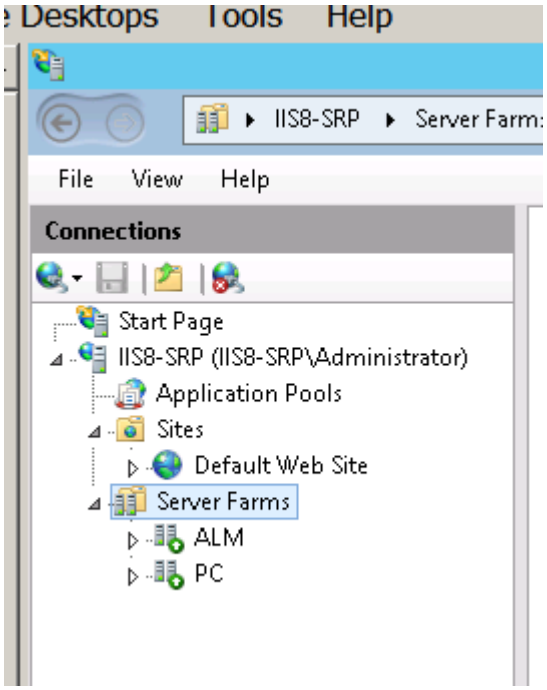
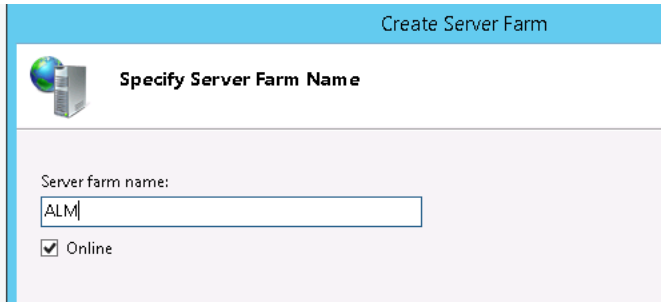
Using IIS with Smartcard Authentication in ALM 12.x

