CA SSO and CA APIM Integration Guide Part 2

Version: CA SSO R12.8 SP1, CA API Gateway 9.3, Tool kit 4.2

CA SSO configuration – Integration with JWT Authentication

- 1. Create Private Key for JWT token Signing in APIM Gateway
 - Login APIM Policy Manager
 - Go to Tasks -> Certificate, Keys and Secretes -> Manage Private Keys

The Luit	TOSKS	view riep		
Conne		Identity Providers	>	Preferences
Assertio	9 4	Users and Authentication	>	
Search	0	Services and APIs	>	~
	~	Transports	>	
÷ 🗂	F	Certificates, Keys and Secrets	2	Manage Certificates
••••••••••••••••••••••••••••••••••••••		Data Sources	2	📮 Manage Private Keys
÷ 🖬	1	Global Settings	2	Manage Stored Passwords
÷ 🖬	⊠ ₽	Extensions and Add-Ons	>	
	~	Logging and Auditing	>	
÷. 📬	Polic	v Logic		-

• Create new Private Key. In Alias, input "jwscert". Then, click "Create" button

ge Private Ke	eys	Ca Create Private Ke	ey X							
Certificates S	s w Sub N=	Basic Advanced Alias: Subject DN:	jwscert CN=jwscert]							
									Key type: Days until expiry: CA capable:	2048 bit RSA ✓ 1825 □ Certificate will be used to sign other certificates
			Create Cancel							

• After creating, select newly created key (jwscert) and double click "properties".



• Click "Export Key" and input the password. (Any password) Then save the exported key file with p12 format.

Private Key Details	
Location: Software DB	
Alias: jwscert	
Key Type: RSA 2,048 bits	
Certificate Chain	
CN=jwscert View Certificate	
Other Actions	
Generate CSR Replace Certificate Chain Export Key	
Mark as Special Purpose Delete Key	
OK Cancel	
Ca Enter Export Passphrase	
Password:	
Password:	
Password:	
Password: Verify password:	
Password: Verify password: OK Cancel	
Password: Verify password: OK Cancel	
Password: Verify password: OK Cancel Ga Save As PKCS#12 File	n.
Password: Verify password: OK Cancel Ca Save As PKCS#12 File Save in: Export_APIM_Policy]+
Password: Verify password: OK Cancel Ca Swe As PKCS#12 File Save in: Export_APIM_Policy]+
Password: Verify password: OK Cancel Ca Save As PKC5#12 File Save in: Export_APIM_Policy	3+
Password: Verify password: OK Cancel Ca Save As PKC5#12 File Save in: Export_APIM_Policy Recent Items	9-
Password: Verify password: OK Cancel Ca Save As PKCS#12 File Save in: Export_APIM_Policy	3+
Password: Verify password: OK Cancel Ca Save As PKCS#12 File Save in: Export_APIM_Policy	9-
Password: Verify password: OK Cancel	9-
Password: Verify password: OK Cancel Ca Save As PKC\$=12 File Save in: Export_APIM_Policy Recent Items Deskop Documents	9-
Password: Verify password: OK Cancel	9 .
Password: Verify password: OK Cancel	3.

- 2. Create JWT Authentication Scheme in CA SSO
 - Login CA SSO Admin UI and go to Infrastructure -> X509 Certificate Management -> Trusted Certificates and Private Key. Then, click "Import New"

X

technologies	n-On							siteminder Server s	so.forwardinc.ca	Sign out 🛛 Help
asks «	Trusted Certifica	tes and Private K	eys							
nfrastructure –										
Agent Authentication	To import cer the correspond	tificates/private ng option under t	eys, click the Imp he Actions button	oort New button. To c	reate a new cer	tificate request	click Request Certific	ate button. To delete	or export a certifi	cate alias, click
Directory	Filter Certificate	s and Private Ke	/s							
 Hosts X509 Certificate Management 			Search F	or: Alias	• =	•		Search		
Certificate Authorities	Certificate and	Private Key List						Get Update	s Import New R	equest Certifica
CDS Settings Contificate Validity		1							,	0-0 of 0 Show
OCSP Configuration	Action	~ Alias	~ Туре	Signing Status	Issued To	~ Issuer	Revoked?	Expiration Date	* FIPS Status	Dependenci
olicies Φ	Legend : Cert Cert	ficate is expired ficate is not expir	ed							
ederation Φ	🔔 Cert	ficate will expire	soon							
eports 👳										
dministration 👳										

