

Добавление SSO через Authentik

Заходим в интерфейс администратора
в провайдеры и создаем новый.

Выставляем настройки. По сути,
практически все по умолчанию,
выбираем flow, вписываем имя.

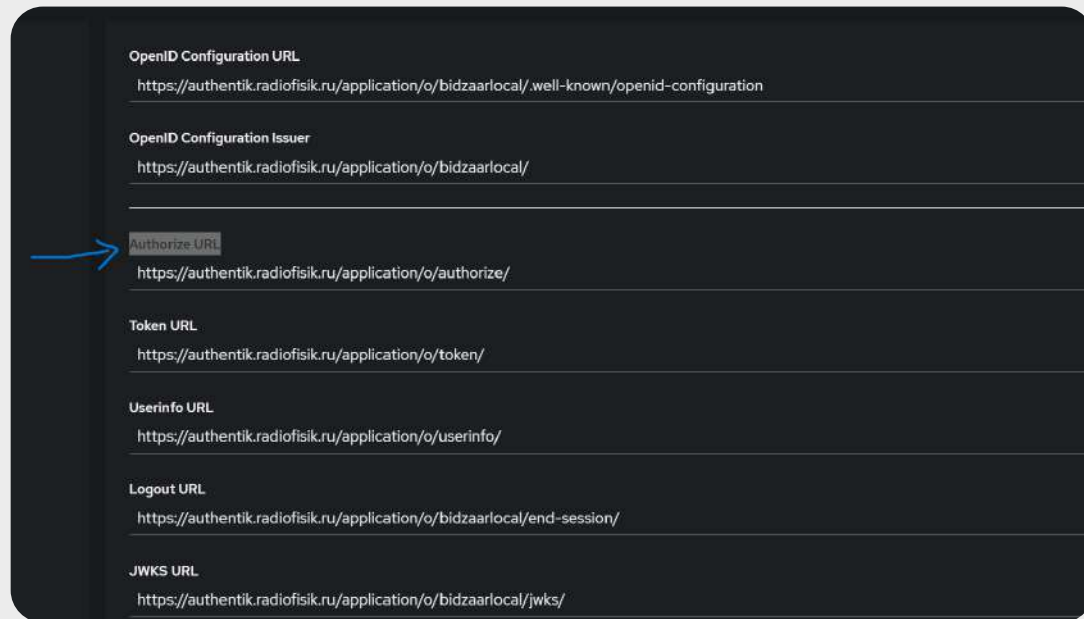
RedirectUrl в данном случае можно не
писать, он определится сам при первой
удачной аутентификации, но в других
провайдеров это может быть не так

По итогу из этого интерфейса нам нужно
скопировать **ClientId**, **ClientSecret**, и
возможно **redirectUrl** если прописан тут

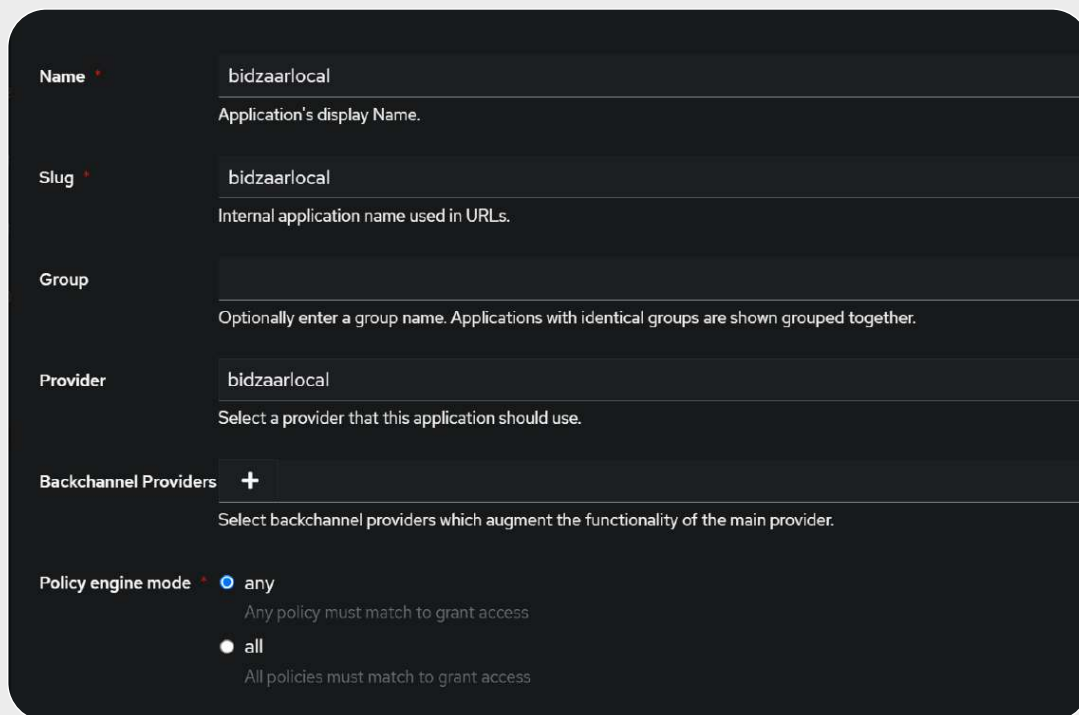
The image shows the Authentik user interface. On the left is a sidebar menu with the following sections: 'User interface' (highlighted in orange), 'Dashboards' (containing Overview, User Statistics, System Tasks), 'Applications' (containing Applications, Providers (highlighted with an orange bar), Outposts), 'Events', and 'Customization'. The main content area is titled 'Update OAuth2 Provider'. It contains the following fields and sections:

