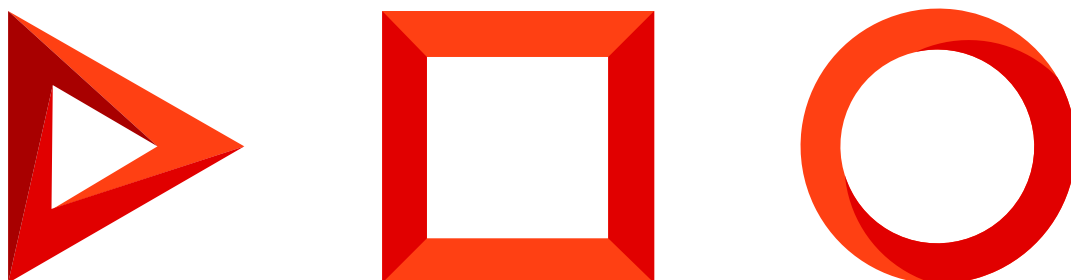


Настройка дополнительных параметров и интеграций

Версия 8.0



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

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

Содержание

Настроить интеграцию с Google	4
Настроить интеграцию с лендингами	4
Настроить уведомления о разрешении обращений	5
Настроить сервис обогащения данных	5
Настроить запуск массовых рассылок	5
Настроить интеграцию с облачным сервисом отправки рассылок Cloud Email Service (для пользователей on-site)	6
Настроить список доменов отправителя	7
Выполнить дополнительные настройки интеграции с сервисом отправки рассылок	7
Разрешить мониторинг email-рассылок в Creatio on-site	8
Настроить горизонтальное масштабирование	9
Общий порядок развертывания	9
Установить балансировщик HAProxy	12
Настроить балансировщик HAProxy	13
Настроить безопасный доступ к порталу	17
Настроить систему управления версиями для среды разработки	18
Установить SVN и создать хранилище для Creatio	19
Подключить созданное хранилище к Creatio	20
Настроить доступ к сервису чатов	23
Настроить авторизацию интегрированных приложений по протоколу OAuth 2.0	23
Установить и настроить Identity Service	23
Настроить интеграцию с Identity Service на стороне Creatio	26
Настроить авторизацию приложений по протоколу OAuth 2.0	27
Настроить интеграцию с файловым хранилищем S3	28
Шаг 1. Настроить хранилище S3	29
Шаг 2. Настроить хранение файлов	30

Настроить интеграцию с Google

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для того чтобы настроить интеграцию с сервисами Google, пользователям приложений Creatio on-site необходимо:

1. Зарегистрировать и настроить учетную запись Google.
2. Открыть доступ к Calendar API.
3. Сгенерировать ключи для интеграции ("Client ID" и "Client Secret").
4. Ввести полученные ключи в Creatio в качестве значений системных настроек.

Подробнее читайте в статье [Зарегистрировать приложение Creatio в Workspace](#).

Настроить интеграцию с лендингами

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Функциональность доступна во всех продуктах, в которых есть **раздел Лендинги и web-формы**.

Клиентам, у которых приложение Creatio развернуто on-site, может потребоваться дополнительная настройка для корректного формирования HTML-кода на странице лендинга. Настройку необходимо выполнить, если по требованиям безопасности URL, который отображается в браузере пользователя, и URL, используемый для внешнего доступа к Creatio, различаются. Например, если адрес блокируется с помощью firewall.

Для настройки:

1. Перейдите в дизайнер системы —> [*Системные настройки*].
2. В группе [*Настройки раздела Лендинги*] откройте системную настройку "**URL сервиса приема данных со страниц лендингов**".
3. В поле [*Значение по умолчанию*] введите **полный внешний адрес** вашего приложения Creatio, например, `http://creatio-marketing.mydomain.com`, и сохраните настройку.

В результате в HTML-коде, встраиваемом на вашу посадочную страницу, будет использоваться корректный адрес для вызова веб-сервиса, отвечающего за создание нового лида в Creatio, например:

```
serviceUrl: "http://mysite.creatio-marketing/ServiceModel/GeneratedWebFormService.svc/SaveWebFor
```

Если вы используете **протокол защищенного соединения**, то введите адрес с указанием `https://`, тогда адрес для вызова веб-сервиса будет следующим:

```
serviceUrl: "https://mysite.creatio-marketing/ServiceModel/GeneratedWebFormService.svc/SaveWebFc
```

На заметку. По умолчанию значение данной настройки не заполнено, путь к приложению формируется автоматически.

Настроить уведомления о разрешении обращений

ПРОДУКТЫ: **SERVICE ENTERPRISE** **CUSTOMER CENTER**

Чтобы клиент автоматически получил email-сообщение после перевода обращения в статус “Решено”:

1. Перейдите в дизайнер системы —> [*Системные настройки*].
2. Откройте системную настройку **“Адрес сайта”**.
3. В поле [*Значение по умолчанию*] введите полный адрес сайта, используемый для доступа к Creatio, например, <http://creatio.com>.
4. Примените настройки таблицы по кнопке [*Сохранить*].

Настроить сервис обогащения данных

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Для использования функциональности обогащения данных в Creatio должен быть указан ваш персональный ключ облачных сервисов, а также URL подключения к облачным сервисам Creatio. Для этого используются системные настройки:

- “Адрес сервиса обогащения контрагентов”. По умолчанию эта настройка заполнена для всех приложений.
- “API-ключ облачных сервисов Creatio”. Для приложений **cloud** по умолчанию настройка заполнена. Настройку нужно выполнить для приложений, развернутых **on-site**.

Для приложений, развернутых **on-site**, запросите персональный ключ в службе поддержки. После получения ключа:

1. Из дизайнера системы перейдите в раздел [*Системные настройки*].
2. В группе “Creatio cloud services” откройте системную настройку “API-ключ облачных сервисов Creatio”.
3. В поле [*Значение по умолчанию*] введите полученный ключ и сохраните настройку.

Теперь вы можете использовать функциональность обогащения данных.

Настроить запуск массовых рассылок

ПРОДУКТЫ: **MARKETING**

Функциональность доступна в продукте **Marketing Creatio** и в CRM-линейке продуктов Creatio.

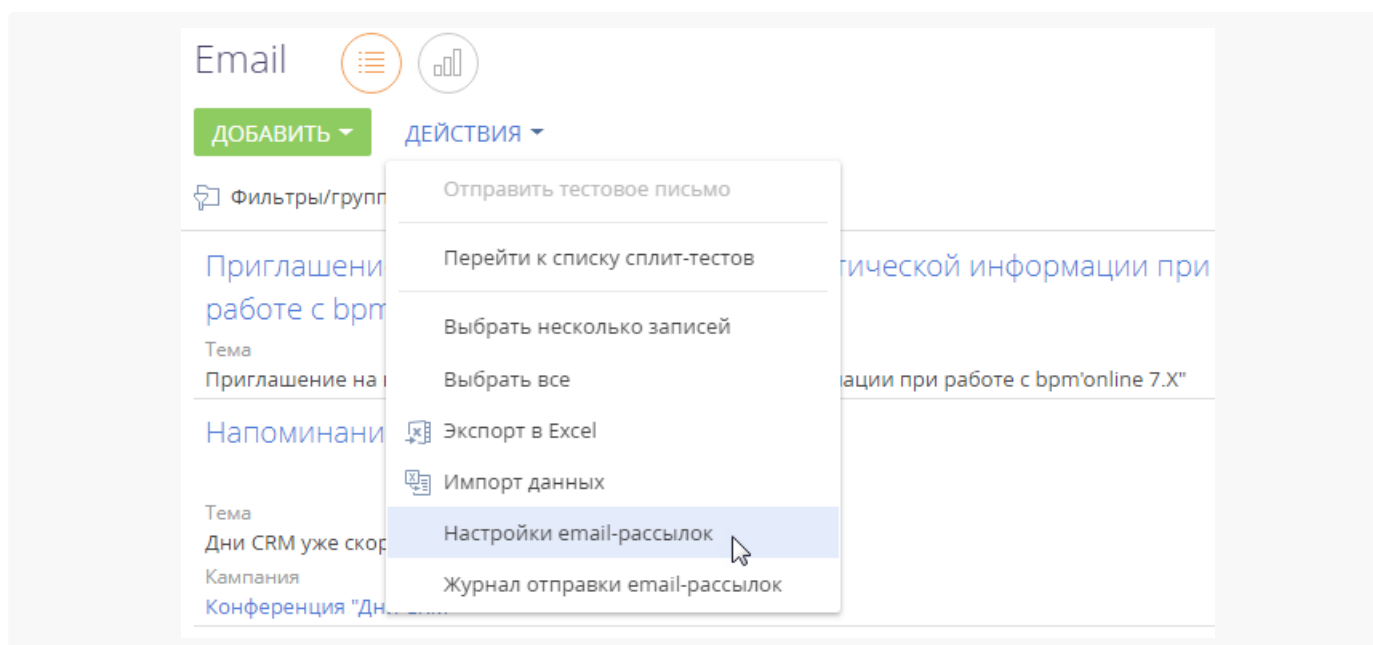
Чтобы иметь возможность запускать рассылки и отправлять по ним тестовые письма, необходимо настроить интеграцию Creatio с сервисом массовых рассылок. Для этого в разделе [*Email*] реализована страница настроек email-рассылок, с помощью которой можно внести или откорректировать общие настройки, список доменов отправителя, а также проконтролировать состояние подключения.

