

Nextcloud

Nextcloud (<https://nextcloud.com>) — это веб-платформа для организации облачного хранилища.

Подключение Nextcloud к Blitz Identity Provider выполняется по протоколу OpenID Connect и состоит из двух этапов:

- Этап 1. Настройки на стороне Blitz Identity Provider
- Этап 2. Настройки на стороне Nextcloud

Важно:

В инструкции для примера указано, что Nextcloud расположен на домене `https://nextcloud.company.com`, а Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне Blitz Identity Provider

В консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения** и выполните следующие действия:


1. **Создайте** новое приложение, задав его базовые настройки:

- **Идентификатор (entityID или client_id):** `nextcloud`
- **Название:** имя приложения Nextcloud, которое будет отображаться на стороне Blitz IDP
- **Домен:** `https://nextcloud.company.com`

Новое приложение

Идентификатор (entityID или client_id)	<input type="text" value="Nextcloud"/>
Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).	
Название	<input type="text" value="nextcloud"/>
Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.	
Домен	<input type="text" value="https://nextcloud.company.com"/>

2. Нажмите **Сохранить**.

3. Далее нажмите кнопку **Параметры**  у предложения Nextcloud и отредактируйте параметры приложения:

- **Протоколы:** выберите и нажмите **Сконфигурировать**

Далее в параметрах укажите данные, как в *Social Login* и другие обязательные параметры:

- **Секрет (client_secret):**
- **Префиксы ссылок возврата:**
- **Допустимые разрешения:**
- **Метод аутентификации при обращении к сервису выдачи маркеров:**
- **Допустимые response type:**

Настройки взаимодействия с приложением

Секрет (client_secret)

eXa12m3PL45e

Секретный ключ подключаемого приложения (client_secret). Если указан, то именно этот секрет должен использоваться подключенным приложением при обращении к Blitz Identity Provider

Дополнительный секрет (client_secret)

Укажите дополнительный секрет для аутентификации приложения

Дополнительный секретный ключ подключаемого приложения (client_secret). Если указан, то может использоваться в качестве альтернативы к основному секрету

Предопределенная ссылка возврата (redirect_uri)

Введите предопределенный redirect_uri

URL, на который по умолчанию будет переадресован пользователь после прохождения авторизации (redirect_uri)

Префиксы ссылок возврата

https://nextcloud.company.com

x

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

x profile

x openid

Разрешения (scope), которые будут доступны приложению.

Разрешения по умолчанию

Для добавления нового score введите его и нажмите Enter

Разрешения (scope), которые будут по умолчанию выданы приложению после авторизации. Если значения по умолчанию не указаны, то в запросе необходимо явно прописать требуемые разрешения.

☐ Не требовать от пользователя согласие на предоставление доступа к данным о себе

☐ Обязательное использование Proof Key for Code Exchange (RFC 7636) для Authorization code grant type

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

Допустимые grant type

x authorization_code

x refresh_token

Список grant type, которые будут доступны приложению. При пустом списке доступны все grant type

Допустимые response type

x code

x token

Список response type, которые будут доступны экземпляру приложения при обращении к URL авторизации (authorization endpoint). При пустом списке доступны все response type.

- Префиксы ссылок возврата при выходе:

https://nextcloud.company.com

Выход из приложения

Префиксы ссылок возврата при выходе

https://nextcloud.company.com

x


Для добавления нового URL введите его и нажмите Enter

Список URL используется для проверки ссылок возврата (post_logout_redirect_uri). Если в запросе на выход указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в выходе будет отказано

4. Нажмите **Сохранить**.

Этап 2. Настройки на стороне Nextcloud

Выполните следующие действия:

1. Для интеграции *Nextcloud* с Blitz Identity Provider необходимо установить приложение *Social Login*. Для этого **Войдите** в Nextcloud под учетной записью администратора. В разделе **Приложения** нажмите **Загрузить** рядом с приложением **Social Login**. Дополнительную информацию можно найти по адресу <https://apps.nextcloud.com/apps/sociallogin>.
2. Далее перейдите в **Параметры сервера** и выберите **Social login**.
3. Далее нажмите кнопку  у предложения *Custom OpenID Connect* и задайте параметры:
 - **Внутреннее имя** - укажите внутреннее название *Сервиса аутентификации*, которое будет отображаться в настройках Nextcloud. Например, `BlitzIDP`.
 - **Название** - укажите название *Сервиса аутентификации*, понятное пользователям. Название будет отображаться на кнопке страницы аутентификации и в настройках Nextcloud. Например, `BlitzIDP`.
 - **Authorize url** - укажите URL для авторизации. Например, `https://login.company.com/blitz/oauth/ae`
 - **Token url** - укажите URL для получения маркера доступа. Например, `https://login.company.com/blitz/oauth/te`
 - **User info URL (optional)** - укажите URL сервиса получения данных пользователя. Например, `https://login.company.com/blitz/oauth/me`
 - **Client id** - укажите уникальное название для идентификации приложения. Например, `nextcloud`.
 - **Client Secret** - задайте секретный ключ для безопасной аутентификации приложения.
 - **Scope** - укажите необходимые разрешения для получения данных. Например, обязательный scope `openid` и стандартный scope `profile`. При указании нескольких разрешений разделите их пробелом.

Параметры пользователя

Личная информация

Безопасность

Social login

Уведомления

Клиенты для ПК и мобильных...

Общий доступ

Внешний вид и доступность

Доступность

Обработка файлов

Конфиденциальность

Параметры сервера

Общие сведения

Основные параметры

Параметры публикации

Social login

Безопасность

Внешний вид

Приложения для совместной ...

Администрирование

Custom OpenID Connect

Внутреннее имя

BlitzIDP

Название

Blitz IDP

Authorize url

https://login.company.com/blitz/oau...

Token url

https://login.company.com/blitz/oau...

Display name claim (optional)

User info URL (optional)

https://login.company.com/blitz/oau...

Logout URL (optional)

Client Id

nextcloud

Client Secret

.....

Scope

openid profile

Groups claim (optional)

Button style

Отсутствует

Default group

Отсутствует

Add group mapping

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в Nextcloud:
<https://nextcloud.company.com>

Версия #4

Admin создал 12 августа 2024 11:30:39

Admin обновил 18 декабря 2024 09:57:12