Using IIS with Smartcard Authentication in ALM 12.x

This guide contains additional detail to what is described in the ALM External Authentication Guide. Specifically, it contains illustrations and expanded troubleshooting.

CONFIGURATION

Step: Create server farm



Step: Add server

1. Define ports in Advanced Settings BEFORE clicking on Add

- 2. Now enter server name
- 3. Click on Add

	IF		
		Create Server	Farm
Add Serve	r		
Server a. 2.s:			3
alm11.test.nt			Add
Online .		l	\sim
Hide advanced settings		[Remove
⊿ applicationRequestF	louti 🚺		
httpPort	8080		
httpsPort	8443		
weight	100		
Server Address	Status		
our creation	otatas	_	
L			

- 4. Click on Finish
- 5. Click Yes in the Rewrite Rules dialog box that opens

Step: Select proxy settings for your Server Farm

- Select the new Server farm element created.
- Double-click Proxy.

Step: Edit Proxy settings

- 1. Set Time-out (seconds) to 35.
- 2. Change Forward encoded client certificate in the following header:

Set it to CERT (as expected by ALM, or change in ALM to match what you have here)

- 3. Set Response buffer threshold to 0.
- 4. Click Apply

File View Help	
Connections Start Page Start Page IIS8-SRP (IIS8-SRP\Administrator) Application Pools A-G Sites ↓ - O Default Web Site Server Farms ↓	Viscon Proxy Use this feature to configure proxy settings for Application Request Routing. HTTP version: Pass through V Keep alive Time-out (seconds): 35 V Reverse rewrite host in response headers Custom Headers Preserve client IP in the following header: X-Forwarded-For I Include TCP port from client IP Forward encoded client certificate in the following header: CERT Amark request logs with GUIDs in the following header: X-ARR-LOG-ID
	Buffer Setting Response buffer (KB): 4096 Response buffer threshold (KB): 0

Step: Select Proxy at Server Level

Select the main tree node (the server name), click Application Request Routing 0 Cache,



 \circ $\;$ and then click Server Proxy Settings in the Proxy section.



Step: Enable proxy at server level

- 1. Check Enable proxy
- 2. Verify that HTTP version is valued with Pass Through.
- 3. Verify that **Reverse rewrite host in response headers** is enabled.
- 4. Click Apply

8)	Internet Information Services (IIS
€ IIS8-SRP →	
File View Help	
File View Help Connections Start Page Start Page Start Page Start Page Start Page Stres Default Web Site Server Farms D-1, ALM D-1, PC	Application Request Routing Use this feature to profigure proxy settings for Application Request Routing. Proxy Setting HTTP version: Pass through (Keep alive Time-out (seconds): 120 Reverse rewrite host in response header Custom Headers Preserve client IP in the following header: X-Forwarded-For Include TCP port from client IP Forwarding proxy header value: Cache Setting Memory cache duration (seconds): 60 Enable request consolidation Query string support: Ignore query string Version and the set of the
Configuration: 'localhost' applicationHost.co	nfia
Configuration: 'localhost' applicationHost.co	ntig

Step: Test Proxy

- Restart IIS webserver
- Verify you can now connect to your ALM site using the following URL: <u>http://IIS/qcbin</u>

Step: Configure IIS as secure reverse proxy

- Import server certificate
- Edit binding
- Ensure that the IIS server trusts the Root Authority certificate of the Certificate Authority that

issued the ALM server certificate.

Step: Test Secure reverse proxy

• Verify you can now connect to your ALM site using the following URL: <u>https://IIS/qcbin</u> Note: If anything goes wrong at any point, delete your Server Farm and start again.

Step: IIS to require a client certificate

• Configure IIS to require a client certificate



- Configure trust to the authority that issued your client certificate:
 - View client certificate and copy to file both Root CA and intermediate CA certificates in base-64 format.
 - Import Root CA certificate into the Trusted Root CA list under the local computer
 - Import Intermediate CA certificate into the Intermediate CA list under the local computer
 - Starting Window 2012: also import the same certificates into Client Authentication Issuers

Step: Test with client certificate

 Verify you can open ALM URL: <u>http://IIS/qcbin</u> after presenting your smartcard certificate though login to ALM is still via ALM login screen (you have not yet enabled External Authentication in ALM)

Step: Handling secure channel termination endpoint

• There is an additional configuration needed depending on where secure channel terminates. If it terminates on ALM it is called *Full SSL* or, if it terminates on the front end webserver, it is called *SSL Offloading*. The table below helps to identify whether or not ALM requires SSL. Basically, if ALM is configured to require SSL you will be able to access it over https, but not over http.

