Yandex Cloud

Yandex Cloud (https://yandex.cloud) — это веб-платформа организации облачных вычислительных мощностей.

Подключение Yandex Cloud к Blitz Identity Provider выполняется по протоколу SAML и состоит из двух этапов:

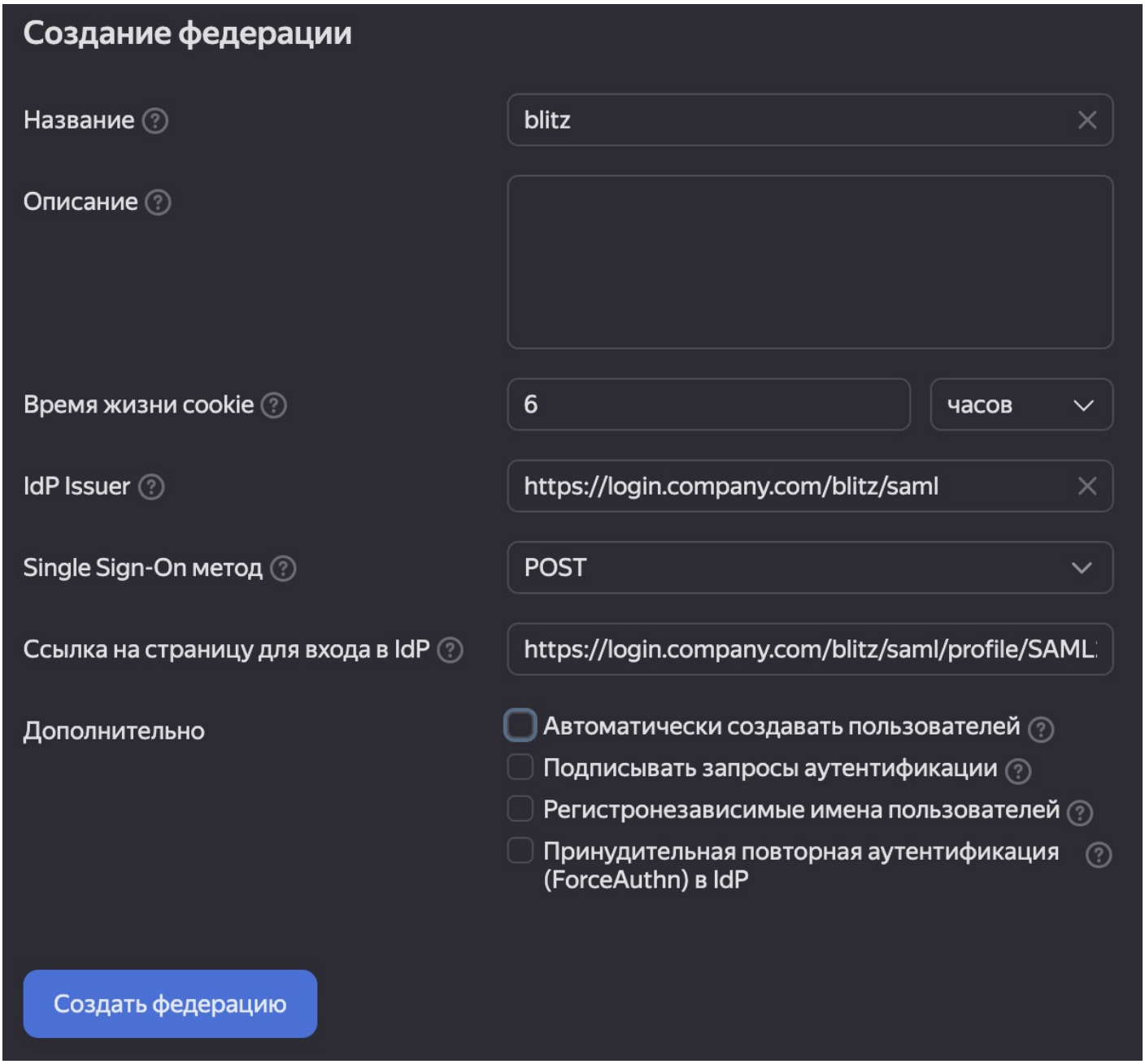
- Этап 1. Настройки на стороне Yandex Cloud
- Этап 2. Настройки на стороне Blitz Identity Provider

