Байтим

Руководство по установке системы

Версия 1.6.16+

Обновлено: 10.1.2026

ООО «Байтим»

Оглавление

1 Введение

1.1 Назначение документа

Настоящее руководство предназначено для системных администраторов и предполагает, что читатели обладают базовыми знаниями в области администрирования корпоративных систем, настройки сетей, а также имеют некоторый опыт работы с контейнерами приложений Java, такими как Tomcat, Jetty, JBoss и другие. Также окажется полезным опыт в администратовании баз данных Postgres.

В документе приведены примеры с использованием команд командной строки. В самом приложении применяется язык JavaScript для выполнения макросов и вызовов функций.

1.2 Сокращения и используемые термины

Термин	Значение
JRE	Java Runtime Environment — среда выполнения Java
JVM	Java Virtual Machine — виртуальная машина Java
MFA	Многофакторная аутентификация
OTP	Одноразовый пароль
Postgres	Система управления объектно-реляционными базами данных, с открытым кодом
Servlet	Инструмент, написанный на Java, для разработки веб-приложений
Space	Логическая изоляция функциональности в системе Byteam
Tomcat	Открытый веб-сервер и контейнер сервлетов, разработанный Apache
WAF	Web Application Firewall

2 Основные понятния

2.1 Пространства и конфигурации

Система Byteam поддерживает мультитеннантность, предоставляя несколько виртуальных пространств в рамках одной установки. Данные различных пространств хранятся отдельно друг от друга; списки пользователей, адаптеры, конфигурации и настройки также разделены. Пространства используют один инстанс Tomcat и могут динамически создаваться, запускаться и останавливаться без перезагрузки Tomcat.

Предопределённое пространство под названием "system", создается автоматически, всегда доступно и не может быть удалено. После новой установки это единственное запущенное пространство (если система не поставляется предварительно настроенной с уже созданными пространствами).

Другие пространства должны быть созданы администратором из доступных конфигураций — набора файлов конфигурации, полностью описывающих конкретное приложение.

2.2 Учетные записи

В системе присутствует центральный список учетных записей, содержащий данные пользователей и учетные данные для авторизации, общий для всех пространств. Учетные записи могут быть заблокированы, удалены или отключены по мере необходимости. Только активные записи имеют доступ к системе. Имя учетной записи должно быть уникальным в пределах списка. Например, адрес электронной почты пользователя — это хороший способ идентификации учетной записи.

Пользователи, получающие доступ к системе, могут аутентифицироваться с использованием локальной базы паролей или удаленной системы, поддерживающей протоколы аутентификации, такие как MS Active Directory, сервер LDAP, Azure Active Directory, SCIM2 и системы с поддержкой OpenID Connect. Допускается использование нескольких внешних баз данных, а также их смешивание с локальными учетными записями. В этом случае комбинация базы данных пользователей и имени учетной записи должна быть уникальной.

Все пользователи имеют доступ к REST API по умолчанию. Доступ к объектам через API предоставляет те же права и видимость объектов, что и при доступе к ним через пользовательский интерфейс. Право доступа может быть отозвано администратором и предоставлено только конкретным ролям или пользователям настройками прав или конфигурационным файлом.

Для локальных учетных записей пользователи могут сами изменять и восстанавливать свои пароли. Для учетных записей, управляемых удаленно, пароли (или другие настройки учетных данных) управляются удаленной системой авторизации и не могут быть изменены средствами системы.

2.3 Пользователи

Пользователь — это представление учетной записи в конкретном пространстве. Для каждого пространства, доступного учетной записи, создается отдельный пользователь, который виден только в этом конкретном пространстве. Некоторые атрибуты учетной записи при изменении автоматически распространяются по всем пространствам. Однако возможно изменять атрибуты пользователя в одном пространстве, не влияя на значения в других доступных пространствах.

Записи пользователей содержат всю информацию о пользователе, настройки интерфейса, предпочтения и другие данные профиля, которые обновляются при использовании системы.

Пользователь может быть одновременно авторизован только в одном пространстве. Существуют функции для переключения пользователя между пространствами, если одна учетная запись имеет доступ к нескольким пространствам. Система запоминает последнее используемое пространство, и пользователь автоматически авторизуется в нем при следующем входе.

Если учетная запись синхронизируется с внешней базой данных LDAP, все данные учетной записи распространяются на атрибуты ее пользователей во всех пространствах.

2.4 Права и роли

В каждом пространстве пользователь может иметь различный набор разрешений. Разрешения — это атомарные права, определяемые в каждой конфигурации (например, "Может экспортировать файлы", "Может администрировать пространства", "Может видеть меню разработки" и так далее). Как правило, разрешения предоставляют доступ к объекту или возможность вызова определённой функции.

Для упрощения управления разрешениями в системе определены роли (например, "Разработчик", "Руководитель проекта"), которые содержат заранее определённый набор разрешений, обычно необходимых сотруднику с определённой должностью или функцией в процессе.

Рекомендуется назначать пользователям роли вместо отдельных разрешений. Если в системе используются группы пользователей (синхронизированные с LDAP или определённые локально), роли предпочтительнее назначать на группы, а не отдельным пользователям.

Эффективные права пользователя формируются из следующих элементов:

- Все права, назначенные непосредственно пользователю
- Все права всех ролей, назначенных пользователю
- Все права всех ролей, назначенных всем группам, в которые входит пользователь

3 Установка системы

Эта глава описывает процесс первичной установки системы Byteam на новый сервер.

На сайте производителя доступны скрипты для автоматической установки Byteam на дистрибутивы Ubuntu, RedHat и CentOS Linux. Эти скрипты выполняют все шаги автоматически, скачивая необходимые файлы, с настройками по умолчанию.

Далее в тексте описан также процесс ручной процесс установки, если стандартные скрипты неприменимы или требуются нестандартные настройки.

Для установки на сервере Linux (nginx+Tomcat+Postgres) используйте подготовленный скрипт:

https://www.byteam.ru/distr/install/linux/install.sh

Скрипт должен выполняться от имени привилегированного пользователя ОС. Скрипт автоматизирует следующее:

- Обновление патчей ОС
- Установку базы данных Postgres (если она не установлена)
- Установку Java (если она не установлена)
- Создание пользователя tomcat с домашним каталогом в /home/tomcat
- Скачивание и установку поддерживаемой версии Tomcat с изменёнными конфигурационными файлами
- Настройку Tomcat как системной службы systemd
- Настройку nginx для работы на порту 80 с использованием Tomcat как обратного прокси
- Скачивание актуальной стабильной версии Byteam и её деплой в приложение Tomcat

Система запускается после завершения выполнения скрипта, где администратору предстоит продолжить настройки через графический интерфейс. На следующем этапе необходимо также проверить конфигурацию nginx в /etc/nginx/sites-enabled и загрузить подготовленный SSL-сертификат для обеспечения защищённого соединения.

3.1 Планирование и выбор оборудования

Система Byteam может быть развернута на большинстве современных аппаратных и программных платформ. Она была протестирована на следующих платформах, совместимость с которыми подтверждена:

- MS Windows 8, 10, 11, Server (64bit и 32bit)
- Linux (Astra Linux, ALT Linux , РЕД ОС, Ubuntu, CentOS, RedHat, Rockit) на процессорах Intel или ARM
- Mac OS X (последние версии)

Как правило, в продуктивной среде активно используются системы Linux, включая российские сборки.

Требуемое программное обеспечение:

- **Сервер:** Java 8 (OpenJDK), сервер приложений Tomcat 9, база данных PostgreSQL (версии 10–16)
- **Клиент:** Современный веб-браузер (Яндекс браузер, MS Edge, Firefox, Chrome, Safari, Opera)

Клиентский интерфейс также работает на мобильных устройствах, где отображение адаптируется к размеру экрана.

3.2 Типовая архитектура

Архитектура развертывания зависит от предполагаемого количества пользователей и сценариев использования. Для небольших установок (до 100 пользователей) база данных и сервер приложений могут размещаться на одном компьютере. Для более крупных установок рекомендуется выделенный сервер базы данных.

Во всех конфигурациях рекомендуется использовать веб-прокси перед сервером приложений, подключённым к порту сервера Tomcat. Если требуется защищённое соединение HTTPS, его следует настраивать на внешнем соединении прокси-сервера, а не на самом Tomcat.

В средах с высоким уровнем защищенности, при использовании WAF, WAF следует размещать перед прокси-сервером NGINX, фильтруя входящий трафик.

Благодаря инновационной внутренней архитектуре приложение потребляет значительно меньше системных ресурсов, чем обычные приложения типа OLTP при такой же нагрузке. В силу этих особенностей, в отличии от классической архитектуры, сервер приложений нагружается меньше, чем сервер базы данных. Поэтому в большинстве ситуаций кластеризация не имеет смысла, так как один сервер приложений

может обслуживать тысячи пользователей. В случае необходимости, система поддерживает различные режимы работы в кластере, что может быть полезно для обеспечения высокой доступности и географической распределенности.

При большом количестве внешних интеграций также рекомендуется использовать выделенный сервер интеграции.

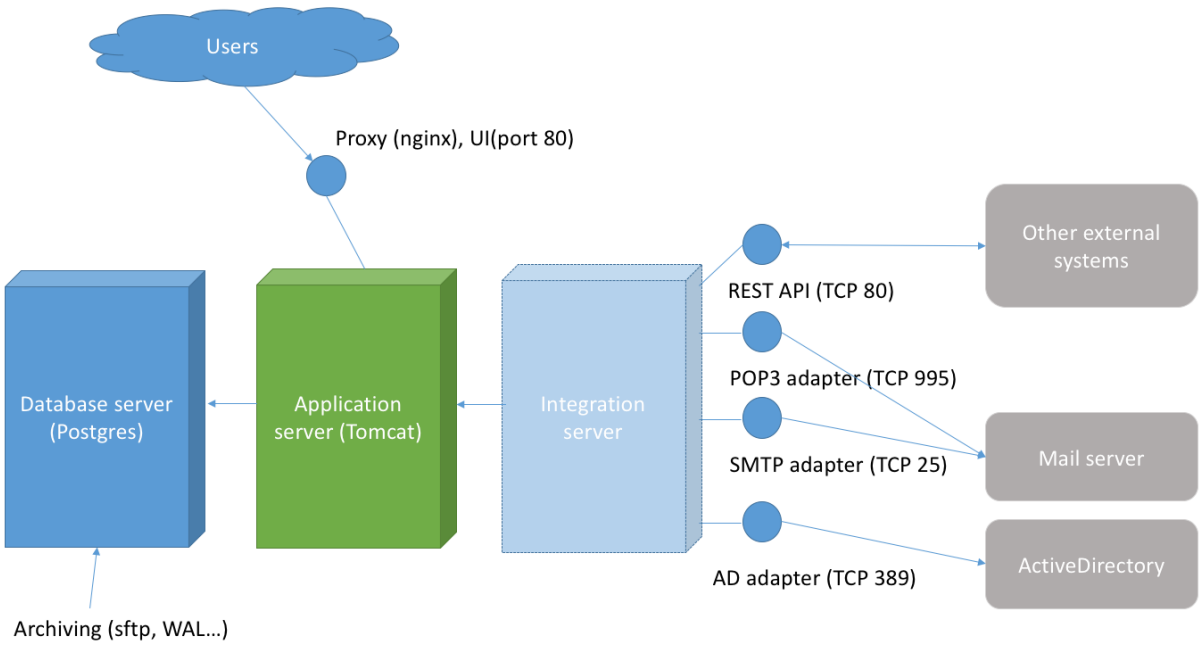

Рисунок 1 Типовая архитектура развертывания

3.3 Настройка нескольких сред

Хорошей практикой является наличие по крайней мере одной среды разработки и одной среды тестирования в дополнение к производственной среде. В высоконагруженных развертываниях также необходимо иметь эталонную среду, аналогичную рабочей, где все изменения тестируются в первую очередь.

При копировании данных из одной среды в другую учитывайте следующее:

Конфигурационные файлы содержат описание среды, такое как имя хоста, расположение файла, конфигурации, настройки ведения журнала и т.д. «ти файлы не должны копироваться между стендами.

База данных содержит некоторые элементы, которые обычно должны быть изменены или анонимизированы при перемещении данных из одной среды в другую:

- Настройки адаптера интеграции, включая системные адреса и сертификаты/пароли
- Лицензионный ключ

- Пользователи, логины, пароли

3.4 Предварительные требования к установке

1. Установка Java

   Если JRE еще не установлена в системе, загрузите и установите последнюю версию JRE для вашей платформы непосредственно у поставщика платформы. Проверьте версию Java, которая должна поддерживаться системой.

   Рекомендуется установить 64-разрядную JRE, если ваша система ее поддерживает. В крупных производственных установках это обязательное требование, в противном случае, Byteam не сможет использовать всю доступную оперативную память системы. Прочтите инструкции по установке Oracle JVM (или другой JVM) для вашей платформы.

   После установки системная переменная JAVA_HOME должна быть определена и видна пользователю приложения, указывающей на правильную версию JRE.

2. Установка Apache Tomcat

   Приложение может быть запущено на существующем по умолчанию Tomcat, предустановленном вместе с вашей ОС, но рекомендуется установить выделенный экземпляр Tomcat в отдельную папку от оригинального дистрибутива в https://tomcat.apache.org

   Убедитесь, что приняты соответствующие меры безопасности для защиты вашей установки. Подробности также доступны в документации Tomcat по адресу https://tomcat.apache.org/tomcat-9.0-doc/setup.html Рекомендуется создать отдельного пользователя ОС для Tomcat, чтобы избежать запуска приложения под учетной записью административной системы.

   При установке для платформы Windows рекомендуется скачивать tomcat в виде zip-архива с официального сайта, а не в виде установщика службы Windows. После загрузки распакуйте пакет в произвольный каталог, например, C:\tomcat.

   При установке Linux Tomcat обычно предоставляется в системом дистрибутиве, но рекомендуется загрузить пакет .tar с веб-сайта Apache Tomcat, который имеет стандартные настройки

3. Установка СУБД PostgreSQL

   Процедура установки Postgres может варьироваться в зависимости от типа системы. Для большинства дистрибутивов Linux существуют предварительно собранные пакеты, которые могут быть уже частью дистрибутива ОС. Ознакомьтесь с документацией по установке для типа и версии платформы. Общая документация по Postgres доступна здесь: https://www.postgresql.org/docs/current/tutorial-install.html

Рекомендуется помещать индексные файлы базы данных на более быстрый диск, желательно SSD. На тестовых серверах достаточно использовать параметры базы

данных по умолчанию. По параметрам производственной системы проконсультируйтесь с администратором базы данных или представителем поставщика для уточнения оптимальных настроек для данного профиля загрузки конфигурации.

3.5 Настройка Apache Tomcat

Определите нахождение папки конфигурации Tomcat и измените файлы server.xml и context.xml, как показано ниже. Обычно каталог находится в $TOMCAT_HOME/conf.

Обратите внимание: В некоторых дистрибутивах Linux папка конфигурации может отличаться от папки приложения Tomcat. В специализированных средах параметры конфигурации могут находиться в скриптах и т.д. Проконсультируйтесь с системным администратором, если вы не уверены, где находится каталог конфигурации.

Установите параметры сервера Tomcat:

1. В server.xml файле внесите следующие изменения:

   В разделе <Connector> добавьте URLEncoding и атрибуты maxThreads следующим образом:

```
<Connector URIEncoding="UTF-8" maxThreads="400" connectionTimeout="20000"
port="8080" protocol="HTTP/1.1" redirectPort="8443"/>
```

   Примечание: установите атрибут maxThreads близкий к ожидаемому пиковому количеству одновременных пользователей, умноженное на 2. Если это число меньше 400, установите maxThreads в значение 400.

