

Вход в виджеты amoCRM

Для разработчиков виджетов. Подробности устройства — в README репозитория `Buharestskie/widget_auth`.

Зачем отдельный сервис

Виджет живёт внутри интерфейса amoCRM и своему бэкенду может предъявить только одно — токен `X-Auth-Token`, который amoCRM подписывает секретным ключом интеграции. Если проверять этот токен в каждом бэкенде, секрет интеграции окажется во всех виджетах сразу, и утечка из любого из них откроет все.

Поэтому секрет хранится в одном месте — в сервисе `widget_auth` на `https://widget-auth.donula26.ru`. Он проверяет токен amoCRM и выдаёт взамен свой, короткоживущий, подписанный отдельным секретом конкретного бэкенда. Бэкенд виджета секрета интеграции не видит никогда.

Сейчас так входят «Файлы сделки на Яндекс.Диске», чек-листы и шаблоны сообщений.

Как это выглядит со стороны виджета

1. Виджет вызывает обмен через `$authorizedAjax` — amoCRM сама подставит `X-Auth-Token`:

```
self.$authorizedAjax({
  url: 'https://widget-auth.donula26.ru/api/auth/exchange',
  method: 'POST'
}).done(function (response) {
  // response.access_token, response.expires_in (600 секунд)
});
```

2. Полученный `access_token` виджет передаёт своему бэкенду в заголовке `Authorization: Bearer <access_token>`.

3. Через 10 минут токен истекает — бэкенд ответит `401`, и виджет должен заново получить токен.

Как бэкенд проверяет токен

Токен — JWT, алгоритм HS256. Проверять обязательно все четыре вещи:

Что	Чем
Подпись	<code>ACCESS_TOKEN_SECRET</code> — свой у каждого бэкенда
Аудитория <code>aud</code>	<code>ACCESS_TOKEN_AUDIENCE</code> — своя у каждого бэкенда, например <code>yandex-widget-backend</code>
Издатель <code>iss</code>	<code>ACCESS_TOKEN_ISSUER=amocrm-widget-auth-service</code> — общий
Срок <code>exp</code> , <code>nbf</code>	Библиотека JWT проверяет сама; допуск на расхождение часов — несколько секунд

```
payload = jwt.decode(token, ACCESS_TOKEN_SECRET, algorithms=["HS256"],
                      audience=ACCESS_TOKEN_AUDIENCE, issuer=ACCESS_TOKEN_ISSUER, leeway=5)
```

Кто пришёл — в полях `account_id` и `user_id` (то же в `sub` как `"account_id:user_id"`). Это id пользователя amoCRM — по нему и решайте, что ему можно.

Не пропускайте проверку `aud`: именно она не даёт токену одного виджета пройти в бэкенд другого.

Подключить новый виджет

Делает администратор, у которого есть доступ к серверу:

1. В настройках интеграции amoCRM взять её ID (`client_uuid`) и секретный ключ.
2. Добавить виджет в список `widget_auth`: ID и секрет интеграции, новый случайный секрет бэкенда (от 32 символов) и уникальную аудиторию для него. Перезапустить сервис — список читается только при старте.
3. В настройки бэкенда виджета вписать тот же секрет бэкенда, ту же аудиторию и общий издатель.

Порядок команд и формат записи — в README репозитория, раздел «Подключить новый виджет».

Если вход не работает

Ответ	Что проверить
401 Missing X-Auth-Token от widget_auth	Запрос идёт не через <code>\$authorizedAjax</code> , а обычным <code>\$.ajax</code> или <code>fetch</code> — amoCRM подставляет токен только в первом случае
401 Invalid X-Auth-Token от widget_auth	Виджета нет в списке, неверный секрет интеграции или не совпала аудитория входящего токена. Обычно ошибка в только что добавленной записи
401 от своего бэкенда	Токен истёк (прошло больше 10 минут) или секрет / аудитория в бэкенде не совпадают с записью в widget_auth
Ошибка CORS в консоли браузера	Виджет открыт не в нашем аккаунте amoCRM — обмен разрешён только со страниц <code>donula.amocrm.ru</code>

Версия #1
Admin создал 2026-09-24 10:34:48 UTC
Admin обновил 2026-09-24 10:34:48 UTC