

ABAP SDK Implementation guide for Azure Active Directory

https://github.com/Microsoft/ABAP-SDK-for-Azure

Author: Microsoft SAP Team

Version: 1.0



Contents

What is Azure Active Directory?	3
Prerequisites	3
How to setup Azure Active Directory in Azure?	3
Generate keys for your application	5
Steps to use AAD authentication from SAP using ABAP SDK for Azure	9
Creation of RFC destination to Azure Active Directory	9
STRUST Setup	10
Configuration	12
ZREST_CONFIG	12
ZREST_CONF_MISC	12
ZADF_CONFIG	
DEMO Program	14
ABAP SDK Monitor	14
Auto re-processing of failed messages	15



What is Azure Active Directory?

Azure Active Directory (Azure AD) provides an easy way for businesses to manage identity and access, both in the cloud and on-premises. Your users can use the same work or school account for single sign-on to any cloud and on-premises web application. Users can use their favorite devices, including iOS, Mac OS X, Android, and Windows. An Organization can protect sensitive data and applications both on-premises and in the cloud with integrated multi-factor authentication ensuring secure local and remote access. Azure AD extends your on-premises directories so that information workers can use a single organizational account to securely and consistently access their corporate resources. Azure AD also offers comprehensive reports, analytics, and self-service capabilities to reduce costs and enhance security. The Azure AD SLA ensures that your business always runs smoothly and can be scaled to enterprise levels.

For more details on Azure Active directory, visit Microsoft Azure Active Directory

Prerequisites

Make sure you have installed ABAP SDK for Azure in your SAP system. Refer document 'ABAP SDK for Azure – GitHub' for more details, Visit <u>https://github.com/Microsoft/ABAP-SDK-for-Azure</u>

How to setup Azure Active Directory in Azure?

Login to Microsoft Azure portal.

Note: If you do not have an account already. please create a new Azure account. You can startfree

Once you are logged into portal, go to all services and search for Azure Active Directory and Select

"Azure Active Directory" as shown below.



Create a new tenant for your organization in case it hasn't been created.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant



Click on 'App Registrations' on left side menu as shown below and click the button 'New application Registration'



Specify details of your Application and press 'create' button.

Prev	view	Microsoft Azure	Report a bug	, С a		
			Home > microsoft - App re	gistrations > Create		
+-	Create	a resource	Create	=	×	
	All ser	vices	* Name			
*	FAVORIT	ES	ABAPSDKDEMO-APP		-	
			Application type 6			
< <u>>></u>	Functio	on Apps	Web app / API	~	•	
3	SQL da	atabases	* Sign-on URL 6		-	
2	Azure	Cosmos DB	https://localhost:4000	~	-	
	Virtual	machines				
-	Load b	palancers				
-	Storag	e accounts				
	Virtual	networks				
•	Azure	Active Directory				
0	Monite	or				
-	Adviso	nr.	Create			

Application is created successfully.

ABAP SDK for Azure



Preview Microsoft Azure	e Report a bug 🔎 a				× (2°)>_	(j)) () 🗣
* *	Home > microsoft - App registrations						
+ Create a resource	microsoft - App registration Azure Active Directory	s				0	
i∃ All services	Search (Ctrl+/)	«	New application registration	Endpoints	🗙 Troubleshoot	Successf	ate application ully created applicati
	1 Overview		To view and manage your registra	tions for converg	ed applications, pleas	e visit the N	Aicrosoft Application
Function Apps	Getting started		Search by name or AppID	My app	s	~	
👼 SQL databases	MANAGE				APPLICA	TION TYPE	APPLICATION
🬌 Azure Cosmos DB	🛓 Users		AB ABAPSDKDEMO-APP		Web ар	ip / API	75098752-6
🧧 Virtual machines	🝰 Groups	1					
🔶 Load balancers	Roles and administrators						
Storage accounts	Enterprise applications						
Virtual networks	Devices						
Azure Active Directory	App registrations						

Generate keys for your application

 Once your application is created, go to your application by clicking on it. Copy the application id which will be required in the implementation of code in ABAP SDK. This application id is client Id.



Click on 'Settings' in the above screen, go to the 'Required Permissions' under API Access as shown below.