ALM requires SSL	Test	Expected Result
Υ	Open <u>http://ALM:8080/qcbin</u>	Should fail
Υ	Open https://ALM:8443/qcbin	Should load

Ν	Open <u>http://ALM:8080/qcbin</u>	Should load

Full SSL (endpoint=ALM)

If ALM server requires SSL, you need to perform the following in order to avoid HTTP error 502:

• Select the main tree node (the server name), click URL Rewrite

V				Inte	ernet Inform	nation Servi	ces (IIS) Mar	nager			
€ SRP →											
File View Help											
Connections Connections Connections Connections Connections	Eiltan	8-SRP Ho	ome	- Show All	Group but A		- 📼 -				
IS8-SRP (IIS8-SRP\Administrator) Application Pools Sites Default Web Site		.2	2			404				n	
A ∰ Server Farms ▶ -₩ ALM ▶ -₩ PC	Application Request R	Authentic	c. ression	Default Document	Directory Browsing	Error Pages	Failed Request Tra	Handler Mappings	HTTP Respon	Logging	MIME Ty
	411 Modules	Output Caching	Request Filtering	Server Certificates	URL Rewrite Provid	Worker Processes les URL and co	ontent rewriting	capabilities b	ased on rules.]	
	Manageme Configurat Editor	nt Feature Delegation	Shared Configurat								

Desktops Loois Help							
	Internet Information Services (IIS) Manager						
€ IIS8-SRP →							
File View Help							
Connections							Actions
🔍 - 🔄 🖄 🕵							Add Ru
Start Page	Provides rewriting capabilities ba	sed on rules for the requ	uested URL address and the conten	it of an HTTP response.			Manag
Application Pools	Inbound rules that are applied to	the requested URL add	ress:				View S
⊿ - 🙆 Sites	Name	Input	Match	Pattern	Action Type	Action U	Manag
👂 😌 Default Web Site	🗄 🧮 ARR_ALM_loadbalance	URL Path	Matches	(^qcbin(.*))	Rewrite	https://A	View R
⊿ 🚛 Server Farms	🗄 🚞 ARR_PC_loadbalance	URL Path	Matches	(^loadtest(.*)) (^snv(.*))	Rewrite	https://P	View P
							Outbound
							View P
							View C
							🕢 Help
						I	

- Open the URL Rewrite Rule for **qcbin**
- Expand server variables list and make sure it is empty
- Change the protocol in **Scheme** field from **http** to **https**.

• 🗔 🕅 👷	🛛 🌒 Edit	Inbound Rule			
📲 Start Page	Pattern:				
IIS8-SRP (IIS8-SRP\Administrator)	(^acbin(.*))				
Application Pools					
⊿ - 👩 Sites	Janore ca				
A Server Farms	ignore ca.	,c			
⊳ II ALM					
⊳ 	Conditions				
	Conditions				
	Server Variable	25			
	Name	Value	Repla	ce	
	Action				
	Action type:				
	Route to Ser	ver Farm 💌			
	A.1. B				
	-Action Prop	erties			
	Scheme:	Server farm:		Path:	
	https://		~	/(B:0)	
	(incepsit)		•	[vir. and	

SSL Offloading (endpoint=IIS)

Otherwise, if secure channel terminates on IIS and ALM server does not require SSL:

- Edit the qcbin inbound rule and add the following server variable: Set name="HTTP_X_FORWARDED_PROTO" value="https".
- 2. In **Action Properties**, change the protocol from **https** to **http**.

l 🔤 📴 Start Page	Edit	Inbound Rule				
IS8-SRP (IIS8-SRP\Administrator)	Input	Туре	Pattern		Add	
Application Pools Sites					Edit	
Default Web Site Server Farms					Remove	
⊳- ⊪ 5 ALM ⊳- ⊪ 5 PC					Movella	
					move op	_
					Move Dow	n
	Name UTTD X 50	PWARDED BROTO	Value	Replace	Add	
	HTTP_X_FO	RWARDED_PROTO	https	True	Edit	
					Remove	
					Move Up	
	<		ш		> Move Dow	n
	Action Action type: Route to Ser Action Prop	ver Farm v http erties	כ			

• Restart IIS so it will read the configuration.