• Import certificate, which is exported from API Gateway(jwscert). Then, input the password.

1 Select File	2 Password (if needed)	3 Select Entries	4 Confirm
ct a file. PKCS#12 files (priva	te key and certificate) must en	d in '.p12' or '.pfx'. Any	other extension will be trea
Input File Use as •	AS: Single Key/Cert File CA: Yes No File: C:\fakepath\jwscert.p12	Separate Key File a	nd Cert File

• After verify the certificate, click "Finish" button.

Trusted Certificates and Privat	te Keys			
View Certificates and Private Keys > Im	nport Certificate/Private Key			
				Back Next Finish Cancel
	1 Select F	ile 2 Password (if needed) 3	Select Entries Confirm	
Review and confirm select	ctions for import.			
Entries to Import				
Show Details	Alias	Туре	Issued To	
📥 Hide	jwscert	Private Key and Certificate	CN=jwscert	
	Issued To: CN=jwscert Issued By: CN=iwscert			
	Valid From: Oct 18, 2018	8 07:48 AM PDT	Valid To: Oct 17, 2023 07:48 AM PDT	
	Key Algorithm: RSA		Version: 3	
	Serial Number: 11:A5:D7:A	1:61:31:C7:61		
	SHA-256 Fingerprint: 82:88:DF:CF	F:B8:13:17:E2:CF:92:89:EF:2B:2C:B7:47	AB:FE:8B:C8:6C:46:A7:99:C1:70:3F:9C:B6:91:43:42	
	SHA-1 Fingerprint: E1:7D:C5:5	5:8F:20:2F:26:9C:0E:6A:17:65:5B:8D:3E	:33:35:3D:3B	
	MD5 Fingerprint: 02:71:08:29	9:6F:3B:6F:69:C1:9C:17:D5:FC:E1:F8:80		
				Back Next Finish Cancel

- Go to Infrastructure -> Authentication -> Authentication Scheme -> Create Authentication scheme.
 - Name : JWT Auth Scheme
 - o Authentication Scheme Type: JSON Web Token Template
 - User Lookup : sub
 - Certificate Alias List: jwscert

Create Authentication Scheme:	JWT Auth Scheme	
Authentication Schemes > Create Authe	ntication Scheme: JWT Auth Scheme	
• = Required		
General	-	
(T		
• Name	JWT Auth Scheme	Description
Scheme Common Setup		
Authentication Scheme Type	JSON Web Token Template	
Protection Level	5	[1-1,000,hig
Deseword Policies enabled t	for this Authentication Scheme	
	or this Authentication Scheme	
Schome Setur		
JWT Token Authentication /	Attribute for Validation	
• User Lookup:	sub]
Certificate Alias List:	jwscert	1
Use JOSE Header KID as C	ertificate Alias	k
Use JOSE Header KID as C HMAC Shared Key :	ertificate Alias	ka I

• Go to APIM Domain (which is created in part 1) and click modify button. Go to Realms and click "Create Realm".

