

API противодействия мошенничеству (антифрода)

Оглавление

- # Общие обозначения и договоренности
- # Методы API
 - # Блокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по номеру телефона)
 - # Блокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по его идентификатору)
 - # Разблокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по номеру телефона)
 - # Получение списка заблокированных RooX UIDM OAuth клиентов для учетной записи (вариант адресации учетной записи по номеру телефона)
 - # Блокировка/Разблокировка учетной записи
 - # Понижение уровня авторизации для сессии учетной записи пользователя по RooX UIDM OAuth-клиенту
 - # Блокирование OAuth клиентов с помощью OpenAM REST API
 - # Обработка ошибок
- # Ссылки

Общие обозначения и договоренности

- {{sso_host}} - базовый адрес сервера RooX UIDM, например <https://sso.rooxteam.com>
- В случае успешного выполнения запроса, HTTP статус ответа будет 20X, в случае проблем, код статуса будет - 4XX-5XX, в теле ответа будет описание ошибки.
- При запросах к API ошибки со статусом 503 всегда приходят в виде HTML.
- При каждом запросе необходимо использовать Basic авторизацию, например:

```
Authorization: Basic dGVzdGxvZ2luOnRlc3RwYXNzd29yZA==
```

- Каждый сервис защищаемый RooX UIDM представляется как отдельный OAuth клиент

Методы API

Блокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по номеру телефона)

Блокирование учетной записи происходит по номеру телефона пользователя путем создания записи блокировки с указанием RooX UIDM OAuth клиента.

ВАЖНО

Список доступных OAuth клиентов предоставляется в документации по внедрению.

Пример запроса

```
POST /sso/antifraud/blockedResourceService?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "resourceServiceId": "selfcare",
  "blockedTo": "2015-02-18T12:00:00.000+00:00"
}
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- resourceServiceId - строковое поле, имя oauth клиента.
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

Блокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по его идентификатору)

Блокирование учетной записи происходит путем создания записи блокировки с указанием RooX UIDM OAuth клиента и идентификатором пользователя.

ВАЖНО

Список доступных OAuth клиентов предоставляется в документации по внедрению.

Пример запроса

```
POST /sso/antifraud/blockedResourceService
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "resourceServiceId": "selfcare",
}
```

```
{
  "blockedTo": "2015-02-18T12:00:00.000+00:00",
  "principal": {
    "id": "sso___1918181789261"
  }
}
```

- principal.id - строковое поле, с идентификатором учетной записи пользователя
- resourceServiceId - строковое поле, имя oauth клиента.
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

Разблокировка доступа учетной записи к заданному приложению (вариант адресации учетной записи по номеру телефона)

Разблокировка учетной записи происходит также по номеру телефона пользователя и названию RooX UIDM OAuth клиента.

Пример запроса

```
DELETE /sso/antifraud/blockedResourceService?resourceServiceId=selfcare&msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- resourceServiceId - строковое поле, имя OAuth клиента

Получение списка заблокированных RooX UIDM OAuth клиентов для учетной записи (вариант адресации учетной записи по номеру телефона)

Получение списка заблокированных идентификаторов OAuth клиентов происходит по номеру телефона пользователя.

Пример запроса

```
GET /sso/antifraud/blockedResourceService?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

Пример ответа:

```
[
  {
    "resourceServiceId": "selfcare",
```

```
{
  "blockedTo": "2015-02-18T12:00:00.000+00:00"
}
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры

Блокировка/Разблокировка учетной записи

Блокирование учетной записи происходит путем создания объекта Block с полем blockedTo.

Разблокирование учетной записи происходит путем удаления объекта Block.

Пример запроса для блокировки пользователя

```
POST /sso/antifraud/blocks?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "blockedTo": "2015-02-18T12:00:00.000+00:00"
}
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

Примеры запросов для "вечной" блокировки пользователя

```
POST /sso/antifraud/blocks?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "blockedTo": ""
}
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

```
POST /sso/antifraud/blocks?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "blockedTo": "9999-01-01T00:00:00.000+00:00"
}
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

Пример запроса для разблокировки

```
DELETE /sso/anti-fraud/blocks?msisdn=9211234567
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

- msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- blockedTo - дата, время в формате ISO, без временной зоны - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

Понижение уровня авторизации для сессии учетной записи пользователя по RooX UIDM OAuth-клиенту

Для получения списка всех токенов для пользователя по OAuth-клиенту нужно выполнить запрос

```
GET /sso/antifraud/tokens?principal.msisdn=9211234567&clientId={{client}}
Host: {{sso_host}}
Accept: application/json
```

- principal.msisdn - строковое поле, с номером телефона длиной 10 символов, только цифры
- clientId - идентификатор OAuth клиента

который вернет список вида

```
[
  {
    "tokenId": "ecb28a80-c5be-4a00-8c8a-446242637b23",
  }
]
```

```
]  {
  "authLevel": 5
}
```

- tokenId - идентификатор токена
- authLevel - назначенный уровень авторизации для токена

Для понижения уровня авторизации по токену нужно выполнить запрос

```
PUT /sso/antifraud/tokens/{tokenId}
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

