

Создание приложений с SSO-аутентификацией через ADVANTA

Оглавление

Что такое SSO	3
Порядок SSO-аутентификации в ADVANTA	3
Регистрация идентификаторов приложений в ADVANTA	4
Особенности передачи токена для приложений и веб-сервисов	4
Удаленная передача токена	4
Локальная передача токена	5
Примеры использования SSO-авторизации в приложениях	6
Пример приложения с локальной передачей токена	7
Процесс работы примера	8
Описание исходного кода примера	11
Пример приложения с удалённой передачей токена	12
Процесс работы примера	13
Описание исходного кода примера	17

Single Sign-On (SSO) – это метод получения доступа, который позволяет пользователям с помощью одной учётной записи входить в разные приложения, связанные с единым сервером авторизации. Этот сервер управляет проверкой учетных данных и автоматически выдает связанным с ним приложениям токены доступа.

Система ADVANTA может являться сервером SSO-аутентификации начиная с версии 3.29. Создание и хранение учётных записей может производиться, как в собственной базе данных ADVANTA, так и в специализированной внешней системе, например, <u>Active Directory</u>, <u>Blitz</u> <u>Identity Provider</u> и подобных.

Порядок SSO-аутентификации в ADVANTA



Диаграмма последовательности действий при SSO-аутентификации:

Последовательность действий при SSO-аутентификации:

1. Пользователь инициирует процесс авторизации в клиентском приложении.

2. Приложение формирует ссылку на страницу авторизации ADVANTA. Ссылка содержит два параметра:

- идентификатор приложения;
- URL-адрес для отправки токена.

3. Приложение либо автоматически переадресует пользователя на страницу авторизации в браузере, либо предлагает ему перейти по созданной ссылке самостоятельно.

4. При входе пользователя на страницу авторизации в браузере, ADVANTA проверяет, авторизован ли он:

• если пользователь недавно уже выполнял авторизацию на этом сервере, ADVANTA автоматически применяет его учётные данные;

• если пользователь не был авторизован – просит его ввести логин и пароль.

5. ADVANTA проверяет зарегистрирован ли идентификатор приложения на этом стенде.

6. Если все проверки прошли успешно, ADVANTA отправляет токен аутентификации AspNetSessionId приложению на указанный URL-адрес.

7. Приложение, получив токен, использует его для выполнения запросов к APIфункциям ADVANTA с уровнем доступа авторизовавшегося пользователя.

Перечень АРІ-функций, в которых можно использовать токен (в качестве идентификатора AspNetSessionId), можно найти на странице Wiki «Описание методов API».

Регистрация идентификаторов приложений в ADVANTA

Для каждого Приложения, в котором будет использован механизм SSO-авторизации, в конфигурационном файле ADVANTA client.config должен быть зарегистрирован идентификатор. Он вводится в параметре AllowedExternalApplicationClientIds. Если предполагается использовать SSO-авторизацию в нескольких приложениях, их идентификаторы указываются в этом параметре через точку с запятой.

В примере ниже будет использован идентификатор AuthDemold. В конфигурационном файле он может выглядеть, например, так:

<add key="AllowedExternalApplicationClientIds" value="application1;AuthDemoId;application3"/>

Особенности передачи токена для приложений и веб-сервисов

В случае успешной авторизации пользователя, ADVANTA возвращает информационной системе токен доступа на адрес, указанный в параметре <u>ReturnUrl</u>. Инициатором передачи является именно система аутентификации.

В зависимости от типа информационной системы, принимающей токен, возможны два способа передачи:

- удаленно через вызов АРІ-функции приложения;
- локально через localhost.

Удаленная передача токена

Если информационная система является веб-приложением, она должна предоставить для приёма токена API-функцию, вызов которой возможен через Интернет. В случае успешной аутентификации, сервер системы ADVANTA выполнит запрос этой API-функции, отправив ей сообщение методом POST. В теле сообщения он передаст в формате JSON токен доступа (в параметре tokenValue) или текст ошибки (в параметре errorMessage). Пример сообщения:

```
POST
{
    "tokenValue":"...",
    "errorMessage":"..."
}
```

Пример ссылки переадресации пользователя при удалённой передаче токена:

https://advantaservername.ru/Pages/Login.aspx?ClientId=AuthDemoId&ReturnUrl=https://clientservername.ru/api/v1/authcallback/

где:

- https://advantaservername.ru сервер ADVANTA, выполняющий аутентификацию;
- /Pages/Login.aspx? стандартный путь к странице авторизации ADVANTA;

• AuthDemoId – идентификатор клиентского приложения, зарегистрированный в файле client.config;

 https://clientservername.ru – сервер клиентской информационной системы, принимающей токен;

• /api/v1/authcallback/ — путь к API-функции на сервере клиентского приложения, которая получит и обработает токен доступа.

Локальная передача токена

Примечание: Способ локальной передачи токена доступен начиная с версии ADVANTA 3.30.

Если авторизация выполняется в обычной программе на компьютере пользователя, токен передаётся путём Get-запроса на локальный сетевой адрес localhost. Удалённый вызов API-функции приложения обычно невозможен из-за ограниченных прав пользователя, настроек брандмауэра или сетевой архитектуры. Передачу сообщения с токеном в этом случае выполняет страница авторизации, открытая пользователем в браузере.

Для реализации данного способа приложение должно включить в переменную ReturnUrl adpec localhost или «127.0.0.1», а также номер порта. До переадресации пользователя на страницу авторизации ADVANTA программе необходимо начать «прослушивание» указанного порта.

