TACACS and Radius Authentication for Management Login to WLC

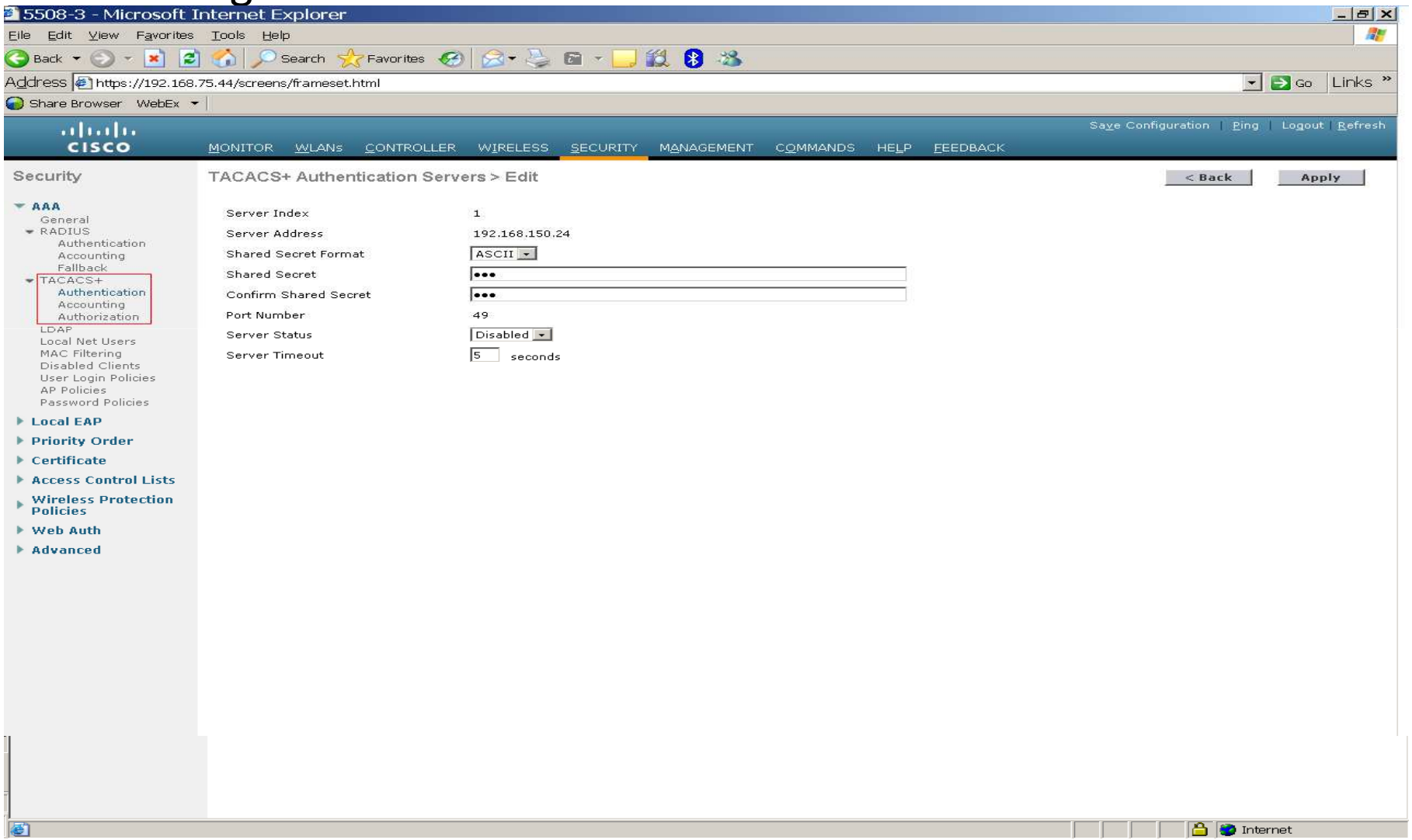
Nasir Majeed

Management Login to WLC

- 3 Methods to add users to login to the WLC for management
- Local User on the WLC
- TACACS Account on ACS
- RADIUS Account on ACS

Management Login to WLC using TACACS Account on ACS 4.2

- Configuration of WLC

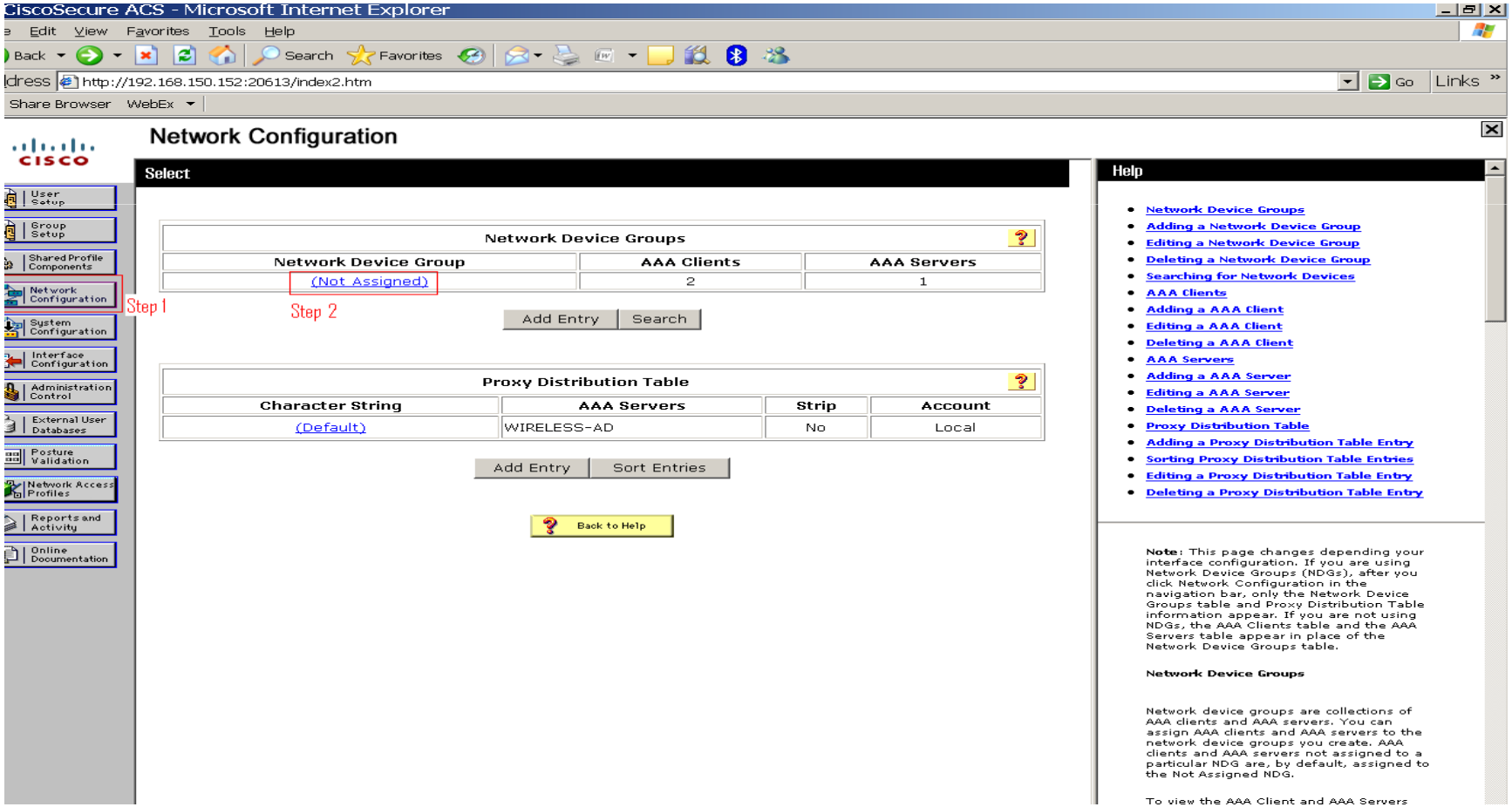


Configure WLC to use TACACS for Login to the GUI of WLC.

- We will need to change the Local Management Authentication on the WLC GUI→ Security, as shown below:

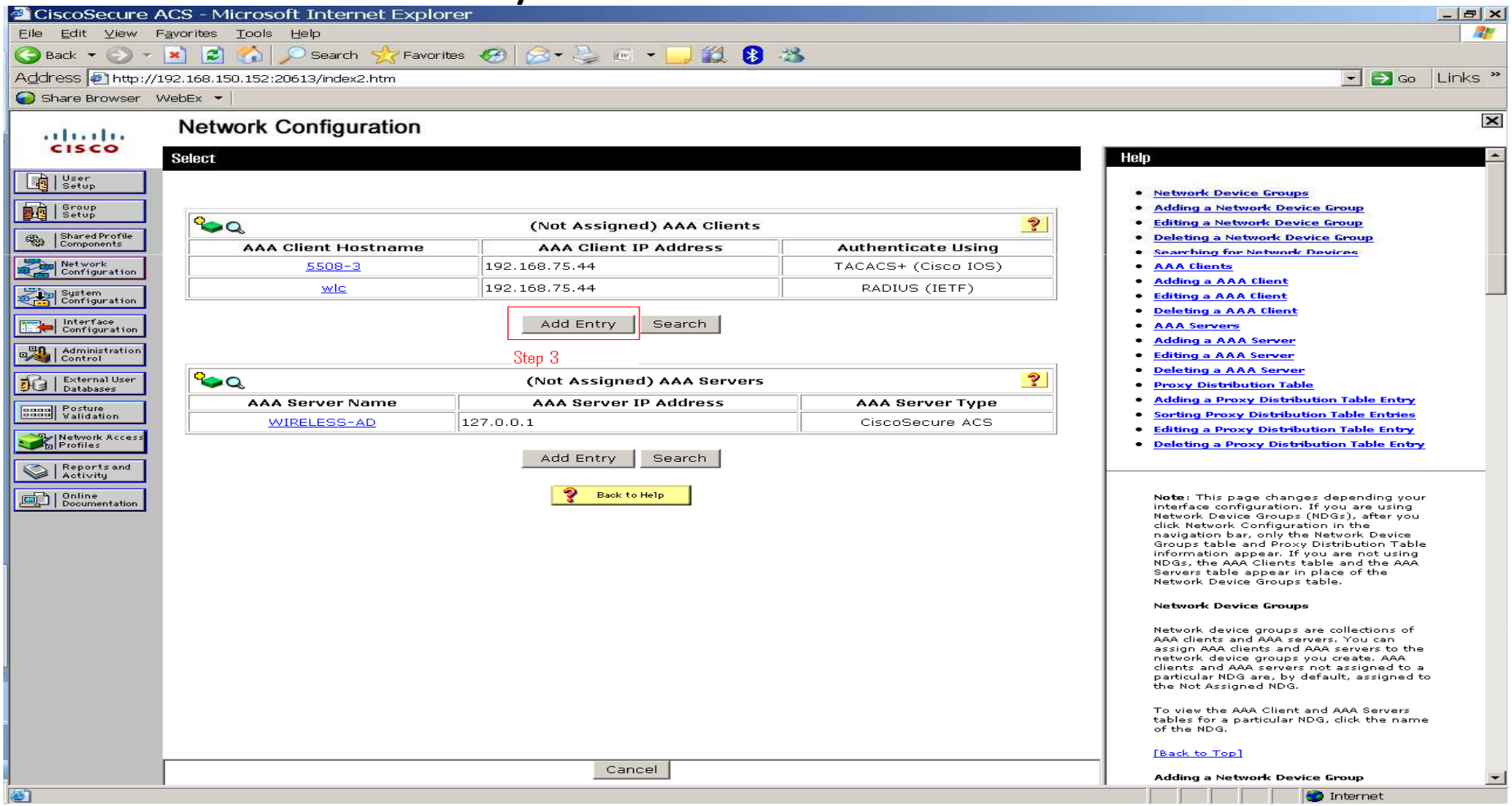
Management Login to WLC using TACACS Account on ACS 4.2

- Add WLC as AAA client on ACS.



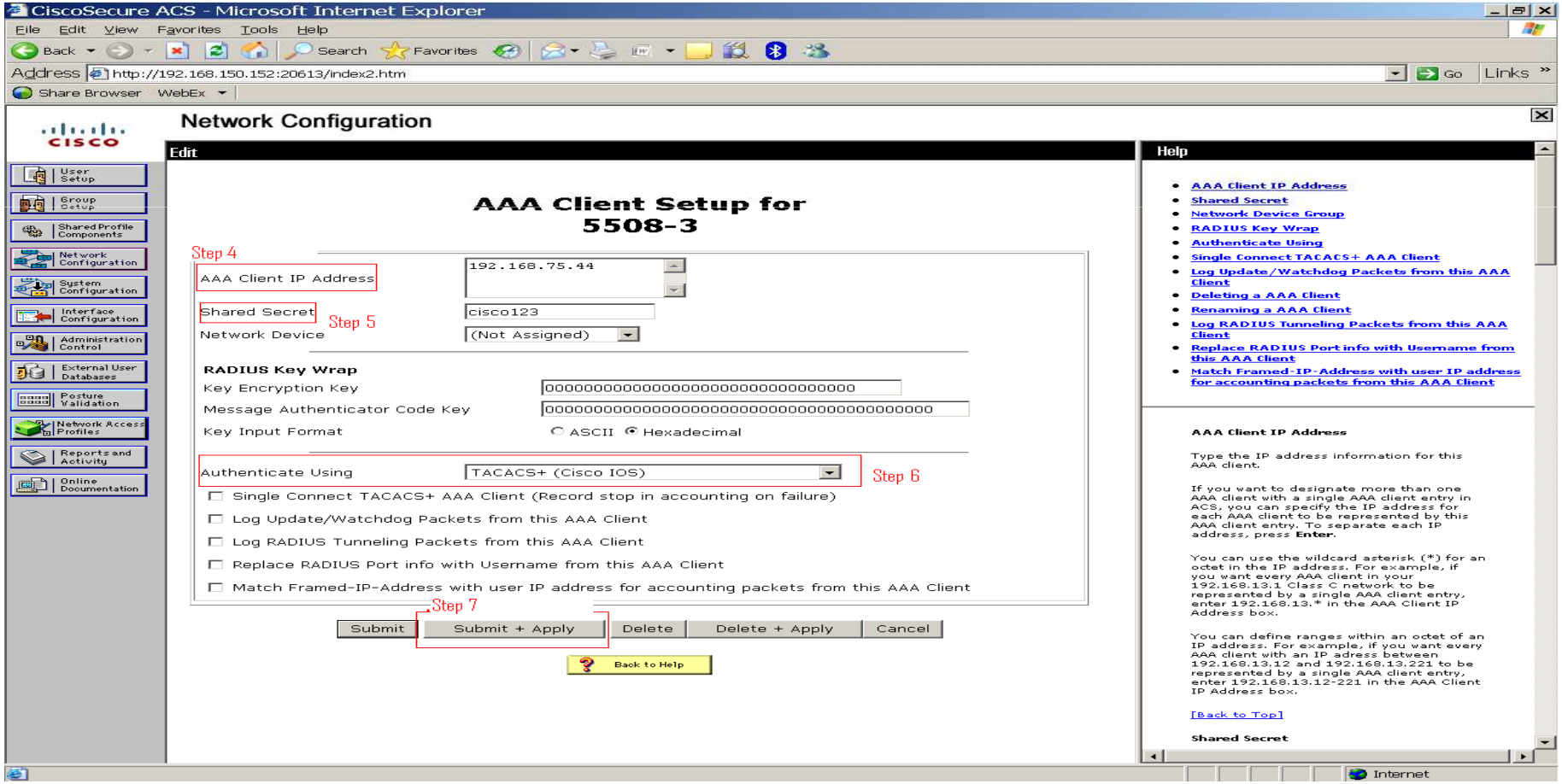
Management Login to WLC using TACACS Account on ACS 4.2

- Click on Add Entry to add the WLC.



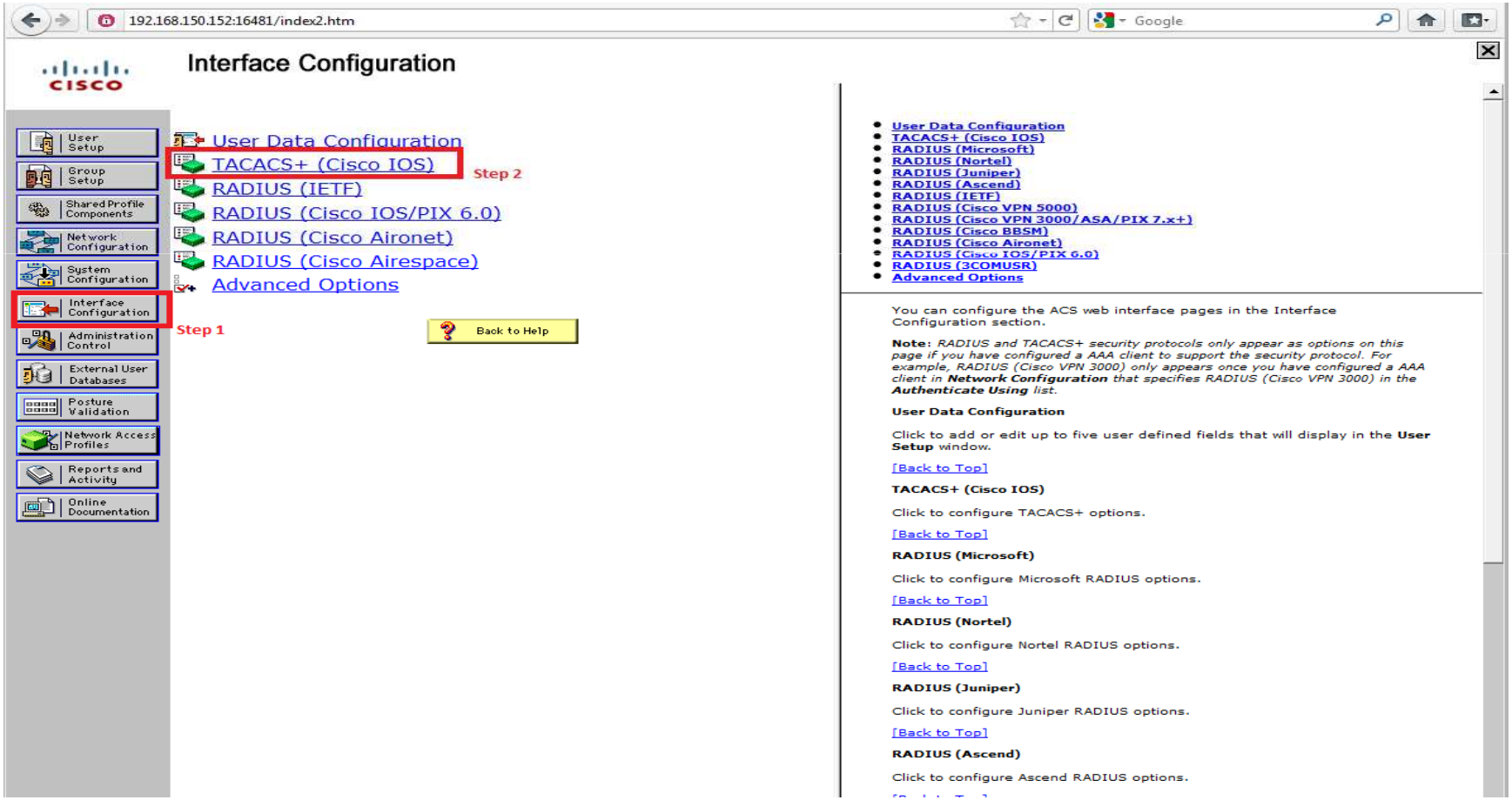
Management Login to WLC using TACACS Account on ACS 4.2

- Add IP address of WLC, Shared Secret and also add the method of Authenticate user TACACS+ (Cisco IOS)

