Суперапп VK WorkSpace

Настройки безопасности Супераппа

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

В инструкции описаны настройки безопасности клиентского приложения VK WorkSpace — Сураппа (ранее — VK Teams). Документ предназначен для использования администраторами организации.

Предварительные действия

Ознакомьтесь с этим разделом, если вы включаете следующие настройки:

- Запретить создание скриншотов и запись экрана.
- Запретить скачивание и шаринг файлов.
- Запретить копирование текста из Сураппа.
- Включить доступ к Сураппу по паролю.
- Отображать баннер о подключенном VPN.

Данные настройки можно включить двумя способами — через конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** или через Панель администратора (при ее наличии).

Если вы включаете настройки конфигурационный файл, пропустите данный раздел — он актуален только для включения безопасности через Панель администратора. Перейдите к необходимому разделу статьи ниже.

Если вы включаете настройки безопасности через Панель администратора, выполните следующие шаги:

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и убедитесь, что в нем есть переменные с любым значением:

   ```
   "screenshots-allowed": false #запрещает создание скриншотов и записи экрана
   "disable-downloads": true #запрещает скачивание и шаринг файлов
   "copy-protection": true #запрещает копирование текста из Сураппа
   "pin-required": true #включает доступ к Сураппу по паролю
   "vpn-detect": true #включает отображение баннера о подключенном VPN
   ```

   Если переменных нет — добавьте их.

2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

4. Подключитесь к серверу Супераппа и сгенерируйте client_id и client_secret:

```
creds=$(curl -s http://onpremise.stroma-1.weave.local:8036/api/v1/private/
generate_credentials); \
    client_id=$(echo $creds | jq -r ".client_id"); \
    client_secret=$(echo $creds | jq -r ".client_secret"); \
    client_secret_hash=$(echo $creds | jq -r ".client_secret_hash"); \
    echo "tokeeper.request.add_application('biz', 'biz admin', '$client_id',
'$client_secret_hash', '')" | sudo tarantoolctl eval tokeeper-1

echo $client_id
echo $client_secret
```

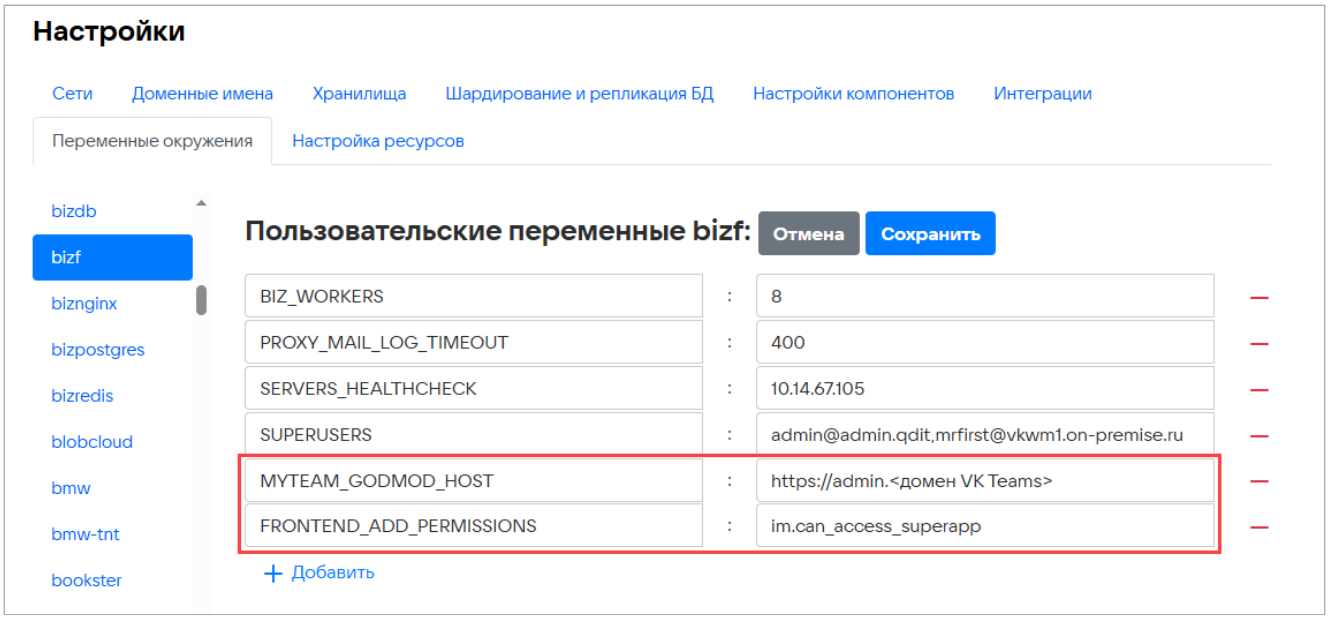
   Запомните выводы команд.