> **Важно:**
>
> В инструкции для примера указано, что Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне Yandex Cloud

1. Создайте федерацию удостоверений. Для этого Перейдите в сервис https://org.yandex.cloud/ и выберите на панели **Федерации**. Нажмите **Создать федерацию**:

- **Название**: Задайте уникальное имя федерации. Например, `blitz`.
- **IdP Issuer**: `https://login.company.com/blitz/saml`
- **Ссылка на страницу для входа в IdP**: `https://login.company.com/blitz/saml/profile/SAML2/Redirect/SSO`



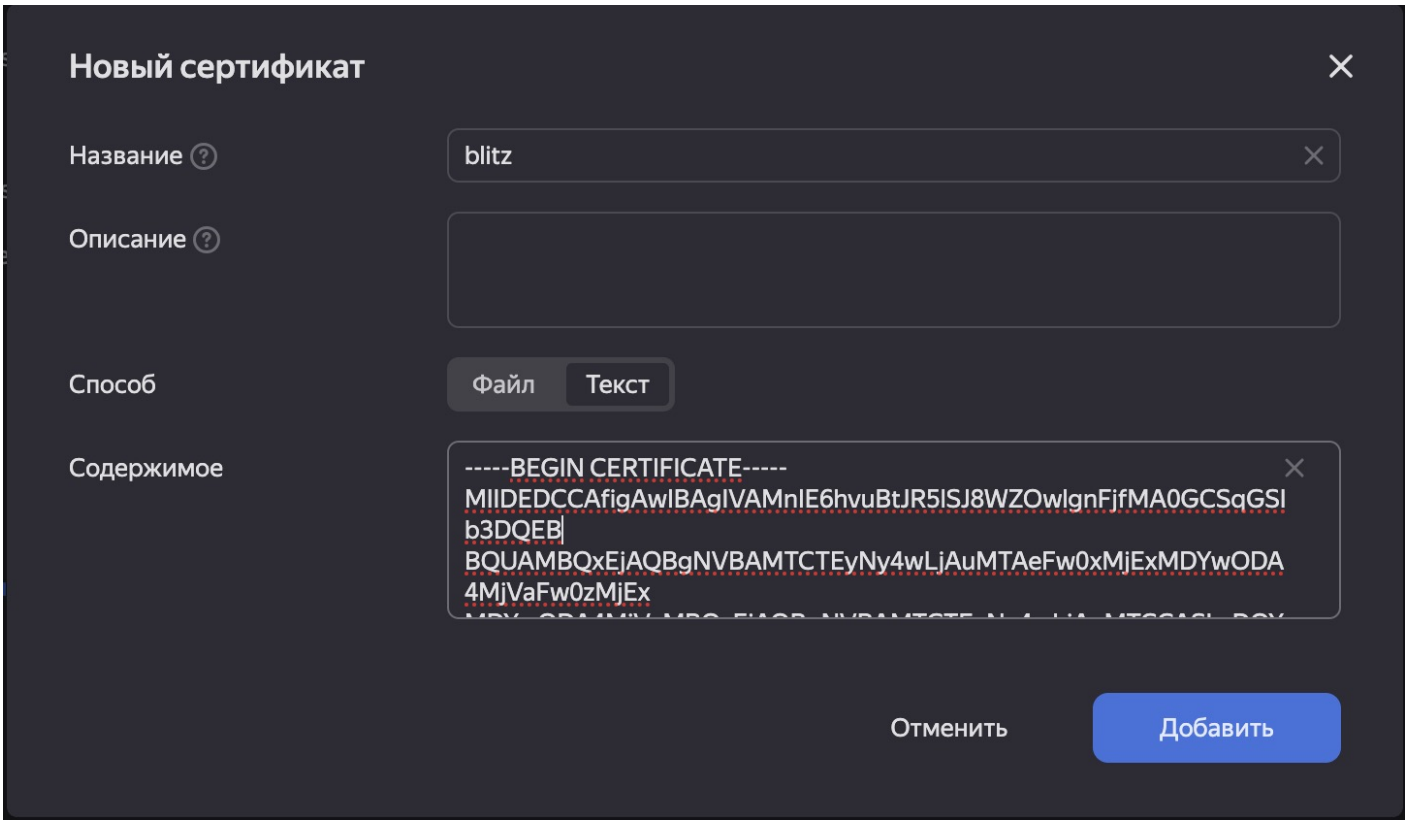
2. Нажмите **Создать федерацию**.
3. Далее передайте сертификат Blitz IDP в федерацию. Для этого перейдите по ссылке `https://login.company.com/blitz/saml/profile/Metadata/SAML`, откройте XML документ с метаданными и найдите раздел `<ds:X509Certificate>`. Например:



4. **Скопируйте** сертификат.
5. Для добавления сертификата в Yandex Cloud нажмите на имя созданной федерации и **Добавить сертификат**:

- **Название**: введите название сертификата. Например, `blitz`.
- **Способ**: `Текст`.
- **Вставьте** сертификат в PEM-формате:

```
-----BEGIN CERTIFICATE-----
 <значение сертификата>
 -----END CERTIFICATE-----
```

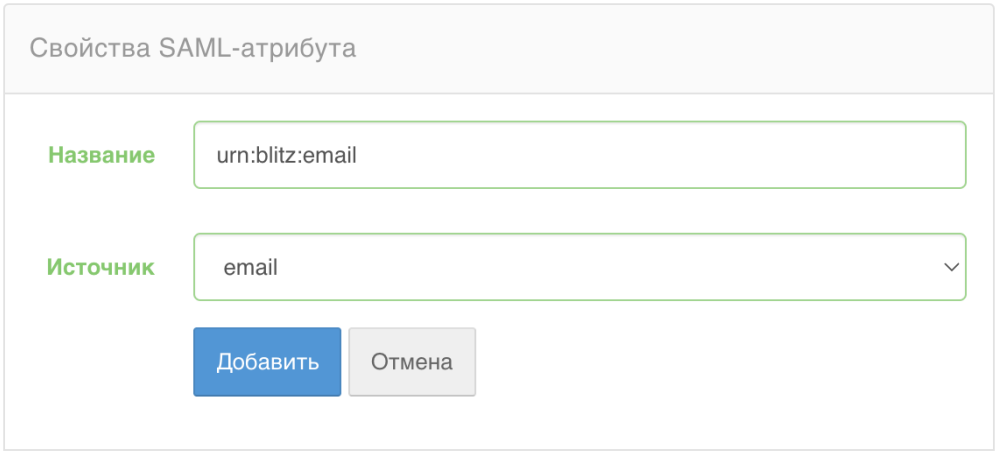


6. Нажмите кнопку **Добавить**.

