Central Web Authentication on Converged Access and Unified Access WLCs Configuration Example

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Topology 1
- Topology 2
- Topology 3
- Example
- Topology 1 Configuration Example
  - Configuration on the ISE
  - Configuration on the WLC
- Topology 2 Configuration Example
  - Configuration on the ISE
  - Configuration on the WLC
- Topology 3 Configuration Example
  - Configuration on the ISE
  - Configuration on the WLC

Verify

Troubleshoot

Introduction

This document describes how to configure central web authentication on the Converged Access Wireless LAN Controller (WLC) and also between the Converged Access WLC and Unified Access WLC (5760 and also between 5760 and 5508).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco WLC 5508, 5760, 3850
- Basic knowledge of Identity Services Engine (ISE)
- Basic knowledge of Wireless Mobility
- Basic knowledge of guest anchoring

Components Used

The information in this document is based on these software and hardware versions:

- WLC 5760 that runs Cisco IOS® XE Release 3.3.3
- WLC 5508 that runs Cisco Aironet OS Release 7.6
- Switch 3850 that runs Cisco IOS XE Release 3.3.3
- Cisco ISE that runs Release 1.2

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

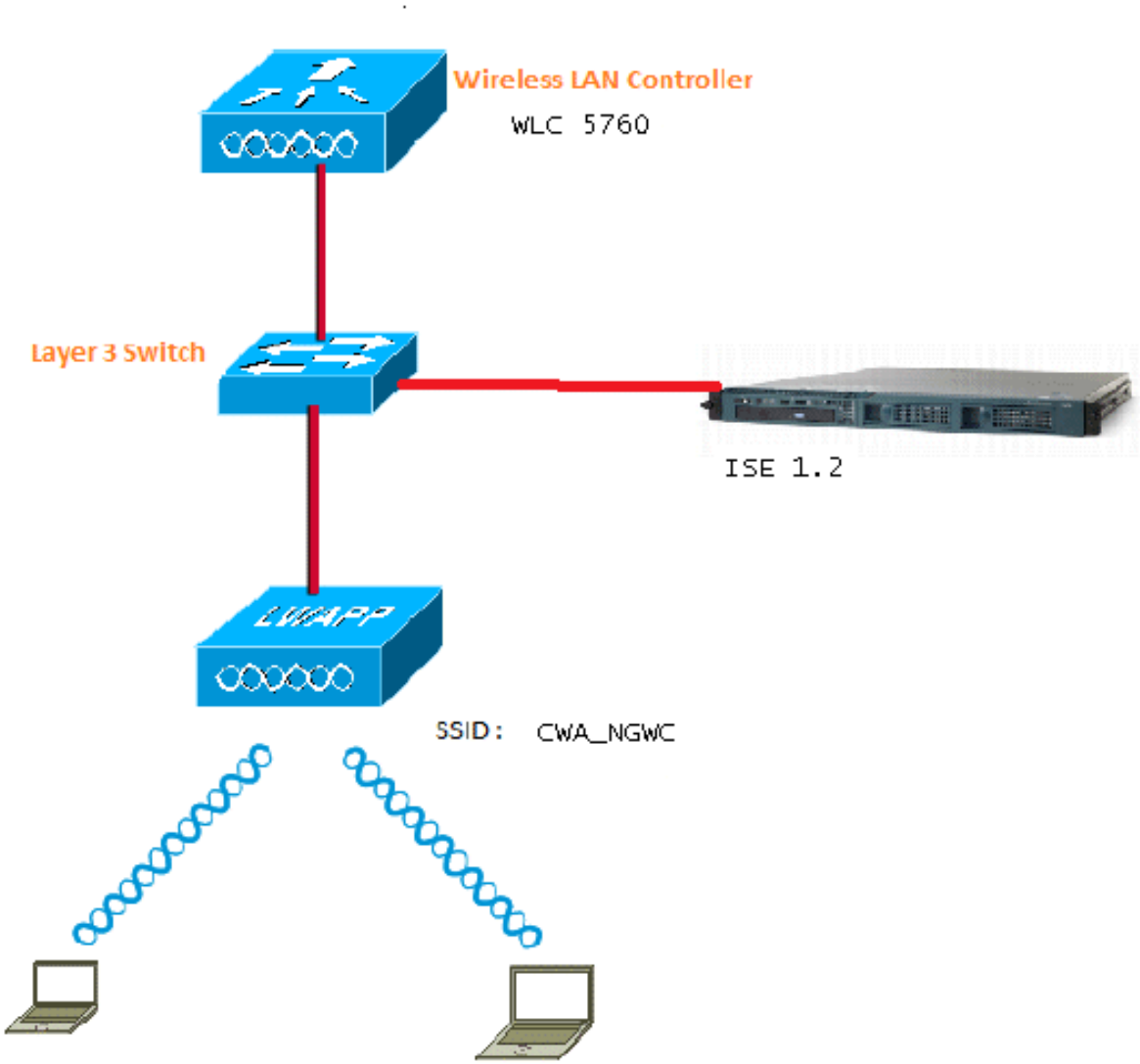
The flow includes these steps:

1. The user associates to the web authentication Service Set Identifier (SSID), which is in fact open+macfiltering and no Layer 3 security.
2. The user opens the browser.
3. The WLC redirects to the guest portal.
4. The user authenticates on the portal.
5. The ISE sends a RADIUS Change of Authorization (CoA - UDP Port 1700) in order to indicate to the controller that the user is valid, and eventually pushes RADIUS attributes such as the Access Control List (ACL).
6. The user is prompted to retry the original URL.

Cisco uses three different deployment setups that cover all the different scenarios to accomplish Central Web Authentication (CWA).

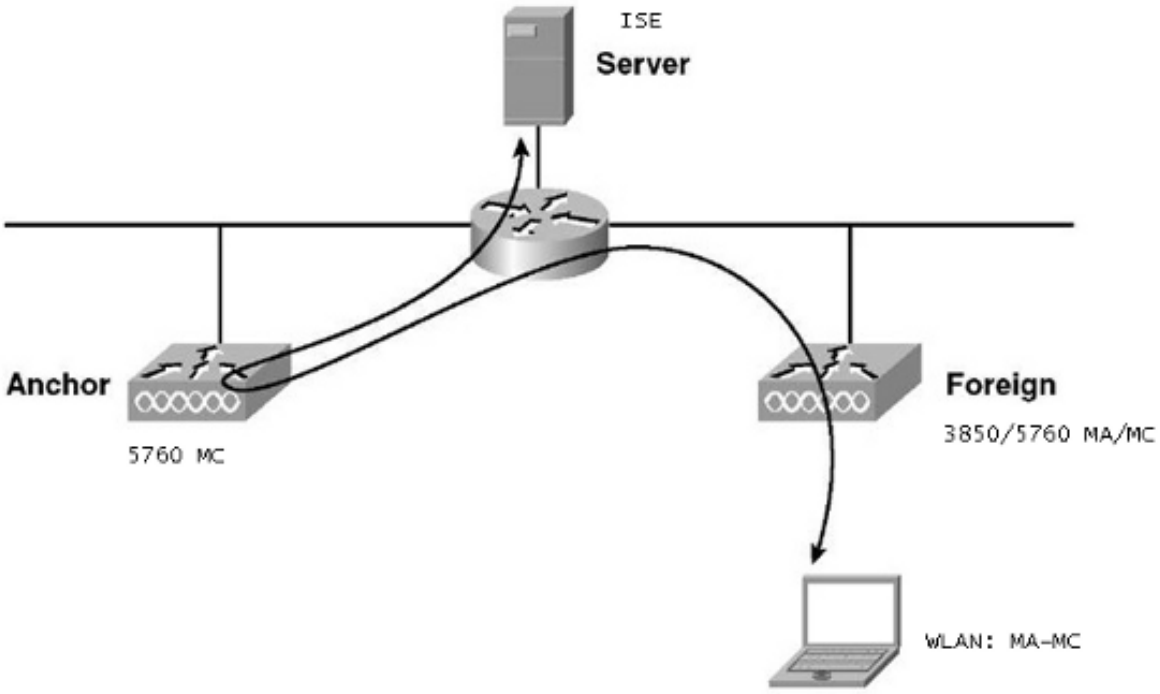
Topology 1

The 5760 WLC acts as a standalone WLC and the Access Points terminate on the same 5760 WLC. The clients are connected to Wireless LAN (WLAN) and are authenticated to the ISE.



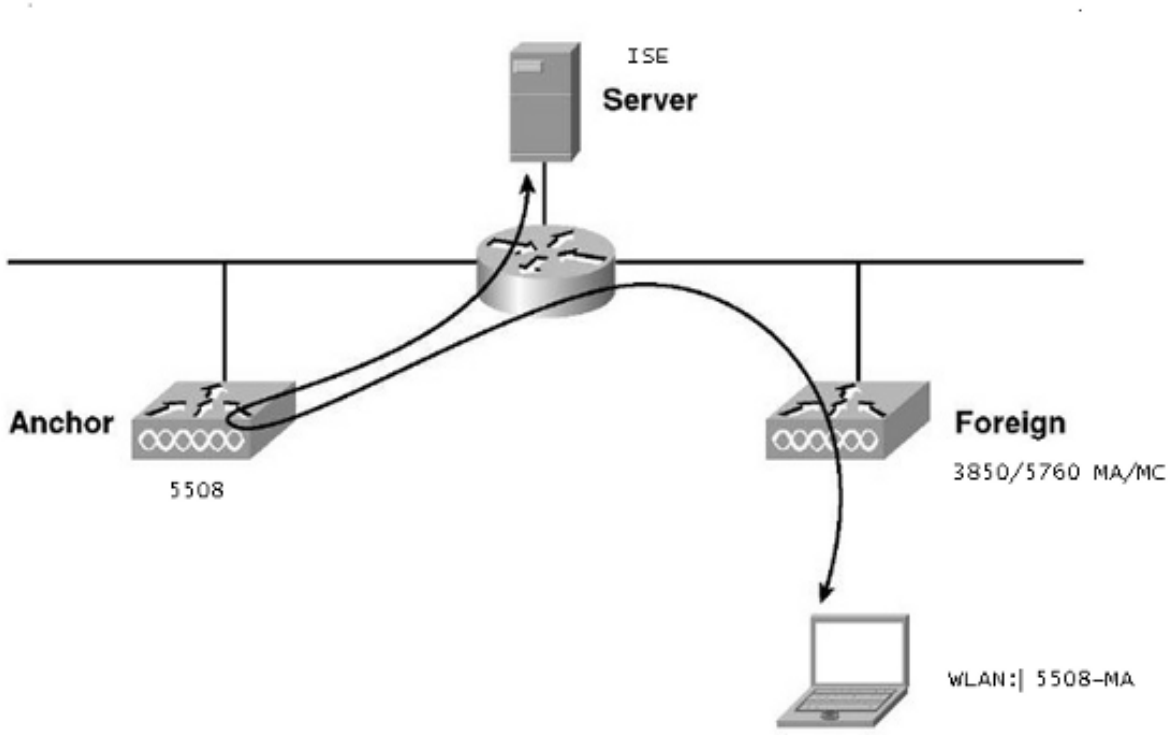
Topology 2

Guest anchoring between the Converged Access WLC with one that acts as a Mobility Controller and the other that acts as a Mobility Agent. The Mobility Agent is the Foreign WLC and the Mobility Controller is the Anchor.