2. Отключите кэширование статического контента в context.xml:

```
<Context cachingAllowed="false">
```

3.6 Конфигурация базы данных

Если вы используете отдельные серверы для экземпляра базы данных и экземпляра приложения, убедитесь, что ваш брандмауэр разрешает подключение к базе данных, а настройки безопасности Postgres разрешают удаленное подключение с сервера приложений.

Этапы настройки:

- Создание пользователя базы данных Postgres
- Создайте новую базу данных Postgres и предоставьте пользователю все права доступа к этой базе данных.
- Убедитесь, что ваша база данных настроена на правильную кодировку символов и сортировку для выбранного языка.

Например, чтобы создать базу данных 'byteam' с пользователем 'jupiter' и паролем 'first' выполните следующие команды из консоли psql. Команды также могут выполняться из клиента с графическим интерфейсом, такого как pgAdmin или подобного.

```
create user jupiter with password 'first';
create database byteam;
grant all privileges on database byteam to jupiter;
```

Для Postgres версий 12 и выше отключите jit. Jit включен по умолчанию, начиная с версии 12, и может вызвать проблемы с производительностью. В **файле postgresql.conf** найдите строку, содержащую "jit=", или добавьте одну строку, чтобы она выглядела следующим образом:

```
jit = off
```

3.7 Конфигурация приложения

Шаги:

1. Создайте локальную директорию, в которую будут размещены конфигурационные файлы. После создания определите переменную среды с именем BYTEAM_PATH, которая указывает на расположение этого каталога. Рекомендуется установить переменную в скрипте запуска Tomcat или скрипте пользовательской среды (.profile и т.д.), чтобы переменная загружалась при каждом запуске сервера. Отредактируйте файл и вставьте команду, например:

```
SET BYTEAM_PATH=/home/tomcat/byteam
```

   Убедитесь, что переменная настроена при перезагрузке системы, введя команду в init или login скрипте.

2. Если Tomcat запускается как системная служба, эта переменная окружения может быть установлена скриптом определения демона.
3. В папке из шага 1 создайте подпапку с именем "conf" и внутри этой папки создайте файл с именем "default.properties". В приведенном выше примере файл будет расположен по адресу:

   /home/tomcat/byteam/conf/default.properties

4. Поместите конфигурацию подключения к базе данных в файл default.properties или скопируйте значения по умолчанию из файла шаблона

```
# Пример конфигурационного файла:
dbname=jupiter
```

```
dbport=5432
dbhost=localhost
dbuser=jupiter
dbpassword=..
dbmaxconnections=20
dbinitconnections=10
dbdriverclass=org.postgresql.Driver
```

5. Разверните архив WAR в Tomcat, скопировав архив в папку tomcat webapps. Процесс развертывания см. в документации Tomcat. Для тестирования среды можно использовать autodeploy. В производственных средах автоматическое развертывание должно быть отключено, чтобы избежать непредвиденных перезапусков приложений.

Параметр dbmaxconnections должен быть настроен в соответствии с типом установки. Для производственных систем используйте не менее (количество одновременных пользователей / 2). Для тестирования или разработки используйте минимальную настройку 10. Для систем общего назначения без большой нагрузки 20 является безопасным выбором.

3.7.1 Генерация нового пароля для пользователя базы данных

В этом примере конфигурации зашифрованный пароль по умолчанию имеет значение "first". Система ожидает этот пароль

Если вы не предоставите никакой конфигурации. Если вы хотите установить другой пароль базы данных, вы можете использовать утилиту шифрования паролей EncryptPassword. Утилита написана на java, поэтому ее можно запустить из командной строки в любой операционной системе. Запустите его с помощью следующей команды:

```
java -jar EncryptPassword.jar
```

Вам будет предложено ввести пароль и повторно ввести его на следующем шаге, чтобы проверить, совпадает ли новый пароль. После этого создается зашифрованный хэш из пароля. Используйте этот хеш в атрибуте dbpassword файла default.properties, как показано выше.

3.8 Запуск сервера

Управление запуском/остановкой сервера осуществляется с помощью запуска/остановки сервера приложений Tomcat.

3.8.1 Управление запуском/остановкой сервера осуществляется с помощью запуска/остановки сервера приложений Tomcat.

3.8.2 Запуск системы

После новой установки сначала запустите систему, вручную запустив Tomcat, и проверьте файлы журналов tomcat на наличие возможных ошибок (по умолчанию они находятся в файле **catalina.out**).

Перед запуском сервера можно проверить, запущен ли процесс для базы данных *postgres* (без него приложение не запустится).

В системе Linux с запущенным по умолчанию tomcat в качестве системной службы выполните:

```
sudo service tomcat start
```

При выборочной установке вместо этого запустите скрипт запуска Tomcat.

Когда в журнале появляется следующее сообщение, запуск системы выполнен правильно:

<init>@<none> INFO server.BootUp - Byteam started with state: OK

Предположим, что ваш WAR-файл называется "byteam.war", развертывание называется "byteam", откройте WEB-браузер и перейдите в **http://yourhostname:8080/byteam**. Если вы изменили имя развертывания или имя архива, путь будет другим.

3.8.3 Вход в систему

В веб-браузере вы должны увидеть окно с запросом на вход в систему. Используйте известные учетные данные по умолчанию для входа в систему:

Username: admin

Password: admin123

Затем измените пароль пользователя admin при первой удобной возможности. Это можно сделать в настройках приложения в разделе Безопасность.

3.8.4 Остановка системы

Остановите экземпляр Tomcat, выполнив специальный скрипт или системную команду.

Например, в системе Linux с запущенным по умолчанию tomcat в качестве системной службы выполните:

```
sudo service tomcat stop
```

При остановке системы все пользователи будут выведены из системы, соединение с базой данных будет закрыто, внешние службы и службы синхронизации будут остановлены. В файле журнала вы должны увидеть сообщение с подтверждением:

INFO server.BootUp - Shutdown complete

3.9 Процедура удаления

Чтобы удалить программу:

1. Остановите Tomcat (сервисом операционной системы или другим способом)
2. Удалите файл *Byteam.war* и папку *Byteam* в подкаталоге Tomcat "webapps"
3. Если есть какие-либо скрипты автозапуска, удалите их из папок автозагрузки системы (в зависимости от платформы).
4. Удалите все файлы из папки $BYTEAM_PATH
5. Удалите базу данных Postgres (см. руководство пользователя Postgres), согласно инструкции для вашей платформы

Перед удалением системы желательно сохранить резервную копию данных.

4 Обслуживание системы

4.1 Регламентные процедуры проверки

Действия, которые администраторам следует выполнять периодически (или автоматизировать с помощью скриптов):

- Проверять наличие достаточного свободного места в файловой системе сервера приложений и сервера базы данных. Если задан слишком низкий (подробный) уровень логирования, при высокой нагрузке приложение может создавать значительный объем лог-файлов
- Отслеживать сообщения в логах. Сообщения с уровнем логирования CRITICAL необходимо устранять немедленно. Периодически появляющиеся сообщения с уровнем ERROR также должны быть устранены
- Если выдана временная лицензия или лицензия имеет ограничения по сроку действия, рекомендуется выполнить необходимые действия для продления лицензионных ключей не менее чем за несколько дней до истечения их срока действия

4.2 Мониторинг

Рекомендуется использовать общедоступные скрипты/адаптеры мониторинга для выбранной системы мониторинга и настроить регулярный мониторинг в соответствии со стандартами эксплуатации заказчика как минимум для следующих компонентов системы.

- Серверы приложений (java/tomcat)
    - Мониторинг процесса Java/Tomcat (PID соответствующего процесса Java)
    - Мониторинг свободного места на диске или в дисковом томе
    - Мониторинг загрузки ЦП
    - Мониторинг свободной/используемой памяти
    - Мониторинг области кучи (heap) памяти

- Сервер базы данных (Postgre/SQL)
    - Мониторинг процесса Postgre/SQL (PID соответствующего процесса)
    - Мониторинг загрузки ЦП
    - Мониторинг свободной/используемой памяти

Также рекомендуется настроить мониторинг других детальных параметров приложения исходя из потребностей и опыта эксплуатации заказчика. Например:

- Результат выполнения регулярной процедуры резервного копирования

- Разбор системных логов и логов приложения с поиском известных сообщений об ошибках и ключевых слов
- Мониторинг интегрированных систем (SMTP, POP3, LDAP, ...)
- Доступность пользовательского интерфейса приложения (веб-интерфейса), процедуры входа в систему и т. д.

4.3 Определение текущей версии программного обеспечения

Чтобы узнать, какая версия приложения используется в настоящий момент, войдите в приложение, щелкните свое имя пользователя в левом углу и в отобразившемся меню выберите пункт About.

На экране «О программе» отображается версия ядра приложения и версия конкретной пользовательской конфигурации.

4.4 Журнал событий

Большинство событий приложения, событий безопасности, ошибок и общей информации о состоянии системы можно отслеживать в системном лог-файле. Стандартный файл Tomcat «catalina.out» размещается в каталоге «logs» сервера Tomcat. Этот файл представляет собой вывод консоли Tomcat, который является логгером по умолчанию.

С помощью файла «default.properties» администраторы могут задавать дополнительные лог-файлы, уровни логирования, формат и фильтрацию.

Для логирования общего назначения в системе используется широко известная библиотека log4j. Каждое записываемое сообщение содержит дополнительные атрибуты, такие как IP-адрес, логин, отметка времени, идентификатор потока, имя класса и уровень значимости.

Для уменьшения размера логов логирование следует ограничивать необходимым уровнем. Параметры логирования можно задать в файле default.properties, чтобы настроить период ротации логов и уровень логирования каждого модуля по отдельности.

Ознакомьтесь со статьей https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/Level.html, чтобы узнать об уровнях логирования, доступных в этой библиотеке.

Некоторые базовые примеры настройки уровня логирования приведены в стандартном файле default.properties и закомментированы.

Пример конфигурации с пользовательским шаблоном вывода и дополнительным лог-файлом, ротация которого выполняется после заполнения 800 МБ:

```
# Set root logger level to INFO and define two appenders: one console, one file-located
log4j.rootLogger=INFO, console, file
```

```
# A1 is set to be a ConsoleAppender.
log4j.appender.console=org.apache.log4j.ConsoleAppender
# A1 uses PatternLayout.
log4j.appender.console.layout=org.apache.log4j.PatternLayout
log4j.appender.console.layout.ConversionPattern=%d %X{login}@%X{space} %-5p %c{2} - %m%n
# Direct log messages to a log file
log4j.appender.file=org.apache.log4j.RollingFileAppender
log4j.appender.file.File=/home/tomcat/logs/custom-output.log
log4j.appender.file.MaxFileSize=800MB
log4j.appender.file.MaxBackupIndex=10
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d %X{login}@%X{space} %-5p %c{2} - %m%n
```

4.5 Настройка параметров конфигурации сервера

Большинство настроек можно изменить в графическом интерфейсе в режиме онлайн, и их изменение не требует перезапуска системы. Однако для некоторых настроек, влияющих на общее поведение системы или на процедуру запуска, Байтим использует параметры, задаваемые в файле, которые описаны в этой главе. Значения по умолчанию и примеры см. в примере файла конфигурации, поставляемом с вашей установкой Байтим.

На платформе Windows, если требуется указать имя файла или путь к каталогу, не забудьте надлежащим образом экранировать символ \ (например, c:\\Байтим, а не c:\Байтим).

Первоначальный файл default.properties устанавливается автоматически с помощью предоставляемых скриптов

В примере файла приведены настройки по умолчанию и пояснения возможных значений.

Перечень поддерживаемых параметров конфигурации в файле default.properties

Параметр	Значение
accessibleDirectories	Список системных папок, которые будут доступны приложению для функций файлового API.
attachments.wipe.enable	Удаление стертых вложений — стирание по умолчанию отключено. Раскомментируйте для включения: attachments.wipe.enable=true
attachments.wipe.interval	Интервал стирания в секундах

autoupgrade.enable	Установите значение true, чтобы разрешить обновление версий конфигурации из репозиториев GIT непосредственно из графического интерфейса. Доступно только системным администраторам
bookspath	Список каталогов для поиска конфигураций, разделенный двоеточиями
crypto.crl	Использовать списки отзыва для проверки того, не были ли сертификаты отозваны. По умолчанию отключено. Требуется доступ сервера в интернет. Пример: crypto.crl=true
crypto.downloadCertificates	Включить загрузку отсутствующих сертификатов в цепочке при проверке сертификатов X509 или при подписании документов. По умолчанию отключено. Для загрузки требуется доступ в интернет Пример: crypto.downloadCertificates=true
customerLogoImage, customerLogoImage2x	Позволяет задать альтернативное изображение логотипа и логотип высокого разрешения для конкретной среды заказчика. Логотип отображается на экране входа в систему. Файлы могут быть предоставлены в формате PNG или JPG (JPEG). Пример: customerLogoImage=$BYTEAM_PATH/img/N_logo_90x90px.png customerLogoImage2x=$BYTEAM_PATH/img/N_logo_180x180px.png
dbhost	Имя хоста или IP-адрес сервера базы данных
dbmaxconnections	Максимальное количество одновременных подключений к базе данных. Рекомендуется значение 20
dbname	Имя базы данных
dbpassword	Пароль базы данных, в закодированном виде
dbport	Номер порта базы данных
dbquerytimeout	Тайм-аут запроса к базе данных (в секундах) позволяет прерывать длительно выполняющиеся SQL-запросы, чтобы защитить систему от чрезмерной нагрузки, вызванной нежелательными сложными запросами. Значение по умолчанию: 60
dbuser	Имя пользователя для входа в базу данных
entitylocktimeout	Задает в секундах тайм-аут «ленивой» блокировки сущности. Например, если задать entitylocktimeout = 600, это означает, что после начала редактирования сущности запись будет заблокирована на 10 минут, если редактирование не будет завершено до истечения тайм-аута. Пока сущность заблокирована, другим пользователям не разрешается ее изменять.