Пример ссылки для получения токена через localhost:

https://advantaservername.ru/Pages/Login.aspx?ClientId=AuthDemoId&ReturnUrl=http://local host:5000/

где:

https://advantaservername.ru – сервер ADVANTA, выполняющий проверку учётной записи;

• /Pages/Login.aspx? – стандартный путь к странице авторизации ADVANTA;

• AuthDemoId – идентификатор клиентского приложения, зарегистрированный в файле client.config;

• http://localhost:5000/ – адрес localhost и номер порта, на который будет отправлен запрос с токеном. Порт лучше выбрать в диапазоне от 1024 до 49151. На прослушивание портов в этом диапазоне права администратора пользователю обычно не требуются.

В случае успешной аутентификации страница авторизации отправит токен в запросе, в параметре «token = ...»:

←	\rightarrow	C	O A https://pr	mo.a2	nta.ru/p	ages/Login	.aspx?Client	Id=AuthDemoId	&ReturnUrl=	http%3	A%2F%	2Floc	alhosť	%3A50	000
							A D V	A N T-A							
				В	ход в с	истему									
				И	мя поль	зователя									
					admin										
				п	ароль										
					•••••										
					Запо	омнить ме	ня		Забыли пар	оль?					
						Токен авто	ризации усг http://loca	пешно передан на alhost:5000	а адрес						
							Bc	йти							
							Зарегистр	оироваться							
R	φи	нспектој	р ▷ Консоль		тладчик	↑↓ Сеть	{} Стили	🞧 Профайлер	🕼 Память	🖯 Xp	анилиц	4e 🕇	г Поди	ержка	досту
Û	∀По	иск URL									11	+ 0	0	Bce	нтм
Статус	Me	тод	Домен	Φί	айл						Иници	атор			
200	GET	r	🔒 pmo.a2nta.ru	i Lo	gin.aspx?	'ClientId=Au	thDemoldℜ	turnUrl=http://locall	host:5000		docum	ent			
200	GET	r	localhost:500	0 /?	token=ey	JhbGciOiJlUz	11NilsInR5cCl6	ikpXVCJ9.eyJodHRw	Oi8vc2NoZW1h	cy54bWx	Login.	aspx:14	<u>6</u> (fetch)	

Примеры использования SSO-авторизации в приложениях

SSO-авторизация с передачей токена через API-функцию используется, например, в чатботах, создаваемых для работы с ADVANTA через мессенджеры. При первом подключении пользователя к такому чат-боту он выведет пользователю сообщение с просьбой перейти на страницу авторизации ADVANTA. Оно может выглядеть так:

AO a2 office		-	Q	:
Для начала работы требуется войти в А	dvanta ₁	6:03		
Для начала работы требуется войти в А Войти 16:03	dvanta ₁	6:03	•	

Ссылка «Войти» содержит параметры ClientId и ReturnUrl, как указано выше.

API-функция, указанная в параметре ReturnUrl, должна быть реализована в серверной части чат-бота.

Локальная SSO-авторизация, через localhost, реализована в <u>модуле импорта составов</u> <u>проектов из Microsoft Project</u>. Если он установлен на компьютере пользователя, в окне MS Project, на закладке «Надстройки» появляются кнопки для обмена данными с ADVANTA. В диалоге «Подключение к службе», который появляется при нажатии кнопки «Выгрузить в Адванту», есть кнопка «Войти через браузер». По нажатию этой кнопки происходит переадресация пользователя на страницу SSO-авторизации ADVANTA. После авторизации токен доступа передаётся модулю обмена данными через localhost.

Выгру	зить в Адванту	🖶 [v2.4.0.0] Подключе	ение к службе			×	Сохран	ить настройки							
	\searrow	Адрес http://pmo.a2	hta.ru	2	Ô		🔺 В	ход в систему	×	+				-	×
A		Порт 8887 Ве	ойти через браузер	÷	С	ŵ	Ć	https://pmo 🖉	☆		۵	• •		(3 (≦	 ٠
BPEMEHH	Начало 3 Ср 01.01.25 С,	Показывать лог							A D V	A N T	Ā				Í
	 Режик задачи • 	Название задачи	👻 Длительнс 👻					Вход в систему							
1		⊿ Проект2	30 дней	C	~										
2	×	Задача1	10 дней 20 лной	c				Имя пользователя							
4	→ \$	Задача2	5 дней	Г				admin							
5	*	Задача4	5 дней	r											
								Пароль							
								•••••							
								💙 Запомнить меня				Забыли пар	оль?		
HTA				-				Токен автори	изации у http://lo	спешно п calhost:88	ередан на 887	адрес	>		
AMA FA				-					E	Войти					
диаграл									Зарегист	трироват	ъся				
				_				3.29.5 © Ад Система управл	388.15018 ванта Кон тения про	3-9baedad 3 нсалтинг 20 ектами и б	SQL Server 004-2025 і́изнесом «А	Адванта»			

Пример приложения с локальной передачей токена

В прилагаемом архиве «A2-SSO-Demo.zip» приведён исходный код консольного приложения на языке C#, которое демонстрирует работу SSO-аутентификации в ADVANTA. Код создан в бесплатной среде разработки Visual Studio Code. Для его запуска требуется, чтобы на ПК был установлен набор библиотек «.net SDK» версии не ниже 8.