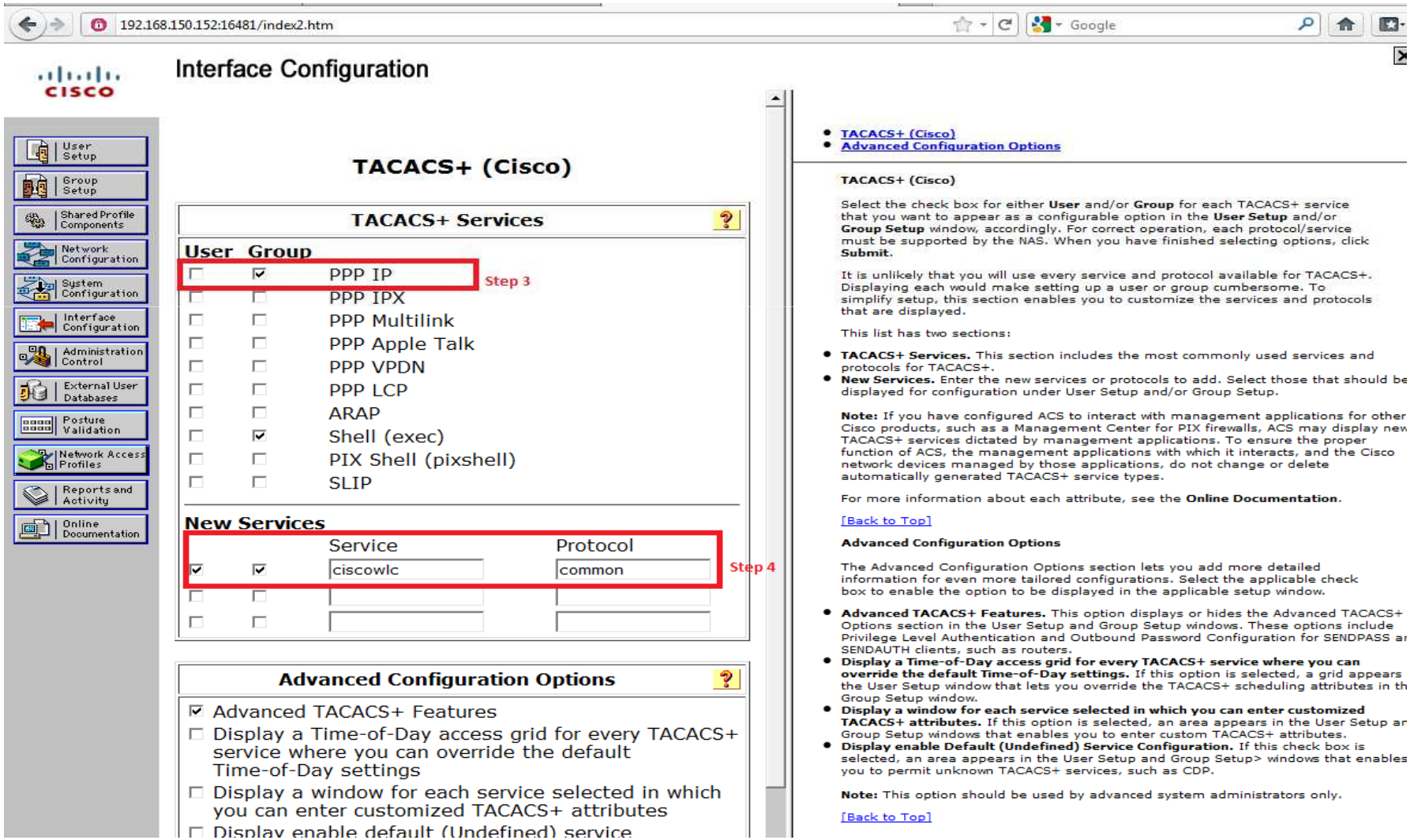


Configure ACS 4.2 Server to Allow TACACS Protocol to login

- Configure the ACS to allow Cisco WLC attribute

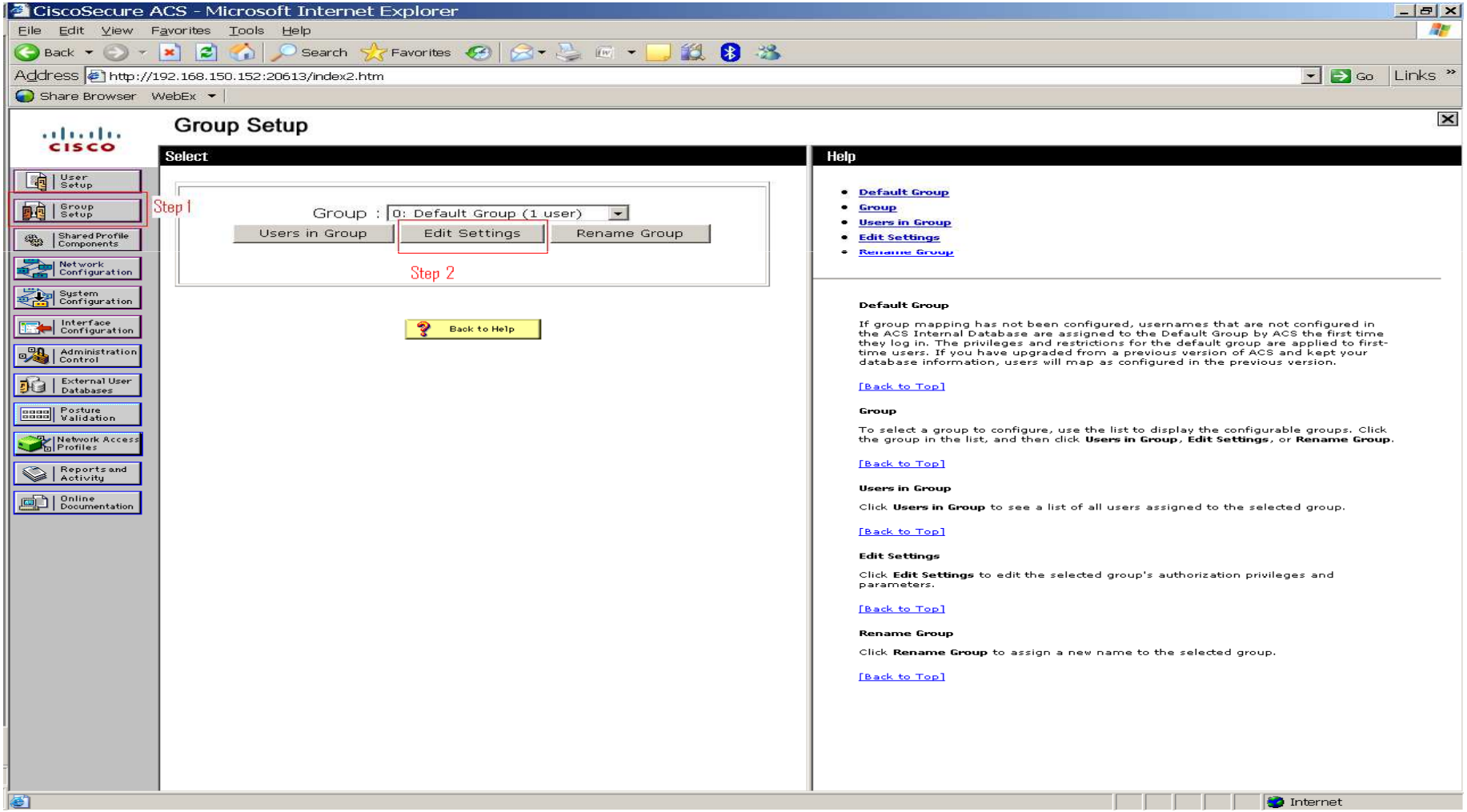


Configure ACS 4.2 Server to Allow TACACS Protocol to login



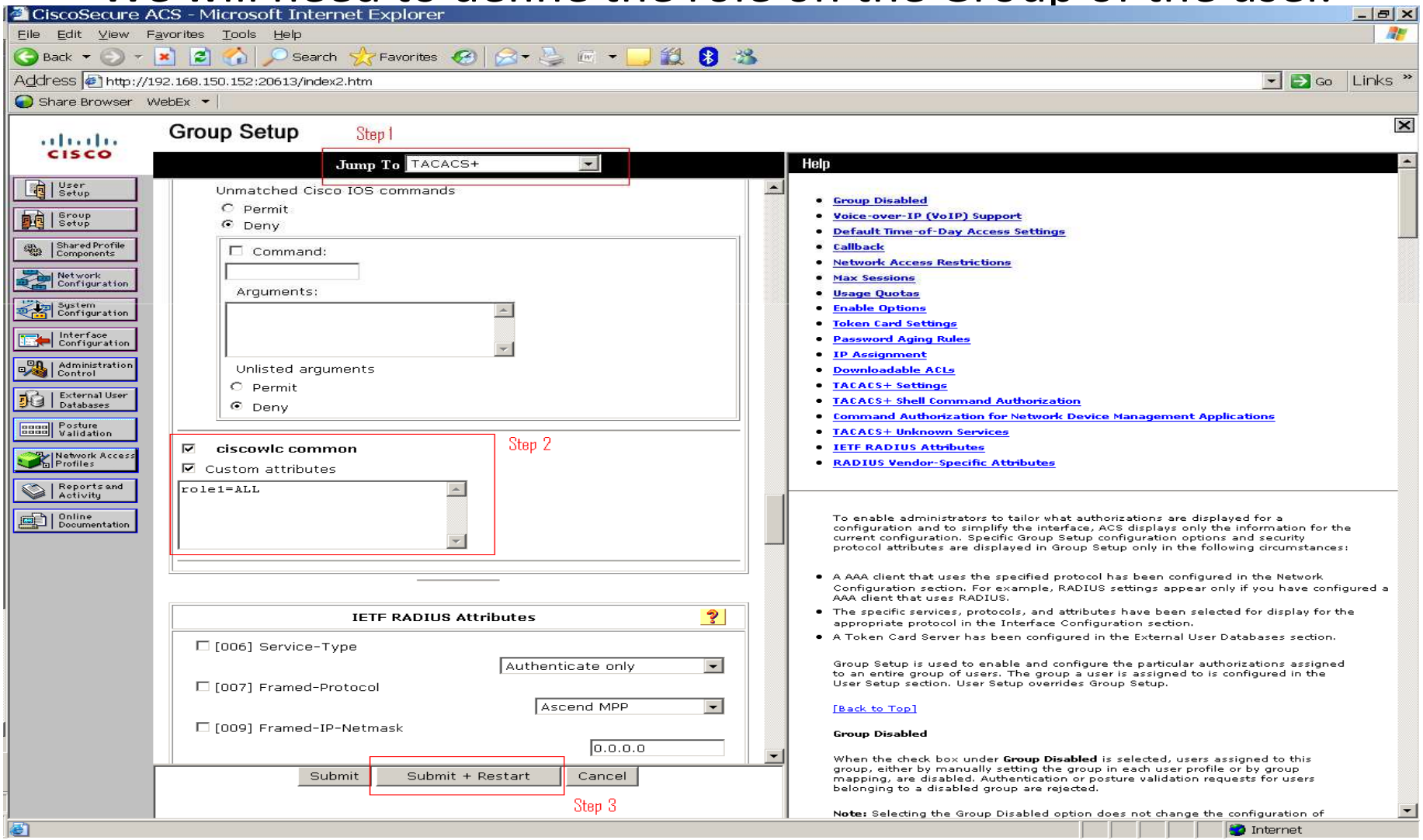
Add Role to the User Group which the ACS user name is tied

- Define group role on ACS.



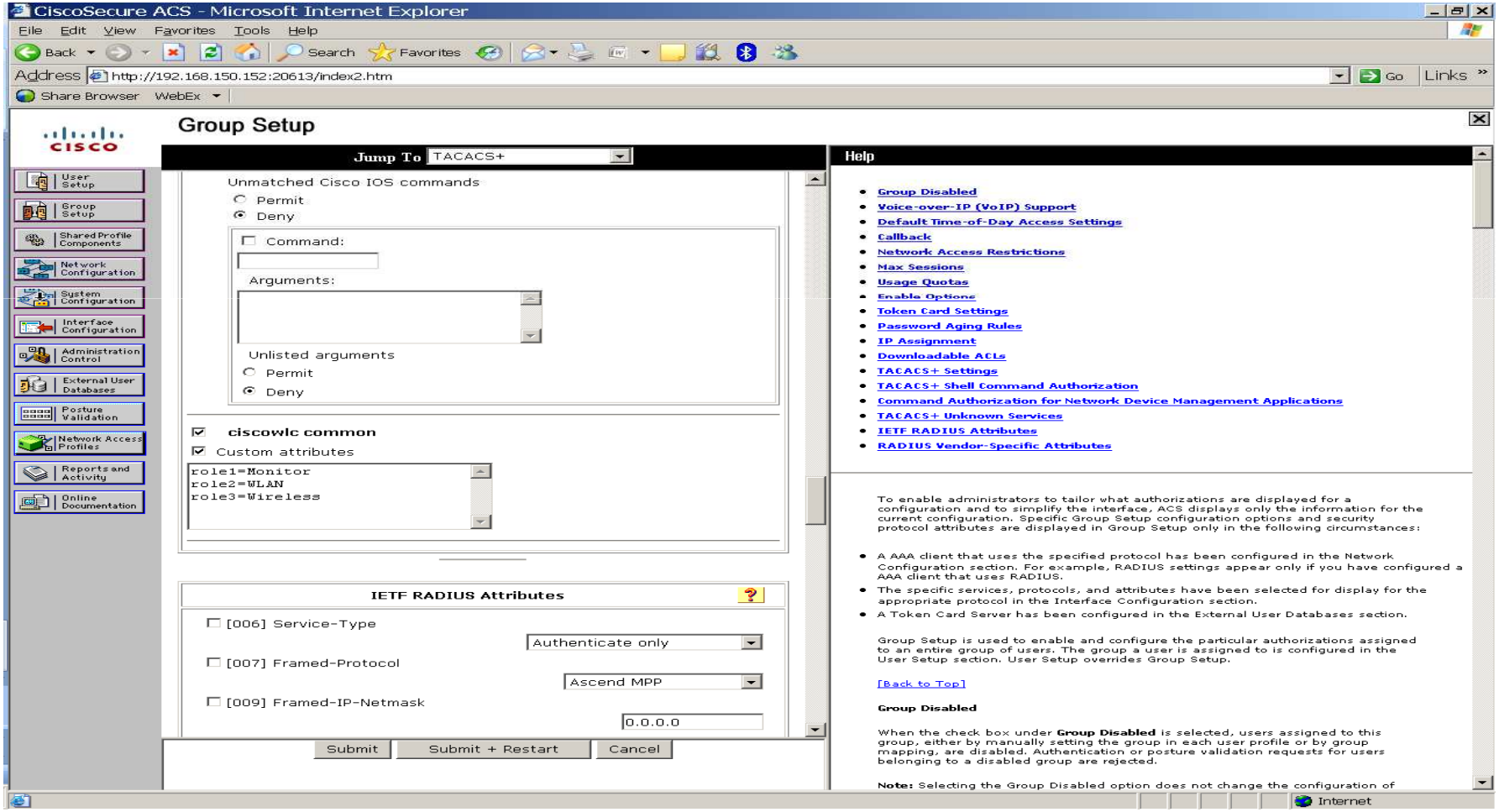
Define Role of the Group on the ACS

- We will need to define the role on the Group of the user.



Define Role of the Group on the ACS

- Multiple Roles defined for Group



Debugs on the WLC for TACACS login

- The debug on the WLC for TACACS login is debug aaa tacacs enable.
- The output below shows successful authentication of TACACS user.

(Cisco Controller) >*spamApTask5: Dec 14 12:07:50.989:

spamApTask6: Dec 14 12:07:55.439:

spamApTask4: Dec 14 12:08:01.645:

tplusTransportThread: Dec 14 12:08:02.234: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:08:02.236: tplus auth response: type=1 seq_no=2 session_id=e9a68809 length=16 encrypted=0

tplusTransportThread: Dec 14 12:08:02.236**: TPLUS_AUTHEN_STATUS_GETPASS**

tplusTransportThread: Dec 14 12:08:02.236: **auth_cont get_pass reply: pkt_length=28**

tplusTransportThread: Dec 14 12:08:02.236: processTplusAuthResponse: Continue auth transaction

tplusTransportThread: Dec 14 12:08:02.237: tplus auth response: type=1 seq_no=4 session_id=e9a68809 length=6 encrypted=0

tplusTransportThread: Dec 14 12:08:02.237: tplus_make_author_request() from tplus_authen_passed returns rc=0

tplusTransportThread: Dec 14 12:08:02.237: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:08:02.245: author response body: status=1 arg_cnt=2 msg_len=0 data_len=0

tplusTransportThread: Dec 14 12:08:02.245: **arg[0] = [14][role1=COMMANDS]**

tplusTransportThread: Dec 14 12:08:02.245: **arg[1] = [16][role2=MANAGEMENT]**

tplusTransportThread: Dec 14 12:08:02.245:

User has the following mgmtRole 180

Debugs on the WLC for TACACS Login

- Unsuccessful TACACS login when the user roles are not defined correctly.

(Cisco Controller) >*tplusTransportThread: Dec 14 12:23:12.470: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:23:12.477: tplus auth response: type=1 seq_no=2 session_id=da5851d2 length=16 encrypted=0

tplusTransportThread: Dec 14 12:23:12.477: **TPLUS_AUTHEN_STATUS_GETPASS**

tplusTransportThread: Dec 14 12:23:12.477: **auth_cont get_pass reply: pkt_length=28**

tplusTransportThread: Dec 14 12:23:12.477: processTplusAuthResponse: Continue auth transaction

tplusTransportThread: Dec 14 12:23:12.478: tplus auth response: type=1 seq_no=4 session_id=da5851d2 length=6 encrypted=0

tplusTransportThread: Dec 14 12:23:12.479: tplus_make_author_request() from tplus_authen_passed returns rc=0

tplusTransportThread: Dec 14 12:23:12.479: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:23:12.481: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0

tplusTransportThread: Dec 14 12:23:12.481: **arg[0] = [14][role1=commands]**

tplusTransportThread: Dec 14 12:23:12.481:User has the following mgmtRole 0

Debugs on WLC for TACACS Login

- When the user fails authentication, incorrect username and password.

tplusTransportThread: Dec 14 12:32:25.462: Forwarding request to 92.168.150.152 port=49

tplusTransportThread: Dec 14 12:32:25.465: tplus auth response: type=1 seq_no=2 session_id=f7f0855f length=16 encrypted=0

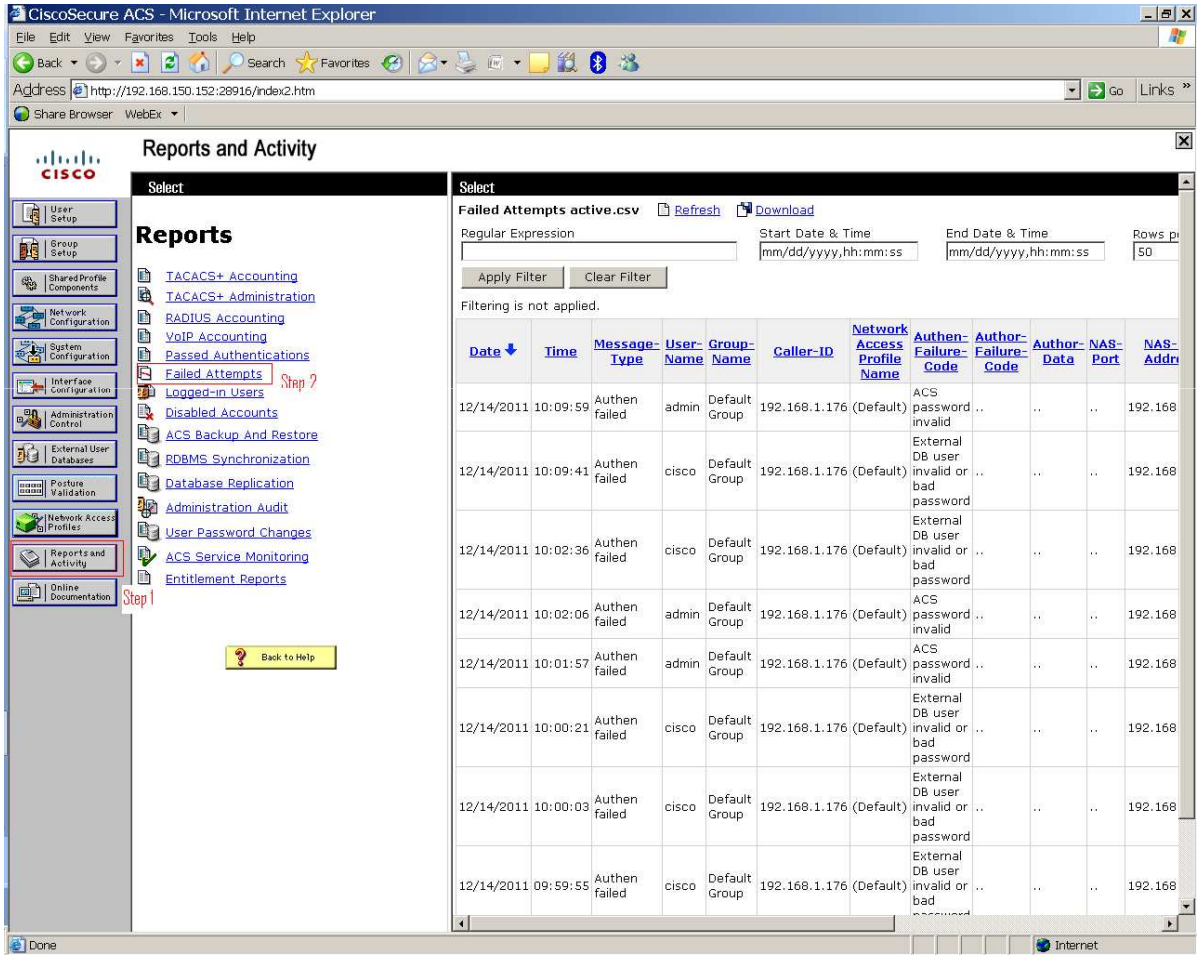
tplusTransportThread: Dec 14 12:32:25.465: TPLUS_AUTHEN_STATUS_GETPASS

tplusTransportThread: Dec 14 12:32:25.465: auth_cont get_pass reply: pkt_length=25

tplusTransportThread: Dec 14 12:32:25.465: processTplusAuthResponse: Continue auth transaction

