

??????

????????????????

Инструкции по настройке Blitz Identity Provider

- [Вход в консоль управления через SSO](#)

???? ? ?????????? ?????????????? ?????? SSO

В примере будет рассмотрен способ настройки входа в консоль управления через текущую установку Blitz Identity Provider. В качестве атрибута с ролями будет использован атрибут `memberOf`.

????????????????? ??????????????????

В консоли Blitz Identity Provider в разделе `Приложения` необходимо зарегистрировать приложение, от имени которого сервис `blitz-console` будет обращаться к сервису `blitz-idp`.

Новое приложение

Идентификатор (entityID или client_id)
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).

Название
Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.

Домен

Основные параметры приложения:

- В настройке `Префиксы ссылок возврата` указать домен установки Blitz Identity Provider.
- В настройке `Допустимые разрешения` указать scope `openid`.

Префиксы ссылок возврата

Для добавления нового префикса введите его и нажмите Enter

Префикс используется для проверки ссылок возврата (redirect_uri). Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано

Допустимые разрешения

Разрешения (scope), которые будут доступны приложению.

- В настройке `Метод аутентификации при обращении к сервису выдачи маркеров` указать `client secret post`.

Метод аутентификации при обращении к сервису выдачи маркеров

client secret post

Указанный метод аутентификации должен использоваться при обращении к сервису выдачи маркеров (token endpoint). При пустом значении доступны все методы

- В настройке `Добавляемые в маркер идентификации (id_token) утверждения` указать название `claim`, в котором будут передаваться роли.

Добавляемые в маркер идентификации (id_token) утверждения

x memberOf

Дополнительные утверждения (claim), которые будут добавлены в маркер идентификации (id_token).

????????? ?????????? ????????????????

В конфигурационном файле `console.conf` необходимо задать следующие параметры:

```
"login" : {
  "fp" : {
    "authUri" : "https://demo.identityblitz.com/blitz/oauth/ae",
    "clientId" : "blitz-console",
    "clientSecret" : "client-secret-value",
    "logoutUrl" :
"https://demo.identityblitz.com/blitz/login/logout?post_logout_redirect_uri=https://demo.identityblitz.com/blitz/console",
    "roleClaim" : "memberOf",
    "scopes" : [
      "openid"
    ],
    "subjectClaim" : "sub",
    "tokenUri" : "https://demo.identityblitz.com/blitz/oauth/te"
  }
},
"net" : {
  "domain" : "demo.identityblitz.com"
}
```

Подробное описание параметров представлено в [документации](#).

???????? ???? ? ???? ????
????????

В конфигурационном файле `credentials` необходимо создать роль с названием соответствующим значению, которое будет приходить в `roleClaim`, и необходимыми правами доступа.

```
{
  "name" : "cn=blitz-console-adm,ou=groups,ou=demo,dc=reaxoft,dc=loc",
  "privileges" : [
    "w_app",
    "w_system",
    "w_ui",
    "w_user",
    "r_audit"
  ]
},
```

Подробное описание прав доступа представлено в [документации](#).