Настроить интеграцию с облачным сервисом отправки рассылок Cloud Email Service (для пользователей on-site)

Чтобы настроить интеграцию с облачным сервисом отправки рассылок:

1. Перейдите в раздел [*Email*]. В меню действий раздела выберите **Настройки email-рассылок** (Рис. 1).

Рис. 1 — Переход к настройкам email-рассылок



2. Заполните поля вкладки [*Общие настройки*].

Важно. Чтобы сменить провайдера сервиса email-рассылок, обратитесь в службу технической поддержки.

- a. В поле **Домен для получения откликов** укажите адрес домена вашего приложения Creatio в формате `http://www.yourdomain.com`.

Важно. POST-запросы всегда отправляются и принимаются по порту 443 вне зависимости от порта, через который доступно приложение Creatio. Мы рекомендуем проверить связь по порту 443 после завершения настроек. Для этого откройте в браузере полученный URL подключения к облачным сервисам Creatio в формате `https://url_address.com`.

В результате должна открыться пустая страница. Если страница не открывается, то необходимо проверить, корректно ли открыт порт.

- b. В поле **API-ключ** укажите персональный ключ доступа к сервису массовых рассылок.
- c. В поле **URL подключения к облачным сервисам Creatio** укажите адрес облачного сервиса рассылок в формате `https://url_address.com`.
- d. В поле **Auth ключ** укажите ключ аутентификации для получения откликов.
Для получения API-ключа и Auth-ключа, а также URL подключения к облачным сервисам рассылок после установки лицензий продукта обратитесь в службу технической поддержки.
- e. Поле **Email-провайдер** будет автоматически заполнено названием вашего провайдера сервиса email-рассылок сразу после корректного заполнения полей [*API-ключ*] и [*URL подключения к облачным сервисам Creatio*].

Настроить список доменов отправителя

Для отображения в рассылках корректного имени отправителя, а также чтобы избежать несанкционированных рассылок от вашего имени, необходимо:

- перечислить на странице настроек email-рассылок список ваших доменов;
- верифицировать каждый домен с помощью специальных текстовых SPF-, DKIM- и DMARK-записей;
- Сохраните изменения на странице системной настройки.

Для этого:


1. Добавьте список ваших доменов по кнопке  детали на вкладке [*Домены отправителя*].

На заметку. В списке отображаются все добавленные домены, включая те, которые уже не используются. Удалить домен из списка невозможно.

2. Выберите из списка домен, который необходимо верифицировать. В правой части экрана отобразится инструкция по настройке DKIM/SPF, актуальная для выбранного домена. В инструкции будут сформированы значения DKIM- и SPF-записей.

На заметку. Инструкции по настройке DKIM/SPF отличаются для разных доменов. Для того чтобы отобразилась корректная инструкция, выберите нужный домен из списка добавленных.

3. Выполните настройки верификации домена. Подробнее: [Рекомендации по настройке для популярных DNS-провайдеров](#).

В результате в поле [*Состояние подключения*] страницы настроек email-рассылок отобразится индикатор успешного подключения  и комментарий “Подключение активно”.

Выполнить дополнительные настройки интеграции с сервисом отправки рассылок

Для корректной работы функциональности рассылок **настройте один из вариантов доступа** к Creatio для сервиса рассылок (Creatio Cloud Email Service).

1. В межсетевом экране продуктового сервера настройте доступ для приема POST-запросов из Internet к домену, на котором развернуто ваше приложение: `http://www.yourdomain.com`.
2. В межсетевом экране продуктового сервера настройте доступ для приема POST-запросов из Internet к конкретному веб-сервису. Если ваше приложение развернуто по адресу `http://www.yourdomain.com`, то из Сети должен быть доступен сервис `http://www.yourdomain.com/0/ServiceModel/CESWebHooksService.svc/HandleWebHooks`.

На заметку. В Creatio нет необходимости настраивать обработку запросов отписки от рассылок и проверять возможность получения сервером приложений Creatio GET-запросов. Обработка запросов на отписку от рассылок осуществляется автоматически.

Важно. Если доступ к приложению осуществляется с использованием защищенного соединения HTTPS, то необходимо, чтобы на сервере приложений был установлен действующий сертификат. В случае изменения протокола передачи данных или адреса приложения, соответствующие изменения можно внести на странице настройки email-рассылок.

Не рекомендуется использовать “белые списки” IP-адресов для ограничения доступа к открытым портам, поскольку служба рассылок Creatio Cloud Email Service может присылать аналитическую информацию об отклике с различных IP-адресов и использовать прокси. Если в таком “белом списке” будет отсутствовать IP-адрес, с которого отправляется аналитическая информация, то эта информация будет утеряна.


Также при использовании “черных списков” рекомендуется проверить, что полученные IP-адреса не запрещены (не находятся в данном списке).

Разрешить мониторинг email-рассылок в Creatio on-site

Перед началом работы с рассылками рекомендуем настроить возможность мониторинга состояния email-рассылок для сотрудников службы поддержки. Так они смогут оперативно помочь вам восстановить отправку рассылок в случае сбоев, например, задержек или ошибок отправки. Показатели, которые будет анализировать служба поддержки, содержат только агрегированные данные по конкретной рассылке и не содержат таких данных, как персональные email-сообщения, шаблоны рассылок и т. д.

На заметку. Настройка различается для приложений, развернутых on-site и cloud. Подробнее о настройке для приложений cloud читайте в статье [Разрешить мониторинг состояния рассылок службе поддержки](#).

Для настройки:

1. Перейдите в дизайнер системы по кнопке  в правом верхнем углу приложения и откройте раздел [Системные настройки].
2. Откройте системную настройку [Включить возможность мониторинга показателей состояния email-рассылок] и на ее странице установите признак [Значение по умолчанию]. Сохраните изменения на странице системной настройки.

3. В межсетевом экране продуктового сервера настройте доступ из Internet к web-сервису

/0/ServiceModel/CESTroubleshootingService.svc/emailstate.

Например, если ваше приложение развернуто по адресу <http://www.yourdomain.com>, то из сети должен быть доступен web-сервис:

<http://www.yourdomain.com/0/ServiceModel/CESTroubleshootingService.svc/emailstate>.

В результате выполненных настроек сотрудники службы поддержки смогут оперативно определять и устранять возможные сбои и восстановить работу ваших рассылок.

Настроить горизонтальное масштабирование

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

В Creatio существует возможность повысить производительность крупных проектов (до нескольких тысяч пользователей) за счет горизонтального масштабирования — увеличения количества серверов, на которых развернуто приложение, и распределения нагрузки между ними.

Балансировщик может быть аппаратным или программным. Для работы в отказоустойчивом режиме используется балансировщик HTTP/HTTPS-трафика с поддержкой протокола WebSocket. Работа приложения тестировалась на программном балансировщике нагрузки HAProxy. Известны случаи успешного использования других балансировщиков Citrix, Cisco, NginX, FortiGate, MS ARR.

На заметку. Установка дополнений Marketplace и пользовательских доработок на среду с балансировщиком отличается от обычного процесса поставки. Подробнее: [Установить приложение Marketplace](#).

Данный документ рассматривает вариант горизонтального масштабирования Creatio с использованием бесплатного open-source балансировщика HAProxy для распределения нагрузки на серверы сессий.

На заметку. Серверное время на нодах (серверах и машинах), на которых развернуты экземпляры приложения Creatio, должно быть синхронизировано во избежание проблем с работоспособностью системы.

Общий порядок развертывания

Для приложений на .NET Framework

Общий порядок развертывания приложения Creatio с горизонтальным масштабированием на **.NET Framework** следующий:

1. Разверните необходимое количество экземпляров приложения Creatio в web-ферме.

На заметку. Рекомендуется, чтобы у всех экземпляров приложения имена в IIS и настройки Application pool совпадали.

- В файле ConnectionStrings.config для всех экземпляров укажите одинаковые базы данных SQL и Redis.

```
<add name="redis" connectionString="host=DOMAIN.COM;db=0;port=6379;maxReadPoolSize=10;maxWrit
<add name="db" connectionString="Data Source=DOMAIN.COM;Initial Catalog=DatabaseName;Integrat
```

- В конфигурационном файле (Web.config) каждого приложения, в блоке <appSettings> добавьте ключ:

```
<add key="TenantId" value="1" />
```

Номер "value" должен быть одинаковым у всех экземпляров приложения в web-ферме.

Важно. Начиная с версии 7.14.1 ключ <add key="TenantId" value="..." /> нужно добавить только во внутренний конфигурационный файл Web.config (путь к файлу Terrasoft.WebApp\Web.config). Добавление ключа во внешний конфигурационный файл может привести к ошибкам в работе приложения.