Найти ссылку на загрузку .net SDK можно на сайте Microsoft: <u>https://dotnet.microsoft.com/ru-ru/download/dotnet</u>.

Visual Studio Code – бесплатный кроссплатформенный редактор кода, созданный Microsoft. Существуют версии для Windows, Linux и MacOS. Скачать можно с официального сайта: <u>https://code.visualstudio.com</u>.

Архив приложения «A2-SSO-Demo.zip» нужно скачать, распаковать и поместить содержащуюся в нём папку «A2-SSO-Demo», например, в каталог «C:\Projects».

Процесс работы примера

Прежде, чем запускать приложение, откройте в браузере страницу демонстрационного стенда ADVANTA: <u>http://pmo.a2nta.ru</u>. Нужно убедиться, что он доступен из вашего сетевого окружения.

Запустите файл «A2-SSO-Demo.exe» из каталога «C:\Projects\A2-SSO-Demo\bin\Release\net8.0\publish».



Появится консоль Windows с предложением нажать ENTER для автоматического перехода на страницу SSO-авторизации ADVANTA на демонстрационном стенде <u>http://pmo.a2nta.ru</u>.



После нажатия ENTER, программа запустит браузер и откроет страницу авторизации по адресу https://pmo.a2nta.ru/pages/Login.aspx с двумя параметрами:

- ClientId = AuthDemoId;
- ReturnUrl = http%3A%2F%2Flocalhost%3A5000.

Где:

• <u>ClientId</u> – идентификатор приложения, зарегистрированного в файле <u>client.config</u> на сервере ADVANTA, в строке <u>AllowedExternalApplicationClientIds</u>;

• <u>ReturnUrl</u> – адрес, на который страница авторизации должна будет переслать токен авторизации в случае успешного ввода логина и пароля пользователем на странице ADVANTA.

В консоли приложения появятся сообщение о переходе по ссылке и о начале прослушивания порта 5000 в ожидании сообщения с токеном.



Если к моменту запуска браузера Вы уже были авторизованы на стенде <u>https://pmo.a2nta.ru</u>, то страница авторизации сразу же получит токен доступа и отправит на adpec http://localhost:5000. При этом появится сообщение, что «Токен авторизации успешно передан...».

•	Ô		🔺 Bxo	од в систему	×	+			
\leftarrow	С	ର	ð	https://pm	o.a2nta.ru/pages/Lo	ogin.aspx?Clientl	d=AuthDemoId&Return	Url=http%3A9	%2F%2Flocalhost%3A500
						🕂 D V	ANTA		
					Вход в сист	ему			
					Имя пользова	ателя			
					Воронов				
					Пароль				
					🗹 Запомни	ть меня	386	ыли пароль?	
					Токе	н авторизации у http://lo	спешно передан на адр calhost:5000	Dec	
						E	Зойти		
						Зарегис	трироваться		

Если Вы ранее не были авторизованы на этом стенде, потребуется ввести логин и пароль, после чего токен будет отправлен и появится сообщение об успешной отправке.

Переданный приложению токен будет выведен в консоль:

🖾 C:\Projects\A2-SSO-Demo\bir 🗙 🕂

Получено сообщение от страницы авторизации (время: 31.01.2025 12:47:30)

Токен доступа:

eyJhbGciOiJIUzIINIISInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2 NsYWltcy9uYW1laWRlbnRpZmllciI6IjdkOGU5YTAxLTk5MjEtNDliNi1hYTczLWRlM2M0ZmE2YjRmZCIsImh0dHA6Ly9zY2hlbWFzL nhtbHNvYXAub3JnL3dzLzIwMDUvMDUvaWRlbnRpdHkvY2xhaW1zL25hbWUiOiLQktC-0YDQvtC90L7QsiIsImh0dHA6Ly9hMm50YS5y dS9pZGVudGl0eS9jbGFpbXMvaW5kZXgiOiIyNyIsImh0dHA6Ly9zY2hlbWFzLm1pY3Jvc29mdC5jb20vd3MvMjAwOC8wNi9pZGVudGl 0eS9jbGFpbXMvcm9sZSI6WyJVc2VyIiwiQWRtaW5pc3RyYXRvciJdLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1zL2xpY2 VuY2VDb2RlIjoiRXhlY3V0b3IiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1zL3BlcnNvbklkIjoiNGE5ZjlmZDUtMTVhN i00NGFkLThlM2QtZDVlNjdjYzc5NjNhIiwiaHR0cDovL3NjaGVtYXMueGlsc29hcC5vcmcvd3MvMjAwNS8wNS9pZGVudGl0eS9jbGFp bXMvZ2l2ZW5uYW1lIjoi0J7Qu9C10LMiLCJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWL tcy9zdXJuYW1lIjoi0JQvtGA0L7QvdC-0LIiLCJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2 NsYWltcy9lbWFpbGFkZHJlc3Mi0iJwcm90b2FkbWluQGFkdmFudGEtz3JvdXAucnUiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1z L3Bob3RvSQQi0iJhZjQ1MDEwZS1jMjhLTRjZTMtOWRkOC02ZDU4ZGU4NjhmMTMiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1z L3Bob3RvSQQi0iJhZjQ1MDEwZS1jMjhkLTRjZTMtOWRkOC02DU4ZGU4NjhmMTMiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1z L3Bob3RvSQQi0iJhZjQ1MDEwZS1jMjhkLTRjZTMtOWRkOC02DU4ZGU4NjhmMTMiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2xhaW1z L3Bob3RvSQQi0iJhZjQ1MDEwZS1jMjhkLTRjZTMt0WRkOC02DU4ZGU4NjhmMTMiLCJodHRwOi8vYTJudGEucnUvaWRlbnRpdHkvY2x hwIjoxNzM4NDA2ODUwLCJpc3Mi0iJBZHZhbnRhIiwiYXVkIjoiR2VuZXJpY0NsaWVudCJ9.hwExWkkdj30RD3ydB_IpcRpAR5HxHE86 9iEJLr32XFQ