Modify Domain: APIM					
Domains > Modify Domain: APIM					
General Realms Policies Res	oonses Rule Groups	/ariables			
• = Required					\frown
Realms					Create Realm
Name		Description		Resource Filter	I of 1
	0	Description	/login	Resource Finter	0
				s	ubmit Cancel

- Create new Realm
 - Name : JWT Protected
 - Agent: secureproxy-01
 - Resource Filter : /protected/
 - Authentication Scheme : JWT Auth Scheme

C	Create Realm: JWT Protected					
	Domains > Modify Domain: APIM > Create Realm: JWT Protected					
	Required					
	General					
	• Name	JWT Protected	Description			
	Domain	APIM				
Ì	Resource					
	• Agent	secureproxy-01	Lookup Agent/Agent Group			
	Resource Filter	/protected/				
	Effective Resource	secureproxy-01/protected/				
	Default Resource Protection	Protected Unprotected	R			
	Authentication Scheme	JWT Auth Scheme 🔻				
	Resource • Agent Resource Filter Effective Resource Default Resource Protection Authentication Scheme	secureproxy-01 /protected/ secureproxy-01/protected/ • Protected Unprotected JWT Auth Scheme •	Lookup Agent/Agent Group			

- Create Rule
 - Name : GET-POST
 - Resource : *
 - Action : GET, POST, PUT

eneral					
		DOOT			
Name	GE	-POST		De	escription
omain	APIN	1		Re	alm
Attributes		_	_	_	
Realm and Resour	се				
Pacauraa	*				
- Resource					
Effective Resource:	secureproxy-01	l/protected/*			
Regular Expression			R		
Allow /Dony and E	nable (Dicable				
Allow/ Delly and L	nable/ Disable			_	
Allow Access					
Dopy Access					
Deny Access					
Enabled 🗹					
Action					
				_	
Web Agent a	ctions		Get	A	
Authenticatio	n events	• Actions	Post		
Authorization	events	 Actions 	Put		
Impersonatio	n events		ProcessSOA	P 🔻	

• Click "OK" button and Submit

Modify Domain: APIM							
Domains > Modify Domain:	APIM						
General Realms	Policies	Responses	Rule Groups	Variables			
• = Required							
Realms							Create Realm
							1-2 of 2
	Name			Description		Resource Filter	
APIM			0		/login		0
L-DJWT Protected			0		/protected/		\frown
							Submit Cancel

• Go to APIM Domain again and click modify button again. Then, go to policies tab. In policies, click APIM modify.

l	Modify Domain: APIM
	Domains > Modify Domain: APIM
	General Realms Policies Resp
l	• = Required
l	Policies
	Name Description

• In policies, go to Rule tab and click "Add rule" button. Then, select JWT Protected Realm

Domains > Modify Domain: APIM > Modify Policy: APIM						
General	Users Rules Expr	ression				
= Requir	ed					
Rules						
Name						
Go Reset						
* Realm	▼ Rule	Response	• Response Group			
APIM	APIM login GET Post Rule			Add Response	$\overline{}$	
Add Rule	0					

reneral	Users	Kules Exp	ression
Availabl	e Rules		
= Req	uired		
_			
Rules	for APIM		
Name			
Go Re	set		
Select	Realm	Rule	Туре
	JWT Protected	GET-POST	Rule
1			

• Click OK button and click Submit Button again.

lify Domain: APIM
naina + Modify Domain: APIM
eneral Realms Policies Responses Rule Groups Variables
= Required
ulicies
Name Description P APIM Preate
Calmit Canal

3. Create JWT Assertion in APIM Policy Manager

 Login API Gateway Policy Manager and create "Publish Web API" Service Name : Issue ID Token Gateway URL: /casso/idtoken*

Ca Publish Web API Wizard	X
Steps 1. Service Information 2. Access Control	Enter the name of the non-SOAP application you want to publish: Service Name: Issue ID Token
	Enter the HTTP URL that the Gateway should forward requests to: Target URL:
	Complete the Gateway URL that will receive service requests: Gateway URL: http(s)://apim.forwardinc.ca:[port]/ /casso/idtoken*
	Specify the connection and routing information for the non-SOAP application.
	Back Next Finish Cancel Help

Then, click "Finish" button

- Click "Import Policy" and select "Issue ID Token (JWT).xml" file.
- It shows Resolve External Dependencies Wizard. For CA SSO, please select "Change assertions to use this CA Single Sign-On configuration. "CA SSO". (It is CA SSO configuration, which is created in part 1.)