- Сгенерируйте для одного из экземпляров приложения уникальное значение machineKey. Подробно об этом читайте в статье [Настроить Web.config](#). Полученное значение скопируйте и укажите для каждого экземпляра приложения в конфигурационных файлах Web.config, которые находятся в корневой папке Creatio и в папке Terrasoft.WebApp.
- Во внешнем конфигурационном файле (Web.config) каждой ноды для всех планировщиков в блоке <quartzConfig> включите кластерный режим:

```
<add key="quartz.jobStore.clustered" value="true" />
<add key="quartz.jobStore.acquireTriggersWithinLock" value="true" />
```

- В случае совпадения настроек instanceId сформируйте уникальные значения для каждой ноды планировщиков.

Способы формирования уникальных instanceId:

- Во внешнем конфигурационном файле (Web.config) каждой ноды для всех планировщиков в блоке <quartzConfig> добавьте строку

```
<add key="quartz.scheduler.instanceId" value="AUTO" />
```

Важно. Для значения AUTO атрибута value необходимо использовать верхний регистр. В другом случае значение будет расцениваться как имя ноды и при работе планировщика могут возникать ошибки.

В результате планировщик автоматически будет генерировать уникальное имя ноды в формате <имя ноды>+timestamp.

- Вручную добавьте уникальные значения quartz.scheduler.instanceId.

7. Для атрибута value настройки quartz.jobStore.clustered установите значение true.

```
<add key="quartz.jobStore.clustered" value="true" />
```

8. Раздайте права на созданные директории приложений пользователю IUSR и пользователю, под которым запущен Application pool в IIS.
9. Настройте балансировщик (например, HAProxy) для распределения нагрузки между развернутыми серверами приложения.
10. При необходимости настройте балансировку нагрузки для серверов баз данных и сессий.

На заметку. Информация о настройке кластеризации доступна в документации [MSSQL](#) и [Oracle](#). Настройка отказоустойчивости системы при помощи Redis Cluster рассмотрена в статье [Настроить Redis Cluster](#).

Для приложений на .NET Core

Общий порядок развертывания приложения Creatio с горизонтальным масштабированием на **.NET Core** следующий:

1. Разверните необходимое количество [экземпляров приложения Creatio](#).
2. В [файле ConnectionStrings.config](#) для всех экземпляров укажите одинаковые базы данных SQL и Redis для всех экземпляров приложения.
3. Перейдите в корневую папку любого из экземпляров приложения и найдите файл Terrasoft.WebHost.dll.
4. Запустите команду:

```
dotnet Terrasoft.WebHost.dll configureWebFarmMode
```

В результате конфигурационные файлы данного экземпляра приложения обновятся.

5. Во внешнем конфигурационном файле (Terrasoft.WebHost.dll) каждой ноды для всех планировщиков в блоке <quartzConfig> включите кластерный режим:

```
<add key="quartz.jobStore.clustered" value="true" />
<add key="quartz.jobStore.acquireTriggersWithinLock" value="true" />
```

6. В случае совпадения настроек instanceId сформируйте уникальные значения для каждой ноды планировщиков.

Способы формирования уникальных instanceId:

- Во внешнем конфигурационном файле (Terrasoft.WebHost.dll) каждой ноды для всех планировщиков в блоке <quartzConfig> добавьте строку

```
<add key="quartz.scheduler.instanceId" value="AUTO" />
```

Важно. Для значения AUTO атрибута value необходимо использовать верхний регистр. В другом случае значение будет расцениваться как имя ноды и при работе планировщика могут возникать ошибки.

В результате планировщик автоматически будет генерировать уникальное имя ноды в формате <имя ноды>+timestamp.

- Вручную добавьте уникальные значения quartz.scheduler.instanceId.

7. Для атрибута value настройки quartz.jobStore.clustered установите значение true.

```
<add key="quartz.jobStore.clustered" value="true" />
```

8. При необходимости настройте балансировку нагрузки для серверов баз данных и сессий.
9. Скопируйте все обновленные конфигурационные файлы в корневые папки других экземпляров приложения.
10. Настройте балансировщик (например, HAProxy) для распределения нагрузки между развернутыми серверами приложения.

На заметку. Подробная информация о создании и настройке кластеров содержится в документации СУБД. Настройка отказоустойчивости системы при помощи Redis Cluster рассмотрена в статье [Настроить Redis Cluster](#).

Установить балансировщик HAProxy

Балансировщик нагрузки HAProxy поддерживает ряд бесплатных open-source ОС. В данном документе мы рассмотрим один из наиболее простых способов развертывания HAProxy на ОС Debian при помощи сервиса haproxy.debian.net.

1. Откройте страницу сервиса установки, перейдя по ссылке <https://haproxy.debian.net/>.
2. Выберите ОС и ее версию, а также версию HAProxy.

На заметку. Чтобы узнать установленную версию Debian, воспользуйтесь командой cat /etc/issue.

В результате сервис сгенерирует набор команд, которые необходимо выполнить в ОС Debian для установки HAProxy.

Рис. 1 — Пример команд установки HAProxy, сгенерированных сервисом haproxy.debian.net

Instructions for latest release

First, you need to enable the [backports repository](#):

```
# echo deb http://httpredir.debian.org/debian jessie-backports main | \
tee /etc/apt/sources.list.d/backports.list
```

Then, you need to enable a dedicated repository:

```
# curl https://haproxy.debian.net/bernat.debian.org.gpg | \
apt-key add -
# echo deb http://haproxy.debian.net jessie-backports-1.8 main | \
tee /etc/apt/sources.list.d/haproxy.list
```

Then, use the following commands:

```
# apt-get update
# apt-get install haproxy -t jessie-backports\*
```

3. Выполните сгенерированные команды одну за другой.

Настроить балансировщик HAProxy

Для настройки HAProxy необходимо внести изменения в файл `haproxy.cfg`. Файл находится по следующему пути:

```
.../etc/haproxy/haproxy.cfg
```

Основные (минимальные) настройки

Минимальные настройки, необходимые для работы HAProxy, состоят в добавлении в файл двух секций: **frontend** и **backend**.

Секция frontend

В секцию frontend необходимо добавить 2 настройки: **bind** и **default_backend**:

- В настройке **bind** укажите адрес и порт, на который будут поступать запросы, распределение

которых будет производить HAProxy.

- В опции **default_backend** укажите имя, которое будет указано для секции backend.

В результате настройка будет выглядеть следующим образом:

```
frontend front
maxconn 10000
#Using these ports for binding
bind *:80
bind *:443
#Convert cookies to be secure
rspirep ^(set-cookie:.* ) \1;\ Secure
default_backend creatio
```

Секция backend

В секцию backend необходимо добавить как минимум 2 обязательные настройки:

- В параметре **balance** укажите тип балансировки, например **roundrobin**. Информация о различных типах балансировки доступна в [документации HAProxy](#).
- При помощи параметра **server** укажите все серверы (или “nodes”), между которыми должна распределяться нагрузка.

Для каждого сервера (развернутого экземпляра приложения Creatio) необходимо добавить отдельный параметр server с указанием адреса сервера, порта и веса. Вес позволяет балансировщику распределять нагрузку на основании физических возможностей серверов. Чем больший вес указан для сервера, тем больше запросов он будет получать. Например, если необходимо распределить нагрузку между двумя серверами Creatio, добавьте в backend 2 параметра server:

```
server node_1 [server address]:[port] weight
server node_2 [server address]:[port] weight
```

В результате настройка будет выглядеть следующим образом:

```
backend creatio
#set balance type
balance roundrobin

server node_1 nodeserver1:80 check inter 10000 weight 2
server node_2 nodeserver2:80/sitename check inter 10000 weight 1
```

Новые настройки вступят в силу после перезапуска HAProxy. Используйте следующую команду для перезапуска HAProxy:

```
service haproxy restart
```

Проверить состояние сервера

С точки зрения балансировщика HAProxy у сервера может быть несколько состояний:

Состояние	Описание
UP	Сервер работает.
UP - transitionally DOWN	Сервер в настоящий момент считается работоспособным, но последняя проверка не удалась. Следовательно, сервер переходит в состояние DOWN.
DOWN - transitionally UP	В настоящее время сервер считается неработоспособным, но последняя проверка прошла успешно. Следовательно, сервер переходит в состояние UP.
DOWN	Сервер не работает.

Изменения рабочего состояния инициируются параметрами проверки работоспособности (health check). Для самой простой проверки работоспособности необходимо ключевое слово `check` в строке настройки `server`. Для запуска проверки работоспособности требуется как минимум IP-адрес и порт TCP от сервера. Пример проверки:

```
server node1 ... check
option httpchk GET /Login/NuiLogin.aspx
option httpchk GET /0/ping
```

Настроить веб-статистику (опционально)

Чтобы включить веб-статистику, добавьте новую секцию `listen` со следующими параметрами: **bind**, **mode http**, **stats enable**, **stats uri**. Секция выглядит следующим образом:

```
listen stats # Define a listen section called "stats"
  bind :9000 # Listen on localhost:9000
  mode http
  stats enable # Enable stats page
  stats uri /haproxy_stats # Stats URI
```

В результате веб-статистика балансировки нагрузки Creatio будет доступна для просмотра в браузере.



При работе веб-фермы запросы пользователей приходят на веб-серверы через балансировщик и/или прокси-сервер. В этом случае по умолчанию в [журнале аудита](#) будет отображаться адрес последнего из прокси-серверов, через которые прошел запрос пользователя, а не его IP-адрес.