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

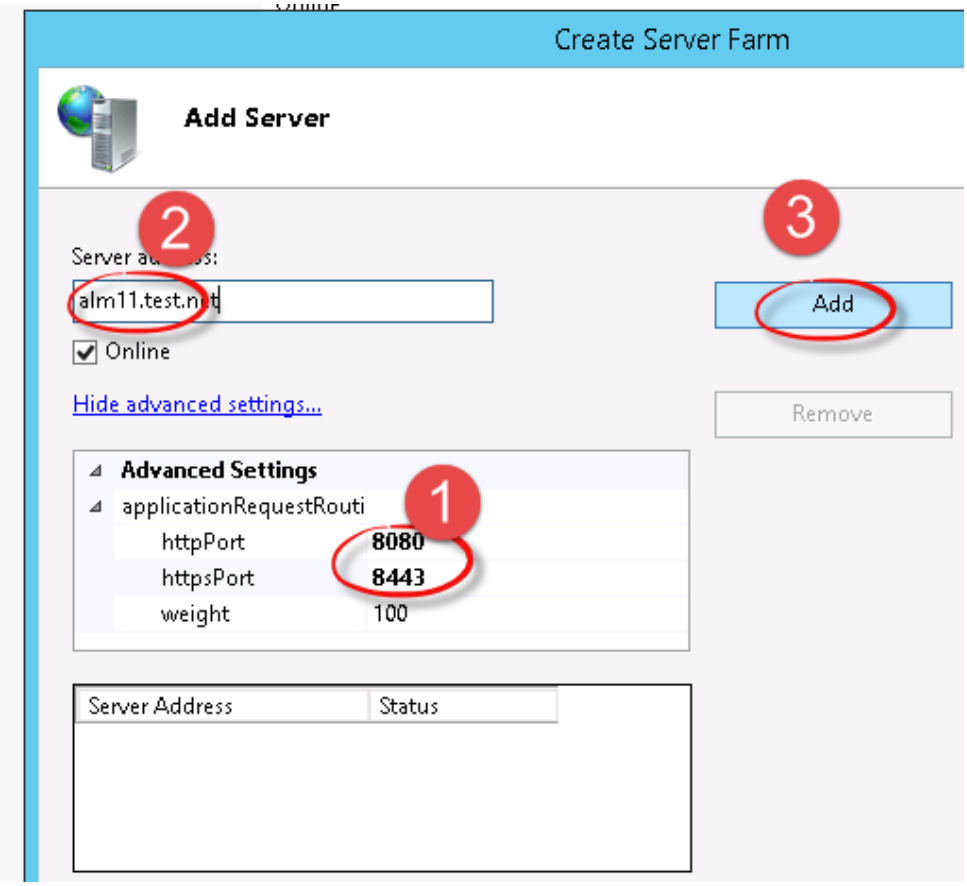




Step: Add server

1. Define ports in Advanced Settings BEFORE clicking on Add

2. Now enter server name
3. Click on Add



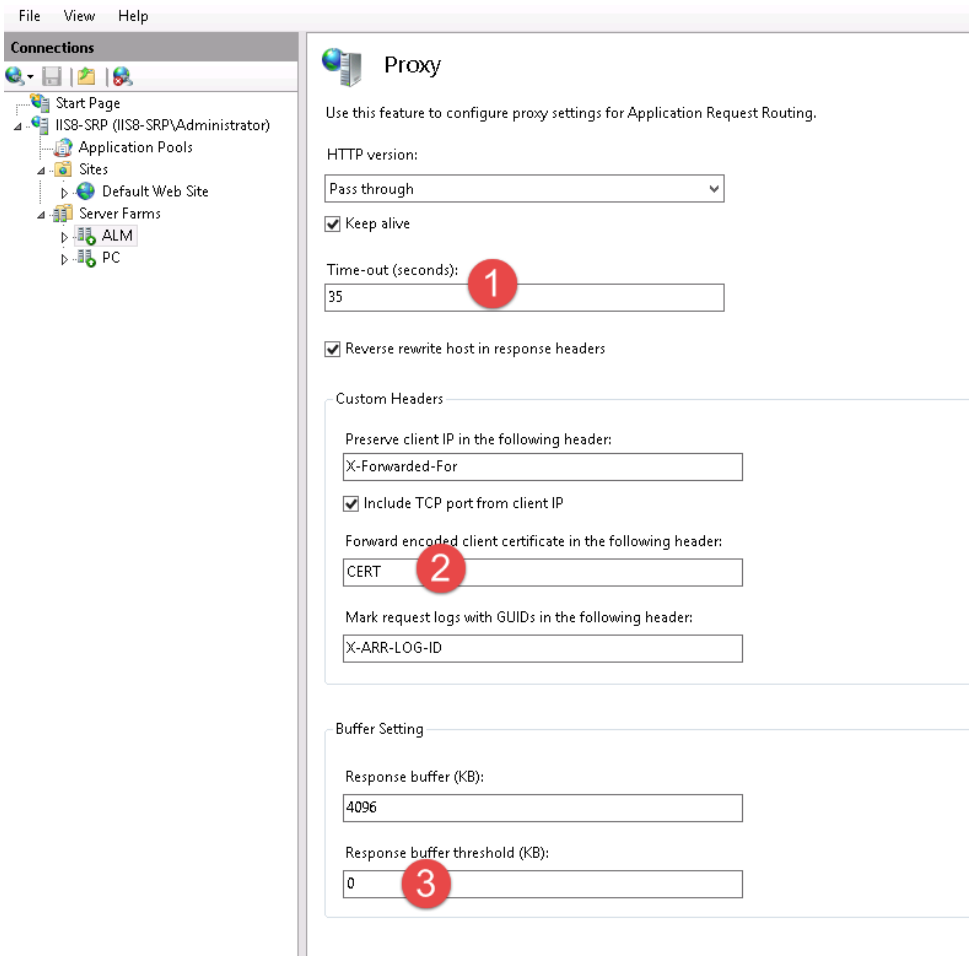
4. Click on Finish
5. Click Yes in the Rewrite Rules dialog box that opens