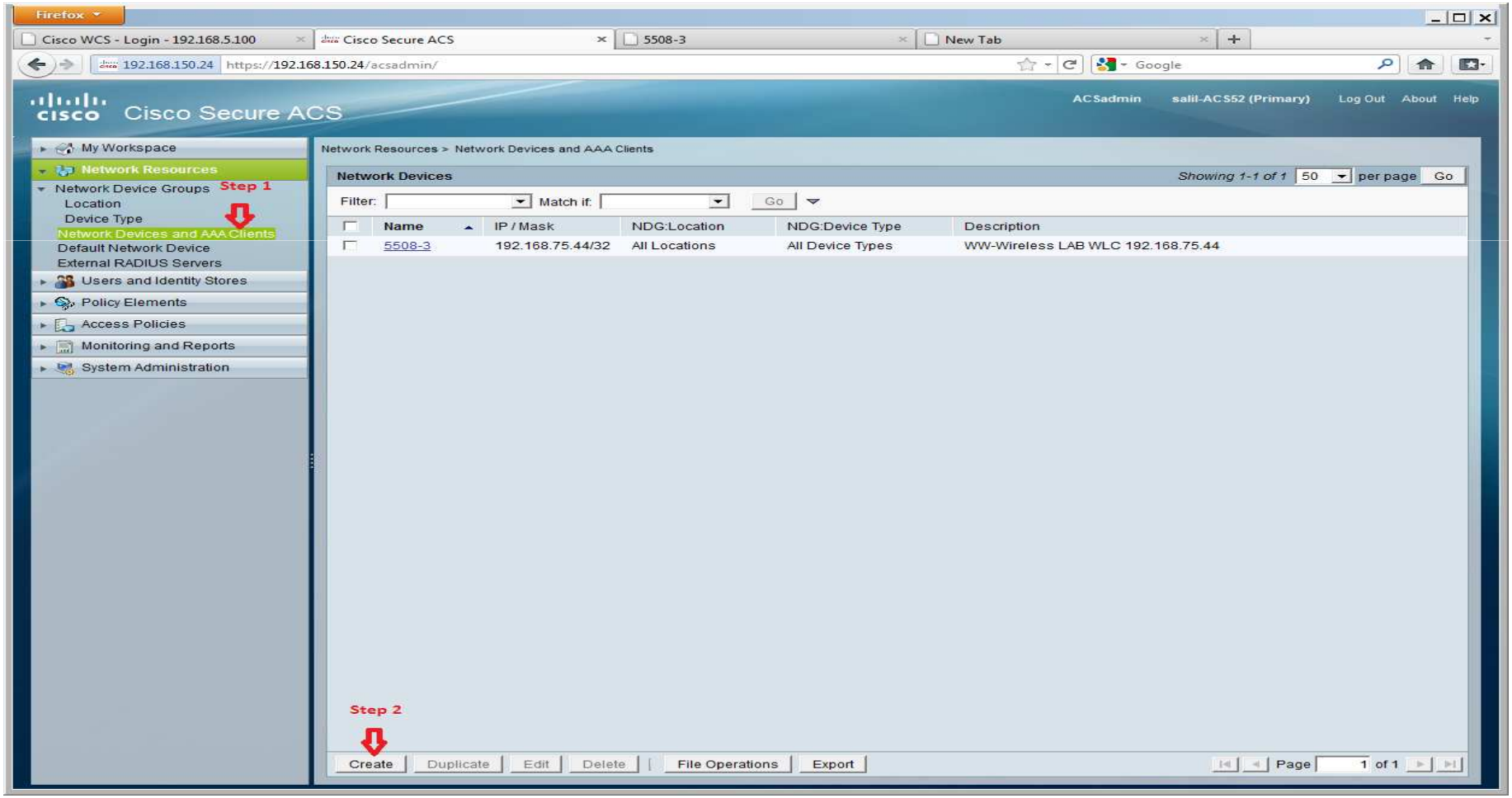
tplusTransportThread: Dec 14 12:32:25.468: tplus auth response: type=1 seq_no=4 session_id=f7f0855f length=6 encrypted=0

Failed Attempt Log on the ACS 4.2



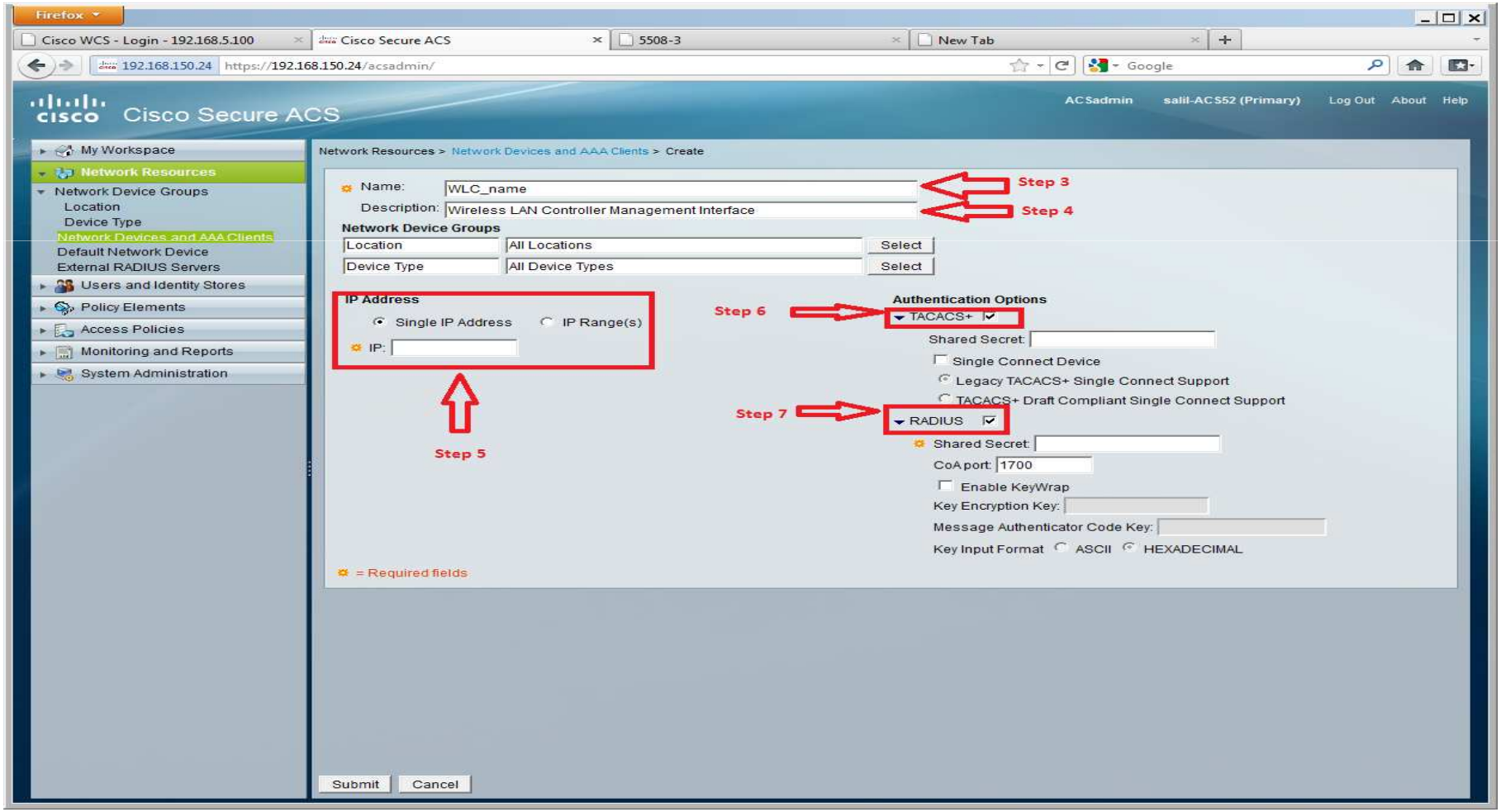
Management Login to WLC using TACACS Account on ACS 5.x

- Add the WLC as Network Device on ACS 5.x.



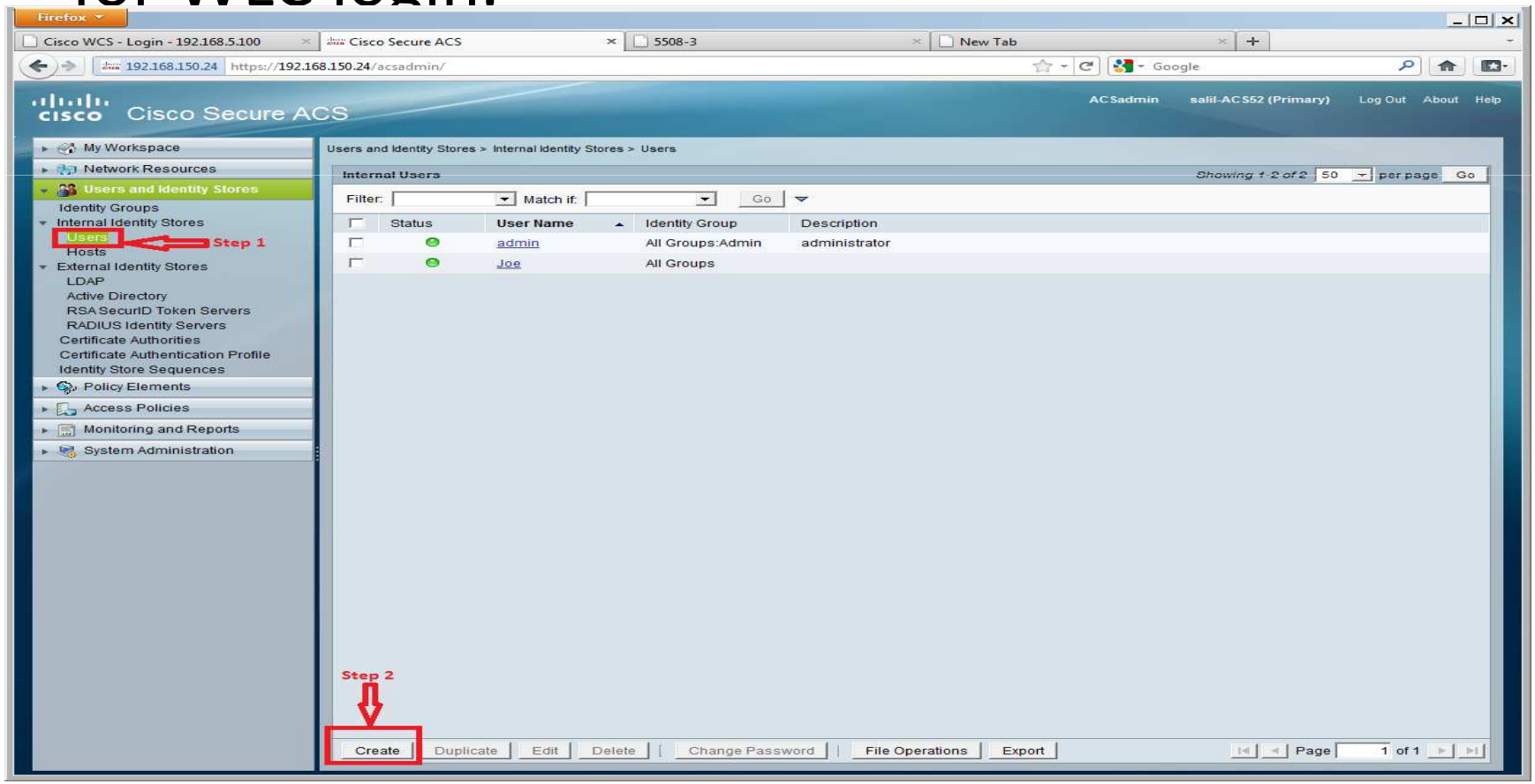
Management Login to WLC using TACACS Account on ACS 5.x

- Add the shared secret on the Radius for WLC.



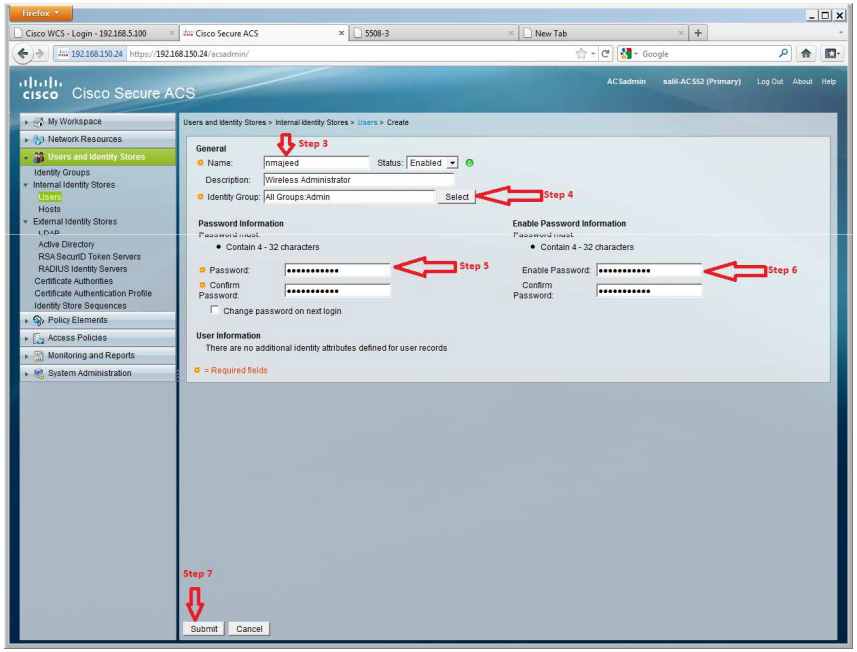
Management Login to WLC using TACACS Account on ACS 5.x

- Create a Local Username on the ACS 5.x to use for WLC login.



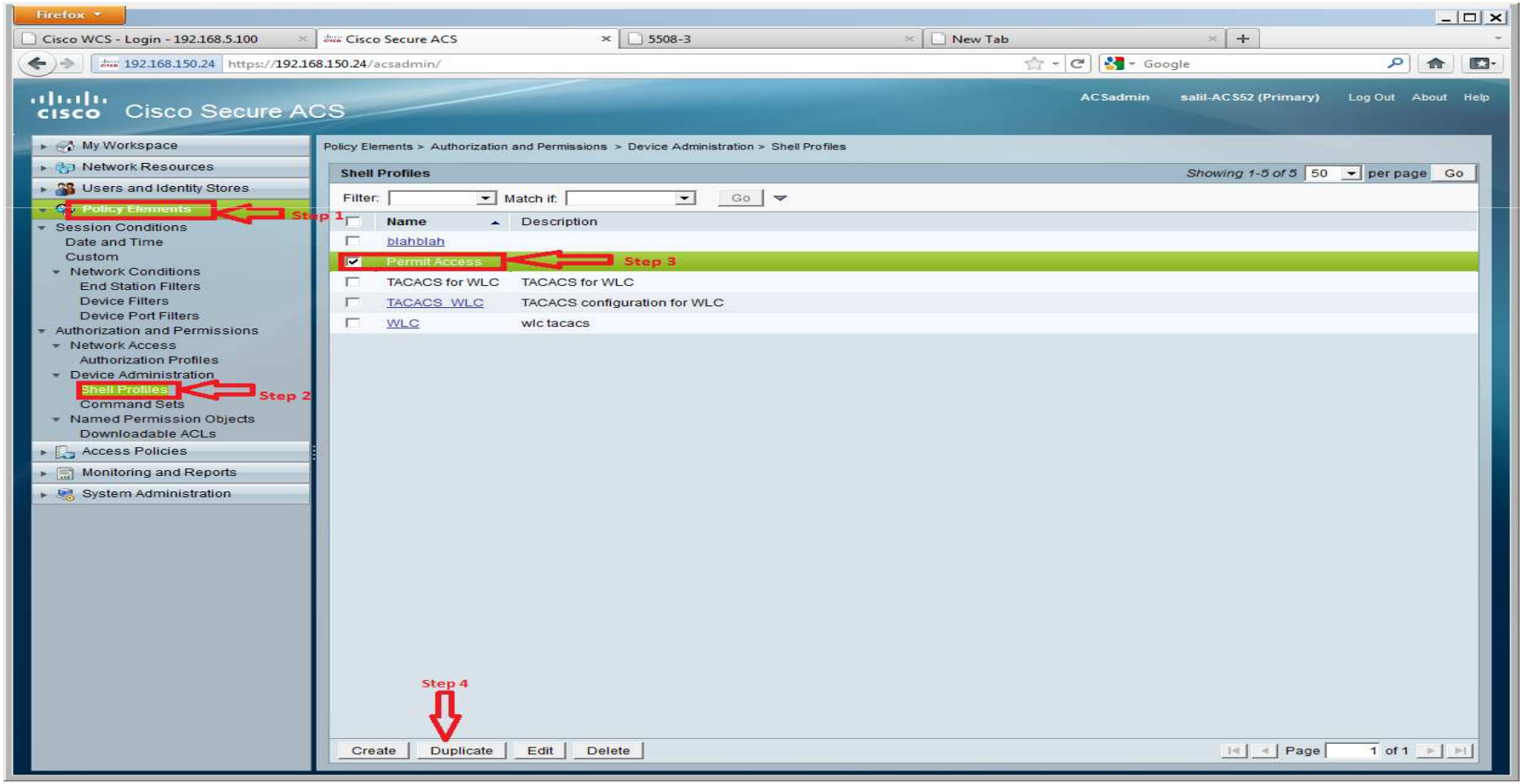
Management Login to WLC using TACACS Account on ACS 5.x

- Add the user name and password on the ACS.



