YouGile

Коробочная версия. Инструкция по администрированию

Содержание

Общее описание

- Коробка YouGile — это приложение для Linux или Windows, которое устанавливается на сервер
- Отвечает на http запросы по порту 8001
- Пишет вывод в stderr и stdout
- Использует диск для хранения локальных данных приложения (см. ниже структуру папок приложения)
- Сервер YouGile не требует подключения к интернету и может полностью работать в локальной сети

Серверное Приложение YouGile выполняет функции, которые необходимы для использования в компании системы управления проектами YouGile. Для полного развёртывания YouGile на своём сервере, необходимо самостоятельно настроить следущее:

- запуск YouGile в виде сервиса, запуск вместе с ОС
- настройка возможности YouGile отправки писем (smtp)
- настройка фронтенд http сервера перед YouGile (nginx, Apache, IIS, ...)
- настройка https на фронтенд-сервере
- настройка хранения и ротации логов
- резервное копирование данных YouGile (на другую машину)

Эти пункты настраиваются по-разному, в зависимости от стека технологий и внутренних политик компании. Ниже в документе приводятся примеры наиболее частых вариантов настройки.

Структура директории серверного приложения YouGile

Внутри рабочей директории приложения yougile находятся:

- **server** (server.exe для Win) — само исполняемое приложение сервера YouGile.
- **conf.json** — файл настроек в формате JSON.
- **machine.key** (появляется после первого запуска) — файл с ключом машины. Идентифицирует машину по её параметрам железа, нужен для генерации лицензии.
- **license.key** — файл лицензии (выдаётся после покупки, добавляется вручную).
- **tasks/** — директория для скриптов команд (про команды см. ниже).
- **user-data/** — директория, в которой хранятся файлы, загружаемые пользователями в YouGile.
- **database/** — директория данных YouGile.
- Остальные файлы используются исполняемым файлом для его работы (библиотеки).

Системные требования

Необходима машина с 64-битной операционной системой Windows или Linux. На сайте https://dist.yougile.com предложены сборки для наиболее распространённых версий linux и windows. В случае необходимости, отправив запрос в поддержку (support@yougile.com), можно получить сборку для более старых версий.

Минимальные требования по оперативной памяти: 500Мб плюс ещё по 500Мб на каждые 100 пользователей. То есть, например, если пользователей 500, то получается 500 + 500 * 5 = 3Гб оперативной памяти.

По процессору и IOPS жёсткого диска узкого места не возникает вплоть до 1000 пользователей.

Необходимое свободное место на диске зависит от того, какие файлы и как часто будут загружаться пользователями в системе. Для начала работы стоит выделить свободного места из расчёта 1Гб на каждые 10 пользователей, с возможностью дальнейшего увеличения этого лимита.

Рекомендуемые характеристики при количестве пользователей более 1000

USERS	1,000	1,500	2,000
RAM	16 GB	Minimum 16 GB Reccomend 32 GB	32 GB
STORAGE	Minimum 512MB Recommend 1TB		1TB

IOPS	Нет высоких требований по iops, подойдёт HDD SATA в raid1		
CPU	Желательно современный процессор с характеристиками тех.процесса минимум 14Нм Например, Intel® Xeon® Processor E 3-1270 v5		
CPU CORES	16	24	32
NETWORK	100Mbit		

Установка

Необходимо скачать дистрибутив с сайта https://dist.yougile.com Для скачивания последней версии используйте следующие ссылки:

- для Windows (7/8/10/Server) — https://dist.yougile.com/win/latest/yougile.zip
- для RHEL, CentOS, CloudLinux, Fedora — https://dist.yougile.com/rhel/latest/yougile.tar.gz
- для Debian, Ubuntu и других дистрибутивов Linux — https://dist.yougile.com/linux/latest/yougile.tar.gz

Распакуйте архив в удобное место на сервере — YouGile обращается в файловой системе только к содержимому этой директории.

Чтобы проверить работу приложения, запустите файл server (server.exe для Win) и зайдите в браузере по адресу http://localhost:8001 внутри машины (либо http://<ip машины>:8001 на компьютере из локальной сети).

Запуск, остановка. Настройка сервиса

Для Linux

YouGile можно запустить, выполнив из рабочей директории `yougile` файл `server` например, если `yougile` был установлен в `/opt`:

```
cd /opt/yougile
./server # запуск
^C # остановка
```

Но для нормальной работы рекомендуется настроить сервис. Для этого создайте файл `yougile.service` со следующим содержимым:

```
[Unit]
Description=YouGile

[Service]
```

```
WorkingDirectory=/opt/yougile
ExecStart=/opt/yougile/server

[Install]
WantedBy=multi-user.target
```

(в примере yougile установлен в `/opt`, замените на своё местоположение). Скопируйте этот файл в директорию `/etc/systemd/system/`, затем выполните

```
systemctl daemon-reload
systemctl enable yougile.service
systemctl start yougile.service
```

После этого можно запускать yougile командой `service yougile start` и останавливать `service yougile stop`. Просматривать вывод yougile можно при помощи стандартного инструмента `journalctl`.

Для Windows

Запустить сервер YouGile можно, нажав на файл server.exe. Но при таком способе запуска, Windows иногда замораживает выполнение приложения. Поэтому предпочтительнее запускать приложение через `cmd`. Откройте терминал Windows `cmd`, перейдите в директорию `yougile` и выполните `server.exe`. Наиболее удобный способ запуска и остановки YouGile — создание сервиса.

Для настройки сервиса необходимо сделать следующее:

1. Скачать утилиту WinSW
2. Скачать sample-minimal.xml
3. Переместить скачанные файлы в директорию, где развернут YouGile
4. Изменить название файла sample-minimal.xml на yougile.xml, а WinSW-x64.exe на yougile.exe
5. Отредактировать файл yougile.xml

```
<service>
  <id>yougile</id>
  <name>YouGile</name>
  <description>YouGile App</description>
  <executable>%BASE%\server.exe</executable>
</service>
```

6. Установить сервис.

- Открыть powershell или command prompt
- Перейти в директорию, где развернута коробка

```
cd path-to-your-directory
```

- В директории выполнить команду `yougile.exe install`

7. Запустить службу в Task Manager или через Server Manager => Tools => Services

Теперь YouGile будет запускаться автоматически при запуске сервера.

Лицензия YouGile

Для коробочной версии предоставляется бесплатный 7-дневный период тестирования. Если у серверного приложения YouGile есть доступ в интернет, то при запуске YouGile можно в интерфейсе нажать на кнопку, которая установит Демо-лицензию YouGile, которая будет активна 7 дней. Также, демо-лицензию можно получить по запросу в поддержку, для этого необходимо прислать файл `machine.key` (он появляется после первого запуска).

Лицензия хранится в файле `license.key` и привязана к параметрам машины (модель процессора, кол-во ядер, к-во памяти и т.д.). Если вы приобрели лицензию и необходимо изменить параметры виртуальной машины, на которой работает YouGile (или перенести YouGile на другой сервер), то лицензию тоже надо перегенерировать. Это можно сделать, обратившись в поддержку и предоставив новый файл `machine.key`

Для организации отказоустойчивости или для создания архивной копии YouGile может потребоваться установить одну и ту же базу данных YouGile на несколько машин. Если у вас есть приобретённая лицензия YouGile, вы можете связаться с вашим персональным менеджером (или службой поддержки) по вопросу предоставления лицензии с поддержкой нескольких машин. Такая лицензия предоставляется бесплатно для команд с большим количеством сотрудников.

Настройка параметров YouGile, файл **conf.json**

В директории `yougile` находится файл `conf.json` — в нём находятся все настройки серверного приложения в формате JSON. Для правильной работы системы необходимо указать значение параметра `mainPageUrl`. `mainPageUrl` — это адрес, по которому YouGile будет доступен для пользователей, например "https://yougile.example.com"

После редактирования `conf.json`, чтобы изменения применились, необходимо перезапустить сервис YouGile.