ABAPSDKDEMO-APP Registered app	~ *	× Settings	□ ×
🌣 Settings 💉 Manifest 🛚 🛅 Delete		P Filter settings	
Display name ABAPSDKDEMO-APP	Application ID	GENERAL	
Application type Web app / API	Object ID	Properties	>
Home page https://localhost:4000	Managed application in local directory ABAPSDKDEMO-APP	🗮 Reply URLs	>
	*	Owners	>
		API ACCESS	
		Required permissions	>
		📍 Keys	>
		TROUBLESHOOTING + SUPPORT	

2. Then click on 'Add' button as shown in the below screen.

Preview Microsoft Azure Report a b	ug Pa	× \$\$ ≥ \$ @ \$
≪ Home > .microsoft - App	registrations > ABAPSDKDEMO-APP > Settings > Req	
+ Create a resource * X	Settings	× Beguired permissions
i≡ All services	✓ Filter settings	+ Add Grant permissions
FAVORITES 5f-58b8b4713ef2	GENERAL	API APPLICAT
Function Apps dac-9bdc5b39e88e local directory	Properties	> Windows Azure Active Directory 0
SQL databases	E Reply URLs	>
🧭 Azure Cosmos DB	Owners 2	>
Virtual machines	API ACCESS	
💠 Load balancers	A Required permissions	>
Storage accounts	Y Keys	>
Virtual networks		

3. Under 'Add API access' section click on 'select an API 'and Search Azure Key Vault and Select the same as shown below.

Note:

In this step, we have chosen Azure Key vault as an external application as an example. In real world scenario, you need to choose your existing API which you want to access with AAD token for authentication.

ABAP SDK for Azure



4. Under Add API access section, click on 'Select permissions' and enabled the checkbox for 'Delegated Permissions' as shown below.

Preview	Microsoft Azu	re Report a bug	,О а				ſ	>_	<u>نې</u>	\odot	0	P
	«	Home > microsoft - App re										
+ Cr	eate a resource	×	Add Af	Pl access	×	Enable Acces	ss					
ie ai	services		1	Select an API	~		N PERMIS	SIONS				
— 🖈 FAV	ORITES	DELEGATED PERMIS	<u> </u>	Azure Key Vault		No application p	ermissio	ns avai	able.			
🤣 Fu	nction Apps	1	2	Select permissions	>	DELEGATED	PERMISS	IONS				
🗟 sc)L databases		2	0 role, 1 scope		Have full ac	cess to	the Azu	re Kev \	/ault ser	vice	
🥭 Az	ure Cosmos DB		1. 01							duitoti		
🛄 Vir	tual machines											
*	100 B				I							

+	Create a resource	×	Required permissions		×	Add A	PI access	
:=	All services		+ Add • Grant permissions			1	Select an API	
*	FAVORITES	-	API	APPLICATION PERMI	DELEGATED PERMIS	1	Azure Key Vault	Ť
% >	Function Apps	^ >	Windows Azure Active Directory	0	1	2	Select permissions	
1	SQL databases	>				2	0 role, 1 scope	× .
2	Azure Cosmos DB	>						
	Virtual machines							
*	Load balancers	ons >						
=	Storage accounts	>						
~ •>	Virtual networks	PORT						
♦	Azure Active Directory	>				_		
۲	Monitor	est >				Done	,	
-	Advisor					Do	ne	

Then click on 'Done' button to complete the Required permissions activity.

5. Click on 'Grant permissions' and press 'Yes' button as shown below.

Microsoft



Preview Microsoft Azure Report a b	ug \mathcal{P} a		× 🗘 >_ 🍪 😳 🕅 🖫
Kome > microsoft - Ap	p registrations > ABAPSDKDEMO-APP > 1		missions
+ Create a resource 💉 🗙	Settings	×	Required permissions
i≣ All services	P Filter settings		+ Add Srant permissions
★ FAVORITES5f-58b8b4713ef2	GENERAL		Do you want to grant the permissions below for ABAPSD
Function Apps ^ dac-9bdc5b39e88e	Properties	>	account in current directory? This action will update any application already has to match what is listed below.
SQL databases	E Reply URLs	<u>></u>	
🧟 Azure Cosmos DB	Search Owners	<u>></u>	No
Virtual machines	API ACCESS		
🚸 Load balancers	🔏 Required permissions	>	

6. Click on 'Keys' section and provide key description and expiry Duration in the below screen. Under 'EXPIRES' dropdown list, you can select the expiry duration.

Preview	Microsoft Azure	Report a bug	, С a		×	⊈>_	\$\$ C	0	P
		Home > microsoft - App regis							
+ Create	a resource	Settings	×	Keys					
i⊟ All ser	vices	P Filter settings		🗜 Save 🗙 Discard		Key			
🛨 FAVORIT	ES	GENERAL		Passwords					
🤣 Functio	on Apps	Properties	>	DESCRIPTION	EXPIRES		VALUE		
🗃 SQL da	atabases	E Reply URLs	>	No results.					
🧭 Azure	Cosmos DB	Owners	>	Key description	Duration	~	Value w	ill be displi	ayed on save
👰 Virtual	machines	API ACCESS							
🔶 Load b	palancers	🔏 Required permission	s >	Public Keys					
🧾 Storag	e accounts	📍 Keys	>	THUMBPRINT			STA	RT DATE	
 Virtual 	networks	TROUBLESHOOTING + SUPPO	RT	No results.					