В момент получения токена доступа демонстрационное приложение вызывает две APIфункции ADVANTA. Функция <u>WhoAmI</u> предоставит информацию о пользователе, токен которого получило приложение. Функция <u>GetProject</u> – информацию о тестовом проекте «<u>Организация</u> мобильной VPN» (UID «a6ed1995-582c-42d3-afa0-6db8c280b212»).

В консоль будет выведена информация о пользователе, которому выдан токен, а также – итог запроса данных о проекте. Если учётная запись, под которой вы прошли авторизацию на стенде <u>https://pmo.a2nta.ru</u>, обладает правами на просмотр проекта «<u>Opraнизация мобильной</u> <u>VPN</u>», то приложение сможет получить его описание в формате XML.

🗟 C:\Projects\A2-SSO-Demo\bir \times + \vee

Пробуем загрузить данные о пользователе через АРІ-функцию WhoAmI...

Результат SOAP-запроса WhoAmI:

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelo pe/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" ><soap:Body><WhoAmIResponse xmlns="http://streamline/"><WhoAmIResult><Id>4a9f9fd5-15a6-44ad-8e34-d5e67c c7963a</Id><PrincipalId>7d8e9a01-9921-49b6-aa73-de3c4fa6b4fd</PrincipalId><IsAdmin>true</IsAdmin><FullN ame>Bopoнob Oner</FullName><LicenseCode>Executor</LicenseCode></WhoAmIResult></WhoAmIResult></whoAmIResponse></soap:Bo dy></soap:Envelope>

Пробуем загрузить данные о проекте с помощью полученного токена, через АРІ-функцию GetProject...

Результат SOAP-запроса GetProject:

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelo pe/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" ><soap:Body><GetProjectResponse xmlns="http://streamline/"><GetProjectResult><UID>a6ed1995-582c-42d3-af a0-6db8c280b212</UID><ParentProjectId>27b97e72-5ffb-48bf-a405-bad7625eecc7</ParentProjectId><Name>OpraH изация мобильной VPN</Name><ProjectTypeId>d46b6deb-eeae-4ca8-9c32-ab77f979a8d8</ProjectTypeId><ProjectT ype>Npoext цифровизации</ProjectType><Status>3</Status><PercentComplete>57</PercentComplete><SystemStar tDate>2023-09-04T08:00:00</SystemStartDate><SystemEndDate>2025-06-02T09:02:24</SystemEndDate><PlannedSt artDate>2023-09-04T08:00:00</PlannedStartDate><PlannedEndDate xsi:nil="true" /><ActualStartDate>2018-11 -02T08:00:00</ActualStartDate><ActualEndDate xsi:nil="true" /><CatualStartDate>2018-11 59-b60a-28a03d40077f</OwnerId><ResponsibleId>4a9f9fd5-15a6-44ad-8e34-d5e67cc7963a</ResponsibleId><Resou rceAssignments /><UsePlannedCost>false</UsePlannedCost<PlannedCost xsi:nil="true" /><CalculatedCost>19 52</CalculatedCost><PlannedDuration>0/PlannedDuration>CurationUnit>DAYS</DurationUnit>StartDateConst raint>MUST_START_ON</StartDateConstraint><CalendarId>e7a48497-ae6e-4c25-be82-15bac256d1ff</CalendarId>

Ожидаем следующего сообщения с токеном.

Если прав доступа к проекту будет недостаточно, вместо информации о нём появится сообщение об ошибке.

К примеру, на странице SSO-авторизации можно сменить учётную запись на «Шилкова» (пароль «123456»). В этом случае API <u>WhoAml</u> будет выполнена успешно, поскольку у каждого пользователя есть доступ к информации о себе. При этом API-функция <u>GetProject</u> вместо