1. Настройте балансировщик таким образом, чтобы каждому запросу, который он перенаправляет на один из экземпляров приложения, был установлен заголовок, имя которого соответствует "ForwardedForHeaderName", а значение — IP-адресу клиента.

- a. Откройте файл `appsettings.json`, который находится в корневой папке приложения.

- b. Отредактируйте блок "ForwardedHeaders":

Где:

"Enable" — включение функции обработки Forwarded headers в веб-приложении;

"ForwardedForHeaderName" — имя заголовка, из которого будет получен IP-адрес;

"KnownProxiesIP" — список доверенных IP-адресов, при получении запроса от которых будет происходить обработка значения **"ForwardedHeader"**. Например, это может быть адрес

балансировщика, reverse proxy и т. д. Если это значение не заполнено, то обработка ForwardedHeader будет выполняться для всех IP-адресов, с которых приходят запросы.

с. Повторите шаги а-б для всех экземпляров приложения, которые входят в веб-ферму.

Пример

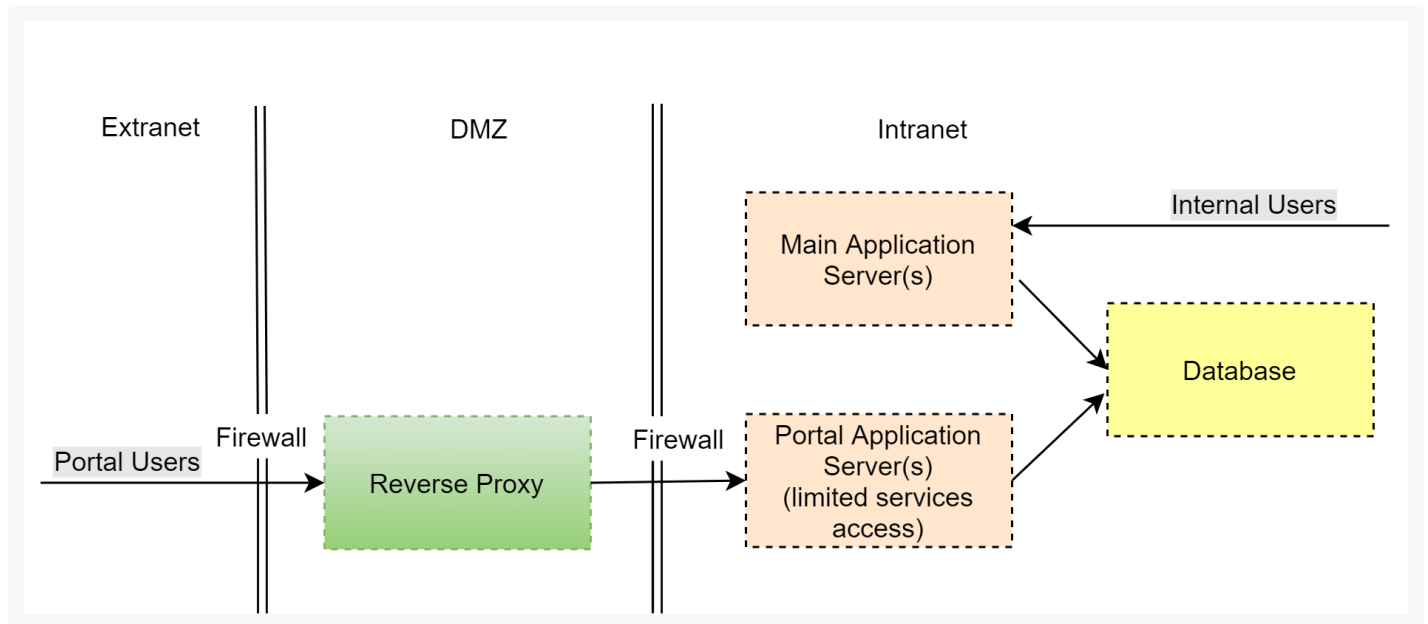
```
"KnownProxiesIP": ["127.0.0.1", "12.34.56.78", "2001:0db8:85a3:0000:0000:8a2e:0370:7334"]
```

Настроить безопасный доступ к portalу

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Для обеспечения безопасности данных при установке портала on-site приложение должно быть развернуто в режиме веб-фермы. Подробно пример настройки веб-фермы рассмотрен в статье [“Настроить горизонтальное масштабирование”](#). Доступ к portalу настраивается по схеме (Рис. 1):

Рис. 1 — Типовая схема установки системы с доступом к portalу из внешней сети



Демилитаризованная зона (DMZ)

- В демилитаризованной зоне публикуется только обратный прокси-сервер (reverse proxy).
- На уровне reverse proxy выполняется первичный мониторинг сетевой активности. Также здесь настраивается ограничение на доступ к конфигурационным веб-сервисам приложения.
- Авторизованные пользователи портала имеют доступ только к тем конфигурационным веб-сервисам, к которым он явно разрешен на уровне приложения.
- При разработке проектного решения выполняются настройки доступа для новых веб-сервисов. Подробно эта настройка описана в документации по разработке, статья [“Ограничение доступа к веб-сервисам для пользователей портала”](#).

Внутренняя сеть (Intranet)

- Для обслуживания пользователей портала в веб-ферме выделяется отдельный набор узлов приложений, который не пересекается с узлами приложений для обслуживания внутренних пользователей.
- Для работы приложения портала и приложения пользователей создаются отдельные учетные записи в базе данных с различным набором прав доступа.
- В настройках приложений портала блокируется возможность входа для пользователей системы (отключаются AuthProviders, кроме пользователей портала). Это необходимо, чтобы из внешней сети (Extranet) можно было создать сессии только пользователям портала.
- Дополнительно можно настроить использование внешних провайдеров идентификации для добавления второго шага проверки при авторизации.
- Узлы приложений портала, СУБД и приложения для пользователей размещаются в отдельных сегментах с ограниченным доступом.

Настроить систему управления версиями для среды разработки

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Управление версиями необходимо при развертывании среды разработки, чтобы при командной работе все участники могли вносить, отслеживать и объединять изменения, выполненные в конфигурации Creatio. Система управления версиями в Creatio выполняет следующие функции:

- перенос изменений между конфигурациями;
- хранение различных версий конфигурационных схем;
- отмена изменений возвращением к одной из предыдущих версий.

Creatio поддерживает интеграцию с системой контроля версий Subversion (SVN) 1.7 и выше. Подробнее об использовании SVN читайте в [документации продукта](#).

На заметку. Встроенные инструменты разработки Creatio совместимы только с системой контроля версий Subversion. Однако вы можете отключить интеграцию с SVN и использовать любую систему контроля версий, включая Git, в режиме разработки файловой системе. Подробнее о работе с Git читайте в статье “Особенности работы с Git” документации по разработке.

Хранилище SVN должно быть единственной точкой соприкосновения для различных сред разработки. В противном случае среда разработки каждого сотрудника должна быть изолирована и работать на независимом сервере приложений, подключенном к базе данных, которая не используется другими экземплярами приложений Creatio.

Подробнее о настройке среды разработки читайте в статье “[Организация среды разработки](#)” документации по разработке.

В общем случае для настройки и подключения SVN вам необходимо:

- [Установить SVN и создать хранилище для Creatio](#)
- [Подключить созданное хранилище к Creatio](#)

Установить SVN и создать хранилище для Creatio

Для установки системы контроля версий:

1. Установить сервер SVN

Вы можете установить систему контроля версий на сервере приложения, сервере баз данных или на отдельном сервере.

Чтобы развернуть сервер SVN на операционной системе Windows, воспользуйтесь одним из общедоступных установщиков:

- [VisualSVN](#)
- [CollabNet](#)

Инструкции по развертыванию SVN на других операционных системах, включая Debian, доступны с [Apache Subversion](#).

Сервер SVN может работать независимо или использовать веб-сервер Apache в качестве внешнего интерфейса (утилиты VisualSVN и CollabNet могут установить его как компонент).

Если сервер SVN работает независимо, то доступ к хранилищам предоставляется по протоколу **SVN**. Если в качестве внешнего интерфейса используется веб-сервер, то доступ к хранилищам предоставляется через протоколы **HTTP** и **HTTPS**.

Рекомендуем для интеграции с Creatio установить веб-сервер в качестве внешнего интерфейса и использовать протоколы **HTTP** и **HTTPS**.