Step: Select proxy settings for your Server Farm

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

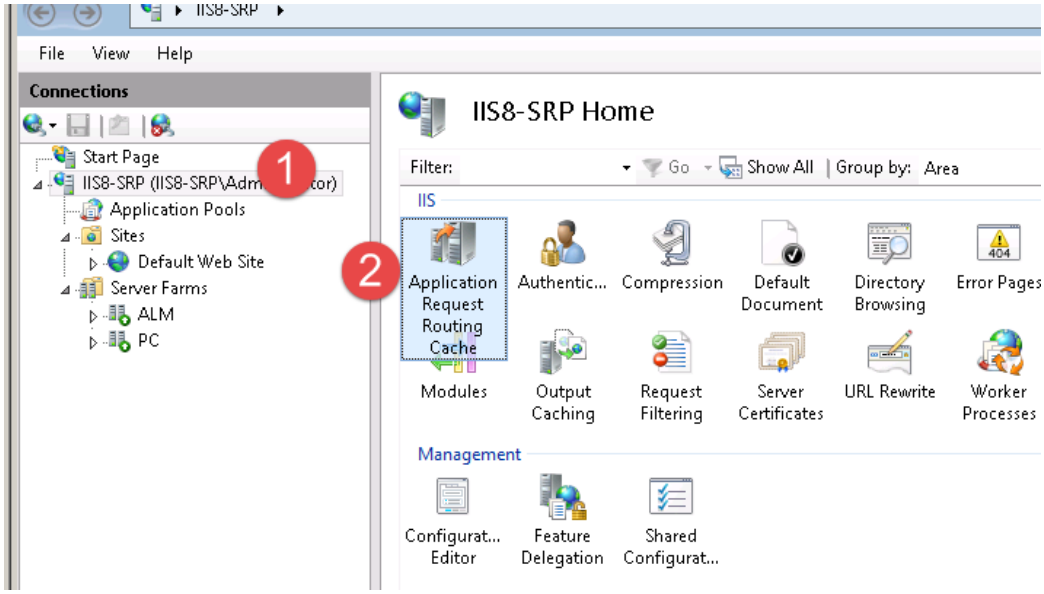
Step: Edit Proxy settings

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

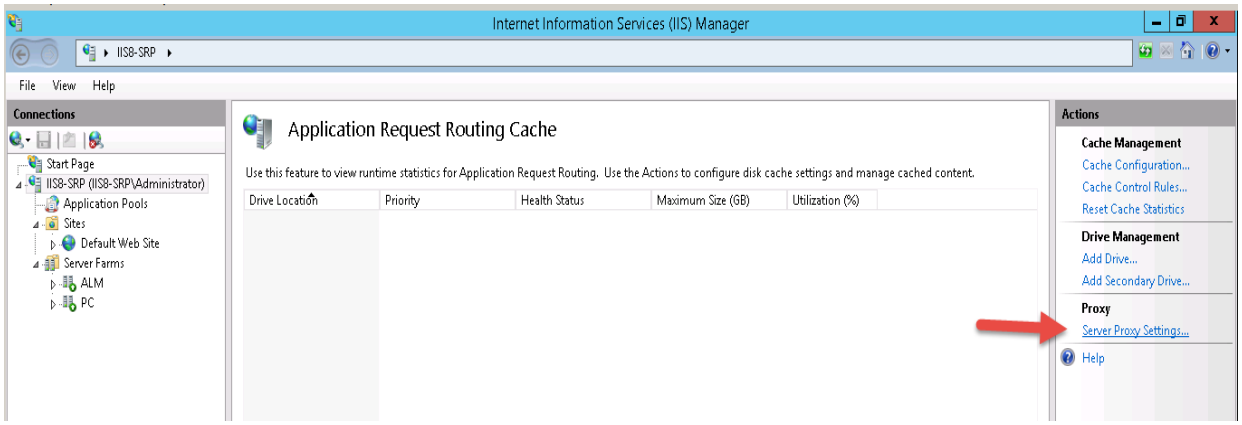


Step: Select Proxy at Server Level

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

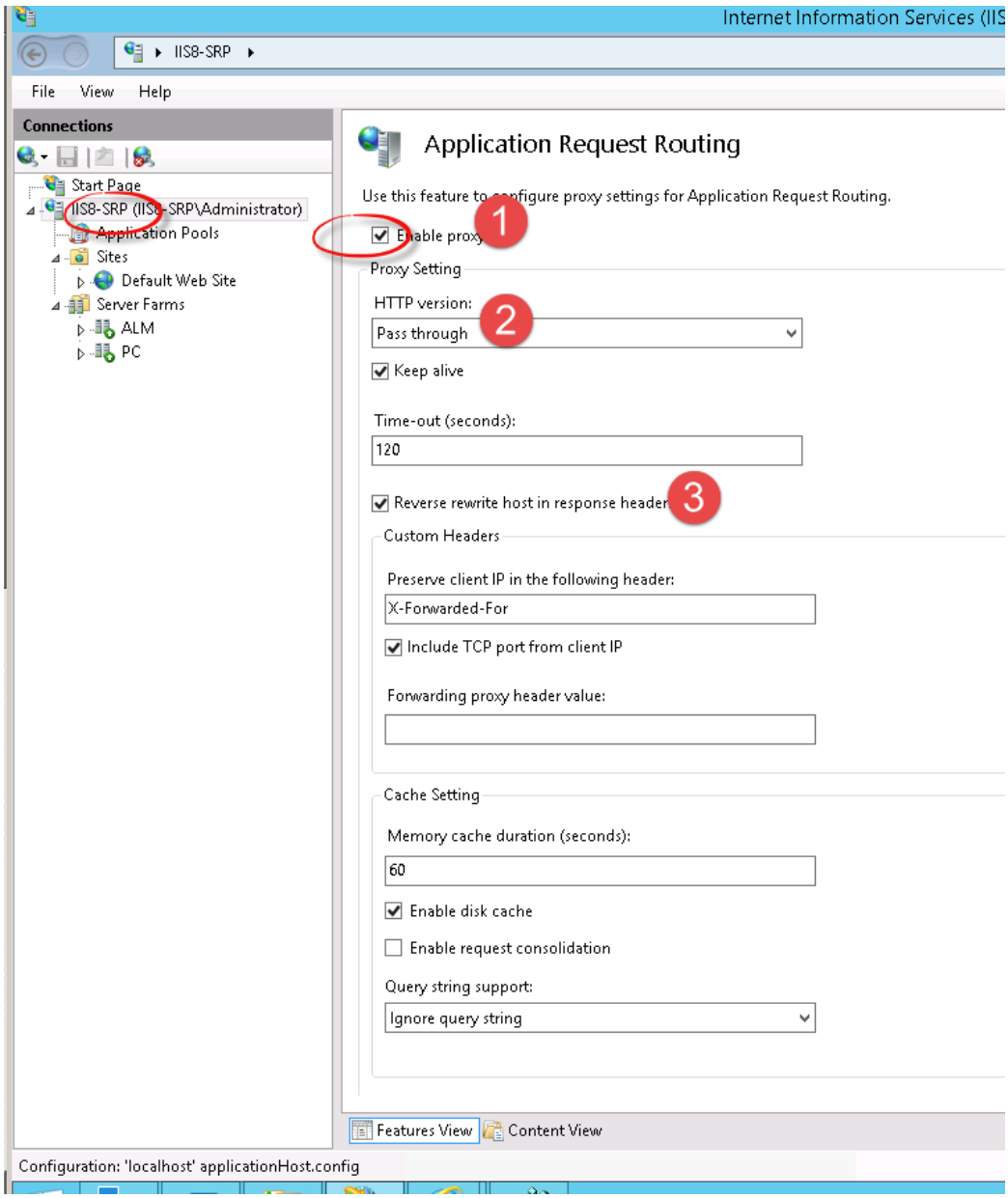


- and then click Server Proxy Settings in the Proxy section.



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



Step: Test Proxy

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

Step: Configure IIS as secure reverse proxy

