

## Справочник событий аудита

### Оглавление

- # Типы протоколируемых событий
  - # Аутентификация и деаутентификация (выход из учётной записи)
  - # Управление токенами
  - # API-токены
  - # Авторизация действий
  - # Управление привязками социальных сетей
  - # Управление привязками мультиаккаунтов
  - # Блокировка и разблокировка пользователей
  - # Изменение пользовательских данных
  - # Управление организациями и организационными ролями пользователей
- # Модель данных протоколируемого события

## # Типы протоколируемых событий

### Аутентификация и деаутентификация (выход из учётной записи)

`sso.auth.success`

Успешная попытка аутентификации пользователя в UIDM

`sso.auth.fail`

Неудачная попытка аутентификации пользователя в UIDM

`sso.auth.revoke`

Принудительное завершение сессии

`sso.auth.logout`

Инвалидация сессии пользователя

`sso.auth.auto.fail`

Неуспешная попытка аутентификации с использованием токена автоматического входа

`sso.auth.autologin.token.created`

Успешная аутентификация с использованием токена автоматического входа (с последующим выпуском токена доступа, токена обновления доступа)

`sso.auth.token.lifetime.end`

Завершение сессии по таймауту

`sso.auth.increase.success`

Успешное повышение уровня доступа в текущей сессии

`sso.auth.increase.fail`

Неуспешная попытка повышения уровня доступа в текущей сессии

`sso.api.session.delete.success`

Удаление сессии через API управления сессиями ( `/sessionlist` ) или APM Контакт-Центра

`sso.api.session.delete.fail`

Неуспешное удаление сессии через API управления сессиями ( `/sessionlist` ) или APM Контакт-Центра

`sso.auth.preauth.success`

Попытки аутентификации пользователей с использованием логина и пароля в UIDM, которые завершились успешно (сам процесс продолжается; следующим шагом может быть ввод одноразового пароля). Токен доступа еще не выпущен, так что это событие можно использовать только для предварительных действий, например «прогрева» кеша бизнес-данных.

## Управление токенами

`sso.auth.get_access_token.success`

Выпуск токена доступа (access token)

`sso.auth.get_access_token.fail`

Неуспешный выпуск токена доступа (access token)

`sso.token_exchange.success`

Успешный выпуск нового токена доступа путем обмена токенов в соответствии со спецификацией OAuth token exchange

`sso.refresh.success`

Успешная выдача нового токена доступа путем обновления старого (OAuth refresh token flow)

`sso.auth.token_introspection.success`

Успешная интроспекция токена ( `/tokeninfo` )

`sso.auth.token_introspection.fail`

Неуспешная интроспекция токена ( `/tokeninfo` )

## API-токены

`sso.apitokens.creation.success`

Успешный выпуск API-токена пользователем

`sso.apitokens.revocation.success`

Успешный отзыв API-токена пользователем

`sso.auth.protected.resource.success_access`

Успешный доступ к защищаемому ресурсу. Достоверность регистрации событий зависит от корректности работы защищаемого ресурса. При доступе по API-токену в этом событии будет указано `authType = apitokens`

## Авторизация действий

`sso.auth.protected.resource.success_access`

Успешный доступ к защищаемому ресурсу. Достоверность регистрации событий зависит от корректности работы защищаемого ресурса. При доступе по API-токену в этом событии будет указано `authType = apitokens`

`sso.auth.protected.resource.fail_access`

Неуспешный доступ к защищаемому ресурсу. Достоверность регистрации событий зависит от корректности работы защищаемого ресурса. При доступе по API-токену в этом событии будет указано `authType = apitokens`

`sso.auth.otp_code.success`

Событие успешного ввода одноразового пароля

`sso.auth.otp_code.fail`

Событие неуспешного ввода одноразового пароля

## Управление привязками социальных сетей

`webapi.social.mapping.create.success`

Успешное создание привязки

`webapi.social.mapping.create.fail`

Неуспешное создание привязки

`webapi.social.mapping.delete.success`

Успешное удаление привязки

`webapi.social.mapping.delete.fail`

Неуспешное удаление привязки

## Управление привязками мультиаккаунтов

`webapi.multiaccount.mapping.create.success`

Успешное создание привязки

`webapi.multiaccount.mapping.create.fail`

Неуспешное создание привязки

`webapi.multiaccount.mapping.delete.success`

Успешное удаление привязки

`webapi.multiaccount.mapping.delete.fail`

Неуспешное удаление привязки

## Блокировка и разблокировка пользователей

`sso.principal.lock.success`

Блокировка пользователя

`sso.principal.unlock.success`

Разблокировка пользователя

## Изменение пользовательских данных

`webapi.customer.credential.login.change.success`

Успешное изменение имени учётной записи (логина) (через Customer WebAPI)

