Спецификация API для ЛК

Оглавление

1. История изменений
2. Авторизация
3. Спецификация SSO REST API для работы с историей аутентификации
4. Самостоятельная блокировка пользователя в ЛК
5. Смена пароля пользователя в ЛК

Версия продукта: sso-server-ocb-{project-version}

1. История изменений

Версия документа	Дата изменения	Комментарий
v1.0.0	2014-12-03	Создание документа
v1.1.0	2015-01-29	Для всех запросов context-path сервера SSO изменен с "/openam" на "/sso".
v1.1.1	2015-08-20	Добавлено предупреждение о возврате 503 ошибки в виде HTML.
v1.1.2	2015-09-23	Добавлена информация по конечным точкам

2. Авторизация

Авторизация запросов в WebSSO будет проходит через HTTP заголовок Authorization в формате "Bearer ‹oauth_token›"

- ‹oauth_token› - OAuth 2.0 токен полученый от RooX WebSSO

3. Спецификация SSO REST API для работы с историей аутентификации

3.1. Общие обозначения и договорености

- {{sso_host}} - базовый адрес сервера SSO, например https://sso.rooxteam.com
- В случае успешного выполения 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 HTML.

3.2. Получение истории попыток аутентификации

Пример запроса

ВАЖНО

Параметры **fromDate** и **toDate** являются обязательными полями.

```
GET /sso/api/operationAudit?msisdn=9211234567&fromDate=2014-10-
14T14:00:00.000Z&toDate=2014-10-
15T14:00:00.000Z&size=20&page=0&opertaions=sso.auth.success,sso.auth.fail
Host: {{sso_host}}
Content-Type: application/json
Accept: application/json
```

- msisdn - строковое поле с номером телефона длиной 10 символов, только цифры
- fromDate - строковое значение даты начала промежутка выборки в формате UTC (в формате ISO 8601)
- toDate - строковое значение даты окончания промежутка выборки в формате UTC (в формате ISO 8601)
- page - номер страницы выборки, значение по умолчанию равно 0
- size - количество элементов на странице, значение по умолчанию равно 20
- operations - имена событий аудита (см. пример ответа), перечисляются через запятую

Пример ответа, содержащий историю попыток аутентификации


```
{
  "content": [
    {
      "id": "sso_____b60c7f02-5d17-4e43-8c7a-4e2e71c3aba9",
      "name": "sso.auth.success",
      "msisdn": "79876543210",
      "imei": "12345678901234567",
      "imsi": "123456789012345",
      "iccid": "1234567890",
      "timeStart": "2015-03-05T09:30:48.524Z",
      "timeEnd": "2015-03-05T09:30:48.524Z",
      "ipAddress": 167772674,
      "ipAddressString": "10.0.2.2",
      "geoIPCountry": "RU",
      "geoIPRegionId": "2097",
```

```
      "geoIPRegionNameNat": "Москва",
      "geoIPCityId": "2097",
      "geoIPCityNameNat": "Москва",
      "geoIPDatabase": "geoipbase",
      "geoIPDatabaseVersion": "2015-01-01",
      "userAgent": "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/40.0.2214.115 Safari/537.36",
      "nodeId": "sso",
      "correlationId": "VNW6AAUQHGLVPA",
      "authType": "login_password",
      "service": "dispatcher",
      "requestAuthLevel": "2",
      "gotoUrl": "https://sso.rooxteam.com/sso/UI/Login?
org=customer&service=uidm&goto=%2Fsso%2Foauth2%2Fauthorize%3Fresponse_type%3Dcode%26redire
ct_uri%3Dhttps%3A%2F%2Fsso.rooxteam.com%2Fsso%2Fsecure%2Flk.jsp%26realm%3Dcustomer%26clien
t_id%3Dselfcare&gotoOnFail=%2Fsso%2Foauth2%2Fauthorize%3Fresponse_type%3Dcode%26redirect_u
ri%3Dhttps%3A%2F%2Fsso.rooxteam.com%2Fsso%2Fsecure%2Flk.jsp%26realm%3Dcustomer%26client_id
%3Dselfcare&ForceAuth=true",
      "referer": "https://sso.rooxteam.com/sso/auth/dispatcher",
      "data": {}
    }
  ],
  "page": {
    "size": 20,
    "totalElements": 1,
    "totalPages": 1,
    "number": 0
  }
}
```