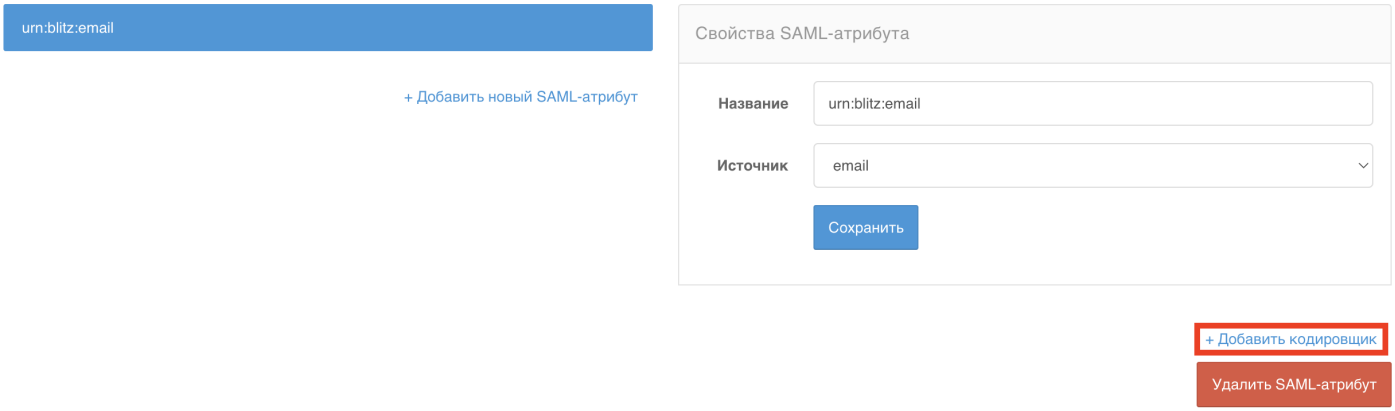
Этап 2. Настройки на стороне Blitz Identity Provider

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

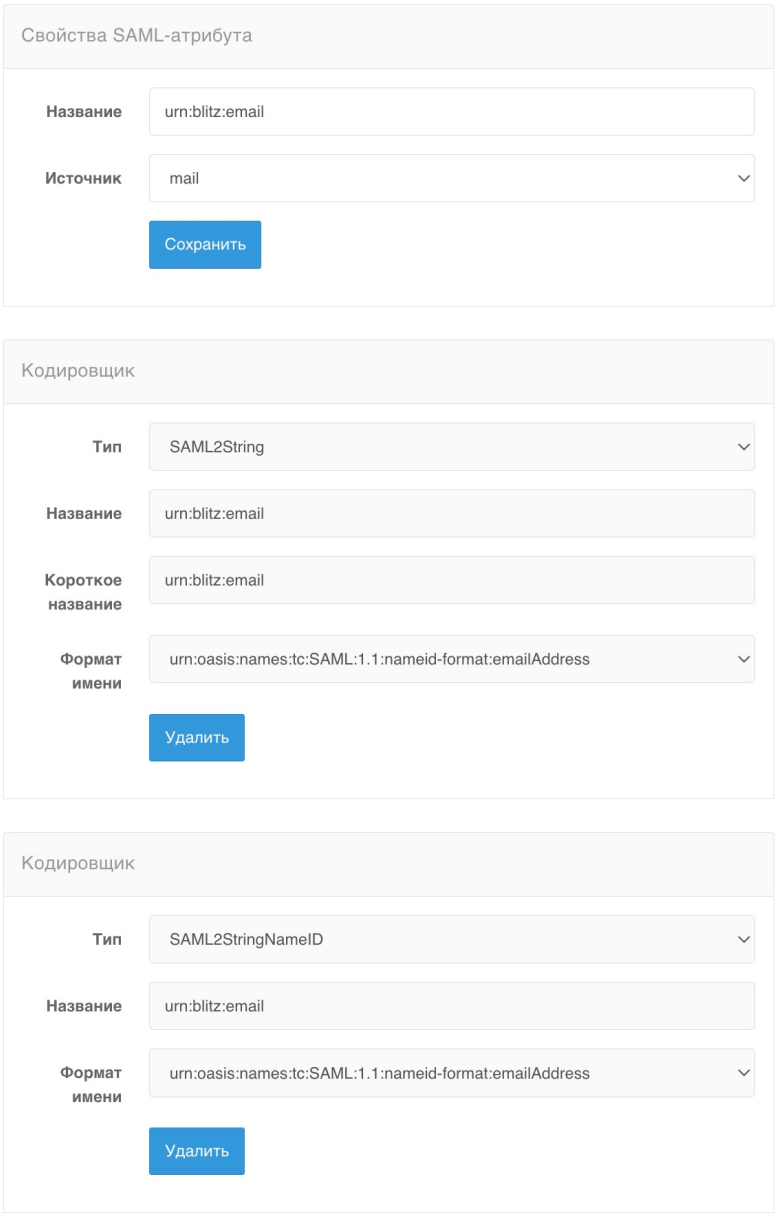
1. Нажмите **Добавить новый SAML-атрибут**.
2. Укажите название атрибута и его источник в хранилище. В данном случае источник `email`. Выберите его из выпадающего списка.
3. После заполнения свойств атрибута нажмите **Добавить**.