сведений о про	екте получит	сообщение	о недостато	очном	уровне	доступа	, посколь	ку у
пользователя	«Шилкова»	доступа	именно	к	указанно	му пр	роекту	нет.
Пробуем загрузить д	анные о пользовате	еле через API-с	функцию WhoAmI					
Результат SOAP-запр xml version="1.0"<br lope/" xmlns:xsi="h ema"> <soap:body><wh 81329364cc8a<p in><fullname>Шилков se></fullname></p </wh </soap:body> <th>boca WhoAmI: 'encoding="utf-8"? ttp://www.w3.org/2 oAmIResponse xmlns rincipalId>74be20c а Элина ap:Envelope></th> <th>2><soap:envelop 001/XMLSchema- ="http://strea 0-c537-4e65-89 <licensecode>8</licensecode></soap:envelop </th> <th>be xmlns:soap= -instance" xml amline/"><whoan 936-d3ca529d9ad Executor<th>"http:/ ns:xsd= mIResul 08nseCode</th><th>/schemas.xm "http://www t><id>3c254 ncipalId><i ><th>lsoap.org/ .w3.org/2 cd1-d389-/ sAdmin>fa sult><th>/soap/enve 001/XMLSch 4fd9-bbe1- lseoAmIRespon</th><td></td></th></i </id></th></whoan </th>	boca WhoAmI: 'encoding="utf-8"? ttp://www.w3.org/2 oAmIResponse xmlns rincipalId>74be20c а Элина ap:Envelope>	2> <soap:envelop 001/XMLSchema- ="http://strea 0-c537-4e65-89 <licensecode>8</licensecode></soap:envelop 	be xmlns:soap= -instance" xml amline/"> <whoan 936-d3ca529d9ad Executor<th>"http:/ ns:xsd= mIResul 08nseCode</th><th>/schemas.xm "http://www t><id>3c254 ncipalId><i ><th>lsoap.org/ .w3.org/2 cd1-d389-/ sAdmin>fa sult><th>/soap/enve 001/XMLSch 4fd9-bbe1- lseoAmIRespon</th><td></td></th></i </id></th></whoan 	"http:/ ns:xsd= mIResul 08nseCode	/schemas.xm "http://www t> <id>3c254 ncipalId><i ><th>lsoap.org/ .w3.org/2 cd1-d389-/ sAdmin>fa sult><th>/soap/enve 001/XMLSch 4fd9-bbe1- lseoAmIRespon</th><td></td></th></i </id>	lsoap.org/ .w3.org/2 cd1-d389-/ sAdmin>fa sult> <th>/soap/enve 001/XMLSch 4fd9-bbe1- lseoAmIRespon</th> <td></td>	/soap/enve 001/XMLSch 4fd9-bbe1- lseoAmIRespon	
Пробуем загрузить д	анные о проекте с	помощью получе	енного токена,	через	АРІ-функцию	GetProje	ct	
езультат SOAP-запроса GetProject: ?xml version="1.0" encoding="utf-8"?> <soap:envelope xmlns:soap="http://schemas.xmlsoap.org/soap/enve
ope/" xmlns:xsd="http://www.w3.org/2001/XMLSch
ma" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><soap:body><soap:fault><faultcode>soap:Server</faultcode><faultstring>System.Web.Services.Protoc ls.SoapException: CepBepy не удалось oбработать запрос> System.Exception: У Вас нет прав на pocMorp проекта в SL.components.Services.APIProjects.GetProject(ProjectIdDataContract contract) в D:\jenkins\works wace\AdvantaBuild_Commit_OnDemand_ByAgent1\SL\components\Services\APIProjects.asmx.cs:строка 690 Конец трассировки внутреннего стека исключений</faultstring></soap:fault></soap:body></soap:envelope>								
Body> <th>je></th> <th></th> <th>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</th> <th></th> <th></th> <th>,</th> <th></th> <td>1</td>	je>		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			,		1
Ожидаем следующего	сообщения с токенс	м.						

Описание исходного кода примера

Рассмотрим основные моменты исходного кода примера.

Запустите Visual Studio Code и откройте каталог с кодом программы командой «File > Open Folder».

🗙 Open Folder				×
← → ∨ ↑	ıa (C:) > Project	s > A2-SSO-Demo	~ C	Поиск в:
Упорядочить 🔻 Новая папка			≣ ▪	?
🗸 🛄 Этот компьютер	Имя	Дата изменения	Тип	Разм
> 🏪 Система (С:)	📒 bin	27.12.2024 16:01	Папка с файлами	
> — Файлы (D:) > 🦉 Сеть	obj	27.12.2024 16:01	Папка с файлами	
Папка: А2-SSO-	Demo	Выбо	р папки Отме	на

Основные моменты, которые могут быть полезны для разработки собственных приложений с SSO-аутентификацией:

1. Для получения токена приложение прослушивает порт с помощью объекта класса HttpListener. Если не открывать порт на брандмауэре, то принять токен можно будет только через localhost. Если потребуется принимать токен через внешний IP-адрес, потребуется открыть порт на доступ через брандмауэр.

2. При формировании ссылки на страницу авторизации требуется экранировать спецсимволы в строке параметра ReturnUrl через метод Uri.EscapeDataString().

3. В обработчике запросов, поступающих на указанный порт, исключаем все типы, кроме GET, поскольку через localhost страница авторизации ADVANTA передаёт их именно этим методом.

75	// Находит токен в поступившем на указанный порт сообщении
	1 reference
76	<pre>private static async Task HandleRequest(HttpListenerContext context)</pre>
77	{
78	// Проверка на тип запроса
79	<pre>if (context.Request.HttpMethod != "GET")</pre>
80	{
81	// Если метод не GET, возвращаем 405 Method Not Allowed
82	<pre>context.Response.StatusCode = (int)HttpStatusCode.MethodNotAllowed;</pre>
83	string responseTextNoGet = "Метод не разрешен. Используйте GET.";
84	<pre>byte[] bufferNoGet = Encoding.UTF8.GetBytes(responseTextNoGet);</pre>
85	<pre>context.Response.ContentType = "text/plain; charset=utf-8";</pre>
86	<pre>context.Response.ContentLength64 = bufferNoGet.Length;</pre>
87	await context.Response.OutputStream.WriteAsync(bufferNoGet, 0, bufferNoGet.Length);
88	context.Response.Close(); // Заканчиваем обработку запроса
89	return; // Прерываем дальнейшую обработку
90	
91	

4. Получение данных через API-функции ADVANTA мы выполняем в методах MakeSoapRequestWhoAmI() и MakeSoapRequestGetProject(). Они принимают в качестве входного параметра токен доступа, полученный от страницы авторизации.