`webapi.customer.credential.login.change.fail`

Неуспешное изменение имени учётной записи (логина) (через Customer WebAPI)

`webapi.customer.credential.password.change.success`

Успешное изменение пароля (через Customer WebAPI)

`sso.credentials_change.success`

Успешное изменение пароля (через WebSSO)

`webapi.customer.credential.password.change.fail`

Неуспешное изменение пароля (через Customer WebAPI)

`sso.credentials_change.fail`

Неуспешное изменение пароля (через WebSSO)

`sso.credentials_change.blocked`

Блокировка возможности смены пароля в результате множественных ошибочных вводов предыдущего пароля

`webapi.customer.settings.set.success`

Успешная установка пользовательских настроек через Customer WebAPI  
`/customers/{principalId}/settings/view` (таблица PrincipalProperty)

`webapi.customer.settings.set.fail`

Неуспешная установка пользовательских настроек через Customer WebAPI

`/customers/{principalId}/settings/view` (таблица PrincipalProperty)

`sso.auth.credential.email.change.success`

Успешное изменение контактных данных пользователя: адреса электронной почты

`sso.auth.credential.phone.change.success`

Успешное изменение контактных данных пользователя: номера телефона

`sso.auth.credential.email.change.fail`

Неуспешное изменение контактных данных пользователя: адреса электронной почты

`sso.auth.credential.phone.change.fail`

Неуспешное изменение контактных данных пользователя: номера телефона

`sso.auth.credential.email.change.verified`

Новый адрес электронной почты пользователя подтвержден установленным способом (переходом пользователя по ссылке, направленной ему на новый адрес электронной почты)

`sso.auth.credential.phone.change.verified`

Новый телефонный номер пользователя подтвержден установленным способом (пользователь ввёл одноразовый пароль, направленный ему на новый номер телефона)

`sso.restore_password_request.success`

Успешный запрос на восстановление пароля

`sso.restore_password_request.fail`

Неуспешный запрос на восстановление пароля

`sso.settings.event-notifier.put`

Смена настроек уведомлений пользователей (в какие каналы направляются уведомления пользователю о том или ином событии)

`sso.settings.event-notifier.delete`

Удаление настроек уведомлений пользователей (сброс к значению по умолчанию)

`sso.settings.login-by-otp.put`

Изменение настроек второго фактора аутентификации (вкл, выкл)

`sso.totp.add-key`

Добавление настроек TOTP в качестве второго фактора аутентификации

`sso.totp.remove-key`

Удаление настроек TOTP в качестве второго фактора аутентификации

`sso.principal.roles_update.success`

Изменение ролей пользователя (принципала)

## Управление организациями и организационными ролями пользователей

`sso.org.created.success`

Создание организации

`sso.principal.org_roles_assign.success`

Назначение пользователю новых организационных ролей

`sso.principal.org_roles_revoke.success`

Отзыв организационных ролей пользователя

## # Модель данных протоколируемого события

`id`

### Описание

Идентификатор данной записи в БД аудита.

### Пример

`sso_6bb72c60-cb98-4faf-a4ef-b1581c841b4b`

`digest`

### Описание

Подпись лог-события

### Пример

Не используется

`ipAddress`

### Описание

IP адрес в виде числа.

### Пример

`3257718304`

`msisdn`

### Описание

Номер телефона пользователя на момент возникновения события (LEGACY поле, не использовать в новых интеграциях)

### Пример

`77123456789`

name

#### Описание

Название данного события в БД аудита.

#### Пример

`sso.auth.success` (успешная аутентификация)

principalId

#### Описание

Уникальный идентификатор пользователя. Жизненный цикл учетных записей должен исключать присваивание одного и то же идентификатора разным пользователям.

#### Пример

`sso_99f016d5-03a1-4185-8bd0-412d8da53492`

timeEnd

#### Описание

Дата и время окончания данного события.