	Этот параметр применяется только к сущностям, поддерживающим блокировки; в метамодели их можно определить по свойству lockMode со значением lazy.
favicon.ico	Позволяет задать альтернативное изображение значка сайта (favicon) для конкретной среды заказчика. Файлы должны быть предоставлены в формате ICO. Пример: favicon.ico=$BYTEAM_PATH/img/favicon.ico
favicon.png	Позволяет задать альтернативное изображение значка сайта (favicon) для конкретной среды заказчика. Файлы должны быть предоставлены в формате PNG. Пример: favicon.png=$BYTEAM_PATH/img/favicon.png
loadjslibs	Список файлов JavaScript (*.js), разделенный двоеточиями, которые будут предварительно загружены в среду JavaScript при запуске в качестве библиотек.
loadjsscripts	Список пользовательских файлов JavaScript (*.js), разделенный двоеточиями, которые будут автоматически загружены и выполнены при запуске системы. В этих скриптах нельзя создавать глобальные объекты. Если необходимо опубликовать глобальный объект, используйте вместо этого loadjslibs
loginBackgroundColor	Значение RGB или название цвета для фона страницы входа в систему
loginBackgroundImage	Настройка фонового изображения экрана входа в систему. Пример: loginBackgroundImage=$BYTEAM_PATH/img/water.jpg
loginBackgroundVideo	Путь к видеофайлу, который может использоваться вместо фонового изображения. Пример: loginBackgroundVideoDark=$BYTEAM_PATH/img/dark-snow.mov
loginBackgroundVideoDark	Фоновое видео экрана входа в систему для темного режима. Если не задано, для светлого и темного режимов будет использоваться loginBackgroundVideo
loginLanguage	Язык экрана входа в систему. Значение по умолчанию: EN Пример: loginLanguage:RU
loginLanguageAutodetect	Установите значение true, чтобы включить автоопределение языка по языковым настройкам браузера пользователя: loginLanguageAutodetect=true
loginLanguages	Список доступных языков, разрешенных для выбора пользователями, через запятую. Пример: loginLanguages=EN,RU

maxChangeSetSize	Максимальное количество записей журнала, хранимых на сервере для получения клиентским окном при каждом сетевом запросе. Увеличьте это значение, если в лог-файлах слишком часто появляются сообщения «trap overflow». В производственных средах значение не должно быть меньше 100, однако увеличение этого предела повышает потребление памяти сервера для каждого пользователя. Значение по умолчанию — 50. Пример: maxChangeSetSize = 51
scriptableclasses	Список классов Java, которые будут доступны фреймворку скриптов. Методы скриптуемых классов должны иметь аннотации @Scriptable и находиться в CLASS_PATH. Подробнее см. документацию Java SDK
servlet.compression	Позволяет отключить сжатие файлов на стороне сервера, включенное по умолчанию. Файлы JSON и некоторые файлы JavaScript сжимаются с помощью gzip для снижения сетевой нагрузки. Если в среде используется межсетевой экран уровня приложений, испытывающий трудности с распаковкой файлов, можно использовать этот флаг. Пример: servlet.compression=false
session.cookie.httpOnly	Позволяет задать параметр httpOnly сеансового cookie. Пример: session.cookie.httpOnly=true
session.cookie.maxAge	Изменяет параметр maxAge сеансового cookie. Время в секундах, по истечении которого cookie будет удален # по умолчанию = -1 --> удаляется, когда пользователь закрывает браузер
session.cookie.name	С помощью этого свойства сеансовый cookie может быть переименован. По умолчанию session.cookie.name=SESSION_CONTEXT_ID
session.cookie.sameSite	Позволяет задать атрибут sameSite сеансового cookie по умолчанию. Значение по умолчанию — пустое. Допустимые значения: Lax, Strict, None Пример: session.cookie.sameSite=lax
session.cookie.secure	Позволяет задать параметр secure сеансового cookie. Пример: session.cookie.secure=true

session.idle.timeout	# Тайм-аут сеанса при простое, в секундах
	# по умолчанию = 1800 [30 мин]
	session.idle.timeout=1800

shutdownDelay	Интервал в секундах, определяющий, как долго приложение будет ожидать пользователей перед их отключением при остановке. Значение по умолчанию — 30
systemmode	Режим работы, влияющий на значения по умолчанию других параметров. Возможные значения: DEVELOPMENT, TESTING, PRODUCTION В режиме PRODUCTION система не выполняет автоматическое обновление метамодели и шаблонов из файловой системы, однако администратор может запустить его вручную. В остальных режимах Байтим автоматически поддерживает метамодель и другие настраиваемые объекты в актуальном состоянии. Подробнее см. в главе «Управление конфигурацией»
sqlcomments	Установите значение false, чтобы отключить вывод сведений об исходном JSON-запросе в комментариях всех SQL-запросов к базе данных. Эта информация полезна для мониторинга производительности и отладки и включена по умолчанию начиная с версии 1.6.271
templatespath	Список каталогов для поиска файлов шаблонов, разделенный двоеточиями
workerPoolMaxSize	Количество обработчиков по умолчанию для очереди и обработки документов

4.6 Резервное копирование и восстановление

Убедитесь, что папки приложения и конфигурации всегда включены в резервное копирование. Папки конфигурации (в каталоге $BYTEAM_PATH) относительно невелики и изменяются нечасто. Все данные приложения и пользовательские настройки хранятся в базе данных, резервное копирование которой следует выполнять как можно чаще.

В настоящее время Байтим поддерживает только базу данных PostgreSQL. Резервное копирование базы данных выполняется в соответствии со стандартными процедурами, описанными по адресу http://www.postgresql.org/docs/9.4/static/backup-dump.html

Существуют более сложные сценарии резервного копирования, которые выходят за рамки данного документа. Для ускорения резервного копирования и восстановления может быть настроено архивирование WAL-файлов или архивирование на дисковом уровне. Для выбора оптимальной стратегии в соответствии с требованиями к аварийному восстановлению и допустимому времени простоя обратитесь к своему системному интегратору.

Для Postgres версии 9.4 и выше для резервного копирования в режиме онлайн может использоваться расширение pglogical. Подробнее см., например, https://2ndquadrant.com/en/resources/pglogical/.

4.6.1 Резервное копирование

Для выполнения однократного резервного копирования базы данных выполните:

```
pg_dump -U <<username>> <<database>> -f backup.sql
```

Если баз данных несколько, их можно скопировать в один файл:

```
pg_dumpall > backup.sql
```

4.6.2 Восстановление

Если требуется восстановить Байтим, убедитесь, что во время восстановления приложение не запущено. Одновременная работа приложения и восстановление данных могут привести к несогласованности или повреждению данных.

Для восстановления базы данных сначала удалите/создайте заново исходную базу данных, а затем выполните:

```
psql <<database>> < backup.sql
```

Где <<database>> — имя базы данных, заданное в файле default.properties, а <<username>> — имя пользователя для входа в базу данных, заданное в том же файле.

4.6.3 Журнал транзакций

В приложении имеется внутренний журнал транзакций, содержащий все изменения всех основных объектов системы. Транзакции регистрируются независимо от их источника: графический интерфейс, API, внутренние скрипты, импортированные данные и т. д. Этот журнал используется для отображения истории изменений и выполнения операций отмены. Кроме того, он может использоваться для создания логических резервных копий данных или извлечения данных во внешнюю систему хранилища данных. Данные хранятся в сущности «journal», которая доступна через REST API, команды скриптов или браузер данных в графическом интерфейсе.

Обратите внимание, что приватные поля в журнале не сохраняются. Для резервного копирования приватных полей всегда используйте резервное копирование на уровне базы данных.

4.7 Выполнение команд и скриптов на стороне сервера

Большая часть бизнес-логики Байтим выполняется в серверном контейнере JavaScript. Байтим позволяет запускать собственные команды JavaScript на сервере с помощью графического интерфейса и получать результаты их выполнения.

Хотя консоль скриптов в большей степени полезна разработчикам, некоторые сложные административные задачи также могут требовать выполнения скриптов на сервере и просмотра результатов. Все административные действия, выполняемые через меню графического интерфейса, также могут быть выполнены с помощью скриптов.

Для доступа к консоли JavaScript необходимо иметь специальное разрешение — Execute server-side scripts, которое находится в разделе разрешений System administration. Для открытия консоли используйте глобальное сочетание клавиш Ctrl + j. Для выполнения команд нажмите кнопку «Execute selection» или используйте сочетание клавиш Ctrl + ENTER.

Если в коде выделен фрагмент текста, будет выполнен только этот фрагмент. Если ничего не выделено, будет выполнено все содержимое редактора.

После завершения выполнения команды результат отображается под окном консоли. Щелкнув по нему, можно открыть предварительный просмотр результата во всплывающем окне.

Если данные предварительного просмотра представляют собой коллекцию (массив объектов), появится вкладка «Table», и данные будут отформатированы в виде таблицы. Кнопка «Copy» позволяет скопировать все данные и вставить их в MS Excel или другие редакторы.

Существует специальная команда JavaScript «show()», которая работает только в консоли JS. Она полезна для целей отладки. Например, чтобы увидеть результат во время выполнения цикла, поместите show(value) в любом месте вызова, где value — любое выражение или переменная JS. Значение будет выведено в консоль синим цветом.

Если требуется код, извлекающий данные из таблиц, для быстрого создания типовых примеров скриптов можно воспользоваться кнопкой «Generate» на экране браузера данных.

4.8 Выполнение обновлений приложения

Обновленные версии распространяются в виде WAR-файлов. Обновление требует перезапуска приложения, поэтому это затронет пользователей — их потребуется отключить от системы. Типовое обновление между минорными релизами занимает до 2–3 минут на сервере средней производительности. Большую часть времени занимает запуск/остановка приложения.

При обновлениях (как минорных, так и мажорных версий) все данные приложения, включая пользовательские настройки и конфигурации, а также все доработки сохраняются. Если требуется миграция данных, она будет выполнена автоматически, поскольку скрипты обновления входят в состав каждой версии дистрибутива. Скрипт выполняется инкрементально, поэтому некоторые версии могут быть пропущены. Например, возможно обновление с 1.2.5 до 1.2.10 или сразу до 1.3.

Для обновления получите актуальную версию WAR-файла на сайте поддержки поставщика. Затем выполните обновление:

1. Внимательно прочитайте прилагаемые примечания к выпуску или инструкции по обновлению, если они предоставлены. При обновлении мажорных версий могут потребоваться дополнительные действия. Они будут описаны в инструкциях по обновлению
2. Остановите Байтим
3. Создайте резервную копию установки, файлов конфигурации и базы данных
4. Скопируйте новый WAR-файл в расположение старого WAR-файла
5. Запустите Байтим
6. Отслеживайте логи, чтобы убедиться, что Tomcat успешно развернул новый WAR-файл и Байтим запустился без ошибок
7. Войдите в приложение и визуально убедитесь, что система работает в обычном режиме

Если во время установки произошла критическая ошибка, можно выполнить сценарий отката:

1. Остановите Байтим
2. Убедитесь, что приложение остановлено и в памяти системы не осталось «висящих» процессов (для проверки используйте средства ОС)
3. Скопируйте и заархивируйте все лог-файлы, содержащие сообщения об ошибках, для последующего анализа
4. Скопируйте старый WAR-файл в расположение, где он находился ранее
5. Удалите все файлы из каталога tomcat webapps/Байтим (или из каталога, соответствующего имени вашего развертывания, если вы задали другое имя)
6. Запустите Байтим
7. Просмотрите лог-файлы и убедитесь, что система работает корректно
8. Обратитесь в службу поддержки и предоставьте заархивированные лог-файлы для диагностики первопричины проблем

Действия по обновлению следует максимально автоматизировать, чтобы избежать ошибок персонала. Вендор предоставляет стандартные скрипты для платформы Linux, упрощающие эксплуатационные операции.

4.9 Управление конфигурацией

Поскольку часть изменений может выполняться администраторами в работающих средах, а часть — разработчиками в последующих релизах, возможны конфликтующие изменения, требующие ручного разрешения.

Чтобы избежать этого и упростить развертывание новых версий, введены следующие настраиваемые объекты, позволяющие построить процесс непрерывного управления конфигурацией с высокой степенью автоматизации.

Вместо развертывания скриптов миграции разработчики публикуют только новую версию кода и объектов. Система автоматически сравнивает предыдущие объекты с новой версией и выполняет необходимые изменения в базе данных. Такой подход также позволяет перескакивать через несколько версий при установке обновлений.

Настраиваемые объекты

Все настраиваемые объекты обладают одинаковыми свойствами:

- Автоматическое развертывание
- Наследование
- Переопределение
- Поведение, зависящее от режима работы системы

Автоматическое развертывание

Автоматическое развертывание приводит к тому, что измененные файлы обновляют объекты в базе данных, если они являются более новыми.

Существуют разные режимы, зависящие от режима работы системы, заданного в файле default.properties:

Режим	Поведение автообновления
DEVELOPMENT	Все измененные файлы обновляют объекты, если файлы новее объектов Обновление выполняется при запуске системы и при изменении любого из файлов в файловой системе (отслеживание в реальном времени). Этот режим поддерживает «горячее» развертывание.
TESTING	Все измененные файлы обновляют объекты, если файлы новее объектов Обновление выполняется только при запуске системы
PRODUCTION	Все измененные файлы обновляют объекты, если файлы новее объектов и для объекта не установлен флаг «userdefined». Обновление выполняется только при запуске системы

Все настраиваемые объекты содержат поле базы данных «userdefined», которое устанавливается в значение «true» каждый раз, когда администратор выполняет какие-

либо локальные изменения. Например, если жизненный цикл изменен в графическом интерфейсе, флаг userdefined устанавливается в true, а в поле «updatetime» записывается время изменения. В соответствии с приведенной выше таблицей объекты сравниваются с файлами с учетом этих двух атрибутов.

Редактор жизненных циклов отображает желтый или красный индикатор рядом с локально измененными жизненными циклами, указывая на возможные конфликты.

Наследование

Наследование означает, что, если объект с одним и тем же именем используется в нескольких конфигурациях, будет использована версия из самой верхней конфигурации в цепочке «родитель — потомок».

Перечень настраиваемых объектов

В следующей таблице приведен перечень настраиваемых объектов, их расположение в файловой системе и в таблицах базы данных:

Тип объекта	Путь к файлам	Сущность
Списки значений (LOV)	config/lovs	lov
Пейджфлоу (Pageflow)	config/pageflow	pageflow
Доработки (Customizations)	config/customizations	customizations
Фильтры	config/filters	filters
SLA (соглашения об уровне обслуживания)	config/sla	sla
Календари	config/calendars	calendars
Часовые пояса	config/timezones	timezones
Приложения	config/applications	applications
Рабочие процессы (жизненные циклы)	config/workflow	lifecycles
Роли пользователей	config/roles	userroles
Шаблоны уведомлений	config/alerttemplates	alerttemplates
Векторы наименования	config/namingvectors	namingvectors
Определения отчетов	config/reportdefs	reportdefs
Отчеты	config/reports	reports

Шаблоны	templates//*.xml	softshell_defs
Метамодель	model/MetaModel.json	-
Ключи локализации	i18n//*.loc	-

Типовой сценарий развертывания предполагает использование нескольких экземпляров приложения для создания экземпляров разработки, тестирования и производственной среды. Изменения кода и конфигурации переносятся между этими средами разработчиками.

Объекты распространяются как в составе стандартного WAR-архива системы, так и через пользовательский GIT-репозиторий, предоставляемый разработчиками конкретной установки. Все изменения при развертывании объединяются в одном экземпляре.

5 Оптимизация производительности

Особенности, влияющие на производительность

При планировании развертывания системы соберите и проанализируйте следующие исходные параметры:

1. Сколько пользователей будет работать в системе?
2. Какие модули и функции будут использоваться?
3. Сколько будет интеграций, какого типа, каков ожидаемый объем трафика?
4. Сколько файлов вложений хранится, каков примерный объем в год?
5. Каково ожидаемое количество записей в год (для наиболее критичных бизнес-объектов)?
6. Будут ли реализованы сложные правила безопасности, например раздельная видимость некоторых объектов для разных пользователей на основании атрибутов этих объектов?

Для наиболее эффективного использования доступного оборудования следует сбалансировать следующие параметры:

- Количество потоков Tomcat должно быть не меньше количества пользователей, работающих одновременно, *2
- Количество подключений к базе данных должно быть не меньше 20 для производственных систем и до 100 для высоконагруженных систем
- Параметры базы данных должны быть настроены с учетом указанного выше количества подключений
- Параметры памяти JVM для Tomcat должны обеспечивать не менее 2 ГБ памяти кучи (heap), настроенных в пределах до 80 % доступной памяти

Пулы потоков ЦП

Приложение обеспечивает гибридную функциональность — от обработки пользовательских запросов фронтенда практически в реальном времени до подготовки BI и отчетов. Для достижения стабильной производительности по всем этим функциям система использует рабочие очереди, обрабатывая ресурсоемкие вычисления в нескольких отдельных пулах потоков.