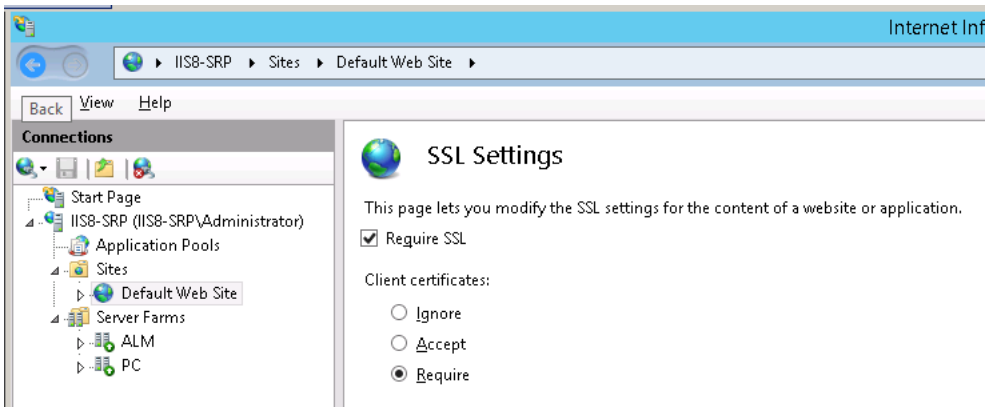
- Import server certificate
- Edit binding
- Ensure that the IIS server trusts the Root Authority certificate of the Certificate Authority that
  issued the ALM server certificate.

Step: Test Secure reverse proxy

- Verify you can now connect to your ALM site using the following URL: https://IIS/qcbin
  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: http://IIS/qcbin 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.

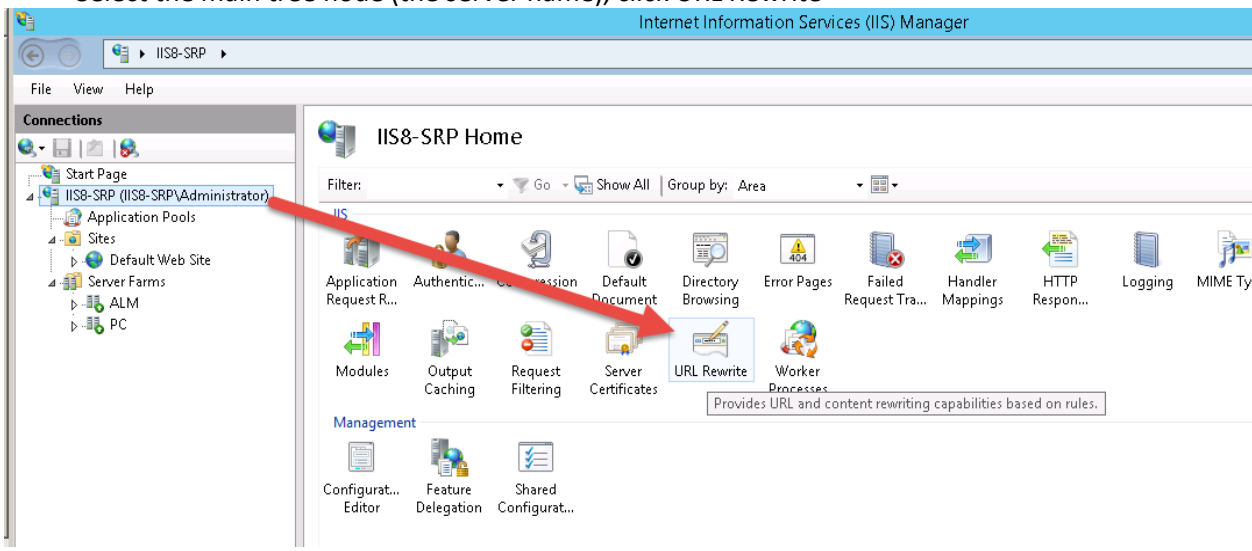
ALM requires SSL	Test	Expected Result
Y	Open http://ALM:8080/qcbin	Should fail
Y	Open https://ALM:8443/qcbin	Should load