#### Пример

`12.07.2017 0:12:29`

timeStart

#### Описание

Дата и время начала данного события (сейчас для всех событий время начала совпадает с временем окончания)

#### Пример

`12.07.2017 0:12:29`

forwardedIpAddresses

#### Описание

Цепочка запроксированных IP-адресов клиента. Работает в случае корректной настройки имени заголовка и всех обратных прокси по пути запроса.

#### Пример

—

geoIPCountry

#### Описание

Названия географических субъектов, определенные на основании IP-адреса пользователя. Заполняется при получении сервером в запросе корректного IP-адреса пользователя и интеграции с базой данных GeoIP

#### Пример

`RU`

## geoIPRegionId

### Описание

Названия географических субъектов, определенные на основании IP-адреса пользователя. Заполняется при получении сервером в запросе корректного IP-адреса пользователя и интеграции с базой данных GeoIP

### Пример

1025

## geoIPRegionNameNat

### Описание

Названия географических субъектов, определенные на основании IP-адреса пользователя. Заполняется при получении сервером в запросе корректного IP-адреса пользователя и интеграции с базой данных GeoIP

### Пример

Московская область

## accessToken

### Описание

Токен доступа, связанный с данным событием. Применимо не для всех событий.

### Пример

—

## clientId

### Описание

Идентификатор приложения — например, личный кабинет, мобильный личный кабинет и т.д., в котором произошло данное событие. Применимо не для всех событий.

### Пример

portal

## userAgent

### Описание

Информация о UserAgent, полученная от браузера пользователя. Обычно содержит данные об устройстве, ОС и браузере. В данном примере — в качестве User Agent выступала система автотестов.

### Пример

roox-autotests

## nodeId

### Описание

Имя конкретного сервера UIDM, на котором произошло событие

### Пример

aws-eu01-node03



## correlationId

### Описание

Идентификатор для сопоставления события с информацией в лог-файлах решения.

### Пример

1SF0P26MNIN6KU

## authType

### Описание

Способ аутентификации пользователя (автовход, логин-пароль, с использованием социальной сети и т. д.).  
Возможные значения:

- login\_password — вход по логину-паролю
- login-by-jwt — вход по identity-токену (jwt)
- apitokens — использование api token для вызова операции
- lite-principal-auth — вход по "легкой" учетке
- mpt — single-sign-on
- srp6a — вход по логину-паролю с использованием протокола srp6a

### Пример

login\_password

## service

### Описание

Название сценария UIDM, при работе которого возникло данное событие

### Пример

dispatcher

## url

### Описание

Запрошенный ресурс, над которым выполняется действие — используется для событий доступа к ресурсу, если в решении используется централизованная авторизация (политики)

### Пример

—

## httpMethod

### Описание

Запрошенный метод для ресурса — используется для событий доступа к ресурсу, если в решении используется централизованная авторизация (политики)

### Пример

—

requestAuthLevel

Описание

LEGACY

Пример

—

gotoUrl

Описание

—

Пример

<https://uidm.example.com>

oauthCode

Описание

Выданный OAuth2 Code в случае использования code flow при аутентификации

Пример

—

geoIPDatabase

Описание

Данные об используемой базе geoIP

Пример

geoipbase

geoIPDatabaseVersion

Описание

Данные об используемой базе geoIP

Пример

default\_2016-04-20

ipAddressString

Описание

IP адрес в виде строки.

Пример

194.44.214.32

geoIPCityId

Описание

Названия географических субъектов, определенные на основании IP-адреса пользователя. Заполняется при получении сервером в запросе корректного IP-адреса пользователя и интеграции с базой данных GeoIP

#### Пример

223

### geoIPCityNameNat

#### Описание

Названия географических субъектов, определенные на основании IP-адреса пользователя. Заполняется при получении сервером в запросе корректного IP-адреса пользователя и интеграции с базой данных GeoIP

#### Пример

Москва

### referer

#### Описание

Заголовок Referer, если событие произошло в вебе

#### Пример

—

### networkType

#### Описание

LEGACY

#### Пример

—

### data

#### Описание

Дополнительная информация о событии в формате ключ-значение. Содержимое зависит от события и настроек.