Существует 3 основных пула потоков:

- Основной http-пул Tomcat — здесь выполняются запросы графического интерфейса и запросы REST API. Параметры пула определяются настройками Tomcat
- Пул асинхронных событий — здесь обрабатываются все асинхронные события системы: KPI, SLA, перерасчеты BI, уведомления, большинство триггеров и т. д.
- Пул заданий — здесь выполняются ресурсоемкие для ЦП задания, например скрипты действий из жизненных циклов. Обычно используется для выполнения

таких задач, как генерация PDF, подписание, обновление больших наборов данных и т. д.

Адаптеры интеграции управляют своими потоками самостоятельно. Каждый адаптер поддерживает как минимум один поток адаптера, некоторые используют 2 потока. Если адаптер может быть настроен на одновременный прием нескольких подключений, каждое подключение может занимать отдельный поток.

Как правило, пулы управляются автоматически. В некоторых сложных сценариях системные администраторы могут захотеть изменить ограничения пулов, чтобы задействовать дополнительную производительность ЦП.

В файле «default.properties» можно настроить следующие свойства:

- eventsPoolCoreSize — начальный размер пула асинхронных событий по умолчанию
- eventsPoolMaxSize — максимальный размер пула асинхронных событий
- jobsPoolCoreSize — начальный размер пула заданий по умолчанию
- jobsPoolMaxSize — максимальный размер пула заданий

Для систем в режиме разработки размеры пулов по умолчанию равны 1, для производственного и тестового режимов — 2. Максимальное значение по умолчанию составляет 10 для всех пулов и режимов работы системы.

Когда система не нагружена сильно, размер пула сохраняется на «базовом» (core) значении. При росте нагрузки пулы могут увеличиваться до «максимальных» (max) размеров. Больший размер пула потребляет больше ресурсов ЦП и памяти, а также создает дополнительную нагрузку из-за переключения потоков. Меньшие размеры пулов уменьшают количество процессов, которые могут выполняться параллельно.

Администраторам следует учитывать эти сведения для наиболее эффективного использования оборудования и вносить изменения постепенно, контролируя их влияние на нагрузку системы и скорость обработки.

Для контроля использования пулов перейдите в меню «Developer tools/Performance metrics...» и найдите разделы «Event processing thread pool» и «Jobs workers thread pool».

Значение queueLength указывает, сколько запросов в настоящий момент ожидает освобождения потока. Значение poolSize показывает текущий размер пула.

6 Управление доступом

Управление доступом включает назначение пользователям определенных функций и ограничение доступа к некоторым функциям и данным. Существуют различные уровни определения управления доступом. Наиболее важные термины:

- Пользователи — пользователи системы, назначенные пространству
- Группы — именованные списки из нескольких пользователей
- Права — отдельные правила предоставления доступа к объекту или функции
- Роли — именованный набор из нескольких прав, который может назначаться пользователям или группам
- Территории — сопоставление пользователей с одной из «зон» безопасности: внутренние пользователи, заказчики, субподрядчики… См. также главу "**Разделение пользователей**", в которой описано, как роли могут автоматически сопоставляться территориям

В большинстве случаев управление доступом пользователей основано на ролях и правах. Права предопределены для каждого модуля приложения и не могут быть изменены администратором. Перечень ролей зависит от установленных модулей и может редактироваться в графическом интерфейсе.

6.1 Предопределенные роли пользователей

Наименование	Описание
Администратор пространства	Обладает административными правами в текущем пространстве. Может добавлять и удалять пользователей всех типов, назначать права пользователям и группам. Может выполнять сервисные команды и просматривать логи в режиме онлайн, задавать свойства пространства, изменять календари, открывать консоль разработки, просматривать все меню.
Разработчик	Обладает правами разработки в текущем пространстве. Может выполнять удаленные команды, просматривать объекты, определять жизненные циклы, списки значений, редактировать компоненты графического интерфейса.
Только модуль Service Desk	
Администратор каталога услуг	Может редактировать записи каталога услуг, определять глобальные избранные элементы.
Оператор ServiceDesk	Может просматривать все инциденты, запросы на обслуживание и записи о проблемах. Может добавлять инциденты от имени других пользователей. Может редактировать и обрабатывать записи службы

	поддержки в соответствии с правилами рабочего процесса. Может сбрасывать SLA по заявкам.
ServiceDesk — создатель записей о проблемах (PR)	Может создавать записи о проблемах в модуле ServiceDesk.
Только модуль управления требованиями и проектами	
Аналитик	Может редактировать и создавать требования, выполняет декомпозицию запросов на требования.
Аналитик по тестированию	Расширенные права на выполнение тестирования. Может просматривать, редактировать и удалять все объекты тестирования
Руководитель аналитиков	Может назначать ресурсы для анализа.
Руководитель эксплуатации	Может оценивать сметы эксплуатационных расходов, получает задачи на установку ПО.
Руководитель тестирования	Может назначать ресурсы для анализа тестирования и тестовых прогонов.
Руководитель программ	Может просматривать все программы, изменять атрибуты и статус программы. Может добавлять проекты в программы.
Руководитель проекта	Может просматривать все проекты, изменять атрибуты и статус проекта. Может просматривать файлы проектов.
Руководитель проектного офиса	Может просматривать все проекты, изменять атрибуты и статус проекта. Может просматривать файлы проектов.
Планировщик релизов	Может планировать проекты в релизы. Может создавать релизы и изменять их параметры.
Менеджер ресурсов	Может планировать доступность ресурсов. Может просматривать и редактировать типы ресурсов и план доступности обрабатываемых ресурсов.
Только модуль управления тестированием	
Тестировщик	Может выполнять предопределенные тесты, сообщать о результатах тестирования, создавать и обновлять дефекты.

Администратор управления тестированием	Может управлять пользователями и правами для модуля управления тестированием. Может просматривать все объекты управления тестированием, редактировать и удалять их.
Тестирование — разработчик	Может просматривать тесты. Может просматривать и редактировать дефекты.
Ведущий специалист по тестированию	Расширенные права на выполнение тестирования. Может просматривать, редактировать и удалять все объекты тестирования.
Пользователь с правом просмотра тестов	Имеет доступ только для чтения к объектам управления тестированием (тесты, тестовые прогоны, дефекты).

Перечень ролей может быть адаптирован в конкретной реализации. Чтобы увидеть фактический перечень ролей, настроенный для конкретной системы, запросите данные из таблицы «userroles» (требуется роль администратора пространства).

Роли, назначенные текущему пользователю, перечислены на странице настроек на вкладке «Security» в самом низу страницы (найдите раздел «My roles»).

6.2 Предопределенные права пользователей

Администрирование системы

Право	Позволяет
Просмотр настроек администрирования	• Запускать, останавливать, перезапускать адаптеры • Просматривать адаптеры интеграции и службы синхронизации с их параметрами • Настраивать параметры пространства • Загружать и удалять лицензию • Задавать настройки авторизации • Приводить состояние БД в соответствие с файловыми конфигурациями • Обновлять текущее пространство из ZIP-файла • Предоставлять группам доступ к пространству • Предоставлять пользователям из некоторой службы доступ к пространству • Просматривать перечень пространств, доступных через службы синхронизации • Принудительно разблокировать службы • Запускать, останавливать, перезапускать службы

Изменение паролей других пользователей	• Позволяет задавать пароли пользователям (с более низким или таким же уровнем привилегий)
Просмотр других пространств	• Просматривать все доступные конфигурации • Просматривать все доступные пространства • Обновлять пространства, метамодель, списки значений из их конфигурации • Изменять уровень логирования • Просматривать логи • Запускать, останавливать, перезапускать пространства • Включать и отключать пространства • Просматривать свойства пространства
Добавление/удаление пространств	• Удалять пространства • Создавать пространства заново • Создавать пространства • Обновлять пространства, метамодель, списки значений из их конфигурации • Запускать, останавливать, перезапускать пространства • Включать и отключать пространства
Резервное копирование пространств	• Создавать резервные копии данных пространства • Восстанавливать данные пространства из резервной копии
Неограниченная работа от имени других пользователей	• Может работать от имени других пользователей (с более низким или таким же уровнем привилегий)
Управление сеансами	• Отключать сеансы всех работающих пользователей • Отправлять текстовые сообщения пользователям
Управление учетными записями входа	• Предоставлять группам доступ к пространству • Предоставлять службе доступ к пространству • Просматривать перечень пространств, доступных через SyncServices • Создавать учетные записи входа и пользователей пространства • Создавать группы и группы пространства • Удалять учетные записи входа и пользователей пространства • Удалять группы и группы пространства • Назначать учетные записи входа пространствам

	• Запрещать учетным записям входа доступ к пространствам • Отменять назначение учетных записей входа пространствам • Приводить учетные записи входа в соответствие с пространствами • Редактировать данные учетных записей входа и пользователей пространства • Редактировать данные групп и групп пространства • Блокировать и разблокировать учетную запись входа
Выполнение серверных скриптов JavaScript	• Может получать доступ к серверной консоли JavaScript (Ctrl+j) и запускать скрипты.

Разработка системы

Право	Позволяет
Включение меню разработки	• Просматривать доработки и инструменты разработчика в главном меню. • Повторно синхронизировать файлы шаблонов • Перезагружать локализации • Обновлять метамодель
Разрешение сохранения компонентов GUI	• Может выполнять операции «Сохранить» и «Сохранить как» в редакторе графического интерфейса и заменять существующие компоненты интерфейса
Разрешение изменения списков значений	• Может просматривать и редактировать все списки значений. Может создавать новые списки значений (LOV).

7 Меню графического интерфейса администрирования системы

Большинство задач администрирования системы можно выполнить на экране «Settings», который открывается после щелчка по имени пользователя в левом верхнем углу окна приложения. Это точка входа для управления пользователями, системой, пространствами и дополнительными модулями.

Существуют панели конфигурации «User», «System» и «This space», позволяющие изменять настройки соответственно для текущего пользователя, всей системы или текущего пространства.

7.1 Настройки пользователя

В этом разделе каждый пользователь может получить доступ к своим личным настройкам приложения, таким как:

- Безопасность, включая смену пароля
- Внешний вид графического интерфейса
- Настройки уведомлений
- Раздел экспорта шаблонов документов

7.1.1 Безопасность

Смена моего пароля

С помощью этой опции вы можете изменить пароль как своей учетной записи, так и учетных записей других пользователей. Это зависит от привилегий, предоставленных вашей учетной записи.

Примечание: функция смены пароля доступна только для локальных учетных записей. Если текущий пользователь подключен к каталогу LDAP/AD/OpenID Connect, сброс пароля должен выполняться в соответствующей системе управления пользователями, например в MS Entra.

Текущий сеанс/выход из системы

Выход из приложения

Мои роли

Отображает перечень ролей, применяемых в настоящий момент к текущему пользователю (назначенных либо непосредственно пользователю, либо группам, в которые он входит). Таблица только для чтения. Изменения могут вносить только администраторы пространства.

7.1.2 Внешний вид

Компоновка меню

Переключение между различными предопределенными вариантами компоновки меню, расположенного в левой части экрана.

Примечание: эта опция недоступна, если она ограничена администраторами (в меню настроек свойств пространства).

Формат времени по умолчанию

Выберите формат времени и даты, который будет отображаться для текущих пользователей. Если формат не задан, будут использованы глобальные значения по умолчанию, установленные администратором пространства. Обратите внимание, что на некоторых экранах могут быть предопределенные форматы даты и времени, на которые это изменение не влияет.

Вложения отображаются как

Выберите тип представления, который будет использоваться для отображения вложений во всей системе. Возможные значения:

- Table — вложения отображаются в виде стандартной таблицы
- Grid — вложения отображаются в виде небольших плиток, организованных в сетку
- Auto — представление по умолчанию. В зависимости от типа сцены или шаблона система автоматически применяет оптимальное представление вложений

Стиль таблиц

Изменение поведения таблиц. Большинство таблиц в системе подчиняется этой настройке. Некоторые таблицы могут иметь пользовательское форматирование и не поддаются настройке.

Возможные варианты:

- Resizable columns — столбцы таблицы с изменяемым размером, ограниченная ширина текста
- Fixed columns — автоматический перенос текста, автоматически вычисляемая ширина столбцов

Размер таблиц

Задание предпочтительного размера таблиц. Большинство таблиц в системе подчиняется этой настройке. Некоторые таблицы могут иметь пользовательское форматирование и не поддаются настройке.

Возможные варианты:

- Normal — большие мониторы и устройства с сенсорным экраном
- Condensed — небольшие мониторы, ноутбуки

Настройки стиля и размера таблиц применяются сразу после изменения. Настройки сохраняются постоянно для каждого пользователя индивидуально.

Сброс всех настроек

Сброс всех ваших персональных настроек в приложении, таких как: сохраненные фильтры для всех объектов, история открытых страниц, вкладок и элементов меню, свернутое состояние левой/правой панели, настройки компоновки меню, формат времени по умолчанию и тип представления вложений.

7.1.3 Уведомления

Настройки уведомлений для ...

Управление способом информирования о новых событиях по электронной почте. Доступны следующие опции:

- Send e-mails with notifications — снятие флажка отключит все письма с уведомлениями для этого пользователя
- Send e-mails for discussion posts — при снятии флажка сообщения чата не будут отправляться по электронной почте
- Send e-mails for my own discussion posts — если флажок установлен, пользователь будет получать по электронной почте уведомления о своих собственных сообщениях в чате
- Send e-mails related to tasks

Уведомления по электронной почте:

Уведомления, отправляемые по электронной почте, информируют вас о новых событиях, таких как создание заявки, решение заявки, назначение заявки исполнителю и т. д. Если снять этот флажок, аналогичные уведомления по-прежнему будут отображаться на панели уведомлений в правой части экрана.

Сообщения обсуждений по электронной почте:

Выберите, хотите ли вы получать уведомления о сообщениях, отправленных участниками обсуждения, а также о своих собственных сообщениях.

Письмо с уведомлением содержит последние пять сообщений обсуждения, поэтому вы можете легко ответить в обсуждении со своего адреса электронной почты.

Отправлять письма о моих собственных сообщениях в обсуждениях

Отправлять письма о сообщениях обсуждения, даже если сообщение было отправлено мной.

Письма, связанные с задачами

Эта опция позволяет выбрать, хотите ли вы получать на свою электронную почту уведомления, связанные с задачами.

7.1.4 Экспорт шаблонов документов

Определите собственные шаблоны для экспорта данных. Документ-шаблон должен быть в формате .docx и может иметь любую необходимую структуру. Документ также должен содержать специальный ключевой текст {{document_body}}, который будет заменен экспортируемыми данными. Из каждой записи по умолчанию экспортируются поля заголовка и описания.

Чтобы добавить новый шаблон, нажмите кнопку «Add template». Для каждого шаблона можно задать:

- Custom label — будет отображаться в меню экспорта Байтим (в основном на сценах с таблицами).
- Visibility settings — определяет, каким пользователям будет доступен шаблон. Возможные варианты:
    - Owner only — только пользователь, добавивший новый шаблон
    - Selected people — выбор конкретных пользователей
    - Everyone — все пользователи
    - Icon — значок
- Export settings — см. следующий снимок экрана

Выберите дополнительные параметры экспорта:

- Export IDs for each record — экспортирует записи с их REFID, который является ссылкой для отслеживания конкурентных изменений и по умолчанию отображается в большинстве таблиц данных.
- Export-related items — для каждой записи также будут экспортированы связанные элементы, если они существуют.
    - Title for related items section — заголовок раздела, который будет содержать экспортированные связанные записи.

Чтобы скачать документ-шаблон, нажмите . Чтобы удалить шаблон, нажмите .