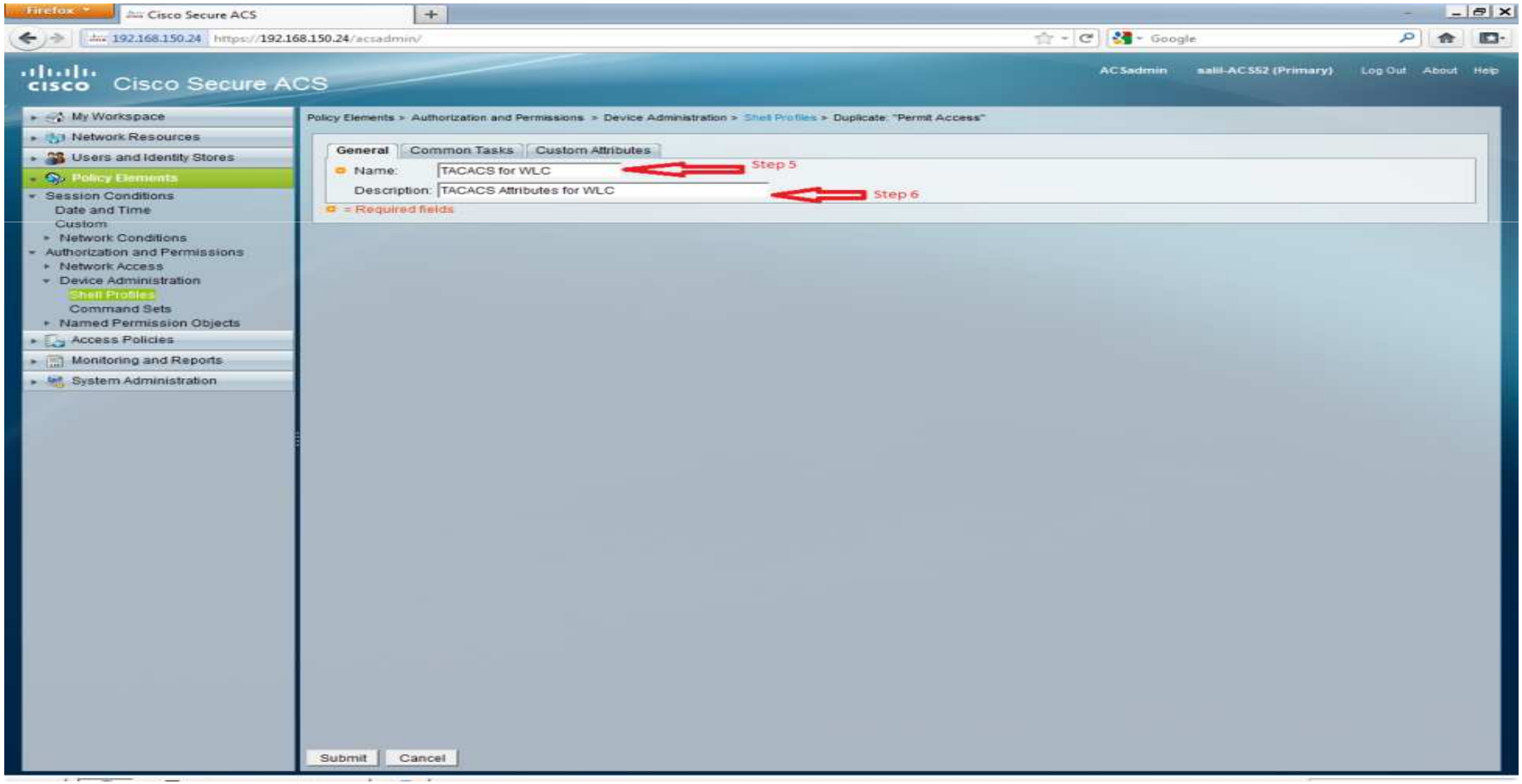
Management Login to WLC using TACACS Account on ACS 5.x

- Defining shell properties on ACS server for user created on ACS5.x



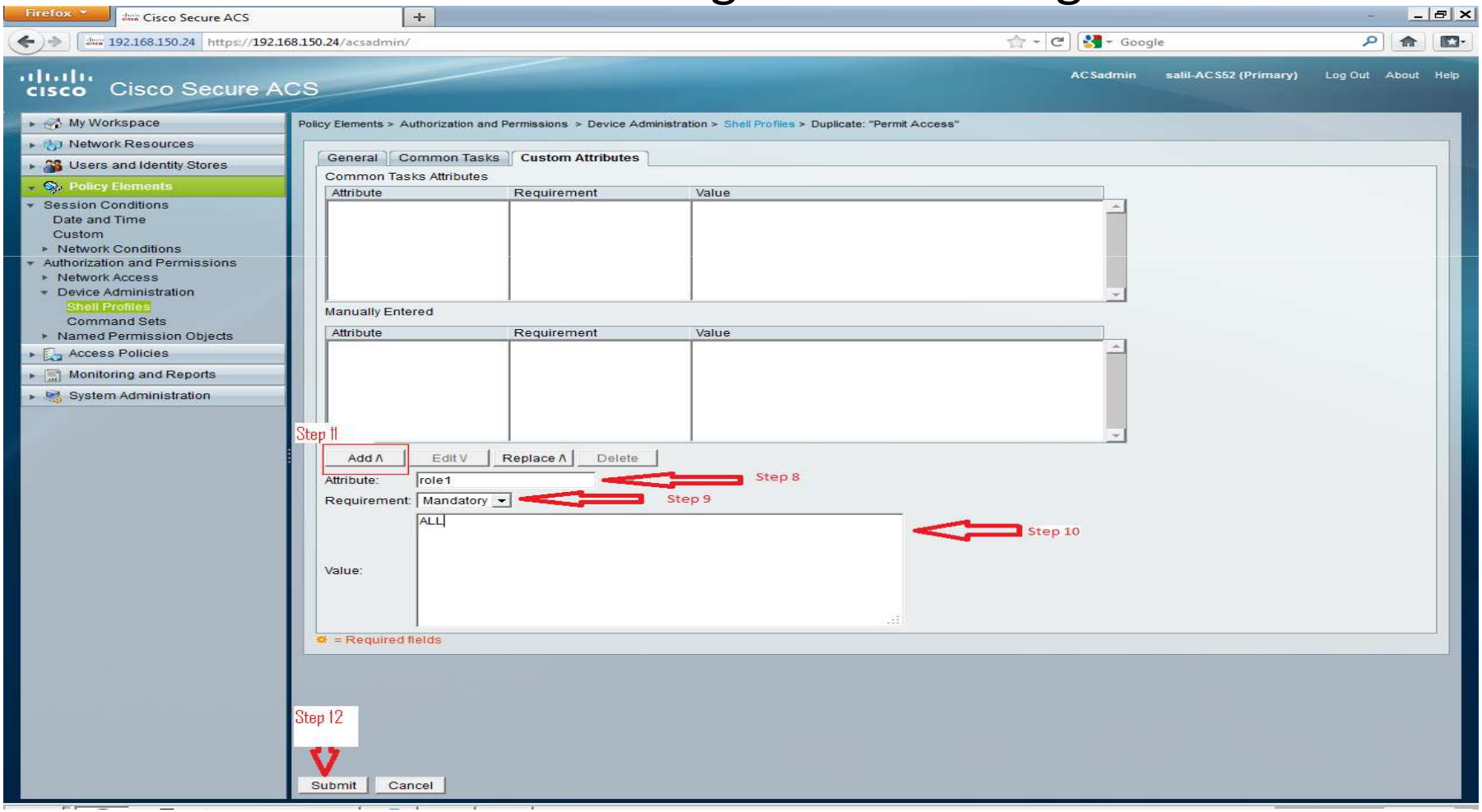
Management Login to WLC using TACACS Account on ACS 5.x

Configure the Name of the Profile and description.



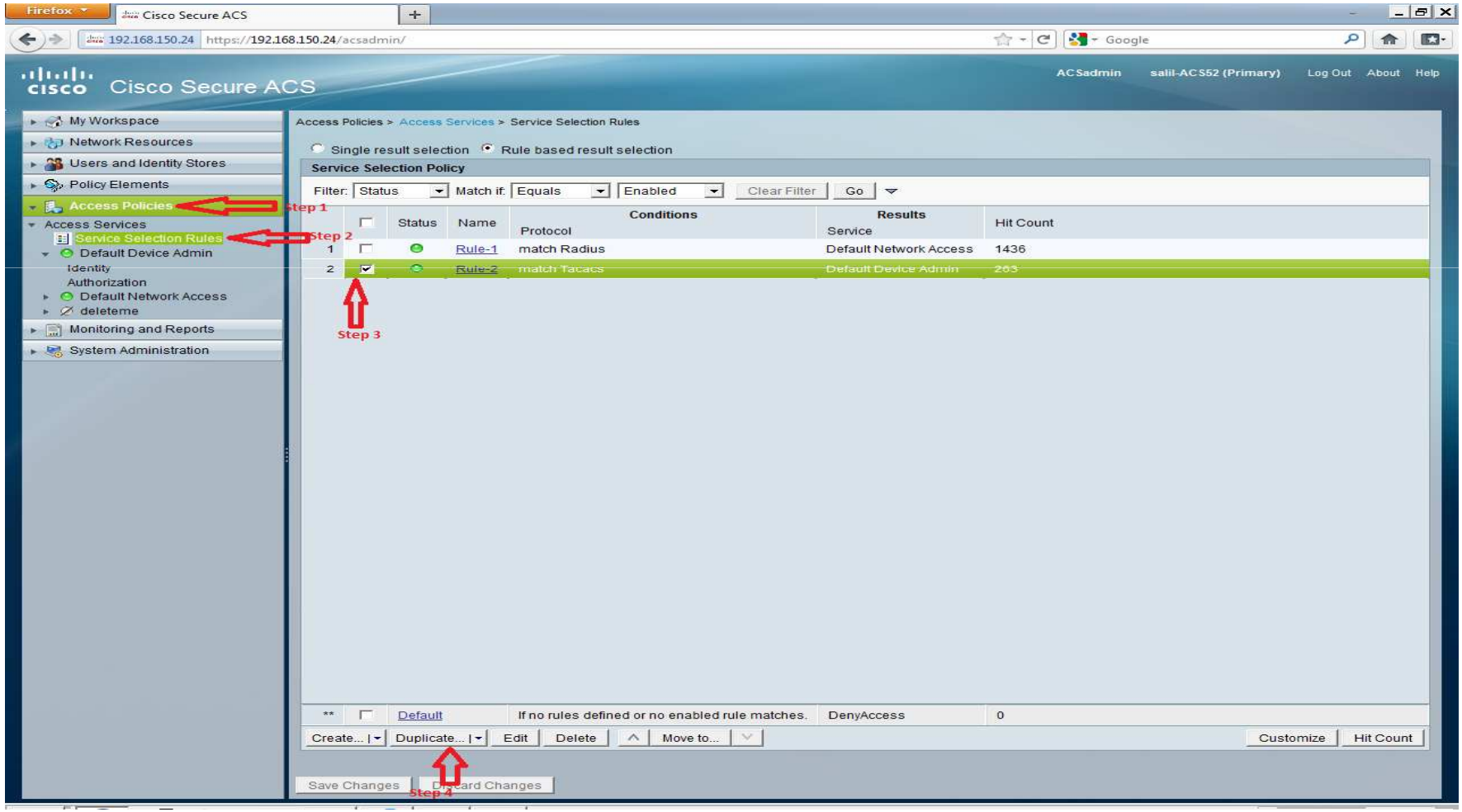
Management Login to WLC using TACACS Account on ACS 5.x

- Define the Role to be Assigned to be assigned.



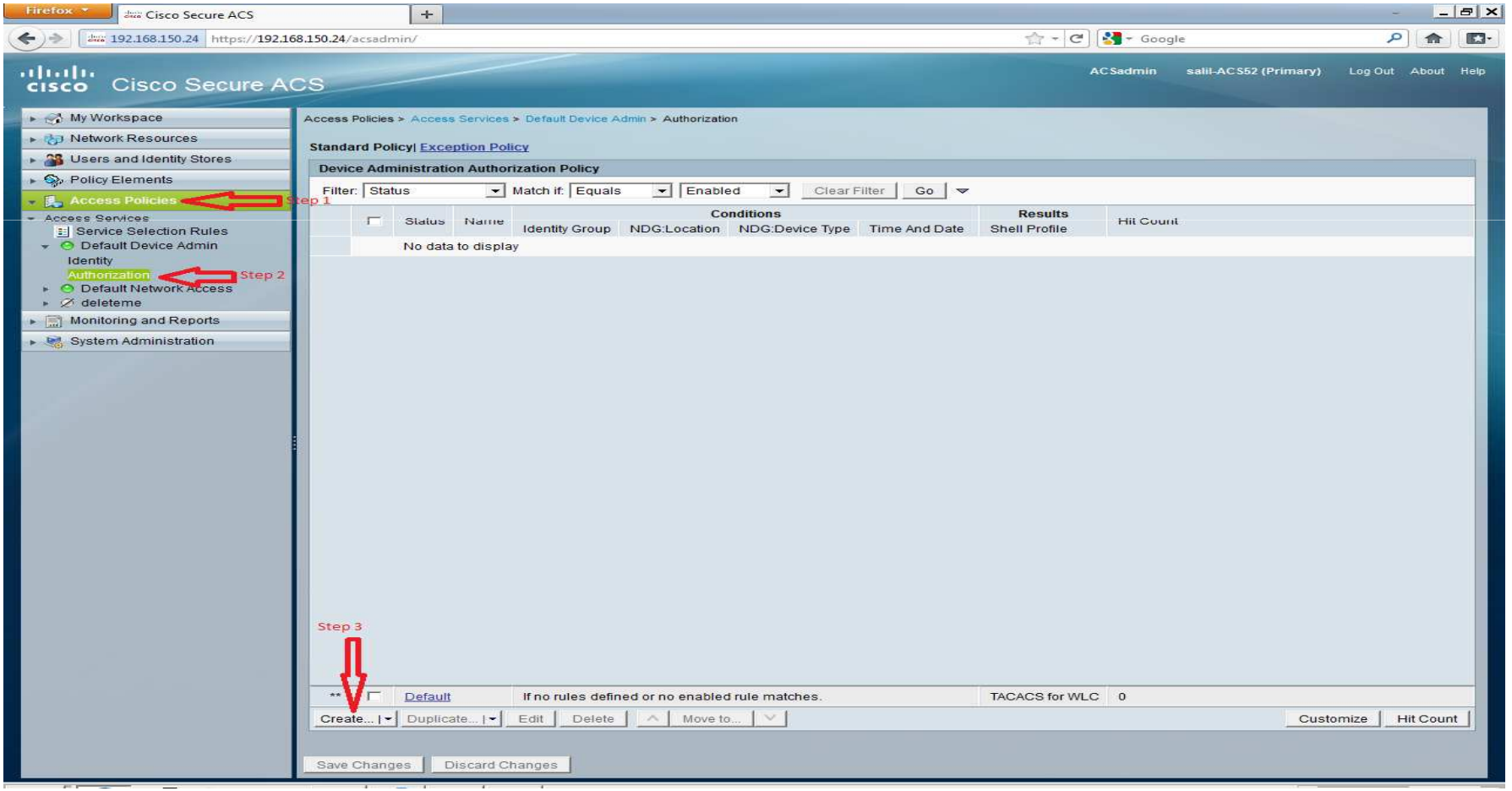
Management Login to WLC using TACACS Account on ACS 5.x

- Define Access Policies on the ACS server for Device configuration in order to pass the Role.



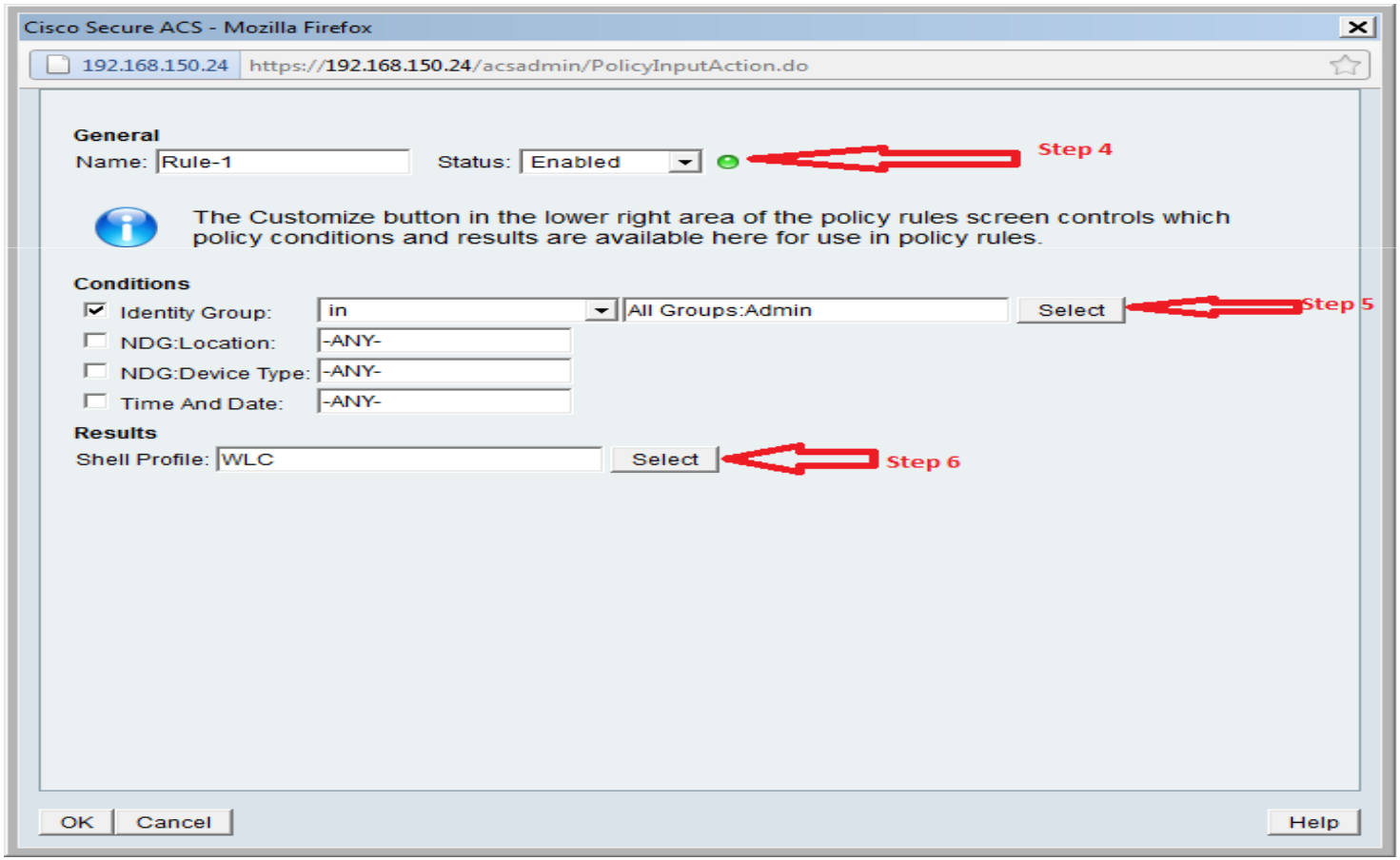
Management Login to WLC using TACACS Account on ACS 5.x

- Create a new Authorization Policy to add the Shell Policy we created earlier along with the User group which we want to allow using the TACACS profile.



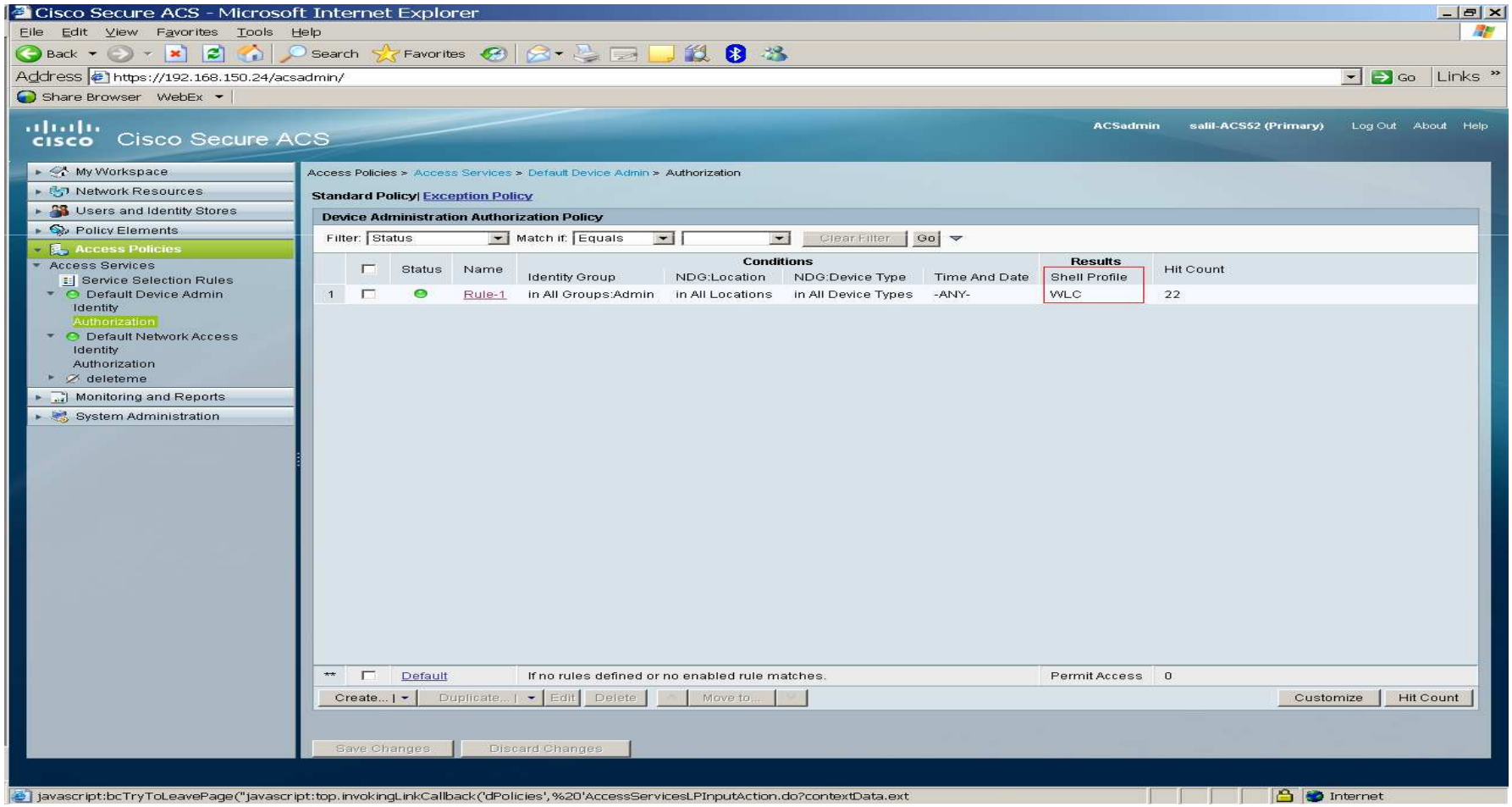
Management Login to WLC using TACACS Account on ACS 5.x

- Define the Group which the user is part of along with the Shell profile we want to allow for the user name to be applied.