Ca Resolve External Dependencies Wizard	>
Steps 1. Unresolved CA Single Sign-On Configuration CASSO 2. Unresolved provider CA SSO User DB	Policy contains assertions(s) refering to unkown CA Single Sign-On Configuration Missing CA Single Sign-On Details Configuration Name CASSO Hostname apim.forwardinc.ca Action Change assertions to use this CA Single Sign-On configuration CASSO Remove assertions that refer to the missing CA Single Sign-On configuration Import erroneous assertions as-is Create CA Single Sign-On Configuration Unresolved CA Single Sign-On Configuration CASSO Import erroneous Configuration CASSO Create CA Single Sign-On Configuration CASSO Casso Configuration CASSO Configuration CASSO Configuration CASSO
	Back Next Finish Cancel Help

Then, click next

• In Wizard, select Import erroneous assertion as-is. "Create New Identity Provider". It will connect CA SSO User Directory.

Steps	Dellas contains constitues that we	ter her eine under sonne Under Albeit einen Under	
	Policy contains assertions that refe	er to an unknown identity provider.	
1. Unresolved CA Single Sign-On Configuration CASSO			
2. Unresolved provider CA 350 USER DB	Name CA SSO User DB		
	Type LDAP		
	Name	Value	
	userCertUseType	NONE	~
	Idapsearchbase	dc=ForwardInc,dc=ca	
	Idapwritebase		~
	Remove assertions that refe Import erroneous assertions Create new Identity Provider	r to the missing identity provider s as-is	
	Unresolved provider CA SSO User I	DB	

• It shows "Create LDAP Identity Provider Wizard" and input correct Bind Password. (CAdemo123). Using "Test" button, please verify the connection. Depending on the environment, LDAP Host file and other information can be changed.

Ca Create LDAP Identity Provider Wizard			×					
Steps		Provider Type:* GenericLDAP ~						
1. Provider Configuration	Provider Name:*	CA SSO User DB						
3. User Object Classes 4. Advanced Configuration 5. NTLM Configuration 6. Certificate Settings	LDAP Host URL:*	ldap://sso.forwardinc.ca:25389	Move Up Move Down					
		Add Edit Remove						
	Search Base:* dc=ForwardInc,dc=ca							
	Bind DN:	uid=superuser,ou=users,ou=northamerica,dc=ForwardInc,dc=ca						
	Bind Password:	•••••	Show Password					
		Allow assignment to administrative roles						
	Allow updates fro	m:						
	Write Base:*							
	Reconnect Timeout:	60000 Use System Default						
	This Wizard allows yo required.	u to configure an LDAP Identity Provider. Fields marked with an aster om" check box determines whether the LDAP server can be updated :	isk "*" are					
	the specified write bas	56.	Ý					
		Back Next Test Finish	Cancel Help					

• Then, click "Next" continually. In User Object classes screen, please verify the Login Name. In CA LDAP, default Login Name should be "uid". When you are using other user directory, it can be different.

eps User	ses	
1. Provider Configuration 2. Group Object Classes 3. User Object Classes	Object Class Name:	inetOrgPerson
4. Advanced Configuration 5. NTLM Configuration	Attribute Mapping	
6. Certificate Settings	Attribute:	Mapped to:
	User Name:	cn
	Login Name:	uid
	Password:	userPassword
	First Name:	givenName
	Last Name:	sn
	Email:	mail
	Certificate:	userCertificate; binary
	Kerberos Principal:	cn
	Kerberos Enterprise Princid	

Then, click Finish button.

• In Resolve External Dependencies Wizard, please select "CA SSO User DB" in Action.