7.1.5 Ключи доступа к API

Пользователи с правом Register API client applications могут создавать собственные токены OAuth2, чтобы внешние приложения могли подключаться к API системы от их имени. Этот пункт меню отображается в пользовательском интерфейсе только при наличии у пользователя соответствующего права. Чтобы фактически вызывать API с помощью зарегистрированного приложения, пользователь также должен иметь право Log in using a REST API. Оба права могут быть предоставлены непосредственно любому пользователю или группе.

На экране Registered applications отображаются все приложения, зарегистрированные текущим пользователем. В списке для каждого приложения показаны его имя, идентификатор клиента, метод аутентификации, области доступа, дата последнего использования и статус активности.

Чтобы зарегистрировать новое приложение, нажмите + Add an application. Откроется диалоговое окно Client application setup со следующими полями:

Name (обязательное) — описательное имя приложения (например, «Calendar»).

Enabled — переключатель, определяющий, активно ли приложение. Новые регистрации по умолчанию включены.

Authorization schemes — метод аутентификации. Выберите OAuth2 для рекомендуемого потока client credentials. Другие методы в этой версии не поддерживаются.

Permitted scopes — область доступа API, к которой приложению разрешен доступ, соответствующая конечным точкам REST API (например, Entity API).

Permitted entities — если выбран Entity API, дополнительно ограничивает, к каким сущностям приложение может обращаться через API (например, «applications, tasks»). Это позволяет тонко управлять данными, которые приложение может читать или изменять.

Обратите внимание, что в отличие от делегированных регистраций уровня администратора, регистрации уровня пользователя не содержат поля «On behalf of» — приложение всегда работает с идентичностью, настройками и правами пользователя, создавшего клиента.

Нажмите Confirm, чтобы сохранить регистрацию. Затем система отобразит диалоговое окно Client application token, содержащее сгенерированные Client ID и Client secret. Секрет клиента отображается только один раз и не может быть восстановлен позднее — обязательно скопируйте и надежно сохраните его перед закрытием диалогового окна.

После этого приложение может использовать поток Client Credentials для получения токена доступа и подключения к службам REST API с использованием выданных идентификатора и секрета клиента.

Каждое зарегистрированное приложение можно деактивировать или удалить с помощью элементов управления в столбце Active списка регистраций. Удаление или отключение учетной записи пользователя автоматически делает недействительными все токены доступа, связанные с зарегистрированными им приложениями.

Чтобы подключить внешнее приложение к REST API с использованием созданных учетных данных, выберите в настройках подключения вашего приложения следующее:

- Authorization Type — OAuth 2.0
- Grant Type — Client Credentials
- Access Token URL: **{url}/oauth/token** *Замените {url} на URL вашего приложения Байтим, например: http://localhost/Байтим/oauth/token*
- Client ID — сгенерированный идентификатор клиента с экрана приложения
- Client Secret — сгенерированный секрет клиента с экрана приложения
- Http Authorization Prefix (необязательно) — Bearer

Байтим поддерживает передачу учетных данных как в заголовке, так и в теле запроса, вы можете использовать любой из вариантов.

7.2 Системные настройки

Этот раздел позволяет управлять:

- пространствами
- системными учетными записями входа
- аутентификацией
- лицензией
- экраном приветствия

7.2.1 Настройки пространства

Пространства создаются на основе определенных конфигураций (например, Service Desk, управление требованиями) и представляют собой базовую часть приложения. В пространствах можно создавать пользователей, настраивать пользовательские параметры и т. д.

При выборе опции «spaces» в левом меню отображается список пространств. В списке пространств можно увидеть ряд полезных сведений, таких как имя, заголовок, конфигурация пространства, отметка времени создания и статус.

На этом экране можно управлять уже созданными пространствами, нажимая значки , или добавлять новые. Синяя точка рядом с именем пространства указывает, что пространство активно.

Контекстное меню предоставляет функции удаления, остановки, перезапуска и отключения пространства.

- Delete — действие удаления полностью стирает выбранное пространство, включая его записи, внешние подключения... Обратите внимание, что системное пространство (System) удалить нельзя.
- Stop — остановленное пространство будет недоступно пользователям. После перезапуска сервера пространство запустится снова, либо его можно запустить вручную, нажав значок контекстного меню и выбрав опцию Start.
- Restart — используйте эту опцию для обновления конфигурации пространства.
- Disable — отключенное пространство будет недоступно пользователям. Кроме того, пространство не будет запущено после перезапуска сервера. Чтобы сделать пространство активным, нажмите значок контекстного меню и выберите опцию Enable.

Новое пространство можно добавить, нажав кнопку «Create new space». В открывшемся окне можно задать имя нового пространства, которое рекомендуется сделать уникальным и которое должно указывать на используемую конфигурацию. Далее можно выбрать предопределенную конфигурацию, на основе которой будет создано пространство. После настройки всех параметров нажмите кнопку «Create and configure space».

Если пользователю назначено более одного пространства, он может переключаться между пространствами в контекстном меню «Switch space», щелкнув свое полное имя в левом углу экрана. Обратите внимание, что это меню вообще не отображается, если пользователю доступно только одно пространство.

7.2.2 Системные учетные записи входа

Создание новых учетных записей входа для пользователей, а также просмотр существующих учетных записей и управление ими.

Чтобы создать новую учетную запись входа, нажмите кнопку «Add login». В открывшемся окне необходимо заполнить все требуемые сведения в разделе BASIC INFORMATION, а затем в разделе SECURITY SETTINGS назначить учетную запись пространству и решить, предоставлять ли административные права для выбранного пространства. Кроме того, для текущей учетной записи можно задать права System admin, которые позволят пользователю управлять конфигурацией системы в разделе System настроек администрирования. Учетные записи с правами System admin обозначаются красным значком в списке учетных записей. Обратите внимание, что для пользователей без прав System admin раздел системных настроек не отображается.

Если новая учетная запись после создания не отображается в списке учетных записей, нажмите значок обновления .

При добавлении новой учетной записи входа также создается новый пользователь пространства с полным именем, указанным в учетной записи. Чтобы перейти к пользователю, откройте раздел Users на панели настроек. Чтобы ознакомиться с концепцией работы пользователей, перейдите в раздел «Пользователи»

.

Нажав значок контекстного меню, вы можете:

- Назначить пространства
- Заблокировать
- Изменить пароль
- Разблокировать
- Удалить

Чтобы назначить новое пространство, выберите опцию «Assign spaces» и в отобразившемся окне отметьте пространства, которые нужно сделать доступными для этой учетной записи.

Чтобы заблокировать пользователя, выберите опцию «Lock» в контекстном меню. Заблокированные пользователи не могут войти в приложение. Учетная запись также блокируется, если пользователь не менее 10 раз вводит неверный пароль при попытке

входа в Байтим. Любого заблокированного пользователя можно разблокировать, выбрав опцию «Unlock».

Чтобы изменить пароль учетной записи входа, выберите опцию «Change password» и введите новый пароль.

Чтобы удалить несколько записей одновременно, выберите нужные записи и нажмите кнопку «Delete», расположенную над таблицей.

Учетные записи входа можно упорядочить, щелкая заголовки столбцов. Также можно применить пользовательский фильтр, чтобы скрыть ненужные учетные записи. Пользовательский фильтр позволяет отфильтровать список по выбранным свойствам.

Редактирование учетной записи входа

Щелчок по учетной записи в списке открывает окно с ее подробными сведениями:

Во всплывающем окне сведений об учетной записи можно редактировать следующие атрибуты:

- Login name — имя, используемое при входе в Байтим
- Full name — полное имя пользователя, отображаемое во всем приложении
- E-mail — может использоваться для получения уведомлений
- Telephone — номер телефона пользователя
- System admin — предоставление/снятие права System admin для учетной записи
- Second-factor token secret — показывает, настроен ли у пользователя токен двухфакторной авторизации

После редактирования атрибутов нажмите кнопку «Save», чтобы применить изменения. Если пользователь назначен какому-либо активному пространству, основные атрибуты будут распространены на пользователя в этом пространстве.

7.2.3 Аутентификация

Могут быть настроены следующие сценарии аутентификации:

- *Local only — аутентификация используется только для локальных пользователей, созданных в системе*
- *External — аутентификация используется для проверки пользователей, хранящихся в Active Directory, подключенном к приложению. Этот вариант может использоваться только в сочетании с локальной аутентификацией. Для использования внешней аутентификации должны быть настроены службы синхронизации каталога пользователей.*

- *Local then External — аутентификация. При входе пользователя система сначала пытается аутентифицировать его по локальному списку пользователей, а затем ищет его в Active Directory, либо наоборот (External then local).*

Пользователям, управляемым локально, разрешено восстанавливать доступ к системе при утере пароля путем получения по электронной почте ссылки одноразового доступа. Функция может быть включена в системных настройках авторизации, а текст письма может быть изменен администраторами.

Чтобы добавить службы синхронизации каталога пользователей (которые будут использоваться для внешней аутентификации), нажмите кнопку «Add service» и заполните все требуемые сведения во всплывающем окне.

Чтобы удалить службу, нажмите значок контекстного меню и выберите опцию удаления.

Перед добавлением служб синхронизации каталога пользователей необходимо создать внешний адаптер, который будет использоваться в службе. См. главу «Внешние подключения», чтобы узнать, как настроить адаптер.

7.2.3.1 Добавление новой службы LDAP

После создания и настройки адаптера LDAP в разделе внешних подключений его можно использовать для добавления новой службы LDAP. В службе необходимо задать имя, выбрать режим и адаптер, задать интервал и назначить службу какому-либо пространству.

Существует два режима:

- Bulk (по умолчанию) — синхронизация всех пользователей в соответствии с фильтром, заданным в параметрах адаптера LDAP (база поиска пользователей, фильтр пользователей). В этом режиме также синхронизируются все группы.
- Lazy — синхронизация пользователей, которые входили в систему хотя бы один раз, и всех групп.

В поле интервала задайте значение времени, которое будет использоваться для запуска синхронизации.

Кроме того, можно задать точное время ежедневного запуска синхронизации LDAP и сохранить это значение в атрибуте Align Job Time. Используйте эту опцию, если в конфигурации LDAP установлены флажки Remove Users или Remove Groups, см. главу «Внешние подключения». Эта настройка приведет к тому, что каждый пользователь Байтим, не соответствующий настройкам фильтра LDAP, будет помечен как удаленный во время синхронизации. Это означает, что пользователь не исчезнет из записей, но не

будет отображаться в адресной книге; кроме того, станет невозможно назначать ему новые записи или входить в систему от его имени.

Выберите пространства, доступ к которым будет разрешен пользователям, созданным данной синхронизацией.

Нажмите «Save», чтобы создать службу. Будет отображен статус службы, и через некоторое время пользователи и группы появятся в списках.

Примечание: в любой момент позже можно добавить дополнительные пространства к любой службе синхронизации. Для этого откройте серверную консоль JavaScript (Ctrl+J) и выполните следующий скрипт:

```
admin.setAccess4Service2Space(adapter_ID, “space_name”, true);
```

- **adapter_ID можно узнать, наведя курсор мыши на адаптер LDAP в списке служб синхронизации каталога пользователей.**
- **space_name — имя пространства, которое должно использовать адаптер. (Например, пространство «name», пользователи которого должны аутентифицироваться через сервер LDAP, настроенный в пространстве «system».)**
- True означает, что доступ к службе для заданного пространства должен быть включен

Некоторые службы LDAP могут иметь дополнительные атрибуты, которые можно сопоставить с полями пользователей Байтим. Стандартное сопоставление полей адаптировано под MS Active Directory и может не работать с другими серверами, такими как OpenLDAP, FreeIPA и т. д. Администраторы могут изменить сопоставление с помощью скрипта. Например, чтобы сопоставить поле LDAP «title» с атрибутом «position» в таблице «users» для адаптера LDAP с guid 1, выполните следующее:

```
var endpointId = 1; // adapter endpoint here

var e = new Entity('integration_endpoints');
e.get(endpointId); // Get current configuration
var rec = e.records[0];
var settings = JSON.parse(rec.settings); // Get settings field value

// Байтим field 'position' <-- LDAP field 'title'
settings['userfield:position'] = "title";  // Replace mapping by required values
e.set(endpointId, {settings:JSON.stringify(settings)});  // Store settings back
```

Стандартная таблица сопоставления полей:

Пользователи

Имя поля LDAP	Настройка
l	userfield:city
countryCode	userfield:country
department	userfield:department
mail	userfield:email
employeeID	userfield:employee_id
givenName	userfield:firstName
sn	userfield:lastName
sAMAccountName	userfield:login
manager	userfield:manager
mobile	userfield:mobile
physicalDeliveryOfficeName	userfield:office
postOfficeBox	userfield:pobox
description	userfield:position
postalCode	userfield:postcode
st	userfield:state
streetAddress	userfield:street
telephoneNumber	userfield:tel

Группы

Имя поля LDAP	Настройка
mail	groupfield:email
name	groupfield:fullname

Учетные записи входа

Имя поля LDAP	Настройка
sAMAccountName	userfield:login

7.2.3.2 Аутентификация Kerberos

Предварительное условие

Должно быть настроено системное пространство:

Адаптер LDAP — см. главу «Службы синхронизации каталога пользователей» — см. главу «Добавление новой службы LDAP».

Действия

1. Настройка Active Directory на сервере Windows:
    a) Создайте сервисную учетную запись

    Создайте в Active Directory непривилегированную сервисную учетную запись с непросроченным паролем.

    например, SVC_HTTP_MYSERVER с паролем $ServiceAccountSecret

    b) Привяжите SPN службы к учетной записи с помощью утилиты Windows setspn. Выполните команду в командной строке Windows:

    setspn -U -S HTTP/mycompany.com SVC_HTTP_MYSERVER

2. Настройка Байтим:

    Задайте пароль учетной записи SPN в конфигурации адаптера LDAP равным $ServiceAccountSecret. Оставьте это поле пустым, если хотите использовать файл keytab (подробнее см. главу «Файл keytab»).

    a) Включите аутентификацию Kerberos — перейдите в Settings, Authentication, Kerberos authentication

3. Настройка браузера клиента:

    Браузер клиента должен быть настроен так, чтобы доменное имя системы было включено в список доверенных сайтов.

    a) IE — Свойства браузера, Безопасность, Местная интрасеть, Сайты, Дополнительно — добавьте веб-сайт в зону «Местная интрасеть»

    b) Chrome — использует настройки из IE

    c) Firefox

        i. Перейдите по адресу about:config в Firefox. Нажмите кнопку «I'll be careful, I promise!»:

        ii. Задайте параметры:

            1. network.automatic-ntlm-auth.trusted-uris

            2. Укажите имена хостов или доменов, разделенные запятыми.

При успешной настройке в логах сервера (TOMCAT_HOME/catalina.out) должны присутствовать следующие сообщения

```
@ INFO  sec.VerboseFormAuthFilter - Sending Negotiate challenge - Kerberos settings is enabled
@ INFO  sso.KerberosValidator - Found valid kerberos ticket for user Administrator@COMPANY.LOCAL (SPN=HTTP/mycompany.com)
```

Файл keytab

Аутентификация SSO в Байтим также поддерживает файлы keytab, которые могут использоваться вместо пароля учетной записи SPN. Для настройки keytab выполните следующие действия:

1. Разместите сгенерированный файл keytab на сервере по пути $BYTEAM_PATH/sso.
2. Назначьте файл адаптеру LDAP в поле Keytab file. В раскрывающемся списке во всплывающем окне LDAP должны отображаться файлы, сохраненные по пути из предыдущего шага. (Перейдите к главе «Внешние подключения», чтобы узнать, как настроить адаптер LDAP.)