5. Перейдите в инсталлятор VK WorkSpace по адресу http://server-ip-address:8888 в раздел **Настройки** → **Интеграции** и включите переключатель **VK Teams поддерживает авторизацию ЕСИА**.
6. Укажите client_id и client_secret и нажмите на кнопку **Сохранить**.
7. Перейдите в раздел **Настройки** → **Переменные окружения**.
8. В левом боковом меню найдите bizf и нажмите на иконку 
9. Нажмите на кнопку **Добавить** и добавьте переменные со следующими значениями:

   MYTEAM_GODMOD_HOST: https://admin.<домен Суперапп>

   FRONTEND_ADD_PERMISSIONS: im.can_access_superapp

> **Внимание**
>
> Не перезаписывайте значение переменной FRONTEND_ADD_PERMISSIONS. Найдите переменную в таблице и добавьте для нее значение im.can_access_superapp без удаления ранее добавленных значений



10. Нажмите **Сохранить**.

11. Выполните шаг up_container для контейнера bizf.
12. Перейдите в расширенную панель администратора по адресу https://biz.<ваш домен>/admin/features/ и добавьте фичу **tmp-myteam-plugins-configuration**.

Шаги 1-12 выполняются один раз. Далее вы можете управлять настройками в Панели администратора.

Запретить использование устаревших версий Супераппа

Начиная с версии 24.2 вы можете запретить пользователям использовать клиентские приложения, версия которых ниже минимально поддерживаемой версии (устанавливается администратором организации). По умолчанию запрет не включен.

Если запрет установлен и версия клиентского приложения ниже минимально поддерживаемой, пользователю для продолжения работы необходимо обновить приложение.

Чтобы установить запрет:

1. В конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** в секции **updates** установите минимально поддерживаемую версию для каждой платформы:

   ```
   "min_supported_version": {
     "version": "10.6.0",
     "build": "528",
     "full_version": "10.6.0.528"
   ```

   где:

   - version — номер версии.
   - build — номер сборки. Если номер сборки неизвестен, допустимое значение — 0.
   - full_version — номер версии и номер сборки, разделенные точкой (full_version: version.build).

   Если минимально поддерживаемая версия указана некорректно, запрет на использование устаревших версий клиентских приложений не будет выполняться.

2. В поле **force_update_enabled** установите запрет на использование устаревших версий клиентских приложений:

   ```
   "force_update_enabled": true
   ```

   где:

   - true — включает запрет на использование устаревших версий клиентских приложений.
   - false — выключает.

3. Укажите в поле **updates.customLandingUrl** адрес dl-лендинга, с которого можно скачать обновление для клиентского приложения:

```
"customLandingUrl": "https://dl.<your_domain>.ru",
```

Если поле **customLandingUrl** не заполнено, пользователю будет предложено скачать обновление с apps.<platform>.url.

Пример настройки запрета в **myteam-config.json** для всех платформ:

```
"updates": {
    "customLandingUrl": "https://dl.<YOUR_DOMAIN>.ru",
    "android": {
      "min_supported_version": {
        "version": "10.6.0",
        "build": "528",
        "full_version": "10.6.0.528"
      },
      "force_update_enabled": true
    },
    "ios": {
      "min_supported_version": {
        "version": "10.6",
        "build": "90186",
        "full_version": "10.6.90186"
      },
      "force_update_enabled": true
    },
    "linux_x64": {
      "min_supported_version": {
        "version": "10.0",
        "build": "9706",
        "full_version": "10.0.9706"
      },
      "force_update_enabled": true
    },
    "mac_x64": {
      "min_supported_version": {
        "version": "5.0",
        "build": "9702",
        "full_version": "5.0.9702"
      },
      "force_update_enabled": true
    },
    "win_x32": {
      "min_supported_version": {
        "version": "10.0",
        "build": "9707",
        "full_version": "10.0.9707"
      },
      "force_update_enabled": true
    }
  }
```

4. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

5. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Отключить синхронизацию черновиков между клиентскими приложениями

Начиная с версии 25.2 вы можете отключить синхронизацию черновиков сообщений между клиентскими приложениями одного пользователя, чтобы исключить утечку данных. После отключения синхронизации черновики продолжат работать в рамках одного клиентского приложения.