- Name:** bidzaarlocal
- Authorization flow:** default-provider-authorization-explicit-consent (Authorize Application)
Flow used when authorizing this provider.
- Protocol settings:** (expanded section)
 - Client type:** Confidential (selected with a blue dot). Description: Confidential clients are capable of maintaining the confidentiality of their credentials such as client secrets. Public (unselected with a grey dot). Description: Public clients are incapable of maintaining the confidentiality and should use methods like PKCE.
 - Client ID:** QML1EFp7IIJeRJh2b2xaoFIHJ3CI7IgQj8UBOVO8
 - Client Secret:** x2xDNpsZpaegCEGO8VXCwFFnuciN2gbUehhxUpDPvxCgnPnAzU9ZitiDzdcuV82nKnklwox4OMFHWfeGg
 - Redirect URIs/Origins (RegEx):**
 - Strict: https://bidzaar.local.radiofisik.ru/auth/external/sign-radiofisik
 - Strict: https://dev.bidzaar.com/auth/external/sign-radiofisik
 - [+ Add entry](#)
 - Valid redirect URIs after a successful authorization flow. Also specify any origins here for Implicit flows. If no explicit redirect URIs are specified, the first successfully used redirect URI will be saved. To allow any redirect URI, set the mode to Regex and the value to ".*". Be aware of the possible security implications this can have.
 - Signing Key:** authentik Self-signed Certificate
Key used to sign the tokens.
 - Encryption Key:** Select an object.
Key used to encrypt the tokens.
- Advanced flow settings:** (collapsed)
- Advanced protocol settings:** (collapsed)

Далее в получившемся провайдере
ищем **Authorize URL**



OpenID Configuration URL	https://authentik.radiofisik.ru/application/o/bidzaarlocal/.well-known/openid-configuration
OpenID Configuration Issuer	https://authentik.radiofisik.ru/application/o/bidzaarlocal/
Authorize URL	https://authentik.radiofisik.ru/application/o/authorize/
Token URL	https://authentik.radiofisik.ru/application/o/token/
Userinfo URL	https://authentik.radiofisik.ru/application/o/userinfo/
Logout URL	https://authentik.radiofisik.ru/application/o/bidzaarlocal/end-session/
JWKS URL	https://authentik.radiofisik.ru/application/o/bidzaarlocal/jwks/



Name	bidzaarlocal	Application's display Name.
Slug	bidzaarlocal	Internal application name used in URLs.
Group		Optionally enter a group name. Applications with identical groups are shown grouped together.
Provider	bidzaarlocal	Select a provider that this application should use.
Backchannel Providers	+	Select backchannel providers which augment the functionality of the main provider.
Policy engine mode	☒ any	Any policy must match to grant access
	☐ all	All policies must match to grant access

Осталось создать приложение и
указать там наш **провайдер**

По итогу настройки у нас есть такие данные:

ClientId

ClientSecret

AuthorizeURL

RedirectUrl

вида <https://bidzaar.com/auth/external/sign-username>



Далее эти данные передаются сотруднику Bidzaar, который добавляет нового провайдера в систему