Аутентификация

TotalApi SDK

# TotalAPI аутентификация

Перед использованием API необходимо зарегистрировать своё приложение. При регистрации приложения будут предоставлены два уникальных ключа: секретный ключ ApiKey и публичный ключ AppKey.

TotalAPI реализует гибкую модель аутентификации при обращении к интерфейсам API. В зависимости от того вызывается ли API из защищенной среды (например, серверная программа) или неконтролируемой среды (например, веб браузер) используется соответствующий вид аутентификации. Использование правильного вида аутентификации позволяет использовать API, так чтобы не скомпрометировать секретный ключ ApiKey и защитить данные пользователей от несанкционированного доступа.

# Выполнение аутентификации

Аутентификация с использованием ApiKey или AppKey требуется при каждом вызове методов API, кроме редких исключений, таких как функции записи данных с датчиков. Для выполнения аутентификации необходимо заполнить одно или несколько полей класса [TotalApiAuth](#TotalApiAuth) и передать данные одним из следующих способов:

1. Передача TotalApiAuth JSON-объекта как параметр auth в Endpoint URL сервиса (не рекомендуется, т.к. значение ключа можно перехватить):

https://totalapi.io/api/v1/wcf/ITelematicsService?auth={ApiKey:”456”}

1. Передача TotalApiAuth JSON-объекта в заголовке Authorization HTTP‑запроса к серверу (рекомендуется использовать защищённое HTTPS-соединения, чтобы невозможно было перехватить значение ключа):

Authorization: TOTALAPI {ApiKey:”456”}

1. Передача объекта TotalApiAuth в заголовке с именем Authorization WCF-сообщения (только для WCF API). (Рекомендуется использовать защищённый WCF-канал, чтобы невозможно было перехватить значение ключа).

# Виды аутентификации TotalAPI

* ApiKey-аутентификация

Требует значения ApiKey. Используется при работе с API в защищенной среде (например, в backend Web-приложения). При успешной аутентификации предоставляется полный доступ ко всем данным приложения, для которого сгенерирован этот ключ.

* AppKey-аутентификация

Требует значения AppKey. Используется при работе с API в незащищенных клиентских приложениях исключительно для регистрации нового пользователя приложения. При успешной аутентификации разрешены только методы API для задания имени и пароля нового пользователя. Для удаления созданного пользователя требуется ApiKey-аутентификация.

* AppUser-аутентификация

Требует значений AppKey, UserLogin, UserPassword. Используется при работе с API в незащищенных клиентских приложениях. При успешной аутентификации предоставляется доступ ко всем данным только указанного пользователя.

* ***SessionKey-аутентификация***

Требует значения **SessionKey**, полученного предварительным вызовом метода [**GetSessionKey**](BillingAPI.docx#GetSessionKey). Используется при работе с API в незащищенных клиентских приложениях. При успешной аутентификации уровень доступа к данным такой-же, как и при вызове метода [**GetSessionKey**](file:///D:\USS.GIT\TotalApi\documentation\User&Programmer%20Manuals\API%20docs\BillingAPI.docx#GetSessionKey). Для получения **SessionKey** необходима **ApiKey** или **AppUser** аутентификация.

* ***SSID-аутентификация***

Требует значения **SSID**. Используется только при работе подсистем с [подсистемой биллинга](BillingAPI.docx).

* ***SuperApiKey-аутентификация***

Требует валидного значения **ApiKey** суперадминистративного приложения. Используется исключительно при работе с [Billing API](BillingAPI.docx) административным приложением. При успешной аутентификации предоставляется полный доступ ко всем данным биллинга.

# Класс аутентификации

|  |  |  |
| --- | --- | --- |
| **TotalApiAuth** | | |
| **Свойство** | **Описание** | **Тип** |
| ApiKey | Уникальный секретный ключ для доступа к API. | string |
| SSID | Идентификатор подсистемы. Используется только при авторизации подсистем для доступа к некоторым методам интерфейсов [модуля биллинга](BillingAPI.docx). **Не должна использоваться при авторизации из клиентских приложений.** | string |
| AppKey | Уникальный публичный ключ приложения. Выдаётся вместе с **ApiKey** при регистрации нового приложения-пользователя API.  Имеет смысл, только если сторонний разработчик, купивший **ApiKey**, разрабатывает своё клиентское (мобильное, десктопное или js). приложение и не хочет публиковать свой **ApiKey** на клиентской стороне. Смотри подробнее раздел “[Разработка сторонних клиентских приложений](Разработка%20сторонних%20клиентский%20приложений.docx)”. | string |
| UserLogin | Логин пользователя. Используется для аутентификации по пользователю и паролю стороннего клиентского приложения. | string |
| UserPassword | Пароль пользователя. Используется для аутентификации по пользователю и паролю стороннего клиентского приложения. | string |
| SessionKey | Идентификатор временной сессии. Альтернатива использования **AppKey** на клиентской стороне. Используя **ApiKey** или **AppUser** авторизацию, клиент получает временный сессионный ключ, который может быть использован только для данного сеанса определённое время. Компрометация этого ключа не несёт угрозе безопасности, так как он действителен непродолжительное время и только для этого сеанса. | string |
| ClientId | Уникальный идентификатор конкретного экземпляра клиентского приложения. Может генерироваться при старте этого приложения. Никак не влияет на аутентификацию, но важен для оптимизации процесса передачи уведомлений между экземплярами клиентских приложений. | string |