Устранение неполадок

При настройке аутентификации Kerberos могут возникнуть следующие проблемы:

1. При открытии URL системы в браузере отображается всплывающее окно встроенной аутентификации
    a. Домен системы не добавлен в зону «Местная интрасеть» (доверенные сайты). Клиент должен добавить веб-сайт в зону «Местная интрасеть» либо нажать «Отмена», чтобы перейти на страницу входа (вход по-прежнему можно выполнить вручную, но это не рекомендуется)
2. Отсутствует тикет Kerberos — ошибка настройки на шаге 1 (браузер запрашивает тикет Kerberos, например для SPN=HTTP/mycompany.com, но AD не возвращает тикет Kerberos для этого SPN):
    a. Лог сервера (TOMCAT_HOME/catalina.out) содержит следующие сообщения:

```
@ INFO  sec.VerboseFormAuthFilter - Sending Negotiate challenge - Kerberos settings is enabled
@ INFO  sec.Authenticator - Not kerberos ticket --> ignore
```

3. Неверный пароль учетной записи SPN в адаптере LDAP Байтим:
    a. Лог сервера (TOMCAT_HOME/catalina.out) содержит следующие сообщения:

```
@ INFO  sso.KerberosValidator - Invalid ticket for HTTP/mycompany.com@COMPANY.LOCAL: java.security.PrivilegedActionException: GSSException: Failure unspecified at GSS-API level (Mechanism level: Checksum failed)
```

7.2.3.3 Настройка многофакторной аутентификации

Многофакторная аутентификация (MFA) обеспечивает дополнительный уровень безопасности, требуя ввода второго одноразового пароля каждый раз, когда пользователь входит в систему со своим паролем.

По умолчанию MFA отключена, поскольку она требует дополнительных действий от каждого пользователя по настройке устройства для генерации токена второго фактора.

Настройки MFA являются глобальными для приложения и не могут быть включены/отключены для отдельного пространства, поскольку последовательность входа выполняется до того, как пользователь будет назначен конкретному пространству или пространство станет известно.

MFA не влияет на REST API.

При использовании внешней аутентификации SSO, например Open ID, MFA включать не следует, поскольку процесс запроса и проверки второго фактора управляется внешним поставщиком аутентификации.

Чтобы включить MFA:

1. Перейдите в раздел Settings/Authentication/MFA settings и установите флажок «Enable multi-factor authentication».
2. Выберите поставщика кодов: SMS или OTP-устройство
3. Настройте остальные атрибуты согласно подсказкам на экране

Пример конфигурации:

Когда MFA включена, после успешной авторизации по паролю пользователям будет предложено ввести одноразовый пароль (OTP). Способ получения OTP различается в зависимости от настроенного поставщика:

- **Поставщик SMS: SMS-сообщение отправляется на номер мобильного телефона пользователя согласно его данным в таблице «users». Для продолжения пользователь должен ввести код из сообщения**
- **Поставщик OTP-устройства: пользователь должен иметь физический доступ к OTP-устройству или программному OTP-токену, чтобы сгенерировать следующее число последовательности и ввести его в предоставленное поле. Числа изменяются каждые 30 секунд**

Для устройств OTP-токенов предусмотрен дополнительный шаг: после первого успешного входа пользователям предлагается настроить свое OTP-устройство. Пользователь не может продолжить работу с приложением, пока этот шаг не будет завершен.

Каждому пользователю будет представлен следующий экран:

Пользователи могут использовать любое приложение OTP, например MS Authenticator, Authy, Google Authenticator и т. д., которое обычно можно загрузить из магазина приложений.

Чтобы избежать регистрации недействительного или неработающего OTP-устройства, а также предотвратить проблемы при ошибочном вводе кодов, пользователи должны ввести первый сгенерированный устройством пароль для успешного завершения процесса регистрации.

При следующем входе после успешной проверки пароля появится следующий запрос:

Пользователь вводит действительный одноразовый пароль из SMS-сообщения, отправляемого сразу после появления окна, либо из устройства-генератора OTP.

Если правильный код не будет введен после определенного числа попыток, заданного в настройках MFA, учетная запись будет заблокирована. Обратите внимание, что эта настройка отличается от максимального числа попыток ввода неверного пароля, которое также действует в этом сценарии.

Когда MFA включена, администраторы могут сбросить OTP-токен на странице учетной записи пользователя. Перейдите в Settings/System Logins, выберите и щелкните учетную запись в таблице. Окно учетной записи содержит дополнительный раздел для MFA:

Нажмите «Reset currently assigned secret», чтобы сбросить сохраненный в настоящий момент секрет и позволить пользователю зарегистрировать OTP-устройство заново.

Для сценария на основе SMS важно наличие настроенного SMS-адаптера в пространстве «system». SMS-адаптер должен быть включен как активный в настройках коммуникаций (Communication).

Экспериментируйте с настройками MFA осторожно, поскольку они затрагивают и учетные записи администраторов. При неверных настройках администраторы могут лишиться возможности войти в систему.

7.2.4 Регистрация лицензионного ключа

Байтим проверяет наличие лицензионного ключа при попытке входа пользователей или при запуске пространства. Администратор всегда может войти в пространство «system» без действительной лицензии. Для получения действительного лицензионного ключа следует выполнить следующую последовательность действий:

- Скопируйте аппаратный ключ из окна конфигурации «License»
- Отправьте аппаратный ключ своему поставщику программного обеспечения или в службу поддержки для получения лицензионного ключа
- Введите полученный лицензионный ключ обратно в окно настроек
- Перезапустите приложение, чтобы запустились все пространства (либо можно запустить каждое пространство вручную без перезапуска системы)

В этом разделе настроек можно просмотреть сведения о вашей лицензии, а также загрузить новую лицензию, нажав кнопку «Load new license». Чтобы удалить лицензию, нажмите кнопку «Remove license».

Лицензионные ключи могут быть ограничены условиями договора. Например, демонстрационные установки имеют ключи, ограниченные по времени. Как правило, ключ для производственной среды не ограничен по времени. Если срок действия ключей истекает, система продолжит работу до следующего перезапуска без какого-либо влияния на пользователей. Неограниченные ключи не требуют дальнейшего обслуживания в течение всего срока эксплуатации системы.

Если система переносится на другое оборудование, необходимо сгенерировать новый лицензионный ключ по той же процедуре, описанной выше.

Фактическое количество пользователей в динамике по модулям системы можно просмотреть в сущности «moduleusage».

Эта сущность содержит данные об использовании по каждому пространству. Количество пользователей в сети измеряется каждые 10 секунд, а среднее значение сохраняется каждые 10 минут. Существует 3 вида записей:

- Module usage — количество работающих в сети пользователей, использующих указанный модуль. Лицензируемые модули зависят от конкретного продукта и установки
- Space usage — общее количество работающих в сети пользователей в текущем пространстве
- Softshell usage — общее количество работающих в сети пользователей минус количество пользователей, использующих какой-либо из лицензируемых модулей (первый тип). Это значение означает количество пользователей, использующих функции платформы, но не какой-либо конкретный лицензируемый модуль

7.2.4.1 Аппаратный ключ и изменения инфраструктуры

Для защиты интеллектуальной собственности лицензионный ключ напрямую связан с некоторыми элементами аппаратной инфраструктуры и сетевым адресом (IP или имя хоста) сервера, на котором установлено приложение.

Следующие изменения не должны влиять на аппаратный ключ:

- Количество ядер в процессорах
- Изменения параметров ядер ЦП
- Объем и другие параметры жестких дисков
- Объем оперативной памяти
- Параметры операционной системы

Точный перечень элементов, которые могут влиять на аппаратный ключ, может различаться в зависимости от платформы.

Любое общее изменение конфигурации того же сервера, кроме перечисленных выше, не должно требовать обновления лицензионного ключа.

Кроме того, генерация новой лицензии может потребоваться в следующих ситуациях:

- Восстановление приложения в резервном расположении — резервный сервер должен иметь собственный лицензионный ключ
- Перенос приложения на другой сервер

Если вы планируете перенести сервер на другую машину или изменить значимые параметры, перечисленные выше, убедитесь, что имеется достаточно времени для запроса и выпуска новых лицензионных ключей.

7.2.5 Экран приветствия

Раздел экрана приветствия позволяет настроить сообщения, которые будут отображаться на странице входа для всех пользователей. Конфигурация применяется ко всем созданным пространствам приложения, поскольку страница входа является общей для всех созданных в приложении конфигураций.

Для страницы входа можно задать следующие сообщения:

- Welcome message — по умолчанию отображается под логотипом, размещенным на странице входа
- Footer notes — по умолчанию отображаются под кнопкой «Sign in» на странице входа

Результат настройки сообщений показан на следующем снимке экрана:

Параметры выбора языка или логотип могут быть изменены с помощью настроек файла default.properties. Изменение этих настроек требует перезапуска системы.

7.3 Это пространство

Раздел «Это пространство» позволяет управлять настройками текущего пространства:

- управлять пользователями в текущем пространстве
- добавлять внешние подключения
- настраивать общие параметры пространства
- добавлять шаблоны уведомлений
- управлять редактором календарей

7.3.1 Настройки пространства

Этот раздел позволяет администраторам редактировать общие настройки текущего пространства.

Здесь можно задать:

Язык и региональные параметры

- Предлагаемый язык пользовательского интерфейса: определите перечень доступных языков, из которых пользователи могут выбирать. Если пользователь не выбрал конкретный язык, будет применен язык по умолчанию.
- Язык пользовательского интерфейса по умолчанию: выберите основной язык интерфейса, который будет отображаться новым пользователям по умолчанию.
- Единица валюты по умолчанию: выберите единицу валюты по умолчанию, которая будет использоваться во всех валютных полях системы.
- Системный календарь по умолчанию: выберите системный календарь для расчета длительности проектов и задач.

Форматы

- Разделитель десятичной части по умолчанию: задает разделитель для чисел с плавающей запятой (запятая или точка).
- Формат даты и времени по умолчанию: предлагает различные варианты с разными разделителями и форматами, включающими день, месяц, год и время с секундами или без них.

Меню навигации

- Меню пользователя по умолчанию: задайте меню, которое будет отображаться пользователям по умолчанию.
- Раскрытие разделов меню навигации: позволяет выбрать между настройками «Collapse other sections when a new section is expanded» и «Keep all sections expanded».
- Разрешить пользователям выбирать меню: определяет, могут ли пользователи переключаться между различными конфигурациями меню.
- Отображать поле поиска в разделе меню: включает или отключает поле поиска в меню навигации.

Пользовательский интерфейс

- Отключить системную справку: при включении подсказки системной справки отключаются для всех пользователей.

- Вложения отображаются как: выберите формат отображения вложений по умолчанию, например «Grid», «Table» или «Auto».
- Предлагать сохранять вставленные изображения как вложения: позволяет пользователям сохранять изображения как вложения при вставке их в текстовый редактор вместо встраивания в текст.

Идентификация пространства

- Заголовок пространства: введите пользовательский заголовок пространства, который будет отображаться в строке заголовка веб-браузера.
- Цветовая полоса пространства: выберите цветовую полосу, отображаемую в верхней части экрана для визуального выделения этого пространства.
- Системный URL: введите URL или используйте текущий. Этот URL используется для исходящих писем и внешних ссылок и должен быть доступен из сети.

7.3.2 Пользователи

В разделе «Users» отображается список всех пользователей, которым назначено текущее пространство. Этот список можно упорядочить по всем атрибутам, таким как ID, полное имя и т. д. Каждой записью можно управлять, нажав значок . В отобразившемся контекстном меню можно удалять записи, а также изменять тип записи (доступные типы записей перечислены ниже). Чтобы удалить несколько записей одновременно, выберите нужные записи и нажмите кнопку «Delete», расположенную над таблицей.

Обратите внимание, что добавление записи любого типа создает запись локального пользователя. Добавлять связанные записи для внешних пользователей, синхронизированных из Active Directory, невозможно.

При создании локального пользователя войти в систему от его имени будет невозможно. В приложении локальные пользователи ведут себя как виртуальная сущность. Локальные пользователи могут быть, например, связаны с внешними пользователями из Active Directory или других внешних приложений. По этим причинам функциональность добавления пользователей рекомендуется использовать только для создания групп, команд и т. п.

Конфигурации внешних пользователей можно изменить на вашем сервере LDAP.

При создании новой записи можно выбрать один из нескольких типов записей:

- Подразделение
- Персона
- Команда
- Виртуальная команда
- Группа
- Компания

- Внешняя система

Также можно применить пользовательский фильтр , который не допускает появления ненужных записей в списке. Записи можно фильтровать по их имени и виду.

Синяя точка рядом с полным именем пользователя указывает на его статус присутствия в сети.

Чтобы изменить свойства пользователя, щелкните его полное имя. Во всплывающем окне отображаются сведения о выбранном пользователе. Здесь можно изменить информацию о пользователе, просмотреть его группу и назначенные роли.

Содержимое вкладки GENERAL разделено на следующие разделы:

- *GENERAL — содержит основные сведения о пользователе, такие как ID, полное имя, компания и т. д.*
- *CONTACTS — содержит контактные данные пользователя, такие как e-mail, телефон, мобильный телефон, адрес, город и т. д.*
- *OTHER INFORMATION — здесь можно увидеть руководителя пользователя, его права, роли и территорию.*

Территория определяет, какие записи пользователь может видеть в приложении:

- Пользователи территории Internal могут видеть все записи, для которых видимость установлена на территории Internal, Customer и Subcontractor.
- Пользователи территории Customer могут видеть записи, доступные для территорий Customer и Subcontractor.
- Пользователи территории Subcontractor могут видеть только записи с видимостью, установленной для территории Subcontractor.

На данный момент функциональность территорий доступна для управления дефектами. Там можно задать территорию для каждого дефекта, и в соответствии с приведенным выше правилом запись будет видна конкретным пользователям.

На вкладке GROUPS можно увидеть все назначенные пользователю группы, а также добавить пользователей в новую группу. Подробнее см. в главе Add user to group.

Вкладка ROLES содержит информацию о ролях, назначенных пользователю, и о ролях групп, в которые входит пользователь.

7.3.2.1 Создание новой группы

Чтобы создать группу, нажмите кнопку «Add group», заполните все необходимые сведения, включая права и роли, и нажмите кнопку «Save».

Кроме того, можно выбрать режим уведомлений (Notification mode), который доступен только для групп и включает следующие варианты:

- *Direct — этот контакт группы означает, что уведомление будет отправлено на e-mail, указанный в свойствах группы.*
- *Manager of this group — означает, что уведомление будет отправлено руководителю группы, заданному в свойствах группы.*
- *All members of this group — означает, что уведомление будет отправлено на адреса электронной почты всех пользователей, входящих в группу.*

На вкладке GROUPS можно увидеть все назначенные группы, добавить запись в новую группу или отменить назначение.

Вкладка ROLES отображает все роли, назначенные записи.

На вкладке GROUP MEMBERS можно увидеть список пользователей, входящих в группу.

7.3.2.2 Добавление пользователя в группу

Щелкните запись пользователя, и на вкладке GROUPS в окне свойств пользователя вы сможете добавить пользователя в группы, нажав кнопку «Add to groups», либо отменить назначение пользователя группе, нажав значок .

После нажатия кнопки «Add to groups» откроется окно со списком всех групп. В нем можно выбрать одну или несколько групп. После выбора нажмите кнопку подтверждения. Выбранные группы затем появятся в таблице со всеми назначенными группами.

7.3.3 Роли пользователей

В этом разделе можно просматривать все доступные в системе роли пользователей и управлять ими.

Добавить новую роль можно, нажав кнопку «Add».

