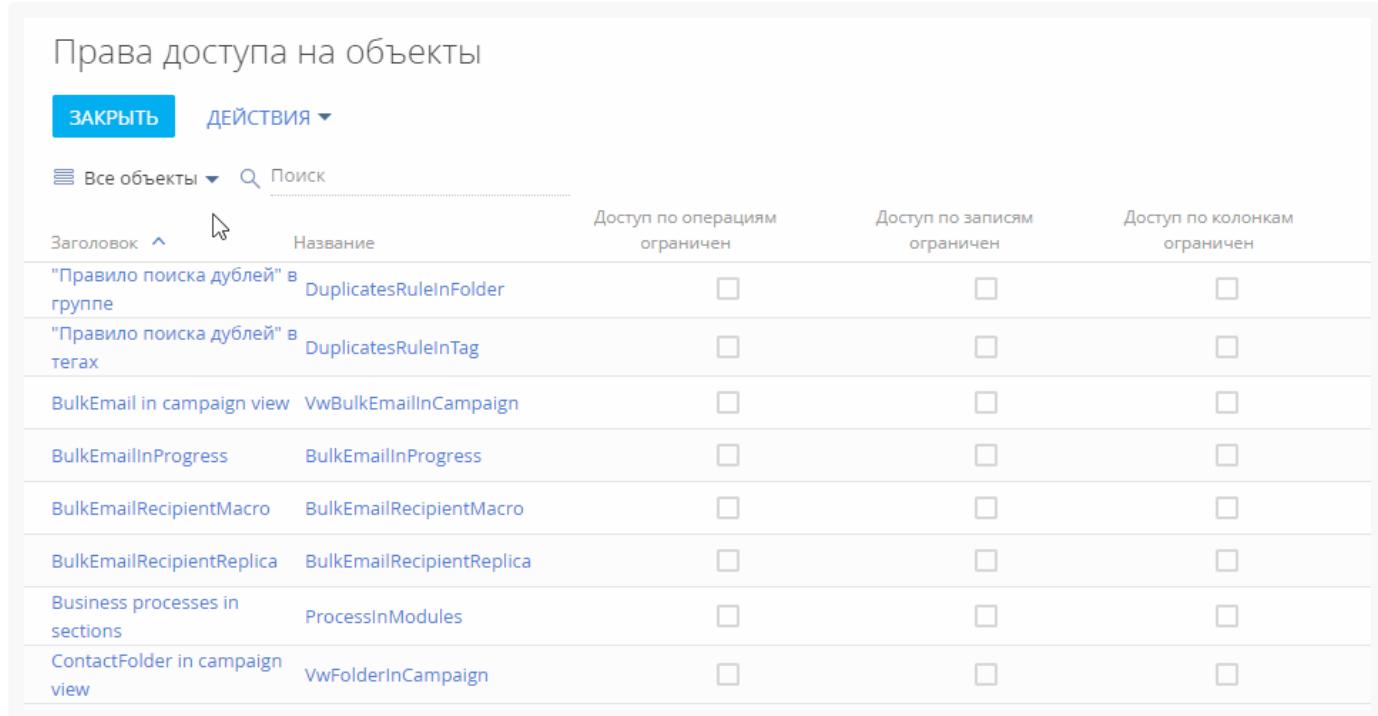
У одного из сотрудников с ролью “Секретари” должна быть возможность просматривать записи раздела, а для остальных секретарей раздел [Продажи] должен быть скрыт.

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.

- 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.
- 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).

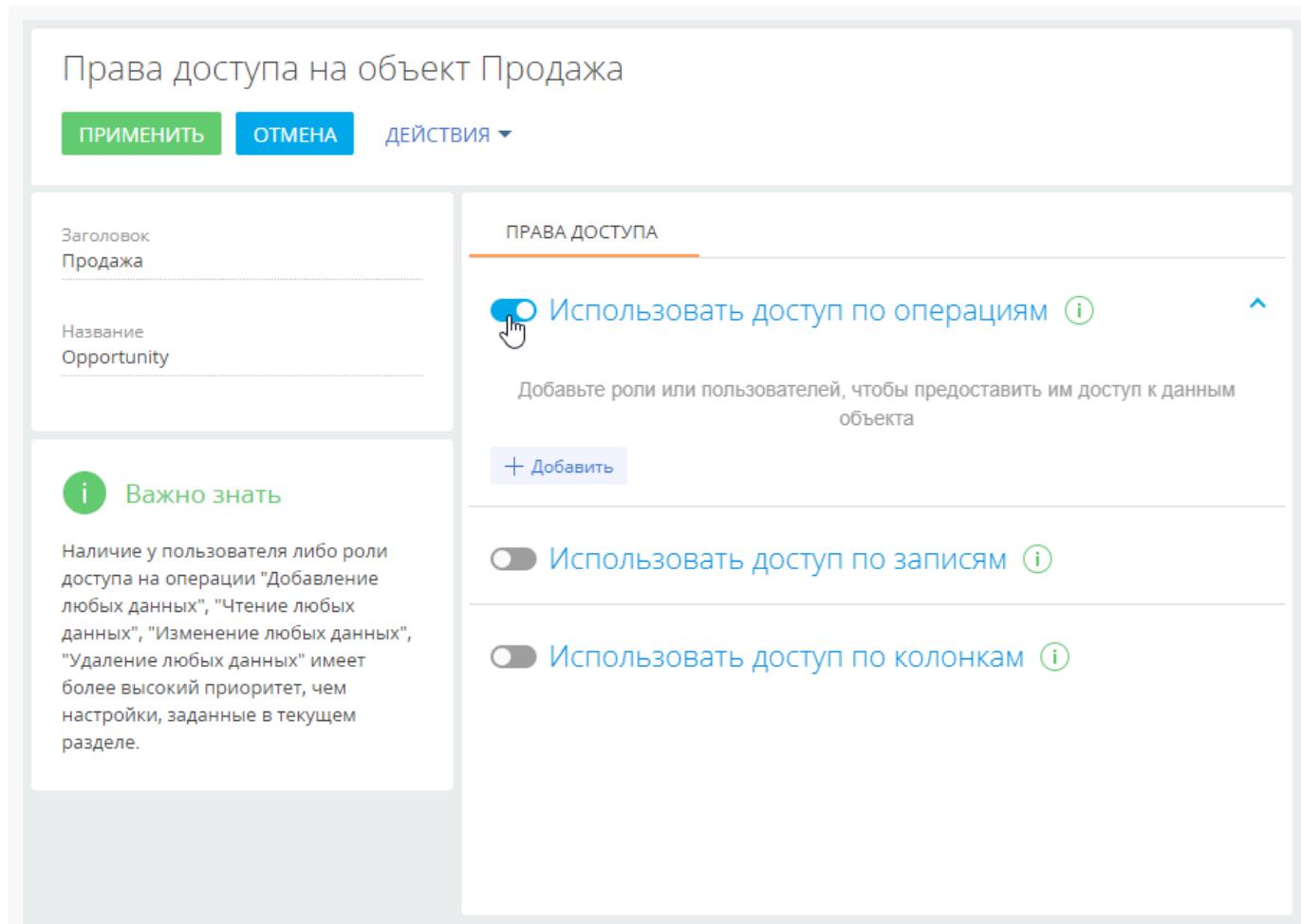
Рис. 1 — Выбор объекта раздела и переход на страницу настройки прав доступа



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"/>

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

Рис. 2 — Включение администрирования по операциям



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:
- роль “All employees” (Все сотрудники) — добавляется автоматически;
 - организационная роль “Менеджеры по продажам”;
 - организационная роль “Менеджеры по продажам. Группа руководителей”;
 - организационная роль “Секретари”;
 - определенный пользователь с ролью “Секретари” (Рис. 3), например, Ульяненко Александра.

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

Права доступа на объект Продажа

ПРИМЕНЕНИЙ **ОТМЕНА** **ДЕЙСТВИЯ ▾**

Заголовок Продажа	ПРАВА ДОСТУПА
Название Opportunity	<input checked="" type="checkbox"/> Использовать доступ по операциям i <input type="checkbox"/> Использовать доступ по записям i <input type="checkbox"/> Использовать доступ по колонкам i
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.	

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 Ульяненко Александра) оставьте признак в колонке [Чтение]. Так пользователь Ульяненко 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.

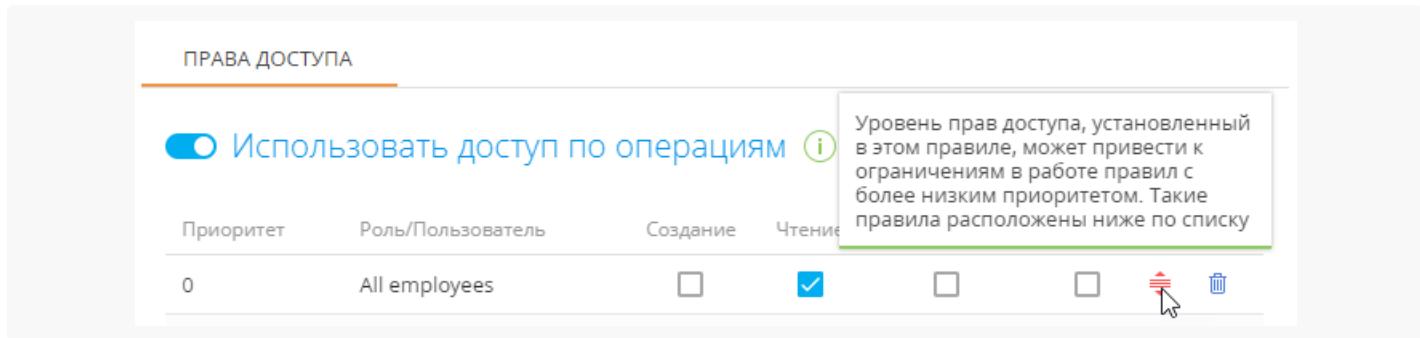
Настроить приоритет прав доступа по операциям

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



ПРАВА ДОСТУПА						
<input checked="" type="checkbox"/>	Использовать доступ по операциям					
Приоритет	Роль/Пользователь	Создание	Чтение	Изменение	Удаление	Установка
0	All employees	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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 вверху 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.

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

Рис. 5 — Настройка приоритета прав доступа

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"/>

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.

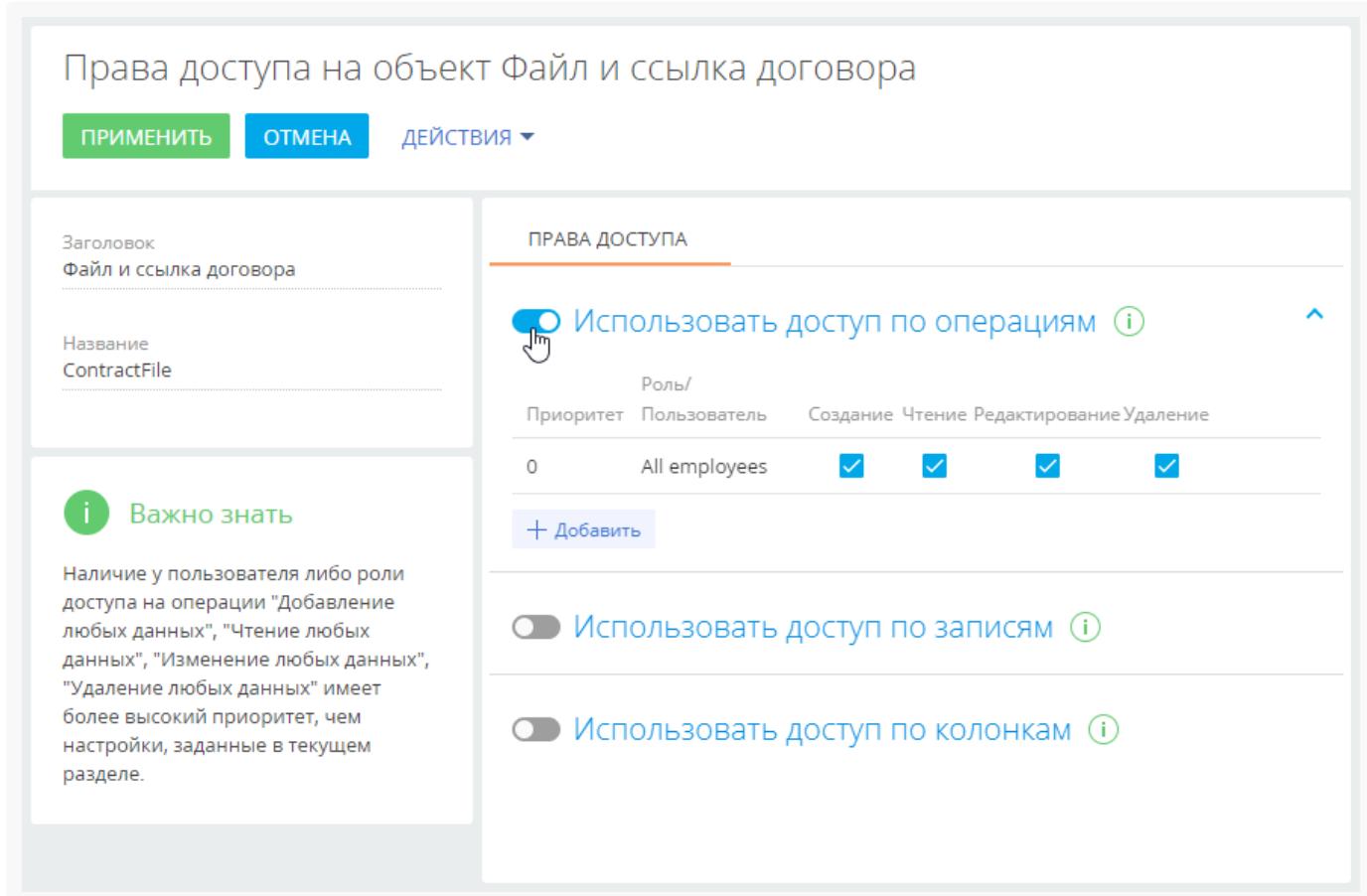
Настроить доступ по операциям в объекте детали

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.

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

Рис. 6 — Включение администрирования по операциям



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

Ускорить обработку сложных запросов к базе данных

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Данная функциональность доступна в Creatio начиная с версии 7.18.4.

Некоторые запросы, отправляемые приложением к базе данных, требуют длительной обработки и могут существенно повлиять на скорость загрузки страницы или выполнения задач. Такие запросы принято называть тяжелыми. К ним относятся:

- сложные фильтры на страницах и в динамических группах;
- сложные аналитические выборки в аналитике разделов;
- сложные пользовательские запросы, реализованные средствами разработки.

Вы можете ускорить обработку тяжелых запросов, перенаправив их на реплику базы данных с доступом только для чтения. Таким образом существенно снижается нагрузка на основную базу данных и освобождаются ресурсы для работы пользователей и других элементов приложения.

Настройка перенаправления тяжелых запросов состоит из следующих шагов:

1. Создать реплику базы данных с доступом только для чтения.
2. Настроить в Creatio доступ к созданной реплике базы данных.

Шаг 1. Создать реплику базы данных.

Создание реплик базы данных отличается для различных СУБД. Подробно этот процесс описан в документации вендоров:

- [Создать реплику базы данных для PostgreSQL](#) (на английском языке).
- [Создать реплику базы данных для MS SQL](#).
- [Создать реплику базы данных для Oracle](#) (на английском языке).

Шаг. 2. Настроить перенаправление тяжелых запросов

1. **Настройте перенаправление** тяжелых запросов на реплику базы данных. Эта настройка выполняется для **Creatio .NET Core** в файле `Terrasoft.WebHost.dll.config`; для **Creatio .NET Framework** в файле `web.config`.

a. Установите признак `UseQueryKinds`.

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

b. Добавьте значение `replicaConnectionStringName="db_Replica"` в параметр `db general`.

Для MS SQL

```
<general connectionStringName="db" replicaConnectionStringName="db_Replica" securityEngine="
```

Для PostgreSQL

```
<general connectionStringName="db" replicaConnectionStringName="db_Replica" maxEntitySchemaSize="
```

2. **Настройте доступ** Creatio к реплике базы данных. Для этого добавьте параметр `db_Replica` в файл `ConnectionStrings.config`:

Для MS SQL

```
<add name="db_Replica" connectionString="Data Source=[ Имя сервера базы данных ]; Initial Catalog=
```

Для PostgreSQL

```
<add name="db_Replica" connectionString="Server=[ Имя сервера базы данных ];Port=[ Порт сервера ]"
```

Для Oracle

```
<general connectionStringName="db" replicaConnectionStringName="db_Replica" currentSchemaName="
```

Для Oracle

```
<add name="db_Replica" connectionString="Data Source=(DESCRIPTION =
(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = [ Database server name ])(PORT = 1521))) (CON
```

Настроить интеграцию с Facebook Messenger

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Вы можете настроить интеграцию с Facebook Messenger, чтобы операторам контакт-центра была доступна возможность обрабатывать в Creatio сообщения, отправленные клиентами в чат вашей публичной страницы Facebook.

1. Настроить обработку чатов в Creatio. [Подробнее >>>](#)

2. Добавить канал Facebook Messenger. [Подробнее >>>](#)

Перед настройкой канала Facebook messenger убедитесь, что в вашем приложении заполнены системные настройки “Адрес Identity сервера” (код “IdentityServerUrl”), “Идентификатор приложения для Identity сервера” (код “IdentityServerClientId”) и “Секретный ключ для Identity сервера” (код “IdentityServerClientSecret”). Если данные системные настройки не заполнены, обратитесь в службу поддержки Creatio.

3. Настроить обработку сообщений внешним чат-ботом (опционально). [Подробнее >>>](#)

Шаг 1. Добавить канал Facebook Messenger

Добавление канала позволяет Creatio получать и отправлять сообщения от имени вашей публичной страницы Facebook. Эта настройка выполняется в разделе [Настройка чатов] дизайнера системы.

1. Перейдите в **дизайнер системы** по кнопке .

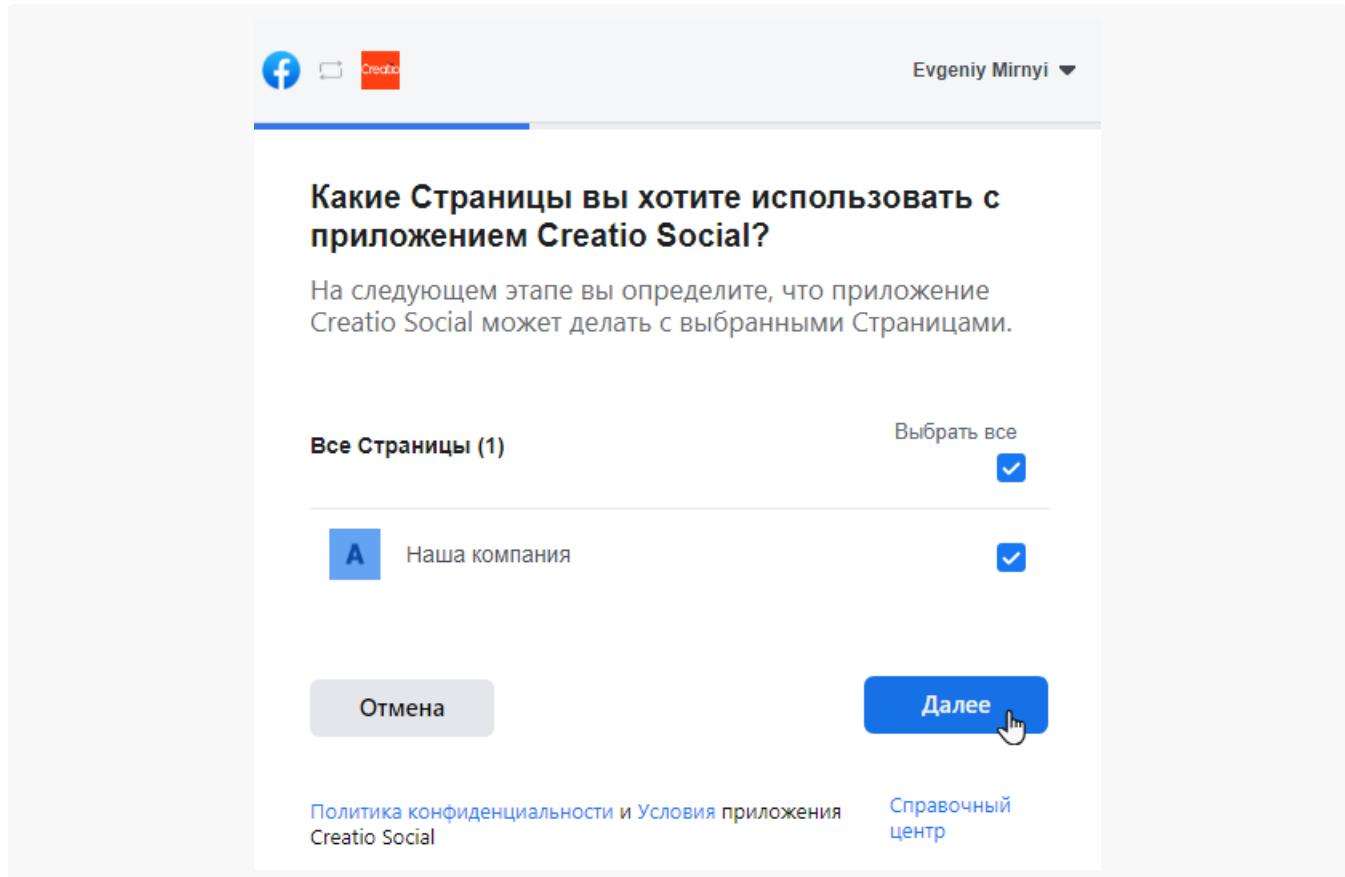
2. Откройте раздел [Настройка чатов].

3. В области [Каналы] нажмите кнопку  . В появившемся меню выберите “Facebook messenger”.

4. В открывшемся окне:

- Авторизуйтесь в Facebook.
- Укажите одну или несколько страниц, которые вы хотите синхронизировать с Creatio. Обратите внимание, что настроить синхронизацию можно только для публичных страниц, но не для личных профилей.
- Нажмите [Далее].

Рис. 1 — Выбор публичной страницы в Facebook для синхронизации с Creatio



- Разрешите Creatio доступ к управлению вашей публичной страницей. Это позволит приложению получать и отправлять сообщения через канал Facebook Messenger от имени вашего бренда. Ограничение доступа к управлению страницей может привести к проблемам в работе чатов.
 - Нажмите [Готово].
- В результате для каждой из выбранных страниц будет создан отдельный канал. Название канала будет соответствовать названию страницы в Facebook, с которой он связан.

Рис. 2 — Настройка доступа к администрированию страницы

Что разрешено делать приложению Creatio Social?

Приложение Creatio Social может работать неправильно, если вы выключите эти опции.

Доступ к перепискам от имени Страницы в Messenger и управление ими ДА

Наша Компания

Показать список Страниц, которыми вы управляете ДА

Наша Компания

Управлять аккаунтами, настройками и Webhooks для Страницы ДА

Наша компания

[Отмена](#) [Назад](#) [Готово](#)

[Политика конфиденциальности и Условия приложения Creatio Social](#) [Справочный центр](#)

5. Чтобы сообщения из созданного канала были доступны для обработки в коммуникационной панели, активируйте канал и привяжите его к очереди.
 - a. В реестре детали [Каналы] кликните по названию созданного канала.
 - b. В открывшейся мини-карточке:
 - Установите индикатор в положение “**Активен**”.
 - Выберите **очередь чата**, в которой будут обрабатываться сообщения, полученные по данному каналу.
 - Укажите **язык**, на котором предполагаете получать сообщения по данному каналу. Это необходимо, чтобы операторы могли использовать шаблоны быстрых ответов на языке клиентов.
 - Нажмите [Применить].
6. При необходимости повторите шаг 5 для всех созданных каналов.

На заметку. Обратите внимание, что одна страница Facebook может быть связана только с одним приложением Creatio. Если вы добавите один канал на несколько приложений, например, среду

разработки, тестовый и продуктовый сайты, то сообщения будут приходить только на тот сайт, интеграция с которым была настроена последней.

Шаг 2. Настроить интеграцию Creatio с внешним чат-ботом (опционально)

Для снижения нагрузки на операторов в Creatio предусмотрена возможность настроить интеграцию с внешним чат-ботом, который обрабатывает типовые запросы пользователей. Данная настройка доступна только для чатов, полученных из канала Facebook Messenger. Процесс настройки чат-бота и его интеграции с Facebook отличается для различных бот-платформ. В общем случае эти инструкции представлены в документации вендоров бот-платформ.

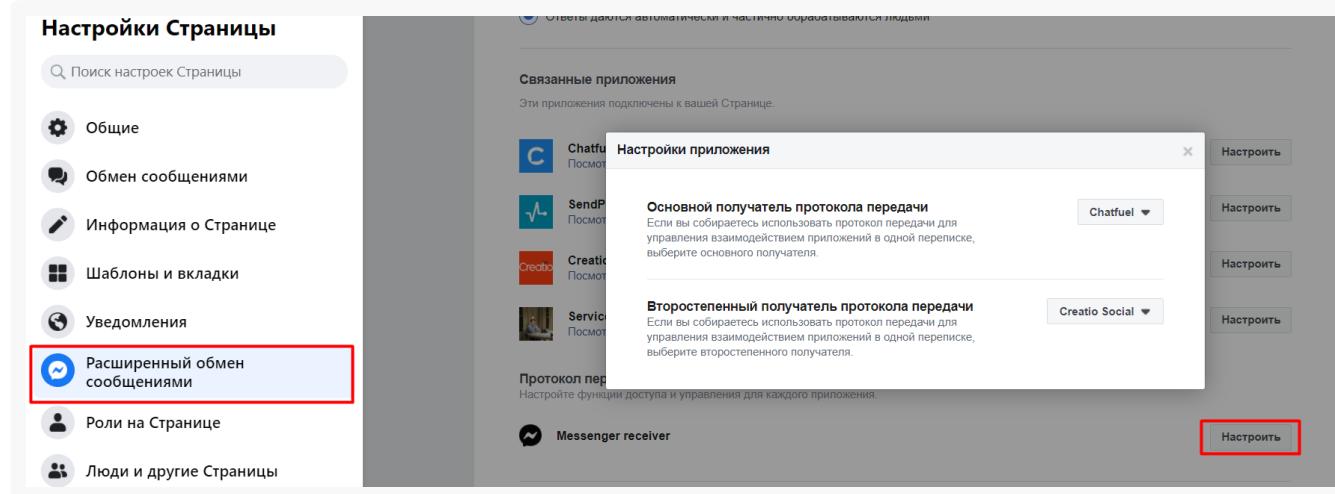
Для работы функциональности вам необходимы:

- Публичная страница на Facebook.
- Настроенный в Creatio [канал Facebook Messenger](#).
- Внешняя бот-платформа, которая поддерживает [протокол передачи](#) (Handover Protocol) и интегрирована с вашей публичной страницей Facebook.

Для настройки интеграции Creatio с чат-ботом:

1. На странице Facebook перейдите в раздел “Настройки” —> “Расширенный обмен сообщениями”.
2. В блоке “Связанные приложения” настройте параметры “Messenger receiver”:
 - Основной получатель протокола передачи — ваша бот-платформа;
 - Второстепенный получатель — приложение Creatio Social.

Рис. 3 — Пример настройки Messenger receiver



В результате сообщения, отправленные клиентами на вашу публичную страницу Facebook, будут обрабатываться чат-ботом, после чего отобразятся в Creatio в разделе [Чаты]. У диалогов, обработанных ботом, поле [Оператор] остается незаполненным.

Настроить фильтры Active Directory

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

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

Формат фильтров

В общем случае фильтры Active Directory имеют следующий формат:

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

В котором <фильтр1> имеет вид:

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

Вы можете использовать необходимое количество операторов и фильтров при настройке фильтрации.

Для создания и настройки фильтров используются следующие операторы:

- = — Логическое равенство.
- ~= — Приблизительное равенство.
- => — Больше или равно.
- <= — Меньше или равно.
- & — “И”.
- | — “Или”.
- ! — “Не”.

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

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

Пример корректно настроенного фильтра

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

Пример некорректно настроенного фильтра

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

Фильтрация пользователей

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

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

В этой функции:

& — Оператор “И” для всех фильтров.

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

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

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

!(isDeleted=TRUE) — Объекты не удалены.

Фильтрация групп

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

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

В этой функции:

& — Оператор “И” для всех фильтров.

objectClass=group — Выбор в массиве всех элементов групп.

userAccountControl — Флаги контроля учетных записей, числовое обозначение.

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

2 — флаг “ACCOUNTDISABLE”.

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

Стандартные фильтры пользователей группы Active Directory

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

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

В этой функции:

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

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

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

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

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

Настроить фильтры для синхронизации пользователей/групп

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

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

Чтобы решить задачу, нужно дополнить фильтр синхронизации пользователей. При поиске объектов по умолчанию используется атрибут `cn` (Common Name). Он обязателен для корректной работы Creatio, так как связан с полем [*ФИО пользователя*]. В условия фильтрации можно также включить атрибут `"displayName"`, который будет отличаться для разных пользователей. То есть, необходимо синхронизировать пользователей с атрибутом `"displayName"`. Для этого:

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

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

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

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

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

Настроить персональный почтовый ящик

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Каждый пользователь системы может настроить для себя интеграцию с одним или несколькими почтовыми ящиками и использовать их для загрузки и отправки почты. Письма из этих почтовых ящиков будут использоваться для обогащения данных контактов, а также связываться с объектами системы: контактами, контрагентами и т. д.

Настроить учетную запись почты преднастроенного провайдера

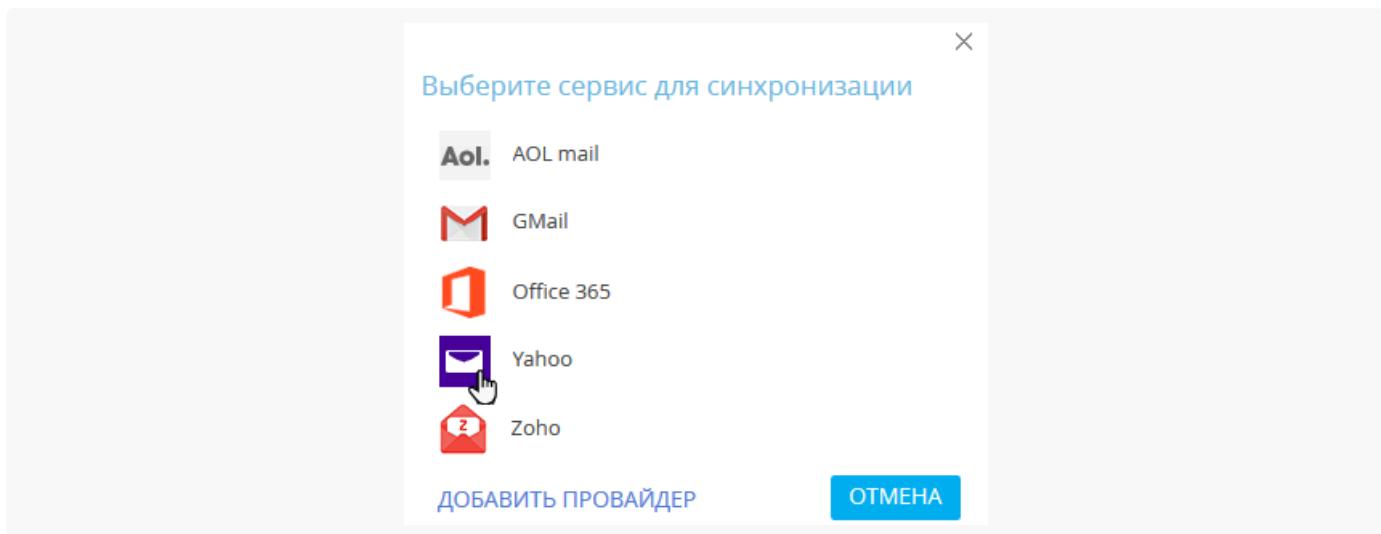
Для добавления учетной записи почты необходимо, чтобы в системе была настроена интеграция с почтовым провайдером. По умолчанию в Creatio настроена интеграция со следующими почтовыми провайдерами, например, AOL, GMail, Yahoo и другими. Для добавления учетной записи в Creatio требуется настроить защищенный доступ для внешних приложений. Настройки выполняются на стороне вашего почтового ящика и различаются в зависимости от используемого провайдера. Подробнее: [Настроить безопасное подключение к почтовому ящику](#).

Если вы пользуетесь услугами другого провайдера, то необходимо настроить синхронизацию по протоколу [IMAP/SMTP](#) или [Exchange](#). Эта настройка выполняется администратором системы.

Для настройки учетной записи почты преднастроенного провайдера:

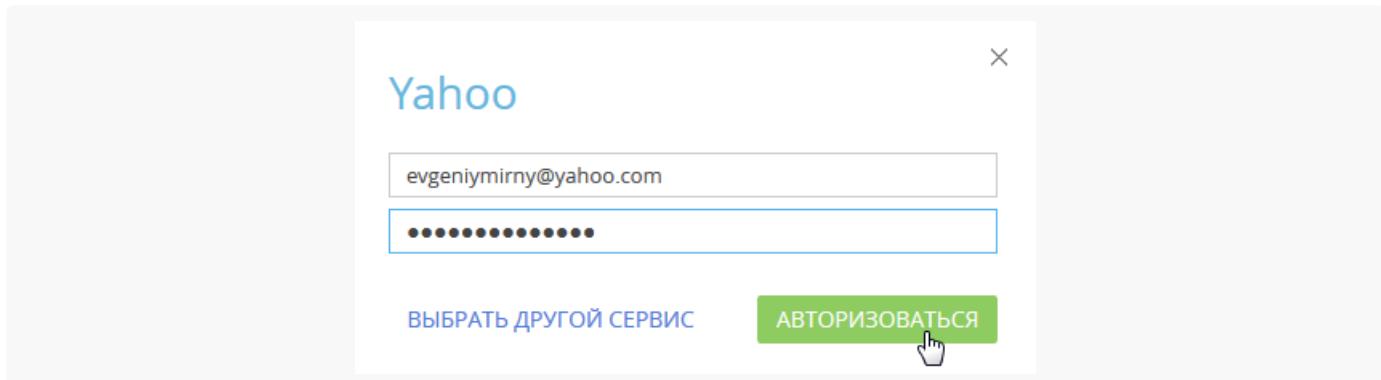
- Перейдите на вкладку [*Email*] коммуникационной панели и в меню кнопки  выберите пункт [*Новая учетная запись*]. В результате откроется окно аутентификации учетной записи.
- Введите адрес электронной почты и нажмите кнопку [*Далее*]. На основании доменного имени система определит почтового провайдера.
- Если почтовый провайдер не был определен автоматически, то откроется окно, в котором вы можете указать нужного провайдера вручную (Рис. 3). В этом случае справочник [*Домены почтовых провайдеров*] автоматически дополнится данными нового почтового провайдера, и при настройке других учетных записей система будет распознавать данного провайдера по доменному имени.

Рис. 3 — Окно выбора почтового провайдера для синхронизации



4. Введите адрес электронной почты и нажмите [Далее]. Система предложит ввести пароль для авторизации учетной записи.
5. Введите пароль для доступа внешних приложений, сгенерированный на стороне провайдера, и нажмите кнопку [Авторизоваться] (Рис. 4).

Рис. 4 — Авторизация учетной записи почты



В результате в системе будет создана учетная запись почты с параметрами по умолчанию. Вы получите уведомление, из которого сможете перейти к загрузке в приложение почты или к [дополнительным настройкам](#) учетной записи, например, добавлению подписи или изменению периода загрузки писем.

Настроить учетную запись почты на корпоративном домене

При работе с корпоративным почтовым доменом необходимо, чтобы в системе была настроена интеграция с почтовым провайдером по протоколу [IMAP/SMTP](#) или [Exchange](#) и соответствие доменных имен почтовым провайдерам. Эти настройки выполняются администратором системы.

На заметку. Для электронной почты на домене Gmail можно настроить вход в учетную запись без ввода логина и пароля (Oauth подключение) предварительно необходимо зарегистрировать приложение в Google Workspace. Подробнее: [Зарегистрировать приложение Creatio в Google Workspace](#).

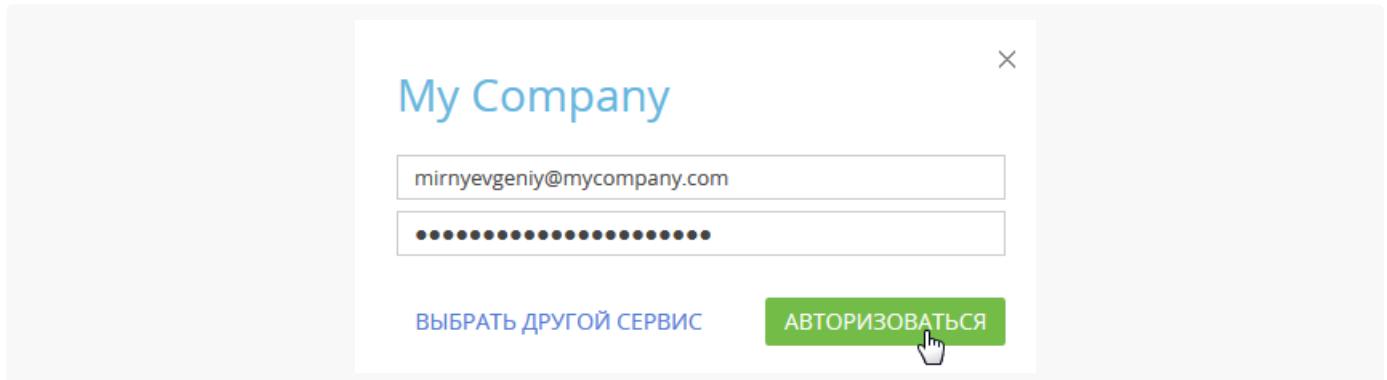
Для настройки учетной записи почты на корпоративном домене:

- Перейдите на вкладку [*Email*] коммуникационной панели и в меню кнопки  выберите пункт [*Новая учетная запись*]. В результате откроется окно аутентификации учетной записи. Этот способ добавления не зависит от наличия настроенных учетных записей.
- Введите адрес электронной почты и нажмите [*Далее*]. На основании доменного имени система определит почтового провайдера.
- Если почтовый провайдер не был определен автоматически, то откроется окно, в котором вы можете указать нужного провайдера вручную. В этом случае справочник [*Домены почтовых провайдеров*] автоматически дополнится данными нового почтового провайдера, и при настройке других учетных записей почты система будет распознавать данного провайдера по доменному имени.

На заметку. Почта с корпоративным доменным адресом, например, mycompany.com, может обслуживаться крупным почтовым провайдером, например, Yahoo или GMail. Если вы не знаете, какой почтовый провайдер выбрать, то уточните эту информацию у системного администратора. Для входа в учетную запись электронной почты на домене Gmail без ввода логина и пароля (OAuth подключение) предварительно необходимо зарегистрировать приложение в Google Workspace. Подробнее: [Зарегистрировать приложение Creatio в Google Workspace](#).

- В появившемся поле введите пароль почтового ящика и нажмите [*Авторизоваться*] (Рис. 5).

Рис. 5 — Авторизация учетной записи почты корпоративного провайдера



В результате в системе будет создана учетная запись почты с параметрами по умолчанию. Вы получите уведомление, из которого сможете перейти к загрузке в приложение почты или к [дополнительным настройкам](#) учетной записи, например, добавлению подписи или изменению периода загрузки писем.

Настройте верификацию для провайдера Elastic Email

ПРОДУКТЫ: MARKETING

Если вы планируете отправлять рассылки в Creatio с помощью провайдера Elastic Email, то верифицируйте ваш email-адрес и корпоративный домен.

В этом случае получатели, которые используют MS Outlook, Hotmail, Gmail и большинство других

современных почтовых сервисов, увидят в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени. В строке отправителя может отобразиться такой текст: "Terrasoft <info@terrasoft.ua> via elasticemail.com".

