

Подключение identity providers

Identity Broker - это настройка, соединяющая поставщиков услуг (в нашем случае, Keycloak) с поставщиками идентификационных данных. Identity Broker создает связь с внешним поставщиком идентификационных данных, чтобы использовать идентификационные данные от поставщика данных для доступа к внутренним службам, предоставляемым поставщиком услуг.

Сервер Keycloak поддерживает для подключения внешних провайдеров OpenID Connect протокол, стандарт SAML (Security Assertion Markup Language), Keycloak OpenID Connect, а также социальных провайдеров (Google, Gitlab и др.)

[OpenID Connect](#) (OIDC) - это протокол аутентификации, который является расширением OAuth 2.0. (построенный поверх фреймворка авторизации OAuth 2.0)

Требования по заполнению базовых конфигурационных параметров при настройке Identity Providers (на примере OIDC)

Наиболее значимые параметры более подробно рассматриваются ниже.

Наименование в UI Keycloak	Описание	Уникальность
Redirect URI	URL-адреса перенаправления для обратного вызова, требуемый протоколом OIDC	Y
Alias	Псевдоним является уникальным идентификатором. Keycloak использует псевдоним для создания URI перенаправления для протоколов OpenID Connect, которым требуется URI перенаправления или URL обратного вызова для связи с поставщиком идентификационных данных.	Y
Enabled	Переключатель. При выключенном состоянии не будет отражаться на странице входа.	-
Hide on Login Page	Когда он включен, Keycloak не отображает этого поставщика на странице входа. Клиенты могут использовать провайдер принудительно, используя параметр 'kc_idp_hint' в URL-адресе для запроса входа в систему.	-
Account Linking Only	Когда переключатель включен, Keycloak связывает существующие учетные записи с этим провайдером. Через этого провайдера пользователи не могут входить в систему. Keycloak не отображает этого поставщика в качестве опции на странице входа в систему.	-
Store Tokens	Когда параметр включен, Keycloak хранит токены от поставщика данных.	-
Stored Tokens Readable	Когда параметр включен, пользователи могут получить сохраненный токен поставщика удостоверений.	-
Trust Email	Когда параметр включен, Keycloak доверяет адресам электронной почты от поставщика данных.	-

GUI Order	Порядок сортировки доступных провайдеров на странице входа в систему.	-
First Login Flow	Здесь указывается аутентификационный поток, преднастроенный в KeyCloak, когда используется данный провайдер для первого входа в Keycloak.	N
Post Login Flow	Аналогично First Login Flow, только выполняется, когда завершается вход в систему пользователем.	N
Sync Mode	<p>Тип обновления информации о пользователе от провайдера через mappers.</p> <p>При выборе legacy Keycloak использует поведение, которое было реализовано, до внедрения параметра legacy (ранее существовала ошибка, данные не обновлялись, только импортировались независимо от настройки, затем это починили и оставили флаг legacy)).</p> <p>Импорт не обновляет пользовательские данные, а только импортирует единожды при первом входе.</p> <p>Force – данные импортируются и обновляются при каждом входе пользователя через провайдер.</p>	N

Последующие параметры соответствуют настройкам OIDC – подключения клиента от внешнего провайдера.

Примечательно, что через Import from URL вы можете автоматически их заполнить (кроме Client ID и Client Secret – идентификационные данные, которые доступны только авторизованным на это администраторам), указав URL-адрес или файл, который указывает на метаданные провайдера OpenID. Если вы подключаетесь к внешнему IDP Keycloak, вы можете импортировать настройки IDP из <root>/realms/{realm-name}/.well-known/openid-configuration. Эта ссылка представляет собой документ в формате JSON, описывающий метаданные о IDP.