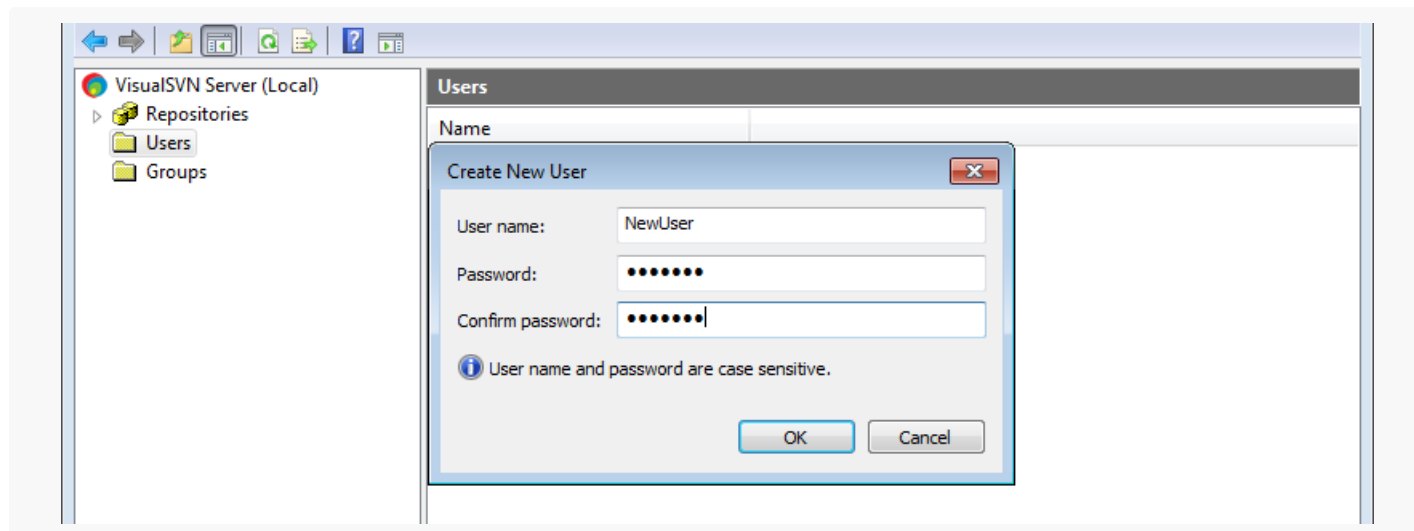
2. Создать пользователя сервера SVN

Для доступа к серверу SVN вам необходимо создать как минимум одного пользователя. Рекомендуется создавать отдельных пользователей для каждого из разработчиков, которые будут работать с системой контроля версий.

Для создания пользователя сервера SVN вы можете воспользоваться стандартными инструментами SVN, которые входят в установочный пакет, например VisualSVN ([Рис. 1](#)).

Для работы с хранилищами Creatio требуется использовать аутентификацию пользователей через логин и пароль.

Рис. 1 — Создание пользователя сервера SVN при помощи утилиты VisualSVN



3. Создать хранилище на сервере SVN

Создайте хранилище SVN при помощи стандартных инструментов, которые входят в установочный пакет сервера SVN, например, VisualSVN и CollabNet.

На заметку. Creatio поддерживает одновременную работу нескольких хранилищ, которые могут быть расположены на разных серверах SVN.

4. Установить клиент SVN (опционально)

При желании вы можете установить на рабочем месте разработчика клиент SVN, например, [TortoiseSVN](#).

На заметку. Рекомендуется использование клиента TortoiseSVN версии 1.8 и выше.

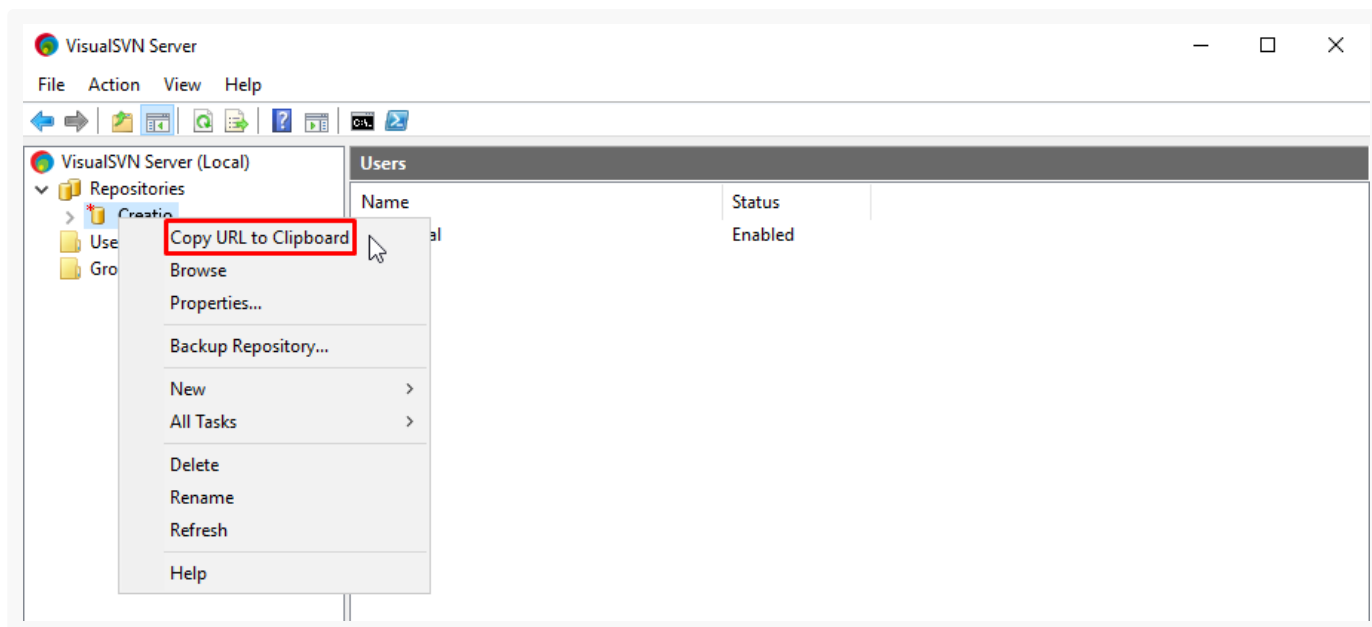
Установка клиента SVN не является обязательной, так как это не влияет на работу Creatio. Клиент SVN удобен для просмотра локальной рабочей копии, истории, возврата к предыдущим версиям, пересмотров и т. д.

Подключить созданное хранилище к Creatio

Для подключения хранилища к Creatio:

1. Скопируйте URL-адрес вашего хранилища. Например, в VisualSVN для этого нужно кликнуть правой кнопкой мыши по хранилищу и в контекстном меню выбрать команду [*Copy URL to clipboard*] (Скопировать URL в буфер обмена) ([Рис. 1](#)).

Рис. 1 — Копирование URL-адреса хранилища




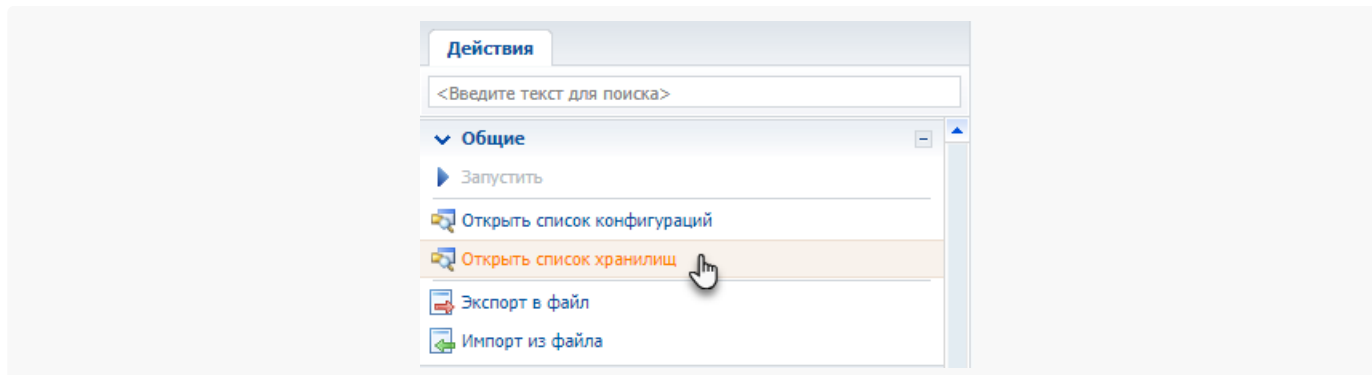
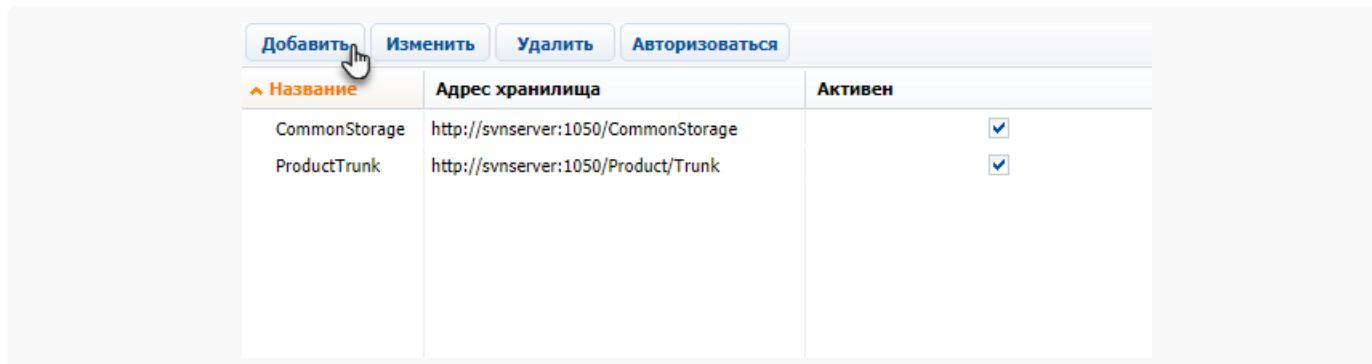
2. По кнопке  в основном приложении Creatio перейдите в дизайнер системы,
3. В группе [*Конфигурирование разработчиком*] перейдите в раздел [*Управление конфигурацией*].
4. На панели действий нажмите [*Открыть список хранилищ*] ([Рис. 2](#)).