Чтобы верифицировать ваши email-адреса и домен, выполните следующие шаги:

1. Добавьте ваш корпоративный домен на страницу настройки email-рассылок. [Подробнее >>>](#)
2. Получите SPF- и DKIM-записи. [Подробнее >>>](#)
3. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена. [Подробнее >>>](#)

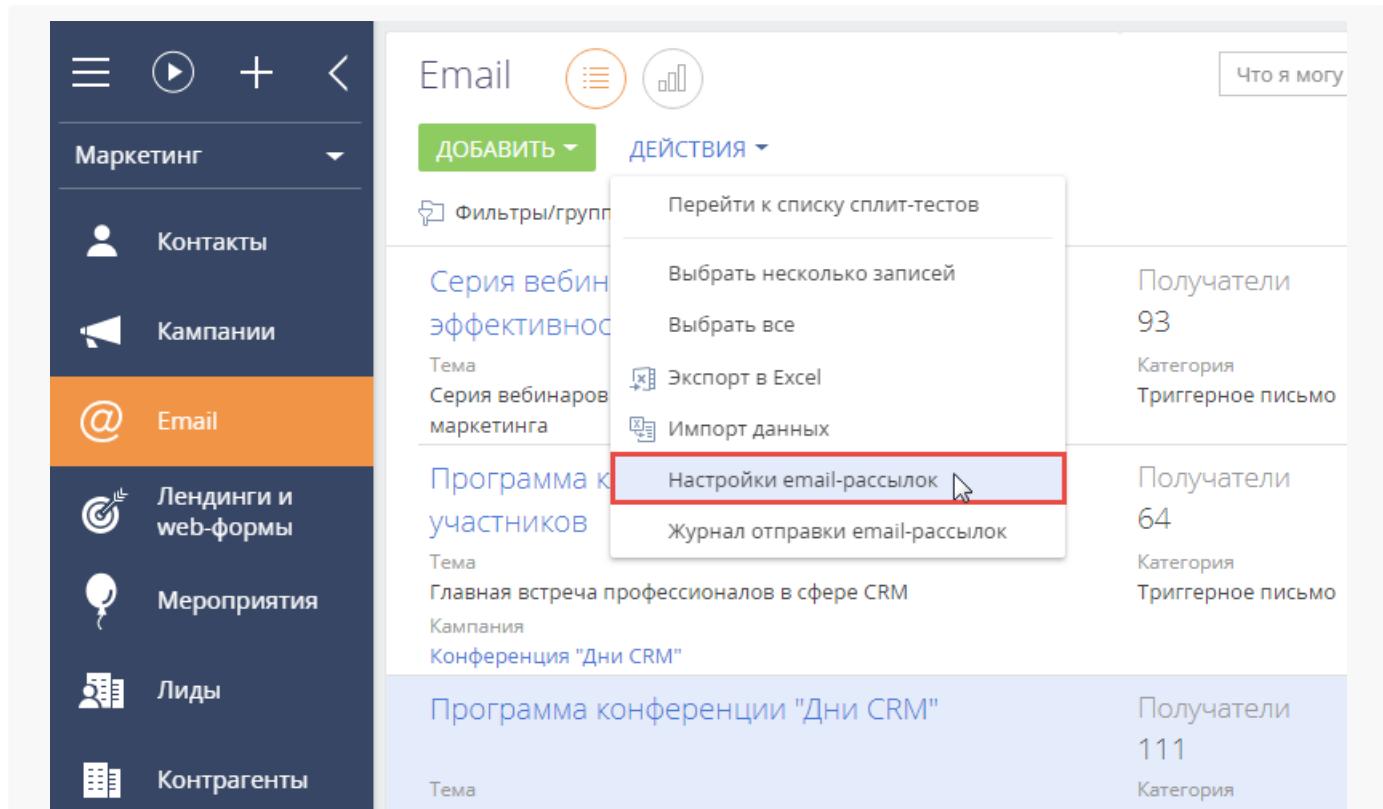
Важно. Если ваш домен не верифицирован, то Elastic Email ограничивает количество отправленных писем до 50 в день.

Добавить корпоративный домен на страницу настройки email-рассылок

До начала отправки массовых рассылок выполните настройки:

1. В разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*] (Рис. 1).

Рис. 1 — Переход на страницу настройки email-рассылок



2. На странице [*Настройки email-рассылок*] на вкладке [*Домены отправителя*] укажите домен вашего email-адреса, с которого будут отправляться рассылки, например "mycompany.com" (Рис. 2).

Рис. 2 — Вкладка [*Домены отправителя*]

The screenshot shows a user interface for managing email settings. At the top, there's a green button labeled 'СОХРАНИТЬ' (Save) and a blue link labeled 'ОТМЕНА' (Cancel). Below this, there are three tabs: 'ОБЩИЕ НАСТРОЙКИ' (General Settings), 'ДОМЕНЫ ОТПРАВИТЕЛЯ' (Sender Domains), and 'НАСТРОЙКА ПРОЦЕССОВ' (Process Configuration). The 'ДОМЕНЫ ОТПРАВИТЕЛЯ' tab is selected and highlighted with an orange border. Inside this section, there's a header with a minus sign, the text 'Домены отправителя', a plus sign, and a 'Обновить' (Update) button. Below this, there's a table with two columns: 'Домен' (Domain) and 'DKIM верифицирован' (DKIM verified). A single row is shown with the value 'mycompany.com' in the first column and 'Нет' (No) in the second column.

Получить SPF- и DKIM-записи

SPF- и DKIM-записи генерируются автоматически в разделе [*Email*] после добавления домена на страницу настройки email-рассылок.

Для получения этих записей в разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*].

SPF- и DKIM-записи будут автоматически сгенерированы в поле [*Инструкции по настройке DKIM/SPF*] на вкладке [*Домены отправителя*] (Рис. 3).

Рис. 3 — Ключи DKIM/SPF для указанного домена

Настройки email-рассылок

[СОХРАНИТЬ](#) [ОТМЕНА](#)

< [ОБЩИЕ НАСТРОЙКИ](#) [ДОМЕНЫ ОТПРАВИТЕЛЯ](#) [НАСТРОЙКА ПРОЦЕССА РАЗБОРА ОТКЛИКОВ](#) >

[Домены отправителя](#) + [Обновить](#)

Домен	DKIM верифицирован
mycompany.com	Нет

Инструкции по настройке DKIM/SPF

Для отправки писем от вашего домена, необходимо чтобы системный администратор поменял DNS запись в хостинге вашего домена. Используйте следующие инструкции для настройки. Примеры настроек для наиболее популярных сервисов хостинга можно найти в [Академии](#).

Инструкции отличаются для разных доменов. Для получения инструкции по домену необходимо добавить и выбрать его в списке.

- Выберите домен в списке на этой странице.
- SPF запись. Добавьте в DNS вашего хостинга первую запись для ключа SPF. Скопируйте и вставьте туда следующий текст:

```
@ TXT v=spf1
include:spf.unisender.com ~all
TXT spf2.0/mfrom,pra
include:senderid.unisender.com ~all
```

* В настройках DNS должна быть только 1 SPF запись. Если SPF запись уже существует, добавьте домен из параметра "include" выше в существующую запись. Убедитесь, что он добавлен до любых IP-адресов.

- Создайте в DNS вторую TXT запись для ключа DKIM. Скопируйте и вставьте туда следующий текст:

```
domainkey TXT o=~ us._domainkey TXT
k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/E
XAe0IP25J4rcfefdN8GScf2rSvv/H+QuGvbwUIb5pqka
fHQ8rcT31b+yBog19y9SheDQXef2RVHO69ImEctbJ6S
oevzgMOLNhivys13Iqk95S+12y6GqrmbRPNaytq5//x
f9gcpEYbJnSTjXBB9qDK4BKjJwolVfZMxmo5EacQIDA
```

* В настройках DNS может быть неограниченное количество записей DKIM

SPF- и DKIM-записи провайдера Elastic Email одинаковы для всех доменов.

Выполнить настройки в DNS-зоне домена

Чтобы обеспечить высокий уровень репутации домена и доставляемости писем, необходимо добавить записи SPF, DKIM, Tracking Domain и политику DMARC в DNS-зону настроек почтового домена.

Для настройки:

- Укажите SPF- и DKIM-записи в DNS-зоне вашего домена:
- Если в DNS-зоне вашего домена еще нет SPF-записи, то ее необходимо скопировать из поля [Инструкции по настройке DKIM/SPF] на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	TXT	v=spf1 a mx include:_spf.elasticemail.com ~all

3. Если у вас уже есть TXT-запись с SPF информацией, то в конец этой записи, перед ее последним оператором (как правило, это **?all**, **~all**, или **-all**) необходимо добавить следующую строку:

Название	Тип	Значение
@	TXT	include:_spf.elasticemail.com

На заметку. В зависимости от DNS-редактора в поле "Host / Name" DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

4. Укажите DKIM-запись в DNS-зоне вашего домена. Для провайдера Elastic Email эта запись имеет такой вид:

Название	Тип	Значение
api._domainkey	TXT	k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbmGbQMzYeMvxwtNQoXN0waGYaciukx8mtMh5czguT4EZJXuCt6V+l56mmt3t68FEX5JJ0q4ijG71BGoFRkl87uJi7LrQt1ZZmZCvrEII0YO4mp8sDLXC8g1aUAoi8TJgxq2MjqCaMyj5kAm3Fdy2tzftPCV/lbdijqmBnWKjtWIDAQAB

На заметку. В некоторых настройках DNS в поле "Host/Name" может потребоваться ввести "api._domainkey.yourdomain.com", заменив значение своим актуальным доменом.

5. Настройте Tracking Domain в DNS-зоне вашего домена.

Чтобы отследить переход по ссылке в полученном письме, Elastic Email переписывает адрес ссылки в шаблоне письма. Поэтому при переходе получателя по ссылке из письма в браузере сначала отобразится адрес с доменом "api.elasticemail.com" и только затем будет выполнена переадресация на указанную при отправке письма ссылку. Чтобы в первой ссылке для отслеживания был указан ваш домен, необходимо создать CNAME-запись в настройках DNS-домена:

Название	Тип	Значение
tracking	CNAME	api.elasticemail.com

6. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена.

Проверка DMARC добавляется только после того, как были добавлены записи SPF и DKIM, и сообщает серверу-получателю, что делать с письмами, отправленными с домена, который не был верифицирован. Чтобы активировать DMARC, добавьте в записи DNS домена правило в виде записи

TXT:

Название	Тип	Значение
_dmarc	TXT	v=DMARC1;p=none;

Тег **v** указывает версию протокола, а **p** — способ обработки писем, которые не прошли проверку.

Больше информации о протоколе в доступно в статье о [DMARC](#) в Википедии. Подробная информация о настройке записей SPF, DKIM, Tracking Domain и DMARC доступна в [инструкции](#) на сайте провайдера Elastic Email.

Управлять лицензиями пользователей

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

При работе в приложении возникает необходимость управлять лицензиями пользователей, например, если необходимо предоставить лицензии новому сотруднику или отзовать их у уволившегося.

Это удобно делать в разделе [*Пользователи системы*]. В этом разделе вы можете управлять лицензиями как для одной учетной записи, так и массово.

На заметку. Также управлять лицензиями можно в менеджере лицензий. Продробнее читайте в статье "[Лицензировать Creatio](#)".

Лицензировать учетную запись пользователя

Аналогичным образом вы можете отзовать лицензии.

- Перейдите в дизайнер системы по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
- В реестре раздела выберите пользователя, которому необходимо предоставить лицензию. На вкладке **Лицензии** страницы пользователя выберите продукты для предоставления лицензии ([Рис. 1](#)).

Рис. 1 — Выбор продуктов для лицензирования

Маянов Дмитрий

ЗАКРЫТЬ



Контакт* Маянов Дмитрий
Тип* Сотрудник компании
Активен

< ОСНОВНАЯ ИНФОРМАЦИЯ РОЛИ **ЛИЦЕНЗИИ** ДЕЛЕГИРОВАНИЕ ПРАВ ПРАВИЛА ДОСТУПА

▲ Лицензии :

a4f dadata connector for creatio cloud	<input checked="" type="checkbox"/>	Выдано 2 из неограничено
account verification for creatio cloud	<input checked="" type="checkbox"/>	Выдано 2 из неограничено
additional details in product selection page for creatio cloud one-time payment	<input type="checkbox"/>	Выдано 1 из неограничено
adobe sign connector for creatio cloud	<input type="checkbox"/>	Выдано 1 из неограничено

4. Закройте страницу.

В результате выбранные лицензии Creatio будут предоставлены либо отозваны для данной учетной записи.

Массово предоставить или отзвать лицензии

- Перейдите в дизайнер системы по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
- Нажмите [Действия] —> **Выбрать несколько записей**.
- Выберите нужных пользователей в реестре, отметив их галочками.
- Нажмите [Действия] —> **Выдать лицензии / Отозвать лицензии**.
- В открывшемся окне выберите продукты Creatio, на которые необходимо предоставить или отзывать лицензии. Отметьте их галочками и нажмите кнопку **Выбрать**.

В результате выбранные лицензии Creatio будут предоставлены либо отозваны для всех указанных пользователей.

Просмотреть логи изменений

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

При работе в Creatio может возникнуть необходимость получения информации об истории изменения

данных в системе. Например, вы можете просмотреть записи контактов, которые редактировались в течение месяца.

Для этого используйте раздел [Журнал изменений] (Рис. 1).

На заметку. По умолчанию логирование журнала изменений отключено. Чтобы изменения логировались, выполните настройки, описанные в статье [Настроить журнал изменений](#).

Рис. 1 — Интерфейс раздела [Журнал изменений]

Заголовок	Название	Логируется
Договор	Contract	<input checked="" type="checkbox"/>
Документ	Document	<input checked="" type="checkbox"/>
Доступ внешних приложений	ExternalAccess	<input type="checkbox"/>
Журнал кампаний	VwCampaignLog	<input type="checkbox"/>
Журнал процессов	VwSysProcessLog	<input type="checkbox"/>
Заказ	Order	<input checked="" type="checkbox"/>
Звонок	Call	<input checked="" type="checkbox"/>
Изменение	Change	<input type="checkbox"/>
Кампания	Campaign	<input checked="" type="checkbox"/>

Журнал изменений логирует добавление, изменение и удаление значений в таблицах базы данных. Это могут быть разделы, детали, справочники и другие объекты системы.

Существуют такие способы получить информацию об изменении данных:

- Логи по всем записям раздела, детали или справочника, в том числе, удаленным, доступны **в журнале изменений**.
- Логи изменений по определенной записи можно открыть непосредственно **с ее страницы**.

Способ 1. Просмотреть логи записи из журнала изменений

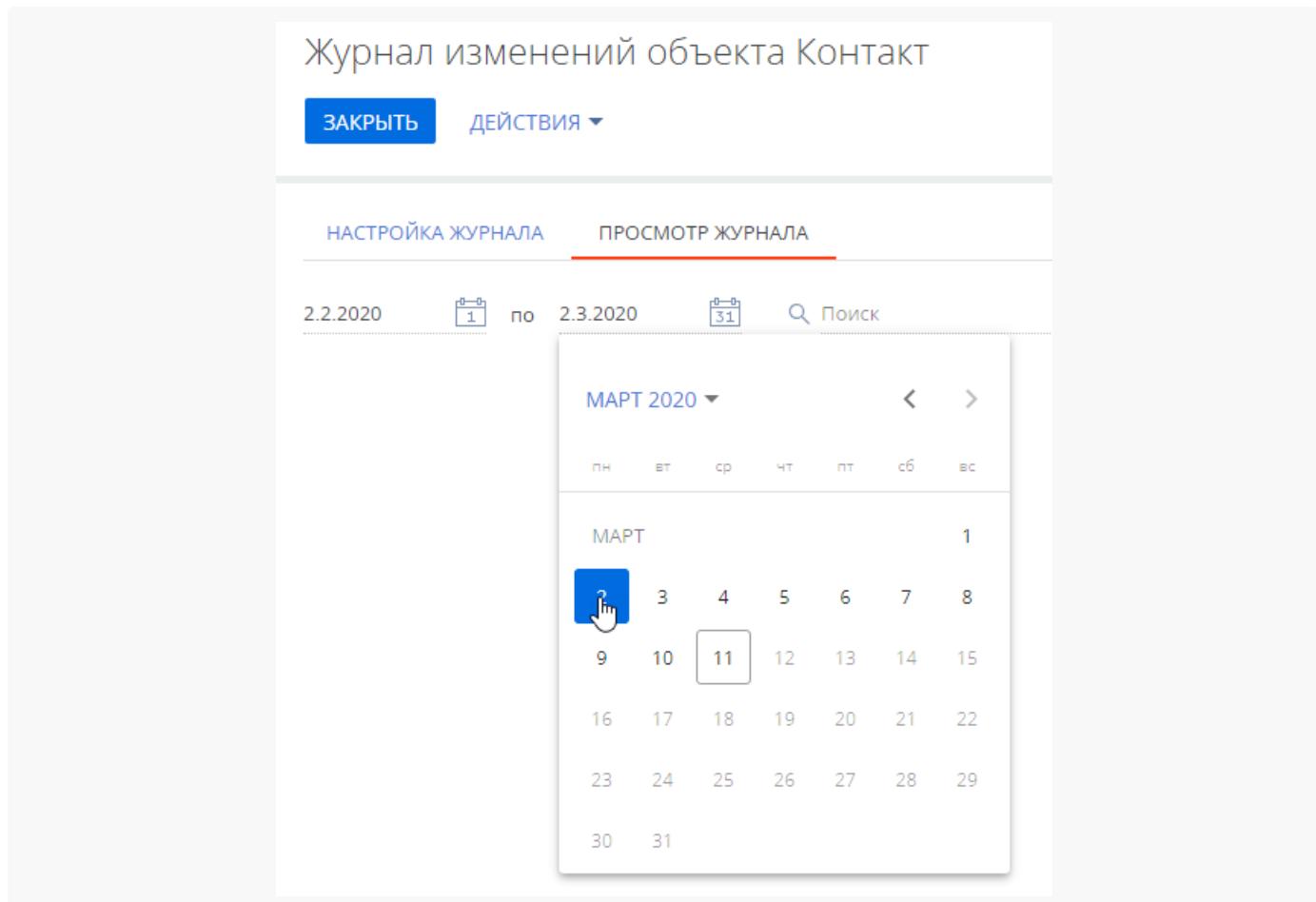
Пример. Необходимо просмотреть все записи контактов, которые менялись в течение прошлого месяца.

- Перейдите в дизайнер системы, например, по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “Журнал изменений”.

На заметку. Для просмотра журнала изменений у вас должны быть настроены права доступа на выполнение системной операции “Просмотр журнала изменений” (код “CanViewChangeLog”).
Подробнее: [Права доступа на системные операции](#).

- Установите фильтр — в нашем случае “Разделы”.
- Выберите необходимый объект при помощи строки поиска или вручную. В нашем примере — в раздел [Контакты]. Кликните по его названию для перехода на страницу изменений.
- Перейдите на вкладку [Просмотр журнала] и установите фильтр по дате изменений (Рис. 2). В нашем примере это период со 2 февраля по 2 марта 2020 года.

Рис. 2 — Настройка фильтрации по дате для логов записи



- Используйте **форму поиска**, чтобы быстро найти нужную запись по названию. В нашем случае — по ФИО контакта (Рис. 3). Чтобы узнать, какие именно значения менялись, кликните по названию записи.

Рис. 3 — Быстрый поиск записи

Журнал изменений объекта Контакт

ЗАКРЫТЬ ДЕЙСТВИЯ ▾

НАСТРОЙКА ЖУРНАЛА		ПРОСМОТР ЖУРНАЛА	
25.2.2020	1	по	2.3.2020 31
			вел
Дата события		Автор изменения	Запись
	25.02.2020, 10:19:23	Молнистая Наталья	Велий Владимир

В результате отобразится перечень записей, в которые вносились изменения в текущем месяце (Рис. 4). Пиктограммы возле даты изменения записи показывают тип выполненных операций: удаление, добавление или редактирование.

Рис. 4 — Просмотр журнала изменений раздела

Журнал изменений объекта Контакт

ЗАКРЫТЬ ДЕЙСТВИЯ ▾

НАСТРОЙКА ЖУРНАЛА		ПРОСМОТР ЖУРНАЛА	
2.2.2020	1	по	2.3.2020 31
			Поиск
Дата события		Автор изменения	Запись
	25.02.2020, 10:19:24	Молнистая Наталья	Велий Владимир
	25.02.2020, 10:19:23	Молнистая Наталья	Велий Владимир
	25.02.2020, 10:08:24	Молнистая Наталья	Этуш Леонид Изяславович
	25.02.2020, 10:04:52	Молнистая Наталья	Жаврук Виталий
	25.02.2020, 10:03:49	Малянов Дмитрий	Варенская Ольга Константиновна
	25.02.2020, 09:55:34	Савченко Ирина	Тепличная Анастасия
	25.02.2020, 09:54:49	Савченко Ирина	Степная Лидия

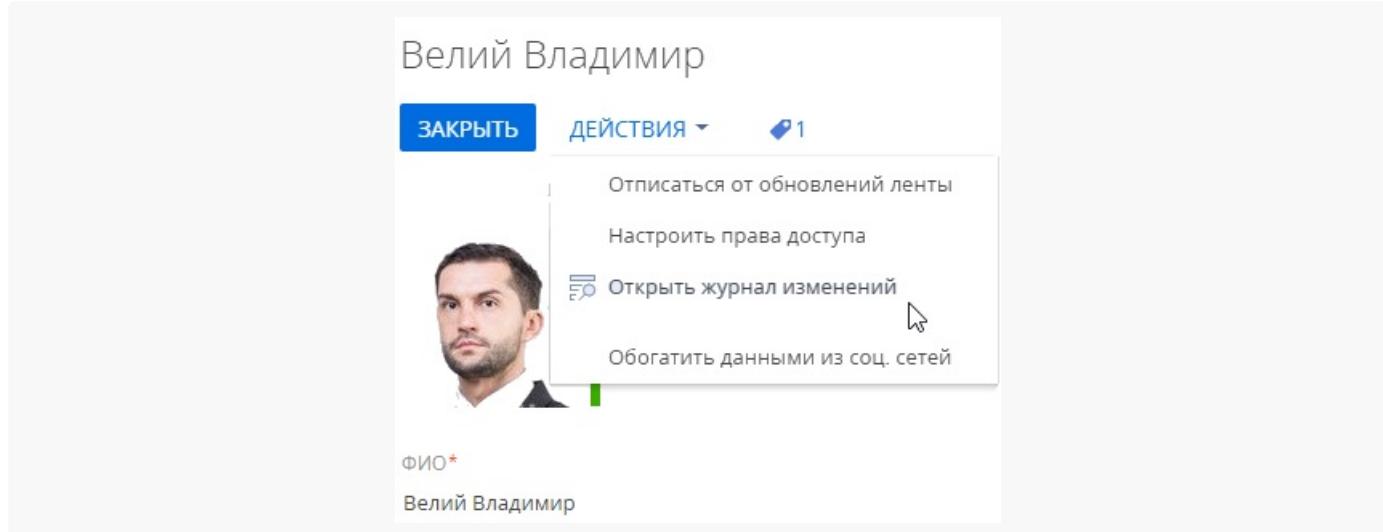
Способ 2. Просмотреть логи со страницы записи

Пример. Необходимо просмотреть историю изменения данных на странице определенного контакта за прошлый месяц.

На заметку. Если у вас не отображается действие [Открыть журнал изменений], проверьте настройку прав доступа на выполнение системной операции “Просмотр журнала изменений” (код “CanViewChangeLog”). Подробнее: [Права доступа на системные операции](#).

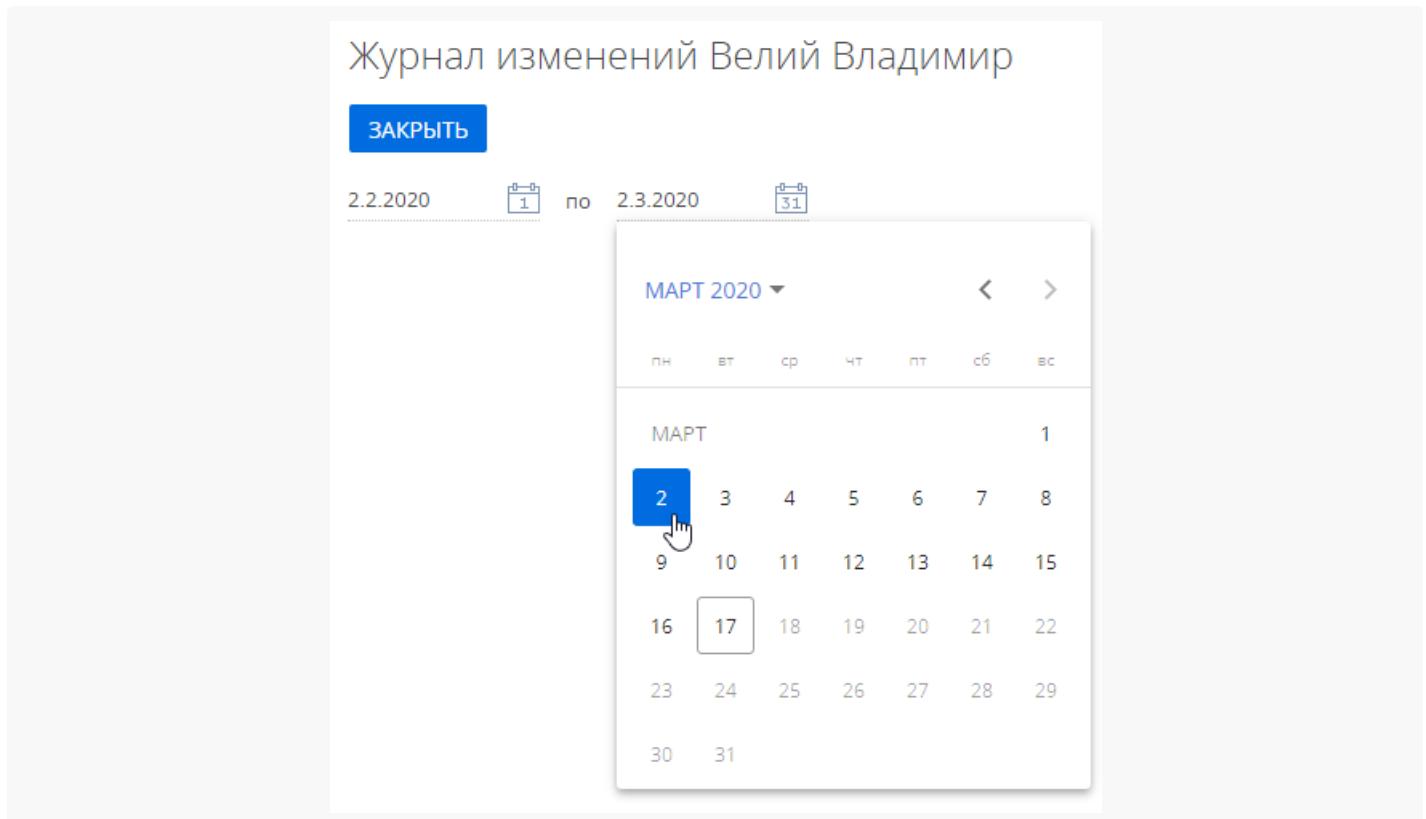
1. Перейдите на страницу нужной записи.
2. Нажмите [Действия] —> [Открыть журнал изменений] (Рис. 5).

Рис. 5 — Действие [Открыть журнал изменений]



3. На открывшейся странице отобразится информация об изменениях выбранной записи:
 - a. даты изменений;
 - b. авторы изменений;
 - c. название записи;
 - d. список колонок, значения которых менялись;
 - e. старые значения колонок;
 - f. новые значения колонок.
4. Установите фильтр по дате изменений, чтобы увидеть логи записи за прошлый месяц(Рис. 6). В нашем примере это период со 2 февраля по 2 марта 2020 года.

Рис. 7 — Настройка фильтрации по дате для логов записи



В результате вы увидите изменения, которые вносились в течение установленного периода в те поля записи, которые были настроены для логирования (Рис. 7).

Рис. 8 — Логи записи

Журнал изменений Велий Владимир					
ЗАКРЫТЬ					
2.2.2020	по	2.3.2020			
Дата события	▼	Автор изменения	Запись	Колонка	Старое значение
	20.03.2020, 14:14:20	Молнистая Наталья	Велий Владимир	Email	vladimirveliy@gmail.com
	25.02.2020, 10:19:23	Молнистая Наталья	Велий Владимир	Email	vladimirveliy@gmail.com
				Мобильный телефон	+380971234567
				Рабочий телефон	+380971234675

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 a web-based application configuration interface. At the top right are buttons for 'MORE ACTIONS' and 'SAVE'. Below them is a navigation bar with tabs: Info, Configuration (which is highlighted with a red underline), Parameters, Rules, SSO, Access, Users, and Privileges. The main content area has a title 'Application Details' and a sub-section for 'creatio site'. Within this section, there is a text input field containing 'site01'. Below the input field is a descriptive note: 'Enter only your personal domain name. For example "name" if your site URL is https://name.creatio.com'.

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:

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

- 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.

- 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.

```
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"
```

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

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

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

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

```
<terrasoft>
<auth providerNames="InternalUserPassword,SSPUserPassword,SsoAuthProvider,SSPSssoAuthProvider">
<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=".AuthCookie" />
</authentication>
```

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

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

b. Выполнение авторизации.

- c. 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 [Настройте 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”).

Создать новый справочник

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Способ создания справочника зависит от того, существует ли в Creatio объект, по которому нужен справочник.

- **Если объект справочника еще не существует**, то справочник будет создан и зарегистрирован автоматически, когда вы добавите и сохраните новое справочное поле в мастере разделов. В этом случае новый справочник будет добавлен в раздел [Справочники], где его можно будет наполнить значениями.
- **Если объект справочника есть в системе**, то необходимо зарегистрировать по нему новый справочник в разделе [Справочники] для управления записями.

Создать справочник в мастере разделов

Справочник создается автоматически при выборе опции [Создать новый справочник], когда вы добавляете новое поле справочного типа в **мастере разделов**.

Пример. В Creatio был настроен пользовательский раздел [Заявки]. На страницу заявки необходимо добавить поле, отображающее тип заявки. Поле будет заполняться информацией из справочника.

Чтобы реализовать данный пример:

1. В разделе [Заявки] перейдите на страницу записи и нажмите кнопку [Вид] —> [Открыть мастер раздела].
2. В дизайнере страницы настройте необходимое поле:
 - a. В области выбора колонки для добавления (в левой части страницы) выберите колонку [Справочник] и перетащите ее на страницу записи.
 - b. В появившемся окне заполните обязательные поля. Если вы хотите, чтобы созданное справочное поле было обязательным для заполнения, то поставьте признак [Обязательное для заполнения].

На заметку. Детально параметры для типа колонки “Справочник” описаны в отдельной статье. [Подробнее >>>](#)

- c. В группе полей [Справочник] выберите опцию [Создать новый справочник] и укажите заголовок и название справочника, который вы хотите создать ([Рис. 1](#)). Поле [Заголовок] соответствует названию справочника в системе и заголовку объекта, а поле [Название] — названию объекта и таблицы в базе данных.
- d. Нажмите кнопку [Сохранить].

Рис. 1 — Создать новый справочник

Новая колонка

СОХРАНИТЬ
ОТМЕНА

Заголовок*	Тип
Название в БД*	UsrRequestType
<input type="checkbox"/> Обязательное для заполнения	
Справочник <ul style="list-style-type: none"> <input type="radio"/> Выбрать существующий справочник <input checked="" type="radio"/> Создать новый справочник 	
Заголовок*	Типы заявок
Название*	UsrRequestTypes
Отображение справочника: <ul style="list-style-type: none"> <input type="radio"/> Всплывающее окно <input checked="" type="radio"/> Список 	

3. Сохраните внесенные в мастер раздела изменения.

В результате после сохранения изменений в мастере раздела созданный справочник будет автоматически зарегистрирован в системе и привязан к пакету, в который мастер сохраняет изменения.

Далее необходимо наполнить его содержимым — перечислить типы заявок. Для этого:

1. Откройте дизайнер системы по кнопке  в правом верхнем углу приложения и в группе [Настстройка системы] кликните по ссылке “Справочники”.
2. С помощью быстрого фильтра по названию найдите созданный справочник [Типы заявок] и откройте его наполнение.
3. По кнопке [Добавить] создайте в справочнике типы заявок ([Рис. 2](#)).

Рис. 2 — Наполнение справочника [Типы заявок]

Справочники

ДОБАВИТЬ ЗАКРЫТЬ ДЕЙСТВИЯ ▾

Типы заявок

Фильтры/группы ▾

Название

Отпуск

Командировка

Больничный

Перенос рабочего дня

В результате вы сможете использовать информацию из созданного справочника [Типы заявок] при заполнении поля [Тип] на странице заявки ([Рис. 3](#)).

Рис. 3 — Справочное поле [Тип]

Тип

Больничный

Командировка

Отпуск

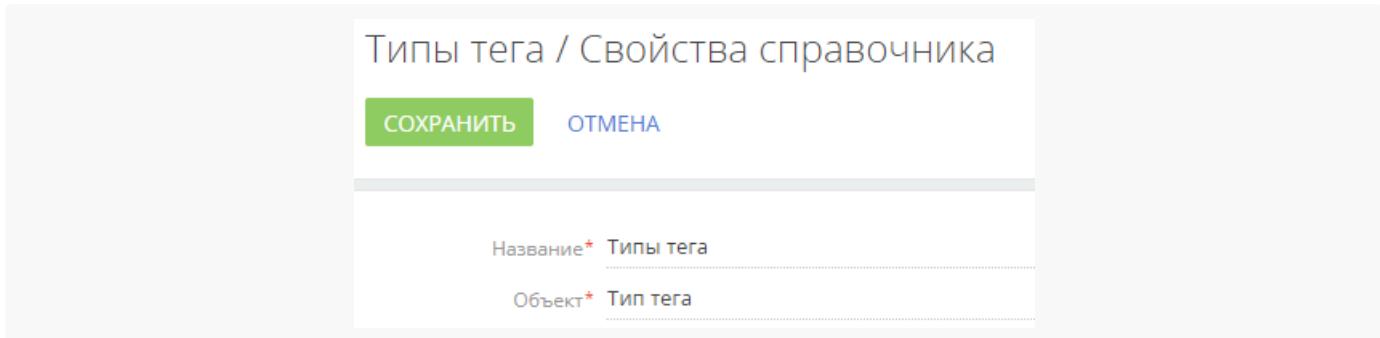
Перенос рабочего дня

Зарегистрировать справочник на основании существующего объекта

Если вы хотите зарегистрировать справочник по **существующему объекту** в системе, то для этого:

1. Откройте дизайнер системы по кнопке в правом верхнем углу приложения и в группе [Настойка системы] кликните по ссылке [Справочники].
2. Нажмите кнопку [Добавить справочник] и укажите название справочника, а также объект, который содержит структуру данных справочника ([Рис. 4](#)).

Рис. 4 — Регистрация справочника по существующему объекту



В результате справочник будет зарегистрирован и заполнен данными в соответствии со структурой объекта.

Синхронизировать контакты с Microsoft Exchange и Microsoft 365

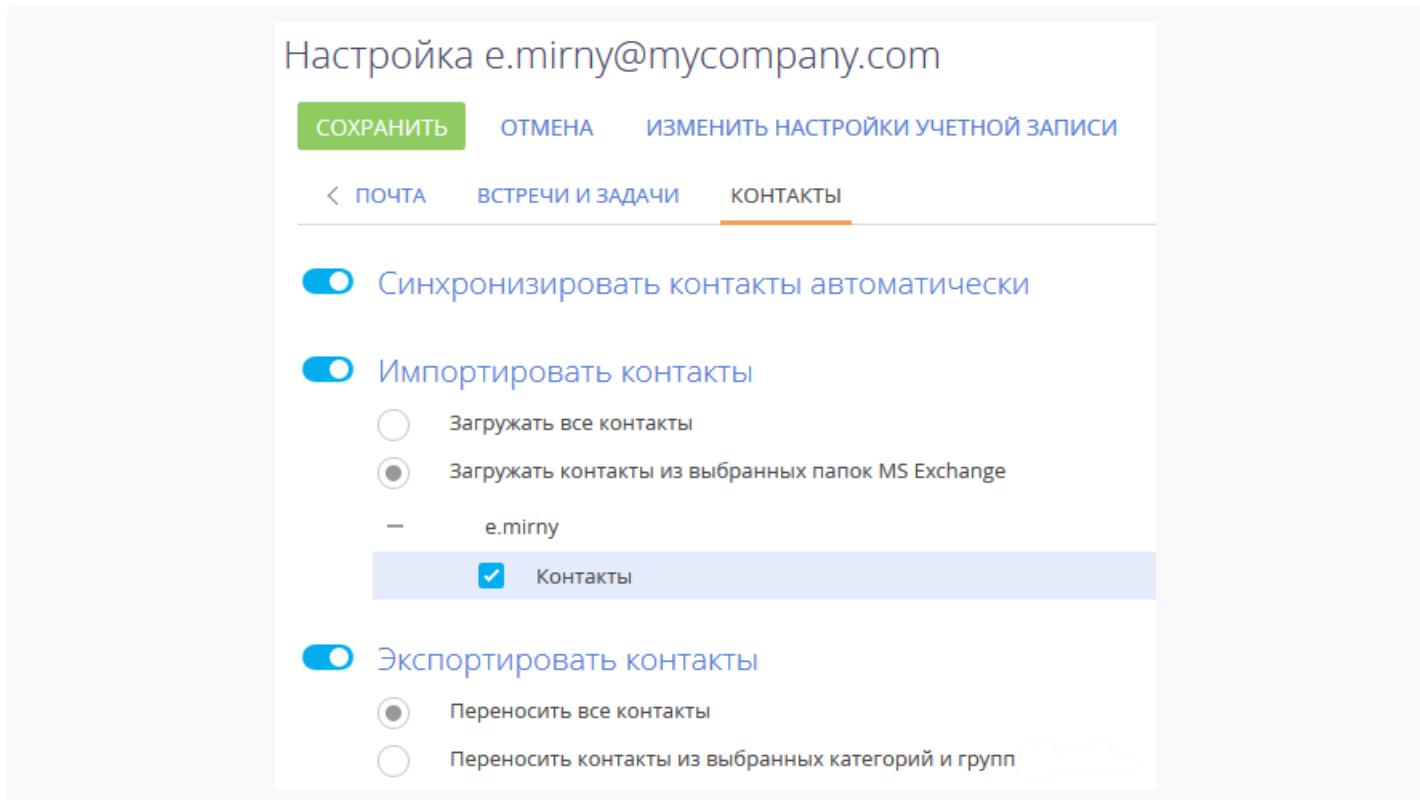
ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Настройка синхронизации контактов Creatio с контактами Microsoft Exchange или Microsoft 365 выполняется на странице настройки учетной записи почты ([Рис. 1](#)). На страницу можно перейти несколькими способами:

- Из коммуникационной панели, нажав —> [Редактировать настройки].
- Из раздела [Контакты], выбрав [Действия] —> [Синхронизировать контакты] —> [Настроить...].

Команда содержит в названии имя учетной записи, например [Настроить example@mail.com].

Рис. 1 — Пример настройки синхронизации контактов Creatio с контактами Microsoft Exchange



Настроить импорт контактов в Creatio

Чтобы настроить импорт контактов из Microsoft Exchange или Microsoft 365 в Creatio:

1. На вкладке [Контакты] страницы настройки синхронизации с почтовым ящиком установите признак [Импортировать контакты].
2. Выберите опцию [Загружать все контакты], чтобы импортировать все записи почтового ящика из папок с типом “Контакты”.
Если вы хотите импортировать контакты только из некоторых папок, то выберите опцию [Загружать контакты из выбранных папок MS Exchange]. Нажмите + и установите признаки напротив необходимых папок.
3. Нажмите кнопку [Сохранить].

На заметку. Creatio автоматически связывает импортированные контакты с контрагентами. Если в Creatio было найдено более одного контрагента с одинаковым названием, то контакт будет импортирован без привязки к контрагенту. Если сотрудник, выполняющий импорт, имеет доступ только к одному из этих контрагентов, то контакт будет импортирован с привязкой к этому контрагенту.

Настроить экспорт контактов из Creatio

Чтобы настроить экспорт контактов из Creatio в Microsoft Exchange или Microsoft 365:

1. На вкладке [Контакты] страницы настройки синхронизации с почтовым ящиком установите признак [Экспортировать контакты].

2. Выберите опцию [Переносить все контакты], чтобы экспорттировать все контактные лица, к которым у вас есть доступ.
3. Если вы хотите экспорттировать только контакты определенных типов либо контакты из указанных групп, то выберите опцию [Переносить контакты из выбранных категорий и групп Creatio].
 - a. Установите признак [Сотрудники] и/или [Клиенты], чтобы при синхронизации экспорттировать все контакты соответствующих типов (будут экспортированы только те контакты, к которым у вас есть доступ).
 - b. Установите признак [Из групп], чтобы экспорттировать контакты, входящие в определенные группы, настроенные в системе, например, "Сотрудники". Раскройте перечень групп и отметьте необходимые группы.
4. Нажмите кнопку [Сохранить].

На заметку. Создание групп рассмотрено в статье "[Группы](#)".

Синхронизировать контакты с Microsoft Exchange и Microsoft 365

Синхронизация ваших контактов между сервером Exchange и Creatio может выполняться автоматически. Чтобы включить автоматическую синхронизацию, на странице настройки синхронизации с почтовым ящиком установите признак [Синхронизировать контакты автоматически]. Чтобы выполнить синхронизацию немедленно, перейдите в раздел [Контакты], нажмите кнопку [Действия] —> [Синхронизировать контакты] —> [Запустить синхронизацию].

Просмотреть и архивировать журнал аудита

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

В журнале аудита системных операций автоматически регистрируются события, связанные с изменением структуры ролей пользователей, распределением прав доступа, изменением значений системных настроек, а также авторизацией пользователей в системе.

Открыть журнал аудита

Перейдите в дизайнер системы, например, по кнопке  в правом верхнем углу приложения и в блоке "Настройка системы" откройте ссылку "Системные настройки". В группе "Пользователи и администрирование" кликните по ссылке "Журнал аудита".

На заметку. Для просмотра журнала аудита системных операций требуется доступ к системной операции "Просмотр раздела "Журнал аудита" (код "CanViewSysOperationAudit"). Для просмотра и выполнения архивации записей требуется доступ к системной операции "Управление разделом

“Журнал аудита” (код “CanManageSysOperationAudit”). Подробнее: [Права доступа на системные операции](#).

В представлении [Журнал аудита] отображается список последних зарегистрированных событий. В представлении [Архив журнала] вы можете увидеть список событий, в отношении которых было выполнено действие [Архивировать журнал]. Архивные события хранятся в отдельной таблице.

На заметку. Если ваше приложение развернуто on-site на .NET Core с использованием горизонтального масштабирования, то для отображения IP-адресов пользователей необходимо выполнить дополнительную настройку балансировщика. Подробнее: [Настроить отображение IP-адресов в журнале аудита для .NET Core](#).

В реестре раздела [Журнал аудита] доступны следующие данные:

- [Тип события] — перечень типов системных событий содержится в справочнике [Типы событий], например, “Авторизация пользователя”, “Сессия пользователя” и т. д.
- [Дата события] — дата и время наступления события.
- [Результат] — перечень результатов системных событий содержится в справочнике [Результаты событий]. Например, попытка авторизации пользователя может завершиться с результатом “Авторизация” или “Отказ авторизации”, если авторизация была неудачной.
- [IP-адрес] — IP-адрес пользователя, выполнившего операцию, в результате которой наступило системное событие. Например, IP-адрес пользователя, совершившего попытку авторизации в системе.