Steps			
1. Unresolved CA Single Sign-On Configuration CASSO 2. Unresolved provider CA SSO User DB	Policy contains assertions that refer to Missing Identity Provider Details Name CA SSO User DB	o an unknown identity provider.	
	Name userCertUseType	Value	<u>^</u>
	Idapsearchbase Idapwritebase	dc=ForwardInc,dc=ca	
	Action Change assertions to use this id Remove assertions that refer to Import erroneous assertions as Create new Identity Provider Unresolved provider CA SSO User DB	entity provider: CA SSO User DB the missing identity provider is	~

Then, click "Finish" button.

• Then, you can see the imported policies in UI. Click "Save and Activate" icon in UI.

Home	x	CAS	SOTes	t [/te	est/cas	sso] (v2/2, a	octive)	×	Ŀ	sue I	D Tol	ken	[/cas	so/i	dtok	en*]	(v1/1,	active) 🗵	1
🗄 Save	and A	ctivate	🗄 S	ave [🕼 Vali	date	C Expo	ort Polic	у	Imp	ort Po	olicy	🖣 Ir	nport	Fro	m UD	DI 🦻	Show	Comm	ents)	×
											~ [1		Δ		Ca	se Sei	nsitive	<mark>⊠ S</mark>	how D	isi
2 4 3 5 14 5 14 7 30 31 32 33 34 35 36 37 38 39 40 41 42		t Mess Toker ast on All asse all asse assertio Custom Custom Set Cor Set Cor Set Cor Set Cor Set Cor Add Au Set Cor Encode Add Au	ages in Lifetin e asse rtions rtions ns mu ize Err re Vari ize Crr itext V itext V itext V dit Det itext V Json V dit Det text V 1	n Poli me CC rtion must must st eve ror Re ariable: ariable: ariable a	ey anfigura must e evalua evalua aluate l esponse le authi le exp a le jwtp "JWT p le jsonh Token; "Signec le idtok	ation evalua ate to ate to to tru e e time a ayloa ayloa heade sign j d JWT cen.re onse	te to tru true true a String as Date/ te/Time d as Me d before ar as Str payload : \${sign sponse to Reg	and is i Time to ssage t e encod ring to: nedjwt. as Mes uesto	not er o: \${{ o: {"s ing: : {"kid comp ssage r	mpty gatev sub": \${jw ":"jw act}' to: {	(case vay.ti "\${us paylo tsigni "statu	e sens me} eer}"," ad.m; ng"}	iss": ainpa); If № "\${ga art}" nticat	Multin atew	value vay.clu "payle	d com uster.l	pare fi hostnai {"sub"	rst valu me}", :"\${us.	e only	,
Hom B Sav	e (ve an	id Act	CASS ivate	SOTe	e st [/ Save	tesi :	t /cass Valida														

• It shows Resolve External Dependencies Wizard. For CA SSO, please select "Change assertions to use this CA Single Sign-On configuration. "CA SSO".

4. Test CA SSO and CA API Gateway Integration

- Download PostMan (REST API Client) and execute it.
- In Postman, input the following information.
 - Method: GET
 - URL : https:// <API GW FQDN>:8443/casso/idtoken
 - User name: allmi01
 - Password: P@ssword01

get 🗸	https://apim:84	https://apim:8443/casso/idtoken								
Authorization •	Headers (1)		Pre-request Script							
Туре			Basic Auth		\sim					
Username			allmi01			The authorization header will be generated added as a custom header				
Password					Save helper data to request					
			Show Password							

Then, click "Send" button.

• After successful authentication in API Gateway, it returns JWT token.