Topology 3

Guest anchoring between the Cisco Unified WLC 5508 and Converged Access WLC 5760/3850 with one that acts as a Mobility Controller and the other that acts as a Mobility Agent. The Mobility Agent/Mobility Controller is the Foreign WLC and the 5508 Mobility Controller is the Anchor.



Note: There are a lot of deployments where the Anchor is the Mobility Controller and the Foreign WLC is the Mobility Agent which obtains the license from another Mobility Controller. In this case, the Foreign WLC has only one Anchor and that Anchor is the one that pushes the policies. Double anchoring is not supported and does not work since it is not expected to work that way.

Example

The WLC 5508 acts as the Anchor and the WLC 5760 acts as the Mobility Controller for a 3850 Switch which acts as a Mobility Agent. For the Anchor Foreign WLAN, the WLC 5508 will be the Anchor for the 3850 Foreign WLAN. There is no need to configure that WLAN on the WLC 5760 at all. If you point the 3850 Switch to the 5760 Anchor, and then from this WLC 5760 to the WLC 5508 as a double anchor, it will not work since this becomes double anchoring and the policies are on the 5508 Anchor.

If you have a setup that includes a WLC 5508 as the Anchor, a WLC 5760 as the Mobility Controller, and a 3850 Switch as the Mobility Agent and Foreign WLC, then at any point of time the Anchor for the 3850 Switch will either be the WLC 5760 or the WLC 5508. It cannot be both the at the same time and the double anchor does not work.

Topology 1 Configuration Example

See Topology 1 for the network diagram and explanation.

The configuration is a two step process:

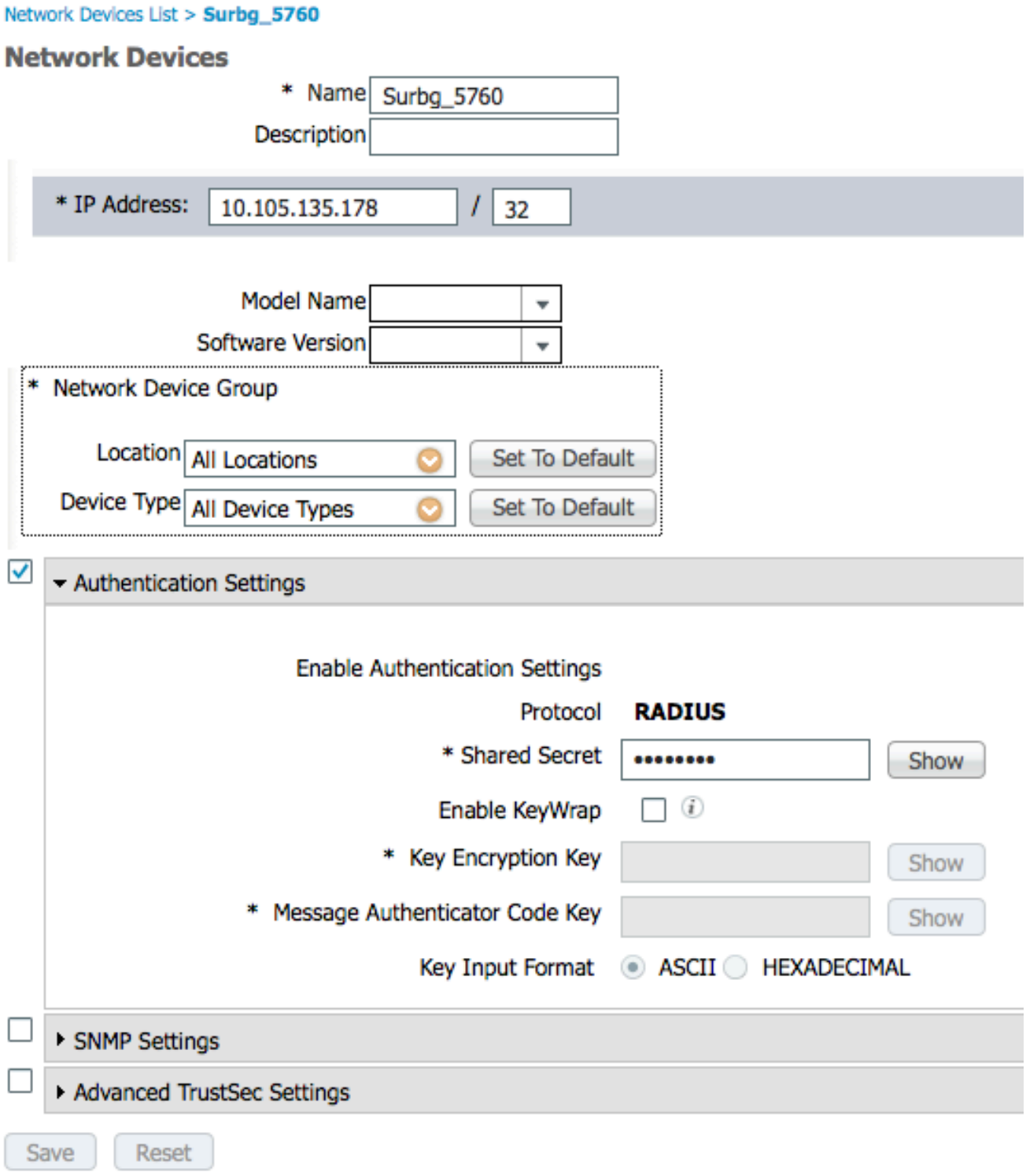
1. Configuration on the ISE.
2. Configuration on the WLC.

The WLC 5760 acts as a standalone WLC and the users get authenticated to the ISE.

Configuration on the ISE

1. Choose **ISE GUI > Administration > Network Resource > Network Devices List > Add** in order to add the WLC on the ISE as the Authentication, Authorization, and Accounting (AAA) client. Ensure you enter the same shared secret on the WLC that is added on the RADIUS server.

Note: While you deploy Anchor-Foreign, you just need to add the Foreign WLC. There is no need to add the Anchor WLC on the ISE as an AAA client. The same ISE configuration is used for all the other deployment scenarios in this document.



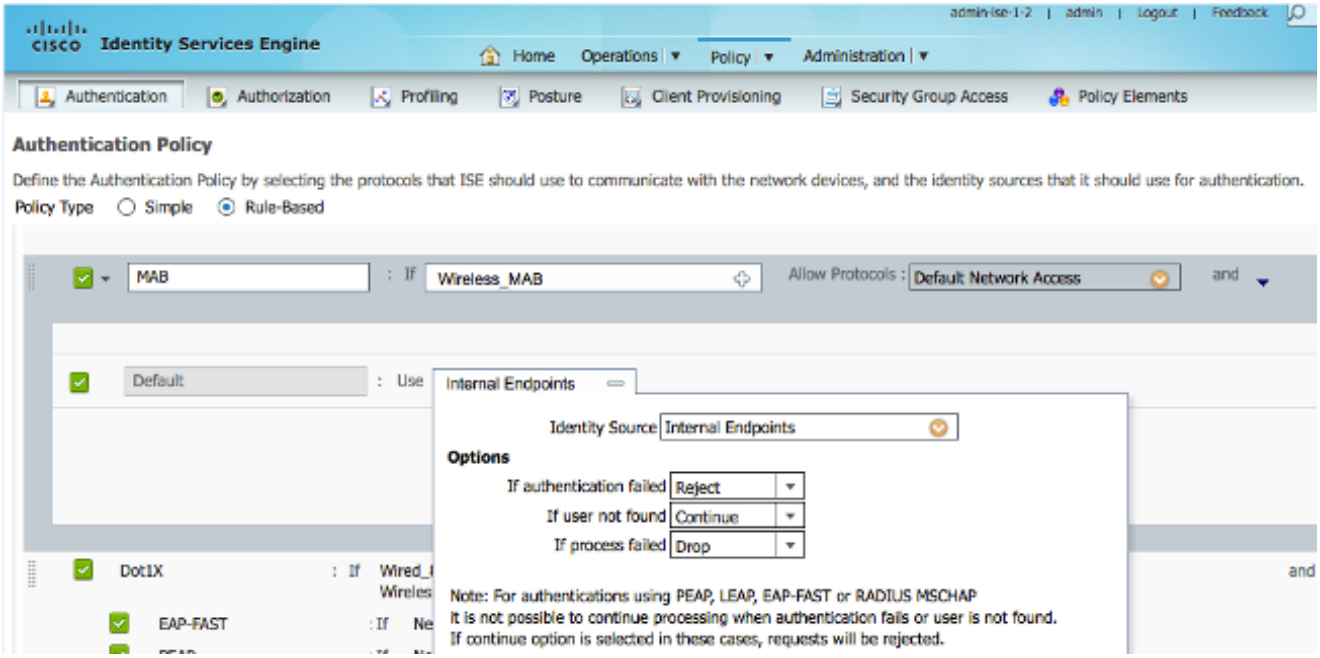
2. From the ISE GUI, choose **Policy > Authentication > MAB > Edit** in order to create the authentication policy. The authentication policy accepts the MAC address of the client, which points to Internal End points.

   Choose these selections in the Options list:

   - From the If authentication failed drop-down list, choose **Reject**.
   - From the If user not found drop-down list, choose **Continue**.
   - From the If process failed drop-down list, choose **Drop**.