При редактировании файла `conf.json`, важно не нарушить формат JSON, иначе, приложение YouGile выдаст ошибку при запуске и не запустится. Редактируйте поля по аналогии с тем, что уже есть в файле и обращайте внимание на запятые и кавычки (можно где-то забыть поставить или, наоборот, поставить лишнюю).

Весь список настроек, доступных в `conf.json`, большинство из них необязательны:

Имя	Пример значения	Описание

Имя	Пример значения	Описание
`mainPageUrl`	`"https://yougile.my.com"`	**Обязательный параметр**. Адрес, по которому YouGile доступен для пользователей. Используется для формирования ссылок на страницы системы, например, ссылка на регистрацию, которая отправляется на почту пользователя при его приглашении, или ссылка для восстановления пароля.
`port`	`8001`	Порт, по которому YouGile принимает запросы HTTP (некоторые значения портов могут требовать определённых прав при запуске YouGile в некоторых ОС)
`smtp`	(см. ниже)	Настройка подключения к почтовому серверу, см. ниже
`emailFrom`	`"\"Yougile\" <info@my.com>"`	Почтовый адрес, от лица которого будут приходить письма пользователей. Если адрес не соответствует аккаунту в настройках поля `smtp`, то многие почтовые серверы могут запретить отправку письма
`dataUrl`	`"https://yougile-data.my.com"`	Адрес, с которого нужно загружать файлы пользователей (которые хранятся в директории `user-data/`), если он совпадает с `mainPageUrl`, то его не нужно указывать
`uploadFileLimit`	50	Максимальный размер загружаемого пользователем файла в мегабайтах (по умолчанию `50`)
`disableInviteUsers`	`true`	Если указано значение `true`, то пользователи не смогут приглашать новых пользователей в систему (нужно, например, при интеграции с ActiveDirectory)
`disableEmailRecovery`	`true`	Если `true`, то пользователи не смогут восстанавливать пароли

Имя	Пример значения	Описание
`lang`	`"ru"`	Язык системы по умолчанию. Если не указан, то язык определяется для каждого пользователя автоматически
`multiCompany`	`false`	Разрешает работу системы в режиме поддержки нескольких компаний (если `false`, то доступна только 1 основная компания). При включенном параметре пользователи добавляются в аккаунт и распределяются по компаниям через приглашения по почте.
`allowAddCompanies`	`true`	По умолчанию, все пользователи могут создавать новые компании. Если указано `false`, то пользователи не смогут создавать новые компании. Можно также вместо `true` или `false`, указать массив email-ов пользователей, которые смогут создавать компании, пример: `["user1@my.com", "user2@my.com"]`
`allowEnterWithoutCompany`	`false`	Если пользователь удалён из всех компаний, то если этот параметр `false`, то пользователь не может войти в систему, если `true`, то пользователь может войти и при этом создаётся новая пустая компания для этого пользователя.
`allowExtensions`	`true`	Разрешить системе подключаться к серверу расширений YouGile. Для работы расширений необходимо, чтобы этот параметр был `true`, чтобы на сервере был доступ по https к адресу plugin.yougile.com и чтобы коробочная версия была доступна по определённому адресу из интернета. При этом будет возможна передача данных между коробочной версией и YouGile

Имя	Пример значения	Описание
`allowMobileClients`	`true`	Разрешить вход в систему с мобильного приложения. Можно указать `true`, `false` или массив email-ов пользователей, которым можно заходить через мобильное приложение.
`rateLimiterOptions`	{ "enabled": true, "countMultiplier": 1, "timeMultiplier": 1, "restApiCount": 30, "restApiInterval": 60000}	Настройка ограничения количества запросов. Критичные http эндпоинты имеют ограничение на количество запросов к ним (например, вход в систему, регистрация и т.д.), базовое ограничение по запросам для одного ip – это 5 запросов в минуту, с помощью этой настройки можно изменить или отключить это поведение. Ограничения запросов к REST API настраиваются отдельно, параметрами restApiCount (количество разрешённых запросов) и restApiInterval – интервал времени в миллисекундах
`init`	(см. ниже)	Настройка запуска серверных скриптов для интеграции (например, для ActiveDirectory). Примеры см. ниже
`logStreams`	`[{"level": "info", "stream": "stdout"}]`	Настройка вывода логов сервера. Пример: `[{"level": "info", "stream": "stdout"}, {"level": "error", "path": "/var/tmp/yougile-error.log"}]`. Подробнее см. настройки bunyan
`keyExpirationTimeout`	259200000	Время в миллисекундах в течение которого действует ключ сессии пользователя
`keyExpireOnLogout`	`false`	Если это значение установлено в `true`, то при выходе из аккаунта пользователя, ключ сессии инвалидируется

Имя	Пример значения	Описание
`eventLogPath`	"./event.log"	Путь к файлу, в который пишется лог событий безопасности. Если параметр не указан, то лог не пишется
`eventLogDailyRotationLimit`	30	Если этот параметр указан, то лог событий безопасности ротируется раз в день и число в этом параметре определяет количество файлов дней лога, которые хранятся
`restrictUserDataAccess`	`false`	Если указано значение `true`, то неавторизованный пользователь не сможет получить файл по ссылке. При значении `false` (значение по умолчанию) любой пользователь может получить файл имея ссылку на него. Для работы параметра необходимо убрать часть location /user-data/ в nginx.conf

Подключение почты

Настройки сервера хранятся в файле conf.json. Все настройки по умолчанию уже прописаны в этом файле после установки, чтобы поменять настройки – отредактируйте этот файл и перезапустите сервер. Для того, чтобы сервер мог посылать email-ы (например, при добавлении новых пользователей) необходимо прописать smtp настройки в файле `conf.json`.

Пример настройки:

```
"smtp": {
  "host": "smtp.example.com",
  "secure": true,
  "port": 465,
  "auth": {
  "user": "me@some.com",
  "pass": "******"
}
```

Следует обратить внимание на то, чтобы в поле `mainPageUrl` был корректно указан адрес сервера и в поле `emailFrom` был правильный адрес отправителя.

Пример настройки почты для `Exchange`:

```
{
  "host": "exchange.mycompany.com",
  "secureConnection": false,
  "port": 587,
  "tls": {
    "cipher": "SSLv3",
    "rejectUnauthorized": false
  },
  "auth": {
    "user": "ourdomain\\someuser",
    "pass": "******"
  }
}
```

Включение двухфакторной аутентификации (2FA)

> Двухфакторная аутентификация (2FA) добавляет дополнительный уровень безопасности в процессе входа пользователей в систему. В коробочной версии YouGile 2FA активируется и настраивается через конфигурационные файлы. Следуйте этой инструкции для настройки и управления двухфакторной аутентификацией в вашей компании. Включение двухфакторной аутентификации не приведет к автоматическому разлогированию пользователей. При использовании встроенного SMS-сервиса YouGile для прохождения авторизации пользователи смогут вводить только российские и белорусские номера телефонов. Для отправки сообщений на номера других стран необходимо самостоятельно настроить связь с оператором, который подходит вам лучше всего.

1. Настройка подключения

Для включения двухфакторной аутентификации администратор должен настроить соответствующие параметры в `conf.json`.

В конфигурационном файле необходимо указать:

- Значение true в настройке `twoFactorAuth`
- Использование сервиса отправки SMS: администратор может выбрать между использованием встроенного сервиса YouGile или подключением собственного SMS-сервиса. Для использования собственного сервиса нужно указать параметр `twoFactorCodeSendCommand`, ниже представлено подробное описание того, как именно это можно сделать.
- Время, после которого код из SMS будет считаться недействительным: `twoFactorCodeLifetime` (по умолчанию - 5 минут), указывается в mls.
- Длину сессии: дефолтная длина задается через `keyExpirationTimeout` и составляет 300 дней.

