Мессенджер и ВКС

Инструкция по настройке SSO-аутентификации (Stroma, SWA)

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

Оглавление

Назначение документа

В документе описана настройка SSO-аутентификации по протоколу OpenID Connect (OIDC) в Мессенджере и Почте VK WorkSpace при помощи сервиса Stroma в составе Мессенджера. Данная функциональность доступна для версии Почты и Мессенджера 25.2.1 и выше.

Чтобы настроить SSO-аутентификацию в Мессенджере, выполните шаги 1-4. Если в инсталляции есть Почта VK WorkSpace и вы хотите настроить для нее сквозную авторизацию в приложении VK WorkSpace, выполните также шаги 5-6.

> **Примечание**
>
> При выполнении шагов 5-6, аутентификация в Почту будет также выполняться с помощью технологии SSO.

Документ предназначен для использования системными администраторами.

Предварительные условия

Для настройки SSO-аутентификации необходимо:

1. Наличие провайдера аутентификации, поддерживающего протокол OIDC.
2. Доступ к серверу Мессенджер и ВКС.
3. Доступ к серверу Почты VK WorkSpace (при ее наличии).
4. Доступ в Панель администратора VK WorkSpace (при ее наличии).

Шаг 1. Включите в инсталляции сервис Stroma

1. Подключитесь к серверу Мессенджер и ВКС и перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json**:

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

2. Убедитесь, что:
   - В файле присутствует флаг **stroma-enabled** и выставлен в значение true.
   - В файле присутствует флаг **messenger-silent-enabled** и выставлен в значение true (необходим для включения флоу сайлент-токенов).
   - В файле указано значение для параметра **stroma-api**, и оно такое же, как у параметра **main-api**:

```
{
  ...
  "api-urls": {
    "main-api": "https://u-<адрес инсталляции>",
    "main-binary-api": "https://ub-<адрес инсталляции>",
    "stroma-api": "https://u-<адрес инсталляции>"
  },
  "stroma-enabled": true,
  "messenger-silent-enabled": true,
  ...
}
```

3. Если вы изменяли файл, пересоздайте pod админ-консоли командой:

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

Шаг 2. Настройте сервис Stroma

1. В конфигурационном файле сервиса Stroma **/usr/local/etc/stroma-1.yaml** указаны ключи подписи токенов по умолчанию. Измените их — задайте свои значения:
   - Ключ подписи Json Web Token — в параметре auth.token_secret
   - Ключ подписи одноразовых токенов — в параметре auth.one_time_code_secret
   - Ключ подписи miniapp-токенов — в параметре auth.miniapp_api_token_salt
   - Ключ подписи silent-токенов — в параметре auth.silent_token_salt

   Далее перезапустите сервис Stroma командой:

```
systemctl restart stroma-1
```

2. Если в инсталляции нет Панели администратора VK WorkSpace, в конфигурационном файле сервиса Stroma **/usr/local/etc/stroma-1.yaml** укажите для параметра **user_management** значение **stentor** и перезапустите сервис Stroma командой:

```
systemctl restart stroma-1
```

3. Если в инсталляции нет сервиса SWA (компонент Почты VK WorkSpace), в конфигурационном файле сервиса Stroma **/usr/local/etc/stroma-1.yaml**:

   • Убедитесь в отсутствии секции **swamail**. При наличии — удалите ее.

   • Перезагрузите сервис Stroma командой:

```
systemctl restart stroma-1
```

Шаг 3. Настройте сервис Swapper

1. Сгенерируйте miniapp api secret для сервиса Swapper:

```
sso token messenger
```

   Запомните вывод этой команды — это miniapp api secret.

2. Вставьте miniapp api secret в ConfigMap сервиса Swapper по пути data → swapper.yaml → секция swap → параметр miniapp_api_token. Команда для изменения ConfigMap:

```
# kubectl -n vkteams edit configmap swapper-config
```

Шаг 4. Запустите программу настройки SSO-аутентификации

Запустите программу настройки SSO-аутентификации под пользователем с правами администратора:

```
# sso setup
```

Укажите параметры SSO-аутентификации:

• Type — тип IDP-провайдера (например ADFS или Keycloak).

• Service Title — название IDP-провайдера.

• Service Description — краткое описание IDP-провайдера.