5. В методе MakeSoapRequestWhoAmI() реализован код для получения данных через APId

функции <u>WhoAml</u> . В теле запроса токен доступа подставляется в параметр <u>ASP</u>	'NETSessionId.
--	----------------

130	// Устанавливаем формат запроса, как указано в описании API WhoAmI
131	<pre>string url = \$"{serverName}/components/services/login.asmx";</pre>
132	<pre>string soapXml = \$@"<?xml version=""1.0"" encoding=""utf-8""?></pre>
133	<pre><soap:envelope ""="" envelope="" htt<="" http:="" pre="" schemas.xmlsoap.org="" soap="" xmlns:soap="" xmlns:xsi=""></soap:envelope></pre>
134	<soap:body></soap:body>
135	<whoami ""="" http:="" streamline="" xmlns=""></whoami>
136	<aspnetsessionid>{/ASPNETSessionId></aspnetsessionid>
137	
138	
139	";
140	

6. Аналогично, в методе MakeSoapRequestGetProject() выполняется запрос к APIфункции GetProject. Здесь также токен подставляется в параметр ASPNETSessionId, а в параметр ProjectId записывается идентификатор проекта.

Пример приложения с удалённой передачей токена

Приложение «A2-SSO-Demo-ASPNETCore» демонстрирует работу SSO-аутентификации для платформы ASP.NET Core. На веб-странице приложения будут отображаться ссылка на страницу авторизации ADVANTA, извлечённый токен и результаты вызова API-функций. Серверная часть приложения будет принимать POST-запросы от сервера авторизации как через внешний IP, так и через localhost.

Примечание: Способ передачи токена через localhost доступен начиная с версии ADVANTA 3.30.

Для запуска приложения необходим веб-сервер с платформой ASP.NET Core 9, который доступен из Интернет. Для тестирования примера можно использовать любой ASP.NET-хостинг, например, бесплатный <u>https://somee.com</u>.

В прилагаемом архиве «A2-SSO-Demo-ASPNETCore.zip» найти каталог «\bin\Release\net9.0\publish» и загрузить файлы из него в директорию вашего тестового сайта на сервере.

rt tickets Summary + > ···· bin > Release > net9.0 > publis @ @ @ 1 Copтировать ~ ·· Имя // Сортировать ~ ·· // Сортировать ~ ·· // Мая // Сортировать ~ ··	File manager Dom — h Поиск в: ри • С	ains / Bindings	IIS applications IIS log viewer Event viewer Dele
+ → ··· bin > Release > net9.0 > publis	– h Поиск в: ри • С	D X Iblish Q В Сведения	C □ 1 1 1 1 Name
 with bin > Release > net9.0 > publis with Copтировать ~ · · · имя A2-SSO-Demo-ASPNETCore.dll A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore.db 	h Поиск в: ри	ıblish Q	Name A2-SSO-Demo-ASPNETCore.deps.json
 Image: Copтировать ∨ Имя A2-SSO-Demo-ASPNETCore.deps A2-SSO-Demo-ASPNETCore.dll A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore 	• C	Сведения	A2-SSO-Demo-ASPNETCore.deps.json
VIMA A2-SSO-Demo-ASPNETCore.deps A2-SSO-Demo-ASPNETCore.dll A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore.pdb			A2-SSO-Demo-ASPNETCore.dll
A2-SSO-Demo-ASPNETCore.deps A2-SSO-Demo-ASPNETCore.dll A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore.pdb	Тип	Дата изменени	A2-SSO-Demo-ASPNETCore.exe A2-SSO-Demo-ASPNETCore.pdb
A2-SSO-Demo-ASPNETCore A2-SSO-Demo-ASPNETCore.pdb	Файл "JSON" Расширение прило	29.01.2025 22:11 29.01.2025 22:33	A2-SSO-Demo-ASPNETCore.runtimeconfig.json
A2-SSO-Demo-ASPNETCore.pdb	Приложение	29.01.2025 22:3:	A2-SSO-Demo-ASPNETCore.staticwebassets.endpoints.json appsettings.Development.json
A2-SSO-Demo-ASPNETCore.runtimeconfig	Program Debug Data. Файл "JSON"	29.01.2025 22:33 29.01.2025 22:17	appsettings.json
A2-SSO-Demo-ASPNETCore.staticwebassets.endpoints	Файл "JSON"	29.01.2025 22:18	default.asp Newtonsoft.Json.dll
appsettings.Development	Файл "JSON" Файл "JSON"	29.01.2025 12:14 29.01.2025 12:14	web.config
Newtonsoft.Json.dll	Расширение прило	08.03.2023 12:09	Showing 1 to 11 of 11 entries
¶⊇ web.config	XML Configuration F	29.01.2025 22:33	

Сразу после загрузки приложение должно быть доступно по адресу вашего сайта. В браузере обязательно должен быть включен JavaScript.

Процесс работы примера

Перейдите на страницу вашего AspNet-сайта в браузере, вы увидите страницу демонстрационного приложения с предложением перейти по ссылке на страницу авторизации демонстрационного стенда ADVANTA.



При переходе по ссылке в новой вкладке браузера будет открыта страница SSOаутентификации ADVANTA. При этом страница автоматически отправит серверу демонстрационного приложения POST-запрос с токеном доступа на адрес API-функции, который тот передал в параметре ReturnURL.