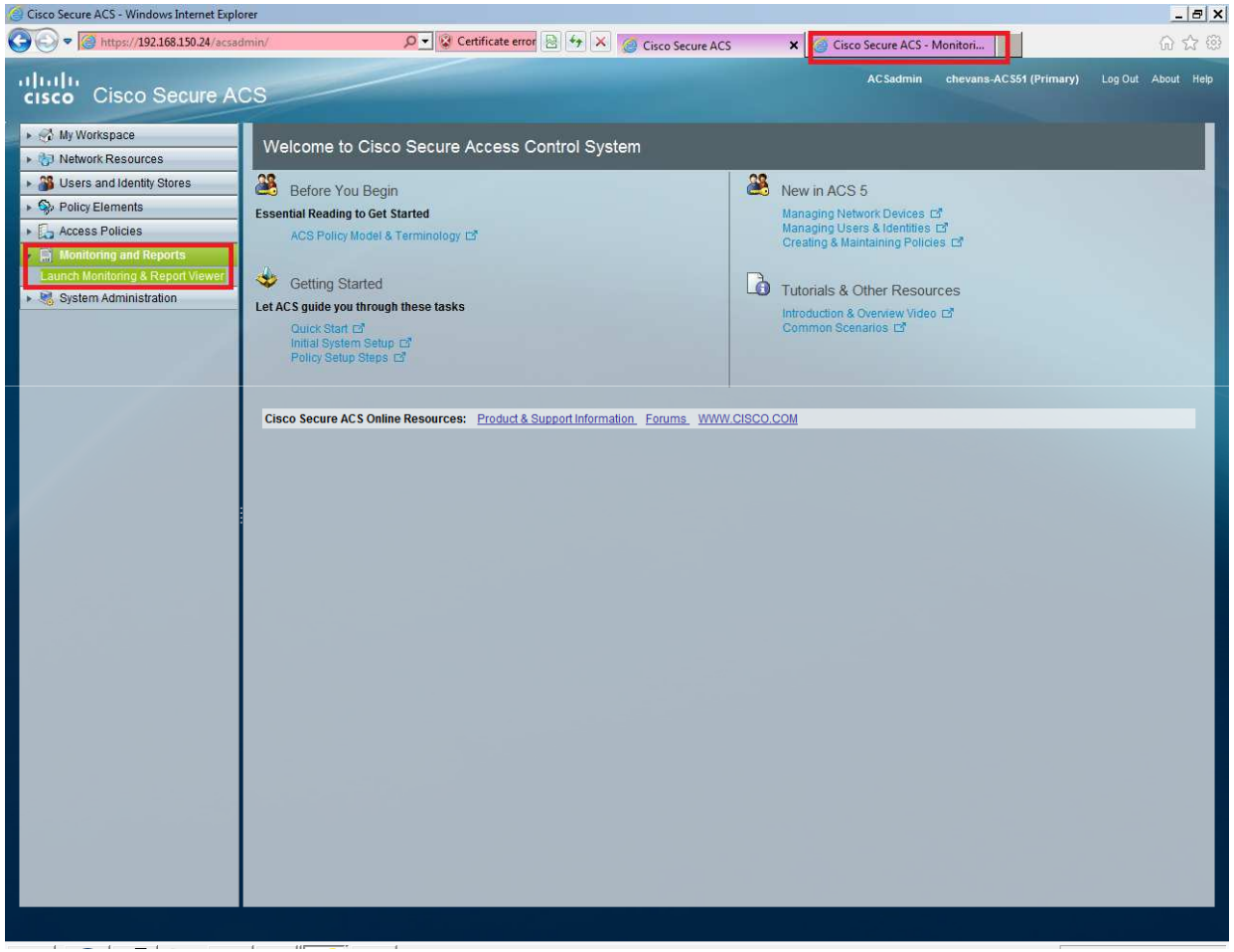


Management Login to WLC using TACACS Account on ACS 5.x

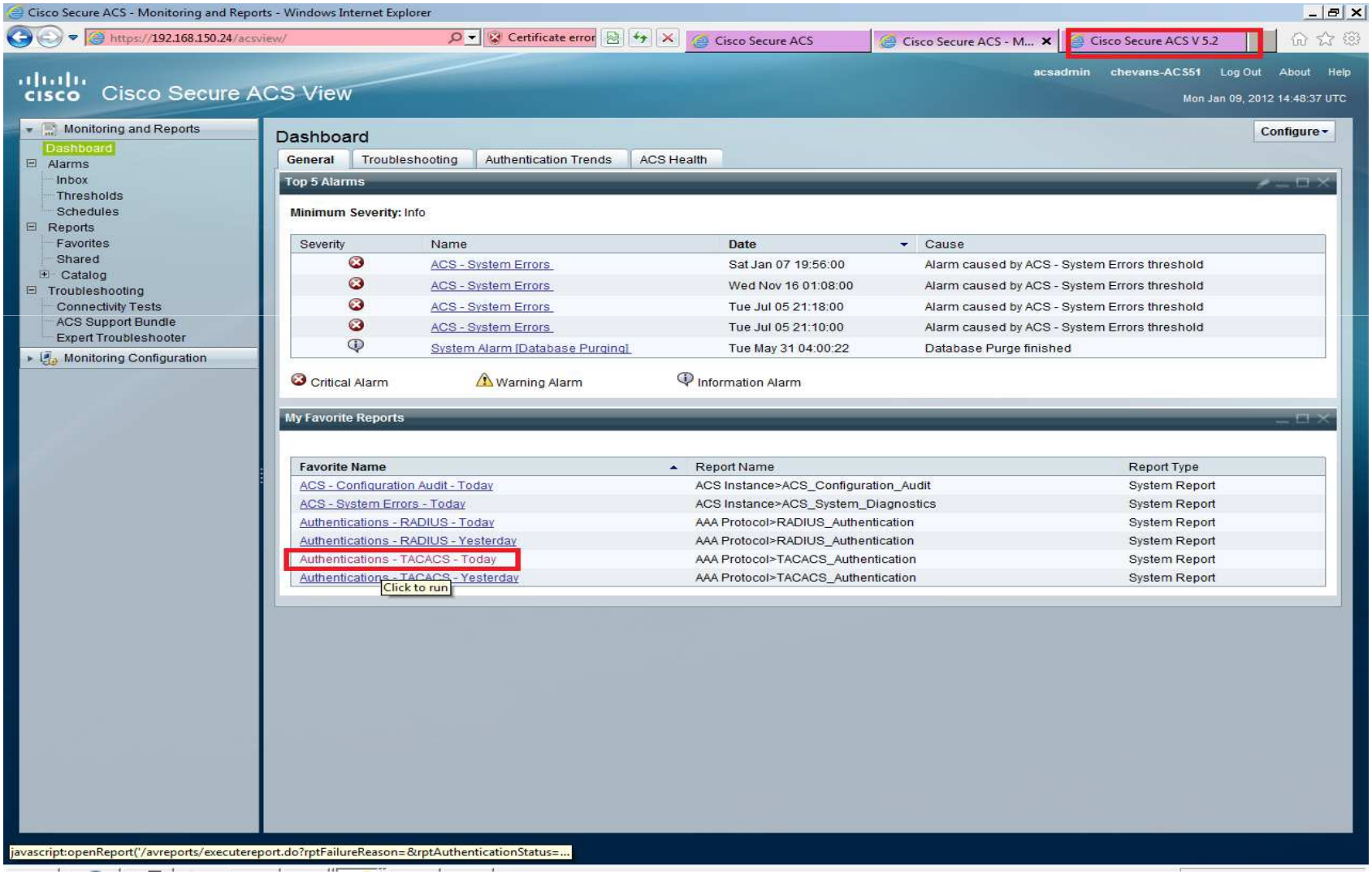
- The shell profile is seen after in the new Policy created.



Failed Attempt Log on the ACS 5.x



Failed Attempt Log on ACS 5.x



Management Login to WLC using TACACS Account on ACS 5.x

- The debug on the WLC show the same output regardless of the ACS server version being used.

debug aaa tacacs enable

portThread: Dec 14 14:29:16.090: Forwarding request to 192.168.150.24 port=49

tplusTransportThread: Dec 14 14:29:16.092: tplus auth response: type=1 seq_no=2 session_id=48f1bb06 length=16 encrypted=0

tplusTransportThread: Dec 14 14:29:16.092: TPLUS_AUTHEN_STATUS_GETPASS

tplusTransportThread: Dec 14 14:29:16.092: auth_cont get_pass reply: pkt_length=28

tplusTransportThread: Dec 14 14:29:16.092: processTplusAuthResponse: Continue auth transaction

tplusTransportThread: Dec 14 14:29:16.095: tplus auth response: type=1 seq_no=4 session_id=48f1bb06 length=6 encrypted=0

tplusTransportThread: Dec 14 14:29:16.095: tplus_make_author_request() from tplus_authen_passed returns rc=0

tplusTransportThread: Dec 14 14:29:16.095: Forwarding request to 192.168.150.24 port=49

tplusTransportThread: Dec 14 14:29:16.098: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0

tplusTransportThread: **Dec 14 14:29:16.098: arg[0] = [9][role1=ALL]**

Management Login to WLC using ACS server

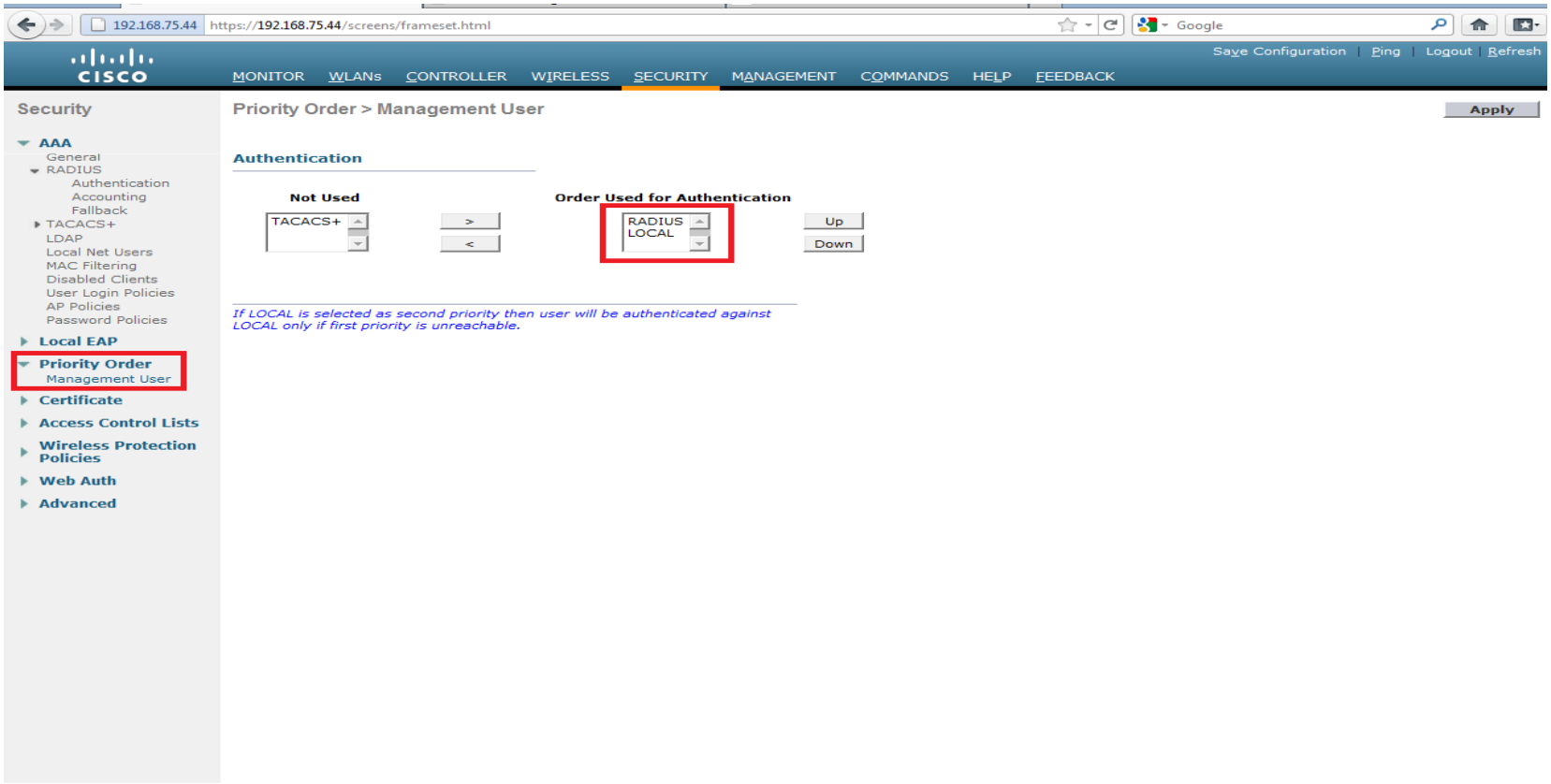
- We can also use Radius server for management user login to WLC GUI.
- Using the Radius is not much granular control as using TACACS, where we can define the user roles on the ACS server.

Management Login to WLC using ACS 4.2 server

- We can use the IETF Radius attribute Service-Type to authenticate users to login WLC GUI.
- The main type of attributes are Administrative, NAS Prompt, and Callback Administrative.
- Administrative is for logging into the WLC with full access to WLC.
- NAS prompt will give read only access to the user.
- Callback Administrator will give Lobby Ambassador Privilege to user.

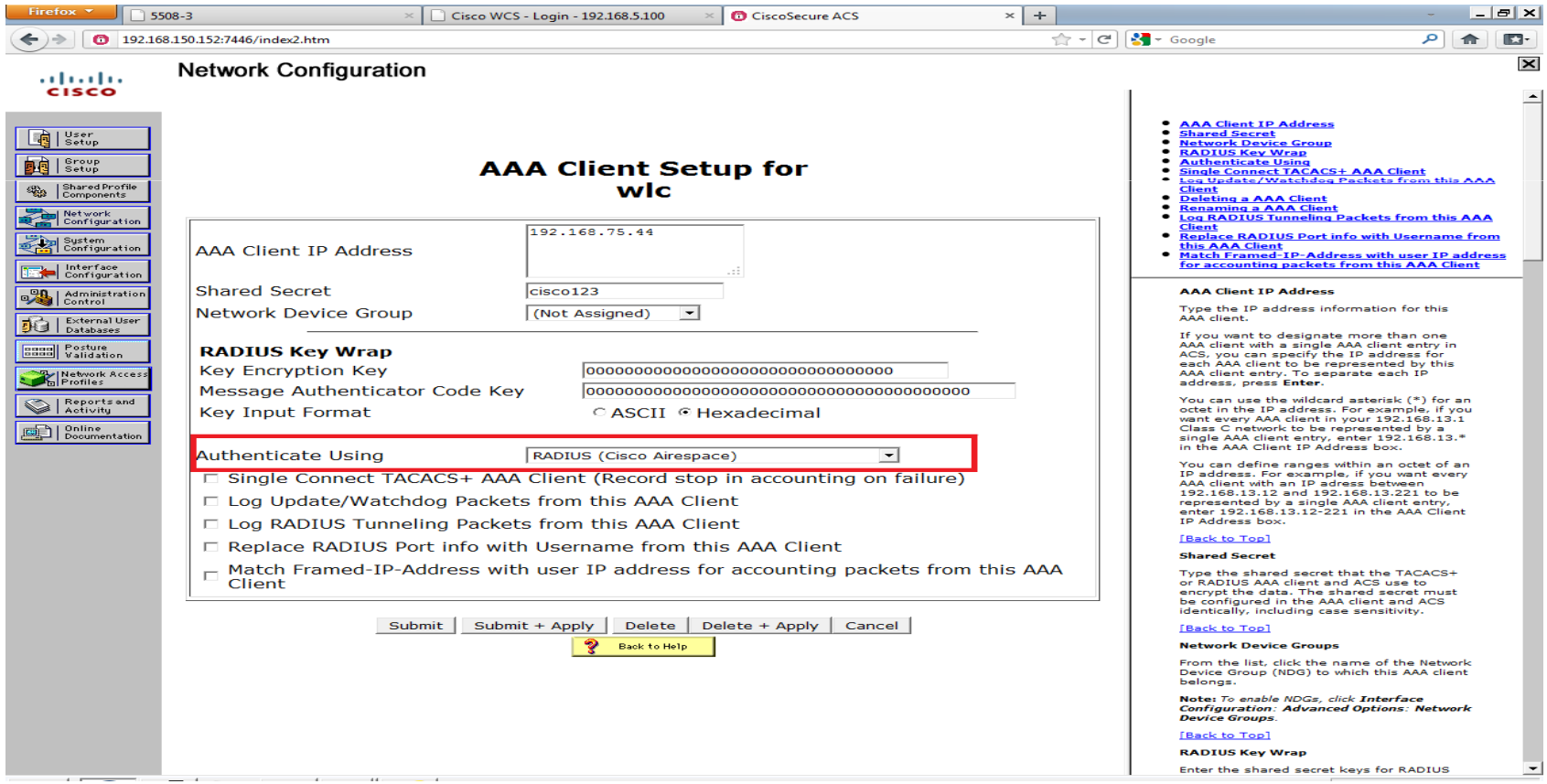
Management Login to WLC using ACS

- We will need to change the Local Management Authentication on the WLC GUI→ Security, as shown below:



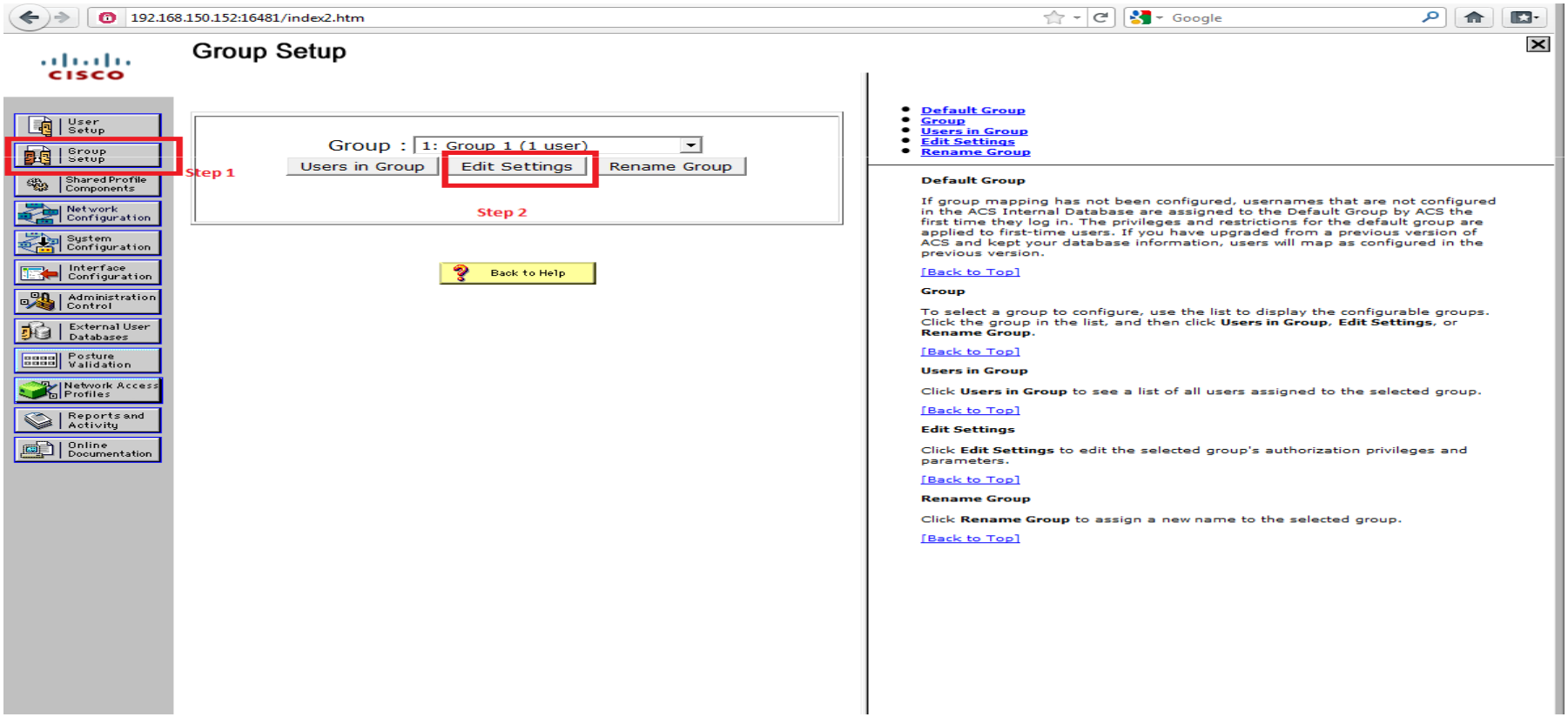
Adding WLC as NAS device on ACS 4.2

- The WLC will be added to ACS 4.2 with Authenticate using Radius Cisco Airspace as shown below:



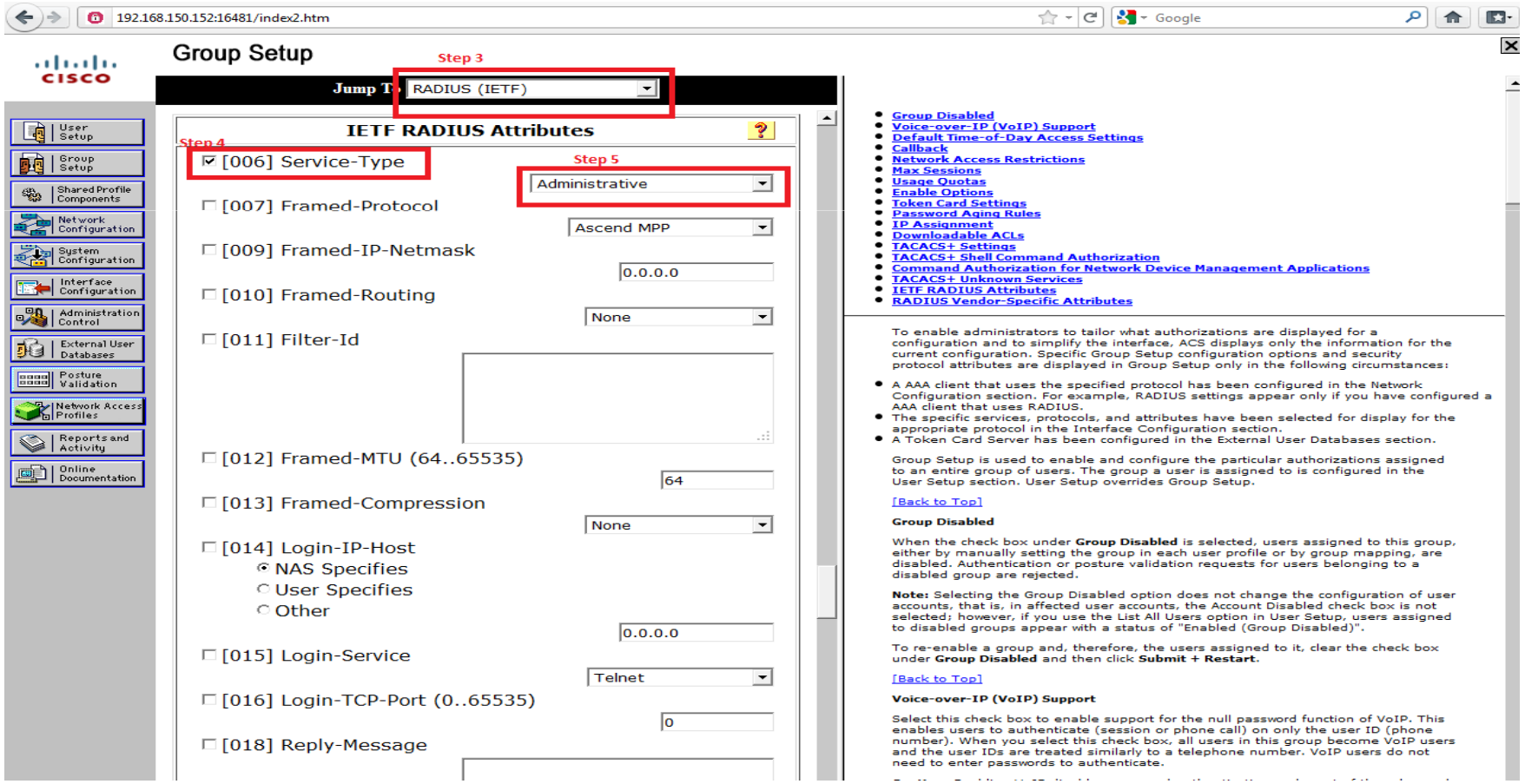
Management Login to WLC using ACS 4.2 server

- Select the User Group in which the user name is added on ACS.

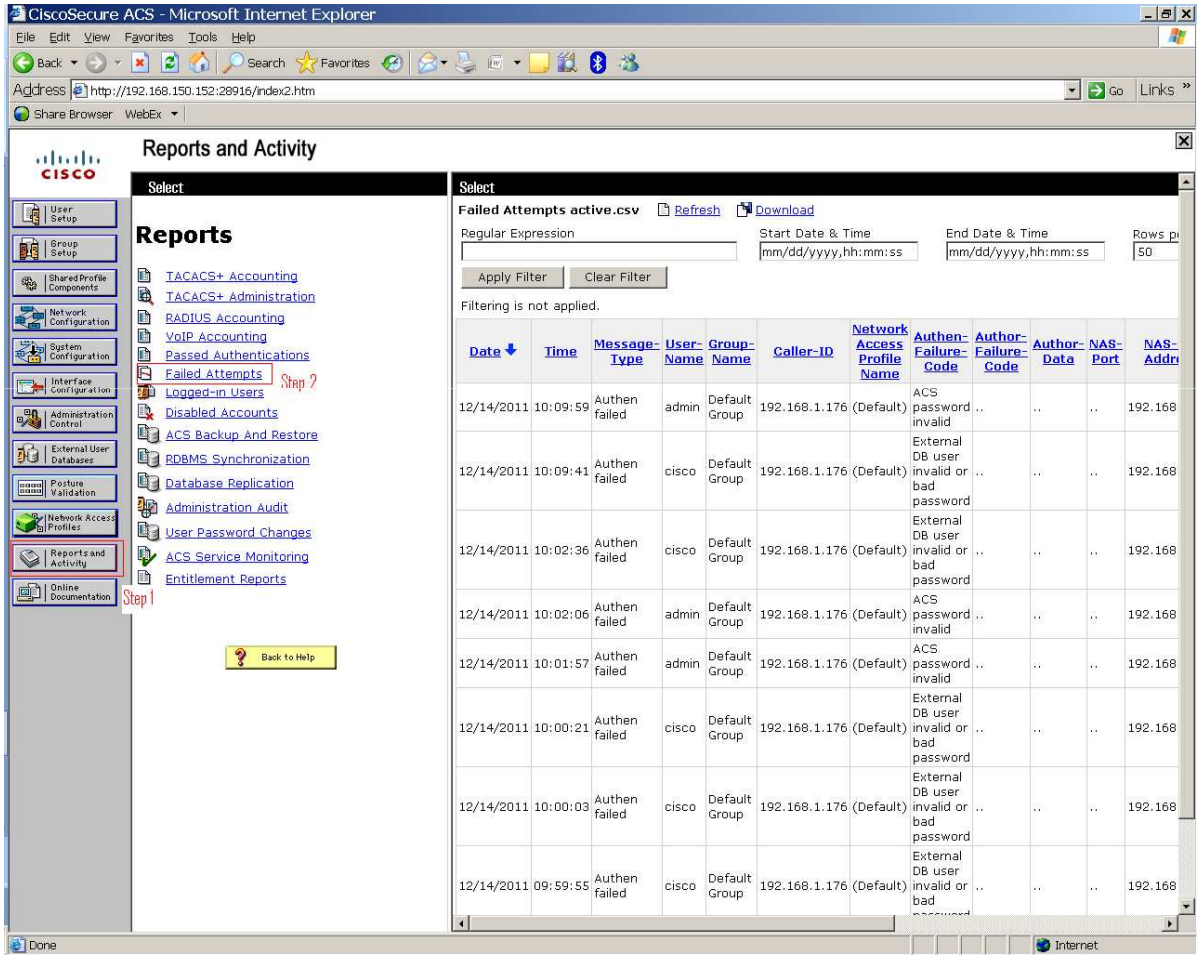


Management Login to WLC using ACS 4.2 server

- Select IETF Radius attributes from the drop down, first attribute 006 is Service-Type which we can configure to give Read only, Read-Write and Lobby Ambassador value.

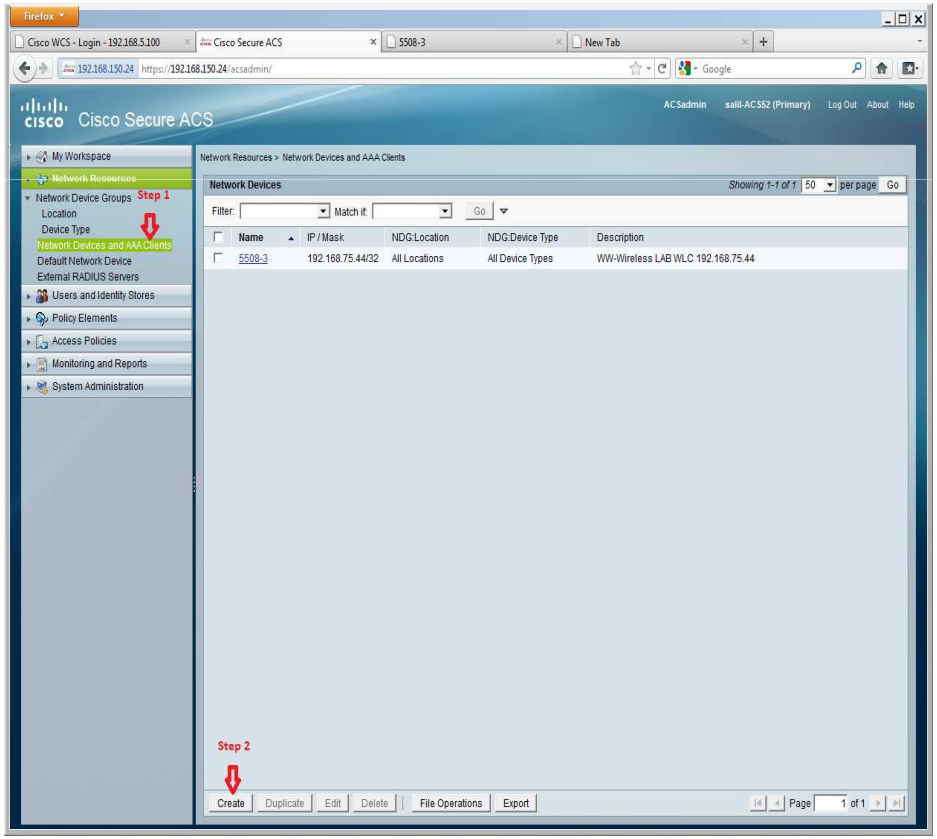


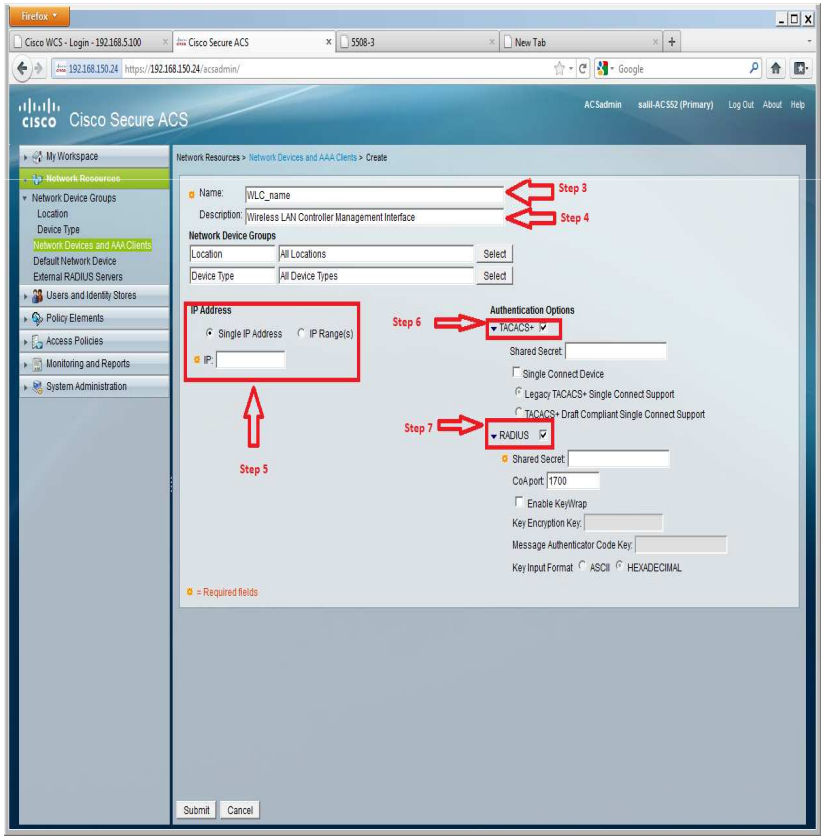
Checking ACS 4.2 Logs for failed attempts



Adding WLC as NAS device on ACS 5.x

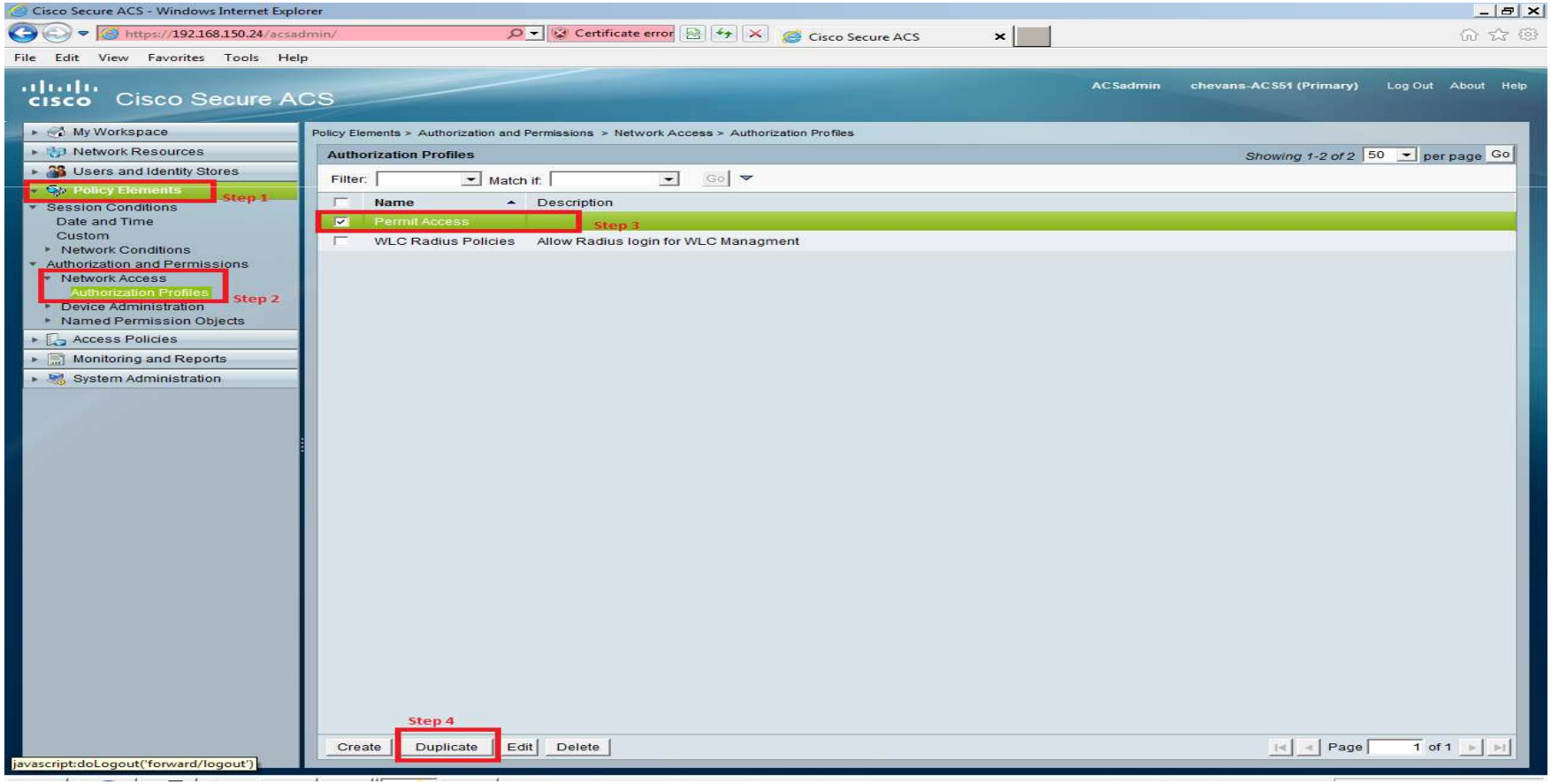
- The WLC will be added to ACS 4.2 with Authenticate using Radius Cisco Airspace as shown below:





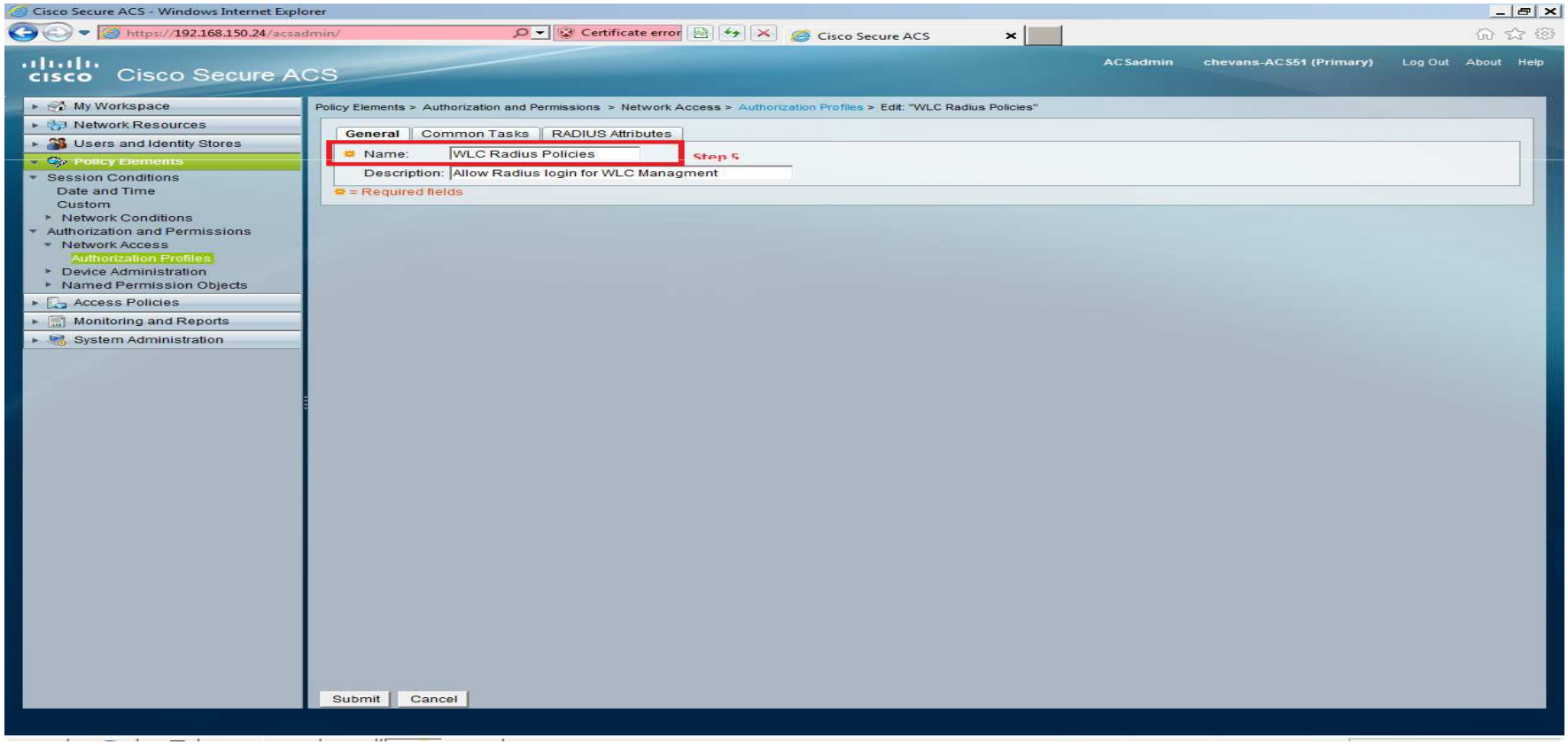
Management Login to WLC using ACS 5.x server

- The same concept applies here where can have to configure the ACS 5.x server to push the Radius attributes after successful user authentication.



