Новый способ авторизации в Wialon

До последнего времени в продуктах Wialon Hosting (Local) применялся не самый безопасный механизм авторизации пользователей. В связи с этим мы провели довольно кропотливую работу по реализации современного более защищённого механизма авторизации по принципу oAuth. Старый способ авторизации (логина) просуществует до **1 октября 2015**. Поэтому клиентам (партнёрам), которые реализовали свои формы входа на сайт мониторинга или использовали ссылки для демо-логина, нужно будет перейти на новый механизм авторизации.

В чём заключается наша реализации oAuth?

1. В целях безопасности форма авторизации для входа на сайты Wialon может использоваться только с доверенных DNS, т.е. только с DNS, которые ведут на *.wialon.com. Иными словами, авторизоваться можно только при помощи формы, которая находится сервере Wialon.

2. В результате авторизации (успешного ввода логина и пароля) на сервере генерируется ключ (токен) и сохраняется в пользователе. По этому токену можно в дальнейшем входить на сайты, использовать в приложениях, а также передавать третьим лицам (если он создан с ограниченными правами).

3. У токена имеются различные свойства: время активации, срок действия, доступные права, название и др. При необходимости можно ограничить срок действия токена и права. По умолчанию срок действия токена 30 дней и права соответствуют правам пользователя.

4. Все созданные токены пользователя можно увидеть, например, в интерфейсе мониторинга: меню пользователя =>Управление приложениями => Авторизованные приложения. Также там выводятся права токенов. Из этого же диалога можно удалить ненужные токены.

5. Просроченные токены удаляются автоматически. Также токены удаляются, если не использовались более 100 дней. В этом случае потребуется снова ввести логин и пароль для получения нового токена.

6. У одного пользователя может одновременно существовать не более 1000 токенов.

7. При входе на сайт по токену учитываются права пользователя и права токена. Т.е. права токена могут только уменьшить права пользователя или оставить неизменными.

Для удобства Вы можете использовать нашу форму авторизации на своих сайтах и в приложениях. На данный момент существует два варианта формы: **расширенная** и **упрощённая**.

Расширенная форма авторизации

Расширенная форма (http://hosting.wialon.com/login.html) в большей степени предназначена для мобильных и иных приложений. Сверху расположен логотип (берётся из «скина» клиента), ниже — поля ввода логина и пароля и кнопка авторизации. В расширенной форме также имеется блок с перечислением доступных прав и их описанием.

В форму можно передать ряд **дополнительных параметров**, например: http://hosting.wialon.com/login.html?client_id=wialon&access_type=0x100&activation_time=0&duration=0&lang=en&flags=0x1&user=user, где:

- client_id — название приложения/сайта/клиента, для которого сгенерировать токен;
- access_type — уровень прав токена (-1 или 0xffff — полные права, 0x100 — только слежение; см. полный список в Приложении);
- activation_time — время активации токена (время UTC в секундах, 0 — сейчас, также можно задать активацию в будущем);
- duration — время жизни токена (в секундах);
- lang — язык (en, ru, ...);
- flags — флаги (0x1 — возвращать в ответе имя пользователя);
- user — имя пользователя (подставится в поле логина);
- redirect_uri — URL, на который переадресовать страницу и передать результаты авторизации.

Все эти параметры **не обязательные**, но многие из них примут значения **по умолчанию**:

- client_id — названия сайта (title);
- access_type — 0x100;
- activation_time — 0 (т.е. сейчас);
- duration — 2592000 (30 дней в секундах);
- flags — 0;

- redirect_uri — сама форма login.html.

В результате **успешной авторизации** по данной форме произойдёт переадресация на redirect_uri и будут переданы следующие GET-параметры:

- access_token — 72-значный токен, который можно сохранить и использовать для авторизации в дальнейшем;
- user_name — имя авторизованного пользователя (если при генерации токена был передан флаг 0x1).

В случае **ошибки** авторизации произойдёт переадресация на форму логина, выведется соответствующая ошибка и будут переданы следующие GET-параметры:

- svc_error — код ошибки;
- client_id;
- access_type;
- activation_time;
- duration;
- flags.

После успешного получения 72-значного токена его можно использовать в своих приложениях для авторизации одним из способов:

1. вызов SDK-метода wialon.core.Session.getInstance().loginToken: function(token, operateAs, callback), где:
    - token — полученный 72-значный access_token;
    - operateAs — имя пользователя, от имени которого нужно залогиниться (можно задать пустым);
    - callback — функция, которую выполнить после авторизации.
2. запрос remote_api http://hst-api.wialon.com/wialon/ajax.html?svc=token/login&sid=<your_sid>&token=<access_token>&operateAs=<optional_sub_user>

Упрощенная форма авторизации

Упрощённая форма (http://hosting.wialon.com/login_simple.html) предназначена для простого встраивания на сайты (сайты-визитки) через iframe (пример: http://sdk.wialon.com/playground/demo/token_simple_form) и дальнейшего быстрого перехода на один или несколько своих сайтов мониторинга после авторизации. Сверху расположен логотип (берётся из скина клиента), ниже — поля ввода логина и пароля и кнопка авторизации.

Эта форма призвана заменить самодельные формы авторизации на сайтах партнёров. Её плюсом является небольшой размер, отсутствие каких-либо замысловатых параметров и необходимости после авторизации самостоятельно вызывать запросы по входу на сайт. После успешной авторизации будет отображена страница с именем авторизованного пользователя и списком сайтов в виде ссылок, куда автоматом будет подставлен полученный токен. При переходе по ссылке в новой вкладке браузера сразу откроется сайт мониторинга. Авторизовавшись в этой форме один раз, полученный токен будет сохранён в браузере для дальнейшего использования. Т.е. при следующих переходах на сайт, где встроена эта форма, будет отображаться авторизованный пользователь и сайты, куда можно перейти.