Body	Cookies Headers (5) Test Results Status: 200 OK	Time: 576 ms
Pretty	Raw Preview JSON V	ūα
1 - 1		
2	"status": "authenticated",	
3 🕶	"payload": {	
4	"sub": "allmi01",	
5	"iss": "apim",	
6	"iat": 1539878468,	
7	"exp": 1539964868,	
8	"aud": "sso.apimca.com",	
9	"auth_time": 1539878468	
10),	
11	"jwt": "eyJaeXAi01XV1QL1C1hb6ci013Vz1UH1IsImtp2C16Tump3dHUp225pbmcifQ .ev0KInN1Y1I6ImFsb61pMDEiLA0KIm1zcy16ImFwaW0LA0KIm1hdC10HTUz0Tg30DQ2CWNCIJ1eHAi0jE1Mzk5NjQ4HjgsDQoiYXVkIjoic3NvLmFwaW1jYS5jb20iLA0KImF1d6 Uz0Tg30DQ20A0KfQ.Z6BRn86ey1FrzdpDw30H6DwP4XkuLnSBmelVguv81LKPqNvrQhhgK0-CEv1xtUT86-96MsAM_R0Pbuu86V8goNF8TZ3B28DdEcpjFay -oNFgj1t8RRTVSgtC1utU32Uxm_jBa2c60g8ojtcNP4eXttocvTf -Rw0wwrqmTUINi4ego2FEoVpNicaB87Nis3hYCzHfN0RiqxSuDUH6oGa8qXrWeQYP3ShN00JujFVDwSXUqkhdCbyhGZWeuR1s8NzQHahCK20sZ1E4a1SPp_1sExxSWcO -VIKVrjTRXxQNybD7XXKF426_q26DV7VvqH5c6-1413BE66Zhw0IXLUw"	hfdGltZSI6MT
12 }		

- After coping JWT toke and sends it to CA SSO protected web page. In Postman client, please input the following information.
 - Method: GET
 - URL : http//<Access Gateway FQDN>:7000/protected/debug.asp (Instead of debug.asp, any page can be used as long as it is existed in backed.)
 - Header : Authorization
 - Value : Bearer </br>

 Value : Bearer
 Value>

 (There is space between Bearer and

GET V http://sso.forwardinc.ca:7000/protected/debug	Para	
Authorization Headers (2) Body Pre-request Script	Tests	
Кеу	Value	Description
Authorization Cookie New key Response	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imp3dHNpZ2 5pbmcifQ.ew0KInN1YIIQsrFsbG1pMDBiLA0KImtzcyl6ImFwaW 0iLA0KImIhdCl6MTuzOTcxNDY5OCwNCiJleHAiOjE1Mzk4MDE w0TgsDQoiYXVkIjoic3NvLmFwaW1jYS5jb20iLA0KImF1dGhfd GltZ5I6MTUzOTcxNDY5OA0KfQ.kCIIMuWAqZw0112XMY9az_ 4vZz2siM2biQ9toRkFaYSvbPgY88vAj1nGwL45Fq2hg3dkURZC Afpw0KbIUYHv8QN2- 265GleMO0c05LN1eG9116enRDeBxx5NGzF8bypRykJisVtzE5D 7mN9oABcA3QxLfV_3v4mUcQfN09Ub1YvVI5bbG- gz4ga4TgrW-xOvMXHqwjKxh4GlvXkIyV-gZ- r2K4/iriZ729EQ93hpEb15zl4j- IkoxzgFlhLXixL85RANMKkQGAEBBHG7Et3RXQ10F8A1bNFyC p7DXjz0tHmIx- 1PjLOkp3GhalMA8X7wgCS_1YYobMdqIuuSgIXtA	

Click "Send" button

• It shows backend result after JWT Authentication.



After closing Postman client and execute again. It requests to access the resource, which is
protected JWT token without providing any token value. It rejects the request.

http://sso.forward	inc • +	No Environment	✓ ③ ‡
GET 🗸	http://sso.forwardinc.ca:7000/protected/debug.asp	Params Send	Save V
Authorization	Headers Body Pre-request Script Tests	0	Code
Туре	No Auth 🗸		
Response			
Body	Cookies Headers (7) Test Results		
Pretty	Raw Preview HTML V		
i 1-	KHTML>		
2 -	<head> <title>401: Access Denied</title></head>		
4			
6	<h1>401: Access Denied</h1>		
7	 		
8			