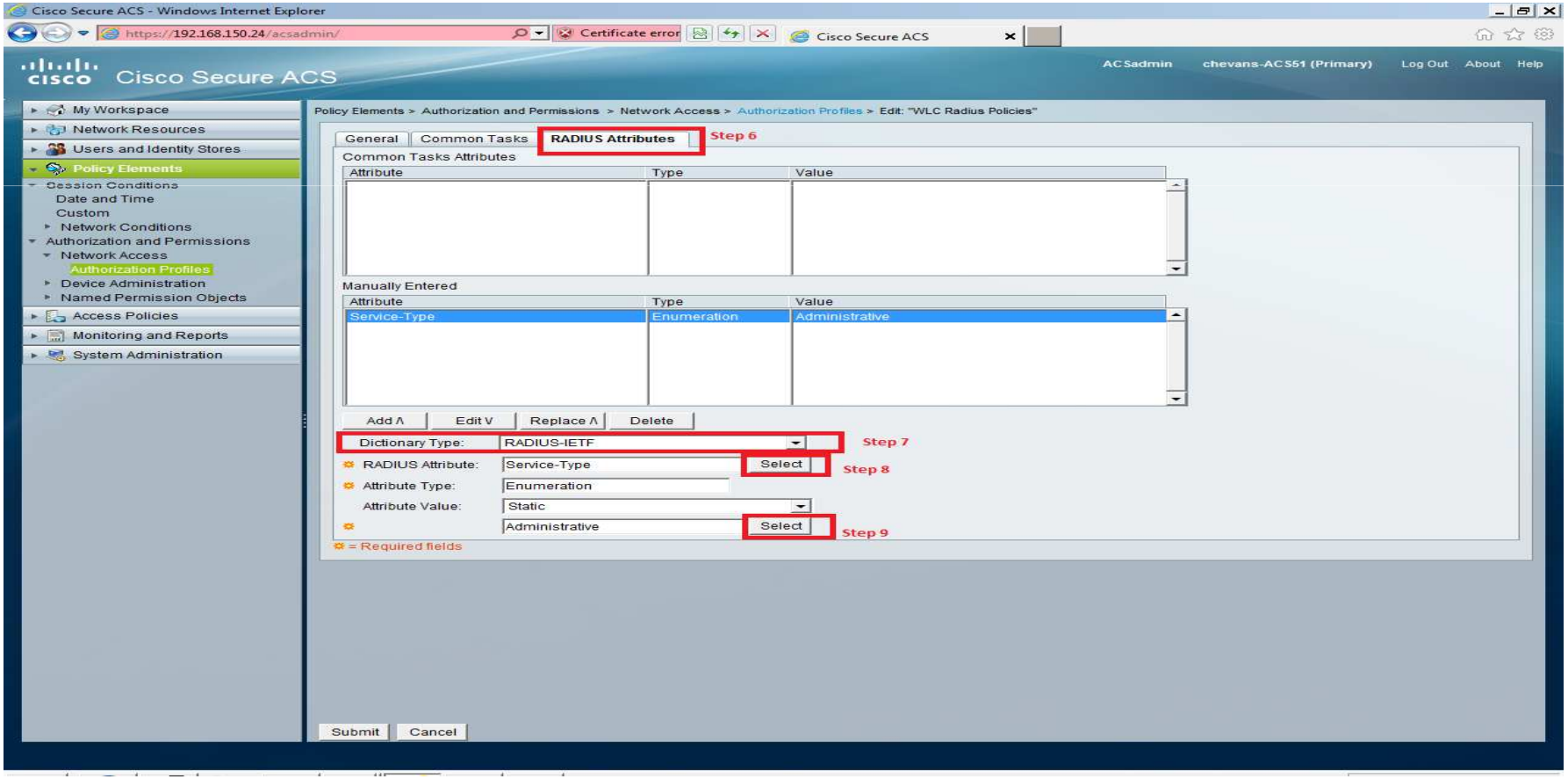
Management Login to WLC using ACS 5.x server

- When we duplicate the policies the screen will look as below which is where I can give the policy name and also define different Radius Attributes.



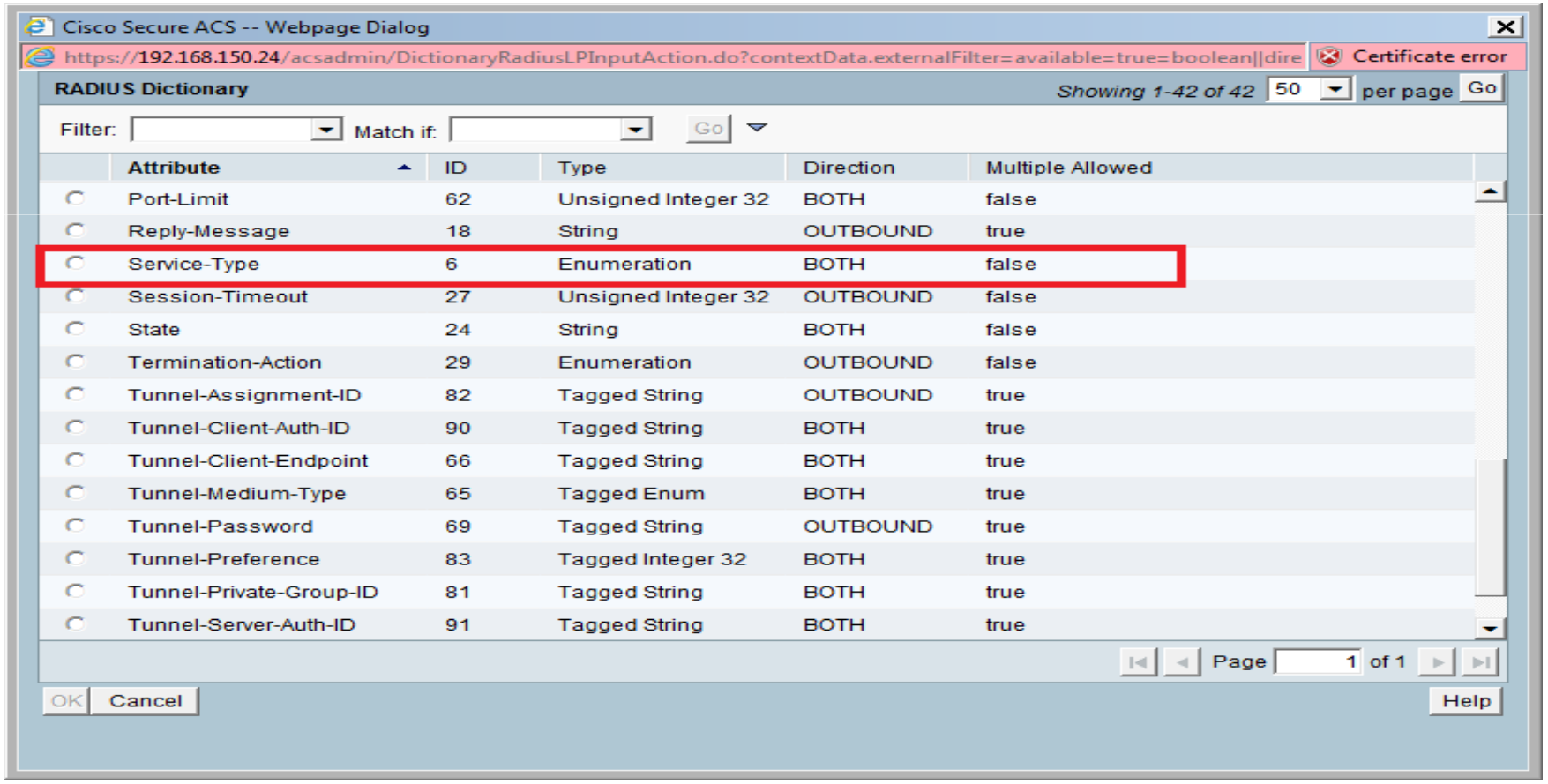
Management Login to WLC using ACS 5.x server

- On the Radius attributes tab, we can define different attributes.



Management Login to WLC using ACS 5.x server

- Step 8, select the Radius attribute Service Type.

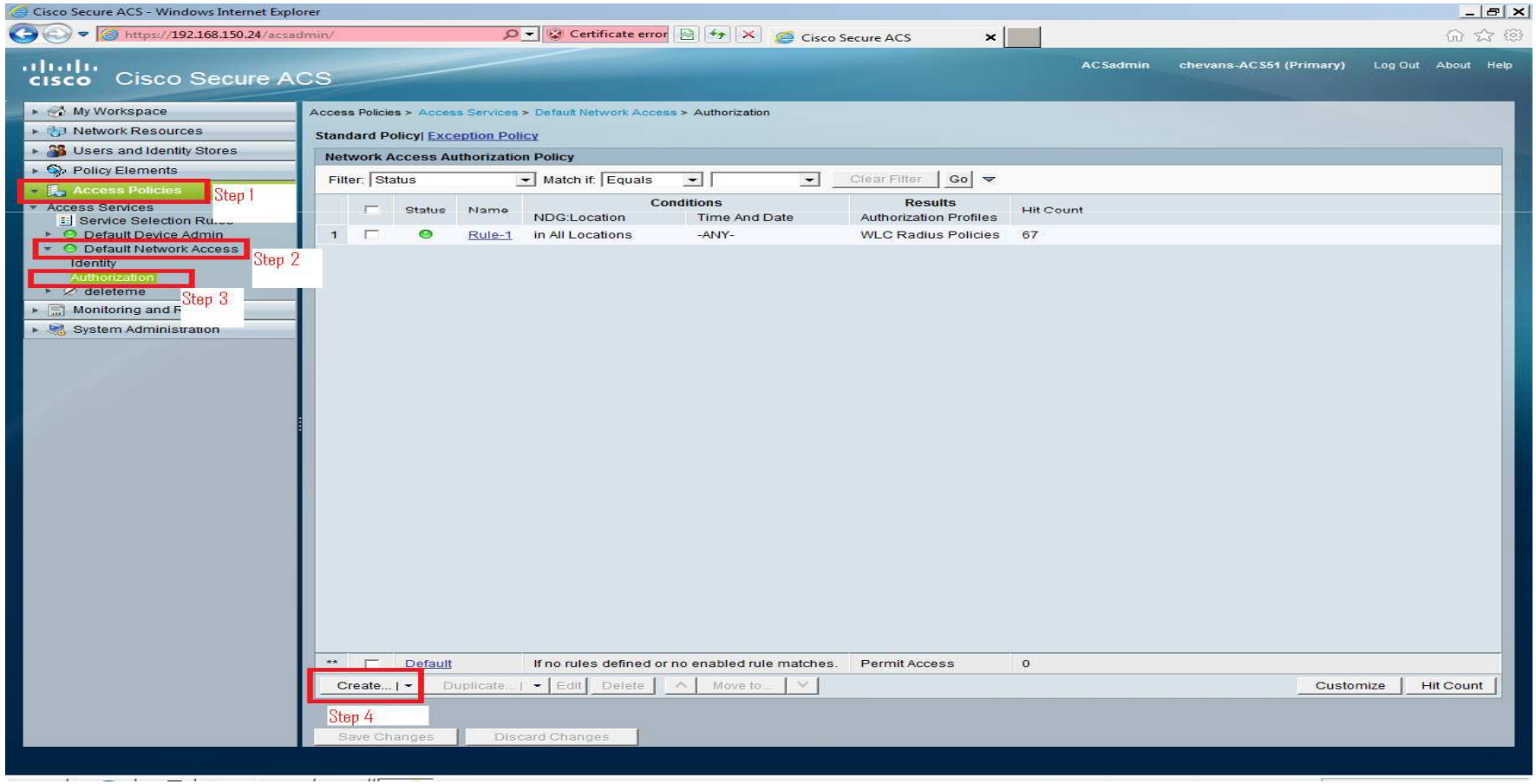


Management Login to WLC using ACS 5.x server

- Step 9, select the value such as Administrative or other attribute as defined in slide 29 to give Read only access, Read-Write Access or Lobby Admin Access.

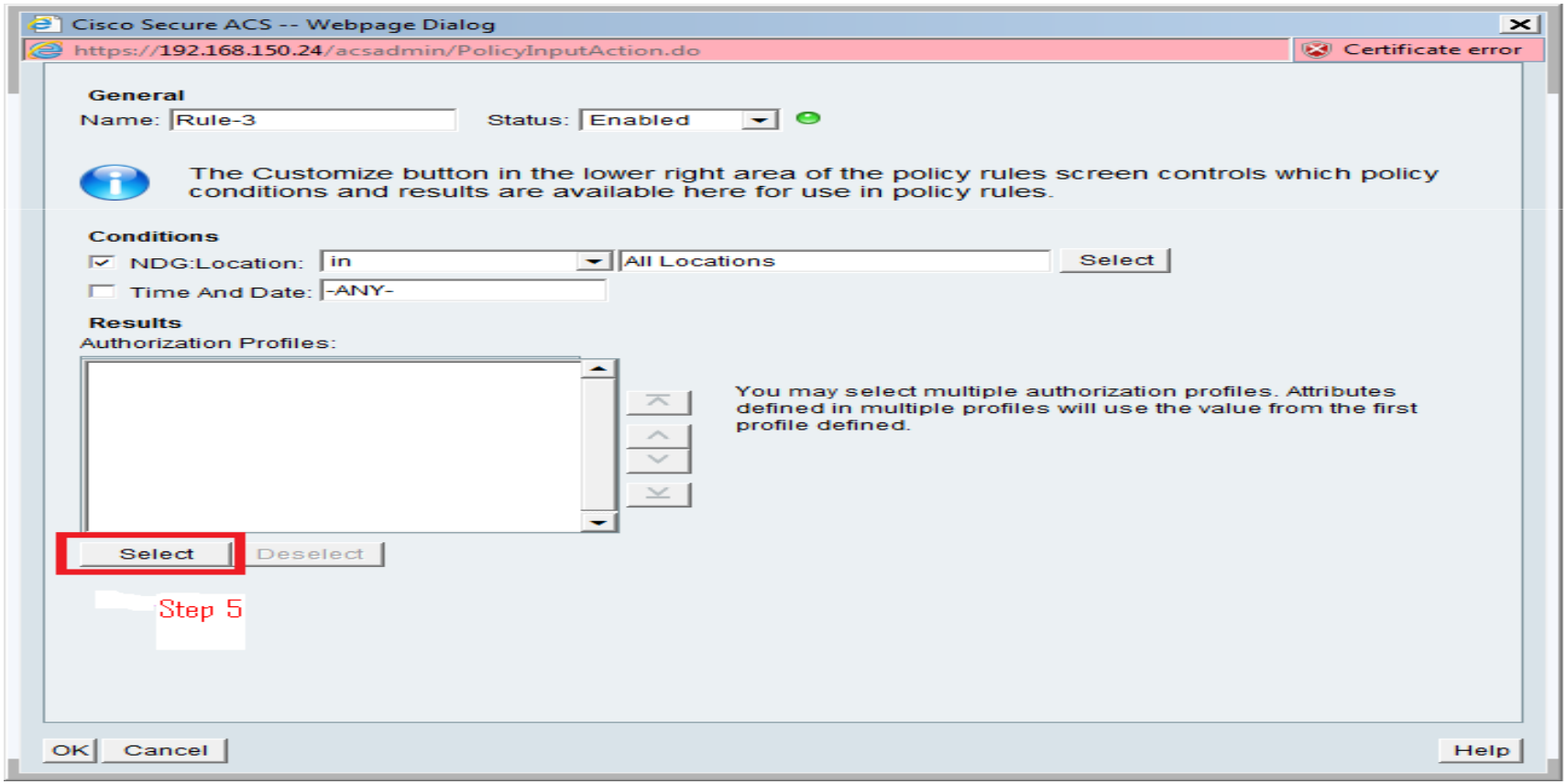
Management Login to WLC using ACS 5.x server

- After defining the Radius Attributes, we have to apply these attributes into Device Access policy on the ACS 5.x.



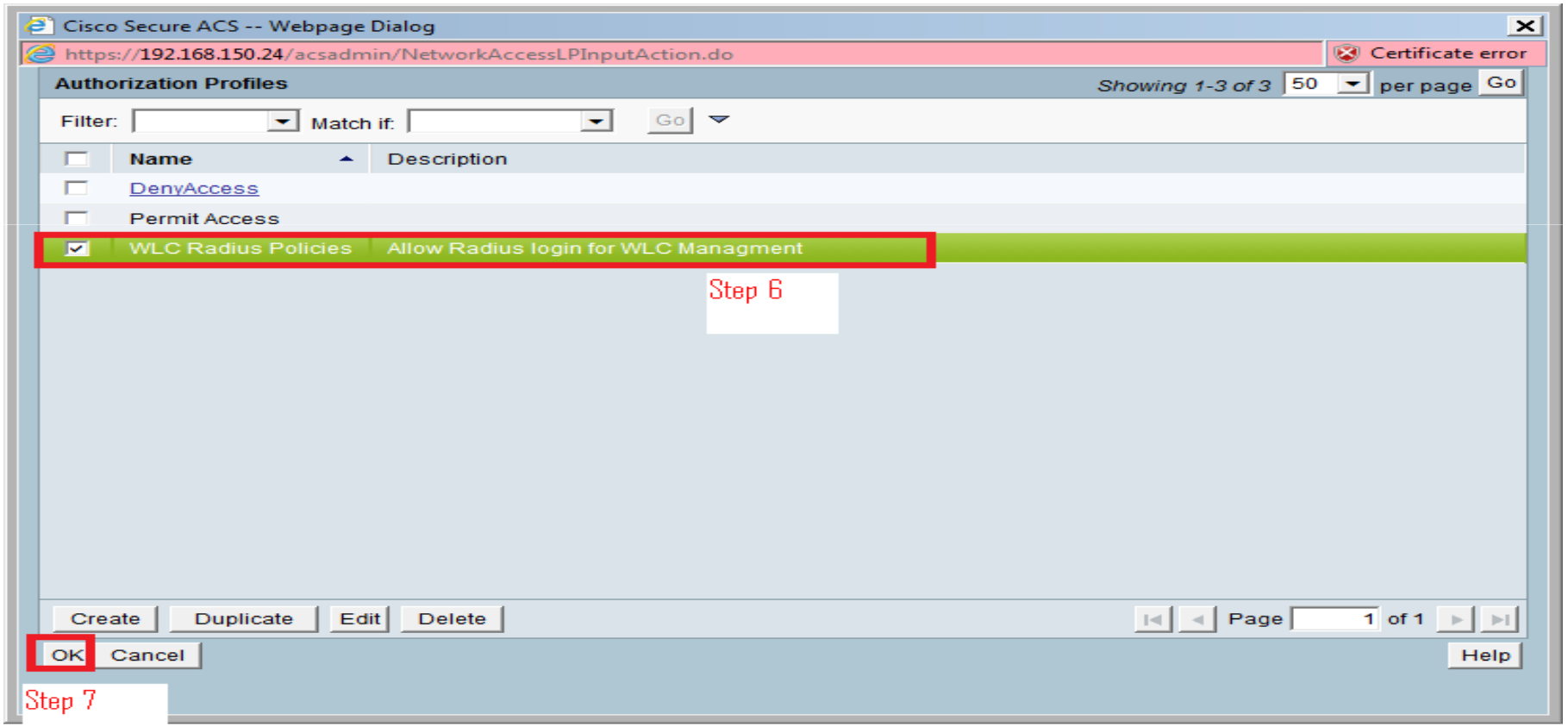
Management Login to WLC using ACS 5.x server

- Select the WLC Access Policy which we defined under Policy Elements with the Radius Attributes for the user group to login.