Пример конфигурации:

```
{
"twoFactorAuth": true
}
```

2. Запрос номера телефона и SMS-кода при входе

2.1 Веб и десктопная версия YouGile

При включенной двухфакторной аутентификации система будет автоматически запрашивать у пользователей номер телефона (если он не указан) и отправлять им код доступа по SMS при входе. Код будет действителен в течение времени, указанного в конфигурации (twoFactorCodeLifetime).

2.2 Мобильное приложение YouGile

В мобильном приложении YouGile подключение второго фактора невозможно. После включения двухфакторной аутентификации пользователям будет необходимо зайти в веб-версию и указать номер телефона при входе. При наличии указанного номера телефона в мобильной версии появится механика указания кода, отправленного по SMS.

3. Команды управления номерами телефонов

Вы можете управлять номерами телефонов пользователей.

3.1. Добавление номера телефона

Для добавления номера телефона пользователю используйте команду:

```
/.server task change-user-auth-phone 'dev@YouGile.com' '+71111111111'
```

для Windows:

```
server.exe task change-user-auth-phone 'dev@YouGile.com' '+71111111111'
```

3.2. Изменение номера телефона пользователя

Для изменения номера телефона пользователя используйте команду:

```
/.server task change-user-auth-phone 'dev@YouGile.com' '+72222222222'
```

для Windows:

```
server.exe task change-user-auth-phone 'dev@YouGile.com' '+72222222222'
```

Удалить номер телефона можно использовав эту же команду, передав пустым второй параметр. В случае отсутствия номера телефона, пользователю необходимо будет самостоятельно указать его при входе в веб-версию.

4. Лимит SMS на компанию

Система учитывает лимиты отправки SMS в зависимости от количества пользователей в лицензии:

- Лимит SMS на день рассчитывается по формуле: 6 * количество пользователей в лицензии (рекомендованная длина сессии – не менее 8 часов, иначе есть риск израсходовать лимит)
- Пользователи могут перезапрашивать код неограниченное количество раз, пока не будет достигнут общий лимит.

Настройка http-фронтенда, HTTPS

Помимо непосредственной пользы от HTTPS, есть ещё ряд ограничений, с которыми можно столкнуться если не настроить HTTPS и предлагать пользователям подключаться через HTTP без шифрования:

- некоторые браузеры не разрешают включать уведомления для http-страниц
- на некоторых мобильных устройствах нельзя подключиться без https в мобильном приложении YouGile (это ограничение самих мобильных ОС)

Чтобы включить https, необходимо поставить между YouGile и клиентами промежуточный http-сервер (nginx, IIS, Apache, ...) и настроить в нём подключение через https.

Пример конфигурации для nginx (nginx.conf)

```
http {
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 120;
    types_hash_max_size 2048;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    gzip on;

    server {
        listen 80;
        server_name <YOUR_SERVER_NAME>;
        return 301 https://$server_name$request_uri;
    }

    server {
        listen 443 ssl;
        server_name <YOUR_SERVER_NAME>;
```

```
        ssl_protocols TLSv1.2;
        ssl_certificate <PATH_TO_CERT>;
        ssl_certificate_key <PATH_TO_KEY>;
        ssl_dhparam <PATH_TO_DHPARAM>;

        ssl_ciphers ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-
RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA:DHE-RSA-AES256-SHA;
        ssl_prefer_server_ciphers on;

        ssl_session_timeout 10m;
        ssl_session_cache shared:SSL:10m;

        client_max_body_size 50M;
        client_body_buffer_size 50M;

        gzip on;
        gzip_http_version 1.1;
        gzip_comp_level 5;
        gzip_min_length 4096;
        gzip_proxied any;
        gzip_types text/plain text/xml text/css application/x-javascript
application/javascript application/json application/x-font-ttf;
        gzip_vary on;

        add_header Strict-Transport-Security "max-age=31536000; includeSubDomains;
preload" always;
        add_header X-Frame-Options SAMEORIGIN;
        add_header X-XSS-Protection "1; mode=block";
        add_header X-Content-Type-Options nosniff;

# Удалите этот блок, если используете параметр restrictUserDataAccess
        location /user-data/ {
            add_header X-YouGile-Served data;
            add_header 'Content-Disposition' 'attachment';

            location ~* \.(jpe?g|png|pdf|gif|mp4|m4p|mp3|avi|wmv)$ {
                add_header 'Content-Disposition' '';
                root /opt/yougile;
                try_files $uri @local-data;
            }

            root /opt/yougile;
            try_files $uri @local-data;
        }
# Конец блока, который нужно удалить

        location ~ /\. {
            deny all;
        }

        location / {
            proxy_pass http://localhost:8001;
```

```
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $remote_addr;
            proxy_set_header Host $http_host;
            proxy_read_timeout 1h;
            proxy_connect_timeout 1h;
            proxy_send_timeout 1h;
            proxy_pass_header Server;
            proxy_max_temp_file_size 0;
        }
    }
}
```

Настройка apache2

Конфигурация для виртуального хоста Apache:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName <YOUR_SERVER_NAME>
    ServerAdmin <YOUR_ADMIN>

    DocumentRoot "/opt/yougile"

    ErrorLog /var/log/apache2/yougile.error.log
    CustomLog /var/log/apache2/yougile.web.log combined

    <Directory /opt/yougile/.well-known/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Require all granted
    </Directory>

    SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
    SSLHonorCipherOrder On
    SSLOptions +StrictRequire
    SSLEngine on

# Настройки для использования самоподписанного сертификата
    SSLCertificateFile /etc/apache2/ssl/yougile.crt
    SSLCertificateKeyFile /etc/apache2/ssl/yougile.key

    Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
    Header always set X-Frame-Options SAMEORIGIN
    Header always set X-XSS-Protection "1; mode=block"
    Header always set X-Content-Type-Options nosniff

# Ограничения на размер тела запроса
```

```
    LimitRequestBody 52428800
    ProxyTimeout 3600

# Gzip сжатие
    AddOutputFilterByType DEFLATE text/plain text/xml text/css
application/javascript application/json application/x-font-ttf
    SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png|pdf|mp4|mp3|avi|wmv)$ no-gzip

# Обработка /user-data/
      Alias /user-data/ "/opt/yougile/"
        <Location /user-data/>
        Header always set X-YouGile-Served "data"
        Header always set Content-Disposition "attachment"

    </Location>
    <FilesMatch "\.(jpe?g|png|pdf|gif|mp4|m4p|mp3|avi|wmv)$">
        Header always unset Content-Disposition
    </FilesMatch>

# Необходимо указать путь для WebSocket-подключений
    <Location /data/ws-native>
        RewriteEngine On
        RewriteCond %{HTTP:Connection} Upgrade [NC]
        RewriteCond %{HTTP:Upgrade} websocket [NC]
        ProxyPass "ws://127.0.0.1:8001/data/ws-native"
        ProxyPassReverse "ws://127.0.0.1:8001/data/ws-native"
    </Location>

    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPass / http://127.0.0.1:8001/ connectiontimeout=3600 timeout=3600
    ProxyPassReverse / http://127.0.0.1:8001/
    ProxyPassMatch ^/(.*)$ ws://127.0.0.1:8001/$1
    RequestHeader set X-Real-IP %{REMOTE_ADDR}s
    RequestHeader set X-Forwarded-For %{REMOTE_ADDR}s

