# Локальный выход (Logout)

Оглавление



---

## # Общие положения

- Все параметры запросов и ответов, атрибуты пользователей и прочие параметры являются регистрозависимыми.
- Все параметры запросов и ответов являются обязательными, если явно не указано обратное.
- Переносы строк в некоторых примерах запросов добавлены для удобства чтения, реальная строка запроса должна быть без них.
- При запросах к API, ошибки со статусом 503 всегда приходят в HTML.

## # Завершение сессии и инвалидация токенов

### Инициирование завершения сессии и инвалидации токенов

Завершение сеанса на RooX UIDM МОЖЕТ быть технически инициировано одним из двух способов:

1. Вызовом AJAX-эндпоинта
2. Переходом на URL выхода

ВАЖНО

Следует использовать AJAX, если нет технических ограничений.

#### Вызов AJAX-эндпойнта

ПРЕДУПРЕЖДАЕМ

Содержимое раздела может измениться

Выданный ранее токен может быть инвалидирован отправкой серверного запроса на соответствующий адрес RooX UIDM. Подключаемый сервис должен поддержать AJAX endpoint, выполняющий серверный запрос к RooX UIDM. Дополнительная аутентификация для этого метода не требуется, достаточно передать действующий access token.

Для этого нужно выполнить POST запрос на соответствующий URL RooX UIDM с указанием access token пользователя.

```
POST /sso/oauth2/revoke HTTP/1.1
Host: sso.uidm.ru
Content-Type: application/x-www-form-urlencoded
Accept: application/json

token=7bdaeacc-3d80-415c-920f-a7c30ca5e743&token_type_hint=access_token
```

- ‹token› — токен для инвалидации
- ‹token_type_hint› — тип токена, всегда access_token

### Успешное завершение сессии

В случае успешной инвалидации пользовательской сессии, RooX UIDM вернет следующий ответ с пустым телом:

```
HTTP/1.1 200 OK
```

### Неуспешное завершение сессии

В случае ошибки инвалидации пользовательской сессии, RooX UIDM сообщит об ошибке в теле ответа с параметрами:

- error - код ошибки согласно спецификации OAuth 2.0 Token Revocation RFC 7009 пункт 4.1.1
- error_description - текстовое описание ошибки

```
HTTP/1.1 400 Bad Request
```

```
{
    "error_description": "Requested token type is not supported.",
    "error": "unsupported_token_type"
}
```

## Вызвать сценарий завершения сессии через редирект

Завершение сессии из RooX UIDM может быть осуществлено переходом аутентифицированного пользователя на URL выхода. При этом RooX UIDM завершит текущую сесиию пользователя и удалит все выданные в рамках данной сессии токены. Желательно добавить в URL параметр goto с адресом обратного перехода, на этот адрес пользователь будет перенаправлен сразу после выхода.

```
https://sso.uidm.ru/UI/Logout?goto=https://client.example.org
```

### Завершение сессии

Пользователь будет перенаправлен на адрес, указанный в параметре goto

## Вызов callback-URL при инвалидации токенов

При инвалидации токена клиента RooX UIDM может выполнить запрос на URL подключаемого сервиса с оповещением о факте инвалидации. Список URL для оповещения регистрируется в опроснике в AUTHZ.15 и настраивается администратором RooX UIDM при подключении сервиса. Внешняя система, получив такое оповещение, должна немедленно инвалидировать локальную сессию пользователя.

ВАЖНО

Недопустимо удаление атрибутов из локальной http-сессии вместо полной ее инвалидации.

# Использование компонента OAuth2.0 Consumer

Компонент OAuth2.0 Consumer позволяет выполнить локальный выход из сессии при этом очистив содержимое cookie с access_token и refresh_token.

## Инициирование завершения сессии и инвалидации токенов

Существует два способа завершение сеанса RooX UIDM через OAuth2.0 Consumer:

1. Вызовом AJAX-эндпоинта
2. С перенаправлением на URL выхода

ВАЖНО

Следует использовать AJAX, если нет технических ограничений.

### Вызов AJAX-эндпойнта

ПРЕДУПРЕЖДАЕМ

Содержимое раздела может измениться

Выданный ранее токен может быть инвалидирован отправкой серверного запроса на соответствующий адрес RooX UIDM. Подключаемый сервис должен поддержать AJAX endpoint, выполняющий серверный запрос к RooX UIDM.

Запрос аутентифицируется через передачу Bearer токена, либо через cookie аутентификации.

### Пример вызова запроса на Logout с авторизацией через cookie

```
GET /sso/oauth2-consumer/logout?revocation&client_id=<agent> HTTP/1.1
Host: sso.uidm.ru
Content-Type: application/x-www-form-urlencoded
Accept: application/json
Cookie: at=<access_token>; reft=<refresh_token>
```

- ‹agent› — имя агента OAuth2, для которого был выдан access token, используется для определения имени cookie с токена доступа (опционально)
- ‹access_token› — токен для инвалидации
- ‹refresh_token› — refresh токен (также будет инвалидирован)

### Пример вызова запроса на Logout с авторизацией через токен в заголовке

```
GET /sso/oauth2-consumer/logout?revocation HTTP/1.1
Host: sso.uidm.ru
Content-Type: application/x-www-form-urlencoded
Authorization: Bearer sso_1.0_<access_token>
Accept: application/json
```

- ‹access_token› — токен для инвалидации

### Успешное завершение сессии

В случае успешной инвалидации пользовательской сессии, OAuth2 Consumer вернет следующий ответ с пустым телом. Если запрос содержал cookie `at` и/или `reft` (имена cookie настраиваются для агента), они будут сброшены.

```
HTTP/1.1 204 No Content
Set-Cookie: at=LOGOUT; Domain=sso.uidm.ru; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/;
Secure; HttpOnly
Set-Cookie: reft=LOGOUT; Domain=sso.uidm.ru; Expires=Thu, 01-Jan-1970 00:00:10 GMT;
Path=/; Secure; HttpOnly
```

## Вызвать сценарий завершения сессии через редирект

Чтобы завершить сессию с удалением авторизационных cookie путем перехода по ссылке, без AJAX-запросов, OAuth2 Consumer позволяет выполнить запрос с последующим переходом на URL логаута RooX UIDM. При этом RooX UIDM завершит текущую сесиию пользователя и удалит все выданные в рамках данной сессии токены и авторизационные cookie. Желательно добавить в URL параметр goto с адресом обратного перехода, на этот адрес пользователь будет перенаправлен сразу после выхода.

```
https://sso.uidm.ru/sso/oauth2-consumer/logout?client_id=
<agent>&redirect_uri=%2F..%2Fsso%2FUI%2FLogout%3Fgoto%3Dhttps%253A%252F%252Fsso.uidm.ru%25
2Flogin%26gotoOnFail%3Dhttps%253A%252F%252Fsso.uidm.ru%252Flogin
```

- ‹agent› — имя агента OAuth2, для которого был выдан access token, используется для определения имени cookie с токена доступа (опционально)

В параметре redirect_uri указывается URI запроса на Logout RooX UIDM, в котором, в свою очередь указываются параметры goto и gotoOnFail указывающие адрес куда будет перенаправлен пользователь при успешной и неуспешной завершении сессии. URL

ЗАМЕТКА

Значения параметров goto и gotoOnFail подвергаются двойному URL-кодированию.