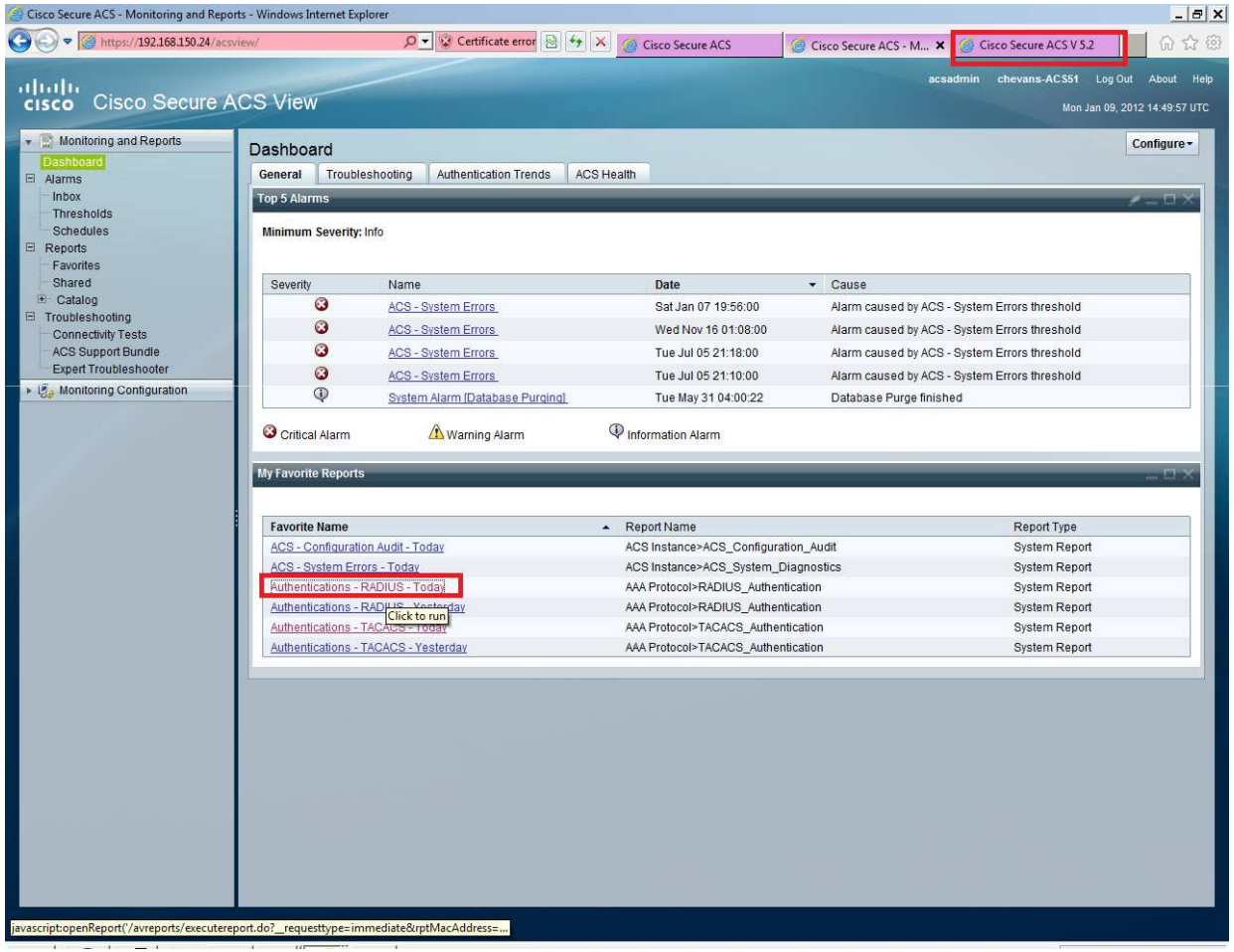


Management Login to WLC using ACS 5.x server

- We select the Policy Element which we created to be applied in this Rule.



Checking failed logs on ACS 5.x



Debug From the WLC when using Radius for Authentication of user

- The output of debugs on the WLC whether using ACS 4.2 or 5.x is the same as below.

```
debug aaa all enable
*aaaQueueReader: Jan 09 10:50:49.194:                Callback.....0x108f11e0
*aaaQueueReader: Jan 09 10:50:49.194:                protocolType.....0x00020021
*aaaQueueReader: Jan 09 10:50:49.194:                proxyState.....00:00:00:0E:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.194:                Packet contains 5 AVPs (not shown)
*aaaQueueReader: Jan 09 10:50:49.195: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Jan 09 10:50:49.195: 00:00:00:0e:00:00 Successful transmission of Authentication Packet (id 148) to 192.168.150.24:1812, proxy state 00:00:00:0e:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.195: 00000000: 01 94 00 41 00 00 00 00  00 00 00 00 00 00 00 00  ...A............
*aaaQueueReader: Jan 09 10:50:49.195: 00000010: 00 00 00 00 01 07 63 69  73 63 6f 02 12 cc 28 41  ......cisco...(A
*aaaQueueReader: Jan 09 10:50:49.195: 00000020: ab 74 b9 56 0b 11 bc 9a  5d 59 ed ca 23 06 06 00  .t.V....]Y..#...
*aaaQueueReader: Jan 09 10:50:49.195: 00000030: 00 00 07 04 06 c0 a8 4b  2c 20 08 35 35 30 38 2d  .......K,..5508-
*aaaQueueReader: Jan 09 10:50:49.195: 00000040: 33                                            3
*radiusTransportThread: Jan 09 10:50:49.198: 00000000: 02 94 00 43 a8 0f 69 59  2f e8 4b 67 e5 ef 10 d0  ...C..iY/.Kg....
*radiusTransportThread: Jan 09 10:50:49.198: 00000010: 57 90 8b 68 01 07 63 69  73 63 6f 06 06 00 00 00  W..h..cisco.....
*radiusTransportThread: Jan 09 10:50:49.198: 00000020: 06 19 22 43 41 43 53 3a  63 68 65 76 61 6e 73 2d  ..''CACS:chevans-
*radiusTransportThread: Jan 09 10:50:49.198: 00000030: 41 43 53 35 31 2f 31 31  35 32 33 32 30 34 39 2f  ACS51/115232049/
*radiusTransportThread: Jan 09 10:50:49.198: 00000040: 31 30 33                                  103
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: 00:00:00:0e:00:00 Access-Accept received from RADIUS server 192.168.150.24 for mobile 00:00:00:0e:00:00 receiveId = 0
*radiusTransportThread: Jan 09 10:50:49.198: AuthorizationResponse: 0x14afbb40
*radiusTransportThread: Jan 09 10:50:49.198:                structureSize.....121
*radiusTransportThread: Jan 09 10:50:49.198:                resultCode.....0
*radiusTransportThread: Jan 09 10:50:49.198:                protocolUsed.....0x00000001
*radiusTransportThread: Jan 09 10:50:49.198:                proxyState.....00:00:00:0E:00:00-00:00
*radiusTransportThread: Jan 09 10:50:49.198:                Packet contains 3 AVPs:
*radiusTransportThread: Jan 09 10:50:49.198:                  AVP[01] User-Name.....cisco (5 bytes)
*RADIUSTRANSPORTTHREAD: JAN 09 10:50:49.198:                  AVP[02] SERVICE-TYPE.....0X00000006 (6) (4 BYTES)
*radiusTransportThread: Jan 09 10:50:49.198:                  AVP[03] Class.....CACS:chevans-ACS51/115232049/103 (32 bytes)
*emWeb: Jan 09 10:50:49.198: Authentication succeeded for cisco
```

Debug From the WLC when using Radius for Authentication of user

- Failed user login:

aaaQueueReader: Jan 09 10:42:00.622: 00:00:00:05:00:00 Successful transmission of Authentication Packet (id 139) to 192.168.150.24:1812, proxy state 00:00:00:05:00:00-00:00

*radiusTransportThread: Jan 09 10:42:00.626: ****Enter processIncomingMessages: response code=3

*radiusTransportThread: Jan 09 10:42:00.626: ****Enter processRadiusResponse: response code=3

*radiusTransportThread: Jan 09 10:42:00.626: 00:00:00:05:00:00 Access-Reject received from RADIUS server 192.168.150.24 for mobile 00:00:00:05:00:00 receiveId = 0

*radiusTransportThread: Jan 09 10:42:00.627: 00:00:00:05:00:00 Returning AAA Error 'Authentication Failed' (-4) for mobile 00:00:00:05:00:00

*emWeb: Jan 09 10:42:00.628: Authentication failed for admin

aaaQueueReader: Jan 09 10:42:14.905: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0

*aaaQueueReader: Jan 09 10:42:14.905: 00:00:00:06:00:00 Successful transmission of Authentication Packet (id 140) to 192.168.150.24:1812, proxy state 00:00:00:06:00:00-00:00

*radiusTransportThread: Jan 09 10:42:14.909: ****Enter processIncomingMessages: response code=3

*radiusTransportThread: Jan 09 10:42:14.909: ****Enter processRadiusResponse: response code=3

*radiusTransportThread: Jan 09 10:42:14.909: **00:00:00:06:00:00 Access-Reject received from RADIUS server 192.168.150.24 for mobile 00:00:00:06:00:00 receiveId = 0**

*radiusTransportThread: Jan 09 10:42:14.910: 00:00:00:06:00:00 Returning AAA Error 'Authentication Failed' (-4) for mobile 00:00:00:06:00:00

*emWeb: Jan 09 10:42:14.910: Authentication failed for admin

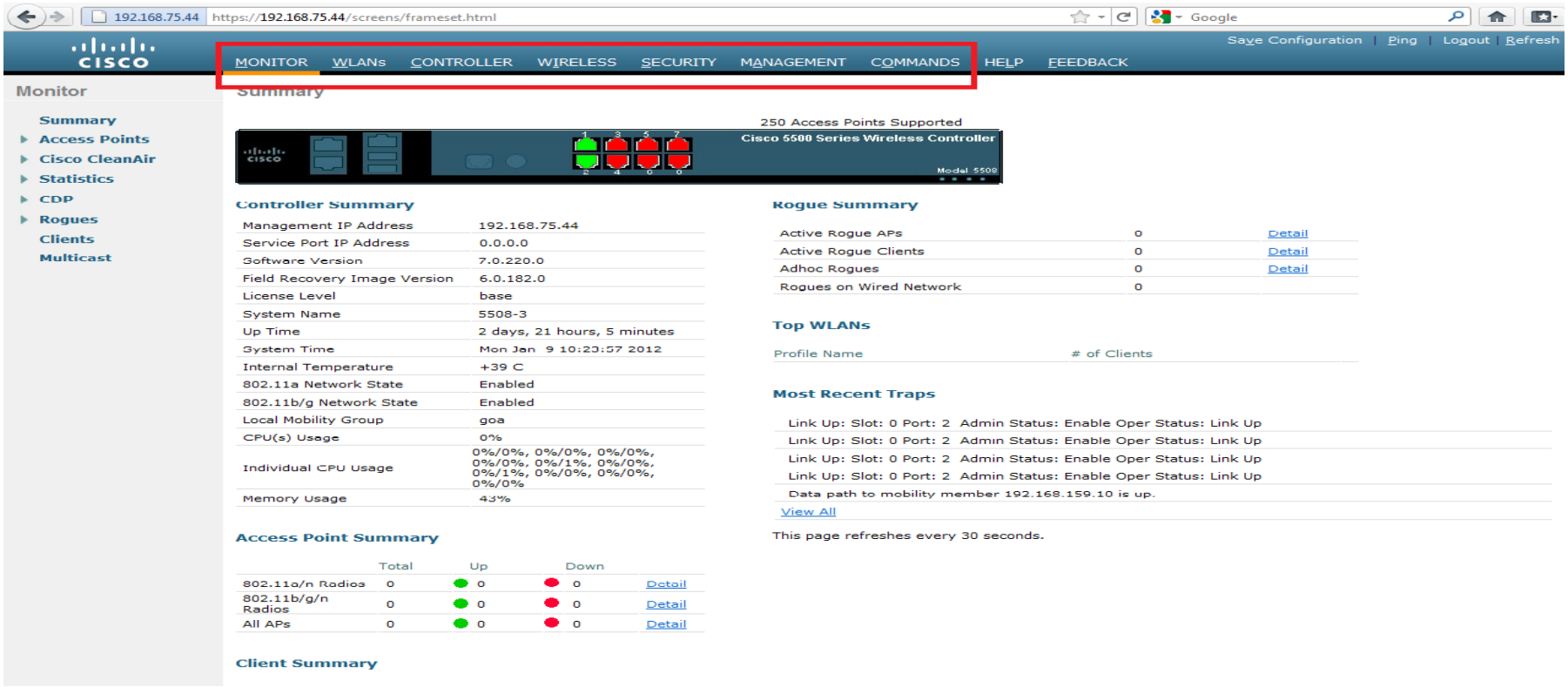
Debug From the WLC when using Radius for Authentication of user

- User passes authentication from Radius but the Attribute is not correct:

```
*aaaQueueReader: Jan 09 10:50:49.194:          Callback.....0x108f11e0
*aaaQueueReader: Jan 09 10:50:49.194:          protocolType.....0x00020021
*aaaQueueReader: Jan 09 10:50:49.194:          proxyState.....00:00:00:0E:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.194:          Packet contains 5 AVPs (not shown)
*aaaQueueReader: Jan 09 10:50:49.195: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Jan 09 10:50:49.195: 00:00:00:0e:00:00 Successful transmission of Authentication Packet (id 148) to 192.168.150.24:1812, proxy state
      00:00:00:0e:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.195: 00000000: 01 94 00 41 00 00 00 00  00 00 00 00 00 00 00 00  ...A............
*aaaQueueReader: Jan 09 10:50:49.195: 00000010: 00 00 00 00 01 07 63 69  73 63 6f 02 12 cc 28 41  ......cisco...(A
*aaaQueueReader: Jan 09 10:50:49.195: 00000020: ab 74 b9 56 0b 11 bc 9a  5d 59 ed ca 23 06 06 00  .t.V....]Y..#...
*aaaQueueReader: Jan 09 10:50:49.195: 00000030: 00 00 07 04 06 c0 a8 4b  2c 20 08 35 35 30 38 2d  .......K,..5508-
*aaaQueueReader: Jan 09 10:50:49.195: 00000040: 33                                           3
*radiusTransportThread: Jan 09 10:50:49.198: 00000000: 02 94 00 43 a8 0f 69 59  2f e8 4b 67 e5 ef 10 d0  ...C..iY/.Kg....
*radiusTransportThread: Jan 09 10:50:49.198: 00000010: 57 90 8b 68 01 07 63 69  73 63 6f 06 06 00 00 00  W..h..cisco.....
*radiusTransportThread: Jan 09 10:50:49.198: 00000020: 06 19 22 43 41 43 53 3a  63 68 65 76 61 6e 73 2d  ..."CACS:chevans-
*radiusTransportThread: Jan 09 10:50:49.198: 00000030: 41 43 53 35 31 2f 31 31  35 32 33 32 30 34 39 2f  ACS51/115232049/
*radiusTransportThread: Jan 09 10:50:49.198: 00000040: 31 30 33                                  103
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: 00:00:00:0e:00:00 Access-Accept received from RADIUS server 192.168.150.24 for mobile
      00:00:00:0e:00:00 receiveId = 0
*radiusTransportThread: Jan 09 10:50:49.198: AuthorizationResponse: 0x14afbb40
*radiusTransportThread: Jan 09 10:50:49.198:          structureSize.....121
*radiusTransportThread: Jan 09 10:50:49.198:          resultCode.....0
*radiusTransportThread: Jan 09 10:50:49.198:          protocolUsed.....0x00000001
*radiusTransportThread: Jan 09 10:50:49.198:          proxyState.....00:00:00:0E:00:00-00:00
*radiusTransportThread: Jan 09 10:50:49.198:          Packet contains 3 AVPs:
*radiusTransportThread: Jan 09 10:50:49.198:              AVP[01] User-Name.....cisco (5 bytes)
*radiusTransportThread: Jan 09 10:50:49.198:              AVP[03] Class.....CACS:chevans-ACS51/115232049/103 (32 bytes)
*emWeb: Jan 09 10:50:49.198: Authentication succeeded for cisco
```

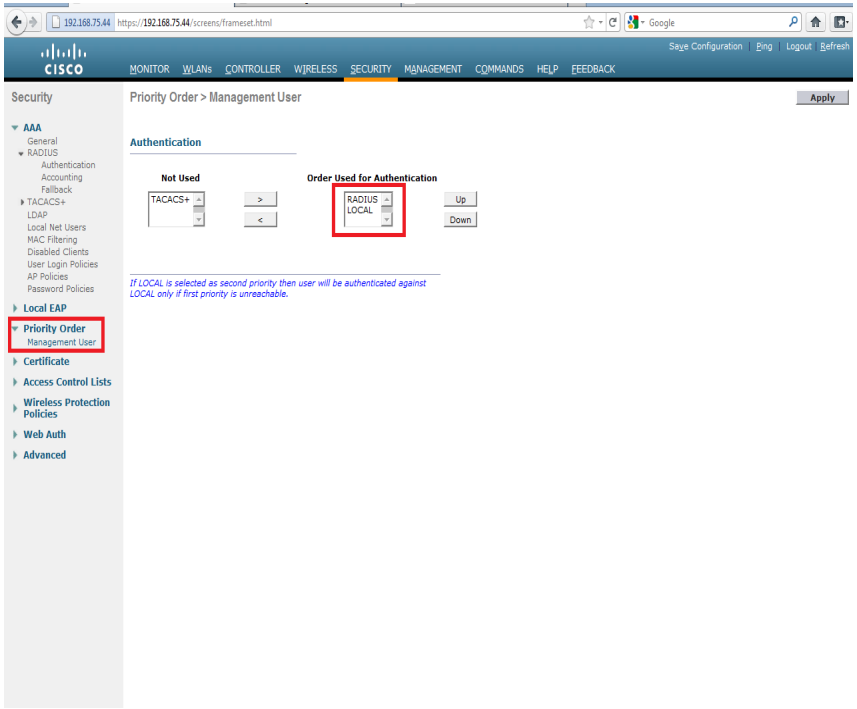
Common Troubleshooting issues

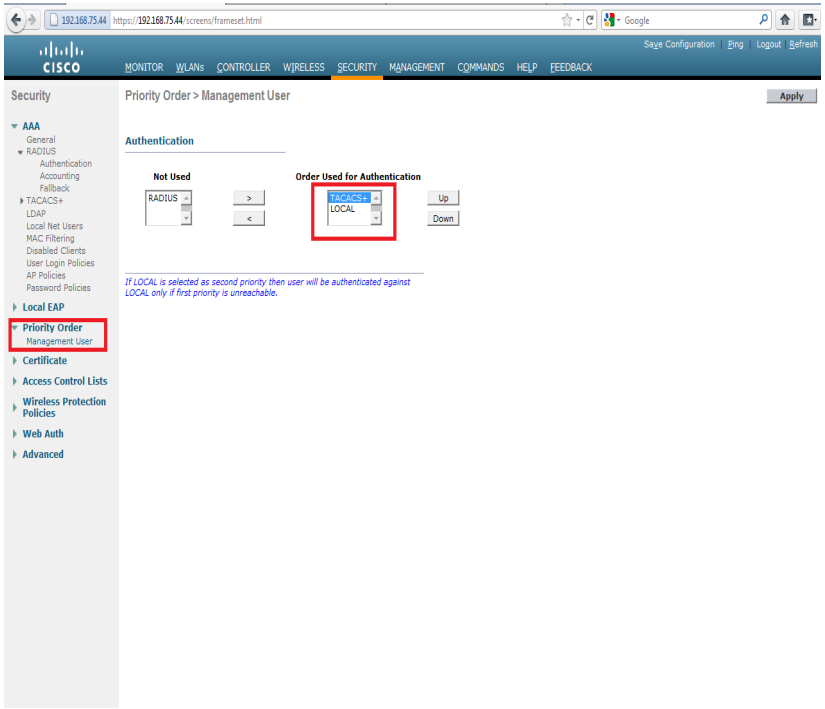
- Usually we see the issue with TACACS login when the role is not defined correctly on the ACS server. The role has to be from the first bar on the WLC as shown below.



Troubleshooting

- Always try to have a backup entry such as WCS or Console session into the WLC before changing the priority on the WLC from Local to TACACS or Radius.





Troubleshooting

- Show tacacs auth statistics, show tacacs acct statistics and show tacacs athr statistics are helpful commands to see any passed and failed attempts.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:
Server Index..... 1
Server Address..... 192.168.150.24
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
Server Index..... 2
Server Address..... 192.168.150.152
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- A new bug on 7.0.220.0 where the AAA queue is full due to which the authentication to the WLC GUI via TACACS is not possible.
- Bug id is : CSCtx03556, we see the TPLUS Transmission Queue is full– Dropping Accounting Packet when running aaa debug on the WLC.

Some Useful Links for Radius and TACACS Login

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a0080871921.shtml

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a0080782507.shtml

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_tech_note09186a0080851f7c.shtml

http://www.cisco.com/en/US/docs/wireless/wcs/7.0/configuration/guide/7_0admin.html#wpmkr1064294