Рис. 2 — Открытие списка хранилищ SVN



5. Нажмите кнопку [*Добавить*] ([Рис. 3](#)). Откроется страница свойств нового хранилища.

Рис. 3 — Добавление нового хранилища к списку хранилищ системы контроля версий



6. На открывшейся странице укажите свойства нового хранилища ([Рис. 4](#)):

- a. [*Название*] — название хранилища, которое отобразится в реестре подключенных хранилищ.
- b. [*Адрес хранилища*] — сетевой адрес существующего хранилища SVN. Укажите адрес, который вы скопировали на шаге 1.
- c. Протокол HTTP (стандартный сетевой протокол), протокол HTTPS (стандартный сетевой протокол, защищенный шифрованием SSL) и протокол SVN (собственный сетевой протокол системы Subversion) поддерживаются при адресации хранилища.
- d. [*Активен*] — установите этот признак, чтобы разрешить использование хранилища в системных операциях. Для каждого нового хранилища данный признак по умолчанию установлен.

На заметку. Вы можете работать только с активными хранилищами. Также все хранилища, из которых планируется обновлять пакеты, должны быть активны. К ним относятся хранилище, из которого обновляется исходный пакет, и хранилища, из которых обновляются все пакеты зависимости исходного пакета.

Рис. 4 — Заполнение свойств нового хранилища

7. Выберите добавленное хранилище в списке и нажмите кнопку [*Авторизоваться*] ([Рис. 5](#)).

Рис. 5 — Аутентификация хранилища

Название	Адрес хранилища	Активен
CommonStorage	http://svnserver:1050/CommonStorage	<input checked="" type="checkbox"/>
CustomStorage	http://svnserver:1050/CustomStorage	<input checked="" type="checkbox"/>
ProductTrunk	http://svnserver:1050/Product/Trunk	<input checked="" type="checkbox"/>

8. Подключитесь к хранилищу, используя учетные данные одного из созданных пользователей сервера SVN ([Рис. 6](#)).

Рис. 6 — Ввод учетных данных пользователя сервера SVN

В результате ваше хранилище SVN будет подключено к Creatio. Используйте новое хранилище для создания пользовательских пакетов и установки созданных пакетов в рабочее пространство.

Подробнее о [работе с пакетами при помощи SVN](#), [переносе изменений через SVN](#) и [работе с SVN](#) читайте в документации по разработке Creatio.

Настроить доступ к сервису чатов

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Для работы с каналами чатов Facebook Messenger и WhatsApp в приложениях, развернутых on-site, необходимо:

- Перевести Creatio с http на https. Подробно эта настройка описана в статье [Перевести Creatio с HTTP на HTTPS](#).
- Настроить на сервере приложения доступ к сервису чатов по адресу <https://sm-account.creatio.com/>.
- Настроить на сервере приложения для сервиса чатов sm-account.creatio.com возможность входящего подключения по протоколу https и защиту валидным сертификатом.

Для работы с каналами чатов Telegram сервер приложений должен иметь доступ в Интернет.

Для приложений Creatio, использующих двухэтапную аутентификацию, необходимо настроить доступ на входящие запросы из внешних сетей для сервисов FacebookOmnichannelMessagingService, TelegramOmnichannelMessagingService, WhatsappOmnichannelMessagingService.

Настроить авторизацию интегрированных приложений по протоколу OAuth 2.0

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

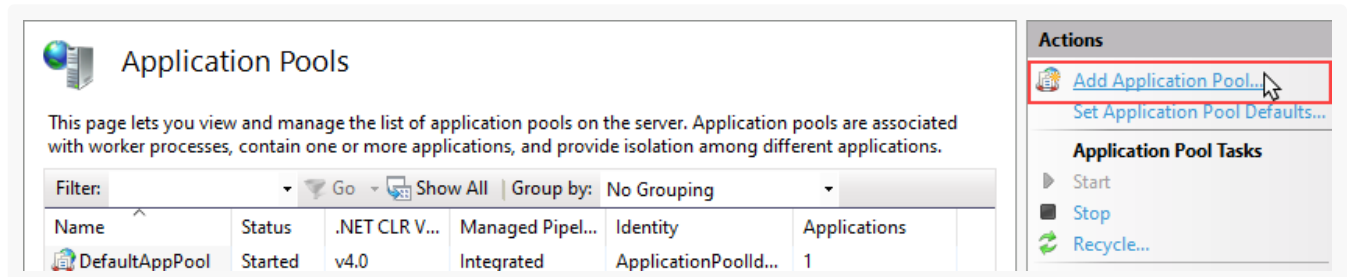
Вы можете настроить для приложений и веб-сервисов, интегрированных с Creatio, безопасную авторизацию по протоколу OAuth 2.0. Эта технология позволяет не передавать сторонним приложениям логин и пароль Creatio, а также ограничить права внешних приложений на действия в Creatio.

Установить и настроить Identity Service

Установка и настройка Identity Service выполняется после развертывания сервера базы данных и сервера приложения Creatio. Чтобы установить Identity Service:

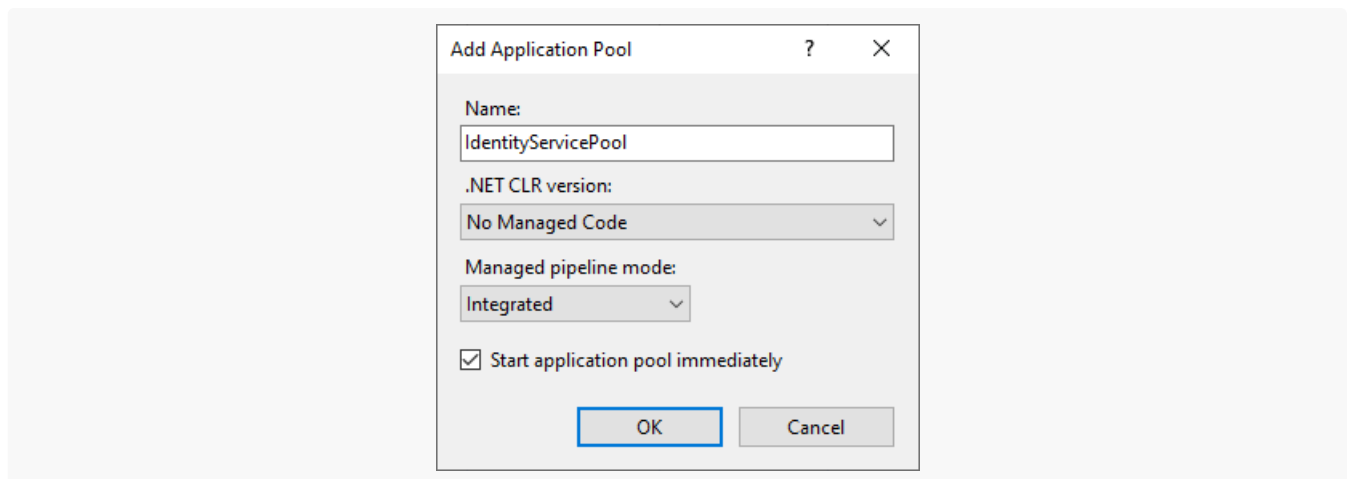
1. Перейдите на сервер приложения.
2. Установите .NET Core runtime 2.2. [Скачать установочный файл](#)
3. Установить .NET Core Hosting Bundle. [Скачать установочный файл](#)
4. Перезапустите IIS.
5. В папке с установочными файлами Creatio найдите архив **IdentityService.zip** и распакуйте его.
6. Добавьте в IIS новый **пул** приложения для Identity Service.
 - a. В области [*Connections*] окна управления IIS перейдите в секцию [*Applications Pools*].
 - b. В области [*Actions*] выберите действие [*Add Application Pool...*].

Рис 1. — Добавление пула в IIS



- c. В окне настройки пула укажите его название, например, "IdentityServicePool". В поле [*.NET CLR Version*] укажите значение "No Managed Code".