Токен создаётся со сроком жизни 30 дней, права пользователя никак дополнительно **не ограничены**.

В форму также можно передать ряд **необязательных** параметров, например: http://hosting.wialon.com/login_simple.html?lang=ru&cms_url=http://cms.wialon.com&cms_title=CMS&lite_url=http://lite.wialon.com&mobile_url=http://m.wialon.com&demo_title=Try&demo_url=http://hosting.wialon.com/?token=86b4f6a78d664b3ee665983eba3e54fc5DCA0BDE4E17F1A45ACCF93B537ABFCE0A603653&title=Monitoring&css_url=http://my.dns.com/my.css, где:

- lang — язык (en, ru, ...);
- cms_url — URL к сайту CMS Manager (например, http://cms.wialon.com; если задан — будет добавлен в список сайтов для быстрого перехода);
- cms_title — название, которое вывести в ссылке;
- lite_url — URL к сайту Wialon Hosting Lite (например, http://lite.wialon.com; если задан — будет добавлен в список сайтов);
- lite_title — название, которое вывести в ссылке;
- mobile_url — URL к сайту Wialon Mobile (например, http://m.wialon.com; если задан — будет добавлен в список сайтов);

- mobile_title — название, которое вывести в ссылке;
- title — название сайта мониторинга, которое вывести в ссылке;
- demo_url — URL для демо-логина (например, http://hosting.wialon.com/?token=86b4f6a78d664b3ee665983eba3e54fc5DCA0BDE4E17F1A45ACCF93B537ABFCE0A603653);
- demo_title — название для ссылки демо-логина;
- css_url — URL к CSS-файлу с произвольными стилями для формы.

Ссылка для демо-логина (если задана через переменную demo_url) добавится на форму авторизации ниже кнопки “Войти”. Эта ссылка должна иметь указанный выше формат. **Создать** такую ссылку можно при помощи этой же формы. Предварительно нужно создать пользователя с ограниченным доступом и возможностями на сайте мониторинга или CMS Manager. Далее авторизоваться им через эту форму. На результирующей странице скопировать адрес полученной ссылки (не логинясь по ней на сайт). Затем нажать стрелку для выхода. Добавить этот адрес в login_simple.html параметром demo_url.

Чтобы встроить на свой сайт упрощённую форму авторизации, достаточно в нужную область сайта добавить HTML-код:

```
<iframe src="http://hosting.wialon.com/login_simple.html?lang=ru" scrolling="no"
style="width: 230px; height: 290px; border: 0; margin: 10px;">
```

Тем партнёрам, у кого на сайтах присутствует своя форма авторизации для мониторинга, нужно заменить её на указанный iframe. Тем партнёрам, у кого на сайте присутствует только ссылка на демо-логин нужно сгенерировать новую ссылку для демо-логина с токеном и заменить на сайте.

Примеры использования форм на PlayGround

- http://sdk.wialon.com/playground/demo/token_simple_form
- http://sdk.wialon.com/playground/demo/advanced_form
- http://sdk.wialon.com/playground/demo/app_auth_token

Приложение: Флаги прав доступа с расшифровкой

0x100 — Слежение онлайн

- Просмотр элемента и его основных свойств
- Просмотр подробных свойств
- Просмотр произвольных полей
- Запрос сообщений и отчетов
- Просмотр и скачивание файлов
- Просмотр POI
- Просмотр геозон
- Просмотр шаблонов отчетов
- Просмотр водителей
- Просмотр элементов агро
- Просмотр прицепов
- Экспорт сообщений
- Просмотр команд

0x200 — Просмотр данных

- Действовать от имени этого пользователя
- Просмотр уведомлений
- Просмотр заданий
- Просмотр интервалов техобслуживания

0x400 — Редактирование малозначительных данных

- Переименование элемента
- Управление произвольными полями
- Редактирование не упомянутых свойств
- Изменение иконки
- Загрузка и удаление файлов
- Создание, редактирование и удаление POI
- Создание, редактирование и удаление геозон
- Регистрация и удаление обработок
- Управление событиями
- Создание, редактирование и удаление команд

0x800 — Редактирование важных данных

- Управление доступом к элементу

- Управлять правами доступа пользователя
- Изменять флаги пользователя
- Создание, редактирование и удаление уведомлений
- Создание, редактирование и удаление заданий
- Создание, редактирование и удаление шаблонов отчетов
- Создание, редактирование и удаление водителей
- Редактирование элементов агро
- Создание, редактирование и удаление прицепов
- Запуск и остановка ретранслятора, редактирование его свойств
- Редактирование свойств маршрута
- Создание, редактирование и удаление интервалов техобслуживания
- Изменение детектора поездок и расхода топлива

0x1000 — Редактирование критических данных

- Удаление элемента
- Управление журналом
- Просмотр административных полей
- Управление административными полями
- Редактирование настроек подключения (тип устройства, уникальный ID, телефон, пароль доступа, фильтрация сообщений)
- Создание, редактирование и удаление датчиков
- Редактирование счетчиков
- Удаление сообщений
- Импорт сообщений

0x2000 — Выполнение команд

- Выполнение команд

-1 — Неограниченный доступ.