```
{
  "authLevel": 3
}
```

- tokenId - идентификатор токена, полученный на предыдущем шаге
- authLevel - требуемый уровень авторизации

В случае, если переданный уровень авторизации выше действующего, то метод вернет 400 со специальным кодом в теле ответа

```
{
  "error": {
    "code": -1101,
    "message": "RX_SSO_PROVIS_9016: Unable to decrease authLevel because current authLevel '3' is less than required '5'."
  }
}
```

Блокирование OAuth клиентов с помощью OpenAM REST API

ВАЖНО

В данной версии продукта этот функционал требует дополнительной конфигурации

Авторизация

Для блокировки/разблокировки OAuth клиентов нужно получить token доступа.

Пример получения token доступа

```
POST /sso/json/authenticate HTTP/1.1
```

```
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
X-OpenAM-Username: {{username}}
X-OpenAM-Password: {{password}}
```

```
{
  "tokenId":
  "AQIC5wM2LY4SfcwN9407g8Qmn0hGEud07eLYtB2wFcuK73A.*AAJTSQACMDIAA1NLABQtMzQ0MjQzMDg5MTU0NDI3
  MzYxMwACUzEAAjAx*",
  "successUrl": "/sso/console"
}
```

- username - имя пользователя
- password - пароль пользователя
- tokenId - авторизационный token
- successUrl - адрес консоли управления

Получение списка OAuth клиентов

```
GET /sso/json/customer/agents/?_queryID=* HTTP/1.1
Host: {{sso_host}}
st: {{tokenId}}
Accept: application/json
```

Пример ответа:

```
{
  "result": [
    "provision",
    "antifraud"
  ],
  "resultCount": 2,
  "pagedResultsCookie": null,
  "remainingPagedResults": -1
}
```

- result - список доступных OAuth клиентов
- tokenId - авторизационный token
- pagedResultsCookie - куки для постраничного вывода результата запроса
- remainingPagedResults - оставшееся количество страниц результата запроса

Блокирование и разблокирование клиентов

Пример запроса блокировки/разблокировки OAuth клиента.

ВАЖНО

Блокировка и разблокировка OAuth клиентов может быть применена не сразу. Максимальное время реакции задается настройкой и по умолчанию составляет 60 секунд.

```
PUT /sso/json/customer/agents/{{client}} HTTP/1.1
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
st: {{tokenId}}
```

```
{
  "sunIdentityServerDeviceStatus": [
    "Inactive"
  ]
}
```

- tokenId - авторизационный token
- sunIdentityServerDeviceStatus - статус OAuth клиента, ["Active", "Inactive"]

Временная блокирование клиентов

Пример запроса блокировки/разблокировки OAuth клиента.

ВАЖНО

Блокировка и разблокировка OAuth клиентов может быть применена не сразу. Максимальное время реакции задается настройкой и по умолчанию составляет 60 секунд.

```
PUT /sso/json/customer/agents/{{client}} HTTP/1.1
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
st: {{tokenId}}
```

```
{
  "sunIdentityServerDeviceStatus": [
    "Active"
  ],
  "blockedTo": [
    "2015-02-18T12:00:00.000+00:00"
  ]
}
```


- tokenId - авторизационный token
- sunIdentityServerDeviceStatus - Для временной блокировки нужно использовать статус Active.
- blockedTo - дата, время в формате ISO с временной зоной - определяет срок блокировки. Разблокировка происходит автоматически по достижению указанного времени. Если передать дату "9999-01-01" или пустое значение (""), то учетная запись сможет быть разблокирована только администратором системы.

ЗАМЕТКА

Использование массивов в REST API является деталью реализации ForgeRock OpenAM.

Получение статуса OAuth клиента

Пример запроса получения статуса OAuth клиента.

```
GET /sso/json/customer/agents/{{client}}?_fields=sunIdentityServerDeviceStatus HTTP/1.1
Host: {{sso_host}}
st: {{tokenId}}
Accept: application/json
```

Пример ответа:

```
{
  "sunIdentityServerDeviceStatus": [
    "Active"
  ]
}
```

- tokenId - авторизационный token
- client - идентификатор OAuth клиента
- sunIdentityServerDeviceStatus - статус OAuth клиента, ["Active", "Inactive"]

Обработка ошибок

Если операция завершилась неуспешно - будет возвращен соответствующий HTTP статус и описание ошибки следующего вида в теле ответа. Все HTTP коды кроме **20X** следует расценивать как ошибки provisioning-a, логировать код.

Пример тела ответа с ошибкой

```
{
  "error": {
    "code": 404,
    "message": "RX_SSO_PROVIS_9001: User with msisdn '9211234567' not found"
  }
}
```

```
{
  "error": {
    "code": 404,
    "message": "RX_SSO_PROVIS_9002: Resource 'wrong_resource' not found"
  }
}
```

```
{
  "error": {
    "code": 400,
    "message": "RX_SSO_PROVIS_9002: Object block already exists"
  }
}
```

- code - код ошибки
- message - описание ошибки

Ссылки

E.164 формат - http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.164-200502-S!!PDF-R&type=items