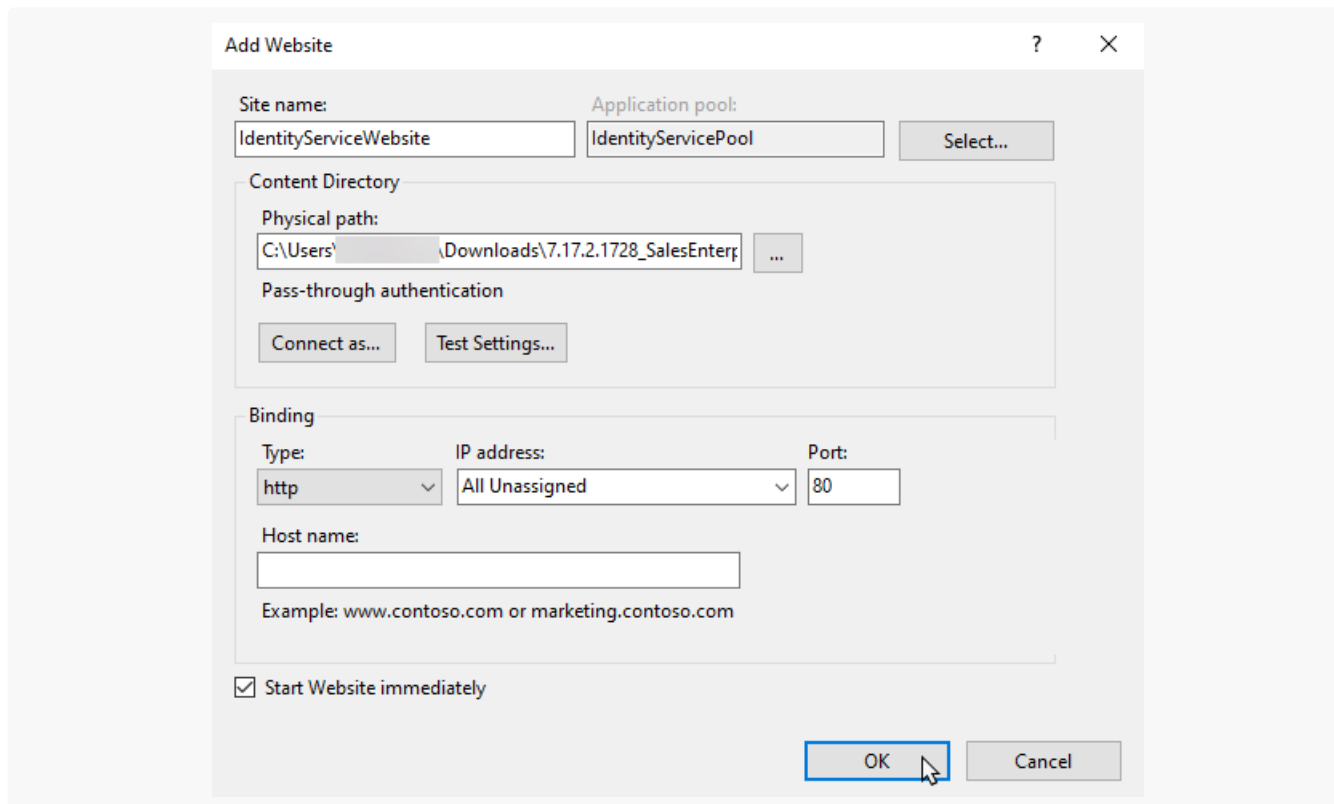
Рис. 2 — Пример настройки пула Identity Service



7. Настройте **доступ** к пулу приложения:
 - a. Кликните правой кнопкой мыши по созданному пулу. В контекстном меню выберите [*Advanced Settings...*].
 - b. В открывшемся окне в поле [*Identity*] укажите пользователя для подключения к Identity Service с правом доступа к папке приложения.
8. Создайте в IIS новый **сайт** для Identity Service.

- a. В окне управления IIS щелкните правой клавишей мыши по [Sites] и выберите [Add Website] в контекстном меню.
- b. Укажите название сайта, пул и путь к корневому каталогу с файлами Identity Service.

Рис. 3 — Пример настройки сайта в IIS



9. Настройте сайт на работу с **СУБД** вашего приложения Creatio. Для этого в конфигурационном файле **appSettings.json**, который находится в корневом каталоге Identity Service:
 - a. В параметре "DbProvider" укажите "MsSqlServer" или "Postgres".
 - b. В настройке MsSqlConnection или PostgresConnection укажите строку соединения. Рекомендуется задавать то же значение строки, что и в основном приложении Creatio. При этом важно, чтобы у пользователя, под которым выполняется подключение к БД, были права на создание и редактирование таблиц.

На заметку. Для подключения Identity Service к приложениям, которые работают с СУБД Oracle, необходимо развернуть дополнительный экземпляр БД на PostgreSQL или Microsoft SQL.

10. Настройте **системного пользователя** Identity Service. Для этого придумайте уникальные значения ClientId, ClientName, ClientSecret и укажите их в блоке "Clients" конфигурационного файла **appSettings.json**, который находится в корневом каталоге Identity Service. Эти значения будут использоваться для настройки взаимодействия между Identity Service и Creatio. Для всех значений можно использовать большие и маленькие буквы, цифры, специальные символы, например, скобки или знаки препинания.

Рекомендуемые параметры:

- ClientId — 16 символов;
- ClientSecret — 32 символа;
- ClientName — произвольное количество символов.

Пример настройки блока “Clients”

```
"[{"ClientId": "{сгенерировать ClientId}", "ClientName": "{сгенерировать имя}", "Secrets"
```

На заметку. Во избежание ошибок при запуске Identity Service в файле appsettings.json в настройке “**X509CertificatePath**” необходимо указать полный путь к файлу openssl.pfx, который находится в корневом каталоге папки с Identity Service.

11. Переведите Identity Service на работу по протоколу **HTTPS**. Настройки аналогичны тем, которые необходимо выполнить для приложения Creatio. Подробнее: [Перевести Creatio с HTTP на HTTPS](#).

12. Включите **логирование** работы Identity Service.

- В файле web.config, который находится в папке приложения Identity Service, для параметра “stdoutLogEnabled” установить значение “true”.
- В том же файле для параметра “stdoutLogFile” укажите путь к папке, где будут храниться логи приложения.
- Настройте уровень логирования в appsettings.json, который находится в корневом каталоге Identity Service:

```
"Logging": {
  "LogLevel": {
    "Default": "Error"
  }
}
```

Настроить интеграцию с Identity Service на стороне Creatio

1. **Включите** функциональность интеграции с приложением по протоколу OAuth 2.0. Для этого выполните для базы данных вашего приложения приведенный ниже скрипт. Он универсален и может использоваться для Microsoft SQL и PostgreSQL.

```
UPDATE "AdminUnitFeatureState"
```

```

SET "FeatureState" = 1

WHERE "FeatureId" = (

    SELECT

        "Id"

    FROM "Feature"

    WHERE "Code" = 'OAuth20Integration')

```


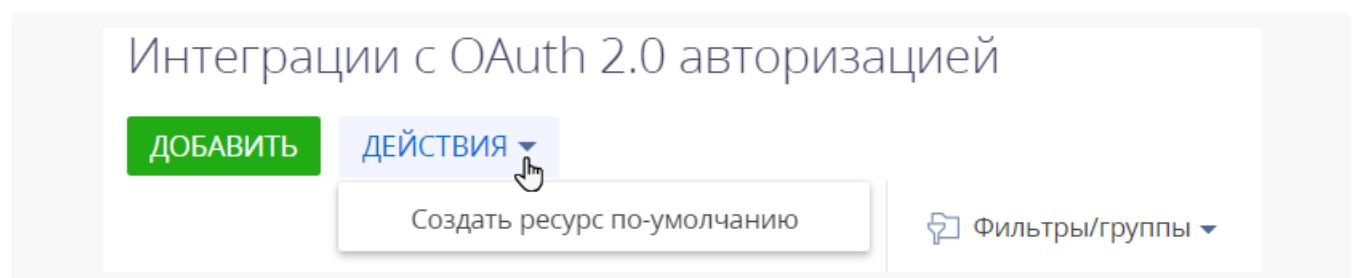
2. Заполните [системные настройки](#), которые входят в группу “OAuth 2.0”:
 - a. **“Адрес сервера авторизации для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerUrl”) — адрес IdentityServer, например, <http://isEndpointExample>.
 - b. **“Идентификатор приложения для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerClientId”) — идентификатор системного пользователя, указанный в параметре “ClientId” файла appSettings.json при настройке IdentityServer.
 - c. **“Секрет клиента для интеграций по OAuth 2.0”** (код “OAuth20IdentityServerClientSecret”) — секретный ключ системного пользователя, указанный в параметре “ClientSecret” файла appSettings.json при настройке IdentityServer.
3. Создайте ресурс приложения по умолчанию. Это действие выполняется один раз при настройке интеграции Identity Service с Creatio.
 - a. Откройте дизайнер системы по кнопке .
 - b. Перейдите в раздел [*Интеграции с OAuth 2.0 авторизацией*].
 - c. В меню действий выберите [*Создать ресурс по умолчанию*].

Рис. 4 — Создание ресурса по умолчанию




В результате в приложении будет создана запись ресурса по умолчанию с учетными данными вашего Identity Service.

