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

Инструкции по настройке Blitz Identity Provider

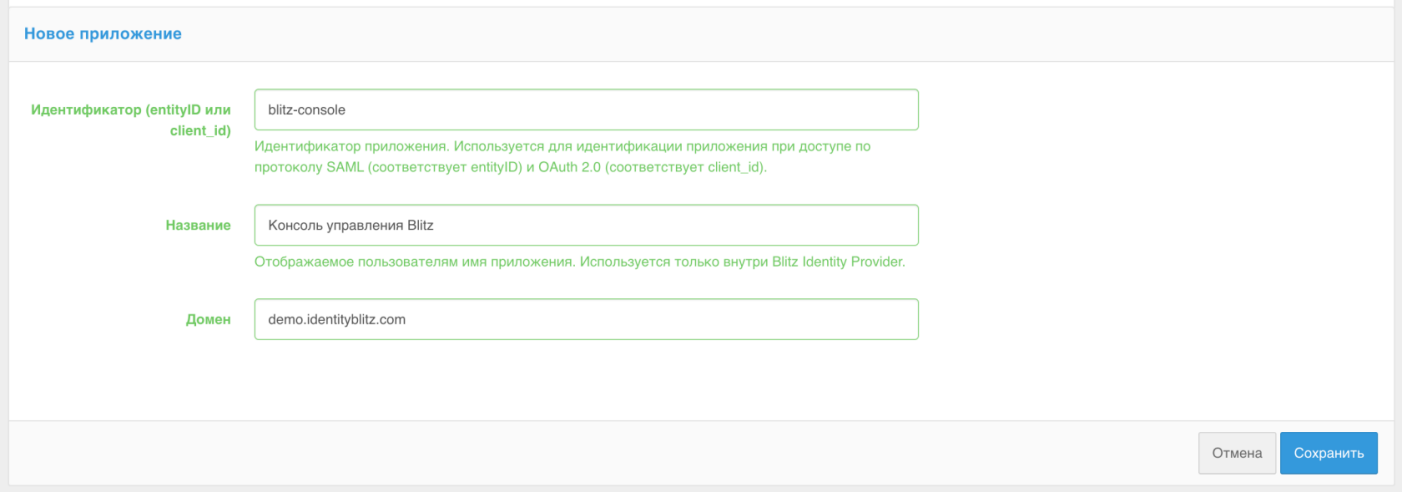
- Вход в консоль управления через SSO

???? ? ??????? ??????????? ????? 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`.

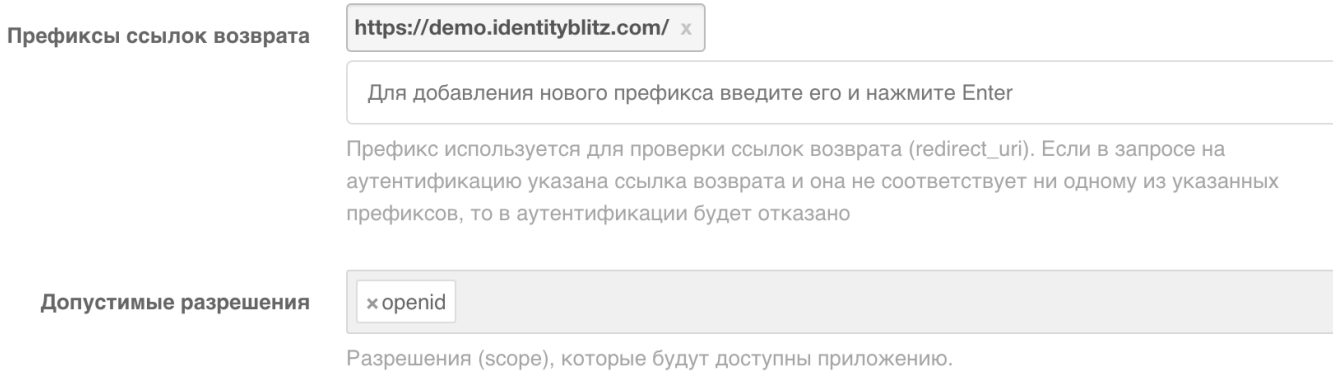
???????????? ???????????

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

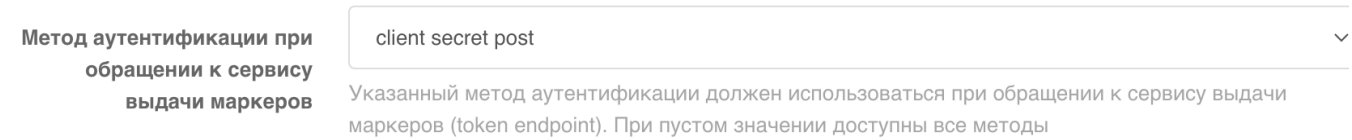


Основные параметры приложения:

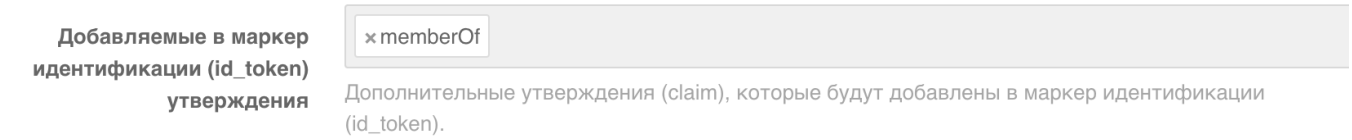
- В настройке `Префиксы ссылок возврата` указать домен установки Blitz Identity Provider.
- В настройке `Допустимые разрешения` указать scope `openid`.



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



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



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

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.ident
ityblitz.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.