В отобразившемся окне заполните следующие сведения:

- *Title — название роли, которое будет отображаться во всей системе.*
- *Permissions – назначьте новой роли доступные права. Перечень прав приведен в этой главе. Подробнее см. главы «Права и роли» и «Управление доступом».*
- *Key — значение, используемое как уникальный идентификатор роли. Его можно оставить без изменений или задать другие уникальные значения.*

- *Description — введите описание роли. Например, какие действия роль может выполнять в системе.*

После настройки всех параметров нажмите кнопку «Save». Вновь созданная роль появится в таблице ролей пользователей.

Если какие-либо роли больше не используются, их можно удалить, нажав значок , расположенный рядом с каждой записью в таблице.

7.3.4 Делегированные ключи доступа к API

Администраторы пространства могут создавать токены OAuth2, чтобы внешние приложения могли подключаться к API системы. OAuth2 является предпочтительным методом интеграции внешних приложений и значительно безопаснее использования учетных данных (логина и пароля) с базовой аутентификацией.

На экране Delegated application registrations отображаются все зарегистрированные внешние приложения и их свойства, включая имя приложения, идентификатор клиента, делегированного пользователя, от имени которого работает приложение, метод аутентификации и предоставленные области доступа.

Чтобы зарегистрировать новое приложение, нажмите + Add new application access. Откроется диалоговое окно Delegated client application setup со следующими полями:

Name (обязательное) — описательное имя внешнего приложения (например, «Calendar APP»).

Client ID — назначается системой автоматически после подтверждения регистрации.

Enabled — переключатель, определяющий, активно ли приложение. Новые регистрации по умолчанию включены.

On behalf of (обязательное) — пользователь системы, от имени которого приложение будет проходить аутентификацию и работать. Делегированный пользователь должен существовать, быть активным и иметь действительную учетную запись входа в систему. Все действия, выполняемые приложением через API, будут осуществляться с правами и учетной идентичностью этого пользователя.

Authorization schemes — метод аутентификации. Выберите OAuth2 для рекомендуемого потока client credentials OAuth2.

Permitted scopes — области доступа API, к которым приложению разрешен доступ. Выберите All scopes для предоставления неограниченного доступа либо выберите отдельные области из раскрывающегося списка. Доступные области включают Entity API, Remote functions calling, Attachments download, Images download и Data export to document format. Области соответствуют соответствующим конечным точкам REST API (описаны далее в руководстве по REST API). В качестве рекомендации по безопасности следует ограничивать области только тем, что требуется приложению.

Права

Применяемые права будут подмножеством разрешенных областей доступа и прав, назначенных пользователю. Например, если пользователь может видеть только некоторые задачи, отфильтрованные фильтром прав просмотра, то установка области

entity[tasks] предоставит ему доступ только к конечной точке Entity REST, только к таблице «tasks» и только с применением его фильтров согласно правам просмотра. Если сущность не указана, пользователь может обращаться ко всем сущностям в соответствии со своими правами. То же относится к операциям создания, обновления и удаления.

Нажмите Confirm, чтобы сохранить регистрацию. Затем система отобразит диалоговое окно Client application token, содержащее сгенерированные Client ID и Client secret. Секрет клиента отображается только один раз и не может быть восстановлен позднее — обязательно скопируйте и надежно сохраните его перед закрытием диалогового окна.

После этого приложение может использовать поток Client Credentials для получения токена доступа и подключения к службам REST API с использованием выданных идентификатора и секрета клиента.

Каждое зарегистрированное приложение можно деактивировать или удалить с помощью элементов управления в столбце Active списка регистраций.

Чтобы подключить внешнее приложение к REST API с использованием созданных учетных данных, выберите в настройках подключения вашего приложения следующее:

- Authorization Type — OAuth 2.0
- Grant Type — Client Credentials
- Access Token URL: **{url}/oauth/token** *Замените {url} на URL вашего приложения Байтим, например: http://localhost/Байтим/oauth/token*
- Client ID — сгенерированный идентификатор клиента с экрана приложения
- Client Secret — сгенерированный секрет клиента с экрана приложения
- Http Authorization Prefix (необязательно) — Bearer

Байтим поддерживает передачу учетных данных как в заголовке, так и в теле запроса, вы можете использовать любой из вариантов.

7.3.5 Настройки жизненного цикла

В этом разделе можно настроить основные параметры функций, основанных на жизненном цикле.

Доступны следующие настройки:

- *Show unavailable lifecycle buttons — если этот флажок установлен, кнопки действий в записях будут отображаться как неактивные, то есть пользователь видит все доступные действия для перехода статуса записи, но сможет нажать только те, которые соответствуют его ролям. Если флажок снят, недоступные кнопки действий отображаться не будут. Эта настройка может быть переопределена в конфигурации конкретного жизненного цикла*

- *On manual step transitions (superusers) ask for comments — ручной переход между шагами доступен только пользователям, назначенным суперпользователями (Superuser) для жизненного цикла, что настраивается в редакторе жизненных циклов. Можно задать следующие варианты:*
    - Do not ask — при выполнении ручного перехода у пользователя не будет запрашиваться комментарий
    - Ask – optionally — при выполнении ручного перехода пользователь может ввести комментарий
    - Ask – mandatory — при выполнении ручного перехода пользователь обязан ввести комментарий
- Кнопки действий жизненного цикла будут скрываться по:
    - Outlet types — если большое количество кнопок не вписывается в ширину экрана, часть кнопок будет скрыта, начиная с тех, нажатие которых менее вероятно, в соответствии с типом кнопки
    - Outlets ordering — то же, что и выше, но приоритет скрытия кнопок определяется непосредственным порядком выходов (outlets): первыми скрываются кнопки последнего выхода
- Отслеживание комментариев к изменениям в редакторе жизненных циклов
- Эта настройка может использоваться для документирования изменений, вносимых администраторами в определения жизненных циклов в сложных средах, чтобы понимать, кто внес то или иное конкретное изменение (журнал изменений). Журнал хранится в жизненном цикле и сохраняется при экспорте и импорте определения в файл. Возможные значения:
    - Disabled — никогда не запрашивать комментарий к изменению жизненного цикла
    - Enabled - optional comments — пользователи могут при желании указать комментарий к изменению
    - Enabled - mandatory comments — пользователи обязаны указывать комментарии к любому изменению жизненного цикла

7.3.6 Настройки задач

В этом разделе можно настроить общие параметры задач.

- Кто может быть выбран получателем задачи

Каждая задача может быть назначена пользователю, ответственному за ее решение. С помощью этой опции можно выбрать, могут ли задачи назначаться только пользователям или как пользователям, так и группам.

- Только пользователи/группы с ролью

Ограничение получателей задач по системной роли. В этом случае при назначении задачи для выбора будут доступны только пользователи/группы с выбранными ролями.

- Получатель обязателен

Установите этот флажок, если хотите сделать получателя задачи обязательным значением.

- Срок выполнения обязателен

Установите этот флажок, если хотите сделать срок выполнения задачи обязательным значением.

- Показывать выбор срока выполнения с открытой панелью времени

Открывать панель выбора времени при выборе срока выполнения задачи

- Показывать список задач на панели совместной работы

Панель совместной работы по задачам (справа), если она видна текущему пользователю, будет отображать в самом верху кнопку открытия таблицы всех задач.

- Пользователи могут указывать контекст при создании новых задач

Контекст задачи, например связанный проект, может редактироваться пользователями непосредственно при создании новой задачи. Отключение этой опции устанавливает более строгие правила в отношении того, что пользователи могут изменять при создании задачи.

- Разрешить публикацию сообщений в журнале истории задачи

Вкладка «History» задачи может использоваться для публикации любых сообщений пользователем, что позволяет вести обсуждения вокруг задачи. Если функция не включена, на вкладке отображаются только системные сообщения, создаваемые действиями жизненного цикла

- Создание подзадач

Таблица позволяет задать сопоставление полей родительской задачи с полями вновь создаваемой дочерней задачи. Столбец исходного поля (Source field) содержит имя поля в таблице задач, которое будет скопировано в поле дочерней задачи, выбранное в столбце «Target field». Например, если приоритет задачи должен распространяться на дочерние задачи, нажмите кнопку «Add mapping rule» и выберите «priority» в оба поля.

7.3.7 Настройки обсуждений

В этом административном разделе можно настроить глобальные параметры обсуждений.

Как видно на рисунке выше, доступные параметры и их значения следующие:

Параметр	Значение
Кто может изменять настройки обсуждения:	владелец, участники, все
Кто может добавлять новых участников:	владелец, участники, все
Кто может удалять участников:	владелец, участники, все
Кто может публиковать сообщения в публичных обсуждениях:	участники, все
Публикация сообщения в обсуждении автоматически добавляет участника:	true / false

Владелец — пользователь, создавший обсуждение

Участники — все пользователи, которые могут публиковать сообщения в обсуждении и присутствуют в списке участников во всплывающем окне обсуждения. Любого участника можно удалить из обсуждения.

- Кто может изменять настройки обсуждения

Определяет, какие пользователи могут в дальнейшем изменять настройки созданного обсуждения. Доступные настройки обсуждения:

  - Пометить обсуждение как приватное (только участники видят обсуждение и только они могут публиковать сообщения)
  - Пометить обсуждение как решенное (закрыть обсуждение)
  - Переименовать обсуждения...
  - Добавить участников
  - Поделиться...

- Кто может добавлять/удалять участников

Определяет, какие пользователи могут добавлять/удалять участников обсуждения.

- Кто может публиковать сообщения в публичных обсуждениях

Определяет, какие пользователи могут добавлять/удалять участников обсуждения. Публичные обсуждения доступны каждому пользователю системы. С помощью этой настройки можно выбрать, какие пользователи смогут также публиковать сообщения в публичных обсуждениях.

- Публикация сообщения в обсуждении автоматически добавляет участника

Установите этот флажок, если хотите, чтобы каждый пользователь, публикующий сообщение в обсуждении, также становился его участником.

- После настройки всех параметров нажмите кнопку «Apply changes», чтобы применить конфигурацию.

Используйте кнопку «Reset to defaults», чтобы применить заводские настройки обсуждений.

7.3.8 Коммуникации

Страница настроек коммуникаций определяет способ распространения системных уведомлений. Она связывает адаптеры, обеспечивающие технологический уровень коммуникаций, с каналами сообщений, которые выбираются при отправке конкретного уведомления.

Для доступа к правилам обработки почты и управления ими нажмите кнопку «Edit e-mail rules» на экране настроек коммуникаций. Это действие откроет таблицу со всеми зарегистрированными правилами обработки почты. Подробные сведения о создании, редактировании правил и управлении ими см. в главе «Правила обработки почты» документации.

Нажмите кнопку «Show communication log», чтобы увидеть таблицу всех зарегистрированных сообщений коммуникаций.

Кнопка «Send a test message» позволяет выбрать группу или отдельного пользователя, которому нужно отправить тестовое уведомление, указать тему и составить сообщение в поле «Message text». Сообщение может быть отправлено по электронной почте или по SMS.

Электронная почта

Существует один канал электронной почты по умолчанию, который должен быть всегда настроен, если система должна отправлять какие-либо уведомления по электронной почте. Альтернативные каналы могут быть настроены для отправки отдельных сообщений с другими настройками.

Например, ваша компания может отправлять часть уведомлений конечным заказчикам с подписью компании, колонтитулом и выделенным адресом отправителя. Для внутренних сотрудников письма отправляются по простому шаблону из внутреннего почтового ящика. В этом случае следует настроить соответственно один канал по умолчанию и один альтернативный. В редакторе уведомлений для шаблонов уведомлений, адресованных заказчикам, следует выбрать канал для заказчиков.

Для настройки канала коммуникаций электронной почты для исходящих писем необходимо задать следующие параметры:

- Endpoint — выберите адаптер, который будет использоваться для коммуникаций по электронной почте. Адаптеры настраиваются в разделе «Внешние подключения». Выберите тип адаптера, подходящий для отправки электронной почты, например SMTP-адаптер.

- From — введите имя отправителя, которое будет отображаться во всех исходящих письмах
- Footer — укажите необязательный колонтитул для всех сообщений электронной почты; обычно может использоваться для уведомления об ограничении ответственности компании.
- Test mode — для тестовых серверов, чтобы избежать отправки писем реальным пользователям, укажите один адрес электронной почты, на который будут поступать все сообщения. Это полезно для тестирования, систем разработки и т. п., но никогда не должно использоваться в производственной среде
- Group messages by thread — добавляет специальные заголовки письма, чтобы почтовые клиенты, такие как MS Outlook или Gmail, группировали сообщения, относящиеся к одному объекту (например, к одной задаче)

Нажмите кнопку «Add another alternative», чтобы добавить альтернативную конфигурацию канала

SMS

Для настройки канала SMS-коммуникаций для исходящих SMS-сообщений необходимо выбрать в разделе внешних подключений адаптер, поддерживающий SMS-коммуникации (он должен быть уже настроен), который будет использоваться как Endpoint.

Протоколы SMS-шлюзов различаются, и единого адаптера для всех SMS-центров не существует. Для выбора конкретного адаптера, подходящего для вашего шлюза, обратитесь к поставщику системы.

Параметры:

- Maximum SMS length — ограничение текста заданной длиной
- Prefix — добавление указанного текста перед отправкой любого сообщения
- Postfix — добавление указанного текста после любого отправляемого сообщения

Нажмите кнопку «Add another alternative», чтобы добавить альтернативную конфигурацию канала

Альтернативные конфигурации могут использоваться, например, для рассылки отдельных сообщений через другой адаптер или с другими настройками. Альтернативу можно выбрать в любом конкретном шаблоне уведомления.

7.3.8.1 Правила обработки почты

Правила обработки почты в настройках коммуникаций позволяют администраторам автоматизировать обработку входящих писем путем создания правил, которые автоматически обрабатывают входящие письма на основе предопределенных критериев, оптимизируя рабочий процесс и сокращая объем ручных операций.

Примечание: перед созданием правил обработки должно быть настроено внешнее подключение «Incoming e-mail adapter». Подробнее см. главу «Внешние подключения»

Создание новых правил:

- Чтобы начать создание нового правила обработки почты, нажмите кнопку «+Add rule».

  Во всплывающем окне укажите описательное имя правила и выберите нужное действие из раскрывающегося списка («Ignore» или «Create a new business object from email»).

- Определение критериев соответствия:

  Если правило применяется только к одному конкретному входящему адаптеру, укажите источник входящих писем, выбрав соответствующую конечную точку из раскрывающегося списка.

  Определите конкретные условия или фильтры на основе атрибутов письма, чтобы определить, когда правило должно применяться.

- Выбранный тип действия определяет действие правила и последующие параметры

- Настройка сведений о действии:

  Свяжите правило с соответствующей сущностью системы, чтобы обеспечить корректную обработку входящих писем.

  Используйте функцию сопоставления полей (Fields Map) для сопоставления атрибутов письма с соответствующими полями выбранной сущности, обеспечивая точную интеграцию данных.

  Выберите, копировать ли вложения из исходного письма, и при необходимости укажите остановку дальнейшей обработки входящих писем после применения правила.

- Добавление комментариев:

  Укажите дополнительный контекст или примечания к правилу, что облегчает его понимание и управление им.

После сохранения правила доступны для просмотра и управления в структурированной таблице.

Обратите внимание, что правила обрабатываются в том порядке, в котором они заданы. Если конечная точка не указана, правило применяется ко всем конечным точкам.

7.3.9 Редактор календарей

Календари используются всякий раз, когда система пытается вычислить разницу во времени между двумя датами или рассчитать рабочее время для целей планирования ресурсов или измерения SLA.

Редактор календарей можно использовать для создания новых календарей, отметки государственных праздников и определения стандартных часов рабочего дня. Выходные и праздничные дни задаются на вкладке «Holidays and free days».