Step: Configure External Authentication in ALM

- In ALM Site Admin, use External Authentication wizard
- If needed provide custom pattern to extract user id from the certificate (see below).
- Keep administrator session open in the browser
- Test login from a separate session
- If user can login to ALM using smartcard, you are done
- Otherwise, see Troubleshooting below

TROUBLESHOOTING

To see the details of failure in IIS, enable Tracing in IIS:

- 1. Go to Default WebSite
- 2. Failed Requests Tracing Rules [if you don't see it, use Server Manager to Add Role and Feature]
- 3. Add trace:
 - a. Actions->Add
 - b. Status codes: 403 (access denied) or 403-405, etc
- 4. Edit site tracing
- 5. Click on enable
- To view failed request, open latest file in %SystemDrive%\inetpub\logs\FailedReqLogFiles



10/19/2015 2:27 PM - Screen Clipping

- 1. Problem loading ALM URL
 - a. Error: HTTP 403-Forbidden: Access is denied.
 - b. IIS tracing shows the detail:

ModuleName="IIS Web Core", Notification="BEGIN_REQUEST", HttpStatus="403", HttpReason="Forbidden", HttpSubStatus="16", ErrorCode="A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider. (0x800b0109)", ConfigExceptionInfo=""

- c. Solution:
 - i. View client certificate and copy to file both Root CA and intermediate CA certificates in base-64 format.
 - ii. Import Root CA certificate into the Trusted Root CA list under the local computer
 - iii. Import Intermediate CA certificate into the Intermediate CA list under the local computer
 - iv. Needed starting Window 2012: We also imported the same certificates into Client Authentication Issuers
 - v. This next step was crucial in this case as evidently IIS could not tell that Intermediate CA certificate was not Root CA. (Possibly wrong indicator on the certificate itself). In this case, we had to import the Intermediate CA certificate into the Trusted **Root** CA list.
- 2. Problem loading ALM URL:

Error: HTTP 502 (bad gateway).

SSL is required on the ALM server, but the IIS URL Rewrite Rule contains an indicator for SSL offloading.

Resolution:

If the ALM server requires SSL, remove the HTTP_X_FORWARDED_PROTO server variable from the URL Rewrite Rule for qcbin and change Scheme from http to https.

- 3. Problem login to ALM
 - a. Error: Certificate not valid
 - b. ALM sa logs: certificate revoked (not true, but real problem: it could not reach CRL server)
 - c. Workaround:
 - i. add site parameter to disable this check on ALM (IIS already does it):
 - 1. EXTERNAL_AUTH_CERTIFICATE_CRL_CHECK = N
- 4. Problem login to ALM
 - a. Error: Cannot find valid ALM user. No ALM user was found for given external authentication data
 - b. Solution:
 - i. Set pattern to look for uid in the subject of the cert. E.g.:

.*?[uU][iI][dD].*= *([\d]+).*

- ii. User in ALM must have the same UID value in the Description field.
- iii. Either manually update it with the content of appropriate attribute in ActiveDirectory (using Attribute Editor) or import from LDAP

- 5. Problem login to ALM when using custom pattern
 - a. Error: Cannot find valid ALM user. No ALM user was found for given external authentication data
 - b. Solution:
 - i. Test your pattern using <u>http://myregexp.com/</u>
 - 1. Enter pattern you want to test. Make sure there are no spaces left at the tail end of the pattern.
 - 2. Enter your string to test. This should be copied from the certificate or from the LDAP, or it could be obtained from the ALM site admin logs (see below).
 - Look at the bottom of the screen for pattern match under Capture Group #1
 Important: If you do not get result under Capture Group #1, you do not have the right pattern

How to see the contents of the certificate passed to ALM in a request header:

- 1. Enable DEBUG on Site Admin logs
- 2. Add site parameter DUMP_REQUEST_HEADERS with value 'Y'.

For example, this pattern .*?[oO][iI][dD].*= *($[\d]$ +).* will look for string that starts with OID, is followed by any number of characters, up to the equal sign, followed by any number of digits (we place parentheses around this group to indicate to ALM that this is the string we want captured).

Regular Expression	Text to test	Capture group #1 (ALM will use it)
.*?[oO][il][dD].*= * <mark>([\d]+)</mark> .*	OIDxdsadads1.1.2.3.4.5.66666666= <mark>123</mark> ,CN=My Test	<mark>123</mark>



This is sandbox to test JavaScript regular expression. To test JAVA regular expression you can use java-

Regular expression (JavaScript)	.* is for any number of characters
.*?[o0][iI][dD].*= *([\d]+).*	

Text to test

DIDxdsadads1.1.2.3.4.5.66666666=123	CN=My Test Jal UID are ts after the al sign and efore the comma

Capture groups