Here key description is provided as client_secret and it expires on 8/2/2019.

Preview	Microsoft Azure	Report a bug	, Ра			×	Ľ.	>_	ŝ	\odot	0	P
		Home > microsoft - App regis										
+ Create	a resource	Settings		× Kevs Save	l							
i All serv	rices	P Filter settings		R Save	X Discard		ic Key					
- 🛨 FAVORITE	s	GENERAL		Passwo	ords							
🤣 Functio	on Apps	Properties	>	DESCRIPT	TION	EXPIRES			VALU	Ē		
👼 SQL da	tabases	E Reply URLs	>	client_se	cret	8/2/2019	1					
🧟 Azure (Cosmos DB	Sources Owners	>	Key des	scription	Duration		~	Val	ue will b	e displa	yed on sa
🕎 Virtual	machines	API ACCESS										
🚸 Load b	alancers	& Required permission:	s >	Public	Keys							
🧱 Storage	e accounts	📍 Keys	>	тнимвр	RINT					START D	DATE	
↔ Virtual	networks	TROUBLESHOOTING + SUPPO	RT	No result	ts.							

 Click on 'Save' button to generate secret key. Copy this key and it will be used in ABAP SDK implementation. Please remember you won't be able to retrieve this key once you leave the screen.



+ Create a resource	Settings	×	Keys			
i∃ All services	P Filter settings		R Save X Discard	T Upload Public Key		
+ Favorites	GENERAL		A Copy the key value.	. You won't be able to retriev	e after you leave this blade.	
Function Apps	Properties	>	Passwords			
💈 SQL databases	🗮 Reply URLs	>	DESCRIPTION	EXPIRES	VALUE	
🧭 Azure Cosmos DB	Owners	>	client_secret	8/2/2019		
Virtual machines	API ACCESS		Key description	Duration	Value will be displayed on sav	e
🔶 Load balancers	🔏 Required permissions	>				
Storage accounts	Y Keys	>	Public Keys			
😔 Virtual networks	TROUBLESHOOTING + SUPPORT		THUMBPRINT		START DATE	EXPIRES
Azure Active Directory	X Troubleshoot	>	No results.			

Steps to use AAD authentication from SAP using ABAP SDK for Azure

Creation of RFC destination to Azure Active Directory

Go to transaction SM59 in your SAP system and create new RFC destination of type 'G'. Maintain your Azure Active directory endpoint in the Target host and path prefix for authorization token as shown below.

Target host: login.microsoftonline.com

Port: 443

Path Prefix: /<Input Tenant ID>/oauth2/token

For Tenant ID details and creating a new tenant id in Azure Active Directory, please refer this document section 'How to setup Azure Active Directory in Azure?'

onnection Test				
RFC Destination		AZURE_ABAPSDKKDEMO-AAD		
Connection Type	G	HTTP Connection to External Serv	Description	
Description				
Description 1	Desti	nation to Azure AAD		
Description 2				
Description 3				
Administrati Target System Settin	Technical S	Logon & Security Special Options		
Administrati Target System Settin Target Host	Technical S ngs	ettings Logon & Security Special Options	Service No.	44
Administrati Target System Settin Target Host Path Prefix	ngs Iogi	ettings Logon & Security Special Options	Service No.	44 n
Administrati Target System Settin Target Host Path Prefix	Technical S	Settings Logon & Security Special Options	Service No.	144 n
Administrati Target System Settin Target Host Path Prefix HTTP Proxy Options Global Confi	Technical S ngs logi [/	Settings Logon & Security Special Options	Service No.	44 n
Administrati Target System Settin Target Host Path Prefix HTTP Proxy Options Global Confil Proxy Host	Technical S Iogi [/]	Settings Logon & Security Special Options	Service No.	n 44
Administrati Target System Settin Target Host Path Prefix HTTP Proxy Options Global Confi Proxy Host Proxy Service	Technical S Ings Ilogi I/	Settings Logon & Security Special Options	Service No.	n 44
Administrati Target System Settin Target Host Path Prefix HTTP Proxy Options Global Confit Proxy Host Proxy Host Proxy User	Technical S	Settings Logon & Security Special Options	Service No.	144 n



Now go to 'Logon & Security' tab and choose radio button SSL 'Active' and select SSL certificate 'DFAULT SSL Client (Standard)'.