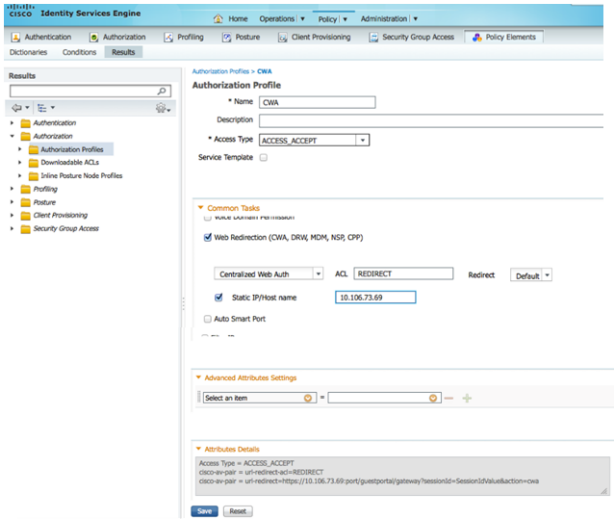
   When you configure with these options, the client that fails MAC authorization proceeds with the

guest portal.



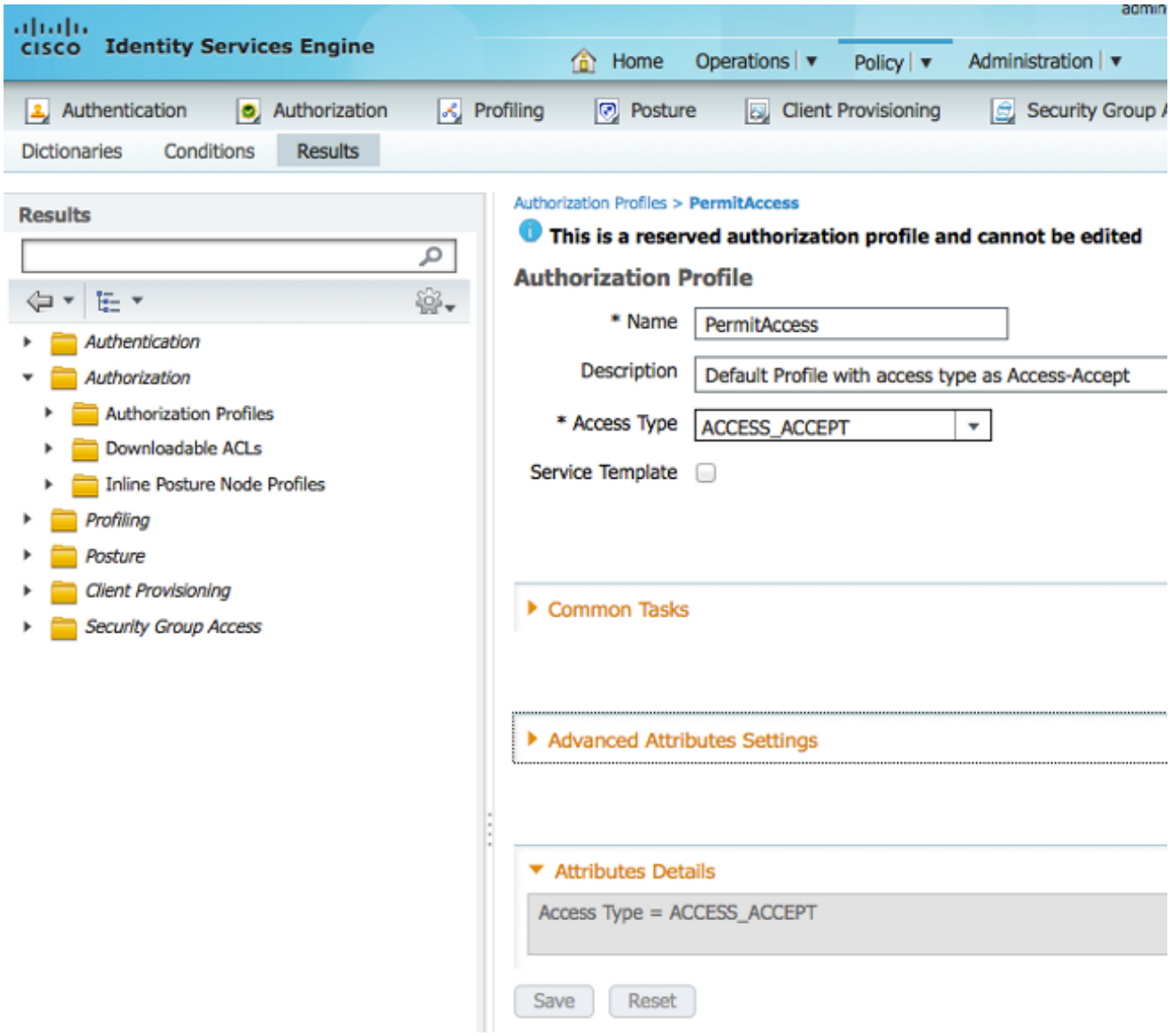
3. From the ISE GUI, choose **Policy > Authorization > Results > Authorization Profiles > Add**. Fill in the details and click **Save** in order to create the Authorization profile.

   This profile helps the clients to get redirected to the Redirect URL after the MAC authentication,



   where the clients enter the Guest Username/password.

4. From the ISE GUI, choose **Policy > Authorization > Results > Authorization Profiles > Add** in order to create another Authorization profile to permit access to the users with the correct credentials.

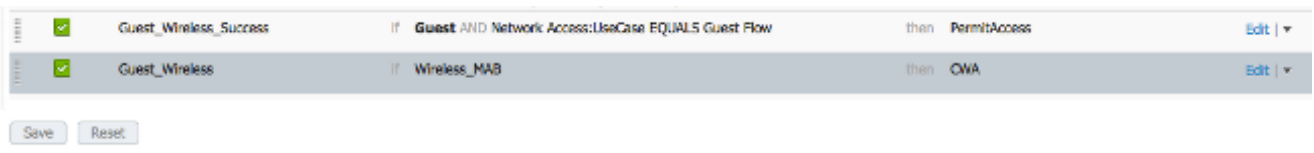


5. Create the Authorization policies.

   The Authorization policy 'Guest_Wireless' pushes the Redirect URL and Redirect ACL to the client session. The profile pushed here is the CWA as shown previously.

   The Authorization policy 'Guest_Wireless-Sucess' gives full access to a guest user who is succesfully authenticated via the guest portal. After the user is successfully authenticated on the guest portal, dynamic authorization is sent by the WLC. This reauthenticates the client session with the attribute 'Network Access:Usecase EQUALS Guest Flow'.

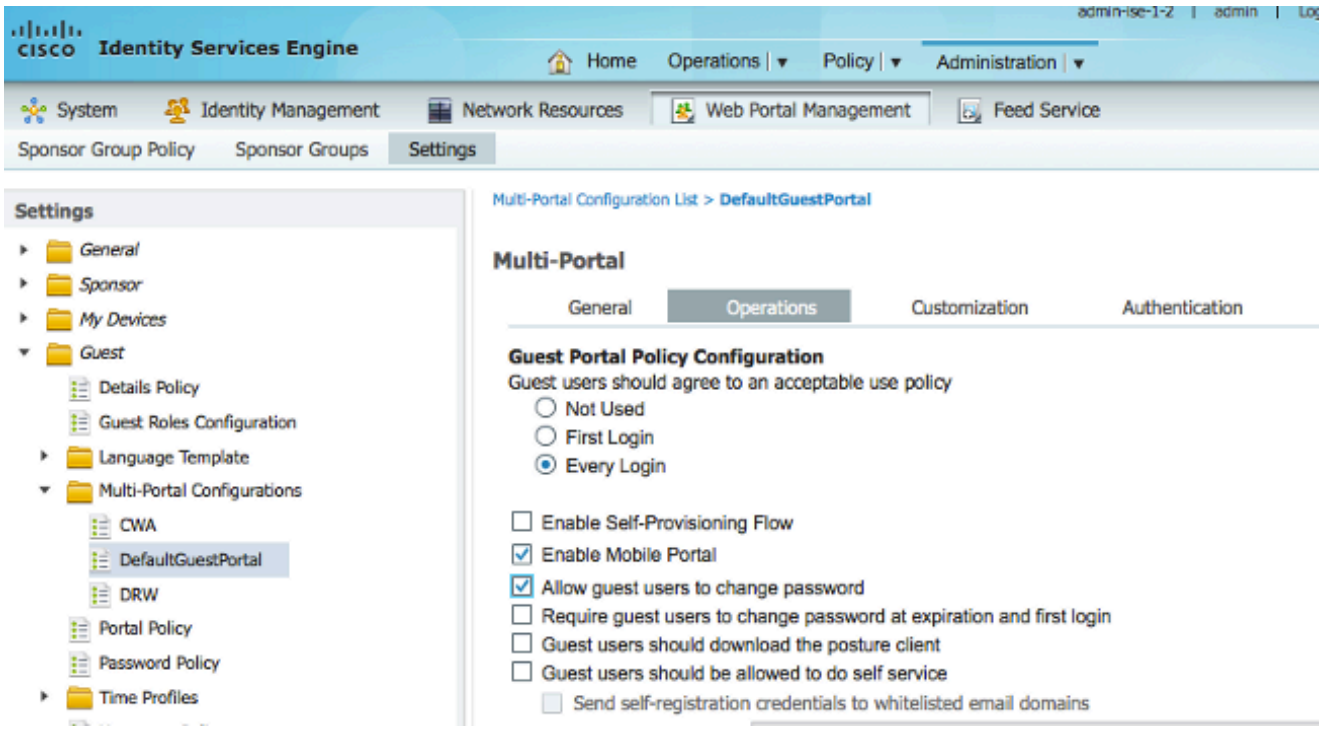
   The final Authorization policies look like:



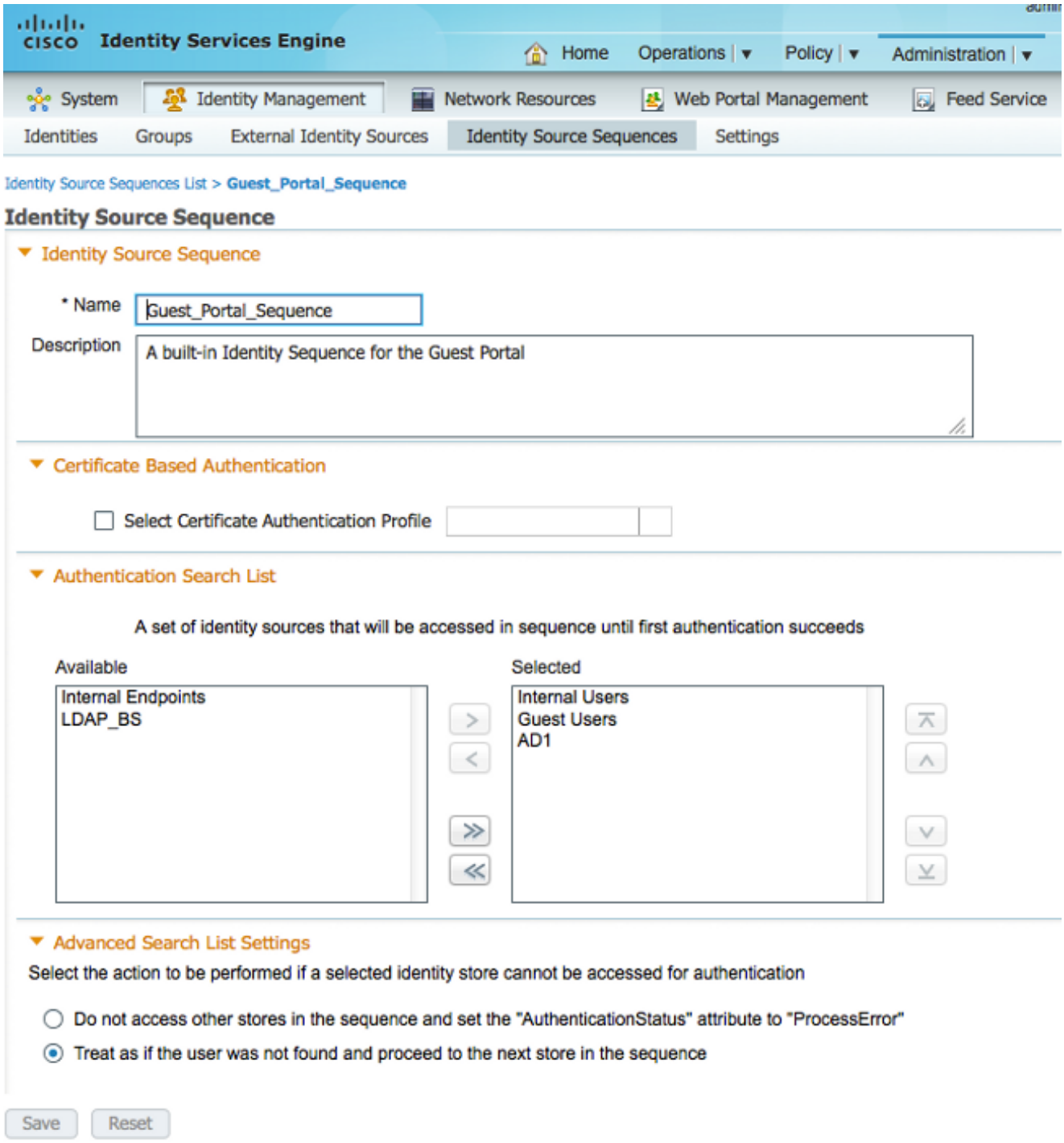
6. Optional: In this case default multiportal configurations are used. Based on the requirements, the same can be changed in the GUI.

   From the ISE GUI, choose **Administration > Web Portal management > Multi Portal**

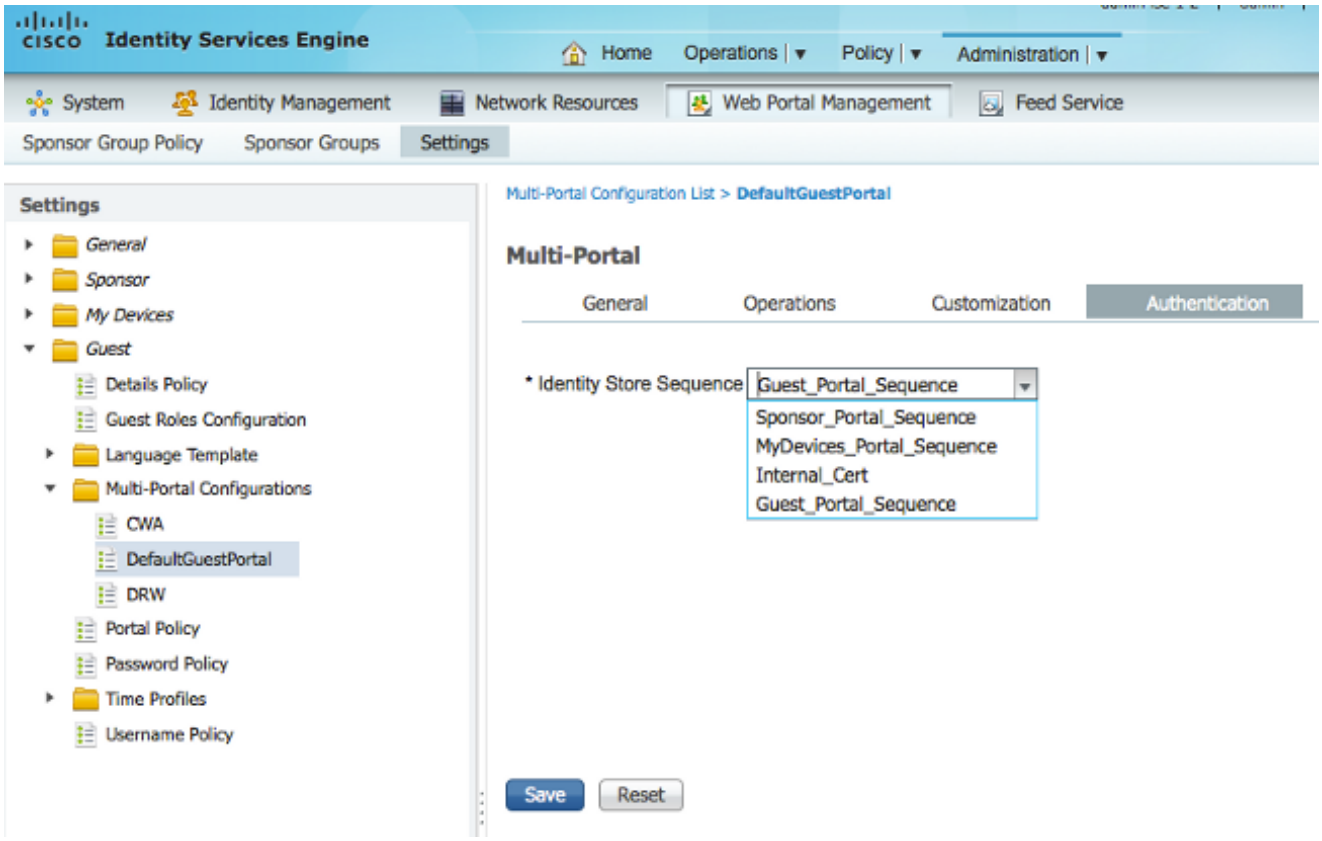
Configurations > DefaultGuestPortal.



The Guest_Portal_sequence is created that allows the Internal, Guest, and AD users.



7. From the ISE GUI, choose **Guest > Multi-Portal Configurations > DefaultGuestPortal**. From the Identify Store Sequence drop-down list, choose **Guest_Portal_Sequence**.



Configuration on the WLC

1. Define the ISE Radius server on the WLC 5760.
2. Configure the RADIUS server, server group, and method list with the CLI.
   <#root>

```
dot1x system-auth-control


radius server ISE


address ipv4 10.106.73.69 auth-port 1645 acct-port 1646


 timeout 10


 retransmit 3


 key Cisco123


aaa group server radius ISE
```

```
server name ISE

deadtime 10

aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author

client 10.106.73.69 server-key Cisco123

auth-type any
```

3. Configure the WLAN with the CLI.
<#root>

```
wlan CWA_NGWC 10 CWA_NGWC

 aaa-override

accounting-list ISE

client vlan VLAN0012
```

```
no exclusionlist

mac-filtering MACFILTER

nac

no security wpa

no security wpa akm dot1x

no security wpa wpa2

 no security wpa wpa2 ciphers aes

 security dot1x authentication-list ISE

 session-timeout 1800

 no shutdown
```

4. Configure the Redirect ACLs with the CLI.

   This is the url-redirect-acl that ISE returns as an AAA override along with the redirect URL for the guest portal redirection. It is a direct ACL which is used currently on the Unified architecture. This is a 'punt' ACL which is sort of a reverse ACL that you would normally use for Unified architecture. You need to block access to DHCP, the DHCP server, DNS, the DNS server, and the ISE server. Only allow www, 443, and 8443 as needed. This ISE guest portal uses port 8443 and the redirection still works with the ACL shown here. Here ICMP is enabled, but based on the security rules you can either deny or permit.

   <#root>

```
ip access-list extended REDIRECT

 deny icmp any any
```

```
deny udp any any eq bootps

deny udp any any eq bootpc

deny udp any any eq domain

deny ip any host 10.106.73.69

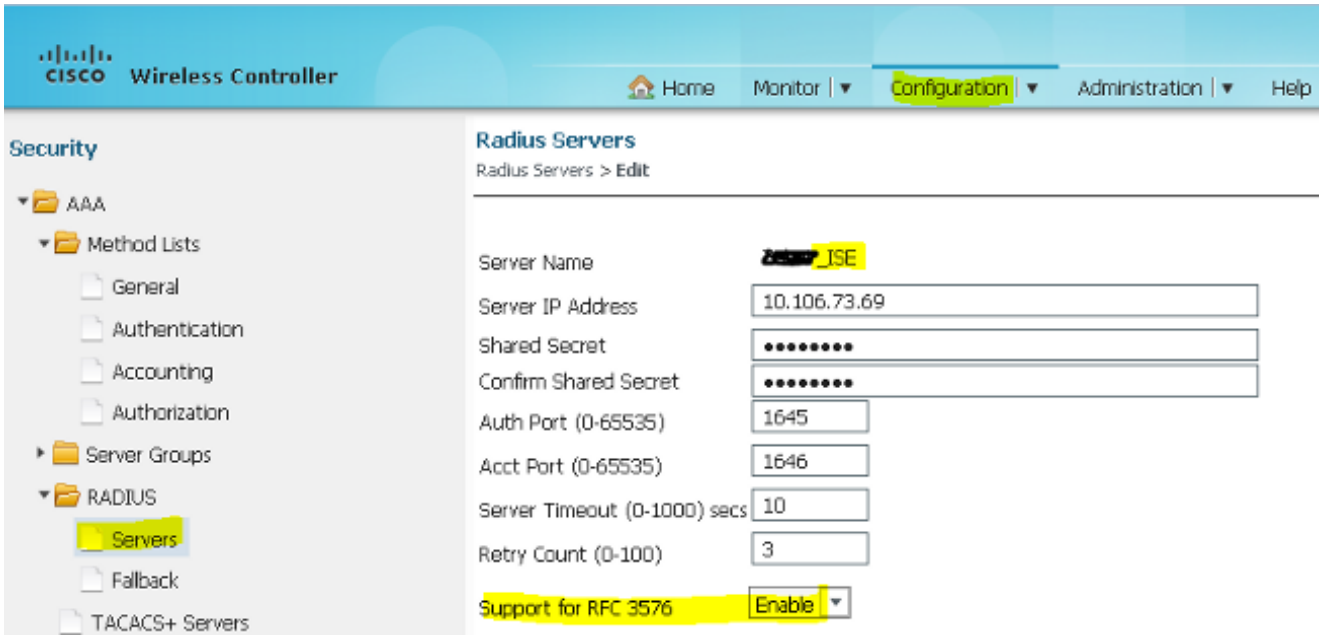
permit tcp any any eq www

permit tcp any any eq 443
```