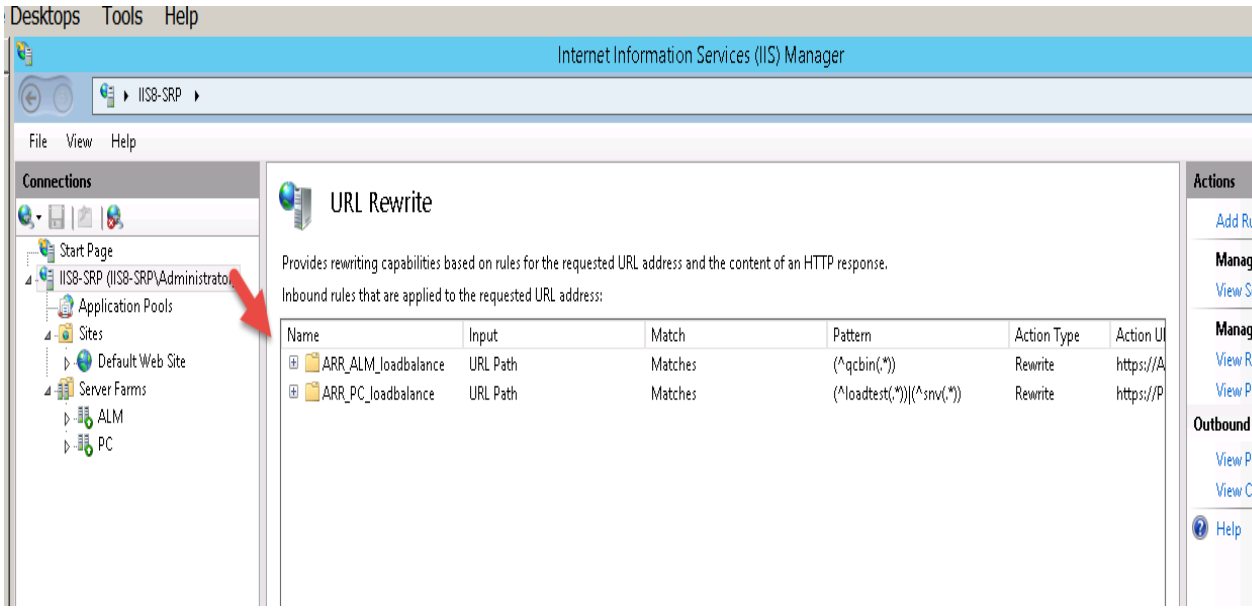
N	Open http://ALM:8080/qcbin	Should load