На заметку. В случае, если пользователь заходит через VPN или запрос проходит через несколько прокси-серверов, перечислены IP-адреса каждого последующего прокси-сервера. В этом случае самый правый IP-адрес — это IP-адрес самого последнего прокси-сервера, а самый левый IP-адрес — это первый IP-адрес, который можно отследить.

- [Ответственный] — пользователь, выполнивший операцию, в результате которой наступило системное событие. Например, имя сотрудника, который совершил попытку авторизации в системе.
- [Описание] — подробное описание события, например, “Авторизация пользователя Евгений Мирный. IP-адрес: 192.168.0.7”. Описание событий генерируется системой автоматически.

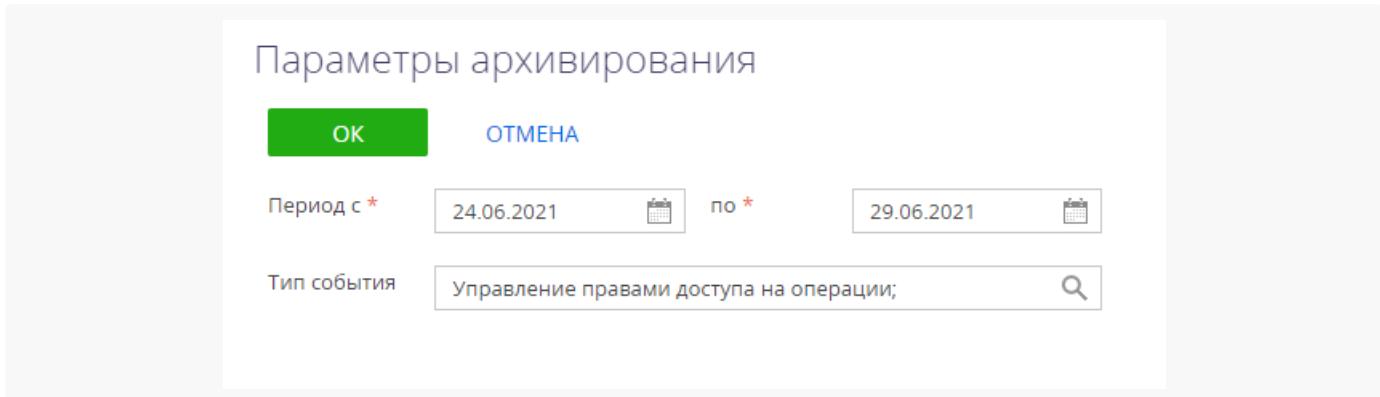
Архивировать журнал аудита

Журнал аудита системных операций содержит действие [Архивировать журнал], при выполнении которого записи журнала копируются в отдельную архивную таблицу.

Для архивации журнала аудита:

1. Нажмите  , чтобы открыть реестр раздела [Журнал аудита].
2. Нажмите [Действия] —> [Архивировать журнал].
3. На открывшейся странице [Параметры архивирования] (Рис. 2) настройте параметры архивации.

Рис. 2 — Окно [Параметры архивирования]



4. [Период с], [по] — период, за который необходимо архивировать события. Будет выполнена архивация только тех событий, дата которых попадает в указанный диапазон.
5. [Тип события] — выберите типы событий для архивации. Будут архивированы только те события, типы которых совпадают с выбранными. Вы можете выбрать несколько типов.

На заметку. Выполнение действия архивации логируется в журнале как “Управление журналом аудита администрирования”. По завершении операции отображается сообщение, информирующее о количестве архивированных записей.

В результате вы увидите список заархивированных событий, даты которых попадают в указанный период, в представлении «Архив журнала» () раздела [Журнал аудита].

Синхронизировать контакты и активности с Google

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Настроить синхронизацию

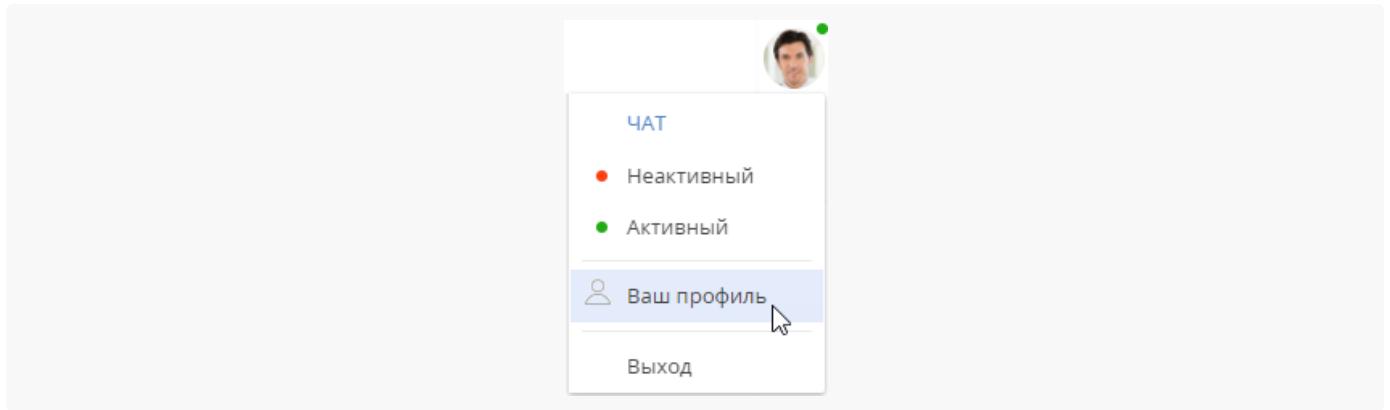
Чтобы вы могли синхронизировать контакты и календари Google с Creatio, необходимо выполнить предварительную настройку:

1. Настроить доступ для вашей учетной записи Creatio к календарям и контактам Google. [Подробнее > > >](#)
2. Настроить автоматическую синхронизацию Creatio с Google. [Подробнее > > >](#)

Шаг 1. Настроить доступ к учетной записи пользователя Google

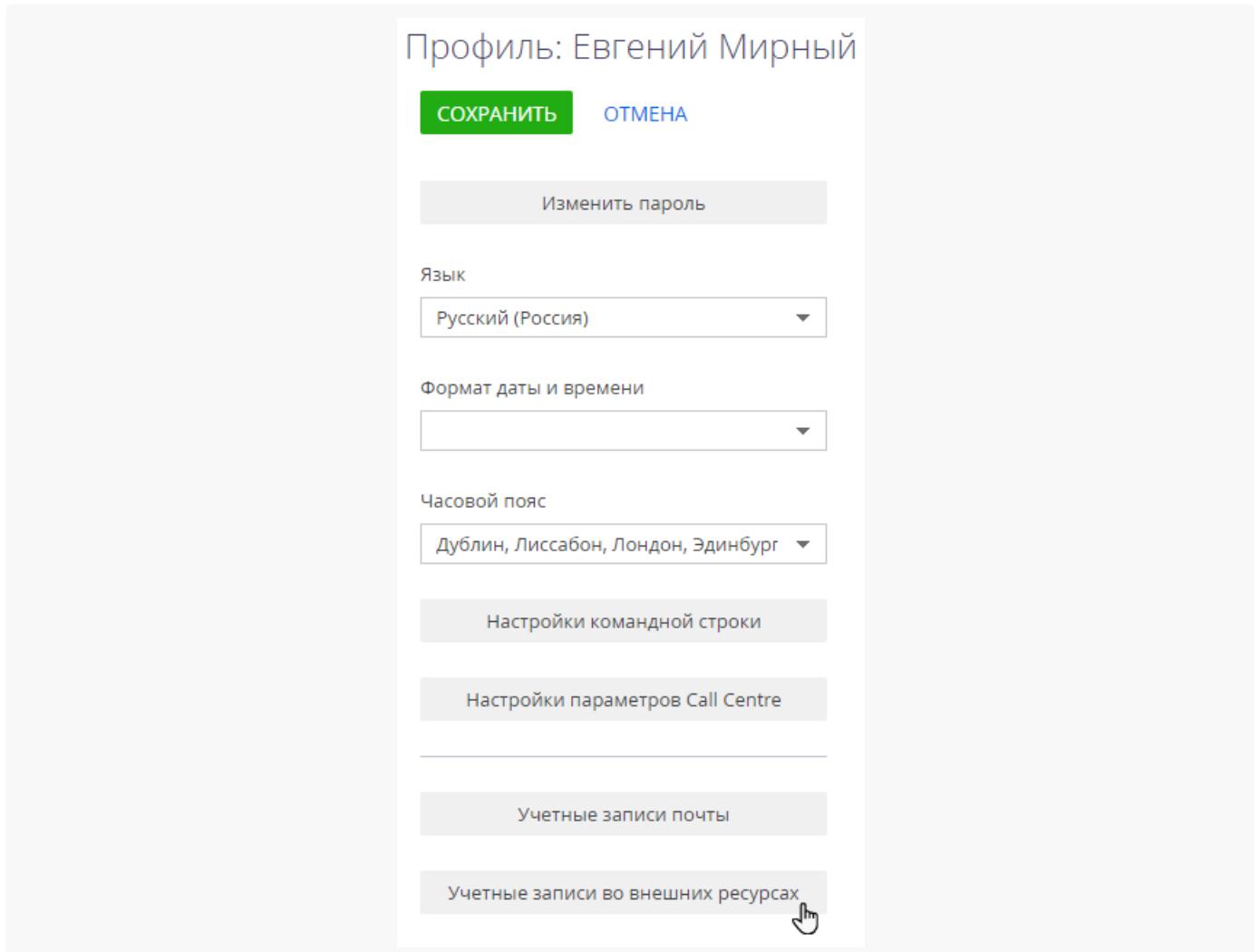
1. Перейдите в ваш профиль, например, нажав на фотографию в правом верхнем углу приложения, и выбрав пункт [Ваш профиль] (Рис. 1).

Рис. 1 — Переход к профилю пользователя



- На странице профиля нажмите кнопку [Учетные записи во внешних ресурсах] (Рис. 2)

Рис. 2 — Учетные записи во внешних ресурсах



- На открывшейся странице нажмите [Добавить] → Google.
- Выберите в появившемся списке учетную запись Google с корпоративной почтой.
- Разрешите приложению Creatio доступ к календарям и контактам вашего аккаунта Google

Рис. 3 — Пример настроенной синхронизации с учетной записью Google

Учетные записи

Что я могу для вас сделать? >

Creatio
7.18.4.1532

ДОБАВИТЬ ▾ ДЕЙСТВИЯ ▾ ЗАКРЫТЬ

Внешний сервис ^ Логин Пользователь Общая

Google Нет

Шаг 2. Указать параметры синхронизации в контактах

Рассмотрим пример настройки синхронизации в разделе [Контакты]:

1. Перейдите в раздел [Контакты].
2. Создайте [личный тег](#), по которому будет проводиться синхронизация, например, “Синхронизация с Google”.

На заметку. Синхронизация проводится только по тем записям, которые отмечены личным тегом. Записи, отмеченные корпоративным или публичным тегом, не синхронизируются.

3. В меню кнопки [Действия] выберите команду [Синхронизировать контакты] — > [Настроить...]. Откроется страница настроек, в которой:
 - a. Для автоматической синхронизации активностей установите признак [Синхронизировать активности автоматически] и выберите период синхронизации. Для запуска синхронизации с определенной даты в поле [Синхронизировать начиная с] выберите необходимую дату.
 - b. Для автоматической синхронизации контактов установите признак [Синхронизировать контакты автоматически] и выберите период синхронизации.
 - c. Для синхронизации контактов с определенным тегом в поле [Из Creatio в Google передавать все контакты с тегом] выберите нужный тег.
4. Нажмите кнопку [Сохранить].

На заметку. Дата и время выполнения последней синхронизации отображается на странице настроек.

В результате в системе будет сохранена ваша учетная запись в Google и тег контактов для синхронизации, а в указанном временном интервале будет запускаться автоматическая синхронизация контактов.

На заметку. Аналогично выполняется настройка синхронизации с Google в разделе [Активности]. Обратите внимание, что в настройках синхронизации раздела [Активности] нет необходимости указывать тег для синхронизации задач.

Синхронизировать контакты Creatio с контактами Google

Используйте возможность синхронизации для добавления в Creatio контактов из Google. Синхронизация контактов из Creatio в Google выполняется только для записей, отмеченных личным тегом, указанным в настройках синхронизации.

Для первичного запуска синхронизации:

1. Перейдите в раздел [Контакты].
 2. В меню кнопки [Действия] выберите команду [Синхронизировать контакты] —> [Запустить синхронизацию].
- Запустится процесс синхронизации, в результате которого у вас в Gmail будет добавлена новая группа контактов “Creatio”.
3. Переместите необходимые вам контакты Gmail в группу контактов “Creatio”.
 4. Повторно запустите синхронизацию контактов, выбрав действие [Синхронизировать контакты] —> [Запустить синхронизацию].

В результате контакты Gmail, которые находились в группе “Creatio”, будут добавлены в Creatio с личным тегом, который был указан при настройке синхронизации с Google.

На заметку. В случае настройки автоматической синхронизации процесс запускается автоматически.

В дальнейшем синхронизация контактов Google и Creatio выполняется в обе стороны. Синхронизация выполняется только с теми записями, которые были изменены или добавлены с момента выполнения предыдущей синхронизации.

Если запись была параллельно изменена в Gmail и Creatio, то при следующем запуске синхронизации останутся те изменения, которые были выполнены позднее.

При удалении записи в Gmail или Creatio при следующей синхронизации эти записи не будут удалены из Creatio или Gmail. В первом случае из таких записей будут удалены теги. Во втором случае записи будут исключены из группы “Creatio”.

Синхронизировать активности Creatio с календарем Google

Если наряду с расписанием Creatio вы используете календарь Google для планирования задач, то рекомендуем синхронизировать эти данные.

Обязательным условием для синхронизации расписания Creatio с календарем Google является предварительная регистрация приложения Creatio в G Suite. Подробнее: [Зарегистрировать приложение Creatio в G Suite](#).

Для запуска синхронизации из раздела [Активности] нажмите кнопку [Действия] и выберите команду [Синхронизировать активности] —> [Запустить синхронизацию].

При выполнении действия запускается синхронизация активностей Creatio с календарем учетной записи Google, указанной в настройках синхронизации. Из Creatio синхронизируются все активности с отметкой [Отображать в расписании]. Синхронизация происходит по полю [Организатор]. При этом, если у

организатора встречи не настроена синхронизация, поле [*Организатор*] заполняется тем участником активности, который провел синхронизацию. Если коллективная задача создана в Google, то при синхронизации с Creatio у автора будет добавлена коллективная задача со списком участников на детали [*Участники*]. В список участников добавляются контакты, у которых в блоке [*Средства связи*] указан e-mail адрес, совпадающий с указанным e-mail адресом коллективного мероприятия в Google. При этом у участников эта коллективная задача отобразится только после выполнения ими синхронизации с Google.

Если организатор коллективной задачи, созданной в Creatio посредством синхронизации с Google, внес в нее изменения, то все изменения отобразятся в Google.

На заметку. Синхронизация также может запускаться автоматически во временном интервале, указанном в настройках синхронизации.

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 в 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**".

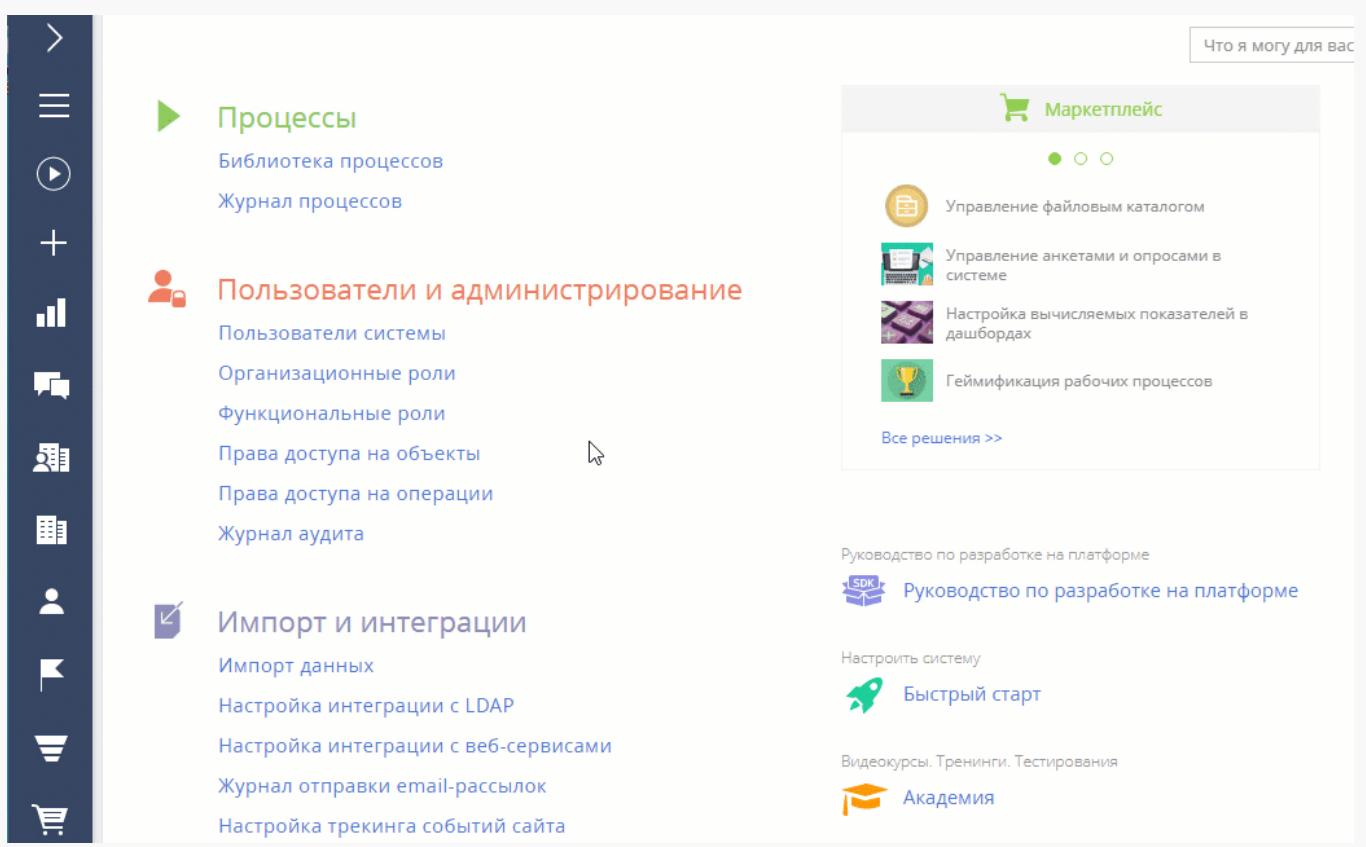
2. Нажмите кнопку [Добавить]. В открывшемся окне введите название роли.

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”.

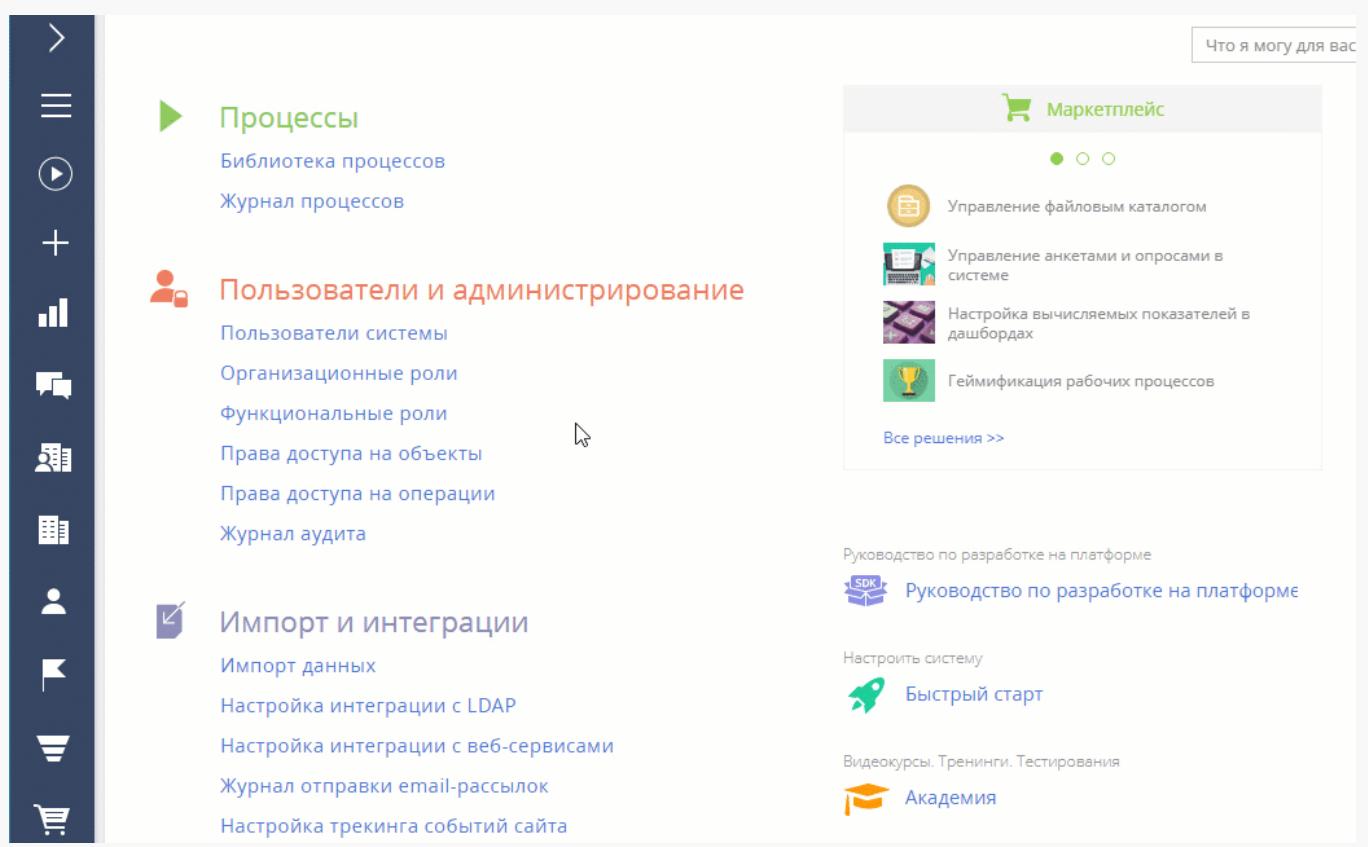
Для того чтобы связать функциональную роль с организационными ролями:

- Нажмите —> “Функциональные роли”.
- В списке функциональных ролей **выберите нужную функциональную роль**. Справа откроется страница выбранной роли.
- 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".

- 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:

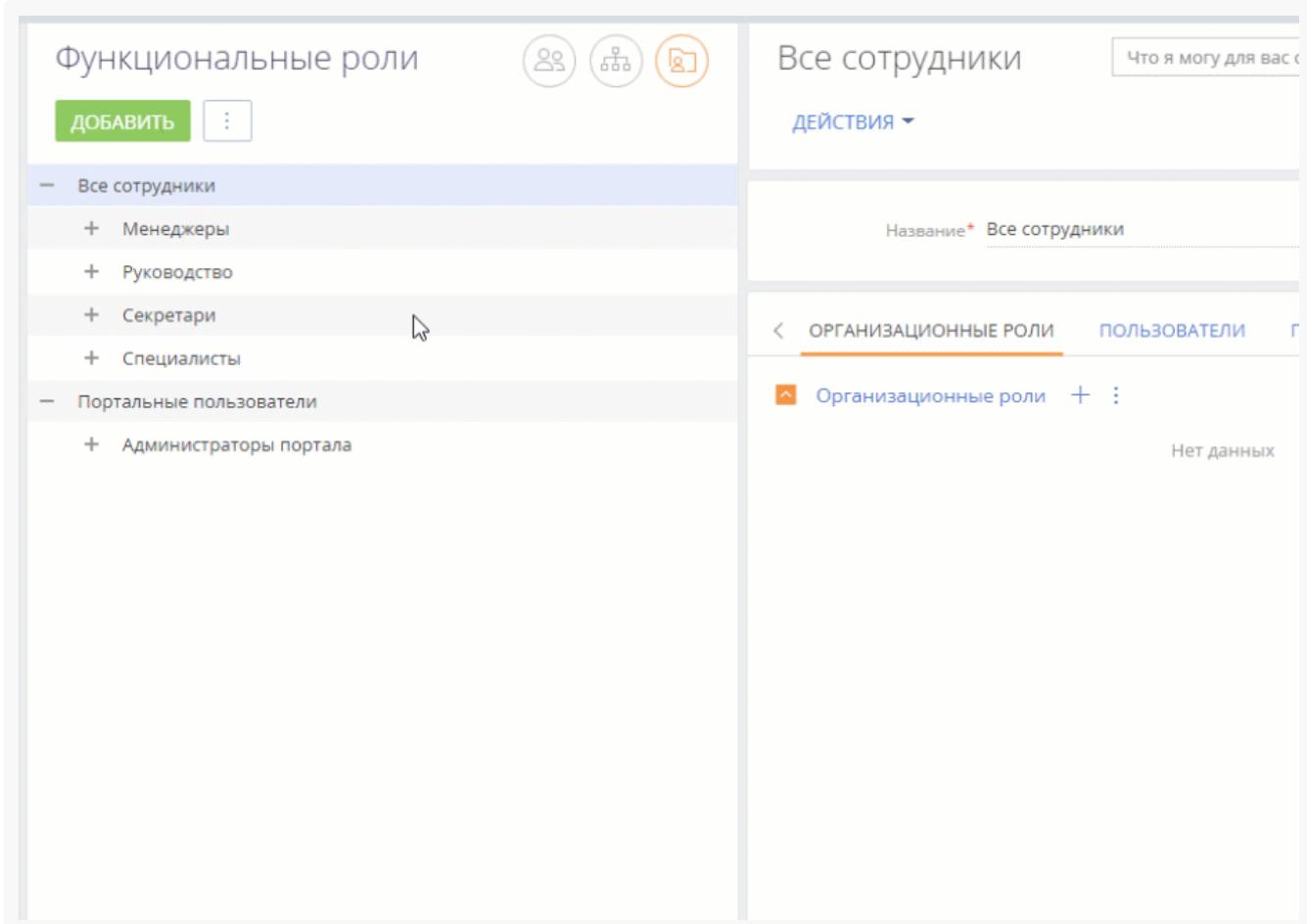
- Добавить существующих пользователей (выбрать из списка пользователей).
- Создать и добавить нового пользователя (нужно будет заполнить страницу нового пользователя).
- Импортировать пользователей LDAP. [Подробнее >>>](#)

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



	Организационные роли	Пользователи	Группы
	Организационные роли	 :	
Нет данных			

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 managing company information. At the top, there are tabs: 'ОСНОВНАЯ ИНФОРМАЦИЯ' (highlighted in orange), 'КОНТАКТЫ И СТРУКТУРА', 'ОБСЛУЖИВАНИЕ', and 'ХРОНОЛОГИЯ'. Below the tabs, the object name 'AlfaBusiness' is displayed. Under the 'Основная информация' tab, there are several sections: 'Альтернативные названия' (Alternative names), 'Код' (Code) - 34, 'Категоризация' (Categorization) with fields 'Количество сотрудников' (Number of employees) - 501-1000 and 'Форма собственности' (Type of ownership) - АО, and a red-bordered 'Годовой оборот' (Annual Turnover) field which is empty. Another section 'Средства связи' (Communication methods) lists 'Web' (www.alfabizness.com), 'Основной телефон' (Main phone) (+7 495 277 01 96), 'Факс' (+7 495 277 01 98), and 'Дополнительный телефон' (+7 495 384 02 18). Each communication method has a small green phone icon next to it.

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

ПРАВА ДОСТУПА

Использовать доступ по операциям i

Использовать доступ по записям i

Использовать доступ по колонкам i

Доступ к колонкам не ограничен

+ Добавить

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.

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

Колонка	Приоритет	Роль/Пользователь	Уровень прав
Годовой оборот	0	All employees	
+ Добавить	1	Менеджеры по продажам	
+ Добавить	2	Секретари	

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 ограничивает 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):

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

Рис. 5 — Пример настройки приоритета прав доступа по колонкам

Колонка	Приоритет	Роль/Пользователь	Уровень прав
Годовой оборот	0	Менеджеры по продажам	Б
	+ Добавить		
Секретари	1	Секретари	Б
	+ Добавить		
All employees	2	All employees	Б
	+ 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).

Рекомендуемые настройки

информационной безопасности

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 не определены точные требования.

Длина пароля. Рекомендуем использовать пароли, состоящие из 8 и более символов. Установить сложность пароля вы можете в следующих [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 сравнить 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 у следующих системных настроек снят признак в значениях по умолчанию:

- “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 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 скрипtingа (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-sr
```

Ответы на запросы для Creatio on-site

Ограничите количество и тип информации, доступной в ответах на запросы. Для этого измените файл [Web.config](#) 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 сессий 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.

Настроить интеграцию с Telegram

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Вы можете настроить интеграцию с Telegram, чтобы операторам контакт-центра была доступна возможность обрабатывать в Creatio сообщения, отправленные клиентами вашему чат-боту Telegram.

Для настройки канала Telegram в Creatio вам необходим предварительно созданный и настроенный чат-бот в Telegram. Подробнее о создании и настройке ботов читайте в [документации Telegram](#).

На заметку. Перед настройкой интеграции убедитесь, что в [системной настройке](#) “Адрес сайта” (код “SiteUrl”) адрес приложения Creatio, которое будет синхронизироваться с Telegram, указан в формате <https://yoursite.domain.com/0>.

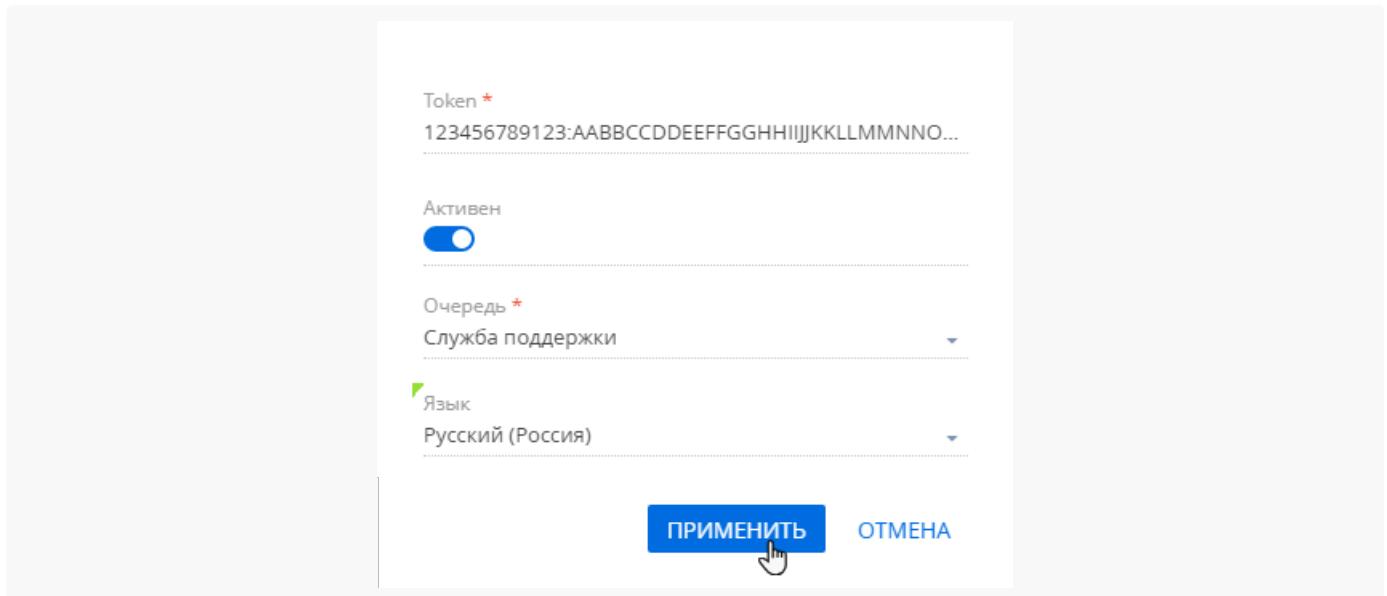
Вы также можете не указывать значение системной настройки, в этом случае оно заполнится автоматически при добавлении канала.

1. Перейдите в **дизайнер системы**, например, по кнопке .
2. Откройте раздел [*Настройка чатов*].
3. В области [*Каналы*] нажмите кнопку  . В появившемся меню выберите “Telegram”.
4. В открывшейся мини-карточке заполните **параметры канала**:
 - a. Укажите **токен**, сгенерированный на стороне Telegram для вашего чат-бота.
 - b. Установите индикатор в положение **“Активен”**, чтобы сообщения чата были доступны для обработки в коммуникационной панели.
 - c. Выберите **очередь чата**, в которой будут обрабатываться обращения, полученные по данному каналу.

На заметку. Для корректной работы канала телеграм-бот, с которым вы настраиваете интеграцию, не должен использоваться на других ресурсах. Если вы не уверены, что бот, который вы добавляете, не интегрирован с другими сайтами или приложениями, рекомендуем перед настройкой канала в Creatio перегенерировать токен бота.

- d. Укажите **язык**, на котором предполагаете получать сообщения по данному каналу. Это необходимо, чтобы операторы могли использовать шаблоны быстрых ответов на языке клиентов.
5. Нажмите [*Применить*].

Рис. 1 — Пример настройки канала Telegram



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 общий почтовый ящик

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Общий почтовый ящик позволяет организовать многопользовательскую работу с почтой: настроить доступ к просмотру писем для различных групп пользователей, дать возможность нескольким

пользователям или группам пользователей обрабатывать входящую почту и отправлять письма с одного адреса.

Например, общий почтовый ящик можно использовать:

- Для коммуникации между клиентами и службой поддержки, для регистрации обращений, отправки клиентам уведомлений и переписки по обращению.
- Для обработки запросов информации о продуктах компании. Так, можно создать общий ящик отдела продаж и предоставить к нему доступ сотрудникам рекламного отдела, которые смогут отправлять письма с новостями или специальными предложениями.

На заметку. Все входящие и исходящие письма общего почтового ящика в коммуникационной панели, хронологии и истории доступны для просмотра пользователю, который зарегистрировал в Creatio данный почтовый ящик, и тем, кому он дал доступ для работы с письмами.

Важно. Для настройки общего почтового ящика необходимо обладать правом на выполнение [системных операций](#) [Доступ к подключению общего почтового ящика] и [Настройка синхронизации с общими почтовыми ящиками].

Настройка общего почтового ящика аналогична настройке индивидуального почтового ящика, но требует выполнения дополнительных действий:

1. На странице настройки почтового ящика выберите опцию [Доступ для других пользователей].
2. Чтобы добавить сотрудников, которые смогут пользоваться общим почтовым ящиком, нажмите кнопку +. В появившемся поле нажмите и укажите пользователя системы или название роли, если доступ необходимо дать группе сотрудников. Нажмите кнопку [Сохранить]. Если вы хотите дать доступ к почтовому ящику нескольким пользователям или группам пользователей, то для каждой из них повторите данный шаг.
3. Настройте для добавленных пользователей права доступа к общему почтовому ящику: на доступ к письмам, отправку писем или настройку ящика. Для этого установите признак в нужной колонке ([Рис. 1](#)).

Рис. 1 — Пример настройки прав доступа к общему почтовому ящику

Доступ для других пользователей

Настройте возможность другим пользователям работать с загруженными письмами, отправлять письма с этого адреса, а также изменять настройки этой учетной записи

Какие права доступа добавить?

Пользователь / Роль	Доступ к письмам	Отправка писем	Настройка ящика
Отдел клиентского сервиса	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Для управления доступом к почте в системе предусмотрены следующие опции:

- a. “Доступ к письмам” — позволяет видеть письма, полученные на этот почтовый ящик, в разделах системы, например, на вкладке [Хронология]. При этом корреспонденция из общего почтового ящика не будет отображаться в коммуникационной панели пользователя, которому предоставлен доступ к письмам. Данная опция используется в тех случаях, когда с почтой из одного ящика работают несколько сотрудников. Например, для обращений в службу поддержки, зарегистрированных на основании писем.
 - b. “Отправка писем” — позволяет отправлять письма с данного почтового ящика. Он будет доступен в поле [От кого] при отправке писем и настройке бизнес-процессов, а также видеть входящие и исходящие письма в коммуникационной панели.
 - c. “Настройка ящика” — позволяет нескольким администраторам вносить изменения в настройки данного почтового ящика.
4. Сохраните изменения.

Настроить верификацию для провайдера SendGrid

ПРОДУКТЫ: MARKETING

Если отправка рассылок в Creatio осуществляется с помощью SendGrid, то вам необходимо верифицировать ваш email-адрес и корпоративный домен, чтобы провайдер мог отправлять электронные письма от вашего имени.

Если ваши получатели используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, они могут увидеть в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени.

На заметку. В строке отправителя может отобразиться такой текст: “Your Manager <info@creatio.com> via sendgrid.net”.

Процедура верификации домена для провайдера SendGrid состоит из следующих этапов:

1. Добавьте ваш корпоративный домен на страницу настройки email-рассылок. [Подробнее >>>](#)
2. Получите MX-, SPF- и DKIM-записи. [Подробнее >>>](#)
3. Укажите MX-, SPF-, и DKIM-записи в DNS-зоне вашего домена. [Подробнее >>>](#)

Добавить ваш корпоративный домен на страницу настройки email-рассылок

Пользователям SendGrid нужно добавить корпоративный домен в Creatio до начала отправки массовых рассылок. Для этого:

1. В разделе **Email** в меню **Действия** выберите **Настройки email-рассылок** ([Рис. 1](#)).

Рис. 1 — Переход на страницу настройки email-рассылок

Маркетинг

- Контакты
- Кампании
- Email**
- Лендинги и web-формы
- Мероприятия
- Лиды
- Контрагенты

Email

ДОБАВИТЬ ДЕЙСТВИЯ

Фильтры/группы

Серия вебинаров по эффективности маркетинга

Тема Серия вебинаров по эффективности маркетинга

Экспорт в Excel

Импорт данных

Настройки email-рассылок

Журнал отправки email-рассылок

Получатели 93
Категория Триггерное письмо

Серия вебинаров по эффективности маркетинга

Тема Главная встреча профессионалов в сфере CRM

Кампания Конференция "Дни CRM"

Программа конференции "Дни CRM"

Получатели 64
Категория Триггерное письмо

Получатели 111
Категория

2. На странице **Настройки email-рассылок** на вкладке **Домены отправителя** укажите домен вашего email-адреса, с которого будут отправляться рассылки, например “mycompany.com” ([Рис. 2](#)).

Рис. 2 — Вкладка [Домены отправителя]

Настройки email-рассылок

СОХРАНИТЬ ОТМЕНА

ОБЩИЕ НАСТРОЙКИ ДОМЕНЫ ОТПРАВИТЕЛЯ НАСТРОЙКА ПРОЦЕССОВ

Домены отправителя		Обновить
Домен	mycompany.com	DKIM верифицирован
		Нет

Получить ключи настройки для домена

MX-, SPF- и DKIM-записи генерируются автоматически в разделе **Email** после добавления домена на страницу настройки email-рассылок. Для получения этих записей в разделе **Email** в меню [Действия] выберите **Настройки email-рассылок**.

SPF- и DKIM-записи будут автоматически сгенерированы в поле **Инструкции по настройке DKIM/SPF** на вкладке **Домены отправителя** ([Рис. 1](#)).

Рис. 1— Ключи MX/DKIM/SPF для указанного домена

Настройки email-рассылок

ЗАКРЫТЬ

ОБЩИЕ НАСТРОЙКИ **ДОМЕНЫ ОТПРАВИТЕЛЯ** **НАСТРОЙКА ПРОЦЕССА РАЗБОРА ОТКЛИКОВ**

Домены отправителя + Обновить

Домен	Домен верифицирован
creatioes.com	Нет

Домен «creatioes.com»: Инструкции по настройке DKIM/SPF

Для отправки писем от вашего домена, необходимо чтобы системный администратор поменял DNS запись в хостинге вашего домена. Используйте следующие инструкции для настройки. Примеры настроек для наиболее популярных сервисов хостинга можно найти в [Академии](#).

Инструкции отличаются для разных доменов. Для получения инструкции по домену необходимо добавить и выбрать его в списке.

Выберите домен в списке на этой странице.

MX запись. В настройках DNS записи домена создайте первую запись MX. Скопируйте и вставьте настройки из поля ниже:

```
em867.creatioes.com mx mx.sendgrid.net.
```

*Добавление MX записи обязательно только для провайдера Sendgrid. Для других провайдеров этот блок остается не заполненным.

SPF запись. Добавьте в DNS вашего хостинга первую запись для ключа SPF. Скопируйте и вставьте туда следующий текст:

```
em867.creatioes.com txt v=spf1 include:sendgrid.net ~all
```

*Настройках DNS должна быть только 1 SPF запись. Если SPF запись уже существует, добавьте домен из параметра "include" выше в существующую запись. Убедитесь, что он добавлен до любых IP-адресов.

DKIM запись. Создайте в DNS вторую TXT запись для ключа DKIM. Скопируйте и вставьте туда следующий текст:

```
m1._domainkey.creatioes.com txt k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAAQNAQCBiQRBqC6e4aX0tRN6raL75IDvNFQPf2aU+wcu9BjluWj1XNMePXQWnUg5gNH+CELVtcrgrQ2i2Ic5Q03cB3g+GWEHEeB1SYvcXdiPfftm/Ta gaIn73p/6CGK1HzyMbtOrfT0lFREyL+0lpWTbj1V/vYyE9Ujf3NXEGq7apoN9pd+cxyKOI DAQAB
```

*Настройках DNS может быть неограниченное количество записей DKIM

Важно. MX-, SPF- и DKIM-записи провайдера SendGrid отличаются для разных доменов.

Выполнить настройки в DNS-зоне вашего домена

Чтобы верифицировать почтовый домен при использовании провайдера рассылок SendGrid, необходимо добавить записи MX, SPF и DKIM в DNS-зону настроек почтового домена, иначе не гарантируется высокий уровень репутации домена и доставляемости писем.

На заметку. Рекомендуем также ознакомиться с примерами в статье [«Рекомендации по настройке для популярных DNS-провайдеров»](#).

Указать MX-запись в DNS-зоне вашего домена

MX-запись — это основная запись в доменной зоне, указывающая на имена почтовых хостов домена. Почтовый сервер выполняет обязательную проверку наличия MX-записей в DNS-зоне домена и их соответствия IP-адресу отправителя. В случае отсутствия или несоответствия данных, удаленный сервер с высокой вероятностью откажет в отправке и получении электронной почты.

Синтаксис MX-записей отличается от SPF- и DKIM-записей наличием приоритетов.

Приоритет указывается в виде целого числа от нуля включительно и указывает для данного домена порядок доступности почтовых серверов, если их используется несколько. Чем меньше число, тем выше приоритет. то есть, наивысший приоритет — 0. Допускается наличие в системе нескольких

MX-записей с равными приоритетами.

MX-запись будет выглядеть следующим образом:

Имя	Приоритет	Тип	Значение
subdomain.yourdomain.com	0	mx	mx.sendgrid.net.

Имя поддомена (subdomain) является уникальным и формируется провайдером.

Указать SPF-запись в DNS-зоне вашего домена

Скопируйте SPF-запись из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
subdomain.yourdomain.com	TXT	v=spf1 a mx include:_spf.sendgrid.com ~all

Имя поддомена (subdomain) является уникальным и формируется провайдером. Поэтому для каждого из поддоменов необходимо добавлять отдельную SPF-запись.

Указать DKIM-запись в DNS-зоне вашего домена

После настройки записи SPF необходимо добавить записи DKIM. Для провайдера SendGrid эта запись выглядит следующим образом:

Название	Тип	Значение
m1._domainkey	TXT	k=rsa; t=s; p=XXXXXXXXXXXXXX

В приведенной записи XXXXXXXXXXXX — это **индивидуальный ключ** для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [**Домены отправителя**].

В некоторых настройках DNS в поле “Host/Name” может потребоваться ввести “m1._domainkey.yourdomain.com”, заменив значение поддоменом, который был сформирован провайдером.

На заметку. Подробная информация о настройке записей MX, SPF и DKIM доступна в [инструкции](#) на сайте провайдера SendGrid.

Особенности лицензирования Marketing

Creatio

ПРОДУКТЫ: MARKETING

Для работы с **Marketing Creatio** и **CRM-линейкой Creatio** помимо основных лицензий используются:

- Лицензии на **маркетинговые кампании** (“marketing creatio”). Дают доступ к функциональности всех разделов продукта Marketing Creatio. Количество лицензий должно соответствовать количеству пользователей системы.
- Серверные лицензии на **активных контактов** (“marketing creatio 1000 active contacts”). Используются для создания записей в разделах [Email], [Кампании] и [Мероприятия]. Количество лицензий должно соответствовать или превышать размер базы активных контактов, по которым выполняется рассылка.

На заметку. В названии лицензий содержатся приставки, обозначающие способ развертывания приложения — onsite или cloud. Эти данные стоит учитывать, чтобы загруженная лицензия соответствовала конфигурации сборки.

Активные контакты — это контакты, с которыми в течение года была выполнена хотя бы одна из перечисленных ниже коммуникаций:

- контакт входил в аудиторию рассылки и по результатам отправки был получен отклик;
- контакт входил в аудиторию мероприятия;
- контакт входил в аудиторию кампании;
- контакт является участником программы лояльности и совершил минимум одну покупку в течение года (при использовании продуктов Marketplace по автоматизации программ лояльности).

Срок действия лицензий ограничен **периодом лицензирования**. Период лицензирования равен 360 дням и начинается с даты отсчета срока действия лицензии, а заканчивается датой, которая указана в менеджере лицензий как “Дата завершения”.

За период лицензирования контакт может стать активным только один раз. Если контакт был активным в предыдущем периоде лицензирования, но с ним не было маркетинговых коммуникаций в течение текущего периода, то контакт не считается активным в текущем периоде.

Для эффективной работы в системе **необходимо контролировать, чтобы количество активных контактов (используемых лицензий) не превышало количество оплаченных лицензий**.

Если используемых лицензий больше, чем оплаченных, то могут возникать ограничения и блокировки в работе системы:

- при сохранении или отправке рассылок;
- при редактировании шаблона рассылки в дизайнере контента;
- при переходе кампании на шаг [Email-рассылка];
- также может быть ограничена доступность некоторых операций в разделах [Мероприятия] и [Кампании].

Creatio отправляет уведомления пользователям в том случае, если число доступных лицензий на активные контакты становится меньше порогового процента от общего количества оплаченных лицензий (по умолчанию — 10%). Уведомления отправляются только системным пользователям, контакты которых — ответственные или создатели рассылок, кампаний, мероприятий за последние 30 дней. Таким пользователям рекомендуется **регулярно проверять вкладку [Центр уведомлений]** на коммуникационной панели.

На заметку. Вы можете изменить пороговый процент в системной настройке “Активные контакты - условие предупреждения, %” (код “ActiveContactsWarningThreshold”).

Если количество активных контактов превышает количество купленных лицензий, то необходимо приобрести дополнительные лицензии. Для этого обратитесь в службу технической поддержки Terrasoft.

Чтобы **предупредить возможные ограничения и блокировки из-за недостаточного количества доступных лицензий**, учитывайте следующие факторы:

- При добавлении группы контактов в аудиторию рассылки обязательно проверяйте условия фильтрации, настроенные для этой группы. Настройки фильтров могли быть изменены, вследствие чего в группу могут попасть те пользователи, которые не являются целевой аудиторией рассылки или кампании. Подсчет количества активных контактов и доступных лицензий выполняется по расписанию (один раз в четыре часа), а также после завершения отправки рассылки. Поэтому в момент формирования аудитории рассылки информация о несоответствии количества лицензий количеству доступных контактов может быть недоступна.
- Если на момент запуска рассылки или кампании количество активных контактов не превышает количество доступных лицензий, то система отправит столько email-сообщений, сколько адресатов вы добавите в аудиторию. Например, если у вас есть 10000 лицензий, 9999 активных контактов, а в аудиторию рассылки были добавлены 50000 адресатов, то письма будут отправлены всем контактам из аудитории рассылки. После отправки рассылки будет выполнен пересчет количества активных контактов и доступных лицензий, зафиксировано недостаточное количество лицензий и в результате может произойти ограничение работы функциональности Creatio.
- При отправке email-рассылок учитываются следующие настройки, которые позволяют управлять отправкой писем и ограничивают отправку для неактивных контактов:
 - Запрет на использование электронного адреса контакта (признак [Не использовать Email] на детали [Средства связи] контакта).
 - Возможность подписки на определенные типы рассылок или отписки от них.

Определить количество используемых лицензий на активных контактов

Количество используемых лицензий (активных контактов) можно узнать в разделе [Итоги] на вкладке [Лицензии]. Эти показатели могут незначительно отличаться от фактических показателей на текущий момент, т. к. рассчитываются не в режиме реального времени, а раз в день.

Превышение количества активных контактов и недостаточное количество доступных лицензий могут быть зафиксированы только в ходе планового пересчета или после отправки рассылки. Поэтому при

подготовке email-коммуникаций с клиентами очень важно контролировать наличие достаточного количества лицензий на активных контактов.

Чтобы просмотреть список активных контактов, настройте фильтр в разделе [Контакты], как на Рис. 1.

Важно. Обратите внимание, что этот фильтр не учитывает участников программы лояльности.

Рис. 1 — Фильтр для определения количества активных контактов

The screenshot shows a complex filter structure. It starts with a main condition: "Отклик в Email (по колонке Контакт) существует" (Email response exists). This is followed by an "И" (And) connector, then another condition: "Отклик ≠ Не отправлено (email дублирован); Не отправлено (email не указан); Не отправлено (домен отправителя не подтвержден); Не отправлено (имя отправителя не валидно); Не отправлено (неактуальный email); Не отправлено (некорректный email); Не отправлено (отписан от всех email); Не отправлено (отписан по типу рассылки); Не отправлено (шаблон отсутствует); Готов к отправке" (Email response ≠ Not sent (email duplicated); Not sent (email not specified); Not sent (sender domain not confirmed); Not sent (sender name invalid); Not sent (invalid email); Not sent (incorrect email); Not sent (unsubscribed from all emails); Not sent (unsubscribed by type of mailing); Ready to send). Below this is a date range condition: "Дата создания ≥ 05.06.2021".

Below the main condition is an "ИЛИ" (Or) connector, followed by another condition: "Участник кампании (по колонке Контакт) существует". This is followed by an "И" (And) connector, then another condition: "Дата создания ≥ 05.06.2021".

Below this is another "ИЛИ" (Or) connector, followed by a condition: "Участник мероприятия (по колонке Контакт) существует". This is followed by an "И" (And) connector, then another condition: "Дата создания ≥ 05.06.2021".

At the bottom of the filter interface, there is a "+ Добавить условие" (Add condition) button.

В этом фильтре “Дата создания” — это дата, с которой начинается отсчет срока действия лицензий. Для расчета нужной даты выполните следующие действия:

Рис. 2 — Просмотр срока действия лицензии

The screenshot shows the "Менеджер лицензий" (License Manager) interface. At the top, there are buttons for "ЗАКРЫТЬ" (Close) and "ЗАГРУЗИТЬ ЛИЦЕНЗИИ" (Load License). A search bar contains the text "marketing".

Название	Тип	Дата начала	Дата завершения	Статус	Всего
marketing creatio 1000 active contacts	Серверная	01.02.2016	31.05.2022	Активна	1 000

The "Дата завершения" (End Date) cell for the single contact entry is highlighted with a red border.

- Перейдите в дизайнер системы по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “**Менеджер лицензий**”.
- На открывшейся странице с помощью формы поиска найдите нужную лицензию и посмотрите дату ее завершения (Рис. 2).
- Отнимите от этой даты 360 дней. Для правильного расчета даты рекомендуется использовать онлайн-калькулятор.

В результате вы получите дату отсчета, которую необходимо ввести в колонку [*Дата создания*] при построении фильтра для отбора активных контактов. Например, если лицензия действует до 31.05.2022, как на Рис. 2, то дата отсчета для построения фильтра — 5.06.2021.

Очистить логи журнала изменений

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

При работе с Creatio вы можете очищать историю журнала изменений, чтобы избежать хранения устаревших записей в системе. Например, вы можете очистить записи логов для определенного контракта, который был создан в указанный период времени.

На заметку. Мы рекомендуем регулярно очищать записи логов, чтобы в разделе [*Журнал изменений*] содержалась только актуальная на данный момент информация.

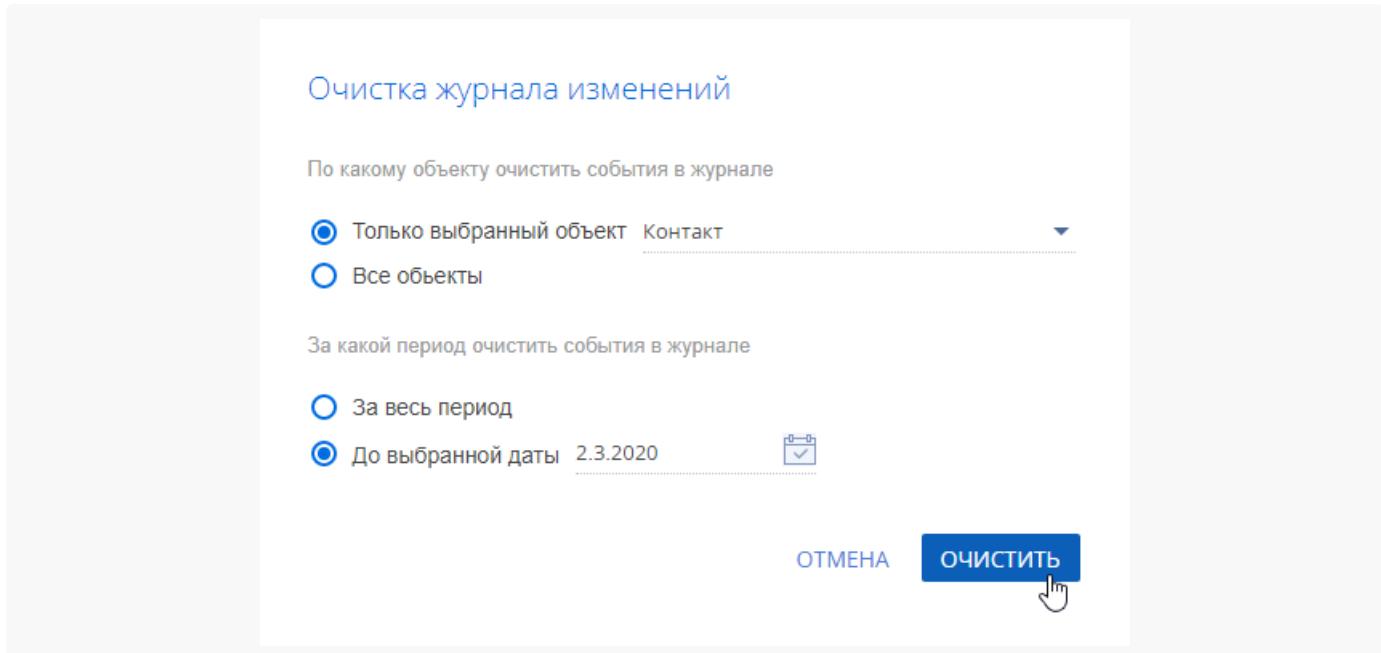
- Перейдите в дизайнер системы, например, по кнопке .
- В блоке “Пользователи и администрирование” перейдите по ссылке “*Журнал изменений*”.
- Нажмите [*Действия*] —> [*Очистить журнал изменений*].

На заметку. Для выполнения этого действия у вас должны быть настроены права доступа на выполнение системной операции “Доступ к очистке журнала изменений” (код “CanClearChangeLog”).

Подробнее: [Права доступа на системные операции](#).

- Выберите, за какой период и по каким объектам нужно удалить логи. Нажмите кнопку [*Очистить*] (Рис. 1), чтобы удалить данные записи.

Рис. 1 — Удаление записей журнала изменений



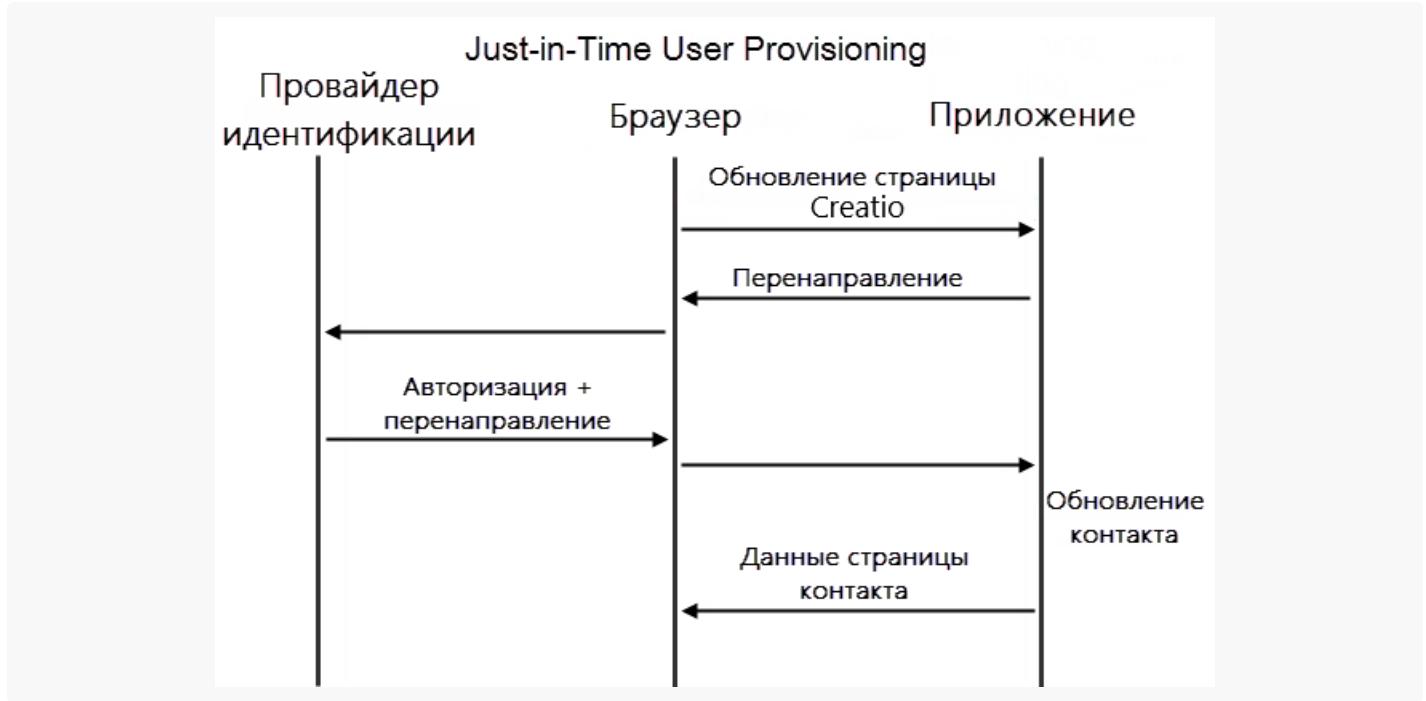
В результате выполнения действия выбранные записи будут удалены.

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 “[Настройте Single Sign-On через ADFS](#)” и “[Настройте 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

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.

- 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

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	

- 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		
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	

- 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”.
- При необходимости, для провайдера идентификации OneLogin можно добавить пользовательские параметры и поместить в них макросы. Подробнее о работе с макросами читайте в [документации OneLogin](#).

Управление системными настройками

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Раздел [Системные настройки] используется для дополнительной настройки разделов системы. Например, здесь вы можете указать цвет фона панели разделов, задать цвет для просроченных активностей, выбрать базовую валюту для расчетов финансовых показателей, задать параметры отправки email-сообщений и т.д.

При помощи системных настроек также можно задать значение по умолчанию, которое автоматически будет заполняться для поля при создании записи, например, состояние для активности.

Важно. Для управления системными настройками требуется доступ к системной операции “Доступ к разделу “Системные настройки” (CanManageSysSettings). Кроме того, если объект

справочника управляется операциями, записями или колонками, пользователю необходимы соответствующие права, чтобы получить возможность управлять записями этого объекта.

Перейти к системным настройкам

Чтобы перейти к **системным настройкам**, откройте раздел [Системные настройки] из рабочего места [Студия] или из дизайнера системы.

Рис. 1— Переход к разделу [Системные настройки] из рабочего места [Студия]

Контакт	Должность	Рабочий телефон
Макаренко Андрей Контрагент ИТ Плюс	Email a.makarenko@gmail.com	Мобильный телефон +7 495 578 42 11
Макаров Дмитрий Контрагент Our company	Должность Руководитель отдела Email dmitry-makarov@yandex.ru	Рабочий телефон +7 915 277 36 81 Мобильный телефон +7 915 123-65-65
Максимов Игорь Контрагент Альфабизнес	Должность Директор по продажам Email maximov.igor@yandex.ru	Рабочий телефон +7 499 654 42 45 Мобильный телефон +7 915 500-00-22
Маянов Дмитрий Контрагент	Должность Специалист Email	Рабочий телефон +7 925 281 56 95 Мобильный телефон

Рис. 2— Переход к разделу [Системные настройки] из дизайнера системы

Имя	Должность	Рабочий телефон
Сергеевич	Контрагент Персонал	Email: alexander.z@gmail.com Мобильный телефон: +7 905 190 38 77
Золотов Ярослав Викторович	Должность Руководитель отдела	Рабочий телефон: +7 495 046 5218
	Email: yaroslav.zolotov@gmail.com	
Золотов Ярослав Викторович	Должность Руководитель отдела	Рабочий телефон: +7 495 250 74 15
	Контрагент Камелия	Мобильный телефон: +7 915 046 52 18
Исхаков Александр		Рабочий телефон: 5209
	Контрагент Our company	Мобильный телефон: +7 915 44 82 991

Изменить системные настройки

Для изменения значения системной настройки:

- Перейдите в раздел [Системные настройки]. Найдите нужную настройку в реестре раздела и кликните по ее названию.

В разделе [Системные настройки] используются стандартные [фильтры](#) и [группы](#).

- Заполните страницу системной настройки:

- Измените значение системной настройки, заполнив поле [Значение по умолчанию].
- Установленный признак [Кешируется] обозначает, что значение системной настройки необходимо считывать однократно после входа в систему, так как эти значения меняются достаточно редко.

Например, кешируемыми настройками являются логотип для главного меню, цвет просроченных активностей или базовая валюта. Примером некешируемой системной настройки может быть номер статьи базы знаний, так как значение настройки должно обновляться каждый раз при создании новой статьи, или дата последнего поиска дублей.

Чтобы значение системной настройки было индивидуальным для каждого пользователя, установите признак в поле [Сохранять значение для текущего пользователя]. В результате каждый раз при смене значения данного параметра оно будет изменено только для этого пользователя.

- Нажмите кнопку [Сохранить].

Предоставить доступ к отдельным системным

настройкам

Вы можете разрешить или запретить доступ к отдельным системным настройкам вне раздела [Системные настройки] пользователям, у которых нет прав на выполнение системной операции “Доступ к разделу “Системные настройки” (CanManageSysSettings). Такие пользователи могут получить доступ к значениям системных настроек другими способами, например, через консоль веб-браузера.

Важно. Не используйте стандартные права доступа на объекты SysSettings и SysSettingsValue для управления доступом к системным настройкам, поскольку это приведет к прекращению работы Creatio.

Чтобы назначить права доступа, найдите нужную системную настройку в реестре раздела и кликните по ее названию. Заполните блоки [Доступ внутренних пользователей на чтение], [Доступ внутренних пользователей на изменение] и [Доступ пользователей портала].

Доступ внутренних пользователей на чтение:

- [Разрешить всем] — право на просмотр системной настройки предоставляется всем пользователям системы.
- [Запретить всем] — право на просмотр системной настройки ограничено для всех пользователей системы.
- [Разрешить по операции] — право на просмотр системной настройки предоставляется только пользователям, имеющим разрешение на выполнение определенной системной операции, название которой необходимо выбрать в открывшемся поле. Вы можете добавить новую системную операцию по нажатию кнопки [Добавить] в открывшемся окне.

Доступ внутренних пользователей на изменение:

- [Разрешить всем] — право на редактирование системной настройки предоставляется всем пользователям системы. Доступ на изменение системной настройки автоматически предоставляет доступ и на чтение.
- [Запретить всем] — право на редактирование системной настройки ограничено для всех пользователей системы.
- [Разрешить по операции] — право на редактирование системной настройки предоставляется только пользователям, имеющим разрешение на выполнение определенной системной операции, название которой необходимо выбрать в открывшемся поле. Вы можете добавить новую системную операцию по нажатию кнопки [Добавить] в открывшемся окне. Доступ на изменение системной настройки автоматически предоставляет доступ и на чтение.

Доступ пользователей портала: [Разрешить чтение пользователям портала] — право на просмотр системной настройки предоставляется всем пользователям портала.

Синхронизировать расписание Creatio с календарями Microsoft Exchange и

Microsoft 365

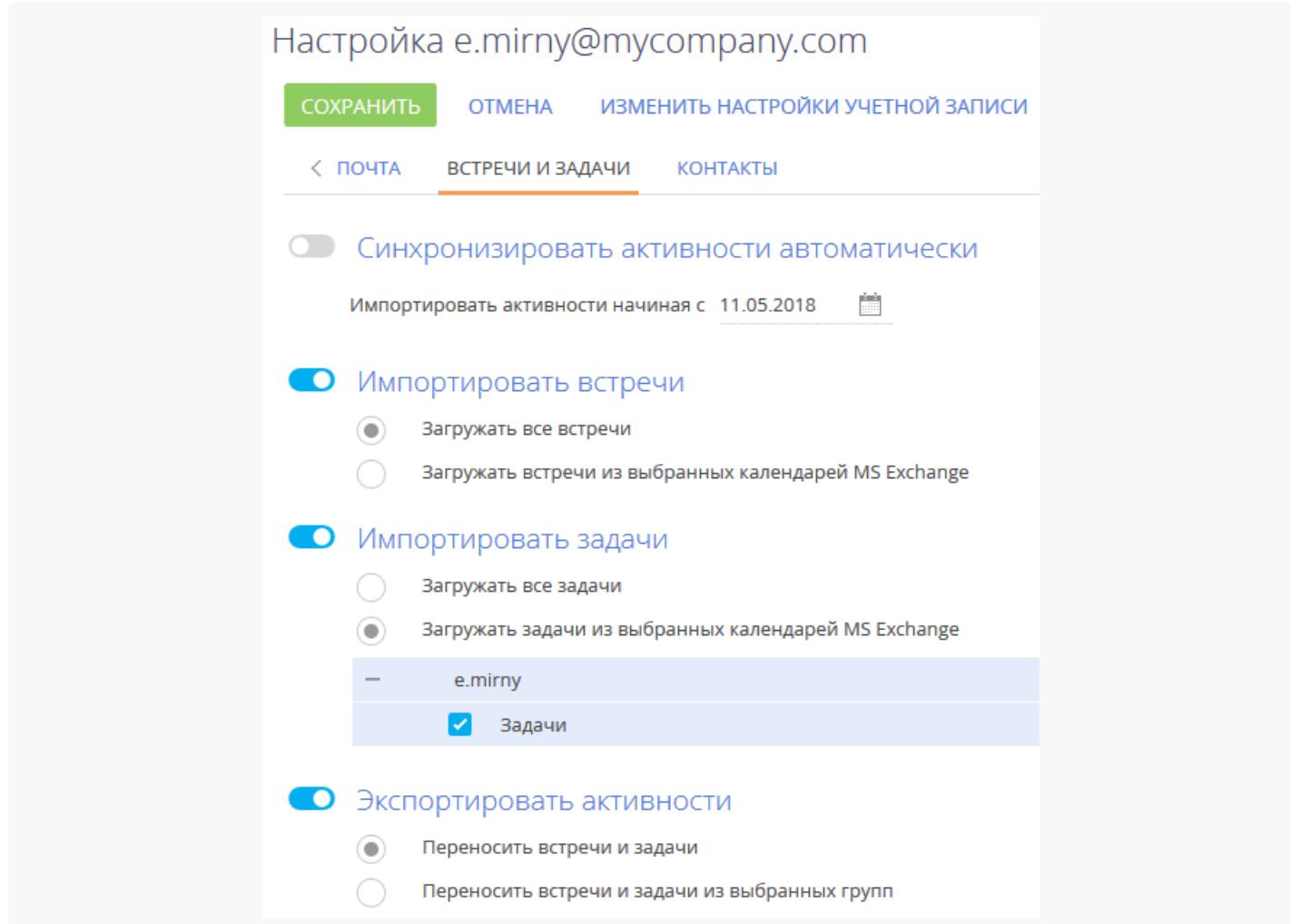
ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Настройка синхронизации активностей Creatio с задачами и встречами Microsoft Exchange или Microsoft 365 выполняется на странице настройки учетной записи почты ([Рис. 1](#)). На страницу можно перейти несколькими способами:

- Из коммуникационной панели, нажав  —> [Редактировать настройки].
- Из раздела [Активности], выбрав [Действия] —> [Синхронизировать активности] —> [Настроить...].

Команда содержит в названии имя учетной записи, например [*Настроить example@mail.com*].

Рис. 1 — Пример настройки синхронизации активностей Creatio с календарем Microsoft Exchange



Настройте импорт активностей в Creatio

Чтобы настроить импорт **встреч** Microsoft Exchange или Microsoft 365 в Creatio:

- На вкладке [Встречи и задачи] установите признак [Импортировать встречи].
- Выберите опцию [Загружать все встречи], чтобы импортировать все записи из календарей Microsoft Exchange или Microsoft 365.

Если вы хотите импортировать записи из выбранных календарей, то выберите опцию [Загружать встречи из выбранных календарей MS Exchange]. Раскройте перечень календарей и установите признаки напротив необходимых календарей.

- Аналогично настройте параметры импорта задач Microsoft Exchange или Microsoft 365: установите признак [Импортировать задачи] и, при необходимости, выберите папки, задачи которых должны быть импортированы.
- Нажмите кнопку [Сохранить] страницы настройки синхронизации с почтовым ящиком.

В результате импорта в Creatio будут добавлены задачи из календаря. При этом импортируются только задачи, ответственный которых является текущим пользователем Creatio. Настройка импорта задач выполняется аналогично настройке импорта встреч.

Настроить экспорт активностей из Creatio

Чтобы настроить экспорт активностей из Creatio в Microsoft Exchange или Microsoft 365:

- На вкладке [Встречи и задачи] установите признак [Экспортировать активности].
 - Выберите опцию [Переносить встречи и задачи], чтобы экспортировать все активности, к которым у вас есть доступ.
- Если вы хотите экспортировать только активности из указанных групп, то выберите опцию [Переносить встречи и задачи из выбранных групп]. Список групп соответствует группам, настроенным в разделе [Активности].
- Нажмите кнопку [Сохранить] страницы настройки синхронизации с почтовым ящиком.

В результате при экспорте задач с признаком [Отображать в расписании] в Microsoft Exchange или Microsoft 365 будут созданы активности с типом “Встреча”. При экспорте задач без признака [Отображать в расписании] в Microsoft Exchange или Microsoft 365 будут созданы активности с типом “Задача”.

Синхронизация активностей с Microsoft Exchange и Microsoft 365

Синхронизация ваших активностей между сервером Exchange и Creatio может выполняться автоматически. Чтобы включить автоматическую синхронизацию, на странице настройки синхронизации с почтовым ящиком установите признак [Синхронизировать активности автоматически] и в поле [Импортировать активности начиная с] выберите из календаря дату. Чтобы выполнить синхронизацию немедленно, перейдите в раздел [Активности], нажмите кнопку [Действия] —> [Синхронизировать активности] —> [Запустить синхронизацию].

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

Путь к странице: Пользователи и администрирование > Организационные роли

Маркетплейс

- abc Выделение набора полей в карточке по заданным правам
- INFLU Сервис персонализированного маркетинга
- Webtel Экспорт данных в электронные таблицы Excel Коннектор к телефонии и чатботов

[Все решения >>](#)

Руководство по разработке на платформе

[SDK Руководство по разработке на платформе](#)

Настройте систему

[Быстрый старт](#)

Видеокурсы. Тренинги. Тестирования

[Академия](#)

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

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-sladov@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	viktoria_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 Павловна	Камелия	Специалист	UsilovaAnastasiaPavelovna@gmail.com
Умелов Михаил Петрович	Аксиома	Специалист	umelov@gmail.com
Турова Лилия Тимофеевна	Our company	Специалист	TurovaLilyaTimofeevna@gmail.com
Трошин Виталий	ПК - Стайл	Разработчик	troshinv@pcstyle.com
Трошинский Владислав Викторович	Бальвия-фарм	Директор по продажам	TroshchinskiiVladislavVictorovich@gmail.com
Трофимова Ольга	Our company	Специалист	TrofimovaOlga@gmail.com
Тополь Анастасия Петровна	Софт-Плюс	Специалист	TopolAnastasiaPetrovna@bigmir.net
Тюлепова Александра Романовна	Атриус	Специалист	TiulepovaAlexandraRomanovna@yahoo.com

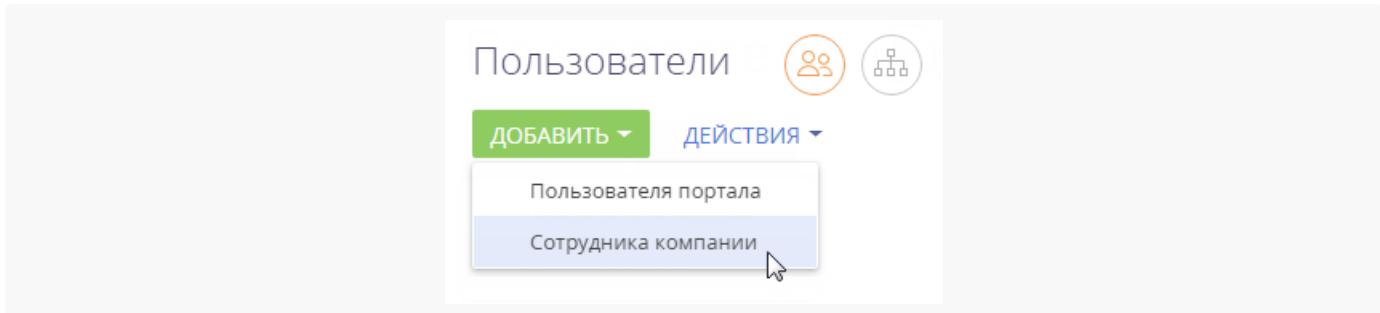
В результате в системе будет создан новый контакт, для которого можно создать пользователя.

На заметку. Вы также можете пропустить этот шаг и создать контакт позже, непосредственно при добавлении нового пользователя. Заполнив 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

- Нажмите —> “Пользователи системы”.
- 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:

- [Контакт] — выберите пользователя из раздела [Контакты].
- [Тип] — система заполнит поле автоматически после выбора типа пользователя в предыдущем шаге. Возможные значения поля — “Сотрудник компании” или “Пользователь портала”.
- [Активен] — признак будет автоматически отмечен для активных пользователей. Чтобы деактивировать пользователя, снимите данный признак.
- [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: [Мультиязычие](#).

- [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.
- [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:

- [Имя пользователя] — укажите логин пользователя, под которым он будет входить в систему. Поле является обязательным для заполнения.
- [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.
- [Пароль], [Подтверждение пароля] — укажите пароль пользователя, с помощью которого он будет входить в систему. Поля являются обязательными для заполнения.
- Дата окончания действия пароля — нередактируемое 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.

Удалить аккаунт Google из Creatio

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для удаления учетной записи Google из приложения выполните следующее:

1. Перейдите на страницу профиля пользователя. Нажмите кнопку [Профиль] на главной странице приложения.
2. Нажмите кнопку [Учетные записи во внешних ресурсах].
3. Выделите учетную запись Google, нажмите кнопку [Действия] и выберите [Удалить]. Нажмите кнопку [Да].

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

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

Использовать доступ по операциям ⓘ

Использовать доступ по записям ⓘ

Раздача прав в зависимости от автора записи ⓘ

Отсутствуют правила раздачи прав в зависимости от автора

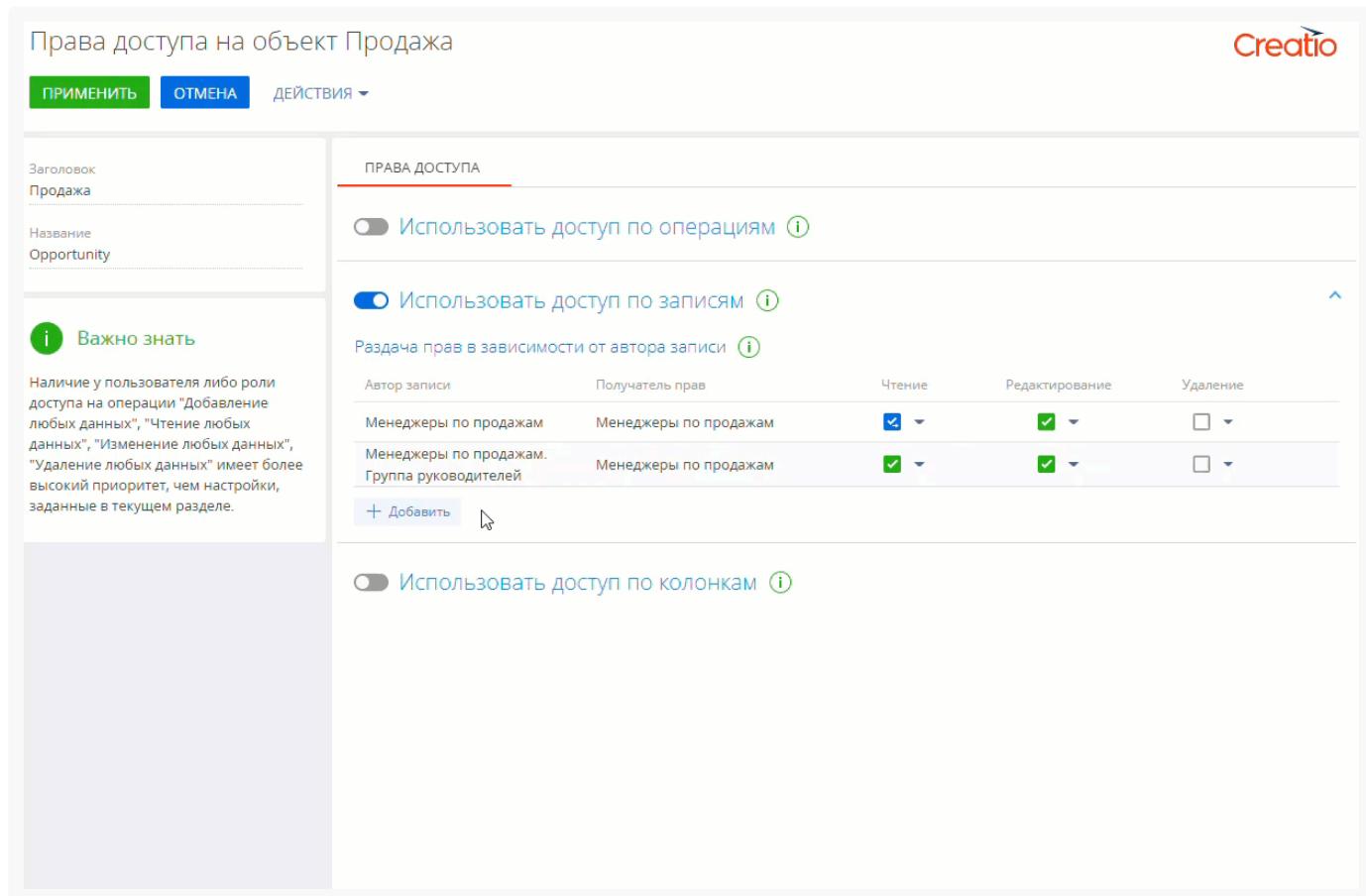
+ Добавить

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



- 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

Автор записи	Получатель прав	Чтение	Редактирование	Удаление
Менеджеры по продажам	Менеджеры по продажам	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Менеджеры по продажам. Группа руководителей	Группа руководителей	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 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”

- делегированием” в колонке [Чтение] и признак “Разрешено” в колонке [Редактирование].
- b. 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].
 - c. 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.

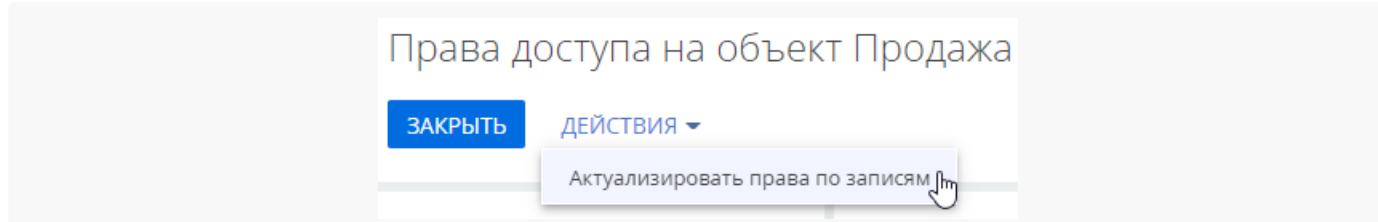
6. Чтобы сохранить настроенные права доступа, нажмите кнопку [Применить].

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

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.

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

Рис. 1 — Пример настройки прав на экспорт реестра

Права доступа на объект Счет

ПРАВА ДОСТУПА **РАСШИРЕННЫЕ ДЕЙСТВИЯ**

Дополнительные разрешения ⓘ

Роль/Пользователь	Операция ^
Руководители финансового отдела	Export

+ Добавить

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

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

Предоставить удаленный доступ службе поддержки Creatio

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Пользователи развернутых в облаке приложений могут предоставлять сотрудникам службы технической поддержки Creatio безопасный и контролируемый доступ к своим сайтам. При этом нет необходимости сообщать службе поддержки свои логин и пароль для доступа к сайту, что обеспечит безопасность персональных и коммерческих данных клиента.

На заметку. Для предоставления безопасного доступа в системе должны быть заполнены системные настройки: “Идентификатор приложения для предоставления доступа (по умолчанию)” (DefaultExternalAccessClientId), “Секретный ключ для Identity сервера” (IdentityServerClientSecret), “Адрес Identity сервера”(IdentityServerUrl), “Идентификатор приложения для Identity сервера” (IdentityServerClientId). Указанные настройки заполняются автоматически.

- Чтобы скрыть данные разделов системы от сотрудников службы поддержки, используется **режим изоляции данных**.
- Чтобы ограничить возможность менять настройки конфигурации для сотрудников службы поддержки используется **режим ограничения доступа на конфигурирование системы**. При этом настройки конфигурации, необходимые для решения обращения клиента, доступны для просмотра.

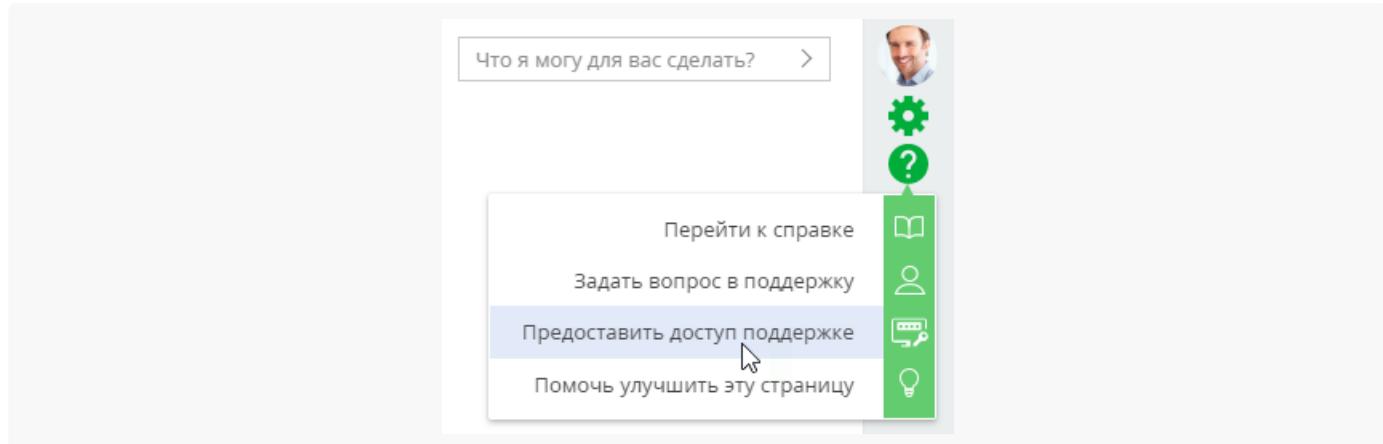
Настройка безопасного доступа выполняется администратором приложения (пользователем с ролью “System administrators”). Сотрудники службы поддержки могут подключаться под ученою записью администратора либо любого другого пользователя приложения. После того, как подключение состоялось, всю необходимую информацию по сеансу доступа можно получить в логах — когда состоялось подключение, а также какие данные были созданы при подключении.

Настроить безопасный доступ

На заметку. Для настройки доступа службы поддержки у вас должно быть право на чтение и добавление записей в объекте “Доступ внешних приложений”. У пользователей с ролью “System administrators” это право есть по умолчанию. Больше информации о правах на выполнение операций в объекте читайте в статье [“Настроить доступ по операциям”](#).

1. В правом верхнем углу приложения кликните  —> “Предоставить доступ поддержке” ([Рис. 1](#))

Рис. 1 — Переход к настройке доступа из справочного меню



2. Заполните поля открывшейся мини-карточки ([Рис. 2](#)):

Рис. 2 — Пример заполнения параметров доступа к клиентскому сайту

The dialog box title is 'Доступ внешних приложений'. The text inside says: 'Вы предоставляете службе поддержки Террасофт доступ к вашему приложению. Это поможет ускорить решение обращений и выполнение технических работ. Укажите параметры предоставления доступа.' with a link 'Подробнее...'. The form fields include: 'Причина предоставления доступа*' (filled with 'Рассмотрение обращения SR00000068'); 'Дата закрытия доступа*' (filled with '23.12.2019'); 'Предоставил' (filled with 'Авдorов Сергей'); checkboxes for 'Запретить доступ к данным' (checked) and 'Запретить конфигурирование' (checked); and buttons 'СОХРАНИТЬ' and 'ОТМЕНА'.

- a. В поле [**Причина предоставления доступа**] укажите, какая проблема привела к необходимости доступа, номер обращения или перечень работ, которые должен провести сотрудник службы поддержки.

- b. В поле [**Дата закрытия доступа**] укажите дату, до которой предоставляется доступ. В 23:59 указанной даты доступ будет автоматически отключен.
- c. В поле [**Предоставил**] по умолчанию указан пользователь, который настраивает доступ. Вы можете указать в этом поле любого пользователя, под учетной записью которого необходимо предоставить доступ сотрудникам службы поддержки.
- d. Признаки [**Запретить доступ к данным**] и [**Запретить конфигурирование**] позволяют предоставлять доступ к системе в режимах изоляции данных и ограничения доступа на конфигурирование. По умолчанию оба признака включены. Это означает, что при доступе к вашему приложению сотрудник службы поддержки не сможет видеть данные в разделах, а также не сможет выполнять настройку системы.
 - Если необходимо, чтобы у службы поддержки были такие же права доступа, как и у пользователя, под чьими учетными данными выполняется подключение, то снимите оба признака.
 - Если необходимо, чтобы сотрудник службы поддержки мог внести изменения в конфигурацию, но не видел данных в разделах системы, то снимите только признак [**Запретить конфигурирование**]. Так у него будет доступ к функциональности дизайнера системы, необходимой для выполнения настроек (например, к разделам [**Справочники**], [**Системные настройки**], [**Библиотека процессов**] и др.). При этом данные основных разделов будут ему недоступны.
 - Если необходимо, чтобы сотрудник службы поддержки мог просматривать данные в разделах, но не мог изменять конфигурацию системы, то снимите только признак [**Запретить доступ к данным**]. При этом у него будет возможность просмотреть настройки конфигурации.

3. Сохраните запись.

В результате в разделе [**Доступ внешних приложений**] вашей системы будет создана новая запись. Сотрудники службы поддержки смогут войти на сайт клиента под учетной записью и с правами пользователя, указанного при настройке доступа, не используя учетных данных клиента. В 23:59 даты, указанной в настройках, доступ будет отключен автоматически.

Просмотреть результаты подключения

1. Перейдите в раздел [**Доступ внешних приложений**] дизайнера системы ([Рис. 1](#)).

Рис. 1 — Раздел [**Доступ внешних приложений**]

Пользователи и администрирование

- Пользователи системы
- Организационные роли
- Функциональные роли
- Права доступа на объекты
- Права доступа на операции
- Журнал аудита
- Журнал изменений
- Доступ внешних приложений**

- Откройте нужную запись в реестре раздела. На странице записи вы можете просмотреть все параметры доступа ([Рис. 2](#)). После того, как сеанс доступа службы поддержки состоится, на вкладке [Сессии] страницы записи автоматически отобразятся все данные, касающиеся этого сеанса — когда он состоялся, а также какие данные были созданы в системе во время сеанса.

Рис. 2 — Пример записи с параметрами доступа в разделе [Доступ внешних приложений]

Настроить интеграцию с WhatsApp

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

WhatsApp является одним из продуктов компании Facebook, поэтому для настройки интеграции с этим мессенджером вам необходимы:

- Учетная запись в **Facebook Business Manager**. Если вы еще не зарегистрированы, воспользуйтесь

[инструкцией Facebook](#) (на английском).

- Интеграция с партнерской платформой Facebook, которая предоставляет доступ к WhatsApp Business API. На данный момент такой платформой является **Twilio**.

Для **ознакомления** с возможностями интеграции с WhatsApp вы можете зарегистрировать тестовую учетную запись с ограниченным доступом к функциональности. Чтобы воспользоваться всеми преимуществами интеграции с WhatsApp, необходимо пройти **верификацию ваших учетных записей**. Это поможет обезопасить ваши данные и ваших клиентов. В общем случае настройка интеграции с WhatsApp состоит из следующих шагов:

- Настроить в Twilio тестовую учетную запись для ознакомления (опционально). [Подробнее >>>](#)
- Настроить в Twilio учетную запись для бизнеса. [Подробнее >>>](#)
- Настроить в Creatio канал чатов WhatsApp. [Подробнее >>>](#)

Для канала WhatsApp действуют следующие **ограничения** на пересылку файлов:

- Изображения** форматов *.jpg, *.jpeg, *.png.
- Аудиофайлы** форматов *.mp3, *.ogg, *.amr.
- Документы** формата *.pdf.
- Видео** формата *.mp4.
- Максимальный размер** файла — 16 Мб.

Подробнее о допустимых форматах файлов читайте в [документации Twilio](#).

На заметку. Список стран, с поставщиками телекоммуникационных услуг которых работает Twilio, ограничен. Ознакомьтесь с их [перечнем](#). (Кроме перечисленных, у Twilio нет ограничений для номеров США). Если Ваш номер не попадает в список допустимых, ознакомьтесь с [инструкцией Twilio](#).

Шаг 1. Настроить тестовую учетную запись (опционально)

Настройка тестовой учетной записи в Twilio не требует верификации и подключения платных услуг платформы. Она позволяет протестировать возможности интеграции Creatio с WhatsApp, обмена сообщениями и файлами в чате. Настройка тестовой интеграции состоит из следующих шагов:

- Настроить в Twilio тестовую учетную запись. [Подробнее >>>](#)
- Настроить в Creatio канал чатов WhatsApp. [Подробнее >>>](#)

Настроить тестовую учетную запись в Twilio

- Зарегистрируйтесь на <https://www.twilio.com/try-twilio>. После завершения регистрации вы сможете настроить тестовую интеграцию. Также вам будет предоставлен лимит средств для проверки функциональности.

На заметку. Если в дальнейшем вы решите перевести созданную учетную запись в полноценный бизнес-аккаунт, то возможности пробного периода и тестовые средства станут недоступны. Рекомендуем использовать разные аккаунты для тестовой и рабочей учетных записей.

- Укажите endpoint URL для передачи чатов в Creatio. Для этого перейдите в настройки “песочницы” (“sandbox”) в Twilio:

[Twilio Console](#) — > Programmable Messaging — > Settings — > WhatsApp Sandbox Settings — > Sandbox Configuration и в поле [WHEN A MESSAGE COMES IN] введите значение “<https://sm-receiver.creatio.com/api/webhook/LeadGen/whatsapp>”.

- Настройте “песочницу” (“sandbox”) в Twilio:

[Twilio Console](#) — > Programmable Messaging —> Try it out —> Send a WhatsApp message.

- Отправьте код, сформированный Twilio, через WhatsApp с вашего номера на номер вашей тестовой учетной записи. Если сообщение будет доставлено успешно, вы получите уведомление в Twilio. В результате ваш номер будет добавлен в Sandbox Participants.

- Если вы хотите использовать для тестирования несколько номеров, повторите шаг 3 для каждого из них. Просмотреть список номеров, которые вы используете для тестовых целей можно в списке Sandbox Participants:

[Twilio Console](#) — > Programmable Messaging — > Settings — > WhatsApp Sandbox Settings — > Sandbox Participants.

После этого вы сможете получать на номер вашей тестовой записи сообщения от номеров, добавленных в Sandbox Participants.

Настроить тестовый канал WhatsApp в Creatio

Перед настройкой канала убедитесь, что в вашем приложении заполнены системные настройки “Адрес Identity сервера” (код “IdentityServerUrl”), “Идентификатор приложения для Identity сервера” (код “IdentityServerClientId”) и “Секретный ключ для Identity сервера” (код “IdentityServerClientSecret”). Если данные системные настройки не заполнены, обратитесь в службу поддержки Creatio.

- Перейдите в **дизайнер системы** по кнопке  .
- Откройте раздел [Настройка чатов].
- В области [Каналы] нажмите кнопку  . В появившемся меню выберите “WhatsApp”.
- В открывшейся мини-карточке заполните **параметры канала**:
 - [Номер телефона] — номер вашей тестовой учетной записи в Twilio.
 - [Номер телефона для подтверждения] — номер телефона, который входит в Sandbox Participants в Twilio.
 - [Id приложения] — SID тестовой учетной записи Twilio, который указан в поле [ACCOUNT SID] Twilio Console.
 - [Токен] — токен, сгенерированный Twilio для тестовой учетной записи. Указан в поле [AUTH TOKEN] Twilio Console.
- Нажмите [Подключить].

6. Активируйте канал чата. Для этого в открывшейся мини-карточке:

- Установите индикатор в положение [Активен].
- Выберите **очередь чата**, в которой будут обрабатываться сообщения, полученные по данному каналу.
- Нажмите [Применить].

В результате в Creatio будет подключен тестовый канал WhatsApp, вы сможете проверить возможности получения и обработки сообщений и файлов.

Шаг 2. Настроить учетную запись для бизнеса

Чтобы воспользоваться всеми возможностями, которые предоставляет Twilio для бизнеса, вам необходимо зарегистрироваться на платформе и пройти верификацию. Подробнее читайте в [документации Twilio](#) (на английском).

В общем случае порядок настройки выглядит следующим образом:

- Зарегистрируйтесь в [Facebook Business Manager](#).
 - Если у вашей компании **уже зарегистрирована** учетная запись, то перейдите к шагу 2.
 - Если **учетной записи еще нет**, то следуйте инструкциям в [документации Facebook](#).
- Зарегистрируйтесь в [Twilio](#).
- Укажите endpoint URL для передачи чатов в Creatio. Для этого перейдите в настройки “песочницы” (“sandbox”) в Twilio:

[Twilio Console](#) —> Programmable Messaging —> Settings —> WhatsApp Sandbox Settings —> Sandbox Configuration и в поле [WHEN A MESSAGE COMES IN] введите значение “<https://sm-receiver.creatio.com/api/webhook/LeadGen/whatsapp>”.
- Пройдите верификацию WhatsApp.
 - Отправьте в WhatsApp [запрос на активацию](#) вашего номера Twilio. В поле [Are you working with an ISV, SI, or third party] укажите “**No**” (Нет). После отправки запроса вы должны получить на указанный при заполнении формы email-адрес письмо с предварительным подтверждением и описанием дальнейших шагов.
 - Добавьте **номер телефона**:
[Twilio Console](#) —> Programmable Messaging —> Senders —> WhatsApp Senders и нажмите кнопку [New WhatsApp Sender].
 Вы можете использовать [свой номер телефона](#) или приобрести [номер Twilio](#).
- На заметку.** При заполнении профиля придерживайтесь [правил для отображаемых имен WhatsApp](#).
- Разрешите Twilio **отправлять сообщения** от вашего имени. Для этого перейдите в Facebook Business Manager и подтвердите запрос Twilio на отправку сообщений от имени вашей компании. Вы можете найти данный запрос:

- На business.facebook.com —> Настройки —> Настройки компании —> Запросы.
- Перейти по ссылке из электронного письма с предварительным подтверждением вашего номера телефона
- f. Пройдите **проверку компании** в Facebook Business Manager. Если ваша компания была подтверждена ранее, то переходите на следующий шаг. Для выполнения проверки перейдите: Facebook Business Manager —> Настройки —> Настройки компании —> Центр безопасности и нажмите кнопку [Начать подтверждение] или [Продолжить] в разделе [Подтверждение компании].
Подробно процесс подтверждения бизнеса описан в [документации Facebook](#).
- g. Подтвердите завершение регистрации, перейдя по ссылке из электронного письма от Twilio.

В результате в течение 24 часов после завершения верификации вам будет подключена возможность общаться с клиентами по WhatsApp с зарегистрированного номера.

Шаг 3. Добавить канал WhatsApp в Creatio

Перед настройкой канала убедитесь, что в вашем приложении заполнены системные настройки “Адрес Identity сервера” (код “IdentityServerUrl”), “Идентификатор приложения для Identity сервера” (код “IdentityServerClientId”) и “Секретный ключ для Identity сервера” (код “IdentityServerClientSecret”). Если данные системные настройки не заполнены, обратитесь в службу поддержки Creatio.

1. Перейдите в **дизайнер системы** по кнопке .
2. Откройте раздел [Настройка чатов].
3. В области [Каналы] нажмите кнопку  . В появившемся меню выберите “WhatsApp”.
4. В открывшейся мини-карточке заполните **параметры канала**:
 - a. [Номер телефона] — номер телефона, подключенный и верифицированный в Twilio.
 - b. [Номер телефона для подтверждения] — номер телефона, на который придет сообщение для подтверждения канала.
 - c. [Id приложения] — SID учетной записи Twilio, который указан в поле [ACCOUNT SID] Twilio Console.
 - d. [Токен] — токен, сгенерированный Twilio для вашей учетной записи. Указан в поле [AUTH TOKEN] Twilio Console.
5. Нажмите [Подключить].

Рис. 1 — Пример настройки канала WhatsApp

Номер телефона *+ [REDACTED]

Номер телефона для подтверждения *br/>+ [REDACTED]

Id приложения *br/>AC99 [REDACTED] 4eff

Токен *br/>bf58 [REDACTED] 25f6

ПОДКЛЮЧИТЬ **ОТМЕНА**

6. Если верификация канала прошла успешно, то откроется мини-карточка редактирования канала. Чтобы сообщения из созданного канала были доступны для обработки в коммуникационной панели, активируйте канал и привяжите его к очереди. Для этого:

- Установите индикатор в положение [Активен].
- Выберите **очередь чата**, в которой будут обрабатываться сообщения, полученные по данному каналу.
- Укажите **язык**, на котором предполагаете получать сообщения по данному каналу. Это необходимо, чтобы операторы могли использовать шаблоны быстрых ответов на языке клиентов.
- Нажмите [Применить].

В результате в Creatio будет подключен канал WhatsApp, операторы контакт-центра смогут обрабатывать сообщения данного канала на коммуникационной панели Creatio. Вся история переписки будет сохранена в разделе [Чаты].

На заметку. Обратите внимание, что один номер WhatsApp может быть связан только с одним приложением Creatio. Если вы добавите один номер на несколько приложений, например, среди разработки, тестовый и продуктовый сайты, то сообщения будут приходить только на тот сайт, интеграция с которым была настроена последней.

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.

- 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.

- 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 TerrasoftWebHost.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 портальных пользователей в секции "SspLdapProvider":

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

4. Сохраните изменения в файле TerrasoftWebHost.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**.
- **TerrasoftWebHost.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 (**NtImlUser**) или среди пользователей портала (**SSPNtImlUser**). Например, чтобы проверка осуществлялась в первую очередь среди пользователей основного приложения, укажите провайдер **NtImlUser** первым в списке значений параметра [*autoLoginProviderNames*].

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

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>:

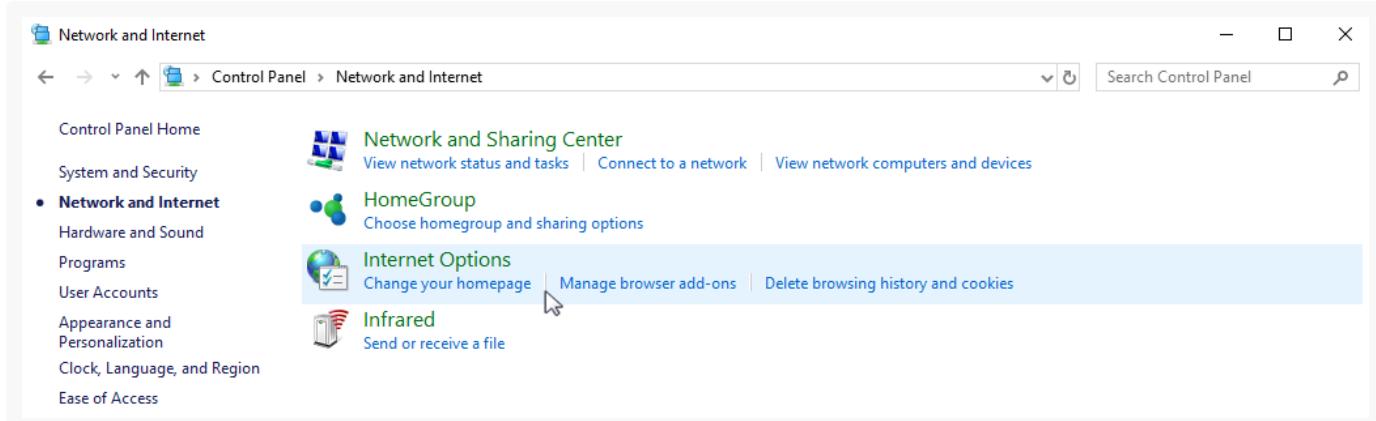
```
<appSettings> <add key="UsePathThroughAuthentication" value="true" /> ... </appSettings>
```

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:

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

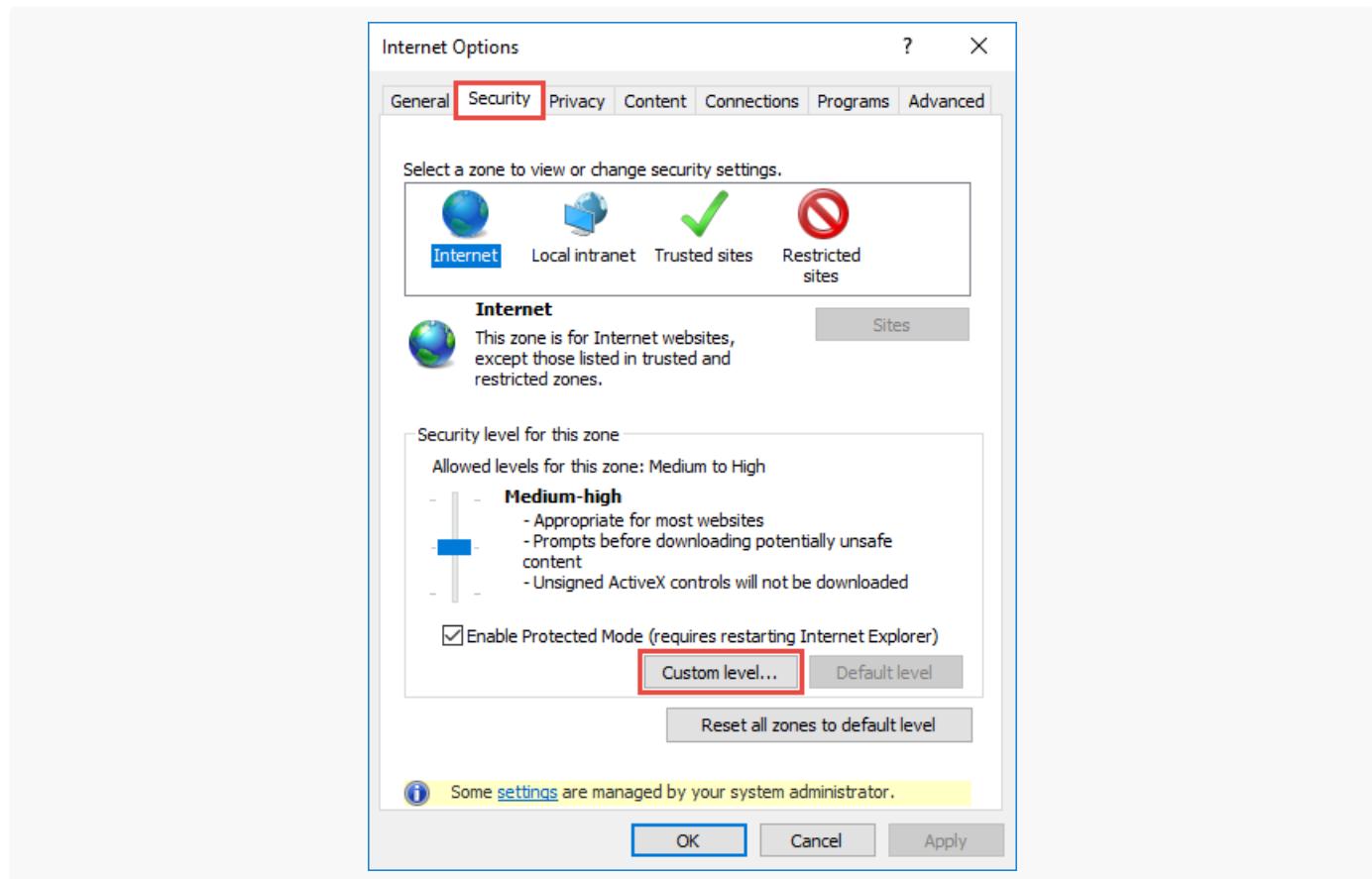
Рис. 1 — Настройка свойств обозревателя



- В открывшемся окне перейдите на вкладку "Безопасность" ("Security") и по кнопке "Другой" ("Custom

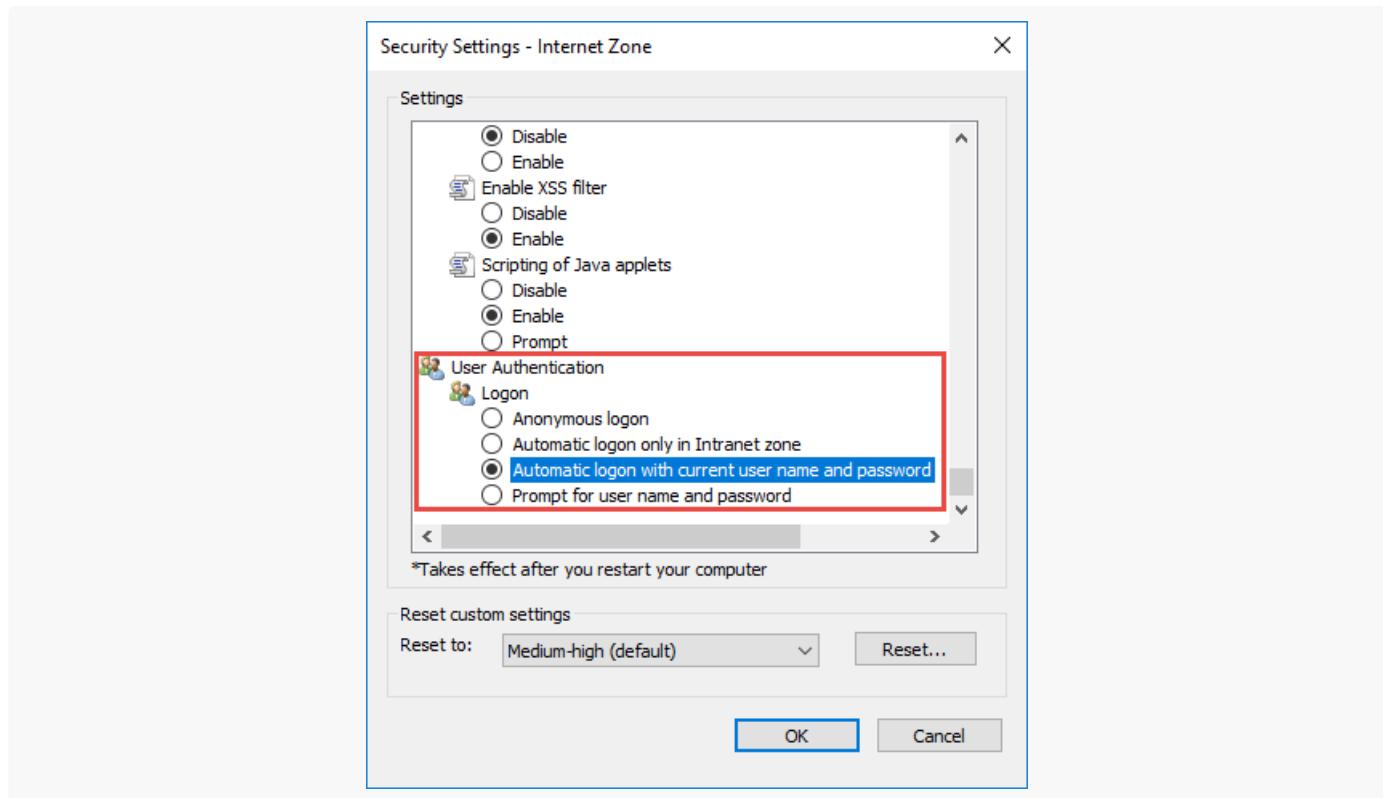
level") перейдите к настройкам безопасности (Рис. 2).

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.

Описание системных настроек

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Автонумерация записей

Наличие этих настроек зависит от используемого продукта Creatio.

Системные настройки этой группы используются для автонумерации записей в системе, например, статей базы знаний или контрагентов. Для объекта предусмотрены две настройки: с помощью первой задается статический текст (маска) номера, а вторая отвечает за хранение непосредственно числового значения номера. Например, если autogenerated номер статьи базы знаний должен быть формата: “Статья базы знаний-23”, где 23 — текущий номер статьи, то введите следующее значение маски статьи: Статья базы знаний-{0}.

Автонумерация предусмотрена для следующих объектов системы:

- “Документ” — настройки “Маска номера документа” (DocumentCodeMask) и “Текущий номер документа” (DocumentLastNumber).
- “Договор” — настройки “Маска номера договора” (ContractCodeMask) и “Текущий договор” (ContractLastNumber).
- “Контрагент” — настройки “Маска кода контрагента (AccountCodeMask) и “Текущий код контрагента” (AccountLastNumber).

- “Статья базы знаний” — настройки “Маска номера статьи базы знаний” (KnowledgeBaseCodeMask) и “Текущий номер статьи базы знаний” (KnowledgeBaseLastNumber).
- “Счет” — настройки “Маска номера счета” (InvoiceCodeMask) и “Текущий номер счета” (InvoiceLastNumber).
- “Обращение” — настройки “Маска номера обращения” (CaseCodeMask) и “Текущий номер обращения” (CaseLastNumber).
- “Сервисный договор” — настройки “Маска номера сервисного договора” (ServicePactCodeMask) и “Текущий номер сервисного договора” (ServicePactLastNumber).
- “Операция” — настройки “Маска номера операции” (CashflowCodeMask) и “Текущий номер операции” (CashflowLastNumber).
- “Проблема” — настройки “Маска номера проблемы” (ProblemCodeMask) и “Текущий номер проблемы” (ProblemLastNumber).
- “Изменение” — настройки “Маска номера изменения” (ChangeCodeMask) и “Текущий номер изменения” (ChangeLastNumber).
- “Релиз” — настройки “Маска номера релиза” (ReleaseCodeMask) и Текущий номер релиза” (ReleaseLastNumber).
- “Заказ” — настройки “Маска номера заказа” (OrderCodeMask) и “Текущий номер заказа” (OrderLastNumber).

Настройка **“Маска номера...”** используется для генерации номера или кода записи при ее создании. С помощью этой настройки задается статический текст (маска), предшествующий либо следующий после числового значения номера.

Тип: текст (500 символов).

Настройка **“Текущий номер...”** используется для генерации номера или кода записи при ее создании. В этой настройке хранится числовой номер последней созданной записи объекта.

Тип: целое число.

Автообновление возраста

Представленные ниже настройки используются для управления расчетом возраста контактов в Creatio.

Подробнее: [Расчет возраста контактов](#).

Актуализировать возраст (ActualizeAge) — управление функциональностью автоматического обновления возраста контактов. Если эта настройка отключена, то вся функциональность расчета возраста — при сохранении записи, автоматически по расписанию и по действию раздела [Контакты] — будет недоступна.

Тип: логическое. Значение по умолчанию: “включена”.

Запустить ежедневную актуализацию возраста (RunAgeActualizationDaily) — управление ежедневным автоматическим обновлением возраста. Если настройка включена, то ежедневно система будет обновлять значение в поле [Возраст] для тех контактов, у которых день рождения сегодня. Если эта настройка отключена, то в системе будет доступна вся функциональность расчета возраста, кроме ежедневного автоматического расчета.

Тип: логическое. Значение по умолчанию: “включена”.

Время запуска автоматического обновления возраста (AutomaticAgeActualizationTime) —