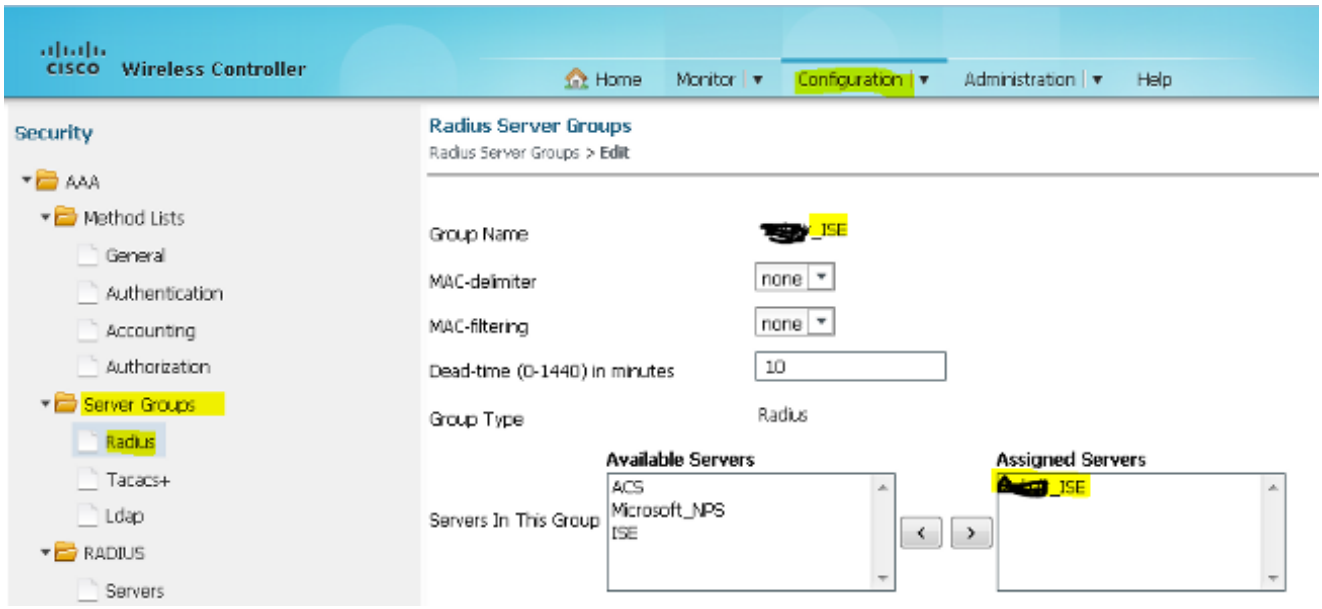
> ⚠ **Caution**: When you enable HTTPS, it might cause some high CPU issues due to scalability. Do not enable this unless it is recommemded by the Cisco design team.

5. From the Wireless Controller GUI, choose **AAA > RADIUS > Servers**. Configure the RADIUS Server, server group, and Method List in the GUI.

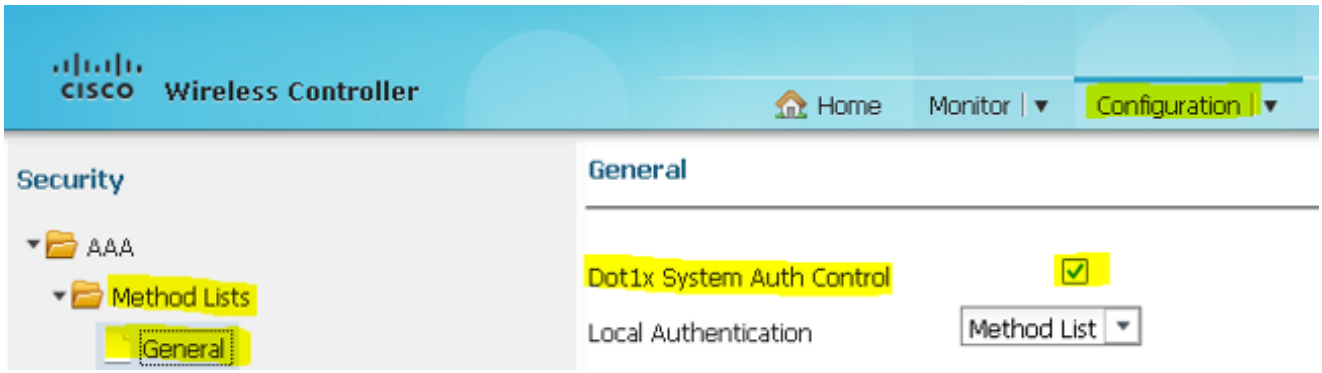
   Fill all the parameters and ensure the Shared Secret configured here matches the one configured on the ISE for this device. From the Support for RFC 3576 drop-down list, choose **Enable**.



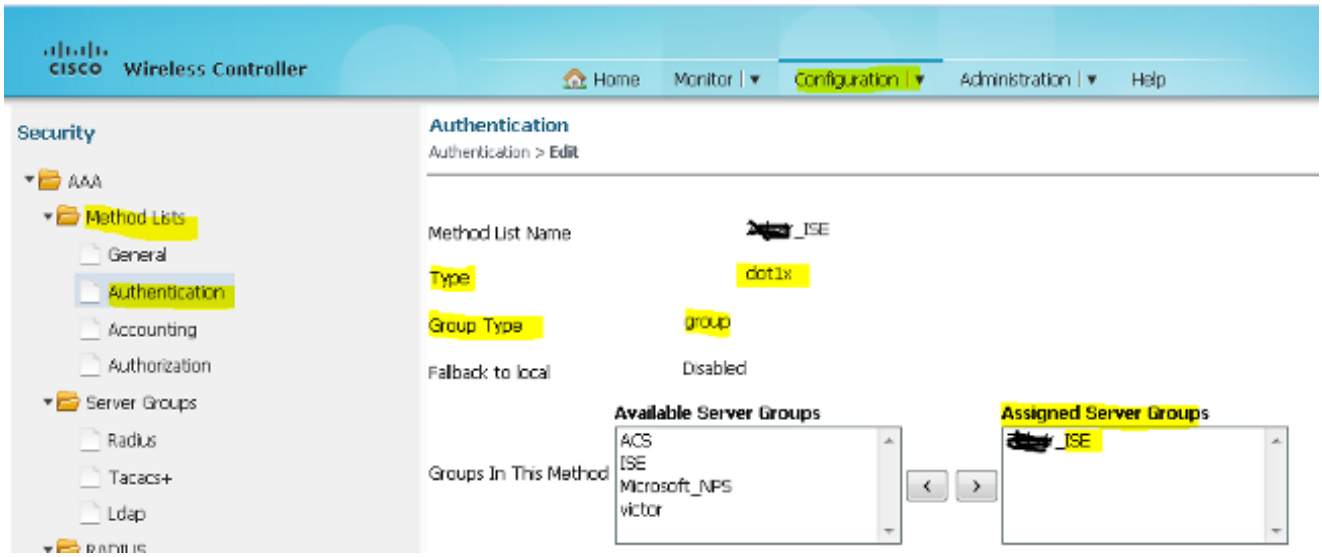
6. From the Wireless Controller GUI, choose **AAA > Server Groups > Radius**. Add the previously created RADIUS server onto the server groups.



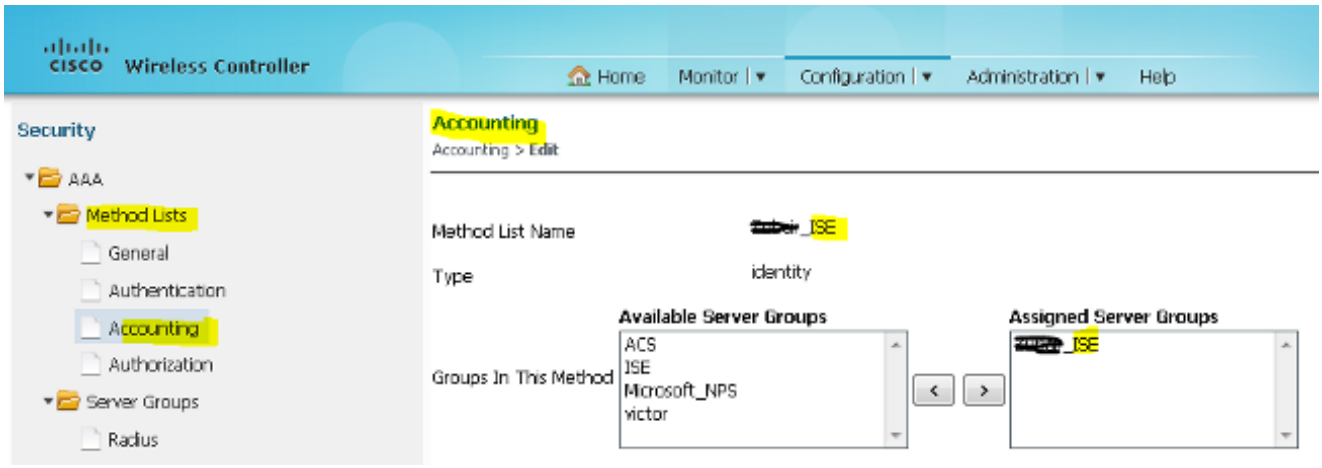
7. From the Wireless Controller GUI, choose **AAA > Method Lists > General**. Check the **Dot1x System Auth Control** check box. If you disable this option, AAA does not work.