Full SSL *(endpoint=ALM)*

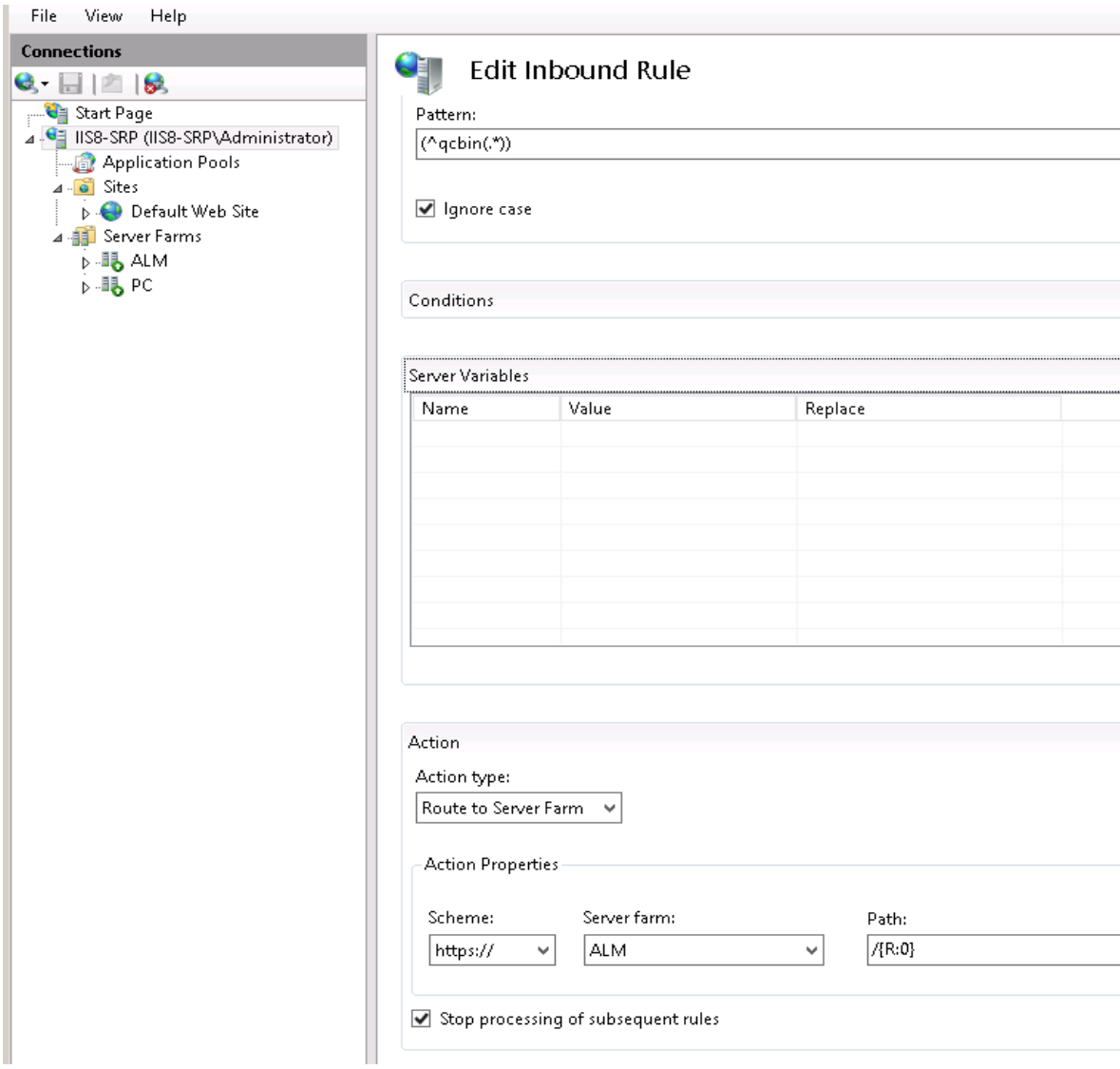
If ALM server requires SSL, you need to perform the following in order to avoid HTTP error 502:

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





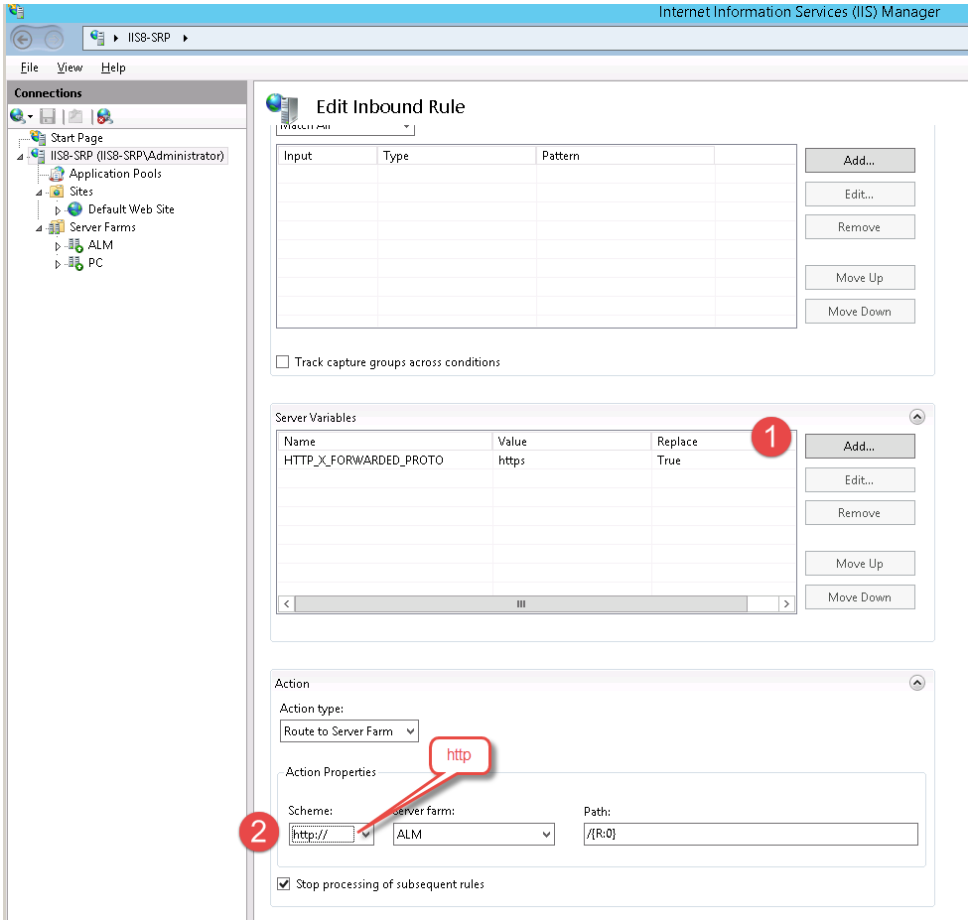
- Open the URL Rewrite Rule for **qcbin**
- Expand server variables list and make sure it is empty
- Change the protocol in **Scheme** field from **http** to **https**.