- id - уникальный идентификатор события
- name - имя события аудита (см. События аудита)
- msisdn - строковое поле с номером телефона абонента, если он существует в БД при попытке логина.
- imei - идентификатор мобильного оборудования
- imsi - идентификатор мобильного абонента
- iccid - индентификатор SIM-карты
- timeStart - дата начала события
- timeEnd - дата окончания события, чаще всего совпадает с датой начала
- ipAddress - числовое представление IP адреса
- ipAddressString - строковое представление IP адреса
- geoIPCountry - страна определенная по IP адресу
- geoIPRegionId - код региона определенного по IP адресу
- geoIPRegionNameNat - название региона определенного по IP адресу
- geoIPCityId - код города определенного по IP адресу
- geoIPCityNameNat - название города определенного по IP адресу
- geoIPDatabase - идентификатор использованной БД GeoIP
- geoIPDatabaseVersion - версия БД GeoIP
- userAgent - user-agent HTTP клиента
- nodeId - имя узла обработавшего запрос
- correlationId - отладочный идентификатор запроса

- authType - модуль, выполнивший аутентификацию
- service - цепочка аутентификации
- requestAuthLevel - запрошенный уровень авторизации
- gotoUrl - адрес для перехода после успешной аутентификации
- referer - инициатор запроса из заголовка Referer
- data - дополнительные атрибуты

В случае использования недопустимых параметров, будет возвращен пустой ответ с HTTP статусом 400. В случае ошибки авторизации, будет возвращен пустой ответ с HTTP статусом 403.

3.3. Обработка ошибок

Если операция завершилась неуспешно, то будет возвращен соответствующий HTTP статус и описание ошибки в теле ответа.

Примеры ответа с ошибкой

```
{
  "error": {
    "code": -901,
    "message": "Long period of time"
  }
}
```

[anchor-1] ==== События аудита

Имя события	Описание
sso.auth.success	Событие успешных попыток аутентификации
sso.auth.fail	Событие неуспешных попыток аутентификации
sso.auth.auto.fail	Событие неуспешных попыток автоматической аутентификации
sso.auth.increase.success	Событие успешных попыток повышения уровня авторизации
sso.auth.increase.fail	Событие неуспешных попыток повышения уровня авторизации
sso.protected.resource.access	Событие доступа к защищенным ресурсам
sso.admin.action	Событие действий администраторов

4. Самостоятельная блокировка пользователя в ЛК

Самостоятельная блокировка SIM-карты пользователем в ЛК возможна после процесса аутентифиции.

ВАЖНО

Самостоятельная блокировка выполняется через существующие механизмы, реализованные в ПО производства Петер-Сервис. Информация о самостоятельной блокировке передаётся в WebSSO через Provisioning API.

5. Смена пароля пользователя в ЛК

Смена пароля возможна после повышения уровня авторизации. (Требуется предварительная аутентификация пользователя в ЛК)

ЛК через WebSSO переводит пользователя на повышение уровня авторизации с помощью OTP.

После успешного повышения уровня проводит авторизацию запроса и допускает пользователя до смены пароля.

ВАЖНО

Смена пароля на данном этапе проекта выполняется через существующие механизмы, реализованные в ПО производства Петер-Сервис. Информация о новом пароле передаётся в WebSSO через Provisioning API.

6. Приложение 1. Базовые адреса конечных точек.

Раздел содержит значения для базовых адресов конечных точек, используемых в проекте.

Таблица 1. Базовые адреса конечных точек WebAPI управленя привязками

Окружение	Базовый адрес	Комментарий
vagrant	http://sso.ocb.hosted:8080/webapi-1.0	
интеграционное		
продуктив		