# Настройки для использования сертификата Let's Encrypt, необходимо прописать свой
путь до цепочки сертификатов
    Include /etc/letsencrypt/options-ssl-apache.conf
    SSLCertificateFile /etc/letsencrypt/live/yougile.example.com/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/yougile.example.com/privkey.pem
</VirtualHost>
</IfModule>
```

Настройки прописываются в файле /etc/apache2/sites-available/yougile-ssl.conf

Для корректной работы конфигурации необходимо выполнить команды:

```
sudo a2ensite yougile-ssl.conf
sudo a2enmod ssl headers proxy proxy_http proxy_wstunnel rewrite
sudo systemctl restart apache2
```

Настройка IIS

Импорт сертификата

Чтобы импортировать ваш SSL-сертификат в IIS на Windows Server, выполните следующие шаги:

1. Конвертация ключа и сертификата в формат PFX: Поскольку IIS требует один PFX файл (который содержит сертификат и приватный ключ), вам нужно объединить файлы .crt и .key в PFX файл. Для этого можно использовать OpenSSL:

```
openssl pkcs12 -export -out your-cert.pfx -inkey your-cert.key -in your-cert.crt
```

Вам нужно будет задать пароль для файла PFX, который потребуется при импорте в IIS.

2. Импорт PFX в хранилище сертификатов Windows:

- Откройте Диспетчер сертификатов Windows. Нажмите Win+R, введите mmc, нажмите Enter.
- В меню нажмите Файл → Добавить или удалить оснастку.
- Выберите Сертификаты и нажмите Добавить.
- Выберите Компьютерный аккаунт и нажмите Далее, затем Готово.
- В левой панели раскройте Сертификаты (локальный компьютер) → Личные → Сертификаты.
- Правой кнопкой мыши кликните по папке Сертификаты и выберите Все задачи → Импорт.
- В мастере импорта выберите ваш PFX файл, укажите путь, введите пароль и завершите импорт.

3. Привязка SSL-сертификата к вашему сайту в IIS:

- Откройте Диспетчер IIS (Internet Information Services).
- В левой панели выберите сервер и перейдите в раздел Сайты.
- Выберите нужный сайт, к которому нужно привязать сертификат.
- В правой панели выберите Привязки
- В открывшемся окне нажмите Добавить, выберите тип https, укажите домен, а также выберите импортированный сертификат.
- Нажмите ОК и закройте окно.

Настройка обратного прокси

1. Установка Application Request и URL Rewrite:

- Перейдите на сайт Application Request Routing. Скачайте и установите его, если он у вас ещё не установлен.
- Перейдите на сайт URL Rewrite. Скачайте и установите его, если он у вас ещё не установлен.

2. Настройка обратного прокси в IIS

Включение параметра "Проксирование запросов":

- Откройте Диспетчер IIS.

- В левой панели выберите сервер и дважды кликните по пункту Application Request Routing.
- В правой панели найдите и откройте раздел Application Request Routing Cache.
- В правой части окна нажмите на Server Proxy Settings.
- Установите флажок Enable Proxy и нажмите Apply.

Настройка правил для проксирования:

- В IIS вернитесь к Диспетчеру IIS.
- В левой панели выберите ваш сайт, для которого нужно настроить проксирование.
- Дважды кликните на URL Rewrite.
- В правой части панели выберите Add Rule(s) и выберите Reverse Proxy.
- В открывшемся окне введите URL целевого сервера, на который вы хотите проксировать запросы (например, `http://localhost:8080`, если ваш сервис YouGile работает на этом порту). Нажмите Apply.

Дополнительная настройка (если требуется):

- В разделе URL Rewrite можно настроить дополнительные параметры, такие как переписывание заголовков или более сложные правила маршрутизации.
- Если ваш целевой сервер работает по HTTPS, убедитесь, что он корректно настроен для приема SSL-трафика.

3. Добавление в IIS поддержки websocket

   Способ 1:

- Откройте Server manager. Кликните Manage → Add Roles and Features
- В Server roles раскройте выпадающий список у Web Server (IIS) → Web Server → Application Development
- Отметьте "галочкой" WebSocket Protocol
- Установите роль

  Способ 2:

- Откройте Control Panel → Programs → Turn Windows features on or off
- В разделе Internet Information Services → World Wide Web Services → Application Development Features активируйте WebSocket Protocol

Дополнительные настройки в IIS

После установки компонента WebSocket выполните следующие действия:

- IIS Manager в панели Connections выберите имя сервера — для настройки на уровне сервера или разверните Sites и выберите конкретный сайт или приложение
- В панели Features View дважды щёлкните Configuration Editor
- В поле Section выберите system.webServer/webSocket

- Установите параметр enabled в значение True для включения поддержки WebSocket
- Убедитесь, что переменная сервера HTTP_SEC_WEBSOCKET_EXTENSIONS добавлена в список разрешённых server variables. По умолчанию IIS не позволяет изменять переменные сервера через правила переписывания, если они не добавлены в этот список
- Добавьте переменную HTTP_SEC_WEBSOCKET_EXTENSIONS в список разрешённых server variables
- В правилах входящего прокси для Web Author добавьте соответствующую переменную сервера

Проверка работы HTTPS

Иногда бывает так, что сертификат для HTTPS настроен неправильно, из-за чего некоторые пользователи не могут войти в мобильное приложение YouGile. При этом, в браузере HTTPS работает нормально. Это происходит из-за того, что сервер присылает неполный сертификат. Проверить это можно, выполнив в командной строке:

```
openssl s_client -connect <домен>:<порт>
```

здесь домен — это домен, с которого доступен YouGile (напр. `yougile.mycompany.com`), порт, как правило, это `443`.

Если есть какие-то ошибки с сертификатом, то они будут написаны в выводе этой команды, например, может присутствовать такая строка:

```
Verify return code: 21 (unable to verify the first certificate)
```

Если коробка YouGile доступна в интернете, то можно также воспользоваться сервисами по проверке правильности настройки https, вот пример таких сервисов:

- SSL Labs
- DigiCert
- SSLShopper

Обычно, при покупке сертификата, вы получаете несколько файлов: сертификат для вашего домена и один или несколько промежуточных сертификатов вплоть до корневого. Их необходимо объединить в один файл и поставить его в качестве сертификата на ваш сервер. Если вы поставите только сертификат для вашего домена, некоторые клиенты не смогут проверить его подлинность, нужно именно объединить эти сертификаты. Чтобы объединить сертификаты, достаточно скопировать текст, который в них содержится в один файл. Посмотрите на сайте издателя вашего сертификата, скорее всего, там есть подробные инструкции.

Обновления

Если есть доступ в интернет

Обновления выходят приблизительно раз в месяц. Чтобы проверить наличие обновлений, выполните в директории yougile:

```
./server task show-updates
```

Для windows:

```
server.exe task show-updates
```

Чтобы установить обновление необходимо сделать следующее:

1. сделать резервную копию yougile (или убедиться, что она есть)
2. остановить сервис yougile
3. выполнить в директории **yougile**: `./server task update latest` (на Windows: `server.exe task update latest`)
4. запустить сервис yougile

Эту процедуру можно выполнять автоматически раз в некоторое время.

Без доступа в интернет

Проверить наличие обновлений можно на сайте https://dist.yougile.com.

Чтобы установить обновление, скачайте архив для нужной операционной системы, затем внутри директории `yougile` создайте директорию `tmp` (если она уже есть, то очистите её содержимое). Распакуйте архив в директорию `tmp`, у вас должно получиться, что в директории `yougile` содержится директория `tmp`, в которой содержится директория `yougile` (из архива) и в ней уже разные файлы. Скорируйте файл `tmp/yougile/tasks/lib/install.js` в директорию `tasks/` внутри основной директории `yougile` (не той, что из архива, а той, где установлена система). И затем, внутри директории, где установлена система выполните команду:

```
./server task install
```

для Windows:

```
server.exe task install
```

Вот полный пример действий по обновлению для Linux:

```
cd /opt/yougile
rm -r tmp
mkdir tmp
```

```
cd tmp/
# скачать нужный файл yougile.tar.gz из dist.yougile.com и поместить в tmp/
# поскольку нет доступа в интернет, это делается вручную
tar -xf yougile.tar.gz
rm yougile.tar.gz
cd ..

cp tmp/yougile/tasks/lib/install.js tasks/
./server task install
```

здесь предполагается, что YouGile установлен в `/opt/yougile`.

Резервное копирование

Резервное копирование (бэкап) в коробочной версии осуществляется методами, принятыми в компании (например, с помощью инструментов `rsync`, `bacula` и т.д.). Необходимо копировать директорию с приложением yougile (ту директорию, которая разархивировывается при установке коробки).

В директории `yougile` ценными являются:

- директория `database` – там хранится база системы
- директория `user-data` – хранятся загруженные файлы пользователей
- `license.key` – файл лицензии
- `conf.json` – настройки

Можно бэкапить отдельно эти файлы и директории, либо всю директорию yougile целиком.

Как часто создавать резервную копию и сколько хранить по времени — вы сами решаете для себя. Резервная копия даёт возможность в случае необходимости откатиться назад на состояние, где всё было нормально, и в этом случае вы потеряете только ту часть работы, которая была произведена после создания резервной копии.

Мы рекомендуем делать бэкап несколько раз в течение рабочего дня, например, в 8, 10, 12, 14, 16, 18, 21 часы. Это гарантирует, что вы не потеряете более 2 часов работы в случае экстренной ситуации.

Отказоустойчивость

Можно организовать высокий уровень отказоустойчивости коробочной версии YouGile. Для этого необходимо выполнить следующий набор рекомендаций.

Настройка доступной памяти

По умолчанию сервис YouGile использует только ограниченных объём доступной памяти на машине (приблизительно 1Гб). Чтобы YouGile использовал бОльшее количество памяти, доступное на машине, необходимо запускать приложение с переменной окружения `NODE_OPTIONS=--max-old-space-size=<память в Мб>` (при использовании systemd, поменять поле Environment в файл сервиса systemd), либо

задать эту переменную в переменных окружения пользователя, под которым запускается YouGile. Количество памяти должно вычисляться из расчёта: вся память доступная на машине минус 300Мб. Пример файла `yougile.service` для `systemd`:

```
[Unit]
Description=yougile

[Service]
WorkingDirectory=/opt/yougile
ExecStart=/opt/yougile/server
Environment="NODE_OPTIONS=--max-old-space-size=5000"
LimitNOFILE=500000
LimitNPROC=500000

[Install]
WantedBy=multi-user.target
```

Бэкапы

Необходимо убедиться, что резервное копирование удовлетворяет требованиям по отказоустойчивости:

- должно быть настроено инкрементальное резервное копирование папок `user-data/` и `database/` с регулярностью 10 мин (или лучше 5 мин если время инкрементального копирования меньше 1 минуты)
- помимо наиболее свежей версии должны быть также доступны точки восстановления 1 час назад, 3 часа назад, 1 день назад, 2 и 3 дня назад (можно больше точек восстановления)
- резервное копирование не должно создавать существенной нагрузки на машине (диск, память, процессор, сеть)
- бэкап должен храниться на другой хост-машине (лучше если в другом датацентре)
- бэкап должен быть доступен для быстрого восстановления.

Резервная машина

Для возможности быстрого восстановления работы YouGile при сбое, необходимо настроить резервную машину с YouGile:

- установить на резервную машину лицензию (запросить в поддержке ключ для новой машины, либо запросить специальный ключ с поддержкой нескольких машин)
- проверить работоспособность резервной машины (зайдя в аккаунт в браузере на резервной машине)
- настроить переключение на аварийный режим по нажатию одной кнопки (выполнению одной команды / запроса).

При переключении в аварийный режим (если основная машина с YouGile доступна, необходимо остановить сервис, после этого выполнить обновление бэкапа). Последний бэкап развернуть на резервной машине и запустить сервис. Публичный ip основной машины должен быть передан резервной машине **(использовать DNS для переключения нельзя)**.

Для переключения в аварийный режим можно настроить автоматику, но переключать обратно в штатный режим нужно только вручную (решение о переключении обратно в штатный режим может принять ответственный сотрудник после анализа ситуации и проверки работоспособности основной машины).

Алертирование

Чтобы можно было следить за доступностью YouGile для пользователей и реагировать на сбои (переключать на резервную машину), необходимо реализовать событийный мониторинг по доступности YouGile — http запрос к адресу `/data/check` должен выдавать status 200. По этому алерту можно судить о доступности системы. Нужно сделать, чтобы по срабатыванию этого алерта происходило аварийное реагирование (ответственные сотрудники должны получать уведомление, например sms, звонок или сообщение в telegram).

Необходимо также сделать событийное алертирование по использованию памяти – оно должно срабатывать, если на машине осталось менее 1 Гб памяти. Это событие указывает на необходимость увеличения количества памяти на машине, даже если затем ситуация исправляется и потребление памяти приходит в норму. Для увеличения памяти создаётся новая машина, для которой отдельно запрашивается лицензионный ключ в поддержке (или используется специальный ключ с поддержкой нескольких машин) и после проверки работоспособности машины, производится переключение и удаление старой машины.

Логирование

Настроить систему логирования для исследования возможных проблем. Необходимо убедиться, что системные логи и логи YouGile сохраняются после перезагрузки машины. Настроить политику ротации этих логов (например, оставлять логи только за последние 30 дней – в зависимости от количества доступного места на диске).

Количественный мониторинг

Убедиться, что есть количественный мониторинг на основной и резервной машине YouGile и на соответствующих хост-машинах. Раз в неделю необходимо проверять потребление ресурсов системой (процессор, память, диск, сеть) и, при необходимости, планировать увеличение ресурсов, либо обращаться за консультацией в поддержку YouGile.

Подключение S3 для хранения файлов

Общая информация

- В YouGile загружаемые пользователями файлы хранятся в директории user-data
- Поддерживаемые инструменты
    - geeseFS (работает лучше для яндекс облака)
    - s3fs-fuse

Реализация (на примере использования GeeseFS)

1. Установить и настроить GeeseFS. Подробная инструкция описана здесь

2. Примонтировать GeeseFS в директорию user-data. Для этого нужно добавить строку в `/etc/fstab` (`/opt/yougile/user-data` при необходимости изменить на свой путь)

```
# /etc/fstab
<имя_бакета>    /opt/yougile/user-data    fuse.geesefs    _netdev,allow_other,--
file-mode=0666,--dir-mode=0777    0    0
```

3. GeeseFS использует статический ключ доступа к Object Storage. Он задается несколькими способами:

- помощью файла credentials, который нужно поместить в директорию ~/.aws/:

```
[default]
  aws_access_key_id=<идентификатор_ключа>
  aws_secret_access_key=<секретный_ключ>
```

- Если файл с ключом находится в другом месте, передайте путь к нему в параметре --shared-config при монтировании бакета:

```
geesefs \
  --shared-config <путь_к_файлу_с_ключом> \
  <имя_бакета> <точка_монтирования>
```

- С помощью переменных окружения:

```
export AWS_ACCESS_KEY_ID=<идентификатор_ключа>
export AWS_SECRET_ACCESS_KEY=<секретный_ключ>
```

Производительность

Скорость работы YouGile сильнее всего зависит от количества задач и объёма данных в текущей открытой компании. Эту информацию по компаниям можно посмотреть с помощью команды `db-stats` (см. раздел Специальные команды YouGile).

YouGile работает быстро, если в каждой из компаний количество задач не превышает 30 тыс. и объём данных не превышает 80Мб (в объём данных не входят заугружаемые файлы, только сами данные задач). В промежутке от 30 тыс. до 50 тыс. задач (и от 80Мб до 120Мб данных) система может начать работать медленнее, а при бОльшем к-ве данных скорость работы может уже быть недопустимой для работы пользователей в системе.

Есть 2 способа контроля производительности в больших командах:

- разбиение работы команды на несколько “компаний”
- удаление (архивирование) старых данных.

Разбиение данных на несколько компаний

В коробочной версии YouGile можно создавать неограниченное количество “компаний”. Каждый пользователь может быть добавлен в несколько компаний одновременно. Если в команде пользуются YouGile более 1000 человек, разбиение на “компании” обязательно для обеспечения долговременного контроля производительности.

Чтобы можно было создавать новые компании необходимо установить поля `multiCompany` и `allowAddCompanies` в файле `conf.json` (см. раздел Настройка параметров YouGile, файл **conf.json**)

Удаление старых данных

Чтобы контролировать количество данных в компании, можно периодически удалять старые данные. Если удалить задачу в системе через интерфейс, она не будет полностью удалена (это сделано для возможности восстановления удалённых задач). Удалённая задача влияет на производительность системы (хотя и меньше), поэтому удалённые задачи необходимо чистить при помощи команды `clean-database` (см. раздел Специальные команды YouGile).

Чтобы массово удалить ненужные задачи, можно воспользоваться функционалом сводок. Для этого необходимо в интерфейсе системы создать сводку, в которой будут по критериям выфильтрованы те задачи, которые необходимо удалить. Затем в окне настройки сводки нужно зажать клавиши `Alt` и `Shift` на клавиатуре и, не отпуская этих клавиш, кликнуть на `Удалить сводку` – появится предупреждение об удалении всех задач в сводке и можно будет согласиться и массово удалить все ненужные задачи. Эта функция доступна, начиная с версии коробки `1.56`.

Если хочется иметь доступ к старым задачам, можно организовать архивную инсталляцию YouGile, где по отдельному адресу будет доступна система со старой версией данных. Для организации такого архива, можно бесплатно получить ключ лицензии в поддержке YouGile (или лицензию с поддержкой нескольких машин).

Таким образом, регулярная процедура очистки старых данных может выглядеть так:

- проверка объёма данных в компаниях при помощи команды `db-stats`
- разворачивание старого состояния базы на другую машину (архив данных)
- удаление старых задач при помощи сводки
- чистка удалённых задач при помощи скрипта `clean-database`

Сбор cpuprofile

В некоторых случаях техподдержка YouGile может запросить профиль нагрузки процессора. Это помогает найти причину проблем с производительностью в конкретном случае и предложить решение проблемы. Для того, чтобы собрать профиль нагрузки (cpuprofile), необходимо:

1. В `conf.json` добавить поле manageKey и поместить туда секретный пароль, который будет использоваться для запроса на сбор профайла, пример:

```
...
"manageKey": "some password",
...
```

2. После этого нужно перезапустить сервер, чтобы настройка применилась.
3. Собирать профайл нужно в момент, когда наблюдаются проблемы с работой системы. Нужно дождаться, когда проблема начнёт проявляться
4. После этого необходимо выполнить curl запрос на машине, где работает yougile:

```
manageKey="some password"
curl -X POST http://localhost:8001/data/profiler/run -H "Content-Type:
application/json" -d "{\"key\": \"$manageKey\", \"seconds\": 100}"
```

5. Запрос будет выполняться 110-200 секунд и после его выполнения в директории yougile/ появится файл `profiler-...cpuprofile`

Запуск YouGile в режиме кластера

В некоторых случаях может потребоваться запустить сервис YouGile в режиме кластера из нескольких процессов на одной машине. Поддержка YouGile может рекомендовать этот вариант если нагрузка на сервис потребует распределения по ядрам. В обычном режиме YouGile использует только одно ядро процессора. Здесь далее будет разобрана настройка варианта разделения на 3 процесса на одной машине. Также возможно разделение на несколько машин и на большее количество процессов, эти варианты может предложить поддержка YouGile при необходимости.

Настройка 3-х процессов на одной машине

В файл `conf.json` необходимо добавить следующий блок:

```
  "cluster": {
    "bootstrapUrl": "http://localhost:8001",
    "cookie": "<secret cookie>",
    "nodes": {
      "http://localhost:8001": "account-main",
      "http://localhost:8002": "company-1/1",
      "http://localhost:8003": "user-events"
    }
  }
```

Затем добавить в директорию `yougile/` дополнительные конфигурационные файлы:

`conf-account.json`:

```
{
  "include": "./conf.json",
  "clusterNodeUrl": "http://localhost:8001",
  "port": 8001
}
```

conf-company.json:

```
{
  "include": "./conf.json",
  "clusterNodeUrl": "http://localhost:8002",
  "port": 8002
}
```

conf-user-events.json:

```
{
  "include": "./conf.json",
  "clusterNodeUrl": "http://localhost:8003",
  "port": 8003
}
```

Здесь `<secret cookie>` – это сгенерированная случайная строка, которая работает как пароль для опознавания нод кластера друг другом. Эта строка должна быть одна и та же во всех конфигурационных файлах.

Далее необходимо создать 3 процесса: `yougile-account`, `yougile-company` и `yougile-user-events`, каждый из которых запускает сервис с соответствующим конфигурационным файлом. Пример для `systemd`:

`yougile-account.service`

```
[Unit]
Description=yougile-account

[Service]
WorkingDirectory=/opt/yougile
ExecStart=/opt/yougile/server --conf conf-account.json
Environment="NODE_ENV=production"
Environment="NODE_OPTIONS=--max-old-space-size=10000"
Environment="HOME=/root"
LimitNOFILE=500000
LimitNPROC=500000

[Install]
WantedBy=multi-user.target
```

yougile-company.service

```
[Unit]
Description=yougile-company

[Service]
WorkingDirectory=/opt/yougile
ExecStart=/opt/yougile/server --conf conf-company.json
Environment="NODE_ENV=production"
Environment="NODE_OPTIONS=--max-old-space-size=10000"
Environment="HOME=/root"
LimitNOFILE=500000
LimitNPROC=500000

[Install]
WantedBy=multi-user.target
```

yougile-user-events.service

```
[Unit]
Description=yougile-user-events

[Service]
WorkingDirectory=/opt/yougile
ExecStart=/opt/yougile/server --conf conf-user-events.json
Environment="NODE_ENV=production"
Environment="NODE_OPTIONS=--max-old-space-size=10000"
Environment="HOME=/root"
LimitNOFILE=500000
LimitNPROC=500000

[Install]
WantedBy=multi-user.target
```

В этом примере каждому процессу выделяется по 10Гб оперативной памяти (`max-old-space-size`) и указывается домашняя директория `/root`. Замените эти параметры, при необходимости. См. также Запуск, остановка. Настройка сервиса

Необходимо убедиться, что обычный процесс YouGile, который не был настроен на кластеризацию, остановлен. После этого запустить эти 3 процесса и проверить, что система работает в браузере или в десктоп-приложении.

Интеграция с ActiveDirectory

В YouGile можно управлять доступом пользователей в систему через ActiveDirectory.

В AD нужно создать группу, которая будет отвечать за наличие доступа пользователя в YouGile. Все пользователи, которые будут добавлены в эту группу, должны иметь уникальное поле mail в AD — это поле будет служить логином в YouGile, а пароль в AD будет служить паролем в Yougile.

В файл conf.json необходимо добавить настройки по следующему примеру:

```
...
"init": {
  "scripts": ["auth/auth-sync-ldap.js", "auth/check-sync.js"],
  "auth": "auth/auth-ldap.js"
},
"activeDirectory": {
  "url": "ldaps://mycompany.com",
  "baseDN": "dc=mycompany,dc=com",
  "username": "yougile_ad",
  "password": "***"
},
"activeDirectoryOpts": {
  "includeDeleted": false,
  "filter": "&(objectClass=user)(mail=*)
(memberOf=CN=yougile_user,OU=app,DC=mycompany,DC=com)"
},
...
```

После перезапуска сервиса yougile, в систему смогут входить только те пользователи, которые подходят под условие, указанное в поле `filter` (в данном примере это пользователи из группы yougile_user).

Если в ActiveDirectory часть пользователей убрать из группы, которая указана в поле `filter`, то они удалятся из YouGile, но если таких пользователей будет больше 10, то удаление не произойдёт. Это сделано для защиты от сбоев в работе ActiveDirectory. Чтобы увеличить это ограничение, можно установить в `conf.json` парамерт `activeDirectoryMaxDelete`, пример:

```
...
"activeDirectoryMaxDelete": 20,
...
```

Также можно подключить одновременно несколько серверов ActiveDirectory, в этом случае, в YouGile будут добавляться все пользователи, которые есть во всех указанных серверах. Для этого в полях `activeDirectory` и `activeDirectoryOpts` необходимо указать массив настроек. Пример:

```
...
"init": {
  "scripts": ["auth/auth-sync-ldap.js", "auth/check-sync.js"],
  "auth": "auth/auth-ldap.js"
},
"activeDirectory": [
  {
```

```
    "url": "ldaps://domain1.com",
    "baseDN": "dc=domain1,dc=com",
    "username": "yougile_ad1",
    "password": "***"
  },
  {
    "url": "ldaps://domain2.com",
    "baseDN": "dc=domain2,dc=com",
    "username": "yougile_ad2",
    "password": "***"
  }
],
"activeDirectoryOpts": [
  {
    "includeDeleted": false,
    "filter": "&(objectClass=user)(mail=*)
(memberOf=CN=yougile_user,OU=app,DC=domain1,DC=com)"
  },
  {
    "includeDeleted": false,
    "filter": "&(objectClass=user)(mail=*)
(memberOf=CN=yougile,OU=app,DC=domain2,DC=com)"
  }
],
...
```

При этом команда `check-ldap` не будет работать, чтобы проверять настройки, нужно оставить в conf.json только одно подключение к ActiveDirectory (без массива) и его проверять через `check-ldap`.

Управление группами и ролями через Active Directory

Создайте свою роль и назначьте ей права на определенные действия с проектами, досками, колонками и задачами. Таким образом можно разграничить просмотр/редактирование выбранных объектов в проекте. Функция доступна начиная с версии 1.95.

Настройка конфигурации для работы через Active Directory

Пример настроек конфигурации conf.json:

```
...
"init": {
  "scripts": ["auth/auth-sync-ldap.js", "auth/check-sync.js"],
  "auth": "auth/auth-ldap.js"
},
"activeDirectory": {
  "url": "ldap://domain.you",
  "baseDN": "dc=domain,dc=you",
  "username": "admin@domain.you",
  "password": "***"
}
...
```

При этом фильтрация в AD настраивается следующим образом:

```
...
"activeDirectoryOpts": {
 "includeDeleted": false,
 "filter": "(&(objectClass=user)(mail=*)(|
(memberOf=CN=yougile_managers,OU=app,DC=domain,DC=you)
(memberOf=CN=yougile_watcher,DC=domain,DC=you)))"
,
"roleUsers": {"Manager":"memberOf=CN=yougile_watcher,DC=domain,DC=you",

"Наблюдатель":"memberOf=CN=yougile_managers,OU=app,DC=domain,DC=you"}
}
...
```

Настройка конфигурации для работы через файл

Добавьте параметры в conf.json:

```
...
"init": {
 "scripts": ["auth/auth-sync.js", "auth/check-sync.js"],
 "auth": "auth/auth.js"
},
...
```

Для создания ролей пользователей используйте файл **users.csv** в папке **database**

```
admin@admin.ad,Admin,yourpassword
some-user1@mycompany.com,Name user1, yourpassword,Manager
some-user3@mycompany.com,Name user3,yourpassword,Наблюдатель
```

Формат в файле должен содержать поля:

- почта, имя, пароль, роль;
- почта, имя, пароль (если пользователю не нужна роль).

Создавать и изменять роли может тот, у кого есть проекты и кто является Управляющим в них.

Интеграция с OpenId Connect

В YouGile встроена возможность использовать OpenId Connect для аутентификации пользователей, например, можно реализовать вход в систему пользователей через KeyCloak и другие сервисы, позволяющие настроить SSO через OpenId Connect. Пользователи при этом будут входить в аккаунт

YouGile по кнопке, которая будет переводить пользователя на страницу аутентификации OpenId провайдера и после успешной аутентификации перенаправит пользователя в YouGile.

При этом можно выбрать 2 варианта для входа пользователей:

- использовать только OpenId для входа
- наряду с OpenId использовать вход через логин и пароль для пользователей, которые добавляются отдельно через интерфейс приглашения пользователей или через команды на сервере

Также можно настроить правила, по которым войти смогут не все пользователи, например, можно ограничить возможность входа только для участников определённой группы и т.д.

Когда пользователь входит первый раз, то автоматически создаётся его учётная запись в YouGile с именем и фамилией и email, которые предоставляются через OpenId (используются поля `family_name`, `given_name` и `email`, обычно эти поля доступны из скоупов `openid` и `email`, обязательным является `email` для создания учётной записи) и эта учётная запись автоматически добавляется в основную компанию (та компания в YouGile, которая была создана первой).

Если сессия OpenId истекла или была удалена вручную администратором, то пользователя разлогинит из YouGile. Также если пользователь будет удалён из OpenId или изменятся условия, по которым ограничивается вход (напр. участие в группе), то пользователя также разлогинит. Сама учётная запись в YouGile при этом не удаляется, в неё нельзя войти, но она сохраняется – это делается специально, чтобы можно было после удаления пользователя найти его задачи и переназначить, а также восстановить его при необходимости. Чтобы удалить ненужных пользователей, можно использовать команду `remove-user`, см. Специальные команды YouGile.

Пример настройки интеграции

Необходимо создать Client в OpenId провайдере и получить id клиента и секрет клиента.

Далее нужно в `conf.json` добавить настройки интеграции, пример:

```
{
  // стандартные настройки
  "port": 8001,
  "mainPageUrl": "https://yougile.mysite.org",
  // ...

  // настройки интеграции с OpenId
  "openId": {
    "issuer": "https://keycloak.mysite.org/realms/Yougile",
    "signInButtonText": "Войти через OpenId",

    "allowOnlyOpenId": true,

    "config": {
      "client_id": "yougile-oidc",
      "client_secret": "2OT0XXzffAbPINZVk0An49AM8uQwcTyG"
    },
    "scope": "openid email my-custom-scope",
```