Настроить авторизацию приложений по протоколу OAuth 2.0

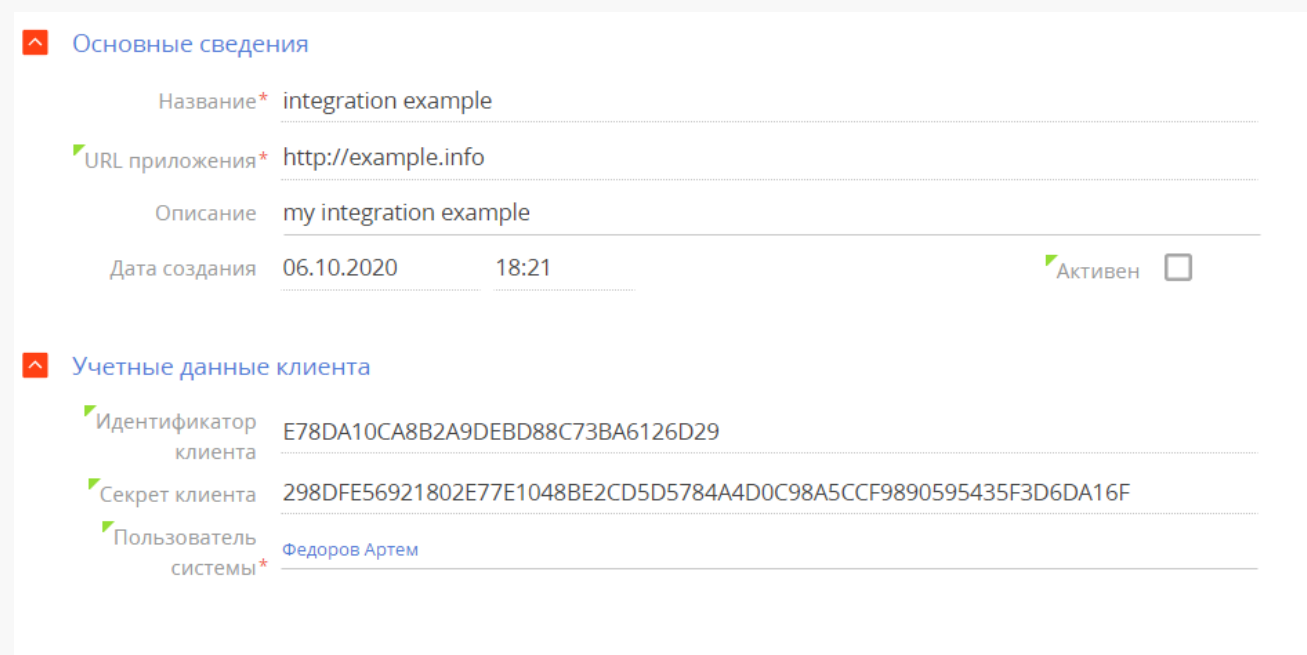
После установки Identity Service и подключения его к Creatio необходимо для каждого из приложений,

которые будут авторизоваться в Creatio по протоколу OAuth 2.0, создать запись клиента. Для этого:

1. Откройте дизайнер системы по кнопке .
2. Перейдите в раздел [*Интеграции с OAuth 2.0 авторизацией*].
3. Нажмите [*Добавить*].
4. На открывшейся странице заполните параметры клиента (приложения, которое будет подключаться к Creatio):
 - a. [*Название*] — заголовок, который будет отображаться в реестре интеграций и логах.
 - b. [*URL приложения*] — адрес приложения или веб-сервиса, который интегрируется с Creatio.
 - c. [*Описание*] — задача, которую решает данная интеграция.
 - d. [*Активен*] — признак определяет, используется ли интеграция с данным приложением или веб-сервисом.
 - e. [*Пользователь*] — пользователь системы с требуемым для данной интеграции набором прав. Рекомендуется настроить права доступа для этого пользователя таким образом, чтобы он имел доступ только на чтение и редактирование тех полей, в которые интегрируемое приложение или веб-сервис будут вносить изменения. Например, для веб-сервиса, передающего в Creatio курсы валют, это поля [*Курс*] и [*Начало*] страницы записи справочника [*Валюты*].

Учетные данные клиента (идентификатор и секрет) заполняются автоматически.

Рис. 5 — Пример настройки клиента



Основные сведения

Название* integration example

URL приложения* http://example.info

Описание my integration example

Дата создания 06.10.2020 18:21 Активен ☐

Учетные данные клиента

Идентификатор клиента E78DA10CA8B2A9DEBD88C73BA6126D29

Секрет клиента 298DFE56921802E77E1048BE2CD5D5784A4D0C98A5CCF9890595435F3D6DA16F

Пользователь системы* Федоров Артем

5. Сохраните запись.
6. Повторите шаги 3–6 для всех приложений, которым необходима авторизация по протоколу OAuth 2.0.

Настроить интеграцию с файловым

хранилищем S3

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Возможность настроить интеграцию с файловым хранилищем S3 доступна в Creatio версии 7.18.1 и выше.

Настройка интеграции с файловым хранилищем необходима для on-site приложений.

S3 (Simple Storage Service) — протокол передачи данных, разработанный компанией Amazon.

Файловое хранилище S3 — это облачный REST-сервис хранения объектов. Особенность хранилища S3 — хранение данных в исходном формате без ограничений по масштабированию.

По умолчанию все файлы, загруженные в приложение, хранятся в базе данных. Файлы, загруженные на детали [*Файлы и ссылки*] или прикрепленные к письмам, можно хранить в хранилище S3. Для этого необходимо настроить интеграцию. Использование хранилища S3 позволяет сократить время выполнения резервного копирования базы данных за счет уменьшения ее размера. Creatio позволяет подключить только одно хранилище S3.

На заметку. При настроенной интеграции файлы, загруженные на детали [*Файлы и ссылки*] через мобильное приложение или с помощью бизнес-процесса, также будут загружаться в хранилище S3.

Этапы настройки интеграции с хранилищем S3:

1. Настройка хранилища S3. [Подробнее >>>](#)
2. Настройка хранения файлов. [Подробнее >>>](#)

Шаг 1. Настроить хранилище S3

1. Создайте аккаунт в сервисе хранения данных, который поддерживает протокол S3.
2. В созданном аккаунте получите “ServiceUrl”. Это конечная точка, по которой Creatio будет получать доступ к хранилищу S3.
3. В созданном аккаунте сгенерируйте “AccessKey” и “SecretKey”. Эти параметры позволяют выполнять авторизованный запрос к хранилищу S3.
4. Создайте корзины (buckets, бакеты) “ObjectBucketName” и “RecycleBucketName” с уникальными именами.
 - “ObjectBucketName” — корзина для хранения файлов. Файлы хранятся неограниченное количество времени.
 - “RecycleBucketName” — корзина для хранения файлов, которые были удалены и хранятся для резервных копий базы данных. В основе работы с корзинами лежит принцип мягкого удаления: после удаления файла из корзины “ObjectBucketName” файл переносится в корзину “RecycleBucketName”. Время хранения файлов в корзине определяется настройками корзины

определенного сервиса. Например, файл может храниться в корзине 90 дней, затем автоматически удаляться. В Creatio время хранения файлов равно времени хранения резервных копий базы данных.

Создание корзины подробно описано в официальной [документации Amazon](#) (материал на английском языке).

Шаг 2. Настроить хранение файлов

Чтобы новые файлы, загруженные на детали [*Файлы и ссылки*], сохранялись в хранилище S3, а не в базе данных, необходимо выполнить настройку на стороне Creatio:

1. В элемент `<connectionStrings>` файла конфигурации `ConnectionStrings.config` добавьте строку с параметрами подключения к хранилищу S3.

Формат строки:

```
<connectionStrings>
  ...
  <add name="s3Connection" connectionString="ServiceUrl=serviceUrl; AccessKey=accessKey; Se
</connectionStrings>
```

Например:

```
<connectionStrings>
  ...
  <add name="s3Connection" connectionString="ServiceUrl=a8*****25; A
</connectionStrings>
```

2. Чтобы при удалении записей разделов связанные файлы корректно переносились в "RecycleBucketName", перейдите на страницу дополнительной функциональности и включите функциональность "UseBaseEntityFileDeleteListener". Подробнее о включении функциональности читайте в статье [Механизм отключения функциональности Feature Toggle](#).

Альтернативным способом включения функциональности является выполнение скрипта в базе данных:

```
UPDATE "AdminUnitFeatureState"
SET "FeatureState" = 1
WHERE "FeatureId" = (
  SELECT "Id"
  FROM "Feature"
  WHERE "Name" = 'UseBaseEntityFileDeleteListener')
```

3. Установите хранилище S3 в качестве активного хранилища файлов. Для этого откройте системную настройку **“Активное хранилище содержимого файлов”** (код `ActiveFileContentStorage`). В поле

[Значение по умолчанию] выберите “Хранилище S3”.

Альтернативным способом установки хранилища S3 в качестве активного хранилища файлов является выполнение скрипта в базе данных:

```
UPDATE "SysSettingsValue"
SET GuidValue = (
    SELECT "Id"
    FROM "SysFileContentStorage"
    WHERE "TypeName" = 'Terrasoft.File.S3.Content.S3FileContentStorage, Terrasoft.File.S3'
)
WHERE "SysSettingsId" = (
    SELECT "Id"
    FROM "SysSettings"
    WHERE "Code" = 'ActiveFileContentStorage')
```

Здесь в поле `Name` следует указать тип активного хранилища файлов:

- "Terrasoft.File.S3.Content.S3FileContentStorage, Terrasoft.File.S3" — для хранилища S3;
- "Terrasoft.File.Content.EntityFileContentStorage, Terrasoft.File" — для базы данных.

Выбор активного хранилища касается только новых файлов. Хранилище ранее загруженных файлов останется прежним. При работе с этими файлами приложение будет обращаться к указанному ранее хранилищу.