O A https://pmo.a2nta.ru/pages/Login.aspx?ClientId=AuthDemoId&ReturnUrl=H	http%3A%2F%2Fmyaspnetprojects.somee.com%2Fapi%2Freceive 🔂
A D VA N TA	Α.
Вход в систему	
Имя пользователя	
Введите логин	
Пароль	
Введите пароль	
🗹 Запомнить меня	Забыли пароль?
Токен авторизации успешно переда aspnetproject.somee.com/	ин на адрес http:// api/receive
Войти	
Зарегистрироватьс	Я

Сразу же после этого можно вернуться на страницу демонстрационного приложения. При этом страница обновится и загрузит полученный от ADVANTA токен доступа и результаты вызова API.

$\leftarrow \ \ \rightarrow \ \ C$	🔿 aspnetproject. somee.com	☆
SSO-ayı	гентификация в AD	VANTA
Эта страница - п	пример информационной системы с автор	изацей через единую учётную запись ADVANTA.
Ниже вы видите	итог авторизации - токен и результаты вы	- ізова АРІ-функций с его применением.
Если хотите зайт Затем вернитесь	ти под другим пользователем, <u>откройте ст</u> ь на эту закладку и перейдите на страниц	<u>раницу стенда</u> в новой закладке и завершите сессию текущего пользователя. у авторизации по ссылке ниже.
Перейти на стра	аницу авторизации ADVANTA	
Токен успешн	но получен:	
eyJhbGciOiJIUzI1	LNIISInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy5	4bWxzb2FwLm9yZy93cy8yMDA1LzA1L21kZW50aXR5L2NsYWltcy9uYW11aWR1bnRpZm11ciI6ImQ0MmFmM2Zh
Peзультат вызов xml version="1<br XMLSchema-instan streamline/"> <wh PrincipalId><isa soap:Body><th>BA API-функции <u>WhoAml</u>: - получение инфи 1.0" encoding="utf-8"?><soap:envelope xmlns:s<br="">rce" xmlns:xsd="http://www.w3.org/2001/XMLSch nomIResult>cld>53017237-883d-4a65-89a3-fc096 ddmin>falseFullName>Moposoв Андрей SEnvelope></soap:envelope></th><th>ЭрМАЦИИ О ПОЛЬЗОВАТЕЛЕ, КОМУ ВЫДАН ТОКЕН ДОСТУПА: oap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/ ema">ssoap:Body>kHoAmIResponse xmlns="http:// bec431d<principalid>d42af3fa-65f6-4b48-97a1-8b7bc7e6d4db<!--<br--><licensecode>Supervisor</licensecode><!--</th--></principalid></th></isa </wh 	BA API-функции <u>WhoAml</u> : - получение инфи 1.0" encoding="utf-8"?> <soap:envelope xmlns:s<br="">rce" xmlns:xsd="http://www.w3.org/2001/XMLSch nomIResult>cld>53017237-883d-4a65-89a3-fc096 ddmin>falseFullName>Moposoв Андрей SEnvelope></soap:envelope>	ЭрМАЦИИ О ПОЛЬЗОВАТЕЛЕ, КОМУ ВЫДАН ТОКЕН ДОСТУПА: oap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/ ema">ssoap:Body>kHoAmIResponse xmlns="http:// bec431d <principalid>d42af3fa-65f6-4b48-97a1-8b7bc7e6d4db<!--<br--><licensecode>Supervisor</licensecode><!--</th--></principalid>
Информация Результат вызов	и о проекте: ва АРІ-функции <u>GetProject</u> - получение инф	рормации о проекте с правами пользователя:
<pre><?xml version="1 XMLSchema-instan streamline/"></pre> ParentProjectId uwppowsauuw ystemStartDate> xsi:nil="true" / e2b2-4759-b60a-2 >VUsePlannedCost PlannedDuration> be82-15bac256dlf	I.0" encoding="utf-8"?> <soap:envelope xmlns:s<br="">hce" xmlns:xsd="http://www.w3.org/2001/XMLSch ttProjectResult>UID>a6ed1995-582c-42d3-afa0- <vlame>Oprawisaaum ao&moshod VPN(Name>CProje ojectType><status>3</status>Percentcomplete 2025-062709:02124/2028-062709:02124/2028-062709:02124/2018-11-02T08:00:0028a03d40077f/OwmerId><responsibleid>4a9ffd >>false/UsePlannedCost>PlannedCost xsi:nil= >CurationUnit>DAYS<!--/DurationUnit--><startdate> Efc/CalendarId></startdate></responsibleid></vlame></soap:envelope>	<pre>ap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/ zma"><soap:body><GetProjectResponse xmlns="http://
ddb62280b212<parentprojectid>27b9782-5fFb-48bf-a405-bad7625eecc7<!--<br-->ctTypeId346b6db-ecea-4ca8-9c32-a09759738045(ProjectTypeIJ)opexT 57C/PercentComplete><systemstartdate>2023-09-04708:00:00</systemstartdate></parentprojectid></soap:body></pre> // ddate> <plannedstartdate>2023-09-04708:00:00// ddate><plannedstartdate>2023-09-04708:00:00// ddate><plannedstartdate>2023-09-04708:00:00// ddate><plannedstartdate>2023-09-04708:00:00// ddate><pre>/plannedStartDate>2023-09-04708:00:00</pre>// ddate><pre>/plannedStartDate>2023-09-04708:00:00</pre>// ddate><pre>/plannedStartDate><0</pre>// ddate><pre>/plannedStartDate><0</pre>// ddate><pre>/plannedStartDate><0</pre>// ddate><pre>/plannedStartDate><0</pre>// ddate><pre>/plannedStartDate><0</pre>// ddate><pre>/plannedStartDate></pre>// ddate><pre>/plannedStartDate></pre>// ddate><pre>/plannedStartDate></pre>// ddate><pre>/plannedStartDate></pre>// ddate><pre>/plannedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate></pre>// ddate><pre>/planedStartDate</pre>// ddate// ddate</plannedstartdate></plannedstartdate></plannedstartdate></plannedstartdate>