• Auth URI — authorization endpoint, полученный из настроек IDP.

- Userinfo URI — user info endpoint, полученный из настроек IDP.
- Token URI — token endpoint, полученный из настроек IDP.
- Introspection URI — introspection endpoint, полученный из настроек IDP.
- Client ID — clientID, полученный из настроек IDP.
- Client Secret — clientSecret, полученный из настроек IDP.
- Domains (comma-separated) — через запятую укажите домены, для которых подключается SSO-аутентификация.

Пример настроек:

```
Type: KK
Service Title: Keycloak
Service Description: Our Keycloak
Auth URI: http://185.241.192.178:8080/realms/sso/protocol/openid-connect/auth
Userinfo URI: http://185.241.192.178:8080/realms/sso/protocol/openid-connect/userinfo
Token URI: http://185.241.192.178:8080/realms/sso/protocol/openid-connect/token
Introspection URI: http://185.241.192.178:8080/realms/sso/protocol/openid-connect/token/
introspect
Client ID: <client id>
Client Secret: <client secret>
Domains (comma-separated): keycloak.sso-test.ru
```

Пример вывода:

```
successfully create IdentityProvider with id: 685b0b03-9e3c-40c9-a08f-181d039cc88e
successfully connect domain keycloak.sso-test.ru with provider 685b0b03-9e3c-40c9-
a08f-181d039cc88e
successfully enable sso on domain: keycloak.sso-test.ru
successfully setup SSO with 685b0b03-9e3c-40c9-a08f-181d039cc88e provider
```

Если в инсталляции отсутствует Почта VK WorkSpace, настройка SSO-аутентификации завершена. Пропустите шаги 5-6.

Шаг 5. Включите SSO-аутентификацию в сервисе SWA

Если в инсталляции присутствует Почта VK WorkSpace и вы хотите настроить для нее сквозную авторизацию в Супераппе, выполните шаги ниже.

> **Примечание**
>
> При выполнении шагов 5-6, аутентификация в Почту будет также выполняться с помощью технологии SSO.

1. Выполните данный пункт до обновления Почты VK WorkSpace на версию 25.2.1.

На стороне Почты перейдите в директорию, в которую был распакован дистрибутив Почты при установке, и далее в конфигурационный файл **configs/onlineconf/MAILAPI.conf**. Удалите все фрагменты текста:

```
&& {{ getCustomEnv "ENABLE_VKT_SSO" "false" }}
```

2. Подключитесь к сервису SWA и получите client_secret при помощи команды:

```
docker exec -it swadb1 mysql -D swa -e "select secret from swa.swa_clients where
client_id='vk-teams';"
```

Запомните вывод команды, он понадобится в пункте 6.

3. В конфигурационном файле **configs/swa/goswa/goswa_acl.yaml** проверьте наличие IP-адресов Панели администратора VK WorkSpace и Мессенджера и ВКС.
4. Подключитесь к БД сервиса SWA:

```
docker exec -it swadb1 mysql
```

и проверьте, что для пользователя swa выделены гранты GRANT SELECT, INSERT, UPDATE:

```
show grants for 'swa'@'%';
```

Пример вывода команды:

```
+---------------------------------------------------------------------+
| Grants for swa@%                                                    |
+---------------------------------------------------------------------+
| GRANT USAGE ON *.* TO swa@%                                         |
| GRANT SELECT ON swa.* TO swa@%                                      |
| GRANT SELECT, DELETE ON oauth.client TO swa@%                       |
| GRANT SELECT, INSERT, UPDATE ON swa.sso_clients TO swa@% |  #необходимые гранты
пользователя swa
+---------------------------------------------------------------------+
4 rows in set (0,01 sec)
```

5. Подключитесь к серверу Мессенджер и ВКС и сформируйте секрет при помощи утилиты:

```
sso token swa
```

Подключитесь к серверу Почты VK WorkSpace и укажите секрет в конфигурационном файле сервиса gofau в секции **idm** в параметре **client_secret**:

```
idm:
  url: "https://u.myteam.vmailru.net"
  client_secret: '${VAULT:secret/gofau/prod/idm:client_secret}'
  debug: false
```

