

[К-5407] 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 "..."/>

```

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 <code>http://<devprom-alm-server>/openid/auth</code>
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.

[К-5773] 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:** Fields for 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:** An empty text field.
- Valid Redirect URIs:** A list with one entry: '*'. Add and remove buttons are present.
- Base URL:** An empty text field.
- Admin URL:** An empty text field.
- Web Origins:** A list with one entry: '*'. Add and remove buttons are present.
- Backchannel Logout URL:** An empty text 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 three expandable sections:

- Fine Grain OpenID Connect Configuration:** Contains dropdowns 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 (not required), and Valid Request URIs.
- OpenID Connect Compatibility Modes:** Contains toggle switches for Exclude Session State From Authentication Response (OFF) and Use Refresh Tokens For Client Credentials Grant (OFF).
- Advanced Settings:** Contains input fields and dropdowns for Access Token Lifespan, Client Session Idle, Client Session Max, Client Offline Session Idle, Client Offline Session Max, OAuth 2.0 Mutual TLS Certificate Bound Access Tokens Enabled (OFF), and Proof Key for Code Exchange Code Challenge Method.

At the bottom, there are dropdowns for Browser Flow and Direct Grant Flow, followed by 'Save' and 'Cancel' buttons.

Настройки Identity Provider

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
...

```