FC Destination	AZURE ABAPSDKKDEMO-AAD	- To
onnection Type	G HTTP Connection to External Serv	Description
escription		· ·
Description 1	Destination to Azure AAD	
Description 2		
Description 3		
Administrati Tec	chnical Settings Logon & Secu Special Options	
Administrati Tec	chnical Settings Logon & Secu Special Options	
Administrati Tec System ID Security Options	chnical Settings Logon & Secu Special Options Client	
Administrati Tec System ID Security Options Status of Secure Pro	chnical Settings Logon & Secu Special Options Client Dtocol	
Administrati Tec System ID Security Options Status of Secure Pro SSL	chnical Settings Logon & Secu Special Options Client Dtocol OInactive OActive	

Do a connection test to make sure it is working. RFC destination is working.

Connection Te	est HTTP D	estination A	ZURE_ABA	PSDKKDEMO-AAD
Destination	AZURE_ABAPSD	KKDEMO-AAD		
Ту.	HTTP Connectio	n to External Server		
Test Res Respor	nse Header Fields	Response Body	Response Text	
Detail	Value			
Status HTTP Response	200			
Status Text	ОК			
Duration Test Call	319 ms			

STRUST Setup

We need to import Microsoft's Certificate and import in STRUST for SSL handshake between SAP system and Azure Active Directory over HTTPS protocol. To download the certificate, in your browser, go to URL with the hostname and path prefix you used for creating RFC destination.

Target host: login.microsoftonline.com

Path Prefix: /<Input Tenant ID>/oauth2/token

ABAP SDK for Azure



C Secure https://login.microsoftonline.com	/oauth2/token			

Click on the Lock symbol you find next to refresh button in Chrome browser and select Certificate to view the certificate used for communication



In the certificate, go to Details tab and Choose button 'Copy to File' to download the certificate to your local machine. Repeat the process and download all the certificate until root. In this case, you need to download two certificates.

- 1. Microsoft IT TLS CA 4
- 2. Baltimore Cyber Trust Root

Certificate X	Certificate X	Certificate ×
General Details Certification Path	General Details Certification Path	General Details Certification Path
G	Show (Alls v	Certification path Certification path Certification CyberTrust Root
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer • Proves your identity to a remote computer • Microsoft IT CPS	Field Wole A Serial number Signature algorithm Signature lago.	Log Marcoll (11 TLS CA 4
* Refer to the certification authority's statement for details. Issued to: stamp2.jogn.microsoftenine.com	Vidid tran	
Issued by: Microsoft IT TLS CA 4		View Certificate
Valid from 12/29/2017 to 12/29/2019		Ortificate status: This ortificate is OK.
Issuer Statement	Folk Properties	
OK	OK	OK



when all the certificates are downloaded, Go to STRUST transaction in your SAP system and Import all these certificates in DFAULT PSE.

Note: We are not going through the process of Importing certificates in STRUST in this document. It is straight forward, and your BASIS team can help you to do this activity.

Configuration

ABAP SDK has following main configuration tables and they need to be maintained. We will create a new Interface ID to establish connection between SAP system and target Azure Active Directory (AAD). A new Interface ID needs to be created for each AAD namespace.

ZREST_CONFIG – Master Table for Interface ID Maintenance. You must define a new Interface name and maintain the RFC destination that was created for target Event hub.

ZREST_CONF_MISC – This is an Interface Miscellaneous table which contains information on Alerts and reprocessing of failed messages automatically.

ZADF_CONFIG – This is an Interface extension table. This stores data that is more specific to Azure Services like SAS keys, AAD secrets and processing Method.

ZREST_CONFIG

Create a new Interface ID like 'DEMO_AAD' and Maintain the RFC destination you created earlier.

Change Vie	ew "Configure Interface UR	I Destination": Overview
🤣 💽 New Entri	es [🔁 🖶 🖪 🖪 🖪	
Configure Interfac	e URI Destination	
Inter ID	RFC Destination	
DEMO_AAD	AZURE_ABAPSDKKDEMO-AAD	-
E		

ZREST_CONF_MISC

Create an entry in table 'ZREST_CONF_MISC' for the above interface Id 'DEMO_AAD'.