Чтобы отключить синхронизацию черновиков:

1. В конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** установите для поля **draft-enabled** значение false.
2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

   ```
   kubectl delete pods -n vkteams -l app=myteam-admin
   ```

Запретить создание скриншотов и запись экрана

Вы можете ограничить на уровне домена создание скриншотов и записей экрана в клиентских приложениях, чтобы предотвратить утечку критически важной или служебной информации. Опция не работает в веб-версиях.

Для Android на уровне системы реализована защита, блокирующая возможность создания скриншотов и записи экрана. При попытке сделать скриншот или запись в результате будет черный экран.

Для iOS отображается визуальное предупреждение о запрете на создание скриншотов. При попытке сделать скриншот в результате будет белый экран.

Для десктоп-приложений:

- Windows — реализована защита от скриншотов и блокировка распространённых средств записи экрана (например, Bandicam). При попытке сделать скриншот, на нем не отобразится окно приложения. Аналогично и при записи экрана.
- macOS — внедрены ограничения на стандартные сценарии снятия скриншотов, с учётом системных разрешений. При попытке сделать скриншот, на нем не отобразится окно приложения

> **Внимание**
>
> Информация о попытке сделать скриншот или запись экрана не передается администраторам или службе безопасности.

Вы можете включить опцию двумя способами — через конфигурационный файл или при помощи Панели администратора VK WorkSpace (при наличии).

Через конфигурационный файл

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и установите для параметра **screenshots-allowed** значение false.
2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

   ```
   kubectl delete pods -n vkteams -l app=myteam-admin
   ```

Через Панель администратора

1. Перейдите в Панель администратора по адресу https://biz.<ваш домен>/ в раздел **Суперапп**.
2. Включите **Защита от скриншотов и записи экрана**.

Запретить скачивание и шаринг файлов

Вы можете запретить пользователям мобильных устройств скачивать файлы и делиться ими через Суперапп. Опция не работает для приложений на Windows, Mac и в веб-версиях и действует на уровне клиентского приложения.

Примечание

Вы также можете настроить запрет на скачивание файлов из Мессенджера в зависимости от IP-адреса, операционной системы, устройства и браузера пользователя. Такой запрет будет действовать на уровне сервера. Подробнее — см. инструкцию по настройке.

Запрет действует на:

- Скачивание файлов из веб-приложений (мини-аппов). Шаринг при этом остается доступным.
- Скачивание и шаринг файлов из Мессенджера (помимо тех, что возможно просмотреть просмотрщиком Мессенджера).
- Скачивание и шаринг файлов из Почты (помимо тех, что возможно посмотреть просмотрщиком Почты).

При этом у пользователей останется возможность пересылать файлы внутри Мессенджера и Почты.

Внимание

Если в инсталляции есть Диск и вы хотите ограничить шаринг файлов из него — необходимо отдельно включить запрет просмотров файлов вне инсталляции в настройках Диска. В таком случае пользователи смогут делиться файлами, но просмотр будет запрещен вне аккаунтов домена.

Запрет скачивания запрещает попытки приложения сохранить данные вне защищенного криптоконтейнера (подробнее о шифровании — см. статью). Сохранение данных кэша производится в зашифрованном виде. При включенном запрете просмотр во внешних приложениях блокируется, просмотр файлов, которые невозможно посмотреть системными методами (которым запрещен шаринг) невозможен. Таким образом, информация никогда не выйдет за контур Супераппа.

Передача зашифрованных файлов между просмотрщиком и Супераппом происходит либо через шифрованный поток, либо через файл в временной директории, к которой нет доступа ни у кого кроме приложения.

Запрет Root и Jailbreak

Root и Jailbreak расширяют права пользователей, предоставляя им возможности, которые потенциально могут нарушить защищенность проекта

- Root (Android) —определяет root-устройства и блокирует взаимодействие с приложением.
- Jailbreak (iOS) — при обнаружении действует аналогично, не конфигурируется.

Вы можете включить запрет на скачивание и шаринг двумя способами — через конфигурационный файл или при помощи Панели администратора VK WorkSpace (при наличии).

Через конфигурационный файл

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и установите для параметра **disable-downloads** значение true.

2. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Через Панель администратора

1. Перейдите в раздел **Суперапп** Панели администратора.
2. Включите опцию **Запрет на скачивание и шаринг файлов**.

Запретить копирование текста из Супераппа

Вы можете запретить пользователям мобильных устройств копировать текст из Супераппа в другое приложение. Опция не работает в приложении на Windows, Mac и в веб-версиях.