4. Далее добавьте кодировщик для атрибута. Для этого выберите атрибут и нажмите **Добавить кодировщик**.

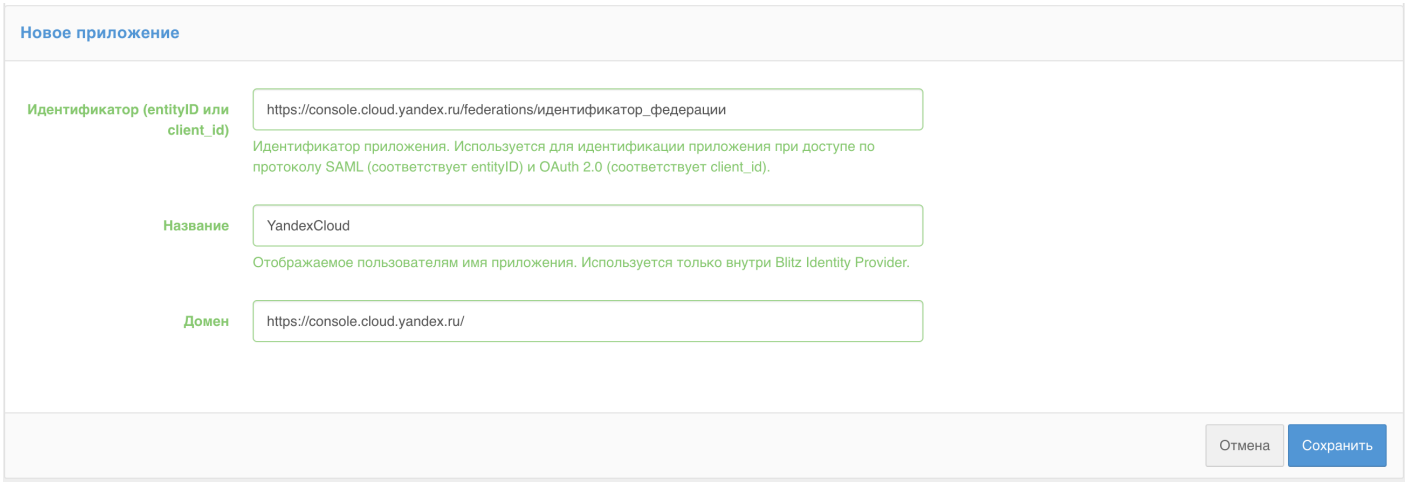


5. Для атрибута добавьте кодировщики `SAML2String` и `SAML2StringNameID`. Присвойте каждому кодировщику название `urn:blitz:email`.
6. Задайте настройки кодировщика по аналогии с приведенным ниже примером:



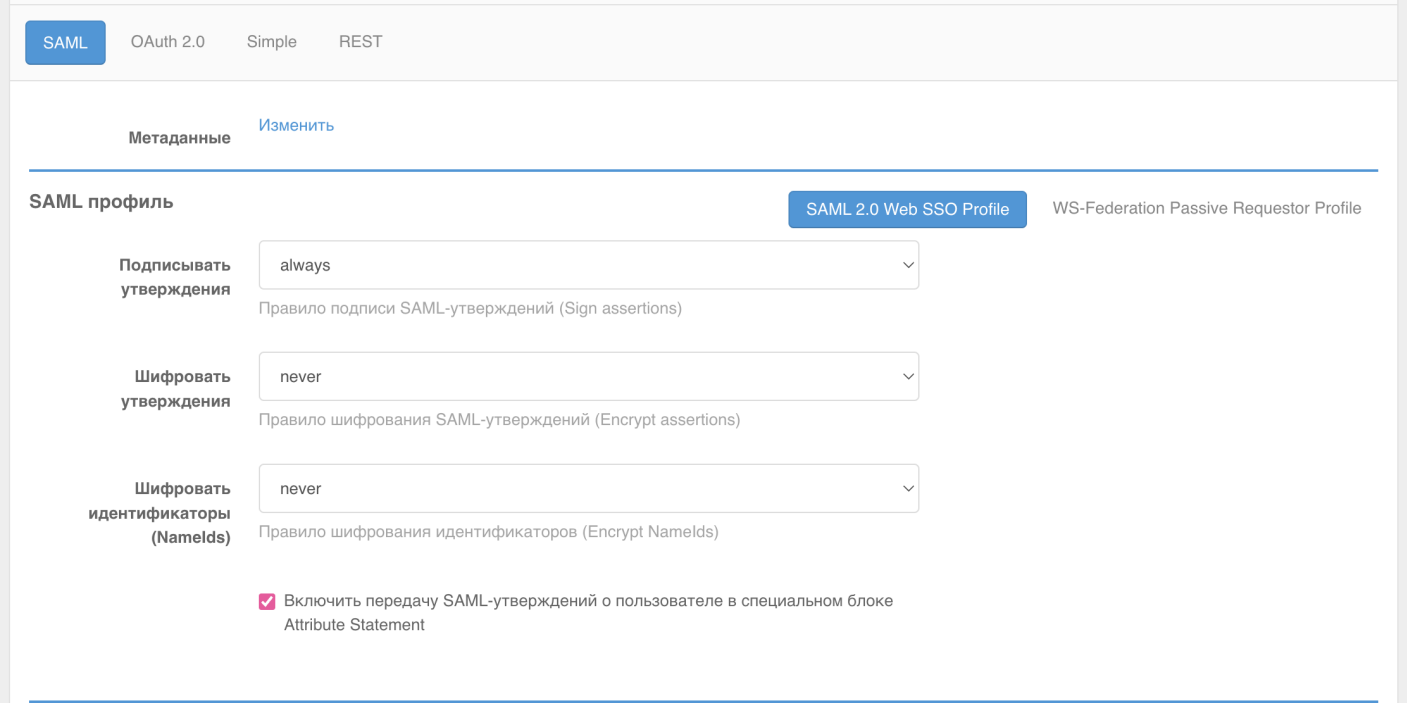
7. Нажмите **Сохранить** после каждого создания кодировщика.
8. Далее в консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения**.
9. Создайте новое приложение, задав его базовые настройки:

- **Идентификатор (entityID или client_id)**: ACS URL из Yandex Cloud в формате `https://console.cloud.yandex.ru/federations/идентификатор_федерации`
- **Название**: укажите название приложения, которое видно только внутри Blitz. Например, `YandexCloud`.
- **Домен**: `https://console.cloud.yandex.ru/`