```
    // дополнительные параметры, нужны не всегда

    "filterUser": "user.myvalue?.includes('/yg-members')",
    "tokenTtl": 60000
  }
}
```

В этом примере:

- `issuer` – адрес OpenId провайдера, который будет использоваться для аутентификации пользователей. Пример для keycloak: `https://kc.my_site.org/realms/MyRealm`
- `signInButtonText` – текст кнопки входа в систему пользователей YouGile.
- `allowOnlyOpenId` – разрешить вход в YouGile только через OpenId провайдер, войти через login/пароль становится невозможно, даже для зарегистрированных пользователей, если этот парамерт `false`, то можно входить обоими способами.
- `client_id` и `client_secret` – id и секрет клиента в OpenId провайдере.
- `scope` – набор scope-ов, которые предоставляются YouGile при аутентификации. `openid` и `email` – обязательные scope-ы, они нужны для создания учётной записи в YouGile, также можно добавить дополнительные scope-ы и использовать их для ограничения входа (напр. по группе пользователя) через фильтр `filterUser`.
- `filterUser` – если не указывать этот параметр, то все пользователи, которые есть в OpenId провайдере, смогут войти в YouGile. В этом параметре можно указать javascript-выражение, которое может использовать переменную `user`, в которой находятся данные, предоставляемые о пользователе OpenId (согласно scope-ам), см. также ниже «Частые вопросы по настройке».
- `tokenTtl` – время жизни токена в миллисекундах, если не указывать этот параметр, то при каждом запросе YouGile будет обращаться в OpenId провайдер с access_token (или refresh_token), в случае, когда пользователей много – это может негативно влиять на производительность провайдера и тогда рекомендуется указать этот параметр. Если параметр указан, то, например, в случае удаления сессии пользователя в OpenId провайдере, он не сразу будет разлогинен в YouGile, а через некоторое время (примерно, равное tokenTtl).

Частые вопросы по настройке

- чтобы изменения в `conf.json` применились, необходимо перезапустить сервис YouGile.
- если для шифрования используется самоподписанный сертификат или сертификат, подписанный своим центром сертификации, то нужно использовать `NODE_EXTRA_CA_CERTS=путь_к_сертификату` – в качестве переменной окружения при запуске YouGile. На время настройки и отладки можно использовать переменную окружения `NODE_TLS_REJECT_UNAUTHORIZED=0`, чтобы убрать ошибки с сертификатами, но при переходе на боевой режим этот вариант использовать нельзя.
- если возникают проблемы с использованием `filterUser`, напр. мы хотим, чтобы могли входить только пользователи с email-ом из домена `mycompany.com`, и мы пытаемся указать это в `filterUser`: `user.email.includes('@mycompany.com')`, но это не работает как надо, тогда можно указать выражение, которое будет также логировать значение `user` или какие-то выражения для отладки фильра, например: `console.log(user) || user.email.includes('@mycompany.com')`, чтобы понять причину неправильной работы.

- чтобы добавить информацию о группе пользователя в keycloak, необходимо в нужном realm добавить в `Client scopes` (`Create client scope`), затем перейти в добавленный scope, во вкладке `Mappers` добавить mapper, выбрав далее `By configuration` и выбрать `Group Membership`, причём, необходимо обязательно указать `Token claim name` – это имя будет доступно в объекте `user` в `filterUser`. После этого, необходимо перейти в `Clients`, выбрать нужного клиента и перейти во вкладку `Client scopes` и добавить созданный scope. Если пользователя нет ни в одной группе, то поле с группами будет отсутствовать, поэтому filterUser лучше указывать таким образом: `user.my_group_claim_name?.includes('/yougile-users')`

Дополнительная интеграция с SSO провайдерами

Это более старый вариант интеграции, рекомендованный вариант описан выше, см. Интеграция с OpenId Connect.

Этот вариант интеграции с OpenId Connect работает по схожей механике, что и интеграция с ActiveDirectory – система сразу создаёт все учётные записи, которые может получить от OpenId провайдера и поддерживает этот список в актуальном состоянии, при этом вход производится по логину и паролю, которые проверяются OpenId провайдером (напр. KeyCloak).

- Для активации провайдера нужно заполнить его параметры в conf.json, а также указать название провайдера в параметре `provider`
- URL для параметров `tokenUrl` и `userInfoUrl` вы можете найти в документации вашего SSO провайдера

Настройка интеграции

- Для настройки интеграции необходимо добавить в файл conf.json следующий блок

```
  "init": {
  "scripts": [
    "auth/auth-sync-oidc.js",
    "auth/check-sync-oidc.js"
  ],
  "auth": "auth/auth-oidc.js"
},
"provider": "sso-provider-name",
"sso-provider-name": {
  "serverUrl": "sso-server-url",
  "realm": "your-realm",
  "clientId": "your-client-id",
  "credentials": {
    "secret": "your-secret"
  ,
  "tokenUrl": "sso-server-get-token-url",
  "userInfoUrl": "sso-server-get-user-info-url",
  "publicKey": "your-public-key"
},
```

Пример настройки для Keycloak

- В настройках клиента в keycloak нужно включить `Client authentication` и `Service accounts roles`
- В разделе "Credentials" в "Client Authenticator" следует выбрать "Client Id and Secret"
- `publicKey` можно найти в разделе "Realm settings" => "Keys". Необходимо взять ключ, имеющий тип RS256
- `secret` можно найти в настройках клиента в разделе "Clients" => "Client_name" => "Credentials" => поле "Client Secret"
- Для работы Keycloak необходимо выдать клиенту следующие дополнительные роли:
  - realm-management - query-users
  - realm-management - manage-users
  - realm-management - view-users
  - broker - read-token

Управление списком пользователей через файл

По умолчанию, добавление пользователей происходит через интерфейс (приглашение пользователя по почте). Но можно настроить, чтобы можно было управлять списком пользователей через файл.

Для этого добавьте в файл `conf.json` следующее:

```
"init": {
  "scripts": ["auth/auth-sync.js", "auth/check-sync.js"],
  "auth": "auth/auth.js"
}
```

Создайте в директории `database` файл `users.csv`, где каждая строка – это email, имя и пароль пользователя через запятую. Пример содержимого users.csv:

```
admin@mycompany.com,Admin,pass1
some-user@mycompany.com,Some user,pass2
```

Перезапустите YouGile, после этого вы можете редактировать файл `users.csv` и изменения будут автоматически применяться без необходимости перезапуска YouGile.

Специальные команды YouGile

В YouGile есть набор команд, которые помогают выполнять часто встречающиеся задачи администрирования. Чтобы посмотреть список команд, в терминале, в директории `yougile` наберите:

```
./server task
```

для Windows:

```
server.exe task
```

Чтобы выполнить команду, необходимо в терминале перейти в директорию `yougile` и выполнить:

```
./server task <название команды> [параметры]
```

для Windows:

```
server.exe task <название команды> [параметры]
```

Доступные команды:

- `show-updates` — показывает список доступных обновлений (если есть доступ в интернет — обращается к dist.yougile.com)
- `update` — обновляет YouGile (если есть доступ к dist.yougile.com)
- `list-companies` — показывает список всех компаний
- `list-users` — показывает список пользователей YouGile
- `set-password` — позволяет установить пароль для пользователя (если нет интеграции с AD или управления через файл)
- `remove-user` — удаляет пользователя (если нет интеграции с AD или управления через файл)
- `change-user` — позволяет сделать пользователя админом или наоборот, убрать из админов
- `check-ldap` — проверяет настройки интеграции с ActiveDirectory, т.е. по полям `activeDirectory` и `activeDirectory` в файле `conf.json` показывает спикок email-ов, которые подходят под критерии по AD
- `add-admin-to-company` — добавляет пользователя администратором в указанную компанию
- `change-email` — изменяет email пользователя, для применения изменений пользователю необходимо заново авторизоваться в системе
- `set-user-name` – позволяет изменить отображаемое имя пользователя
- `check-data` — проверяет корректность файлов данных YouGile
- `check-ldap` — позволяет проверить правильность ldap-запроса при интеграции с ActiveDirectory
- `cleanup-database` — чистит базу данных от удалённых задач
- `db-stats` — показывает информацию по размеру данных компании
- `show-license` — показывает информацию о лицензии
- `check-json` — проверяет все файлы JSON в текущей директории
- `show-usage` — показывает количество пользователей
- `show-usage week` — показывает количество пользователей, активных за неделю
- `show-usage list` — показывает полный список всех пользователей с их датой последней активности. Информация по активности хранится не более 3 месяцев