Поле может содержать клеймы токена, для этого требуется конфигурация. Что такое claims [https://uidm.ru/docs/site/generic/develop/concepts.html#\\_%D0%BA%D0%BB%D0%B5%D0%B9%D0%BC%D1%8B\\_claims](https://uidm.ru/docs/site/generic/develop/concepts.html#_%D0%BA%D0%BB%D0%B5%D0%B9%D0%BC%D1%8B_claims)

Также в поле могут попадать произвольные дополнительные данные от вызывающей стороны (веб-клиента или мобильного приложения), такие как версия приложения, MAC-адрес устройства, статус рутованности и так далее. Требуется конфигурация разрешенных полей.

#### Пример

<data></data>

### imsi

#### Описание

IMSI пользователя, для которого произошло событие. Берётся из профиля пользователя UIDM, если было передано от внешней системы при создании профиля

#### Пример

—

### iccid

#### Описание

ICCID пользователя, для которого произошло событие. Берётся из профиля пользователя UIDM, если было передано от внешней системы при создании профиля

#### Пример

—

### imei

#### Описание

IMEI пользователя, для которого произошло событие. Берётся из профиля пользователя UIDM, если было передано от внешней системы при создании профиля

#### Пример

—

### userAgentDeviceType

#### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent.

#### Пример

Desktop

### userAgentDeviceBrand

#### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent.

#### Пример

Unknown

### userAgentDeviceModel

#### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent.

#### Пример

Unknown Unknown

### userAgentOSFamily

#### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent. Для OCB может формироваться из переданной информации в блоке device\_info (будет использовано поле device\_os) в теле запроса.

#### Пример

Unknown Unknown

#### userAgentOSNameVersion

##### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent. Для OCB может формироваться из переданной информации в блоке device\_info (будет использовано поле device\_os\_version) в теле запроса.

#### Пример

Unknown Unknown Unknown

#### userAgentBrowserType

##### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent.

#### Пример

browser

#### userAgentBrowserFamily

##### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent.

#### Пример

Unknown Unknown

#### userAgentBrowserNameVersion

##### Описание

Информация об устройстве, OS и браузера. Формируется при интеграции с внешним справочником устройств на основании параметра UserAgent. Для OCB может формироваться из переданной информации в блоке device\_info (будет использовано поле app\_version) в теле запроса.

#### Пример

Unknown Unknown Unknown

#### clientGroupId

##### Описание

Группа приложений-клиентов UIDM, если у приложений настроена привязка к группам

#### Пример

LK

#### imeiDeviceBrand

##### Описание

LEGACY

##### Пример

—

#### imeiDeviceModel

##### Описание

LEGACY

##### Пример

—

#### imeiDeviceType

##### Описание

LEGACY

##### Пример

—

#### authEndpointType

##### Описание

LEGACY

##### Пример

oauth2

#### authLevel

##### Описание

Уровень авторизации, вычисленный в ходе данного события аутентификации

##### Пример

5

#### requestedScopes

##### Описание

Перечень запрошенных клиентом областей действия (scope)

##### Пример

—

## authorizedScopes

### Описание

Перечень выданных клиенту областей действия (scope)

### Пример

—

## httpHeaders

### Описание

HTTP-заголовки, полученные UIDM при вызове данной операции

### Пример

```
{
  "host": [
    "uidm.example.com"
  ],
  "accept-encoding": [
    "gzip, deflate"
  ],
  "accept": [
    "application/json"
  ],
  "user-agent": [
    "roox-autotests"
  ],
  "content-type": [
    "application/x-www-form-urlencoded"
  ],
  "cookie": [
    "RX_SID=DDC5F7400F26AFBDD999A6902468E55C;
gotoOnFail=uidm.example.com/sso/oauth2/authorize?
response_type=code&redirect_uri=uidm.example.com; lb=wms"
  ],
  "content-length": [
    "4328"
  ],
  "connection": [
    "close"
  ],
  "x-forwarded-proto": [
    "https"
  ]
}
```

## error

### Описание

Тип ошибки (для событий fail).

### Пример

—

## errorSubtype

### Описание

Дополнительная информация для данного типа ошибки (для событий fail)

### Пример

—

## executionId

### Описание

Уникальный идентификатор сценария. Позволяет связать в БД аудита несколько событий, которые происходили в рамках одного пользовательского сценария. Доступно не для всех событий.

### Пример

a01725f6-60dd-46b2-b654-40aa4dae9c42

## impersonator

### Описание

Для событий входа от имени абонента содержит информацию о том, кто выполнил такой вход.

### Пример

—

### Прочтите также

- [Работа с геолокацией пользователя](#)
- [Потоковая обработка событий аудита](#)

