

Авторизация через SSO (OpenID, OAuth)

Выполните установку необходимых модулей Apache:

```
$ sudo apt-get install libapache2-mod-auth-openidc
```

Включите использование модуля:

```
$ sudo a2enmod auth_openidc
```

В файле настройке сайта добавьте следующие строки:

```
...
LoadModule auth_openidc_module modules/mod_auth_openidc.so

<VirtualHost *:80>
...

    OIDCClaimPrefix "OIDC-"
    OIDCResponseType "id_token"
    OIDCScope "openid email"
    OIDCProviderMetadataURL "... "
    OIDCClientID "... "
    OIDCClientSecret "... "
    OIDCRedirectURI http://<devprom-alm-server>/openid/auth
    OIDCCryptoPassphrase <your-secret-phrase>

    <LocationMatch /openid>
        AuthType openid-connect
        Require valid-user
    </LocationMatch>
</VirtualHost>
```

Пример заполнения параметров для аутентификации через Gmail

OIDCProviderMetadataURL	https://accounts.google.com/.well-known/openid-configuration
OIDCClientID	ClientID можно получить по ссылке https://console.cloud.google.com/apis/credentials для зарегистрированного приложения, где в качестве RedirectURI необходимо прописать путь к приложению <a href="http://<devprom-alm-server>/openid/auth">http://<devprom-alm-server>/openid/auth
OIDCClientSecret	ClientSecret можно получить вместе с ClientID

Дополнительные настройки

В файле `htdocs/settings_server.php` вы можете добавить следующие константы, чтобы настроить работу аутентификации через SSO-сервер.

<code>define('AUTH_OPENID_USED', true);</code>	Отобразить кнопку SSO на странице авторизации для входа через SSO-сервер.
<code>define('AUTH_OPENID_ONLY', true);</code>	Использовать только аутентификацию через SSO, без возможности аутентифицироваться по паре логин/пароль.
<code>define('AUTH_OPENID_CREATE_VISITOR', true);</code>	Автоматически создавать учетную запись для посетителя, успешно аутентифицировавшегося через SSO-сервер.

Пример настройки Keycloak

Настройки клиента Test

The screenshot displays the Keycloak Admin Console interface for configuring a client named 'Test'. The left sidebar shows the navigation menu with 'Clients' selected. The main content area is divided into several sections:

- Client Information:** Client ID (test), Name, and Description.
- Enabled:** A toggle switch set to 'ON'.
- Always Display in Console:** A toggle switch set to 'OFF'.
- Consent Required:** A toggle switch set to 'OFF'.
- Login Theme:** A dropdown menu.
- Client Protocol:** A dropdown menu set to 'openid-connect'.
- Access Type:** A dropdown menu set to 'confidential'.
- Standard Flow Enabled:** A toggle switch set to 'ON'.
- Implicit Flow Enabled:** A toggle switch set to 'OFF'.
- Direct Access Grants Enabled:** A toggle switch set to 'ON'.
- Service Accounts Enabled:** A toggle switch set to 'OFF'.
- Authorization Enabled:** A toggle switch set to 'OFF'.
- Root URL:** A text input field.
- Valid Redirect URIs:** A list of URIs with '+' and '-' buttons for adding and removing entries.
- Base URL:** A text input field.
- Admin URL:** A text input field.
- Web Origins:** A list of origins with '+' and '-' buttons.
- Backchannel Logout URL:** A text input field.
- Backchannel Logout Session Required:** A toggle switch set to 'ON'.
- Backchannel Logout Revoke Offline Sessions:** A toggle switch set to 'OFF'.

Below these are several expandable sections:

- Fine Grain OpenID Connect Configuration:** Contains dropdown menus for Access Token Signature Algorithm, ID Token Signature Algorithm, ID Token Encryption Key Management Algorithm, ID Token Encryption Content Encryption Algorithm, User Info Signed Response Algorithm, Request Object Signature Algorithm, Request Object Required, and Valid Request URIs.
- OpenID Connect Compatibility Modes:** Contains toggle switches for 'Exclude Session State From Authentication Response' and 'Use Refresh Tokens For Client Credentials Grant', both set to 'OFF'.
- Advanced Settings:** Contains input fields for 'Access Token Lifespan', 'Client Session Idle', 'Client Session Max', 'Client Offline Session Idle', and 'Client Offline Session Max', each with a 'Minutes' dropdown. It also has a toggle for 'OAuth 2.0 Mutual TLS Certificate Bound Access Tokens Enabled' (OFF) and a dropdown for 'Proof Key for Code Exchange Code Challenge Method'.
- Authentication Flow Overrides:** Contains dropdown menus for 'Browser Flow' and 'Direct Grant Flow'.

At the bottom, there are 'Save' and 'Cancel' buttons.

Настройки Identity Provider

The screenshot displays the Keycloak Admin Console interface for configuring an OpenID Connect (OIDC) provider. The left sidebar shows the navigation menu with 'Master' selected. The main content area is titled 'Identity Providers > oidc' and contains two sections: 'Settings' and 'OpenID Connect Config'.

Settings:

- Redirect URI: `https://176.9.66.16:8389/auth/realms/master/broker/oidc/endpoint`
- Alias: `oidc`
- Display Name: (empty)
- Enabled: ON
- Store Tokens: OFF
- Stored Tokens Readable: OFF
- Trust Email: OFF
- Account Linking Only: OFF
- Hide on Login Page: OFF
- GUI order: (empty)
- First Login Flow: `first broker login`
- Post Login Flow: (empty)
- Sync Mode: `import`

OpenID Connect Config:

- Authorization URL: `https://hq.devprom.ru/openid/auth`
- Pass login_hint: OFF
- Pass current locale: OFF
- Token URL: `https://hq.devprom.ru/openid/auth`
- Logout URL: (empty)
- Backchannel Logout: OFF
- Disable User Info: OFF
- User Info URL: (empty)
- Client Authentication: `Client secret sent as basic auth`
- Client ID: `test`
- Client Secret: `*****`
- Issuer: (empty)
- Default Scopes: (empty)
- Prompt: `unspecified`
- Accepts prompt=none forward from client: OFF
- Validate Signatures: OFF
- Allowed clock skew: (empty)
- Forwarded Query Parameters: (empty)

At the bottom of the configuration section, there are 'Save' and 'Cancel' buttons.

Настройки Apache

```

...
OIDCClaimPrefix "OIDC-"
OIDCResponseType "code"
OIDCScope "openid email"
OIDCProviderMetadataURL
"https://176.9.66.16:8389/auth/realms/master/.well-known/openid-configuration"
OIDCClientID "test"
OIDCClientSecret "*****"
OIDCRedirectURI "https://hq.devprom.ru/openid/auth"
OIDCSSLValidateServer "Off"
OIDCCryptoPassphrase openstack
...

```