

OpenID и КП

Как обойти ограничение инсталлятора 26.2 и собрать OpenID с контрольной панелью на одном сервере: OpenID переезжает с собственного порта 443 за nginx КП по пути /openid. Шесть шагов ручной настройки и скрипт автоматизации [openid-cp-same-host.sh](#).

Clearway CA · сентябрь 2026

1. Когда это нужно

В 26.2 инсталлятор не ставит КП и OpenID на один хост: OpenID занимает порт 443 сам (ключ `web.https` в `config.yaml`), а тот же порт нужен nginx контрольной панели. Сама компоновка при этом поддерживается: компонент «Единая установка» ставит оба сервиса на одну машину за одним nginx.

Обход: OpenID переезжает с 443 на локальный порт 5556, наружу его отдаёт nginx КП по пути `/openid`. Итоговый адрес входа: `https://<fqdn>/openid`. Файлы при этом считаются установленными штатно, правится только конфигурация.

2. Скрипт автоматической настройки

Рядом с документом лежит `openid-cp-same-host.sh`. Он выполняет шаги 1–5 раздела 4: правит `config.yaml` OpenID, `client_env.js` и конфиг КП, создаёт `openid.conf` и перезапускает `openid`, `controlPanel` и `nginx`.

Скрипт меняет рабочие конфигурации и перезапускает сервисы, вход пользователей сбрасывается. Перед запуском убедитесь, что есть доступ к машине и актуальные резервные копии. Применяйте на свой страх и риск.

Запуск от root на итоговой машине:

```
sudo ./openid-cp-same-host.sh <fqdn>
```

Перед каждым изменением скрипт сохраняет копию файла как `<файл>.bak.<метка-времени>`, поэтому повторный запуск безопасен. При неудачной проверке `issuer` скрипт подсказывает запасной вариант с `web.https` (примечание в шаге 1).

Откат: вернуть `.bak`-копии на место и перезапустить `openid`, `controlPanel` и `nginx`.

3. Согласованные значения

Ключевое правило: один адрес `https://<fqdn>/openid` должен стоять в трёх местах (конфиг OpenID, `client_env.js`, конфиг КП), а адрес КП должен быть прописан в `redirectURIs` OpenID. Здесь и далее `<fqdn>` означает полное имя итоговой машины, путь установки `/opt/itc`.

Значение	Где находится
<code>issuer: https://<fqdn>/openid</code>	<code>config.yaml</code> OpenID
<code>issuer: то же значение</code>	<code>itc/env/client_env.js</code> (фронтенд)
<code>Authority: то же значение</code>	<code>itc/config/itc_api_miniCA_controlPanel_config.json</code>
<code>redirectURIs: https://<fqdn></code>	<code>staticClients</code> в <code>config.yaml</code> OpenID
<code>http://127.0.0.1:5559</code>	<code>Services.OpenId</code> в конфиге КП (админ-API OpenID)

4. Шаги ручной настройки

Подготовка. Если OpenID стоит на другой машине, перенесите на целевую каталог `/opt/itc/openid` и юнит `openid.service` (кладётся в `~/config/systemd/user/` технологического пользователя), затем `systemctl --user enable openid.service`. Параметры БД в `config.yaml` не меняются, переносить базу не нужно. На старой машине выполните `systemctl --user disable --now openid.service`.

Шаг 1. `/opt/itc/openid/config.yaml`

```
issuer: https://<fqdn>/openid      # было: https://<адрес-openid> без пути

web:
  http: "127.0.0.1:5556"           # было: https: "<адрес>:443"
  allowedOrigins: ['*']
  # ключи tlsCert и tlsKey удалить

adminServer:
  http: "127.0.0.1:5559"           # было: <адрес>:5559
```

В `staticClients[0]` поправьте `redirectURIs` на `https://<fqdn>`. `secret` не меняйте: он должен совпадать с `secret` в `client_env.js`. `issuer` зашивается в токены, после смены все пользователи перелогинятся.

Если бинарник `v1.2.2` не примет `web.http` (ошибка старта в `journalctl --user -u openid`), оставьте TLS-вариант: `web.https: "127.0.0.1:5556"` с `tlsCert` и `tlsKey`, а в `openid.conf` замените `proxy_pass http://` на `proxy_pass https://`.

Шаг 2. `/opt/itc/itc/env/client_env.js`

```
issuer: 'https://<fqdn>/openid',
```

`clientId` и `secret` не трогайте, они уже согласованы с `config.yaml`.

Шаг 3. `/opt/itc/itc/config/itc_api_miniCA_controlPanel_config.json`

```
"OpenId": {
  "Authority": "https://<fqdn>/openid",
  ...
},
"Services": {
  "OpenId": "http://127.0.0.1:5559",
  ...
}
```

`Authority` пишется с путём `/openid`, а `Services.OpenId` без пути: это адрес админ-API OpenID на порту 5559, по нему бэкенд ходит за `userinfo`.

Шаг 4. Новый файл /opt/itc/itc/nginx/openid.conf

```
location /openid {
    proxy_pass http://127.0.0.1:5556;
    proxy_http_version 1.1;
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Real-IP $remote_addr;
}
```

Править nginx.conf не нужно: файл подхватится инклюдом `include /opt/itc/itc/nginx/*.conf;` в `server`-блоке на 443. Конфликтов с `controlPanel.conf` (`location /` и `/api/minica`) нет.

Шаг 5. Перезапуск

```
# openid и controlPanel: user-юниты, от имени технологического пользователя
sudo -u <user> XDG_RUNTIME_DIR=/run/user/$(id -u <user>) \
    systemctl --user restart openid.service
sudo -u <user> XDG_RUNTIME_DIR=/run/user/$(id -u <user>) \
    systemctl --user restart controlPanel.service

sudo nginx -t && sudo systemctl reload nginx
```

Обычный `systemctl restart openid` не сработает, это `user`-юниты. Под `<user>` понимается владелец каталогов `/opt/itc/openid` и `/opt/itc/itc.minica.controlPanel`; если пользователи разные, перезапускайте каждым.

Шаг 6. Проверка

```
curl -sk https://<fqdn>/openid/.well-known/openid-configuration
```

В ответе `issuer` должен быть `https://<fqdn>/openid`. Затем откройте КП в браузере и войдите. Все пользователи перелогинятся: старые сессии привязаны к прежнему `issuer`.

5. Примечания

- TLS-сертификат `nginx` должен быть выпущен на `<fqdn>`; на машине КП это уже так.
- Сертификат OpenID после переезда на 5556 наружу не виден: `nginx` сертификат апстрима не проверяет, а у КП стоит `IgnoreCertificateErrors: true`.
- Инструкция сверена с веткой `release/26.2-free` репозитория `distributions`: шаблоны `config.yaml.liquid`, `client_env.js.liquid`, `itc_api_miniCA_controlPanel_config.json.liquid` и `shared/nginx.conf`.