В системе доступны следующие предопределенные календари (могут различаться в зависимости от версии приложения и настроек локализации):

- *NonStop 24x7 — календарь без заданных праздников. При расчете срока SLA не учитываются рабочие часы и праздники. Таким образом, если вы создадите заявку с SLA 24 часа, он истечет через эти 24 часа независимо от праздников или стандартных рабочих часов.*
- *Default — имеет предопределенные стандартные рабочие часы. Помимо изменения рабочих часов, можно также добавить праздники и нерабочие дни. При расчете срока SLA учитываются рабочие часы, обеденное время и праздники. Таким образом, если вы создадите заявку с SLA 24 часа, срок будет рассчитан только в пределах рабочих часов.*

Любой календарь также можно настроить на работу как круглосуточный, установив флажок «Nonstop calendar» (при включении этой опции применяется то же правило, что и для календаря NonStop).

Каждый календарь может иметь следующие параметры:

- Country — упрощает сопоставление календарей или государственных праздников со странами
- Time zone — часовой пояс, определяющий настройки рабочих часов
- Nonstop calendar — игнорирует рабочие часы

Чтобы задать новый календарь, нажмите кнопку «Add calendar» и введите его имя.

Затем отметьте рабочие дни и задайте рабочие часы, щелкая поля времени.

Установите флажок «Nonstop calendar», если хотите, чтобы календарь работал как круглосуточный календарь NonStop 24x7.

Любой календарь может быть настроен как расширение других календарей. В этом случае праздники и выходные дни из календаря будут добавлены к исходному календарю, выбранному в раскрывающемся списке «Extend calendar».

На вкладке «Holidays and free days» к любой дате можно добавить три типа событий:

- Рабочий день
- Нестандартный рабочий день
- Государственный праздник

Чтобы добавить определенный тип дня (события), нажмите кнопку «Add». Задайте подпись, которая будет отображаться при наведении курсора на день в представлении

календаря. Выберите тип дня и укажите конкретную дату. Чтобы удалить конкретную запись, нажмите значок в конце строки записи.

После настройки в представлении календаря будет отображаться выделенная цветом дата, для которой создано событие.

7.3.10 Хранилище файлов

Байтим позволяет редактировать файлы MS Office, загруженные в Байтим, в режиме реального времени непосредственно с вашего ПК. После каждого сохранения на локальном компьютере изменения будут перенесены в файл, загруженный в Байтим. Для использования прямого редактирования на сервере должен быть установлен SSL-сертификат, и подключение к серверу должно выполняться по HTTPS.

Из-за некоторых технических ограничений эта функция несовместима с SSO на основе ADFS/Azure Active Directory.

Прямое редактирование файлов MS Office доступно только для файлов, загруженных в сущность, использующую систему управления документами, например projects:

Далее необходимо открыть сведения о вложении, нажав значок . В сведениях содержится кнопка «Edit with MS Office» для прямого редактирования файла. Кнопка открывает локальное приложение MS Excel на ПК пользователя. Приложение должно быть установлено, и требуется действительная лицензия Microsoft.

Обратите внимание, что для использования прямого редактирования файлов пользователю должна быть назначена роль/право, позволяющее редактировать вложения, загруженные к записи.

7.3.11 Согласования и автозадачи

Системная функция «Approvals and Task Execution Settings» влияет на все согласования и задачи глобально. Эти настройки могут быть переопределены в конкретных определениях согласований.

Доступно несколько настроек, в том числе «Include Stand-Ins», которые определяют, включаются ли в процесс согласования активные заместители и следует ли отправлять уведомления (подробнее см. главу *«Stand-in settings»*). Другие настройки включают «Allow Automatic Timeout Actions for Deleted Approvers», которая определяет, завершать или отменять настройки тайм-аута, если ожидаемые согласующие больше недоступны. Настройка «Recalculate Approvers on Approval Re-Entrance» определяет, выполняет ли

система замещение повторно и заполняет ли согласующих из новых значений полей при повторном запуске процесса согласования.

Функция «Auto-Task Execution Settings» позволяет пользователям редактировать типы фаз задач, вручную запускать фазы для немедленного начала и вручную запускать любую ожидающую задачу, даже если по условиям запускать ее еще рано. Эти настройки дают пользователям больше контроля над процессом выполнения задач.

7.3.12 Разделение пользователей

Стандартное управление пользователями предполагает добавление пользователей в группы, назначение им определенных ролей и отображение данных и элементов графического интерфейса пользователю на основе этих настроек. Дополнительно к этой модели Байтим вводит новый атрибут «Территория» (Territory), который может быть задан для каждого пользователя. Он представляет собой простой инструмент разделения внутренних/внешних сотрудников, заказчиков и т. д. на простые зоны и управления правами для этих зон.

Атрибут территории содержит следующие значения (перечень можно расширить, отредактировав список значений «Territories»):

- Internal
- Customer
- Subcontractor

Хотя эта модель упрощает управление атрибутами прав, она усложняет поддержку состава пользователей каждой группы. Поскольку в большинстве компаний имеются группы AD, содержащие такие списки, например «Internal», «Subcos» и т. д., предусмотрен инструмент, обеспечивающий сопоставление этих групп с территориями:

Когда группа сопоставлена с территорией, все пользователи этой группы наследуют настройку территории. Система отслеживает добавление/удаление пользователей в группах и соответствующим образом корректирует признак территории.

Пример конфигурации территорий:

- Пользователи с территорией Internal могут видеть данные, созданные пользователями, принадлежащими к любой территории.
- Пользователи с территорией Customer могут видеть только данные, внесенные пользователями той же территории.
- Пользователи с территорией Subcontractor могут видеть только данные, внесенные пользователями той же территории и пользователями с территорией Customer.

7.3.13 Тайм-аут неактивного сеанса

Функция тайм-аута сеанса пользователя предоставляет администраторам возможность автоматически завершать неактивные сеансы пользователей по истечении заданного периода бездействия. Эта функция безопасности помогает защитить конфиденциальные данные, гарантируя, что оставленные без присмотра сеансы не будут оставаться активными бесконечно, а также оптимизирует использование системных ресурсов.

Для настройки этой функции перейдите в Settings > This space > Inactive Session Timeout.

Используйте переключатель «Enabled» в разделе настроек «Inactive user sessions timeout», чтобы активировать или деактивировать функцию автоматического истечения сеанса. Если функция отключена, сеансы пользователей будут оставаться активными до выхода из системы вручную или до перезапуска сервера.

Тайм-аут бездействия

Значение по умолчанию: 30 минут

Укажите длительность бездействия пользователя (в минутах), по истечении которой сеанс автоматически завершается. Система принимает значения от 1 минуты до 10 080 минут (1 неделя).

Рекомендации:

- Для сред с высокими требованиями к безопасности: 15–30 минут
- Для стандартных бизнес-сред: 30–60 минут
- Для сред с низкими требованиями к безопасности или сред разработки: 120 минут и более

Время предупреждения

Значение по умолчанию: 2 минуты

Настройте, за сколько минут до истечения сеанса пользователи будут получать диалоговое окно с предупреждением. Эта настройка принимает значения от 1 до 60 минут. Диалоговое окно предупреждения отображает таймер обратного отсчета и предоставляет пользователям возможность продлить сеанс, выполнив любое действие в интерфейсе, например переместив мышь.

Примечание: время предупреждения должно быть меньше длительности тайм-аута бездействия.

Исключения

Используйте кнопку «Add exception», чтобы задать другие значения тайм-аута для отдельных ролей. Например, назначьте более длительный тайм-аут разработчикам или пользователям, работающим с большими объемами данных.

Принцип работы

1. Контроль активности: система непрерывно отслеживает активность пользователя, включая перемещения мыши, щелчки и ввод с клавиатуры во всем приложении.
2. Обнаружение бездействия: если активность пользователя не обнаружена, система начинает отсчет периода бездействия.
3. Фаза предупреждения: когда оставшееся время сеанса достигает заданного порога предупреждения, на экране пользователя появляется модальное диалоговое окно, отображающее:
    - таймер обратного отсчета с указанием оставшихся минут и секунд
    - информацию о предстоящем завершении сеанса
4. Продление сеанса: если пользователь щелкает мышью, перемещает мышь или другое устройство либо возобновляет любую активность, таймер бездействия полностью сбрасывается и сеанс продолжается в обычном режиме. Это также происходит автоматически, когда пользователь активирует ранее неактивную вкладку браузера с приложением
5. Завершение сеанса: если до окончания обратного отсчета не выполнено никаких действий, система:
    - автоматически выполняет выход пользователя (включая все сеансы во вкладках того же браузера)
    - очищает данные сеанса
    - перенаправляет на страницу входа
    - отображает уведомление о том, что сеанс завершен из-за бездействия
6. Администраторы и пользователи с правом «Ignore inactivity timeout» не затрагиваются и никогда не отключаются

Внимание: при истечении сеанса все несохраненные результаты работы будут потеряны. Пользователей следует проинструктировать:

- часто сохранять результаты работы
- своевременно реагировать на предупреждения о тайм-ауте
- использовать функции автосохранения там, где они доступны

Информирование пользователей

При первом включении этой функции или существенном изменении значений тайм-аута рекомендуется:

- заранее объявить об изменении всем пользователям
- предоставить понятную документацию о работе функции
- объяснить преимущества с точки зрения безопасности
- обучить пользователей регулярно сохранять результаты работы

Технические примечания

- Значения тайм-аута хранятся в базе данных системы в секундах, но отображаются в пользовательском интерфейсе в минутах

- Функция использует определение активности на стороне клиента в сочетании с проверкой сеанса на стороне сервера
- Изменения настроек тайм-аута вступают в силу немедленно для новых сеансов; существующие сеансы будут использовать настройки, действовавшие на момент их создания

Рекомендуемые практики

1. Баланс безопасности и удобства: выбирайте значения тайм-аута, которые обеспечивают достаточную безопасность, не раздражая пользователей слишком частыми завершениями сеансов.
2. Учет характера работы: проанализируйте типичный характер работы пользователей в вашей организации. Пользователям, часто читающим длинные документы, могут потребоваться более длительные периоды тайм-аута.
3. Тестирование перед внедрением: протестируйте функцию с различными настройками тайм-аута в непроизводственной среде, прежде чем разворачивать ее для всех пользователей.
4. Отслеживание отзывов пользователей: после включения функции собирайте отзывы пользователей о том, требуется ли корректировка значений тайм-аута.
5. Требования соответствия: убедитесь, что настройки тайм-аута отвечают нормативным требованиям и требованиям соответствия, специфичным для вашей отрасли (например, HIPAA, SOX, GDPR).
6. Документирование политики: создайте и доведите до сведения пользователей понятную политику тайм-аута сеанса, объясняющую, почему функция включена и чего следует ожидать пользователям.

7.3.14 Внешние подключения

В этом разделе можно создавать внешние подключения в приложении и управлять ими. Внешние подключения реализуются адаптерами для каждого типа системы. Одновременно может быть настроено несколько адаптеров для доступа к разным приложениям. Перечень всех доступных адаптеров может различаться в зависимости от библиотек адаптеров, имеющихся в вашей системе.

Чтобы создать подключение, нажмите кнопку «Add connection» и заполните все необходимые сведения, такие как имя и тип подключения. После выбора типа подключения необходимо заполнить дополнительные сведения согласно его описанию.

Каждое подключение можно изменить, нажав кнопку «Configuration». Подключение можно деактивировать или активировать, выбрав кнопку «Disable/Enable».

В списке адаптеров также можно сортировать и группировать записи. Обе функции могут основываться на атрибуте имени или типа. Сортировку также можно выполнять по ключевому атрибуту.

Исчерпывающие сведения об общих принципах, настройке адаптеров и типах подключений см. в главе «Интеграция» настоящего руководства. В этом разделе приведены сведения о настройке различных адаптеров интеграции в Байтим и управлении ими.

7.3.15 События интеграции

События интеграции распознаются пользовательскими функциями, написанными разработчиками. Событие интеграции инициируется на основании определения селектора и фильтра, после чего пользовательская функция идентифицирует событие по его имени и может выполнить соответствующее действие. Обратите внимание, что эта функциональность предназначена для разработчиков и требует дополнительного кода для полноценной работы.

Задайте шаблон события интеграции, нажав кнопку «Add». В отобразившемся всплывающем окне заполните все необходимые сведения:

- Title — заголовок шаблона
- Event name — имя события, распознаваемое пользовательской функцией
- Selector — используется так же, как селектор уведомлений. Подробнее см. главу Selector.
- Filters — используется так же, как селектор уведомлений. Подробнее см. главу Filters.
- Fields — перечень полей, передаваемых в событие интеграции. Передаваемые данные могут использоваться в пользовательской функции.

Событие интеграции может далее обрабатываться другими внешними системами; передача данных в такие системы должна быть определена в пользовательской функции, написанной разработчиком.

7.3.16 Информационная панель

Администраторы могут информировать пользователей системы с помощью информационных сообщений, отображаемых в нижней части экрана системы. Если определено несколько сообщений, они будут чередоваться и показываться одно за другим.

Сообщения отображаются только при включенном для сообщения признаке «Visible». Используйте кнопку «Display message», чтобы создать сообщение с уже включенным признаком. Кнопка «Register message» создает сообщение, которое появится в определенном временном интервале. В этом случае необходимо задать значения даты/времени «From» и «To». При наступлении времени «From» признак «Visible» будет включен. По истечении времени «To» признак будет отключен. Если установлен флажок «Autoremove», сообщение также будет удалено из списка администратора. В противном случае сообщение сохраняется и может быть в любой момент снова сделано видимым.

В некоторых сценариях отображаемые сообщения требуют согласования или дополнительных действий перед отображением. В этом случае определите жизненный

цикл для сущности «informtable» и настройте процесс необходимым образом. На странице настроек нажмите «Settings»/«Specify filter» и задайте фильтр, который будет инициировать отображение сообщений. Например, если согласованные сообщения имеют lcstage==5, укажите это в фильтре.

Сообщения информационной панели также могут публиковаться через REST API или с помощью скриптов. Для этого создайте объект в сущности «informtable» с полем «message», заполненным отображаемым сообщением. Учитывайте и другие атрибуты, описанные в модели.

7.3.17 Сертификаты

Настройки управления сертификатами позволяют хранить известные сертификаты в формате X509, которые могут использоваться для авторизации внешних служб, подписания документов и т. д.

В представлении по умолчанию таблица отображает перечень всех известных сертификатов, импортированных в систему. Нажмите кнопку «Upload new certificate», чтобы открыть мастер импорта сертификата. Затем либо:

1.1.1 Вставьте содержимое файла сертификата в текстовое поле в формате PEM; допускается ровно один сертификат. Закрытые ключи, запросы на сертификат и т. п. не допускаются.

1.1.2 Либо используйте кнопку для импорта сертификата из файла в кодировке PEM. Файлы сертификатов обычно имеют имена *.crt, *.cert, *.pem и т. д. Если файл имеет формат p12 (распространен на платформах Windows), используйте утилиты, например openssl, чтобы извлечь из файла сертификат в формате PEM

Проверьте данные сертификата, отображаемые на второй странице мастера. Можно выбрать альтернативное понятное альтернативное имя (alias), чтобы позднее находить сертификат. Если оно не выбрано, по умолчанию это имя содержит субъект (Subject) сертификата.

Чтобы удалить сертификат, используйте кнопку удаления в контекстном меню. Щелчок по существующему сертификату открывает окно предварительного просмотра со свойствами сертификата.

8 Внешние источники

1. Официальная документация PostgreSQL: http://www.postgresql.org/docs/
2. Документация Apache Tomcat: https://tomcat.apache.org/tomcat-9.0-doc/index.html