В момент получения токена доступа демонстрационное приложение вызывает две APIфункции ADVANTA. Функция <u>WhoAmI</u> предоставит информацию о пользователе, токен которого получило демонстрационное приложение. Функция <u>GetProject</u> – информацию о тестовом проекте «<u>Организация мобильной VPN</u>» (UID «a6ed1995-582с-42d3-afa0-6db8c280b212»). Если потребуется авторизоваться под другой учётной записью, то сделать это надо в три этапа:

1. Сначала перейти на главную страницу демонстрационного стенда ADVANTA по ссылке на странице приложения:



2. На этой странице нужно завершить сессию текущего пользователя:

$\leftarrow \ \ \rightarrow \ \ C$	O A https://pmo.a2nta.ru/cmn.aspx?pageName=Home_Default	
	VANTA Q	
 Мой профиль Справка 	кодящие 🕜 нные (11) Отвеченные	
С Темная тема		
L→ Выход Выход Бжене	і Адванта пельный отчет о статусе проекта	

3. Затем авторизоваться под другой учётной записью (например, «Шилкова»):

O A https://pm	o. a2nta.ru /Pages/Login.aspx	
	А D V A N Вход в систему Имя пользователя	NT-A
	Шилкова Пароль	
	Запомнить меня Войти	Забыли пароль?
	Зарегистриро	ваться

4. После этого нужно вернуться на страницу демонстрационного приложения и с неё перейти по ссылке на страницу SSO-авторизации ADVANTA:



Страница SSO-авторизации отправит демонстрационному приложению токен текущего авторизованного пользователя («Шилковой»).



После этого нужно вернуться на страницу демонстрационного приложения. Через несколько секунд она обновится и будет отображена информация о пользователе «Шилкова». При этом приложение не сможет получить информацию о проекте «<u>Организация мобильной</u> <u>VPN</u>», поскольку у Шилковой нет прав доступа к этому проекту в ADVANTA.



Запустите Visual Studio Code и откройте каталог с кодом программы командой «File > Open Folder».

X Open Folder			×
	A2-SSO-Demo-ASPNETCore	→ ~ С Пои	иск в: A2-SSO-Demo-AS 🔎
Упорядочить 🔻 Новая папка			≣ ▾ 😗
👻 🛄 Этот компьютер	Имя	Дата изменения	Тип Размер
🗸 🏪 Система (С:)	🚞 bin	29.01.2025 22:17	Папка с файлами
✓ [™] Projects	🚞 obj	29.01.2025 22:17	Папка с файлами
> 🔁 A2-SSO-Demo-ASPNETCore	Properties	29.01.2025 12:14	Папка с файлами
Папка: A2-SSO-Demo-ASPNETCore		1	
		Выб	ор папки Отмена

Проект создан на базе простого web-шаблона ASP.NET Core, весь код – в файле Program.cs. Основные моменты, которые могут быть полезны для разработки собственных приложений с SSO-аутентификацией:

1. В принципе, ASP.NET-приложение может принимать токены доступа из ADVANTA как по открытому IP-адресу, так и через localhost. В коде для примера реализованы оба варианта. Код для приёма GET-запроса с query-параметром token — в функции app.MapGet, а для POST-запроса, который передаёт данные в теле, в JSON-формате, в элементе tokenValue — в функции app.MapPost.

2. Режим передачи токена (локально или удалённо) зависит от содержания переменной ReturnUrl. Если она содержит localhost или «127.0.0.1» токен будет отправлен GET-запросом. Иначе – через POST-запрос.

3. Значение переменной ReturnUrl устанавливается автоматически, в зависимости от информации в «контексте» приложения. Если приложение запущено на веб-сервере в интернете, в переменную будет подставлен IP-адрес. Если на клиентском ПК – то localhost.

30	
31	// Получаем хост из текущего запроса
32	<pre>var host = context.Request.Host.Host;</pre>
33	// Выбираем значение clientId в зависимости от хоста
34	<pre>string clientId = host.Contains("localhost") ? clientId_loc : clientId_srv;</pre>
35	

4. В случае передачи токена через Интернет – используется идентификатор «AuthDemold». В реальных приложениях вам следует использовать свой идентификатор, который вы зарегистрируете в файле client.config вашего сервера ADVANTA.

5. В случае, если ADVANTA по каким-то причинам не смогла сформировать токен, она передаст сообщение об ошибке. При GET-запросе – в query-параметре error, а при POST-запросе – в элементе errorMessage JSON-данных, в теле сообщения.

6. Вызов API-функции <u>WhoAml</u> реализован в методе GetUserInfo, а функции <u>GetProject</u> – в методе GetProject. Им передаётся полученный от ADVANTA токен доступа, который подставляется в SOAP-запрос в качестве параметра <<u>ASPNETSessionId</u>>.