определение времени выполнения авторасчета возраста для именинников. Значение настройки можно указать вручную либо по действию [*Настроить время обновления возраста*] в разделе [*Контакты*].

На заметку. Если у вас большая база контактов, то рекомендуется настроить запуск расчета возраста в нерабочее время.

По умолчанию значение настройки задано в формате UTC. Однако, если было выполнено действие [*Настроить время обновления возраста*] в разделе [*Контакты*], даже без изменения времени запуска, то значение системной настройки перезапишется автоматически — время будет пересчитано с учетом часового пояса пользователя, запустившего действие. Например, если пользователь, у которого установлен часовой пояс UTC+1 (Амстердам, Берлин), запустил действие [*Настроить время обновления возраста*], но не изменил значение в окне настройки, то в системной настройке время 01:30 будет изменено на 02:30, формат UTC изменится на UTC+1.

Тип: время. Значение по умолчанию: “01:30 (UTC)”.

На заметку. Обратите внимание, что изменение времени, выполненное через системную настройку, а не через действие раздела [*Контакты*], вступит в силу после ближайшего к нему обновления возраста, через сутки после изменения значения системной настройки. Например, если вы в понедельник в 15:00 изменили значение системной настройки с 01:30 на 04:30, то ближайший запуск авторасчета возраста состоится во вторник в 01:30, а в среду — уже в 04:30. Изменения, внесенные через действие раздела [*Контакты*], применяются при ближайшем запуске авторасчета.

Дата последней актуализации возраста (LastAgeActualizationDate) — дата последнего авторасчета возраста, независимо от того, выполнялся он по расписанию или был запущен через действия раздела.

Администрирование

ID компании для лицензирования (CustomerId) — значение уникального идентификатора вашей компании, используемого при лицензировании приложения. ID компании предоставляется клиенту при приобретении лицензий на программное обеспечение.

Тип: текст (500 символов).

Способ администрирования связанных объектов (QueryJoinRightLevel) — способ администрирования связанных объектов. Например, при отображении информации об основном контакте (должности или дате рождения) из раздела [*Контрагенты*].

Тип: целое число. Значение по умолчанию: “0”. Настройке можно присвоить следующие значения:

- “0” — отображать данные только по записям связанного объекта, к которым у текущего пользователя есть доступ;
- “1” — отображать данные только по записям связанного объекта, к которым у текущего пользователя есть доступ, но в случае отсутствия доступа к записи, отображать данные основного отображаемого поля;
- “2” — отображать данные по всем записям связанного объекта независимо от распределения прав доступа.

Важно. Если у текущего пользователя нет доступа к операции “Чтение” объекта, который содержит связанную запись, то данные связанного объекта не будут отображаться, вне зависимости от значения системной настройки “Способ администрирования связанных объектов”.

ExpireLicenseNotificationTerm (ExpireLicenseNotificationTerm) — управление сроком напоминания о необходимости продлить лицензии приложения Creatio. Значение указывается в днях. Системные администраторы увидят уведомление на коммуникационной панели в случаях, когда в приложении нет лицензий на новый период или их недостаточно.

Тип: целое число. Значение по умолчанию: 14.

Включение прав на сервисные договоры и конфигурационные единицы для пользователей портала (код EnableRightsOnServiceObjects) — управление правом на чтение сервисных договоров и конфигурационных единиц пользователей и организаций портала.

Для просмотра **сервисного договора** контакты пользователей портала и контрагенты организаций портала должны быть указаны на детали Объекты обслуживания данной записи.

Для просмотра **конфигурационной единицы** контакты пользователей портала и контрагенты организаций портала должны быть указаны на детали Пользователи данной записи.

Тип: логическое. Значение по умолчанию: “включена”.

Раздавать права на обращение организации портального пользователя (код GrantCasePermissionsForPortalOrganization) — управление правом на чтение обращений пользователя портала. При включенной настройке все сотрудники организации на портале будут иметь право на чтение обращений, созданных другими сотрудниками этой организации.

Тип: логическое. Значение по умолчанию: “включена”.

Журнал аудита

Регистрировать события управления диапазонами IP-адресов (UseAdminClientIPLog) — возможность логировать изменения или удаления диапазонов допустимых IP-адресов.

Тип: логическое. Значение по умолчанию: “отключена”.

Регистрировать события управления правами доступа к колонкам

(UseAdminEntitySchemaColumnLog) — возможность логировать изменения прав доступа на колонки объектов.

Тип: логическое. Значение по умолчанию: “отключена”.

Регистрировать события управления правами доступа к объекту для внешних ресурсов (UseAdminEntitySchemaExternalServiceLog) — возможность логировать изменения прав доступа на объекты, используемые для интеграции Creatio с внешними сервисами по протоколу OData.

Тип: логическое. Значение по умолчанию: “отключена”.

Регистрировать события управления ролями пользователей (UseAdminUserRoleLog) — возможность логировать добавление пользователей в элементы организационной структуры, исключение пользователей из ролей.

Тип: логическое. Значение по умолчанию: “отключена”.

Язык журнала аудита (AuditLogCulture) — язык сообщений журнала аудита.

Тип: справочник. Значение по умолчанию: “en-US”.

Регистрировать события авторизации пользователя (UseUserAuthorizationLog) — возможность логировать попытки авторизации пользователей в системе (как успешные авторизации, так и отказы).

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления запрещенными операциями(UseDeniedOperationLog) — возможность логировать попытки выполнения запрещенных операций.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления правами доступа на записи по умолчанию (UseAdminEntitySchemaRecordDefRightLog) — возможность логировать изменения прав доступа к записям объектов по умолчанию.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления сессиями пользователей (UseUserSessionLog) — возможность логировать завершение сессий (сеансов) пользователей.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления операциями журнала аудита (UseAdminOperationAuditLog) — возможность логировать выполнение операций в журнале аудита.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления правами доступа на операции (UseAdminOperationLog) — возможность логировать изменение прав доступа на системные операции.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления правами доступа к объекту

(UseAdminEntitySchemaOperationLog) — возможность логировать изменение прав доступа на операции чтения, изменения и удаления в объектах.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления системными настройками (UseAdminSettingsLog) —

возможность логировать изменение значений системных настроек.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления правами доступа на записи

(UseAdminEntitySchemaRecordRightLog) — возможность логировать изменение прав доступа к записям объектов.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления администрируемыми объектами (UseAdminEntitySchemaLog)

— возможность логировать управление разрешенными способами администрирования объектов.

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления организационной структурой (UseAdminUnitAdminLog) —

возможность логировать управление добавлением, изменением и удалением элементов организационной структуры ("ролей" пользователей).

Тип: логическое. Значение по умолчанию: "отключена".

Регистрировать события управления пользователями (UseAdminUserLog) — возможность

логировать управление добавлением, изменением и удалением пользователей системы.

Тип: логическое. Значение по умолчанию: "отключена".

Бизнес-процессы

Бизнес-процессы, которые предлагает Creatio, при необходимости могут замещаться пользовательскими схемами. В системе предусмотрены специальные настройки, которые определяют, какой из процессов, преднастроенный или пользовательский, будет запущен при выборе соответствующего действия.

Процесс создания счета на основании заказа (CreateInvoiceFromOrderProcess) — процесс, который запускается при выборе действия [Создать счет на основании заказа] на странице заказа.

Тип: справочник. Значение по умолчанию: “Настройка доступна во всех продуктах Creatio, где доступны разделы [Счета] и [Заказы]”.

Процесс создания заказа на основании продажи (CreateOrderFromOpportunityProcess) — процесс, который запускается при выборе действия [Создать заказ на основании продажи] на странице продажи.

Тип: справочник. Значение по умолчанию: “Создание заказа на основании продажи”. Настройка доступна в продуктах Sales Creatio, enterprise edition, Sales Creatio, commerce edition и CRM-линейке Creatio.

Процесс корпоративных продаж (OpportunityManagementProcess) — процесс, который запускается при выборе действия [Запустить процесс корпоративных продаж] на странице продажи.

Тип: справочник. Значение по умолчанию: “Корпоративная продажа”. Настройка доступна в продуктах Creatio, содержащих раздел [Продажи].

Блокировка учетной записи пользователя

Представленные ниже настройки используются для настройки условий блокировки учетной записи пользователя в Creatio. Подробнее: [Разблокировать учетную запись пользователя](#).

Количество попыток входа (LoginAttemptCount) — допустимое количество неудачных попыток ввода логина или пароля.

Тип: целое число. Значение по умолчанию: “0”.

Количество попыток входа до предупреждающего сообщения (LoginAttemptBeforeWarningCount) — номер неудачной попытки ввода логина или пароля, после которого отобразится сообщение о возможности дальнейшей блокировки учетной записи пользователя.

Тип: целое число. Значение по умолчанию: “0”.

Время блокировки пользователя (UserLockoutDuration) — время блокировки (в минутах) учетной записи пользователя после неудачных попыток ввода логина или пароля.

Тип: целое число. Значение по умолчанию: “15”.

Визирование

Отправлять email уведомление о необходимости визы (SendVisaEmail) — служебная настройка, может использоваться дополнениями и коннекторами.

Тип: логическое. Значение по умолчанию: “отключена”.

Почтовый ящик для отправки письма информации о визе (VisaMailboxSettings) — учетная запись электронной почты, с которой будут отправлены уведомления о необходимости визирования. В качестве значения настройки можно выбрать любую из зарегистрированных в системе учетных записей электронной почты.

Тип: справочник.

Процесс визирования счета (InvoiceVisaProcess) — бизнес-процесс, который запускается при отправке счета на визирование.

Тип: справочник. Значение по умолчанию: “Визирование счета”. Настройка доступна в продуктах Creatio, содержащих раздел [Счета].

Процесс визирования заказа (OrderVisaProcess) — бизнес-процесс, который запускается при отправке заказа на визирование.

Тип: справочник. Значение по умолчанию: “Визирование заказа”. Настройка доступна в продуктах Creatio, содержащих раздел [Заказы].

Процесс визирования договора (ContractVisaProcess) — бизнес-процесс, который запускается при отправке договора на визирование.

Тип: справочник. Значение по умолчанию: “Визирование договора”. Настройка доступна в продуктах Creatio, содержащих раздел [Договоры].

Шаблон Email для отправки информации о визе счета (InvoiceVisaEmailTemplate) — шаблон email-сообщения, которое автоматически высылается визирующему пользователю или группе пользователей при отправке счета на визирование. Для добавления и редактирования шаблонов используется справочник “Шаблоны email-сообщений”.

Тип: справочник. Значение по умолчанию: “Шаблон уведомления о новой визе счета”. Настройка доступна в продуктах Creatio, содержащих раздел [Счета].

Шаблон Email для отправки информации о визе заказа (OrderVisaEmailTemplate) — шаблон email-сообщения, которое автоматически высылается визирующему пользователю или группе пользователей при отправке заказа на визирование. Для добавления и редактирования шаблонов используется справочник “Шаблоны email-сообщений”.

Тип: справочник. Значение по умолчанию: “Шаблон уведомления о новой визе заказа”. Настройка доступна в продуктах Creatio, содержащих раздел [Заказы].

Шаблон Email для отправки информации о визе договора (ContractVisaEmailTemplate) — шаблон email-сообщения, которое автоматически высылается визирующему пользователю или группе пользователей при отправке договора на визирование. Для добавления и редактирования шаблонов используется справочник “Шаблоны email-сообщений”.

Тип: справочник. Значение по умолчанию: “Шаблон уведомления о новой визе договора”. Настройка доступна в продуктах Creatio, содержащих раздел [Договоры].

Глобальный поиск

Вес объекта по умолчанию для глобального поиска (GlobalSearchDefaultEntityWeight) — повышение приоритета отображения в списке результатов поиска записей, содержащихся в разделе, в котором выполняется поиск. Например, если вы введете поисковый запрос, находясь в разделе [Контакты], то в начале списка результатов отобразятся записи из данного раздела.

Вес первичной колонки по умолчанию для глобального поиска

(GlobalSearchDefaultPrimaryColumnWeight) — повышение приоритета отображения в списке результатов поиска. Применяется, если совпал поисковый запрос и значение, указанное в первичной колонке такой записи (например, для контакта первичной колонкой является поле [ФИО], для контрагента — поле [Название]). Таким образом, если поисковый запрос совпадет со значением в первичной колонке записи, то такая запись будет отображена в начале списка результатов поиска.

Отображать результаты поиска по частичному совпадению (UseInexactGlobalSearch) — отображение в списке результатов поиска данных, которые были найдены с учетом морфологии и распространенных опечаток.

Тип: логическое. Значение по умолчанию: “отключена”.

Доля совпадения для отображения в результатах поиска, % (GlobalSearchShouldMatchPercent) — регулирование выдачи результатов поиска по частичному совпадению. Если в системной настройке задать целое значение от 0 до 100, то чем меньше значение, тем больше результатов с частичным совпадением будет отображено. Это повышает вероятность найти данные, если поисковый запрос неточный.

Журнал процессов

Представленные ниже настройки используются для управления операциями, которые выполняются в журнале процессов Creatio. Подробнее: [Журнал процессов](#). Настройки содержатся в группе “Журнал процессов” раздела [Системные настройки].

Срок пребывания экземпляра процесса в состоянии “Ошибка” (дней)

(AllowedTimeForProcessInErrorHandler) — период, в течение которого экземпляры процессов в состоянии “Ошибка” будут активными в Creatio. По истечении указанного периода такие экземпляры процессов будут автоматически отменены.

Значение по умолчанию: 20. Если задать значение “0”, то экземпляры процесса в состоянии “Ошибка” не будут отменяться (системная настройка будет выключена).

На заметку. Системная настройка “Срок пребывания экземпляра процесса в состоянии “Ошибка” (дней)” позволяет Creatio очищать журнал процессов от просроченных экземпляров процесса в состоянии “Ошибка”.

Количество записей SysProcessLog для архивирования (ProcessLogArchivingRecordsCount) — количество записей раздела [Журнал процессов], которые будут архивироваться за один раз согласно заданной частоте архивации.

Тип: целое число. Значение по умолчанию: “500”.

Срок хранения архивных данных (дней) (ArchiveDataExpirationTerm) — срок, по истечении которого все архивные экземпляры процесса будут автоматически удалены.

Значение по умолчанию: “360”. Если задать значение “0”, то архивные экземпляры процессов не будут удаляться из системы (системная настройка будет выключена).

После этого периода записи журнала процессов будут перенесены в архив

(ProcessLogArchivingPeriod) — временной промежуток в днях, после которого записи журнала будут архивироваться.

Тип: целое число. Значение по умолчанию: “30 дней”.

Максимальная длительность выполнения операций обслуживания журнала процессов (минут) (ProcessMaintenanceJobTimeout) — длительность выполнения перечисленных выше действий по обслуживанию журнала процессов. Если данные журнала процессов не могут быть обработаны в течение указанного в настройке времени, то обслуживание журнала будет приостановлено и возобновлено при следующем запуске операций обслуживания.

Периодичность запуска операций обслуживания журнала процессов (минут) — в настройке задается интервал в минутах между запуском операций обслуживания журнала процессов.

Тип: целое число. Значение по умолчанию: “5 минут”.

Заявки

Настройки доступны в продукте Financial Services Creatio, lending edition.

Основная роль участника заявки (MainParticipantRole) — роль участника сделки, который будет указан в поле [Клиент] страницы заявки.

Тип: справочник. Значение по умолчанию: “Заемщик”.

Тип основного регистрационного документа (MainRegDocumentType) — основной идентификационный документ для анкет физ. лиц.

Тип: справочник. Значение по умолчанию: “Внутренний паспорт”.

Значения по умолчанию

Наличие этих настроек зависит от используемого продукта Creatio.

Иконка для детали файлы и ссылки по умолчанию (FileDetailDefaultIcon) — иконка, которая используется для обозначения в плиточном режиме файлов на детали [Файлы и ссылки], расширение которых не внесено в справочник [Расширения файлов].

Тип: справочник. Значение по умолчанию: “default”.

Происхождение обращения по умолчанию (CaseOriginDef) — тип обращения в поле [Происхождение] на странице обращения.

Тип: справочник: Значение по умолчанию: “Звонок”.

Происхождение обращения на портале по умолчанию (PortalCaseOriginDef) — тип обращения, созданного через портал.

Тип: справочник: Значение по умолчанию: “Звонок”.

Состояние документа по умолчанию (DocumentStatusDef) — состояние, которое указывается для документа при его создании.

Тип: справочник. Значение по умолчанию: “В планах”.

Состояние оплаты счета по умолчанию (InvoicePaymentStatusDef) — состояние оплаты, которое указывается для счета при его создании.

Тип: справочник. Значение по умолчанию: “Не выставлен”.

Состояние поставки заказа по умолчанию (OrderDeliveryStatusDef) — состояние, которое указывается для поставки при создании заказа.

Тип: справочник. Значение по умолчанию: “В планах”.

Состояние оплаты заказа по умолчанию (OrderPaymentStatusDef) — состояние, которое указывается для оплаты заказа при его создании.

Тип: справочник. Значение по умолчанию: “В планах”.

Состояние заказа по умолчанию (OrderStatusDef) — состояние, которое указывается для заказа при его создании.

Тип: справочник. Значение по умолчанию: “В планах”.

Единица измерения по умолчанию (DefaultUnit) — единица измерения, которая указывается при создании продукта.

Тип: справочник. Значение по умолчанию: “штук”.

Состояние проекта по умолчанию (ProjectStateDef) — состояние, которое указывается для проекта при его создании.

Тип: справочник. Значение по умолчанию: “В планах”.

Город для сотрудника по умолчанию (EmployeeCityDef) — город для построения маршрута торговых представителей, если их текущее местоположение не определено.

Источник изменения по умолчанию (ChangeSourceDef) — источник, который указывается для изменения при его создании.

Тип: справочник. Значение по умолчанию: “Проект”.

Категория изменения по умолчанию (ChangeCategoryDef) — категория, которая указывается для изменения при его создании.

Тип: справочник. Значение по умолчанию: “Нормальное”.

Код закрытия обращения по умолчанию (CaseClosureCodeDef) — код обращения, который указывается при его закрытии.

Тип: справочник. Значение по умолчанию: “Предоставлено полное решение”.

Приоритет изменения по умолчанию (ChangePriorityDef) — приоритет, который указывается для изменения при его создании.

Тип: справочник. Значение по умолчанию: “Средний”.

Приоритет обращения по умолчанию (CasePriorityDef) — приоритет, который указывается для обращения при его создании.

Тип: справочник. Значение по умолчанию: “Средний”.

Приоритет релиза по умолчанию (ReleasePriorityDef) — приоритет, который указывается для релиза при его создании.

Тип: справочник. Значение по умолчанию: “Средний”.

Сервисный договор по умолчанию (DefaultServicePact) — базовый сервисный договор, который используется для расчета сроков реакции и разрешения по стратегии, учитывающей сервисный договор, если в системе отсутствует сервисный договор по контакту или контрагенту обращения.

Тип: справочник. Значение по умолчанию: “Сервисный договор по умолчанию”.

Состояние изменения по умолчанию (ChangeStatusDef) — состояние, которое указывается для изменения при его создании.

Тип: справочник. Значение по умолчанию: “Новое”.

Состояние конфигурационной единицы по умолчанию (ConfigurationItemStatusDef) — состояние, которое указывается для конфигурационной единицы при ее создании.

Тип: справочник. Значение по умолчанию: “Используется”.

Состояние обращения по умолчанию (CaseStatusDef) — состояние, которое указывается для обращения при его создании.

Тип: справочник. Значение по умолчанию: “Новое”.

Состояние проблемы по умолчанию (ProblemStatusDef) — состояние, которое указывается для проблемы при ее создании.

Тип: справочник. Значение по умолчанию: “Новое”.

Состояние релиза по умолчанию (ReleaseStatusDef) — состояние, которое указывается для релиза при его создании.

Тип: Справочник. Значение по умолчанию: “Planned”.

Состояние сервиса по умолчанию (ServiceItemStatusDef) — состояние, которое указывается для сервиса при его создании.

Тип: справочник. Значение по умолчанию: “Предоставляется”.

Состояние сервисного договора по умолчанию (ServicePactStatusDef) — состояние, которое указывается для сервисного договора при его создании.

Тип: справочник. Состояние по умолчанию: “Действующий”.

Срок проверки просроченности обращения, минут (CaseOverduesCheckTerm) — частота проверки наличия просроченных обращений в системе. Просроченным является обращение, дата плановой реакции или планового разрешения которого меньше текущей даты, а дата фактической реакции или фактического разрешения не указана. В результате проверки у соответствующего обращения устанавливается признак в колонке [Просрочен по реакции] или [Просрочен по разрешению]. Значение настройки задается в минутах.

Тип: целое число. Значение по умолчанию: “2”.

Тип релиза по умолчанию (ReleaseTypeDef) — тип, который указывается для релиза при его создании.

Тип: справочник. Значение по умолчанию: “Малый”.

Тип сервисного договора по умолчанию (ServicePactTypeDef) — тип, который указывается для сервисного договора при его создании.

Тип: справочник. Значение по умолчанию: “SLA”.

Уровень поддержки обращения по умолчанию (CaseServiceLevelDef) — уровень поддержки, который автоматически указывается для обращений при их создании.

Тип: справочник. Значение по умолчанию: “1 линия”.

Цель изменения по умолчанию (ChangePurposeDef) — цель, которая указывается для изменения при его создании.

Тип: справочник. Значение по умолчанию: “Стандартные изменения”.

Базовый прайс-лист (BasePriceList) — прайс-лист, согласно которому указывается цена продукта.

Тип: справочник. Значение по умолчанию: “Базовый”.

Интеграция с внешними ресурсами

Системные настройки группы “Интеграция с внешними ресурсами” используются при регистрации приложения для интеграции с [социальными сетями](#) и [Google](#). Для каждой регистрации используются настройки:

- **Страница регистрации приложения** (FacebookRegistrationPage, GoogleRegistrationPage, TwitterRegistrationPage) — адрес внешнего ресурса, по которому выполняется регистрация, например, “<https://code.google.com/apis/console/>”.

- **Ключ** (FacebookConsumerKey, FacebookConsumerSecret, GoogleConsumerKey, GoogleConsumerSecret, и т. д.).
- **Секретный ключ** (FacebookConsumerSecret, GoogleConsumerSecret, TwitterConsumerSecret).

Процедура получения значений для системных настроек “Ключ” и “Секретный ключ” этой группы рассмотрена при описании процедуры регистрации приложения в социальных сетях и Google.

Конфигурирование

URI репозитория по умолчанию (DefRepositoryUri) — путь к хранилищу пакетов, используемый системой по умолчанию. Путь по умолчанию используется, если для конфигурации не указан путь к хранилищу пакетов.

Тип: текст (500 символов).

Базовая страница карточки справочника (DefLookupEditPageSchemaUid) — используется при регистрации справочников системы. С помощью этой настройки определяется страница, которая должна использоваться в качестве базовой для карточки записи стандартных справочников системы.

Тип: справочник. Значение по умолчанию: “Базовая страница редактирования справочника”.

Базовая страница окна справочника (DefLookupGridPageSchemaUid) — страница, которая должна использоваться в качестве базовой для реестра стандартных справочников системы, а также при открытии окна любого справочника системы. Используется при регистрации справочников системы.

Тип: справочник. Значение по умолчанию: “Базовая страница реестра справочника”.

На заметку. Регистрация справочников системы осуществляется в разделе [Справочники](#).

Текущий пакет (CurrentPackageld) — пакет, в котором сохраняются все изменения, внесенные в структуру разделов системы при помощи мастера разделов. Это могут быть, например, изменения, связанные с добавлением колонок в объект раздела либо добавление нового раздела в систему.

Тип: справочник По умолчанию в данной системной настройке установлен пакет Custom. Если доработки, выполненные в мастере разделов, нужно перенести в другое приложение, то текущий пакет необходимо изменить. Для этого в поле [Значение по умолчанию] выберите из справочника тот пакет, который вы планируете переносить.

Манифест мобильного приложения (MobileApplicationManifest) — название XML-файла, описывающего мобильное приложение. При указании нескольких манифестов их названия разделяются символом “;”.

Тип: строка (50 символов).

Путь к репозиторию пакетов — путь к папке хранилища, в которой находятся обновленные базовые пакеты конфигурации. Используется при обновлении версии конфигурации. Значение системной настройки предоставляет служба поддержки.

Тип: текст (500 символов).

Отображать предупреждения C# компилятора при компиляции конфигурации

(CodeCompilerWarningLevel) — уровень предупреждений компилятора C#, которые будут отображаться при компиляции файлов конфигурации. Диапазон принимаемых значений от “0” до “4”, где “0” — не выводить предупреждения, “1” — выводить самые важные предупреждения и далее в порядке возрастания.

Тип: целое число. Значение по умолчанию: “2”.

Издатель (Maintainer) — идентификация стороны, которая вносит изменения в конфигурацию. Имя издателя закрепляется за каждым пакетом отдельно. Вы можете вносить изменения только в те пакеты, издателем которых является ваша компания. Настройка используется при разработке пользовательских конфигураций для третьих сторон.

Тип: текст (250 символов).

Максимальное количество строк данных, привязываемых к пакету

(MaxPackageSchemaDataRowsCount) — если при привязке данных к пакету количество привязываемых записей достигнет значения системной настройки, то отобразится соответствующее предупреждение, после чего привязку данных необходимо будет подтвердить.

Тип: целое число. Значение по умолчанию: “100”.

На заметку. Привязка большого количества данных к пакету может занять значительное время.

Префикс названия объекта (SchemaNamePrefix) — управление обязательными префиксами пользовательских объектов. Этот префикс позволяет определить автора конфигурационных элементов, чтобы найти данные для последующего изменения или переноса. Он используется при создании новых конфигурационных объектов в мастере разделов, мастере деталей и разделе [Управление конфигурацией]. Вы можете изменить стандартный префикс, например, на аббревиатуру названия вашей компании. Для указания префикса можно использовать большие и маленькие латинские буквы. Также можно использовать цифры, но префикс не может состоять только из них или начинаться числом.

Тип: строка (50 символов). Значение по умолчанию: “Usr”.

Начальное отображаемое время расписания (SchedulerDisplayTimingStart) — время, к которому будет выполняться переход в представлении [Расписание] раздела [Активности], например, “08:00”.

Начало периода расписания (SchedulerTimingStart) — начало временного промежутка в представлении [Расписание] раздела [Активности]. Например, начало периода можно задать не с 00:00, а с 7:00, указав значение “7”.

Тип: целое число. Значение по умолчанию: “0”.

Окончание периода расписания (SchedulerTimingEnd) — окончание временного промежутка в представлении [Расписание] раздела [Активности]. Например, окончание периода можно задать не в 24:00, а в 18:00, указав значение “18”.

Тип: целое число. Значение по умолчанию: “24”.

Главная страница по умолчанию (DefaultIntroPage) — схема отображения главной страницы приложения. Определяет страницу, которая открывается при запуске приложения. Доступные для выбора значения задаются в поле [IntroPageUid] объекта “Основное меню” (“ApplicationMainMenu”).

Тип: справочник. Значение по умолчанию зависит от используемого продукта Creatio.

Тип сборки (BuildType) — Тип сборки (“Softkey” или “Demo”).

Тип: справочник. Значение по умолчанию: “Softkey”.

Режим отладки (IsDebug) — включение режима для обнаружения, локализации и устранения проблем в конфигурации приложения.

Мобильное приложение (Mobile)

Настройки доступны в продукте Creatio, enterprise edition и CRM-линейке Creatio.

Радиус верификации чек-ина (CheckInRadius) — расстояние в метрах, которое считается допустимым расхождением между GPS-координатами сотрудника на визите и фактическими координатами чек-ина.

Использовать последнее известное местоположение пользователя (UseMobileLastKnownLocation) — возможность мобильного приложения обратиться к последним кэшированным данным о местоположении сотрудника и сохранить их в чек-ин в том случае, если текущие координаты неизвестны.

Тип: логическое. Значение по умолчанию: “включена”.

Настройки раздела Email

Системные настройки доступны в продуктах, которые содержат Marketing Creatio.

Включить логирование получаемых WebHooks (EnableWebHooksLogging) — необходимость логирования в системе откликов получателей рассылки. Для логирования используется инструмент log4net. Лог может быть использован разработчиком для отладки системы.

Тип: логическое. Значение по умолчанию: “отключена”.

Внешний URL-адрес приложения, используемый для получения WebHooks

(WebhooksApplicationUrl) — доступный из Internet адрес для приема откликов получателей рассылки.

Значение системной настройки задается, если при установке системы выполнялась настройка маршрутизации трафика при использовании межсетевого экрана. Тип: текст (500 символов).

Внешний URL-адрес приложения, используемый для получения запросов отписки от Email-рассылок (UnsubscribeApplicationUrl) — доступный из Internet адрес для приема запросов отписки от рассылок. При выполнении процедуры отписки к данному адресу добавляется параметр со значением ключа, который используется для отписки. Например, если значение системной настройки равно “<http://www.site.com/unsubscribe>”, то фактическая ссылка для выполнения отписки будет иметь вид “<http://www.site.com/unsubscribe?key=0123456789>”. Значение системной настройки задается, если при установке системы выполнялась настройка маршрутизации трафика при использовании межсетевого экрана.

Тип: текст (500 символов).

Интервал сбора статистики по рассылкам Email, часов (BulkEmailHourlyStatisticPeriod) — период, отображаемый на графике открытий/переходов вкладки [Итоги рассылки] страницы Email-рассылки. Указывается в часах.

Тип: целое число. Значение по умолчанию: “48”.

Контакт получателя для тестовой отправки Email (TestSendingBulkEmailContact) — контакт, чьи данные будут подставлены в тестовое email-сообщение в качестве значений макросов при выполнении действия [Отправить тестовое письмо] раздела [Email].

Тип: справочник.

Отписывать пользователя от всех рассылок (UnsubscribeFromAllMailings) — автоматическая установка признака [Не использовать Email] для тех контактов, которые отписались от рассылки.

Тип: логическое. Значение по умолчанию: “включена”.

Период (дней) обновления статистики по рассылкам (MailingStatisticUpdatePeriod) — период, в

течение которого фиксируется финальный отклик по каждому контакту — участнику массовой рассылки. Любые отклики, полученные по истечению указанного периода, на статистику по рассылкам не влияют. Указывается в днях.

Тип: целое число. Значение по умолчанию: “30”.

Сайт для перенаправления отписавшихся (RedirectUnsubscribersTo) — адрес web-страницы, на которую автоматически перенаправляется пользователь, когда отписывается от рассылки.

Тип: текст (500 символов).

Интервал проверки наличия запущенных Email-рассылок, минут (MandrillSchedulerTimeStep) — периодичность, с которой система проверяет наличие запущенных рассылок, у которых время начала отправки уже наступило. Значение системной настройки указывается в минутах.

Тип: целое число. Значение по умолчанию: “1”.

Значение по умолчанию поля Список доменов в Email (GoogleAnalyticsTrackingDomains) — адреса сайтов, статистика которых будет отслеживаться при помощи Google Analytics.

Значения вводятся через запятую. Тип: текст (250 символов).

Включение опции “Системная рассылка” (SystemEmailIgnoreUnsubscribeFromAllMailings) — отображение/скрытие признака [Системная рассылка] на вкладке [Параметры] страницы рассылки. Этот признак позволяет выполнять “системные рассылки” — немаркетинговые уведомления. Системная рассылка отправляется контактам, несмотря на признак [Не использовать email], установленный на детали [Средства связи] страницы контакта.

Тип: логическое. Значение по умолчанию: “включена”.

Предотвращать отправку писем получателям с одинаковым email адресом

(PreventDuplicatesSending) — определение дублей email-адресов в рассылке для отправки письма только одному контакту из тех, у кого указан один и тот же email-адрес. Контакт выбирается случайным образом.

Тип: логическое. Значение по умолчанию: “отключена”.

Обращения

Системные настройки доступны в продуктах Service Creatio, customer center edition, Service Creatio, enterprise edition, Financial Services Creatio, bank customer journey edition и CRM-линейке Creatio.

Первая линия поддержки (FirstSupportLine) — преднастроенная группа пользователей, которая соответствует значению “1 линия” справочника “Роли в команде обслуживания”. Используется в процессе управления инцидентами при эскалации инцидента.

Тип: справочник. Значение по умолчанию: “1-я линия поддержки”.

Вторая линия поддержки (SecondSupportLine) — преднастроенная группа пользователей, которая соответствует значению “2 линия” справочника “Роли в команде обслуживания”. Используется в процессе управления инцидентами при эскалации инцидента.

Тип: справочник. Значение по умолчанию: “2-я линия поддержки”.

Третья линия поддержки (ThirdSupportLine) — преднастроенная группа пользователей, которая соответствует значению “3 линия” справочника “Роли в команде обслуживания”. Используется в процессе управления инцидентами при эскалации инцидента.

Тип: справочник. Значение по умолчанию: “3-я линия поддержки”.

Создавать контакты по неопознанным email-адресам (CreateNewContactsForUnknownEmailAddresses)

— управление созданием в системе новых записей контактов заявителей, если обращение было получено с неопознанного email-адреса.

Тип: логическое. Значение по умолчанию: “Включена” (признак установлен).

Количество дней ожидания после запроса оценки (FirstReevaluationWaitingDays) — количество дней ожидания оценки по обращению, прежде чем клиенту будет отправлен повторный запрос.

Тип: целое число. Значение по умолчанию: “1”.

Количество дней ожидания после повторного запроса оценки (SecondReevaluationWaitingDays) — количество дней ожидания после повторного запроса оценки по обращению, прежде чем обращение будет закрыто.

Тип: целое число. Значение по умолчанию: “1”.

Автоматически закрывать решенные обращения (CloseResolvedCases) — управление закрытием обращений в состоянии разрешения. При включенной настройке решенные обращения будут автоматически закрыты по истечении времени ожидания оценки, указанного в системных настройках “Количество дней ожидания после запроса оценки” и “Количество дней ожидания после повторного запроса оценки”.

Тип: логическое. Значение по умолчанию: “Включена” (признак установлен).

Общие

Базовый календарь пользователя (BaseUserCalendar) — календарь, который используется в системе по умолчанию.

- В Service Creatio, customer center edition и Financial Services Creatio, bank customer journey edition календарь по умолчанию используется, если другой календарь не указан в сервисе.
- В Service Creatio, enterprise edition календарь по умолчанию используется, если другой календарь не указан на странице сервиса в сервисном договоре либо на странице сервисного договора.

Тип: справочник. Значение по умолчанию: “Базовый календарь”.

Версия конфигурации (ConfigurationVersion) — текущая версия конфигурации.

Тип: строка (50 символов).

Заголовок блока средств связи на странице логина (LoginPageCommunicationBlockCaption) — название блока на странице авторизации системы, содержащего в себе средства связи.

Тип: строка (50 символов).

Заголовок блока информационных ссылок на странице логина (LoginPageLinksBlockCaption) — название блока на странице авторизации, содержащего в себе ссылки.

Тип: строка (50 символов).

Интервал проверки уведомлений (RemindingsCheckInterval) — частота проверки наличия новых уведомлений в системе. Значение настройки задается в миллисекундах (мс).

Тип: целое число. Значение по умолчанию: “300000 мс” (равно интервалу в пять минут).

Количество записей в пачке для экспорта в Excel (ExcelExportBatchSize) — увеличение значения настройки влияет на скорость выгрузки файла с большим количеством записей, а также на объем используемой оперативной памяти.

Логотип компании (LogoImage) — логотип, который будет отображаться на странице авторизации. По умолчанию отображается логотип приложения Creatio, но вы можете загрузить свой логотип. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Логотип в верхней панели (HeaderLogoImage) — изображение, которое будет отображаться вверху страниц Creatio. По умолчанию отображается логотип приложения Creatio, но вы можете загрузить свой логотип. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Логотип в главном меню (MenuLogoImage) — изображение, которое будет отображаться вверху страницы главного меню Creatio (открывается по умолчанию при входе в систему). По умолчанию отображается логотип приложения Creatio, но вы можете загрузить свой логотип. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Название продукта (ProductName) — заголовок вкладки браузера, в которой открыто приложение.

Тип: текст (250 символов). Значение по умолчанию: “Creatio”.

Домен для перенаправления (DomainToRedirect) — адрес web-страницы, на которую автоматически перенаправляется пользователь при открытии сайта в браузере.

Тип: строка (250 символов).

Максимальная длина тела письма при создании обращения по e-mail

(EmailBodyForCaseMaxLength) — максимально допустимое количество символов из email-сообщения, которое отобразится в поле [Описание обращения].

Тип: целое число. Значение по умолчанию: “600 символов”.

Максимальное количество импортируемых записей из Excel (MaxImportExcelRecordCount) — максимальное количество записей при импорте из файла MS Excel.

Тип: целое число. Значение по умолчанию: “2000”.

Максимальное количество повторений элементов процесса (MaxProcessLoopCount) — максимально допустимое количество запусков одного и того же элемента при выполнении процесса.

Тип: целое число. Значение по умолчанию: “100”.

Максимальный размер загружаемого файла (MaxFileSize) — максимальный размер файла, который можно добавить на деталь [Файлы и ссылки] в разделах системы. Значение настройки задается в мегабайтах (Мб).

Тип: целое число. Значение по умолчанию: “10 Мб”.

Минимальное количество символов для фильтрации списка (StringColumnSearchMinCharCount) — минимальное количество символов для фильтрации значений в раскрывающемся списке поля “справочник”. При вводе искомого значения непосредственно в поле (без открытия при этом окна справочника) отображается раскрывающийся список, содержащий значения справочника, которые соответствуют введенным символам. Минимальное количество символов, необходимое для отображения списка, определяется данной системной настройкой.

Тип: целое число. Значение по умолчанию: “3”.

Отображать информационное сообщение о всплывающих окнах

(ShowBrowserPopupWindowToolbars) — управление отображением панели инструментов браузера во всплывающих окнах Creatio. При работе с Creatio всплывающие окна используются в окне настройки

системы при открытии дизайнеров, карточек системных настроек, окон справочников и т.д.

Тип: логическое. Значение по умолчанию: "отключена".

Тип сравнения для строковых колонок (StringColumnSearchComparisonType) — тип оператора, используемого для фильтрации значений выпадающего списка полей "справочник".

Тип: целое число. Значение по умолчанию: "1". Может принимать одно из двух значений:

- "0" — ищет вхождение подстроки в начале строки.
- "1" — ищет вхождение подстроки в любой части строки.

Email для отправки вопроса технической поддержке (SupportEmailDef) — email-адреса технической поддержки, на которые будут отправляться письма пользователей при выполнении действия [Задать вопрос в поддержку] на коммуникационной панели. Вы можете указать, например, адрес внутренней службы поддержки. Список адресов вводится через точку с запятой.

Тип: строка (50 символов). Значение по умолчанию: "support@creatio.com".

Отправка email-сообщений

Системные настройки доступны в продуктах Service Creatio, customer center edition, Financial Services Creatio, bank customer journey edition календарь и CRM-линейке Creatio.

E-mail службы поддержки (SupportServiceEmail) — адрес электронной почты для получения автоматических извещений о новых обращениях, которые были созданы на портале самообслуживания. Также с него отправляются уведомления клиентам о состоянии их обращения.

Тип: текст (250 символов).

Адрес сайта (SiteUrl) — адрес приложения Creatio в формате <https://yoursite.domain.com/0>. Настройка используется в следующих случаях:

- Для перенаправления пользователя на нужную web-страницу после оценки качества обслуживания по обращению.
- Для синхронизации приложения Creatio с Telegram при добавлении чата.

Тип: текст (250 символов).

Имя пользователя SMTP-сервера (SmtpUserName) — полный email-адрес почтового ящика, с которого клиентам отправляются уведомления о состоянии обращений.

Тип: строка неограниченной длины.

Почтовый ящик регистрации на портале (SSPRegistrationMailbox) — почтовый ящик для отправки уведомлений о регистрации на портале самообслуживания.

Тип: справочник.

Пароль пользователя SMTP-сервера (SmtpUserPassword) — пароль почтового ящика, адрес которого указан в системной настройке "Имя пользователя SMTP-сервера".

Тип: строка неограниченной длины.

Имя или IP-адрес SMTP-сервера (SmtpHost) — координаты SMTP сервера, с которого отправляются исходящие письма. Данные для заполнения этой настройки уточните в документации вашего почтового провайдера.

Тип: строка неограниченной длины.

Порт SMTP-сервера (SmtpPort) — порт, используемый вашим SMTP-сервером для отправки почты. Данные для заполнения этой настройки уточните в документации вашего почтового провайдера.

Тип: целое число.

Использовать протокол SSL для шифрования подключения (SmtpEnableSsl) — поддержка протокола безопасного обмена данными. Возможность использования протокола SSL уточните в документации вашего почтового провайдера.

Тип: логическое.

Логотип не найдено значение оценки (ImageRaitingNotFound) — логотип на web-странице, на которую автоматически перенаправляется пользователь после оценки качества обслуживания по данному обращению. По умолчанию отображается стандартный логотип, но вы можете загрузить пользовательский. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Логотип не найдено обращение (ImageCaseNotFound) — логотип на web-странице, на которую автоматически перенаправляется пользователь после оценки качества обслуживания по данному обращению. Отображается в случае некорректно указанного номера обращения или если данное обращение удалено в системе. По умолчанию отображается стандартный логотип, но вы можете загрузить пользовательский. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Логотип оценка уже выставлена (ImageRaitingAlreadyExist) — логотип на web-странице, на которую автоматически перенаправляется пользователь после оценки качества обслуживания по данному обращению. Отображается в случае если данное обращение закрыто или если поле [Оценка на странице обращения] уже заполнено. По умолчанию отображается стандартный логотип, но вы можете загрузить пользовательский. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Логотип спасибо за оценку (ImageThanksForRaiting) — логотип на web-странице, на которую автоматически перенаправляется пользователь после оценки качества обслуживания по данному обращению. Рекомендуемый формат изображения — PNG.

Тип: изображение.

Поиск дублей

Дата последнего поиска дублей по контактам (LastContactDuplicatesSearch) — дата и время последнего поиска дублирующихся записей в разделе [Контакты].

Тип: дата/время.

Дата последнего поиска дублей по контрагентам (LastAccountDuplicatesSearch) — дата и время последнего поиска дублирующихся записей в разделе [Контрагенты].

Тип: дата/время.

Подбор продуктов

Процесс оформления выбранного продукта ("SelectedProductRegistrationProcess") — процесс оформления покупки по результатам подбора продуктов. Запускаемый процесс определяется системной настройкой в том случае, когда подбор был запущен через меню действий раздела [Продукты]. В

случае, когда подбор продуктов запускается в рамках бизнес-логики, значение системной настройки игнорируется.

Тип: справочник. Значение по умолчанию: “Процесс оформления выбранного продукта - Заявка (пример)”.

Синхронизация с LDAP

Настройки в этой группе используются при синхронизации пользователей с LDAP-сервером.

Важно. Для [настройки синхронизации с LDAP](#) рекомендуется использовать окно настройки синхронизации.

Лицензирование при синхронизации с LDAP

Пакеты лицензий для пользователя LDAP (LdapUserLicPackages) — лицензии, перечисленные в данной системной настройке, будут выданы вновь созданным пользователям при синхронизации с LDAP. Если данная настройка не заполнена, то пользователям будут выданы все лицензии. Значения вводятся через точку с запятой.

Тип: текст.

Настройки подключения к LDAP-серверу

Имя или IP-адрес LDAP-сервера (LDAPServer) — адрес, используемый системой для соединения с LDAP сервером.

Тип: строка (50 символов).

Тип аутентификации LDAP (LDAPAuthType) — тип аутентификации, используемый при авторизации пользователей LDAP. Например, Ntlm, Anonymous, Basic и т.д.

Тип: справочник.

Имя пользователя LDAP-сервера (LDAPServerLogin) — имя учетной записи пользователя LDAP-сервера, от имени которого система будет подключаться к LDAP-серверу. Например, доменное имя администратора.

Тип: строка (50 символов).

Пароль пользователя LDAP-сервера (LDAPServerPassword) — пароль учетной записи пользователя, используемый системой для подключения к LDAP-серверу. Например, пароль доменного имени администратора. Пароль хранится в системе в зашифрованном виде.

Тип: зашифрованная строка.

Настройки синхронизации пользователей

Название атрибута, который содержит ФИО пользователя LDAP (LDAPUserFullNameAttribute) — атрибут элемента в каталоге LDAP, значением которого является полное имя (ФИО) пользователя. Например, таким элементом может быть “name”.

Тип: строка (50 символов).

Название атрибута, который содержит имя пользователя LDAP (LDAPUserLoginAttribute) — атрибут элемента в каталоге LDAP, значением которого является доменное имя пользователя. Например, "AccountName".

Тип: строка (50 символов).

Название атрибута для идентификации пользователя LDAP (LDAPUserIdentityAttribute) — любой атрибут элемента в каталоге LDAP, значение которого является уникальным для всех элементов. Значение указанного атрибута используется как уникальный идентификатор записей при синхронизации пользователей. Например, в Active Directory таким элементом может выступать "objectSid".

Тип: строка (50 символов).

Элемент орг. структуры LDAP со списком пользователей для синхронизации (LDAPUsersEntry) — уникальное имя (distinguishedName, DN) элемента организационной структуры каталога LDAP (папки, группы и т.д.), который содержит синхронизируемые записи пользователей. Например, "CN=Users,DC=example,DC=com". Если каталог содержит несколько таких элементов, то необходимо указать уникальное имя общего родительского элемента. Тип: строка (50 символов).

Условие для формирования списка пользователей LDAP (LDAPUsersFilter) — условие, которому должен соответствовать элемент LDAP, чтобы быть отобранным для синхронизации пользователей. Задается в виде выражения, например, для Active Directory условие может иметь следующий вид:

```
"(&(objectClass=user)(objectClass=person)(!objectClass=computer)
(!userAccountControl:1.2.840.113556.1.4.803:=2))"
```

Тип: строка (50 символов).

Название атрибута, который содержит место работы пользователя LDAP

(LDAPUserCompanyAttribute) — атрибут элемента в каталоге LDAP, значением которого является место работы импортируемого пользователя. Используется при импорте пользователей из LDAP для автоматического заполнения поля [Контрагент] страницы контакта.

Тип: текст (250 символов).

Название атрибута, который содержит email пользователя LDAP (LDAPUserEmailAttribute) — атрибут элемента в каталоге LDAP, значением которого является адрес электронной почты импортируемого пользователя. Используется при импорте пользователей из LDAP для автоматического заполнения поля [Email] страницы контакта.

Тип: текст (250 символов).

Название атрибута, который содержит номер телефона пользователя LDAP

(LDAPUserPhoneAttribute) — атрибут элемента в каталоге LDAP, значением которого является телефонный номер импортируемого пользователя. Используется при импорте пользователей из LDAP для автоматического заполнения поля [Рабочий телефон] страницы контакта.

Тип: текст (250 символов).

Название атрибута, который содержит должность пользователя LDAP (LDAPUserJobTitleAttribute) — атрибут элемента в каталоге LDAP, значением которого является должность импортируемого пользователя. Используется при импорте пользователей из LDAP для автоматического заполнения поля [Должность] страницы контакта.

Тип: текст (250 символов).

Настройки синхронизации групп

Название атрибута, который содержит название группы LDAP (LDAPGroupNameAttribute) — атрибут элемента в каталоге LDAP, значением которого является название группы пользователей. Например, атрибут “cn” в Active Directory.

Тип: строка (50 символов).

Название атрибута для идентификации группы LDAP (LDAPGroupIdentityAttribute) — атрибут элемента в каталоге LDAP, значение которого является уникальным для всех элементов. Значение указанного атрибута используется как уникальный идентификатор записей при синхронизации групп. Например, в Active Directory таким элементом может выступать “objectSid”.

Тип: строка (50 символов).

Элемент орг. структуры LDAP со списком групп для синхронизации (LDAPGroupsEntry) — уникальное имя (distinguishedName, DN) элемента организационной структуры каталога LDAP (папки, группы, и т.д.), который содержит синхронизируемые записи групп. Например, “CN=Groups,DC=example,DC=com”. Если каталог содержит несколько таких элементов, то необходимо указать уникальное имя общего для них родительского элемента.

Тип: строка (50 символов).

Условие для формирования списка групп LDAP (LDAPGroupsFilter) — условие, которому должен соответствовать элемент LDAP, чтобы быть отобранным для синхронизации групп. Задается в виде выражения, например, для Active Directory условие может иметь следующий вид:

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

Тип: строка (50 символов).

Условие для формирования списка пользователей группы LDAP (LDAPUsersInGroupFilter) — фильтр поиска, по которому определяется, какие пользователи входят в каждую из синхронизируемых групп, например, “(memberOf=#LDAPGroupDN#)”. Для указания параметров фильтра, используйте следующие переменные:

- #LDAPGroupDN# — уникальное имя (Distinguished Name) искомой группы;
- #LDAPGroupName# — название искомой группы. Переменная будет содержать значение атрибута, указанного в поле Название группы окна настройки синхронизации;
- #LDAPGroupIdentity# — уникальный идентификатор искомой группы. Переменная будет содержать значение атрибута, указанного в поле Уникальный идентификатор группы окна настройки синхронизации.

Тип: строка (50 символов).

Дополнительные настройки синхронизации с LDAP

Название атрибута, который содержит дату изменения элемента LDAP

(LDAPEntryModifiedOnAttribute) — атрибут элемента каталога LDAP, который содержит дату и время последнего его изменения в формате “generalized time”. Используется для определения новых пользователей в группе LDAP при синхронизации.

Тип: строка (50 символов). Значение по умолчанию: “whenChanged”.

Интервал синхронизации с LDAP, часов (LDAPSyncInterval) — интервал в часах, с которым проводятся сеансы автоматической синхронизации пользователей и ролей с LDAP.

Тип: целое число. Значение по умолчанию: “1”.

Дата последней синхронизации с LDAP — дата и время последней проведенной синхронизации пользователей с LDAP. Значение системной настройки обновляется автоматически. Менять его вручную не рекомендуется. Данная системная настройка используется при проведении автоматической синхронизации с LDAP.

Тип: дата/время.

Телефония

Библиотека обмена сообщениями по умолчанию (SysMsgLib) — библиотека интеграции с телефонией, используемая по умолчанию.

Тип: справочник.

Закрывать соединение с телефонией при выходе из системы (CloseTelephonyConnectionOnLogout) — управление нагрузкой на телефонные линии. Если настройка включена, то при выходе пользователя из системы будет также выполнен выход из агента телефонии, что позволит освободить телефонную линию и рабочее место для других операторов.

Тип: Логическое. Значение по умолчанию: выключена.

Управление паролями

Отображать информацию о блокировке учетной записи при входе

(DisplayAccountLockoutMessageAtLogin), **Отображать информацию о неверном пароле при входе** (DisplayIncorrectPasswordMessageAtLogin) — управление сообщением, которое отображается при вводе неправильного имени пользователя или пароля. Отображаемое сообщение зависит от значений обеих настроек.

Тип: логическое. Значение по умолчанию: “отключена”.

Если значение “отключена” установлено для обеих настроек, то при вводе неправильного имени пользователя или пароля отображается стандартное сообщение: “Вы ввели неверный логин или пароль, либо ваша учетная запись неактивна”.

Если для обеих настроек установлено значение “включена”:

- При вводе неправильного имени пользователя отображается сообщение “Вы ввели неверный логин”.
- При вводе неправильного пароля для существующего пользователя — “Вы ввели неверный пароль”.
- При попытке авторизации заблокированного пользователя — “Ваша учетная запись заблокирована”.

Если включена только настройка “Отображать информацию о блокировке учетной записи при входе”:

- При вводе неправильного имени пользователя или пароля для существующего пользователя — “Вы ввели неверный логин или пароль”.
- При попытке авторизации заблокированного пользователя — “Ваша учетная запись заблокирована”.

Если включена только настройка “Отображать информацию о неверном пароле при входе”:

- При вводе неправильного имени пользователя отображается сообщение “Вы ввели неверный логин либо ваша учетная запись заблокирована”.

- При вводе неправильного пароля для существующего пользователя — “Вы ввели неверный пароль”.
- При попытке авторизации заблокированного пользователя — “Вы ввели неверный логин либо ваша учетная запись заблокирована”.

Количество попыток входа до предупреждающего сообщения — количество неудачных попыток ввода пароля, после которого система отобразит предупреждающее сообщение о том, сколько попыток осталось до блокирования пользователя. Если значение настройки — “0”, то предупреждение не отображается.

Тип: целое число. Значение по умолчанию: “0”.

Количество попыток входа (LoginAttemptCount) — количество неудачных попыток ввода пароля, которое есть у пользователя. Если попытки входа исчерпаны, то учетная запись пользователя будет заблокирована на время, указанное в настройке “Время блокировки пользователя”. Если значение настройки — “0”, то количество попыток не ограничено.

Тип: целое число. Значение по умолчанию: “0”.

Срок действия пароля, дней (MaxPasswordAge) — количество дней с момента создания/изменения пароля, по истечении которых пользователь должен будет сменить пароль. Смена пароля пользователя происходит при входе в систему. Если значение настройки — “0”, то срок действия пароля не ограничен.

Тип: целое число. Значение по умолчанию: “0”.

Напоминание о смене пароля, дней (PasswordChangeReminding) — количество дней, оставшихся до обязательной смены пароля. Если до истечения срока действия текущего пароля осталось указанное или меньшее количество, то при попытке авторизации пользователя система отображает сообщение о количестве дней до обязательной смены пароля и предлагает перейти на страницу изменения пароля. Если значение настройки — “0”, то предупреждение не отображается.

Тип: целое число. Значение по умолчанию: “0”.

Количество анализируемых паролей (PasswordHistoryRecordCount) — количество предыдущих паролей пользователя, с которыми не должен совпадать новый пароль. Обратите внимание, что новый пароль не должен совпадать ни с одним из ранее использованных паролей. При вводе пароля, который совпадает с одним из предыдущих анализируемых паролей, система отобразит ошибку с указанием количества предыдущих паролей, которым не должен соответствовать новый пароль. После успешного изменения пароля предыдущий пароль сохраняется в системе. Если значение настройки — “0”, то новый пароль может быть идентичен предыдущему.

Тип: целое число. Значение по умолчанию: “0”.

Время блокировки пользователя (UserLockoutDuration) — время (в минутах), в течение которого пользователь не сможет зайти в систему после превышения количества попыток ввода пароля. Если значение настройки — “0”, то пользователь заблокирован не будет.

Тип: целое число. Значение по умолчанию: “0”.

Настройки сложности паролей определяют требования, которым должен соответствовать создаваемый или изменяемый пароль пользователя системы. Следующие настройки определяют эти требования:

- **Сложность пароля: Минимальная длина** (MinPasswordLength) — минимальное количество символов в пароле.
Тип: целое число. Значение по умолчанию: “0”.
- **Сложность пароля: Минимальное количество символов нижнего регистра** — минимальное количество букв, которые не являются заглавными.

Тип: целое число. Значение по умолчанию: “0”.

- **Сложность пароля: Минимальное количество символов верхнего регистра** (MinPasswordUppercaseCharCount) — минимальное количество заглавных букв в пароле.

Тип: целое число. Значение по умолчанию: “0”.

- **Сложность пароля: Минимальное количество цифр** (MinPasswordNumericCharCount) — минимальное количество цифр в пароле.

Тип: целое число. Значение по умолчанию: “0”.

- **Сложность пароля: Минимальное количество специальных символов** (MinPasswordSpecialCharCount) — минимальное количество символов, которые не являются буквами или цифрами (#, %, &, !, ?).

Значение по умолчанию: “0”.

Управление файлами

Представленные ниже настройки используются для управления ограничениями на загрузку сторонних файлов в Creatio.

Режим проверки файлов (FileSecurityMode) — способ ограничения загрузки сторонних файлов в приложение.

Тип: справочник. Значение по умолчанию: “Список запрещенных расширений”.

Список запрещенных расширений файлов (FileExtensionsDenyList) — список расширений потенциально вредоносных файлов, которые необходимо запретить для загрузки в Creatio. Список расширений вводится через запятую, без пробелов.

Тип: текст. Значение по умолчанию:

```
ade,adp,apk,app,appx,appxbundle,asp,aspx,asx,bas,bat,bin,cab,cer,chm,cmd,cnt,com,command,conf,cr
```

Список разрешенных расширений файлов — список расширений файлов, которые чаще всего используются сотрудниками компании и разрешены к загрузке в Creatio. Список расширений вводится через запятую, без пробелов.

Тип: текст. Значение по умолчанию:

```
doc,docx,rtf,odt,pages,pdf,xls,xlsx,xlsm,xlsb,csv,ods,ppt,pptx,ppsx,txt,log,json,md,config,zip,r
```

Разрешить работу с неизвестными типами файлов (AllowFilesWithUnknownType) — правила поведения системы при попытке загрузить в нее файлы неизвестного типа. Типы файлов определяются по расширению, а, если оно не указано, то по содержимому файла.

Тип: логическое. Значение по умолчанию: “включена”.

Активное хранилище содержимого файлов (ActiveFileContentStorage) — место хранения содержимого файлов, загружаемых в Creatio. Вы можете реализовать интеграцию с внешним хранилищем, например, в облаке, и подключить его через API по работе с файлами. Это позволит

уменьшить размер базы данных вашего приложения без ограничений на работу с файлами. После регистрации в справочнике [Хранилища содержимого файлов] новое хранилище будет доступно для выбора в поле [Значение по умолчанию]. При изменении активного хранилища содержимое ранее добавленных файлов продолжает храниться там, куда оно было загружено.

Тип: Справочник. Значение по умолчанию: “База данных”.

Фильтр нежелательных обращений

Системные настройки доступны в продуктах Service Creatio, customer center edition, Service Creatio, enterprise edition, Financial Services Creatio, bank customer journey edition и CRM-линейке Creatio.

Создавать обращения по нежелательным письмам (CreateCasesFromJunkEmails) — управление созданием обращений по email-сообщениям с адресов и доменов, указанных в справочнике [Черный список Email адресов и доменов для регистрации обращений].

Тип: логическое. Значение по умолчанию: “Выключена” (признак снят).

Состояние нежелательных обращений по умолчанию (JunkCaseDefaultStatus) — управление состоянием по умолчанию для обращений, зарегистрированных по email-сообщениям с адресов и доменов, указанных в справочнике [Черный список Email адресов и доменов для регистрации обращений].

Тип: справочник. Значение по умолчанию: “Отменено”.

Финансы

Базовая валюта (PrimaryCurrency) — базовая валюта для осуществления финансовых расчетов в системе.

Тип: справочник. Значение по умолчанию: “Доллар”.

Налог по умолчанию (DefaultTax) — налог, который по умолчанию указывается для продукта при его добавлении.

Тип: справочник. Значение по умолчанию: “НДС”. Настройка доступна в продуктах Sales Creatio.

Цена сформирована с учетом налога (PriceWithTaxes) — способ учета процентной ставки налога при формировании стоимости продуктов.

Тип: логическое. Значение по умолчанию: “включена”. Настройка доступна в продуктах Sales Creatio и CRM-линейке.

Чаты

Звук уведомления о новом чате (OmniChatNotificationSound) — управление звуковым сигналом о новых сообщениях в чате.

Тип: двоичные данные.

Количество одновременных чатов (SimultaneousChats) — управление количеством активных чатов, которые доступны оператору для одновременной обработки. Если у оператора в работе максимально доступное количество чатов, то новые он не увидит, пока не завершит хотя бы один чат. Это ограничение распространяется на все доступные для оператора каналы чатов.

Тип: целое число. Значение по умолчанию: “5”.

Таймаут на взятие чата в работу оператором (OmniChatOperatorAcceptChatTimeout) — управление временем, которое дается оператору на взятие чата в работу. Если оператор не берет чат в работу в течение указанного в настройке периода, то выполнится перераспределение на следующего оператора. Тип: целое число. Значение по умолчанию: "5".

Изменить индивидуальные настройки учетной записи почты

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Учетная запись почты добавляется в систему с параметрами по умолчанию. Для каждой добавленной учетной записи вы можете индивидуально настроить параметры:

- загрузки почты;
- отправки почты;
- подписи.

На заметку. Если у вас настроена синхронизация с почтовым ящиком MS Exchange, то на странице настройки учетной записи почты также отобразятся вкладки [Встречи и задачи] и [Контакты], на которых настраиваются параметры синхронизации с календарем и контактами MS Exchange. Подробнее: [Настройка почты, контактов, расписания Microsoft Exchange / Office 365](#).

Все эти настройки выполняются на странице редактирования учетной записи, перейти на которую вы можете, выбрав учетную запись в меню [Редактировать настройки] кнопки .

Рис. 1 — Страница настроек учетной записи почты

Настройка evgeniymirny@gmail.com

[Что я могу для вас сделать? >](#)

[СОХРАНИТЬ](#) [ОТМЕНА](#) [ИЗМЕНИТЬ НАСТРОЙКИ УЧЕТНОЙ ЗАПИСИ](#)

< ПОЧТА >

[Загружать письма в систему](#)

Загружать письма за период 1 неделя ▾

- Автоматически загружать новые сообщения
- Загружать всю почту
- Загружать почту из выбранных папок

[Отправлять письма из системы](#)

- Задать псевдоним при отправке
- Использовать "evgeniymirny@gmail.com" по умолчанию при отправке писем
- Использовать подпись при отправке

[Доступ для других пользователей](#)

Настройте возможность другим пользователям работать с загруженными письмами, отправлять письма с этого адреса, а также изменять настройки учетной записи в bpm'online

Какие права доступа добавить? +

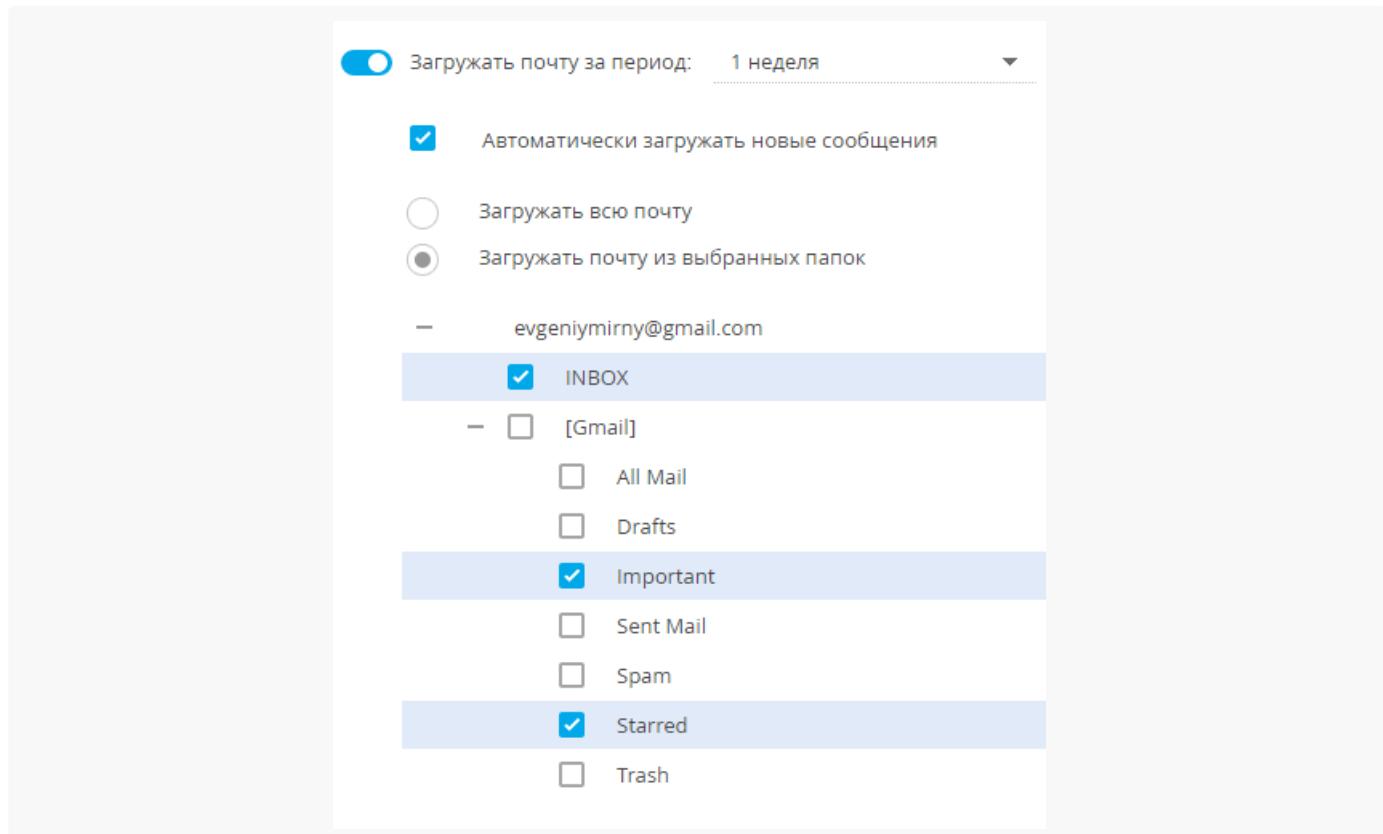
Пользователь / Роль	Доступ к письмам	Отправка писем	Настройка ящика
Нет данных			

Настроить загрузку почты в систему

- Для загрузки в систему сообщений из почтового ящика активируйте признак [Загружать почту за период] и укажите временной интервал (например, день, неделя, месяц), за который будут загружены в систему письма при первой синхронизации. Периодичность выполнения автоматической синхронизации Creatio с почтовым ящиком устанавливается в [системной настройке](#) “Интервал синхронизации с почтовым ящиком” (код “MailboxSyncInterval”).
- Для автоматической загрузки сообщений установите признак [Автоматически загружать новые сообщения].

3. Выберите опцию [Загружать всю почту] для загрузки всех сообщений из почтового ящика либо опцию [Загружать почту из выбранных папок], чтобы в Creatio загружались только сообщения из отдельных папок.
4. Если в Creatio нужно загружать не все письма из внешнего почтового ящика, то выберите опцию [Загружать почту из выбранных папок], нажмите кнопку [+], чтобы отобразить список папок указанной учетной записи и выберите папки, из которых необходимо загружать сообщения ([Рис. 2](#)).

Рис. 2 — Выбор папок для синхронизации



5. Сохраните изменения.

На заметку. Если для загрузки сообщений вы выберете только родительскую папку, то сообщения из вложенных в нее папок загружаться в Creatio не будут. Чтобы почта из вложенных папок загружалась, отметьте эти папки.

Настроить отправку почты из Creatio

Чтобы отвечать на письма непосредственно из системы, настройте параметры отправки email-сообщений. Для этого на странице настройки учетной записи почты:

1. Активируйте признак [Отправлять почту], чтобы использовать данный ящик для отправки сообщений. Если признак выключен, то почтовый ящик не будет доступен для выбора на странице редактирования письма, а также в бизнес-процессах и кейсах.
2. Для использования почтового ящика по умолчанию установите признак [Установить “email-адрес” адресом отправителя по умолчанию]. В этом случае адрес почтового ящика будет указан по

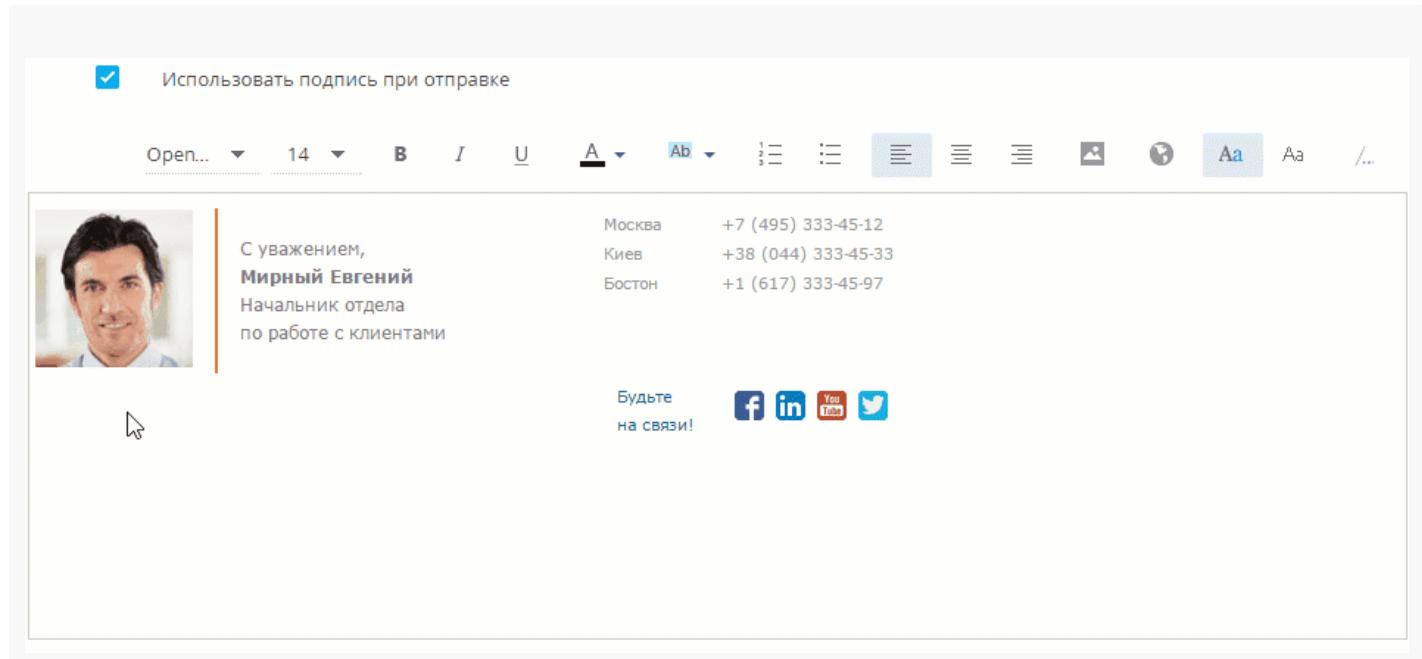
умолчанию в поле [От кого] при создании новых email-сообщений.

3. Сохраните изменения.

Настроить подпись в email-сообщениях

Для того чтобы в исходящие письма автоматически добавлялась ваша подпись, на странице настройки учетной записи почты установите признак [Использовать подпись при отправке] и в окне ввода текста добавьте желаемую подпись ([Рис. 3](#)). Сохраните изменения.

Рис. 3 — Пример добавления подписи для исходящих писем



На заметку. Вы можете скопировать подпись из своего почтового клиента и вставить ее из буфера обмена.

В некоторых браузерах в шаблон подписи можно одновременно скопировать из буфера обмена только одно изображение. Если ваша подпись содержит несколько изображений, то в этом случае оставшиеся изображения необходимо добавлять по очереди.

Рекомендации по настройке для популярных DNS-провайдеров

ПРОДУКТЫ: **MARKETING**

В процессе работы с записями SPF и DKIM учитывайте следующие нюансы:

- Чтобы изменения, внесенные в настройки DNS-сервера вашего домена вступили в силу, все новые и измененные записи должны пройти проверку на корректность. Время, которое занимает проверка, отличается для каждого провайдера и обычно занимает несколько часов из-за кеширования.

Подробную информацию можно найти в документации сервера вашего домена.

2. Возможна ситуация, когда по истечении указанного времени добавленная DKIM-запись не проходит проверку. Причиной могут быть отличия в требованиях разных DNS-серверов к форматированию DKIM-записи. Например, некоторые DNS требуют установки символа "\" перед символом ";" в начале и конце значения DKIM-записи. Некоторые, наоборот, не требуют.
3. При создании DKIM-записи необходимо руководствоваться справочной информацией вашего хостинг-провайдера либо ответами службы поддержки.

Ниже приведены ссылки на сайты часто используемых DNS-провайдеров и описаны некоторые особенности форматирования DKIM-записи:

Bluehost	DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми).
GoDaddy	DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми).
CloudFlare	DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми).
DynDNS	Поле, в которое вы вводите значение каждой записи, должно быть заключено в двойные кавычки.
MS Office 365	DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми).

[Настроить SPF- и DKIM-записи в Microsoft 365](#)

Настройка SPF

Чтобы использовать личный домен в Microsoft 365, в настройки DNS необходимо добавить специальную текстовую SPF-запись, используя команды из таблицы:

Любая почтовая система (обязательно)	v=spf1
Exchange Online	include:spf.protection.outlook.com
При использовании только Exchange Online	ip4:23.103.224.0/19 ip4:206.191.224.0/19 ip4:40.103.0.0/16 include:spf.protection.outlook.com
Microsoft 365 Germany, только Microsoft Cloud Germany	include:spf.protection.outlook.de
Сторонняя почтовая система	include:<доменное имя>, где <доменное имя> — это доменное имя сторонней почтовой системы.
Локальная почтовая система, например Exchange Online Protection с другой почтовой системой	Используйте один из следующих параметров для каждой дополнительной почтовой системы: ip4:<IP address> ip6:<IP address> include:<domain name> где значение <IP address> — это IP-адрес другой почтовой системы, а <domain name> — доменное имя другой почтовой системы, которая отправляет сообщения от имени вашего домена.
Любая почтовая система (обязательно)	Это может быть одно из нескольких значений. Рекомендуется использовать значение -all.

Например, если ваша организация использует только Microsoft 365 и у вас нет локальных почтовых серверов, то SPF-запись будет выглядеть следующим образом:

```
v=spf1 include:spf.protection.outlook.com -all
```

Это один из наиболее распространенных форматов SPF-записи для Microsoft 365. Такая запись подходит в большинстве случаев, независимо от того, где находится ваш центр данных Microsoft 365 — в США, Европе (в том числе, в Германии) или в другом месте.

Создав SPF-запись, обновите ее в службе DNS. Для домена можно создать только одну SPF-запись. Если такая запись уже существует, то следует обновить существующую запись, не добавляя новую.

После добавления SPF-записи выполните ее проверку. Более подробная информация о проверке SPF-записи доступна в статьях на сайте Microsoft.

Настройка DKIM

Для настройки DKIM добавьте на стороне провайдера две CNAME-записи для каждого дополнительного домена и включите DKIM в Microsoft 365.

1. Добавление CNAME-записей.

Для каждого домена, для которого требуется добавить подпись DKIM в DNS, необходимо добавить две CNAME-записи. Запись CNAME указывает, что каноническое имя домена является псевдонимом другого доменного имени. Используйте для записей следующий формат:

Host name	selector1._domainkey.<domain>.
Points to address or value	selector1-<domainGUID>._domainkey.<initialDomain>.
TTL	3600.
Host name	selector2._domainkey.<domain>
Points to address or value	selector2-<domainGUID>._domainkey.<initialDomain>
TTL	3600.

В указанном примере selector1 и selector2 — это селекторы для Office 365. Названия этих селекторов не меняются.

Значение domainGUID совпадает со значением domainGUID, указанным перед mail.protection.outlook.com в пользовательской записи MX для личного домена. Например, в записи creatio1-com.mail.protection.outlook.com это creatio1-com.

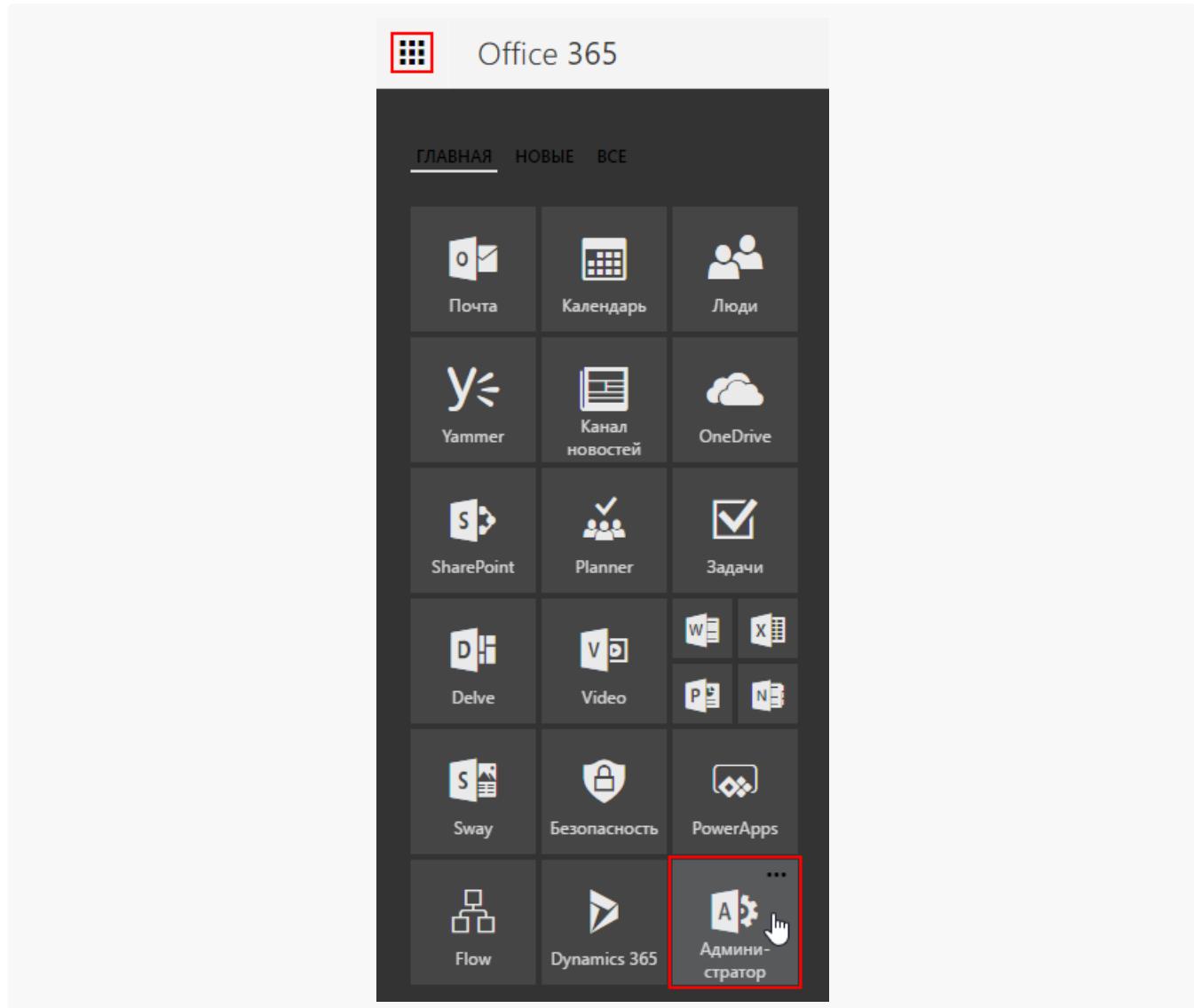
Значение initialDomain — это домен, который вы использовали при регистрации в Office 365.

2. Включение DKIM.

После добавления CNAME-записей в DNS включите подпись с помощью DKIM в Office 365.

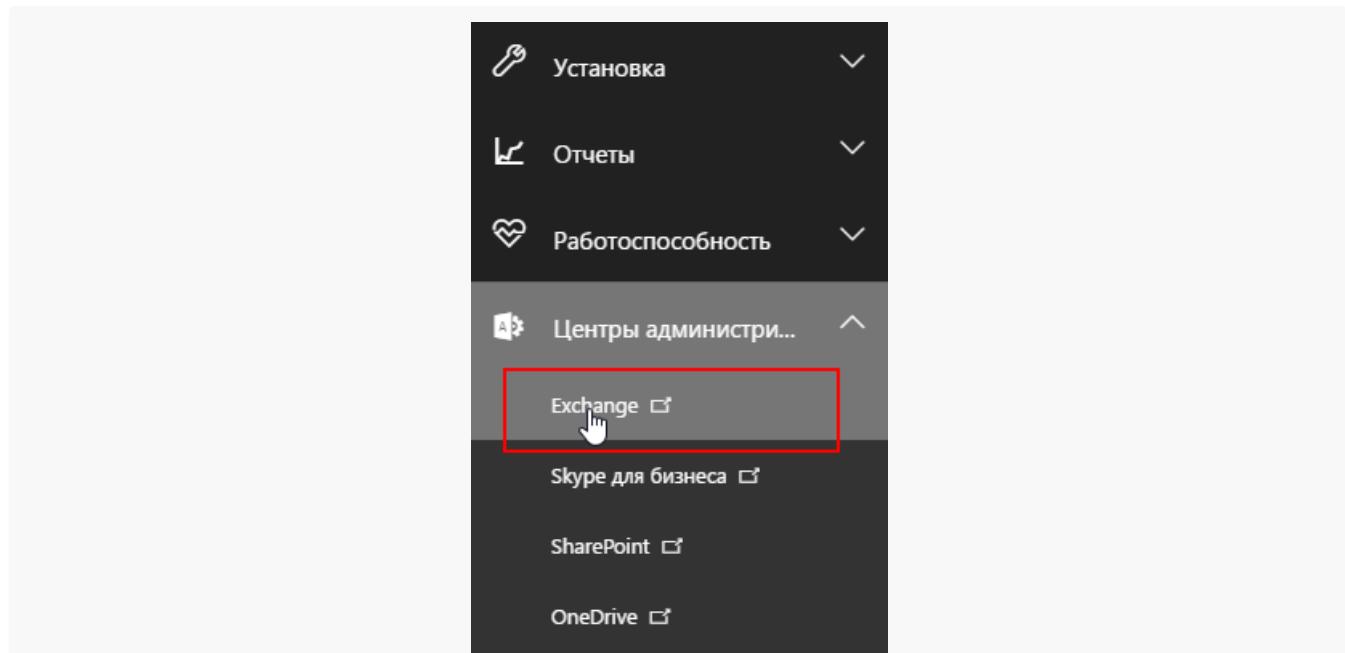
- В левом верхнем углу Office 365 нажмите на иконку запуска приложений и выберите элемент “Администратор” ([Рис. 1](#)).

Рис. 1 — Открытие меню администратора



- b. В области навигации слева внизу разверните пункт меню “Центры администрирования” и выберите элемент “Exchange” ([Рис. 2](#)).

Рис. 2 — Открытие Exchange



- c. Откройте раздел “Защита” и выберите вкладку “dkim”. В списке доменов выберите домен, для которого требуется включить DKIM, а затем в области “Добавлять подписи DKIM в сообщения для этого домена” нажмите “Включить” ([Рис. 3](#)).

Рис. 3 — Включение DKIM для домена

The screenshot shows the Exchange Admin Center interface. On the left, there's a navigation pane with items like панель мониторинга, получатели, разрешения, управление соответствием требованиям, организация, and **защита**, which is highlighted with a red box. The main content area has tabs for фильтр вредоносных программ, фильтр подключений, фильтр нежелательной почты, исходящая нежелательная почта, карантин, Центр поддержки, and **dkim**, also highlighted with a red box. Below this, a table lists domains: имя (Name), обслуживаемый домен (Managed Domain), тип домена (Domain Type), and status. The first row shows bpmonlineemailexample... and bpmonlineemailexample.onmicrosoft.com with the status "Заслужива..." (Needs Attention). To the right of the table, there's a section for adding DKIM signatures to messages for this domain, which is currently disabled ("отключено"). A large red box highlights the "Включить" (Enable) button. Below it, the status message says "Для этого домена не добавляются подписи DKIM." and the last check date is "30.01.2017 19:16".

Повторите этот шаг для каждого личного домена.

Настроить OAuth-аутентификацию для

Microsoft 365

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

OAuth — открытый стандарт аутентификации для делегирования ограниченного доступа. OAuth позволяет предоставить третьей стороне ограниченный доступ к защищенным ресурсам пользователя без необходимости использования логина и пароля. Вы можете настроить OAuth-авторизацию для учетных записей почтового сервиса Microsoft 365, предварительно зарегистрировав OAuth-приложение.

Для этого:

1. Зарегистрируйте приложение в учетной записи администратора службы управления корпоративными удостоверениями Azure Active Directory (Azure AD). Подробно о том, как это сделать, читайте в [документации Microsoft](#).

На заметку. В поле [*Redirect URI*] задайте параметры переадресации, используя следующий шаблон:

`https://<ваш_сайт>.creatio.com/0/rest/Office365OAuthAuthenticator/ProcessAuthenticationCode`.

После завершения регистрации Azure AD присвоит приложению уникальный идентификатор. Он будет отображаться в поле [*Идентификатор приложения (клиент)*] на странице обзора приложения в Azure AD. Данный параметр будет запрашивать Creatio как ключ клиента.

2. Добавьте разрешения, чтобы предоставить пользователям доступ для работы с приложением. Подробнее о добавлении разрешений для доступа к веб-API читайте в [документации Microsoft](#).
 - a. Выберите в перечне поддерживаемых APIs “Office 365 Exchange Online”. Укажите тип разрешений “Делегированные разрешения” и установите признак в поле [*EWS.AccessAsUser.All*].
 - b. Выберите в перечне поддерживаемых APIs “Microsoft Graph”. Укажите тип разрешений “Делегированные разрешения” и установите признак в поле [*User.Read*].
3. Предоставьте согласие на разрешения, настроенные для приложения, по кнопке [*Предоставить согласие администратора для клиента*]. Подробнее о кнопке согласия администратора читайте в [документации Microsoft](#).
4. Создайте секрет клиента, который будет использоваться на стороне Creatio. Как это сделать, описано в [документации Microsoft](#).
5. Скопируйте ключ для дальнейшего использования на стороне Creatio.

В результате вы получите необходимые значения параметров “Идентификатор приложения (клиент)” (“Client ID”) и “Секрет клиента” (“Client Secret”) для продолжения настройки на стороне Creatio, а само приложение Creatio будет указано в параметрах переадресации.

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 пользователячитываются 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: [Настройте 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

Name	Status	Response Type
Anonymous Authentication	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Windows Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
ASP.NET Impersonation	Disabled	

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).

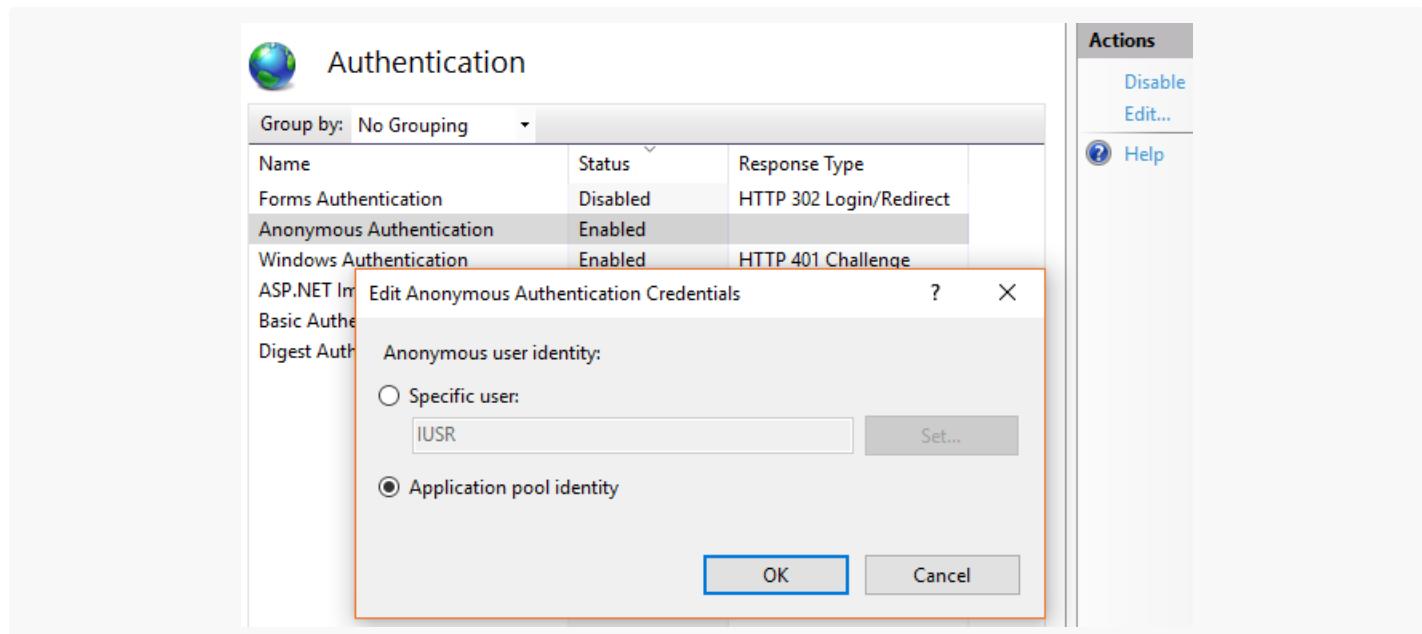
Рис. 2 — Настройки для директории Login

Name	Status	Response Type
Anonymous Authentication	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Windows Authentication	Enabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
ASP.NET Impersonation	Disabled	

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 порталов 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 порталов 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*].

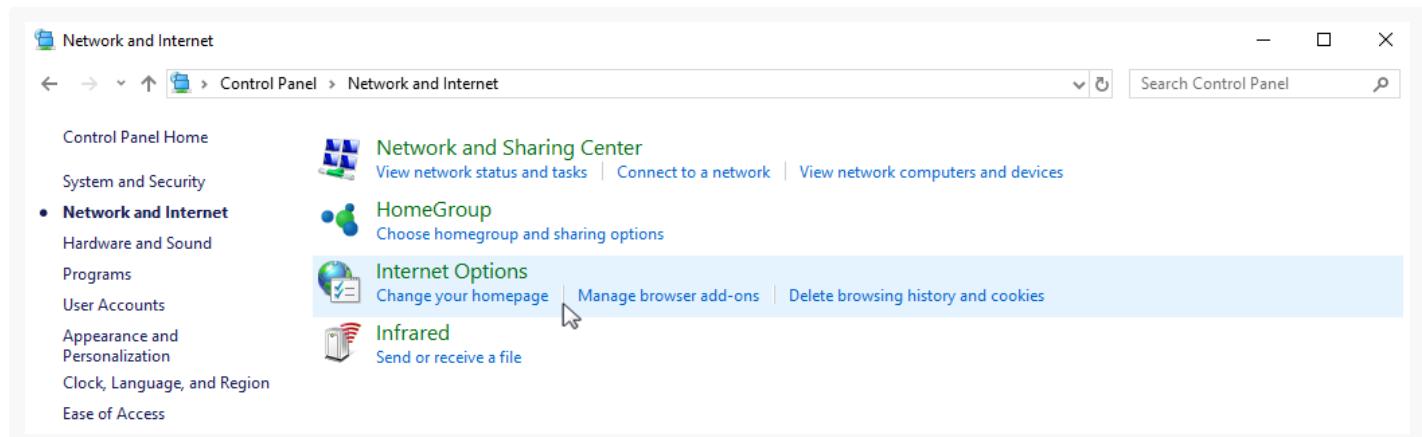
Для отображения страницы входа в систему с доступной ссылкой [*Войти под доменным пользователем*] укажите значение “false” для параметра [*UsePathThroughAuthentication*]. При этом сквозная аутентификация будет выполняться лишь при переходе на главную страницу приложения. Чтобы отобразить страницу входа,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

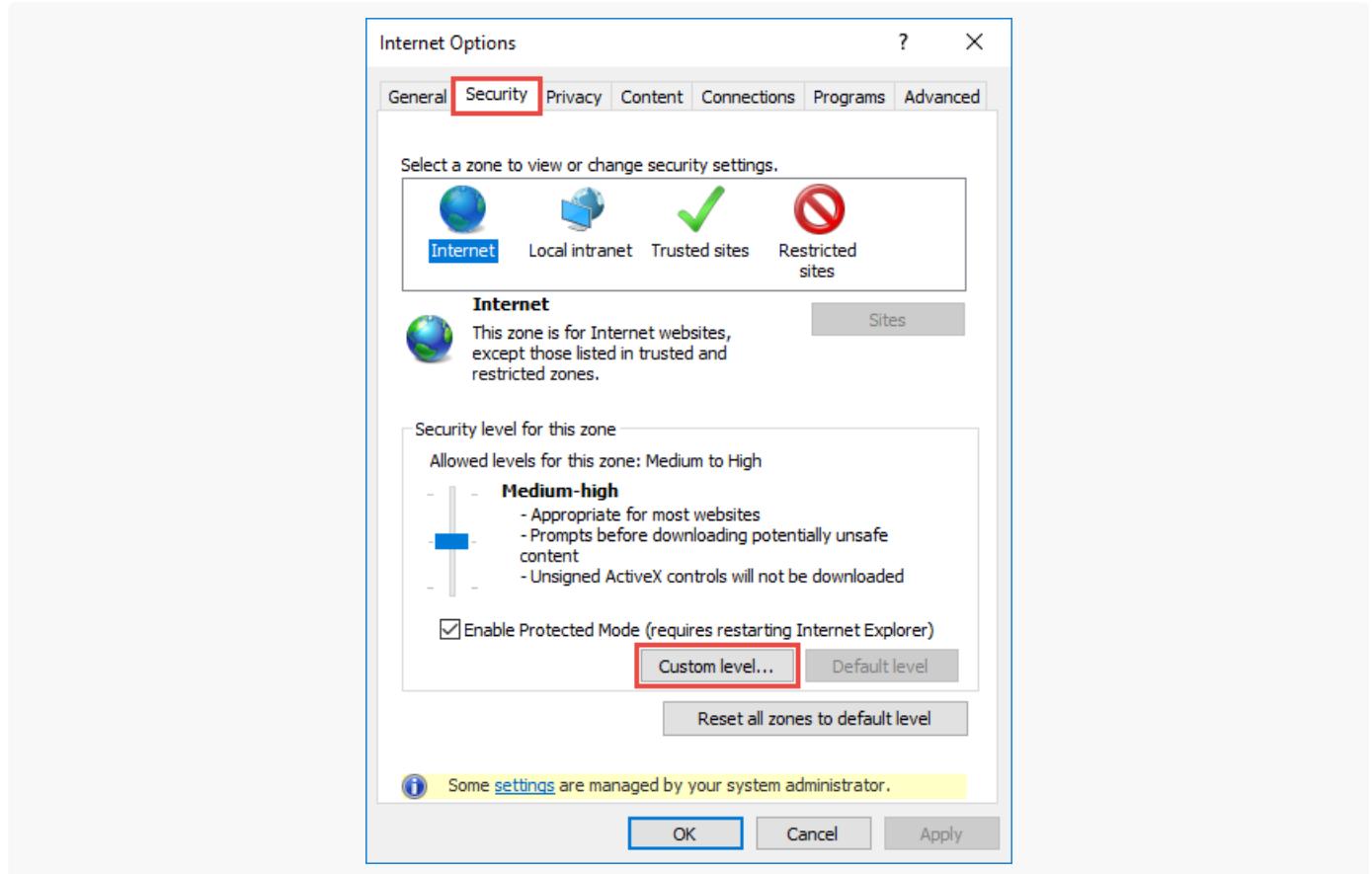
```

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

```

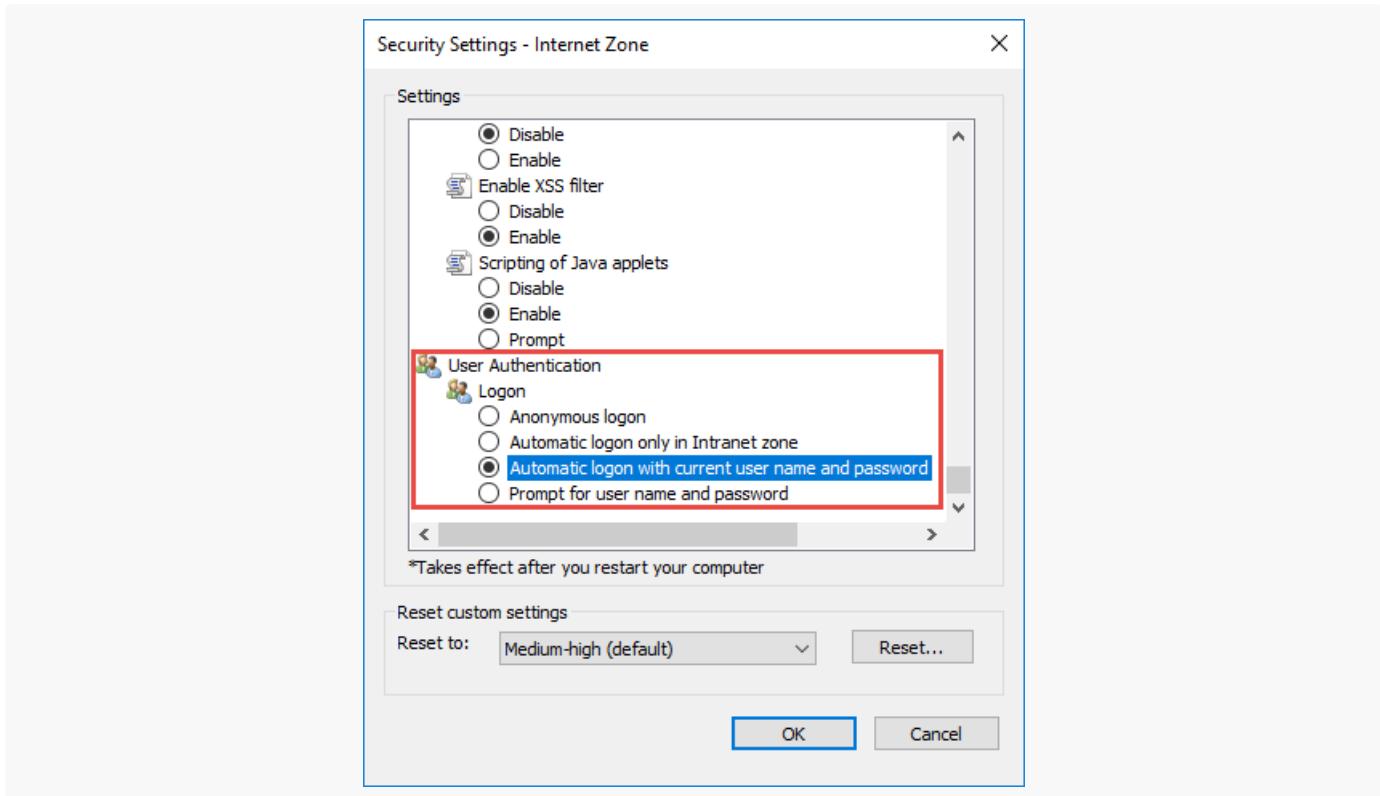
4. В открывшемся окне перейдите на вкладку “Security” и по кнопке “Custom level” перейдите к настройкам безопасности (Рис. 5).

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 разданы **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=TRUE))
```

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 базе 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

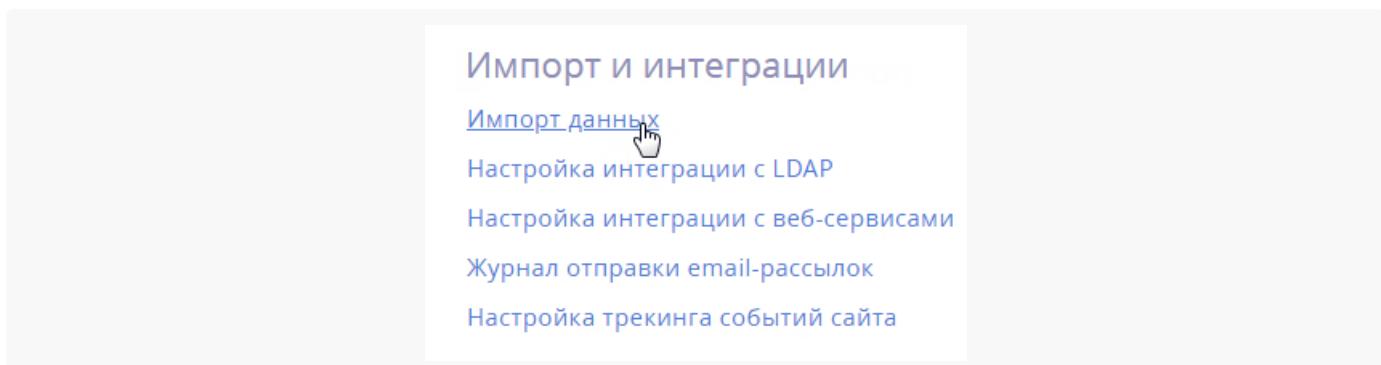
Подробнее: [Подготовить файл импорта](#).