Вы можете включить опцию двумя способами — через конфигурационный файл или при помощи Панели администратора VK WorkSpace (при наличии).

Через конфигурационный файл

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и установите для параметра **copy-protection** значение true.
2. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Через Панель администратора

1. Перейдите в раздел **Суперапп** Панели администратора.

2. Включите опцию **Запрет на копирование в буфер обмена**.

Включить доступ к Супераппу по паролю

Вы можете включить для всех пользователей доступ в приложение по паролю.

Если настройка не была включена ранее, при первом входе приложение предложит пользователю создать пароль. Пароль может быть разный на разных устройствах и сбрасывается, если пользователь заново входит в свою учетную запись.

> **Примечание**
>
> Пользователи также могут самостоятельно включать доступ по паролю в настройках Супераппа.

Вы можете включить опцию двумя способами — через конфигурационный файл или при помощи Панели администратора VK WorkSpace (при наличии).

Через конфигурационный файл

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и установите для параметра **pin-required** значение true.
2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

   ```
   kubectl delete pods -n vkteams -l app=myteam-admin
   ```

Через Панель администратора

1. Перейдите в раздел **Суперапп** Панели администратора.
2. Включите опцию **Обязательный код-пароль**.

Отображать баннер о подключенном VPN

Опция предназначена для организаций, сотрудникам которых не рекомендуется работать с конфиденциальными данными на устройствах с активированным VPN. Настройка доступна для декстоп- и мобильной версии Суперапа.

Вы можете предупреждать пользователей, что на устройстве подключен VPN. Это поможет избежать перехвата чувствительной информации и низкой скорости работы приложения. При включении настройки пользователь увидит баннер с предупреждением в момент запуска приложения. При этом настройка не запрещает пользователю использовать приложение с включенным VPN.

> ⚠ **Внимание**
>
> Опция не заменяет решения по контролю трафика. Если пользователь использует VPN и получил уведомление, информация об этом не передается администратору или сотрудникам отдела безопасности.

Вы можете включить опцию двумя способами — через конфигурационный файл или при помощи Панели администратора VK WorkSpace (при наличии).

Через конфигурационный файл

1. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и установите для параметра **vpn-detect** значение true.
2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

   ```
   kubectl delete pods -n vkteams -l app=myteam-admin
   ```

Через Панель администратора

1. Перейдите в раздел **Суперапп** Панели администратора.
2. Включите опцию **Обнаружение VPN**.

Скрыть содержимое пуш-уведомлений

Вы можете скрыть содержимое пуш-уведомлений на мобильных устройствах пользователей, чтобы защитить данные и избежать утечек информации.

При включении настройки в пуш-уведомлениях не будет видно:

- Содержимое сообщения.
- Имя отправителя и получателя.
- Название группы/канала/бота.

При включении настройки:

- Всплывающие уведомления на веб- и декстоп-клиентах отображаются согласно настройкам клиентов,
- В настройках мобильных приложений приватность уведомлений включена по умолчанию и недоступна для изменения пользователями.

Настройка доступна на уровне всей инсталляции и влияет на все группы/каналы/личные сообщения для всех пользователей без исключения.

Подробнее о работе сервисов уведомлений описано в документации по архитектуре (не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом).

Чтобы скрыть содержимое пуш-уведомлений:

Шаг 1. Включите отправку пуш-уведомлений через сервис VKTPusher

1. Откройте на редактирование конфигурационный файл сервиса Boss в режиме суперпользователя:

   ```
   sudo vi /usr/local/etc/k8s/helmwave/projects/boss/values/boss/bos-pre.tcl.yml
   ```

2. Для параметра **set PNOTIFY_VKT_PUSHER_ENABLE** укажите значение «1» и сохраните изменения:

   ```
   set PNOTIFY_VKT_PUSHER_ENABLE 1
   ```

3. Примените настройку.

   Для инсталляции на одну виртуальную машину выполните команду:

   ```
   sudo hwup -t boss
   ```

   Для кластерной инсталляции:

   ```
   im_deployer --helmwave --update --hw-once --hw-project boss
   ```

Шаг 2. Настройте сервис VKTPusher

1. Откройте на редактирование конфигурационный файл сервиса VKTPusher в режиме суперпользователя:

```
sudo vi /usr/local/etc/k8s/helmwave/projects/vktpusher/values/vktpusher/vktpusher.yml
```

2. Для параметра **erase_sensitive_push_content** укажите значение true и сохраните изменения:

```
erase_sensitive_push_content: true #включаем скрытие контента уведомлений
```

3. Примените настройку.