6. Подключитесь к серверу Мессенджер и ВКС и добавьте в конфигурационный файл сервиса Stroma **/usr/local/etc/stroma-1.yaml** информацию о клиенте и базовом URL-адресе в секцию **swamail**:

```
swamail:
    url: "https://swa.{domain}/api/v1"
    client_id: "vk-teams"
    client_secret: "client_secret" // секрет клиента из пункта 2
    timeout: 5s
```

7. Перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** и скорректируйте секции mail, calendar и cloud:

   - Для параметра **needs_auth** укажите значение true.
   - Если SSO-аутентификация подключается для всех доменов инсталляции, установите значение true для параметра **default** (находится внутри секции **is-public**). Если для определенных доменов — перечислите их в секции **is-public** со значением true.

   Пример заполненной секции mail:

```
"mail": {
  "external": false,
  "mail-android-app-urlscheme": "mail-onpremise-auth://",
  "mail-ios-app-urlscheme": "mailrumail-x-callback://",
  "mail-mobile-url": "https://e.vkwm-01.release.vkwm.ru/inbox",
  "needs_auth": true, #включаем SSO-аутентификацию
  "service-worker-enabled": true,
  "is-public": {
  "$switch-domain": {
    "default": false, #выключаем для всех доменов по умолчанию
    "company_domain_1.ru": true, #включаем для опреленных доменов
    "company_domain_2": true
    }
  },
  "url": "https://e.vkwm-01.release.vkwm.ru/inbox",
  "compose_url": "https://e.vkwm-01.release.vkwm.ru/compose?wv=1"
},
```

Шаг 6. Проверьте, что для домена подключена SSO-аутентификация

Если в инсталляции присутствует Почта VK WorkSpace:

Подключитесь к серверу Мессенджер и ВКС и выполните команду:

```
echo "box.space.domain_providers:select{}" | tarantoolctl eval tokeeper-1
```

В выводе команды будет список доменов, для которых подключена SSO-аутентификация.

Как добавить домен для SSO-аутентификации

Вы можете добавить новый домен в настройки SSO-аутентификации следующими способами:

1. В Панели администратора VK WorkSpace (при ее наличии в инсталляции).
2. При помощи утилиты, если нет Панели администратора VK WorkSpace.

Чтобы узнать, для каких доменов уже подключена SSO-аутентификация, подключитесь к серверу Мессенджер и ВКС и выполните команду:

```
echo "box.space.domain_providers:select{}" | tarantoolctl eval tokeeper-1
```

Если в инсталляции нет Панели администратора VK WorkSpace:

1. Получите ID-провайдера аутентификации:

   ```
   echo "box.space.identity_providers:select()[1]['id']" | tarantoolctl eval tokeeper-1
   ```

2. Добавьте новый домен к IDP-провадеру:

   ```
   sso connect <new_domain> <provider_id>
   ```

   где:

   - new_domain — домен, для которого надо подключить SSO-аутентификацию.
   - provider_id — ID провайдера аутентификации из предыдущего шага.

3. Включите на новом домене SSO-аутентификацию:

   ```
   sso enable_sso <new_domain>
   ```

   где new_domain — домен, для которого надо подключить SSO-аутентификацию.

Как изменить настройки SSO-аутентификации

Вы можете менять настройки SSO-аутентификации и управлять сессиями пользователей при помощи Панели администратора VK WorkSpace.

1. Подключитесь к серверу Мессенджер и ВКС 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.

2. Перейдите в инсталлятор VK WorkSpace по адресу http://server-ip-address:8888 в раздел **Настройки** → **Интеграции** и включите переключатель **VK Teams поддерживает авторизацию ЕСИА**. Укажите client_id и client_secret и нажмите на кнопку **Сохранить**.

3. Подключите следующие фичи самостоятельно или с помощью технической поддержки:

   - sso-enabled.
   - tmp-new-reset-sessions — для управления сессиями пользователей через Панель администратора VK WorkSpace.
   - trust-swa — для создания пользователей.

4. Перейдите в Панель администратора VK WorkSpace в раздел **Конфигурация** → **Настройки** → **Способы аутентификации** и измените настройки SSO-аутентификации на домене. Чтобы управлять сессиями пользователей, перейдите в раздел **Мессенджер** → **Аккаунты**.

Технический писатель: Белова Ирина

27 апреля 2026 г.