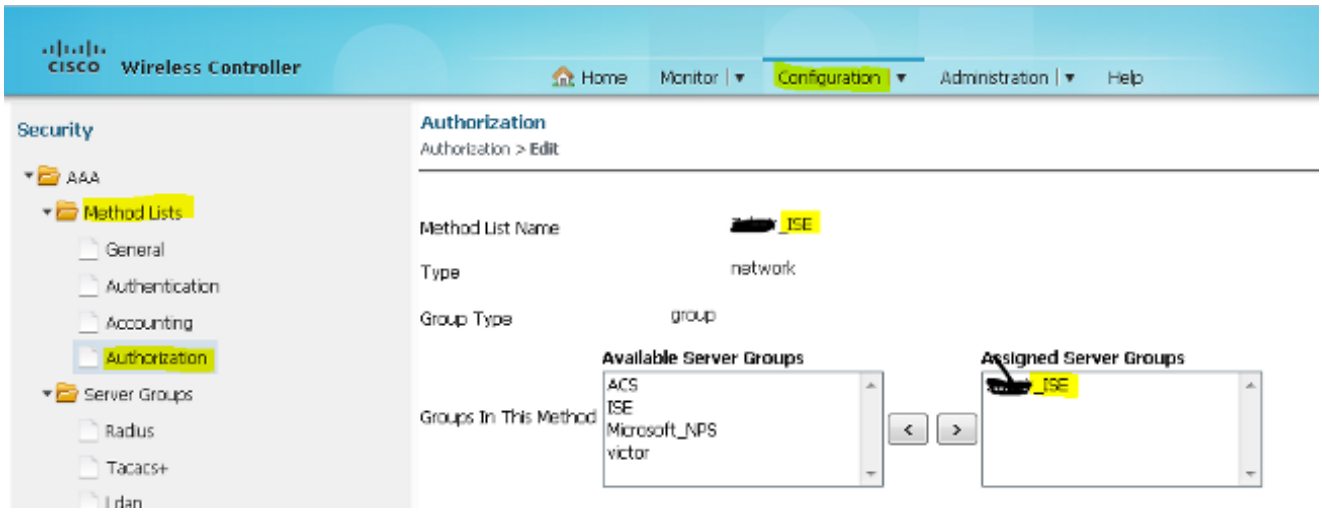
8. From the Wireless Controller GUI, choose **AAA > Method Lists > Authentication**. Create an Authentication method list for Type dot1X. The Group Type is group. Map it to the ISE.



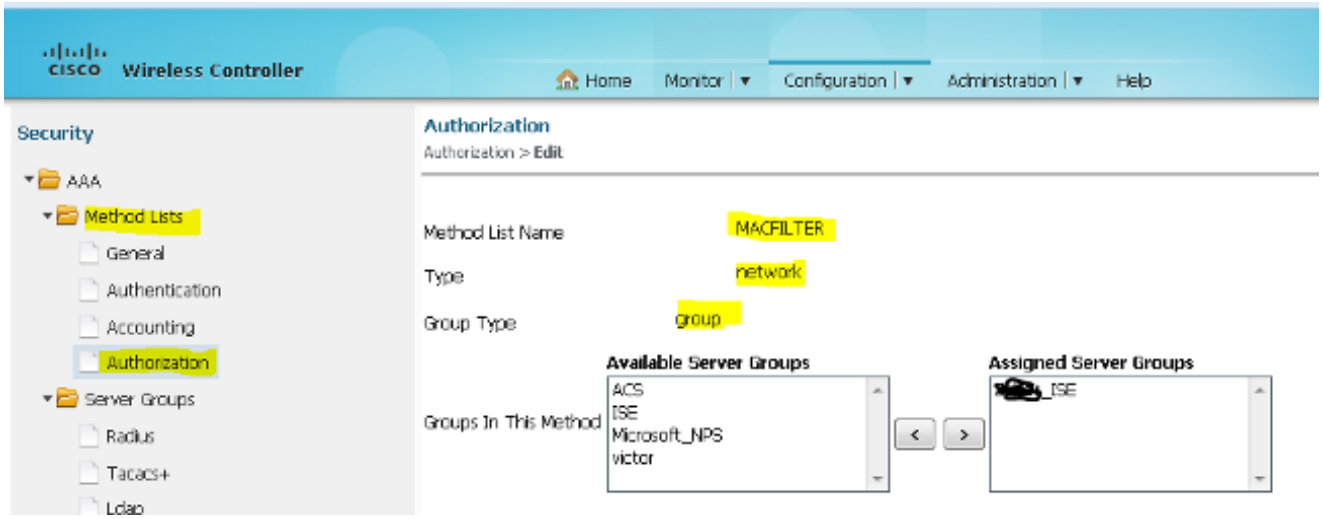
9. From the Wireless Controller GUI, choose **AAA > Method Lists > Accounting**. Create an Accounting method list for Type identity. Map it to the ISE.



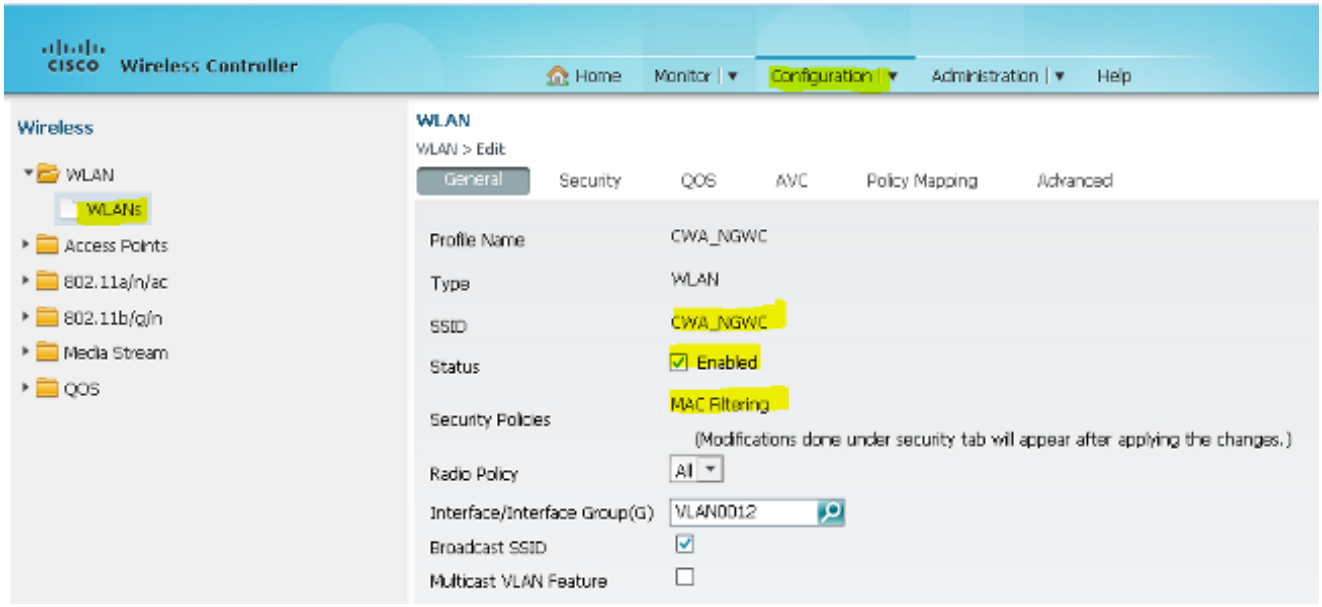
10. From the Wireless Controller GUI, choose **AAA > Method Lists > Authorization**. Create a Authorization method list for Type network. Map it to the ISE.



11. Optional, since there is MAC on failure support as well. Create an Authorization method list MACFILTER for Type network. Map it to the ISE.



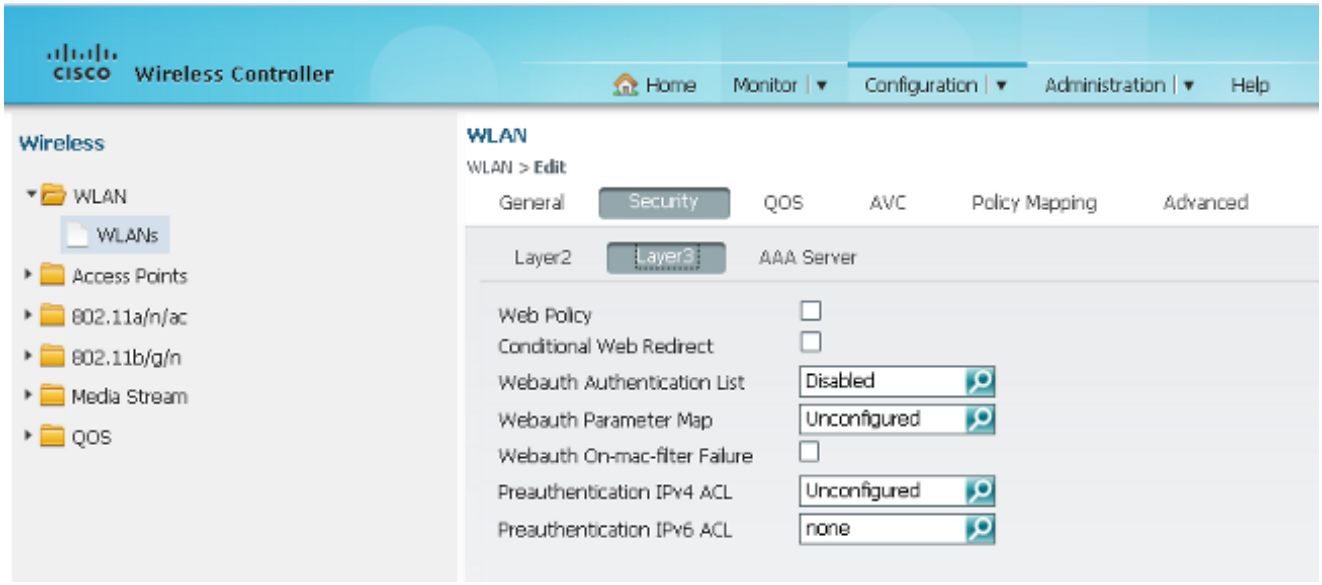
12. From the Wireless Controller GUI, choose **WLAN > WLANs**. Create a new configuration with the parameters shown here.