SSL Offloading *(endpoint=IIS)*

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

1. 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**.



- Restart IIS so it will read the configuration.

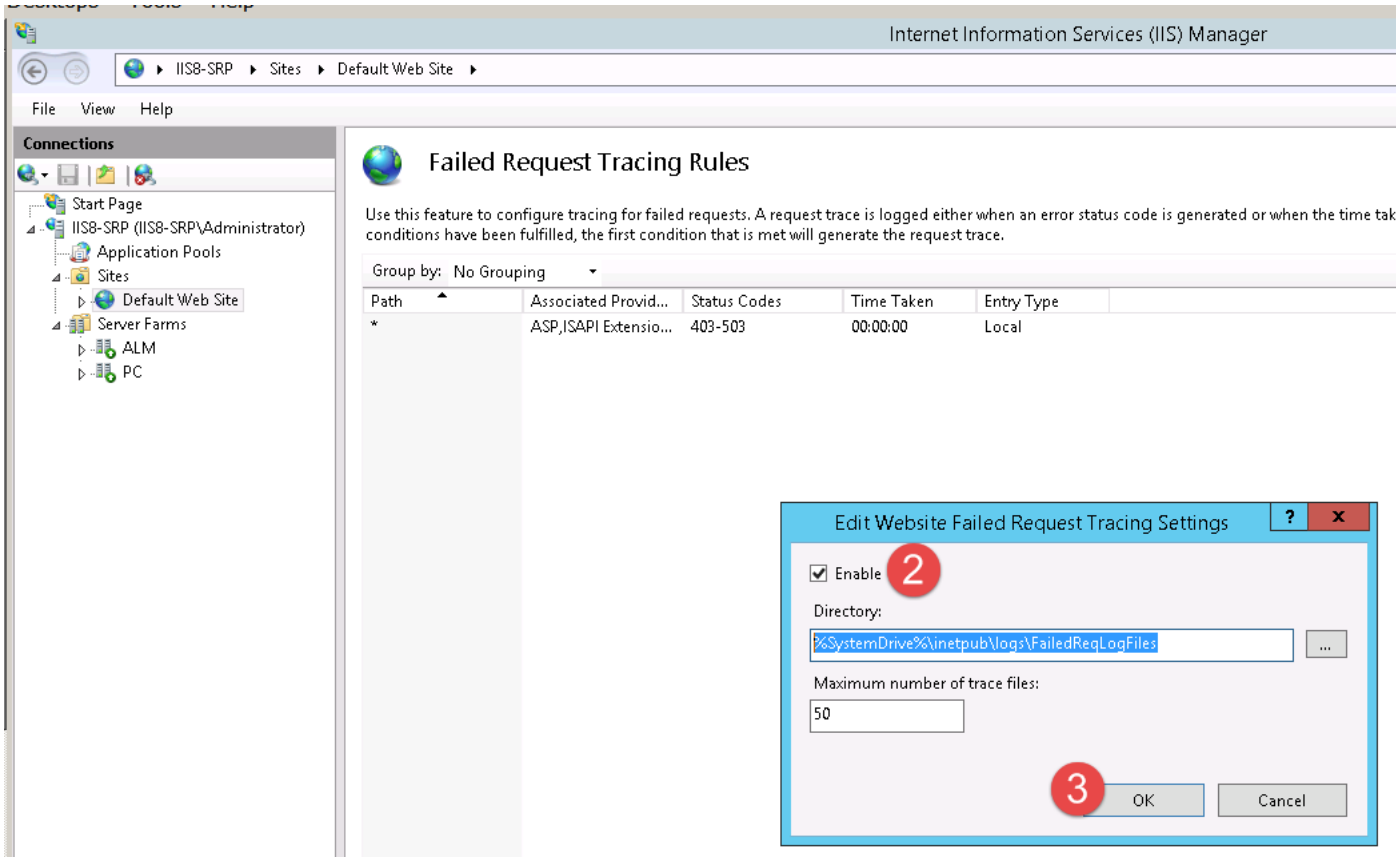
Step: Configure External Authentication in ALM