Запустить импорт

Чтобы импортировать пользователей из Excel:

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

Рис. 1 — Переход к функциональности [Импорт данных]



- Добавьте ваш файл Excel для импорта:** перетащите его на открывшуюся страницу “Загрузка данных” или нажмите [Выбрать файл] и укажите его на вашем компьютере.
- 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 ×

Куда вы хотите загрузить данные?



КОНТАКТ



КОНТРАГЕНТ



ОБЪЕКТ
АДМИНИСТРИРОВАНИЯ

[ДАЛЕЕ](#)

- 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	<input checked="" type="checkbox"/>	Название
Тип	<input checked="" type="checkbox"/>	Тип
Контакт	<input checked="" type="checkbox"/>	Контакт
Активен	<input checked="" type="checkbox"/>	Активен
Культура	<input checked="" type="checkbox"/>	Культура

[ДАЛЕЕ](#)

- 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

Загрузка данных: Параметры дублей

ЗАКРЫТЬ НАЗАД ДАЛЕЕ

Укажите правила поиска дублей при загрузке данных

Записи являются дублями, если у них совпадают такие колонки

- Название
- Тип
- Контакт
- Активен
- Культура

НАЧАТЬ ЗАГРУЗКУ 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.](#)

- 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 дизайнере 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.

- Нажмите —> Дизайнер системы —> **“Права доступа на операции”**.
- Установите фильтр “Название = Экспорт реестра” (или “Код = CanExportGrid”). **Кликните по заголовку** системной операции или выделите ее в реестре и нажмите кнопку [Открыть].
- 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” получат доступ к системной операции [Экспорт

реестра] (Рис. 1).

Рис. 1 — Добавление прав доступа на системную операцию

Пользователь/роль	Уровень доступа	Позиция
System administrators	Да	1

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 отрабатывали 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

Процессы

Библиотека процессов

Журнал процессов

Пользователи и администрирование

- Пользователи системы
- Организационные роли
- Функциональные роли
- Права доступа на объекты
- Права доступа на операции
- Журнал аудита

Импорт и интеграции

- Импорт данных
- Настройка интеграции с LDAP
- Настройка интеграции с веб-сервисами
- Журнал отправки email-рассылок
- Настройка трекинга событий сайта

Приложения

Маркетплейс

- Управление файловым каталогом
- Управление анкетами и опросами в системе
- Настройка вычисляемых показателей в дашбордах
- Геймификация рабочих процессов

Все решения >>

Руководство по разработке на платформе

Настройте систему

Быстрый старт

Видеокурсы. Тренинги. Тестирования

Академия

Найти ответы

Сообщество

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

Способ 2. Назначить роли со страницы ролей

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

Рис. 2 — Назначение ролей через страницы соответствующих ролей

The screenshot shows the Terrasoft application interface. On the left is a vertical sidebar with icons for navigation: a right arrow, three horizontal lines, a circle with a dot, a plus sign, a bar chart, a speech bubble, a document, a person, a flag, and a shopping cart. The main content area has a header with a search bar containing 'Что я могу для вас сделать?' and a right arrow. Below the header, there's a section titled 'Процессы' (Processes) with links to 'Библиотека процессов' (Process Library) and 'Журнал процессов' (Process Journal). A red icon of a person is next to the title 'Пользователи и администрирование' (Users and Administration), which includes links to 'Пользователи системы' (System Users), 'Организационные роли' (Organizational Roles), 'Функциональные роли' (Functional Roles), 'Права доступа на объекты' (Access Rights to Objects), 'Права доступа на операции' (Access Rights to Operations), and 'Журнал аудита' (Audit Journal). Another red icon of a checkmark is next to the title 'Импорт и интеграции' (Import and Integration), which includes links to 'Импорт данных' (Import Data), 'Настройка интеграции с LDAP' (Configure Integration with LDAP), 'Настройка интеграции с веб-сервисами' (Configure Integration with Web Services), and 'Журнал отправки email-пассылок' (Email Passbook Send Log). To the right, there's a 'Маркетплейс' (Marketplace) section with a slide show of four items: 'Модуль универсального визирования' (Universal Visualization Module), 'Интеграция с решениями на платформе 1С' (Integration with 1C Solutions), 'Автоматизация подбора персонала' (Personnel Selection Automation), and 'Уникальный конструктор чатботов' (Unique Chatbot Constructor). Below the marketplace are links to 'Руководство по разработке на платформе' (Development Platform Handbook), 'SDK Руководство по разработке на платформе' (SDK Development Platform Handbook), 'Настроить систему' (Configure System), 'Быстрый старт' (Quick Start), 'Видеокурсы. Тренинги. Тестирования' (Video Courses. Training. Testing), and 'Академия' (Academy). A cursor arrow points towards the 'Import and Integration' section.

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 пользователей 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 [Использовать доступ по операциям] 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	формата *.xlsx. Если у пользователя нет права Описание 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 [Лента], вкладке [Лента] панели уведомлений, а также на вкладке [Лента] страниц просмотра и редактирования разделов системы. Пользователи могут редактировать и удалять собственные сообщения и комментарии, не обладая доступом к данной системной операции.

Настроить регистрацию лидов из LinkedIn

ПРОДУКТЫ: [MARKETING](#)

Функциональность доступна с версии Creatio 7.18.5 в режиме бета-тестирования. Будем благодарны за обратную связь.

Автоматизируйте создание лидов в Creatio благодаря интеграции с механизмом лидогенерации LinkedIn.

Перед настройкой интеграции Creatio с LinkedIn убедитесь, что ваша учетная запись LinkedIn соответствует следующим **требованиям**:

- Вам доступны формы привлечения лидов. У вас настроен рекламный аккаунт в [LinkedIn Campaign Manager](#). Подробнее о настройке рекламного аккаунта читайте в документации LinkedIn: [Создание](#)

[учетной записи LinkedIn Ads](#), [Создание форм для привлечения лидов](#).

- У вашей личной учетной записи LinkedIn есть доступ к рекламному аккаунту.
- Ваша личная учетная запись входит в роль “Суперадминистратор” или “Менеджер форм для привлечения лидов” на странице организации, связанной с рекламным аккаунтом.

Также убедитесь, что в Creatio заполнены следующие [системные настройки](#):

- “Адрес Identity сервера” (код “IdentityServerUrl”);
- “Идентификатор приложения для Identity сервера” (код “IdentityServerClientId”);
- “Секретный ключ для Identity сервера” (код “IdentityServerClientSecret”).

Если данные системные настройки не заполнены, обратитесь в службу поддержки Creatio.

Настроить интеграцию с рекламным аккаунтом LinkedIn

Вы можете настроить интеграцию с любым количеством личных учетных записей LinkedIn. Каждая из них может быть связана с несколькими рекламными аккаунтами. Интеграция с Creatio настраивается отдельно для каждого рекламного аккаунта LinkedIn.

После подключения аккаунта LinkedIn настройте соответствие полей (маппинг) и проверьте корректность передачи данных из LinkedIn в Creatio. Вы также можете воспользоваться маппингом для полей с константными значениями. Эта возможность доступна для следующих типов колонок: “Строка”, “Дробное число”, “Логическое”, “Дата/Время” и “Справочник”. Это поможет определять и фильтровать импортированные записи. Например, в справочном поле [Мероприятие] можно указать “Дни Low-Code”.

В Creatio доступны следующие возможности маппинга:

- **Маппинг по умолчанию** применяется ко всем формам привлечения лидов в вашем рекламном аккаунте. Эта функциональность доступна только для полей, которые входят в блок “Сведения профиля” группы “Сведения о лидах и настраиваемые вопросы” редактора форм LinkedIn. В этих полях содержатся данные типа “Строка” или “Дата”.
- **Пользовательский маппинг** применяется только к определенной форме привлечения лидов. Этот вид маппинга доступен всех полей, которые входят в группы “Сведения о лидах и настраиваемые вопросы” (“Сведения профиля”, “Настраиваемые вопросы”, “Пользовательские флагки”) и “Скрытые поля” редактора форм LinkedIn. В этих полях содержатся данные типа “Строка”, “Дата”, “Логическое”.

Если для формы привлечения лода настроен пользовательский маппинг, то Creatio применит его и проигнорирует настроенный маппинг по умолчанию.

Подробное описание полей формы привлечения лода вы найдете в документации LinkedIn: [Создание форм для привлечения лидов](#), [Поля формы для привлечения лидов](#).

По умолчанию в каждом из вариантов маппинга настроена передача в поле [Заметки] макроса **“not_mapped_fields”**, который передает значения всех полей формы в виде строки. Этот макрос является обязательным для формы привлечения лидов. При необходимости вы можете настроить передачу значений данного макроса в любое поле с типом данных “Строка” и неограниченной длиной.

В результате после настройки интеграции и маппинга полей в Creatio будут автоматически создаваться лиды по уникальным ответам на формы LinkedIn.

В общем случае порядок настройки интеграции Creatio и LinkedIn выглядит следующим образом:

1. Настроить интеграцию с рекламным аккаунтом LinkedIn. [Подробнее >>>](#)
2. Настроить маппинг полей по умолчанию. [Подробнее >>>](#)
3. Настроить пользовательский маппинг (опционально). [Подробнее >>>](#)

Шаг 1. Настроить интеграцию с рекламным аккаунтом LinkedIn.

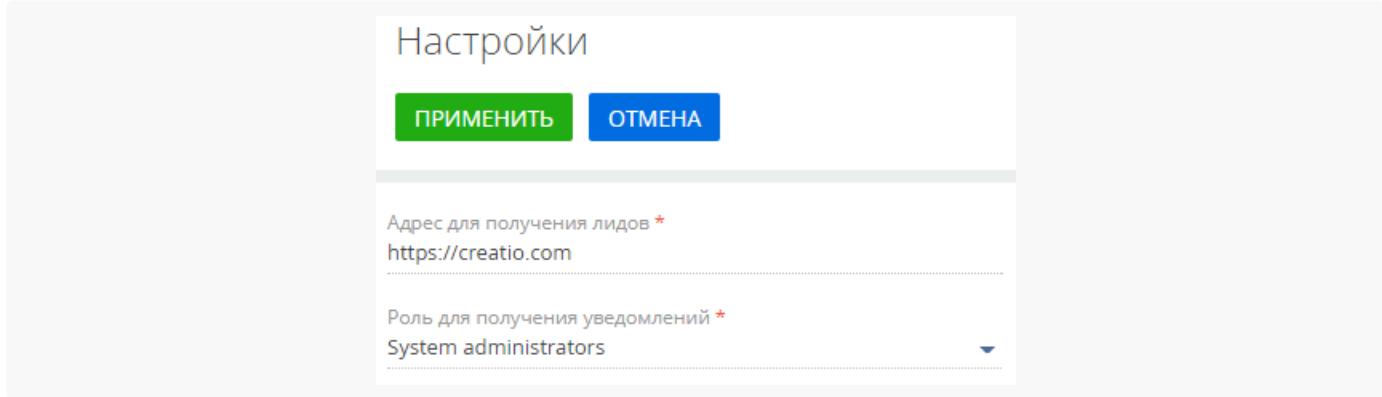
Чтобы настроить интеграцию:

1. Откройте дизайнер системы по кнопке .
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка сервиса лидогенерации социальных сетей”. Страница настройки откроется в новом окне.
3. В поле [Адрес для получения лидов] введите URL-адрес вашего приложения Creatio (Рис. 1). По умолчанию это поле заполнится значением из адресной строки браузера.

На заметку Для корректной настройки интеграции URL-адрес, указанный в поле [Адрес для получения лидов] должен быть открыт для входящих запросов. Если ваше приложение развернуто в закрытой сети, обратитесь в службу поддержки Creatio, чтобы получить список IP-адресов, которым необходимо открыть доступ.

4. В поле [Роль для получения уведомлений] укажите роль, пользователя которой будут получать в коммуникационной панели [уведомления](#) о работе лидогенерации.
5. Нажмите кнопку [Применить], чтобы сохранить настройки. Откроется реестр раздела [Лидогенерация социальных сетей].

Рис.1 — Поле [Адрес для получения лидов]



6. На открывшейся странице нажмите кнопку [Добавить]. Откроется окно выбора социальной сети.
7. Кликните по логотипу сети, интеграцию с которой необходимо настроить.
 - a. В нашем примере это LinkedIn. Нажмите [Далее].
 - b. Войдите в учетную запись LinkedIn и предоставьте Creatio доступ к управлению вашими рекламными аккаунтами. Нажмите [Разрешить].

Эта настройка выполняется только при первом входе в учетную запись.

 - c. Выберите все рекламные аккаунты, с которых вы планируете регистрировать лиды, и нажмите [Далее].

Эта настройка выполняется только при первом входе в учетную запись.

- d. Выберите в выпадающем списке один из синхронизированных аккаунтов и нажмите [Далее]. Откроется страница настройки интеграции с выбранным аккаунтом.
8. Укажите в поле [Название] имя выбранной интеграции, которое отобразится в реестре раздела (опционально).
9. Повторите шаги 6-8 для всех рекламных аккаунтов, с которых вы планируете регистрировать лиды (опционально).

В результате в Creatio будет добавлена новая интеграция с рекламным аккаунтом LinkedIn.

Шаг 2. Настроить маппинг полей по умолчанию.

Настройте маппинг полей по умолчанию, чтобы при создании лида в Creatio заполнялись данные профиля пользователя LinkedIn, который заполнил форму привлечения лиды. Для этого:

1. Перейдите к детали [Маппинг по умолчанию] в левой части страницы. Нажмите [Добавить].
2. Укажите колонки лиды, для которых необходимо настроить передачу данных из LinkedIn. Нажмите [Выбрать]. На деталь будут добавлены поля, для каждого из которых необходимо указать соответствие в форме привлечения.
3. Наведите курсор мыши на появившееся поле и нажмите кнопку . Укажите значение поля (Рис. 2). Это можно сделать несколькими способами:

Рис. 2 — Пример настройки маппинга полей по умолчанию

Новая интеграция с социальными сетями

ПРИМЕНЕНИЙ ОТМЕНА НАСТРОЙКИ ЛОГИ ЗАГРУЗИТЬ ВСЕ ЛИДЫ

Информация о синхронизации лидов

Подписка на получение лидов активна для выбранного рекламного аккаунта. Лиды, созданные на стороне LinkedIn будут переданы в Creatio.

Название.* Новая интеграция с социальными сетями

LinkedIn аккаунт Наша компания. Рекламный аккаунт

Mapping by default

Формы

Поиск

Default mapping 123

Загрузить лиды LinkedIn статус: На проверке

Пользовательский маппинг

Вебинары Академии Tech Hours

Лид Маппинг по умолчанию 16.07.2021

Конференция "LOW-CODE DAY"

Лид Маппинг по умолчанию 16.07.2021

Заметки [#Макрос.not_mapped_fields#]

Мобильный телефон

+ Добавить

Логи

Для данной формы применяются настройки маппинга по умолчанию.

- Для текстовых полей, которые необходимо заполнить значениями из формы привлечения лиды,

выберите в выпадающем списке [Поле формы]. В появившемся окне выберите поле формы привлечения лида и нажмите [Установить].

- Для текстовых полей, которые необходимо заполнить константой, выберите в выпадающем списке [Текстовое значение] и укажите необходимую информацию. Для всех лидеров, зарегистрированных при помощи данной интеграции, поле будет заполняться указанным значением.
 - Для логических полей, например, [Не использовать SMS], выберите значение “Да” или “Нет”. Для всех лидеров, зарегистрированных при помощи данной интеграции, поле будет заполняться указанным значением.
 - Для справочных полей, например, [Источник], выберите значение соответствующего справочника. Для всех лидеров, зарегистрированных при помощи данной интеграции, поле будет заполняться указанным значением.
 - Если у вас не настроен маппинг для макроса “**not_mapped_fields**”, то добавьте строковую колонку в меню кнопки выберите пункт [Другое] → [Не выбранные поля формы]. В эту колонку будут переданы все данные, полученные при заполнении формы привлечения лидов.
4. Повторите действия, описанные в п. 3, для всех полей, где необходимо настроить маппинг. Рекомендуем настроить маппинг всех полей формы с колонками Creatio, чтобы не потерять важные для возвращения лидов данные.
5. Нажмите кнопку [Применить], чтобы сохранить настройки.

Шаг 3. Настроить пользовательский маппинг (опционально).

Настройте соответствие колонок Creatio и полей, которые входят в группы “Сведения о лидах и настраиваемые вопросы” (“Сведения профиля”, “Настраиваемые вопросы”, “Пользовательские флагки”) и “Скрытые поля” редактора форм LinkedIn. Пользовательский маппинг позволяет также настроить автозаполнение колонок Creatio определенными значениями. Для этого:

1. Откройте раздел [Лидогенерация социальных сетей] и выберете интеграцию, для которой необходимо настроить маппинг. Откроется страница настройки.
2. Установите признак [Пользовательский маппинг] в правой части страницы.
3. Нажмите кнопку [Добавить].
4. Настройте поля для пользовательского маппинга. Эта настройка выполняется аналогично настройке маппинга по умолчанию.
5. Нажмите кнопку [Применить], чтобы сохранить изменения.

В результате все лиды, зарегистрированные в Creatio при заполнении данной формы привлечения лидеров LinkedIn, будут иметь уникальный LinkedIn ID.

Настроенные в приложении правила поиска дублей актуальны для всех лидеров, полученных в результате интеграции с социальными сетями. Подробнее: [Поиск дублей лидеров](#), [Поиск и объединение дублей](#).

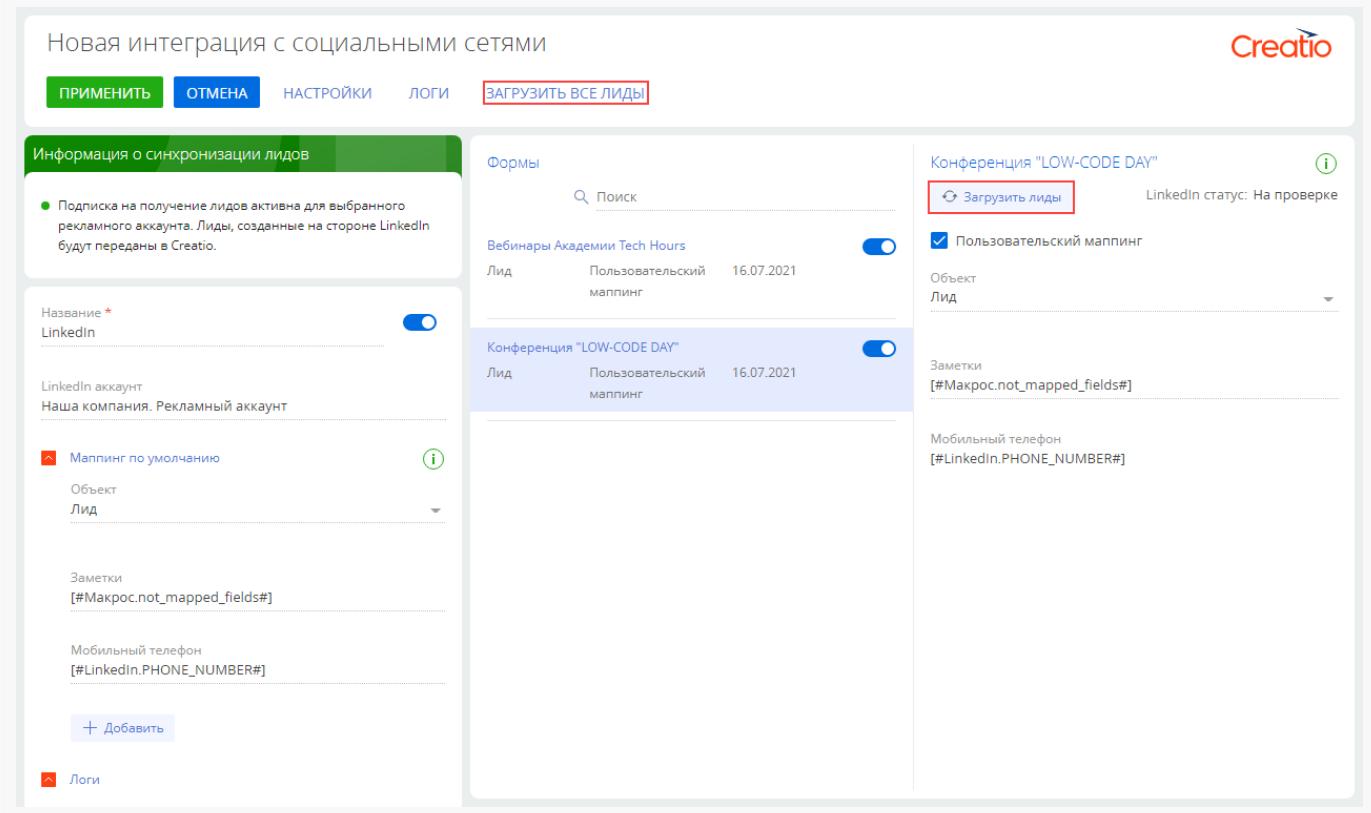
На заметку. Если вы добавляете новые поля в форму привлечения лидеров LinkedIn, не забудьте обновить маппинг в Creatio. Иначе данные из новых полей формы будут переданы только при помощи макроса “**not_mapped_fields**”.

Синхронизировать лиды, зарегистрированные до настройки интеграции

В Creatio будут создаваться только лиды, полученные после настройки интеграции. Чтобы синхронизировать лиды, которые были получены ранее:

1. Откройте дизайнер системы по кнопке .
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка сервиса лидогенерации социальных сетей”.
3. Откройте страницу интеграции, для которой необходимо выполнить настройку.
4. Нажмите [Загрузить все лиды] на панели инструментов, чтобы синхронизировать с Creatio все лиды, полученные вашим рекламным аккаунтом. Вы также можете воспользоваться кнопкой [Загрузить лиды] в правой части рабочей области, чтобы загрузить в приложение только те лиды, которые были получены через данную форму (Рис. 3). Откроется диалоговое окно.

Рис. 3 — Кнопки загрузки лидов



Новая интеграция с социальными сетями

ПРИМЕНить **ОТМЕНА** **НАСТРОЙКИ** **ЛОГИ** **ЗАГРУЗИТЬ ВСЕ ЛИДЫ**

Информация о синхронизации лидов

Подписка на получение лидов активна для выбранного рекламного аккаунта. Лиды, созданные на стороне LinkedIn будут переданы в Creatio.

Название *: LinkedIn

LinkedIn аккаунт: Наша компания. Рекламный аккаунт

Маппинг по умолчанию: **Объект**: **Лид** 

Заметки: [#Макрос.not_mapped_fields#]

Мобильный телефон: [#LinkedIn.PHONE_NUMBER#]

+ Добавить

Логи

Формы

Поиск:

Вебинары Академии Tech Hours

Лид	Пользовательский маппинг	16.07.2021
Конференция "LOW-CODE DAY"		
Лид	Пользовательский маппинг	16.07.2021

Конференция "LOW-CODE DAY" 

Загрузить лиды LinkedIn статус: На проверке

Пользовательский маппинг

Объект: **Лид**

Заметки: [#Макрос.not_mapped_fields#]

Мобильный телефон: [#LinkedIn.PHONE_NUMBER#]

5. Укажите период создания лидов, которые необходимо загрузить в приложение. Обратите внимание, что данные лидов хранятся в LinkedIn не более 90 дней. В Creatio будут загружены все уникальные лиды, созданные в указанный период, независимо от того, была ли активна интеграция с LinkedIn в момент заполнения формы.
6. Нажмите [Загрузить].

В результате в Creatio будут созданы лиды с уникальными идентификаторами LinkedIn, созданные в указанный период.

Отключить лидогенерацию LinkedIn

Отключить лидогенерацию LinkedIn можно несколькими способами. Выбор способа зависит от бизнес-задачи и требований безопасности вашей сети. Например, можно отключить интеграцию на стороне Creatio, сохранив настройки интеграции с учетной записью и рекламными аккаунтами или только с рекламными аккаунтами.

Отключить регистрацию лидов с формы или с рекламного аккаунта

1. Откройте дизайнер системы по кнопке .
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка сервиса лидогенерации социальных сетей”.
3. Откройте страницу интеграции, для которой необходимо выполнить настройку.
4. Установите переключатель рядом с названием необходимой формы в области [Форма] или рядом с полем [Имя] в левой части страницы в положение “Неактивна”.

Рис. 4 — Переключатели загрузки лидов

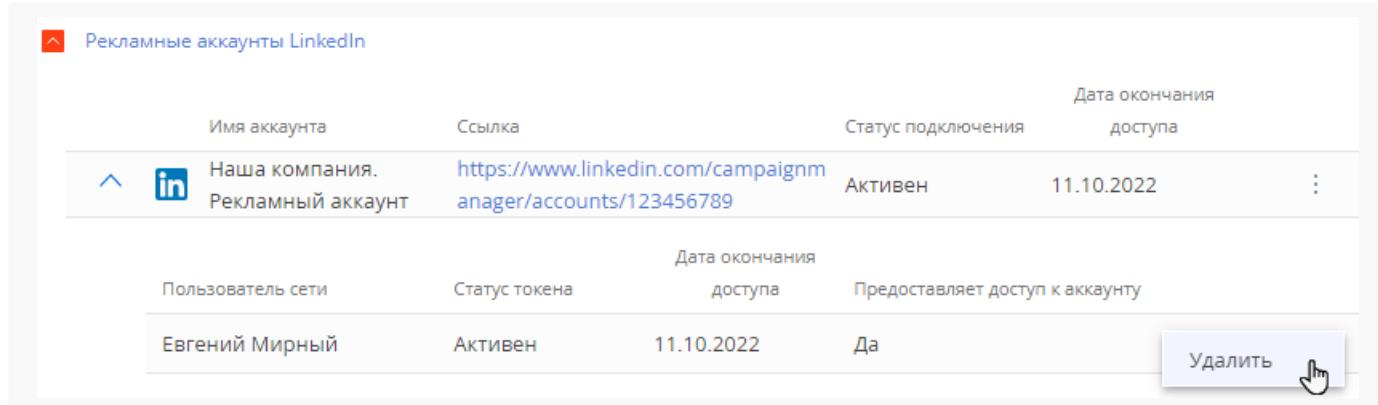
5. Нажмите кнопку [Применить], чтобы сохранить изменения.

В результате в Creatio не будут создаваться лиды, зарегистрированные через указанную форму или рекламный аккаунт. Вы можете восстановить лидогенерацию, вернув переключатели в положение “Активна”.

Отключить персональную учетную запись LinkedIn

1. Откройте дизайнер системы по кнопке .
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка сервиса лидогенерации социальных сетей”.
3. Нажмите [Настройки].
4. Нажмите кнопку  рядом с данными вашей персональной учетной записи на детали [Рекламные аккаунты LinkedIn]. В появившемся меню выберите [Удалить] и подтвердите действие (Рис. 5).

Рис. 5 — Отключить учетную запись LinkedIn



Рекламные аккаунты LinkedIn												
	Имя аккаунта	Ссылка	Статус подключения	Дата окончания доступа								
	 Наша компания. Рекламный аккаунт	https://www.linkedin.com/campaignmanager/accounts/123456789	Активен	11.10.2022								
<table border="1"> <thead> <tr> <th>Пользователь сети</th> <th>Статус токена доступа</th> <th>Дата окончания доступа</th> <th>Предоставляет доступ к аккаунту</th> </tr> </thead> <tbody> <tr> <td>Евгений Мирный</td> <td>Активен</td> <td>11.10.2022</td> <td>Да</td> </tr> </tbody> </table>					Пользователь сети	Статус токена доступа	Дата окончания доступа	Предоставляет доступ к аккаунту	Евгений Мирный	Активен	11.10.2022	Да
Пользователь сети	Статус токена доступа	Дата окончания доступа	Предоставляет доступ к аккаунту									
Евгений Мирный	Активен	11.10.2022	Да									

В результате Creatio больше не будет использовать данные этого пользователя для доступа к рекламному аккаунту. Если удаленная учетная запись была единственной, связанной с рекламным аккаунтом, то лидогенерация из LinkedIn будет прекращена.

Отключить рекламный аккаунт LinkedIn

1. Откройте дизайнер системы по кнопке .
2. В группе “Импорт и интеграции” кликните по ссылке “Настройка сервиса лидогенерации социальных сетей”.
3. Нажмите кнопку  рядом с интеграцией, которая использует аккаунт. В появившемся меню выберите [Удалить] и подтвердите действие.
4. Нажмите [Настройки].
5. Нажмите кнопку  рядом с данными вашего рекламного аккаунта на детали [Рекламные аккаунты LinkedIn]. В появившемся меню выберите [Удалить] и подтвердите действие.

В результате Creatio утратит доступ к вашему рекламному аккаунту, лидогенерация из LinkedIn будет прекращена.

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

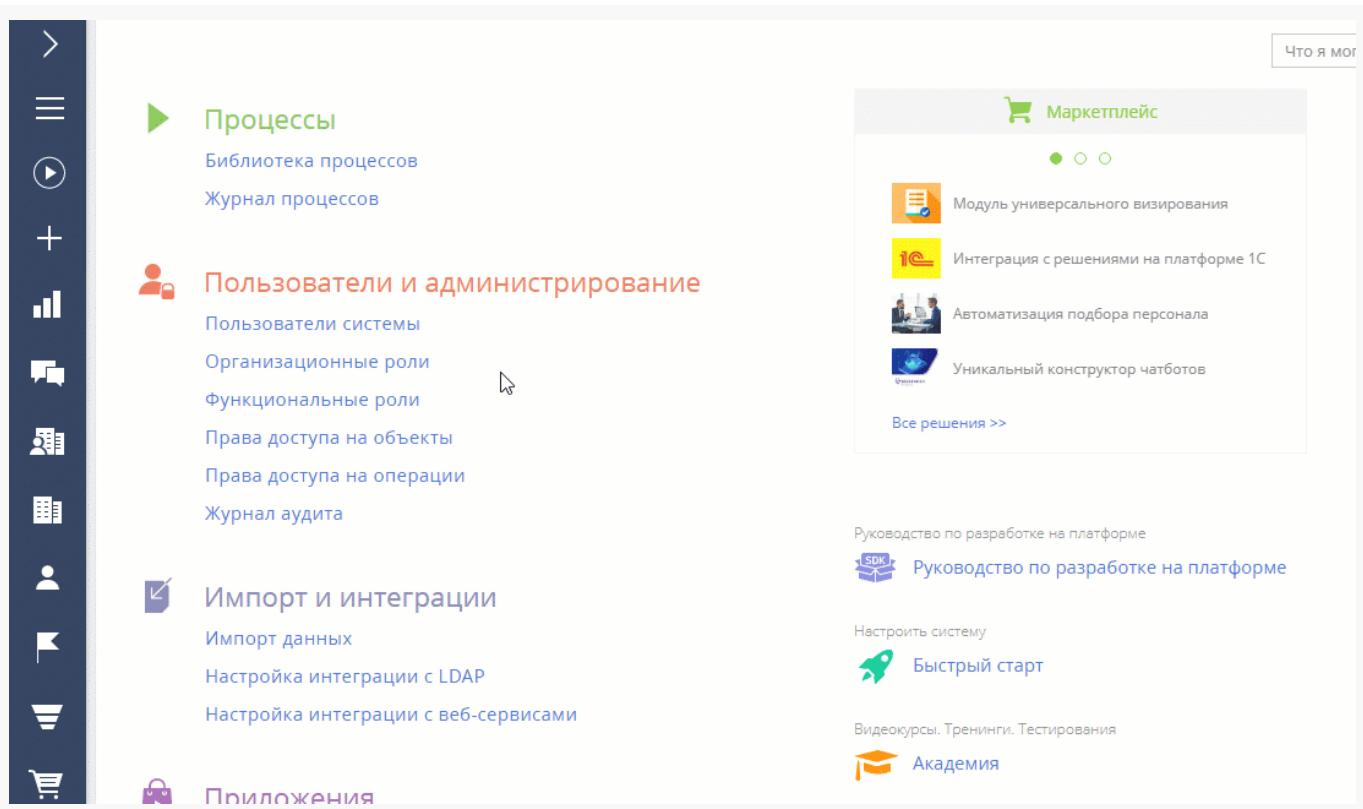
специфической функциональностью продукта, такой как разделы [*Email*] и [*Кампании*]. По умолчанию распределение лицензий между пользователями выполняют системные администраторы.

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:

- Нажмите  —> “**Пользователи системы**”.
- Откройте страницу пользователя, чьи права вы хотите делегировать.
- Откройте вкладку [**Делегирование прав**] —> кнопка [**Делегировать права**].
- В открывшемся окне выберите пользователя или группу пользователей, которые получат права, например организационная роль “Отдел продаж”.
- Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Закрыть**] на странице пользователя.
- 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

Процессы
Библиотека процессов
Журнал процессов

Пользователи и администрирование
Пользователи системы
Организационные роли
Функциональные роли
Права доступа на объекты
Права доступа на операции
Журнал аудита

Импорт и интеграции
Импорт данных
Настройка интеграции с LDAP
Настройка интеграции с веб-сервисами
Журнал отправки email-рассылок
Настройка трекинга событий сайта

Маркетплейс

- Управление файловым каталогом
- Управление анкетами и опросами в системе
- Настройка вычисляемых показателей в дашбордах
- Геймификация рабочих процессов

Все решения >>

Руководство по разработке на платформе

Настройте систему

Быстрый старт

Видеокурсы. Тренинги. Тестирования

Академия

Делегировать права пользователю от других пользователей и ролей

Чтобы передать пользователю права от других пользователей и ролей:

- Нажмите —> “**Пользователи системы**”.
- Откройте страницу пользователя, **который получит права**.
- Откройте вкладку [**Делегирование прав**] —> кнопка [**Получить права**].
- В открывшемся окне выберите пользователя или группу пользователей, **чьи права необходимо делегировать**, например организационная роль “Отдел продаж”.
- Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Закрыть**] на странице пользователя.
- 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_ulanenko@gmail.com
Ткаченко Виктория	Да	Специалист	viktoria_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

- Нажмите —> “Пользователи системы”.
- Откройте страницу пользователя, **делегированные права которого вы хотите удалить**.
- Откройте вкладку [**Делегирование прав**], **отметьте запись**, которую вам необходимо удалить.
- Нажмите —> “Удалить” ([Рис. 3](#)). **Закройте страницу пользователя**.
- 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.

Добавить сервис для подключения к online-встречам

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

В Creatio пользователи могут переходить к online-встречам из расписания задач, если на страницу активности добавлена ссылка на видеоконференцию. Подробнее: [Подключиться к online-встрече](#).

Переход выполняется для ссылок, которые соответствуют маске URL-адреса для выбранного сервиса online-встреч. В справочнике [Ссылки на онлайн сервисы встреч] содержатся маски адресов наиболее популярных сервисов:

- Microsoft Teams,
- Zoom,
- Cisco Webex,
- Join.Me,
- AnyMeeting,
- GoToMeeting,
- Google Meet.

Если в компании используется другой сервис online-встреч или корпоративный аккаунт любого из перечисленных сервисов, то сформированные им URL-адреса будут отличаться от приведенных в справочнике масок. В этом случае необходимо добавить маску адреса в справочник [Ссылки на онлайн сервисы встреч].

Пример. Необходимо добавить маску URL-адреса для корпоративной учетной записи Our Company на платформе Zoom.

1. Нажмите  в правом верхнем углу → [Справочники].
2. Откройте наполнение справочника [Ссылки на онлайн сервисы встреч].
3. Нажмите [Добавить].
4. Для новой записи укажите:
 - a. [Название] — имя сервиса. Например, “Zoom Our Company”.
 - b. [Описание] — краткое описание сервиса. Например, “Корпоративный аккаунт Zoom”.
 - c. [Мaska ссылки] — универсальная маска, в которой перечислены все обязательные компоненты, содержащиеся в каждой ссылке, сформированной сервисом. Например, (`http[s]?://(www\\.)?` `|www\\.|{1}.OurCompany?zoom.us//.+?\\b`
5. Нажмите .
6. При необходимости повторите шаги 3–5 для всех сервисов, которые необходимо добавить.

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 скрипtingа (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-sr
```

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> </system.webServer>
```

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.