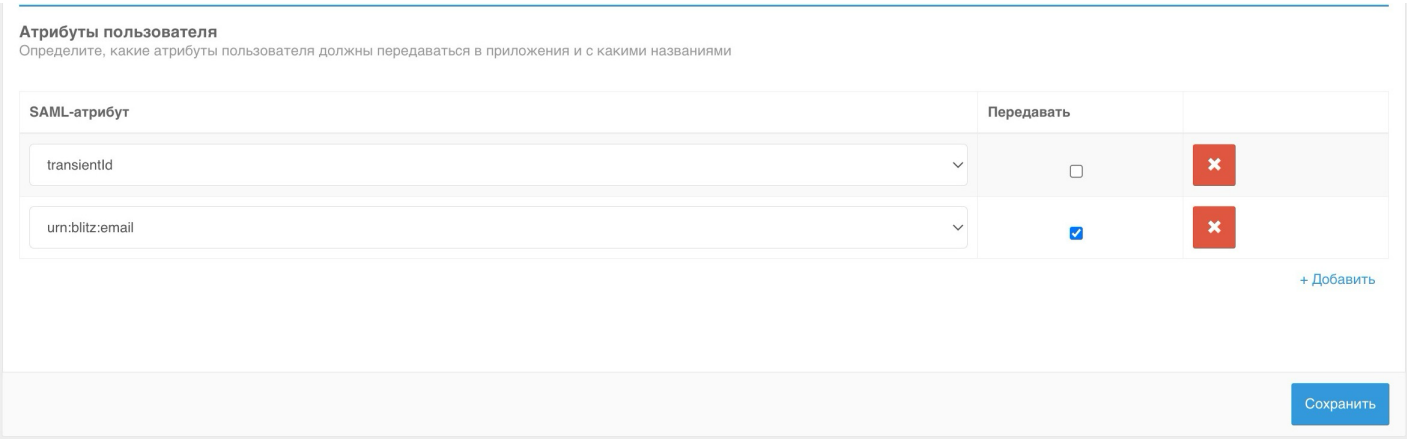


10. Нажмите **Сохранить**.
11. Далее нажмите кнопку **Параметры**  у предложения YandexCloud и отредактируйте параметры приложения:

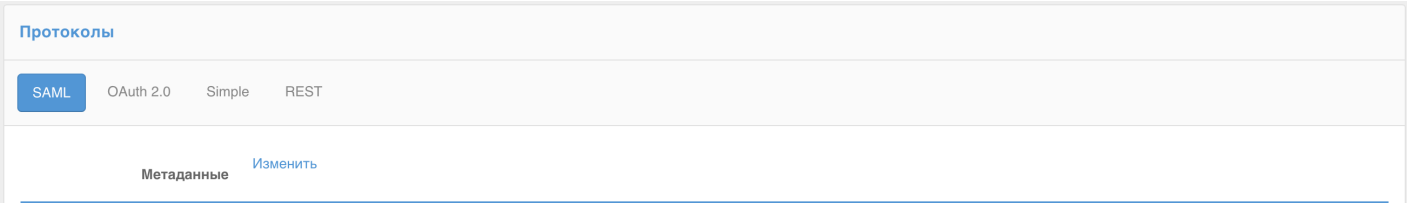
- **Протоколы**: выберите `SAML` и нажмите **Сконфигурировать**
- Выберите **SAML 2.0 Web SSO Profile** и нажмите **Сконфигурировать**. Установите следующие настройки:
  - **Подписывать утверждения**: `always`
  - **Шифровать утверждения**: `never`
  - **Шифровать идентификаторы (NameIds)**: `never`
  - **Включить передачу SAML-утверждений о пользователе в специальном блоке AttributeStatement**: установить флажок.



12. В разделе **Атрибуты пользователя** настройте передачу в Yandex Cloud атрибута `transientId`, а также созданного на первом этапе SAML-атрибута.



13. Нажмите **Сохранить**.
14. Далее в разделе **Метаданные** нажмите **Изменить**. Скопируйте и вставьте следующий код, заменив ссылку в `entityID` и `Location`, которая находится в Yandex Cloud в поле ACS URL.




```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                     entityID="https://console.cloud.yandex.ru/federations/идентификатор_федерации">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <md:AssertionConsumerService index="1" isDefault="true"
                                 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                                 Location="https://console.cloud.yandex.ru/federations/идентификатор_федерации"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

15. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в Yandex Cloud: `https://console.yandex.cloud/federations/идентификатор_федерации`.

Версия #5
Superadmin создал 2024-08-12 14:34:02 UTC
Superadmin обновил 2025-04-02 10:31:36 UTC