- 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
6. 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

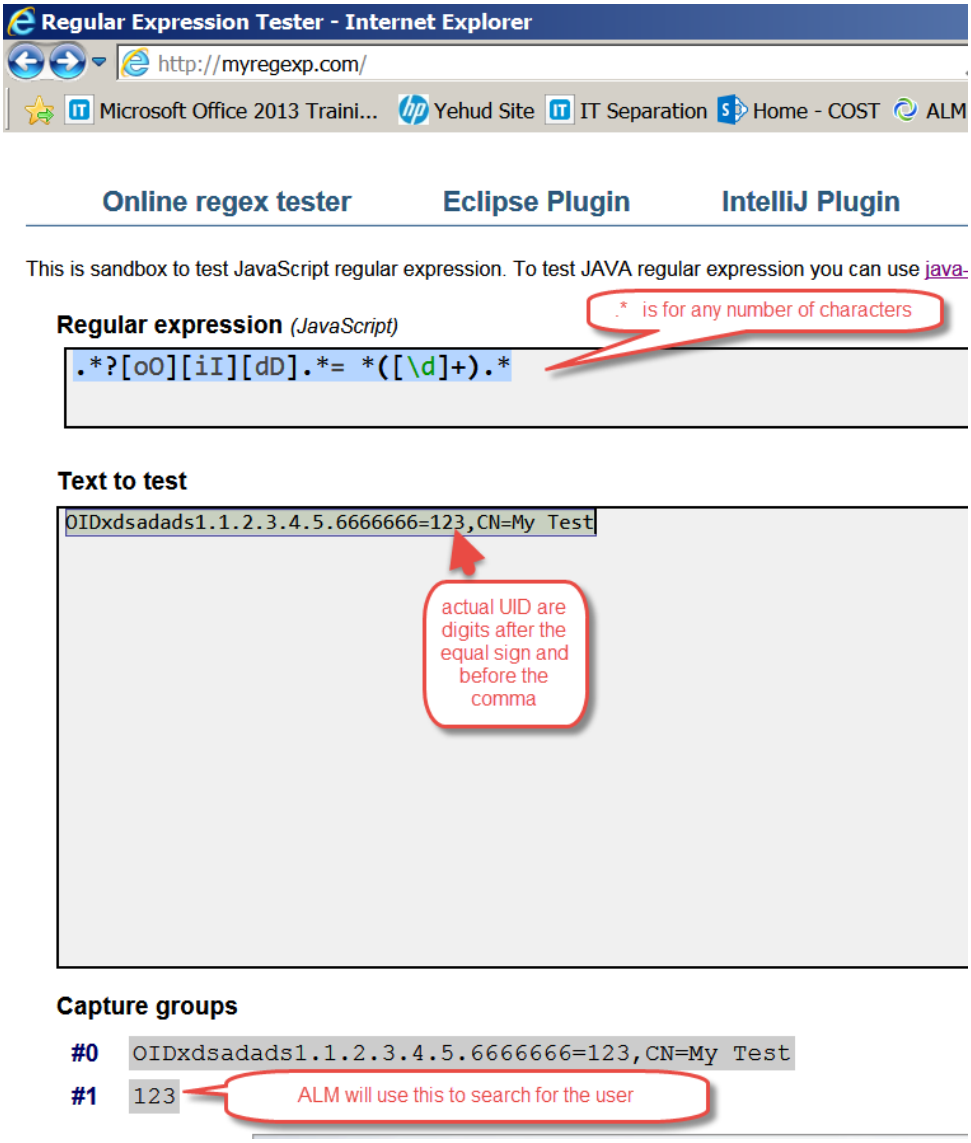
5. Problem login to ALM when using custom pattern
    a. Error: Cannot find valid ALM user. No ALM user was found for given external authentication data
    b. Solution:
        i. Test your pattern using http://myregexp.com/
            1. Enter pattern you want to test. Make sure there are no spaces 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).
            3. 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][iI][dD].*= *([\d]+).*	OIDxdsadads1.1.2.3.4.5.6666666=123,CN=My Test	123


Regular Expression Tester - Internet Explorer
http://myregexp.com/
Microsoft Office 2013 Traini...
Yehud Site
IT Separation
Home - COST
ALM
Online regex tester
Eclipse Plugin
IntelliJ Plugin
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
.*?[oO][iI][dD].*= *([\d]+).*
Text to test
OIDxdsadads1.1.2.3.4.5.6666666=123,CN=My Test
actual UID are digits after the equal sign and before the comma
Capture groups
#0 OIDxdsadads1.1.2.3.4.5.6666666=123,CN=My Test
#1 123
ALM will use this to search for the user