   Для инсталляции на одну виртуальную машину выполните команду:

```
hwup -t vktpusher
```

   Для кластерной инсталляции:

```
im_deployer --helmwave --update --hw-once --hw-project vktpusher
```

Шаг 3. Настройте myteam-config

1. Откройте на редактирование конфигурационный файл myteam-config в режиме суперпользователя:

```
sudo vi /usr/local/nginx-im/html/myteam/myteam-config.json
```

2. Добавьте следующие настройки в файл и сохраните изменения:

```
"force-hide-notification-all-data": true, #вместо текста уведомления отображаем «Новое сообщение», используется для старых клиентов с версией ниже 25.4
"disable-notifications-privacy-settings": true #отключает возможность менять параметры «Скрыть текст»/«Скрыть отправителя» в настройках клиента (параметры выставляются в значение «Включено»), используется для новых клиентов с версии 25.4 и выше
```

3. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

   Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

4. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Переключиться на провайдера пуш-уведомлений RuStore

Вы можете настроить отправку пуш-уведомлений через RuStore, если не хотите использовать зарубежных провайдеров или на мобильных устройствах пользователей отсутствуют Google Services.

Чтобы пользователи могли получать пуш-уведомления через RuStore, необходимо выполнение следующих условий:

1. Приложение RuStore должно быть установлено на мобильных устройствах пользователей.
2. Приложению RuStore разрешена работа в фоновом режиме. Если разрешения нет, пуш-уведомления будут приходить со значительной задержкой.
3. Пользователь должен авторизоваться в приложении RuStore.

Если отправка пуш-уведомлений через RuStore включена и приложение RuStore не установлено, на мобильных устройствах пользователя может отображаться баннер о необходимости установить приложение (настройки описаны ниже).

Чтобы настроить отправку пуш-уведомлений через RuStore:

Шаг 1. Включите отправку пуш-уведомлений через сервис VKTPusher

1. Откройте на редактирование конфигурационный файл сервиса Boss в режиме суперпользователя:

   ```
   sudo vi /usr/local/etc/k8s/helmwave/projects/boss/values/boss/bos-pre.tcl.yml
   ```

2. Для параметра **set PNOTIFY_VKT_PUSHER_ENABLE** укажите значение «1» и сохраните изменения:

   ```
   set PNOTIFY_VKT_PUSHER_ENABLE 1
   ```

3. Примените настройку.

   Для инсталляции на одну виртуальную машину выполните команду:

   ```
   sudo hwup -t boss
   ```

   Для кластерной инсталляции:

   ```
   im_deployer --helmwave --update --hw-once --hw-project boss
   ```

Шаг 2. Настройте myteam-config

1. Откройте на редактирование конфигурационный файл myteam-config в режиме суперпользователя:

   ```
   sudo vi /usr/local/nginx-im/html/myteam/myteam-config.json
   ```

2. Добавьте в файл секцию **push-settings** и сохраните изменения:

```
"push-settings": {
    "push-provider": "rustore",
    "use-rustore-if-fcm-unavailable": true,
    "show-download-rustore-screen": true,
    "show-download-rustore-screen-if-no-one-provider-available": true,
    "show-rustore-screen-every-days-in-first-month": 7,
    "show-rustore-screen-every-days-from-second-month": 30,
    "rustore-url": "https://www.rustore.ru"
}
```

где:

- push-provider — какой провайдер пуш-уведомлений должен использоваться на клиентском приложении. Возможные значения — rustore или firebase.
- use-rustore-if-fcm-unavailable — используем ли RuStore, если Google Services отсутствует на мобильном устройстве пользователя. Если true — используем RuStore.
- show-download-rustore-screen — отображаем ли пользователям баннер об отсутствии приложения RuStore при включенных RuStore пуш-уведомлениях. Если true — отображаем.
- show-download-rustore-screen-if-no-one-provider-available — отображаем ли пользователям баннер об отсутствии приложения RuStore, когда на мобильном устройстве не доступен ни один из провайдеров пуш-уведомлений. Если true — отображаем.
- show-rustore-screen-every-days-in-first-month — через сколько дней должен отображаться баннер в первый месяц.
- show-rustore-screen-every-days-from-second-month — через сколько дней должен показываться баннер, начиная со второго месяца.
- rustore-url — ссылка на скачивание приложения RuStore, используется при отсутствии приложения.

3. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

4. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Технический писатель: Белова Ирина

23 апреля 2026 г.