Details of configuration:

- METHOD is 'POST'.
- MAX_RETRY is number of retry in case of service failure.
- EMAIL_ID is the email id for sending alerts.
- MAIL_BODY_TXT is Text Id to be maintained for the mail content.
- RETRY_METHOD is type of retrial (Regular '0' or exponential '1')



Table ZREST_CONF_MISC Display

MANDT	300
INTERFACE ID	DEMO_AAD
METHOD	POST
MAX RETRY	1
EMAIL ID	temente @microsoft.com
MAIL BODY TXT	ERROR WHILE SENDING MESSAGE TO AAD
RETRY METHOD	

ZADF_CONFIG

Create an entry in table 'ZADF_CONFIG' for the above interface Id 'DEMO_AAD'.

Details of configuration:

- INTERFACE_TYPE is 'Azure Active Directory'.
- SAS_KEY is the shared access key. This is the key which generated in AAD under section 'Generate keys for your application' Step 7 (refer Page 8). You need to change this key in this config table whenever key is changed in Azure.
- URI is left blank. This may be required for future versions.
- SERVICE_TYPE can be synchronous(S) or asynchronous(A)
- IS_TRY is a reprocessing flag, maintain as blank. it can be configured for reprocessing in case of failure of services.

Note: This field can be utilized in our future release to control the reprocessing based on value of X. Presently it's should be enabled as blank.

Table ZADF_CC	ONFIG Display
MANDT	300
INTERFACE ID	DEMO_AAD
INTERFACE TYPE	AAD
SAS KEY	****
URI	
SERVICE TYPE	S
IS TRY	



DEMO Program

Please refer to DEMO program 'ZADF_DEMO_AZURE_AAD' to generate AAD token for AAD based authentication.

Please note that in the demo program, application id generated in step 1 of <u>Generate keys for your application</u> is used as client id.

Report	ZADF_DEMO_AZURE_AAD	Active
27	i	v_business_identifier = gv_message_bid).
28	oref_aad ?= oref.	
29		
30	G TRY.	
31	CALL METHOD oref aad->get aad token	n
32	EXPORTING	
33	iv client id = '***********	" Input glient id as per implementation guide for AAD
34	iv resource =	"Resource for Azure Key vault application
35	IMPORTING	
36	ev aad token = gv aad token	
37	ev response = qv response.	
38	CATCH zcx interace config missing IN	TO cx interface.
39	gy string = cx interface->get text	().
40	MESSAGE gv string TYPE 'E'.	
41	CATCH zcx http client failed INTO cx	http .
42	gy string = cx http->get text().	
43	MESSAGE gy string TYPE 'E'.	

ABAP SDK Monitor

We have provided an Interface Monitor (Transaction ZREST_UTIL), using this monitor you can view history of all the messages that were posted to Azure Services. In case you have a scheduled a background job to post messages to Azure, you can view the statuses of the messages in this monitor. This Monitor can be used for troubleshooting and re-processing of the message as well.

Go to transaction ZREST_UTIL and provide your Interface ID in the selection screen and execute to view all the messages

Microsoft

Ionitor				
>				
Interface ID		to		
Stores Execution Date	08/05/2018	to	08/05/2018	
Stores execution time	00:00:00	to	00:00:00	
Stores Completed Date		to		
Stores Completed time	00:00:00	to	00:00:00	
Http Status		to		
Message Id	000000000000000000000000000000000000000	0 to	000000000000000000000000000000000000000	
Business Identifier		to		

In this monitor, you can view the status of the HTTPs message and its headers, response, payload and so on. In case of errors, you can also re-process the message from this tool.

Exception C	Operation Id Operat 0003A0180251ED8A69AF7D82497C0E2 POST	OK 200	08/05/2018	te Execution T 10:48:23	me Completed de 06/05/2018	te Completed tim 10:48:23	e Time-ms Retry 375	Date Retry At 000	00:00:00	e Host Jogin microsoftonline.com	UR1
	(P) Details										
							_				
	Group description	Celi Cor	0400								
	Convector as	000034	010023160046	94070624970	052						
	Operation	OK.	POST								
	Hittostatus	200									
	Execution date	08/05/2	08/05/2018								
	Execution Time	10:48:2	10:48:23								
	Completed date	08/05/2	018								
	Completed time	10:48:2	3								
	Time-ms	375									
	Host	login.mi	crosoftonline.co	m							
	URI	1	of the local division of	Hard Street of Lot	oeuth2/toke	n					
	Interface Id	DEMO_	WO .								
	Calling Program	ZCL_AD	F_SERVICE								
	Calling Method	SEND									
	User Alles	-									
	Business Identifier	TEST A	AD								

Auto re-processing of failed messages

For auto-processing of messages in case of failures, you must schedule a background job for program 'ZREST_SCHEDULER' as a pre-requisite.