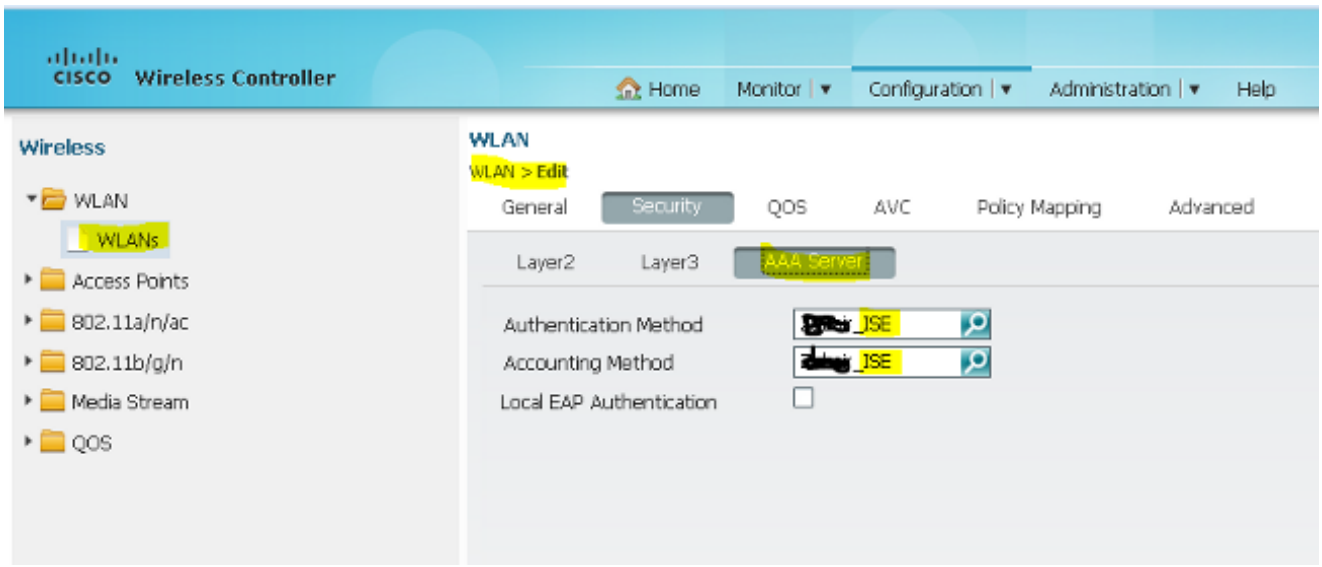
13. Choose **Security > Layer2**. In the MAC Filtering field, enter **MACFILTER**.



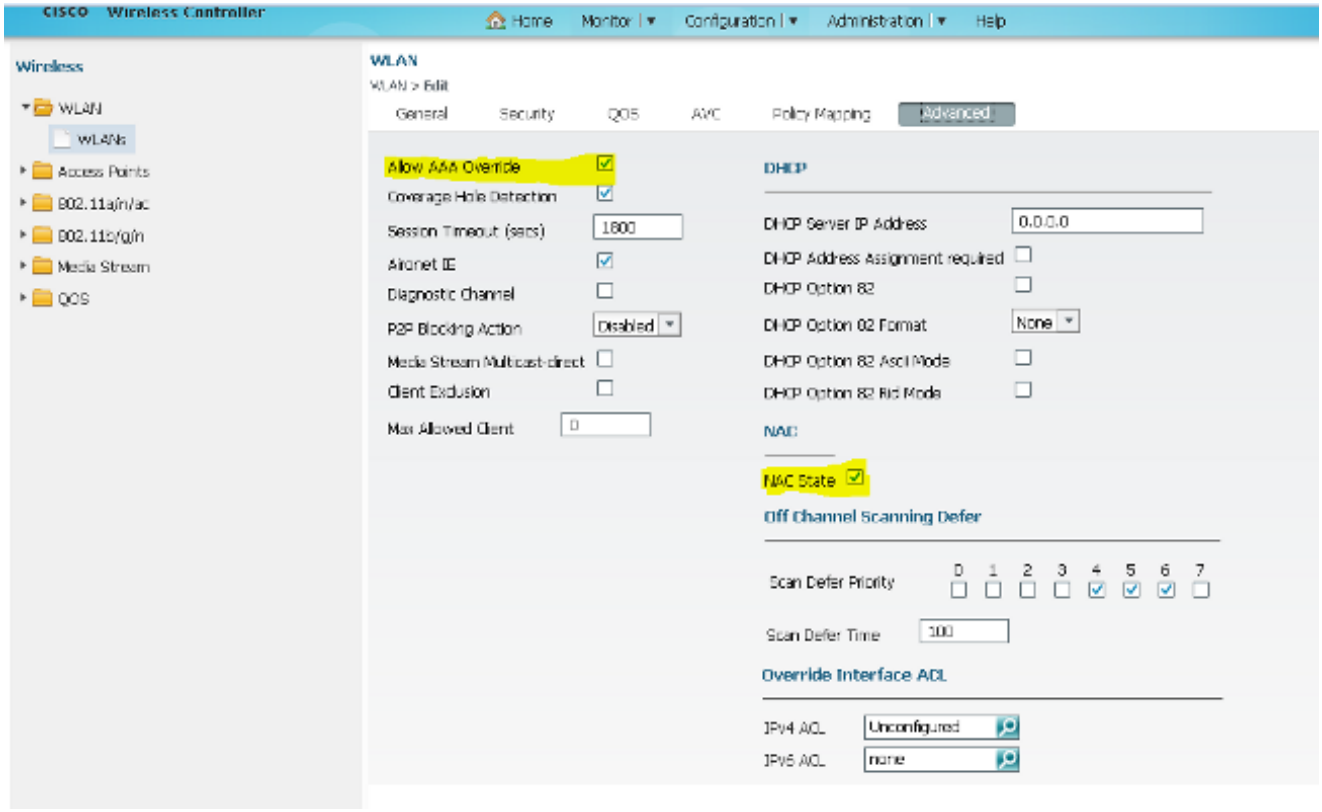
14. It is not necessary to configure Layer3.



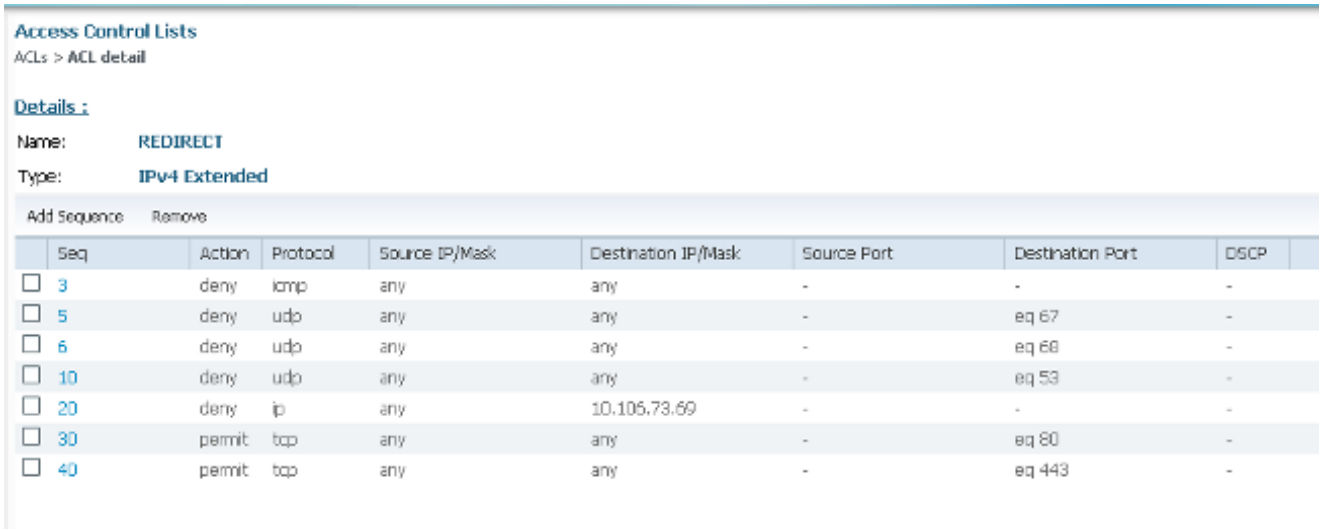
15. Choose **Security > AAA Server**. From the Authentication Method drop-down list, choose **ISE**. From the Accounting Method drop-down list, choose **ISE**.



16. Choose **Advanced**. Check the **Allow AAA Override** check box. Check the **NAC State** check box.



17. Configure Redirect ACLs on the WLC in the GUI.



Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
3	deny	icmp	any	any	-	-	-
5	deny	udp	any	any	-	eq 67	-
6	deny	udp	any	any	-	eq 68	-
10	deny	udp	any	any	-	eq 53	-
20	deny	ip	any	10.106.73.69	-	-	-
30	permit	tcp	any	any	-	eq 80	-
40	permit	tcp	any	any	-	eq 443	-

Topology 2 Configuration Example

See Topology 2 for the network diagram and explanation.

This configuration is also a two step process.

Configuration on the ISE

Configuration on the ISE is the same as for the Topology 1 configuration.

There is no need to add the Anchor Controller on the ISE. You just need to add the Foreign WLC on the ISE, define the RADIUS server on the Foreign WLC, and map the Authorization policy under the WLAN. On the Anchor you just need to enable MAC filtering.

In this configuration example, there are two WLC 5760s that act as an Anchor Foreign. In case you want to use the WLC 5760 as an Anchor and the 3850 Switch as the Anchor Foreign, which is the Mobility Agent, to another Mobility Controller then the same configuration is correct. However, there is no need to configure the WLAN on the second Mobility Controller to which the 3850 Switch gets the licenses from. You just need to point the 3850 Switch to the WLC 5760 which acts as the Anchor.

Configuration on the WLC

1. On the Foreign, configure the ISE server with the AAA Method list for AAA and map the WLAN to a MAC filter authorization.



Note: Configure the redirect ACL on both the Anchor and Foreign and also MAC filtering.

<#root>

```
dot1x system-auth-control



radius server ISE

 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646

 timeout 10

 retransmit 3

 key Cisco123



aaa group server radius ISE

 server name ISE

 deadtime 10



aaa authentication dot1x ISE group ISE



aaa authorization network ISE group ISE
```

```
aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author

 client 10.106.73.69 server-key Cisco123

 auth-type any

wlan MA-MC 11 MA-MC

 aaa-override

 accounting-list  ISE

 client vlan VLAN0012

 mac-filtering MACFILTER

 mobility anchor 10.105.135.244

nac

 no security wpa

 no security wpa akm dot1x

 no security wpa wpa2
```

```
 no security wpa wpa2 ciphers aes


security dot1x authentication-list ISE


 session-timeout 1800


 no shutdown
```

2. Configure Redirect ACLs with the CLI.

   This is the url-redirect-acl that ISE returns as an AAA override along with the redirect URL for the guest portal redirection. It is a direct ACL which is used currently on the Unified architecture. This is a 'punt' ACL which is sort of a reverse ACL that you would normally use for Unified architecture. You need to block access to DHCP, the DHCP server, DNS, the DNS server, and the ISE server. Only allow www, 443, and 8443 as needed. This ISE guest portal uses port 8443 and the redirection still works with the ACL shown here. Here ICMP is enabled, but based on the security rules you can either deny or permit.

   <#root>

```
ip access-list extended REDIRECT


 deny icmp any any


deny udp any any eq bootps


 deny udp any any eq bootpc


 deny udp any any eq domain


deny ip any host 10.106.73.69


 permit tcp any any eq www


 permit tcp any any eq 443
```

> ⚠ **Caution**: When you enable HTTPS, it might cause some high CPU issues due to scalability. Do not enable this unless it is recommemded by the Cisco design team.

3. Configure Mobility on the Anchor.
<#root>

```
wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
```

> ✎ **Note**: If you configure the same with the 3850 Switch as the Foreign, then ensure you define the Switch peer group on the Mobility Controller and vice-versa on the Mobility Controller. Then configure the above CWA configurations on the 3850 Switch.

4. Configuration on the Anchor.

On the Anchor, there is no need to configure any ISE configurations. You just need the WLAN configuration.

<#root>

```
wlan MA-MC 6 MA-MC

 aaa-override

 client vlan VLAN0012

 mac-filtering MACFILTER

 mobility anchor


nac

 nbsp;no security wpa

 no security wpa akm dot1x

 no security wpa wpa2

 no security wpa wpa2 ciphers aes

 session-timeout 1800
```

```
no shutdown
```

5. Configure Mobility on the Anchor.

   Define the other WLC as the Mobility member on this WLC.

   <#root>

   ```
   wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
   ```

6. Configure Redirect ACLs with the CLI.

   This is the url-redirect-acl that ISE returns as an AAA override along with the redirect URL for the guest portal redirection. It is a direct ACL which is used currently on the Unified architecture. This is a 'punt' ACL which is sort of a reverse ACL that you would normally use for Unified architecture. You need to block access to DHCP, the DHCP server, DNS, the DNS server, and the ISE server. Only allow www, 443, and 8443 as needed. This ISE guest portal uses port 8443 and the redirection still works with the ACL shown here. Here ICMP is enabled, but based on the security rules you can either deny or permit.

   <#root>

   ```
   ip access-list extended REDIRECT


    deny icmp any any


    deny udp any any eq bootps


    deny udp any any eq bootpc


    deny udp any any eq domain


    deny ip any host 10.106.73.69


    permit tcp any any eq www


    permit tcp any any eq 443
   ```

⚠ **Caution**: When you enable HTTPS, it might cause some high CPU issues due to scalability. Do not enable this unless it is recommemded by the Cisco design team.

Topology 3 Configuration Example

See Topology 3 for the network diagram and explanation.

This is also a two step process.

Configuration on the ISE

Configuration on the ISE is the same as for the Topology 1 Configuration.

There is no need to add the Anchor Controller on the ISE. You just need to add the Foreign WLC on the ISE, define the RADIUS server on the Foreign WLC, and map the Authorization policy under the WLAN. On the Anchor you just need to enable MAC filtering.

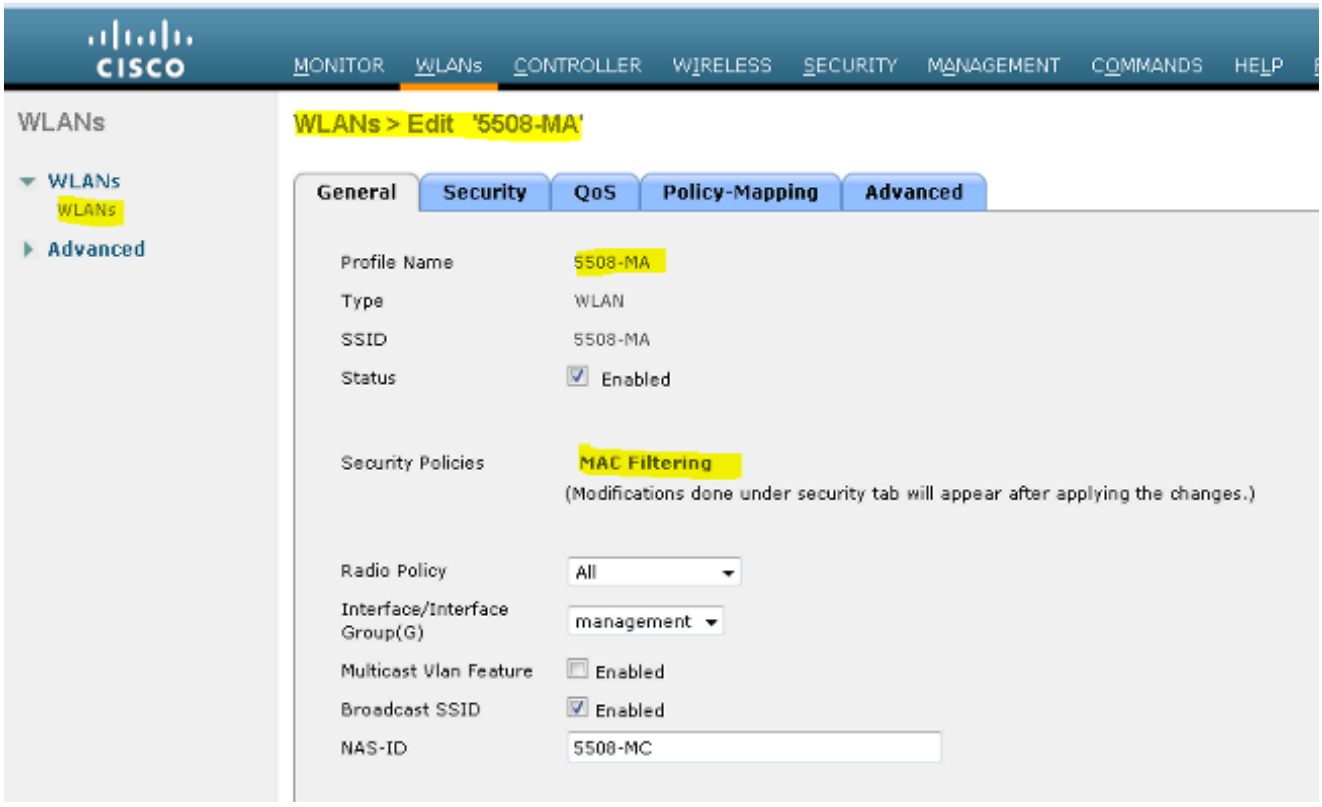
In this example, there is a WLC 5508 that acts as an Anchor and a WLC 5760 that acts as a Foreign WLC. If you want to use a WLC 5508 as an Anchor and a 3850 Switch and Foreign WLC, which is a Mobility Agent, to another Mobility Controller then the same configuration is correct. However, there is no need to configure the WLAN on the second Mobility Controller to which the 3850 Switch gets the licenses from. You just need to point the 3850 Switch to the 5508 WLC which acts as the Anchor.

Configuration on the WLC

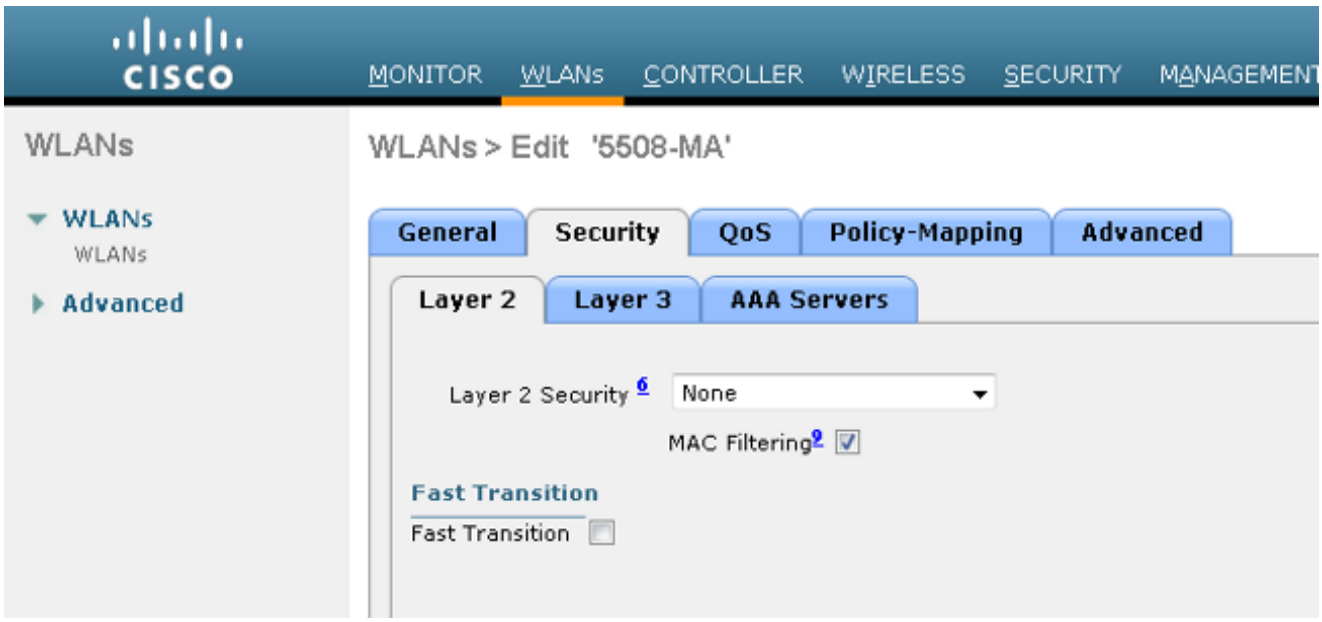
1. On the Foreign WLC, configure the ISE server with the AAA Method list for AAA and map the WLAN to a MAC filter authorization. This is not needed on the Anchor.

   Note: Configure Redirect ACL on both the Anchor and Foreign WLC and also MAC filtering.

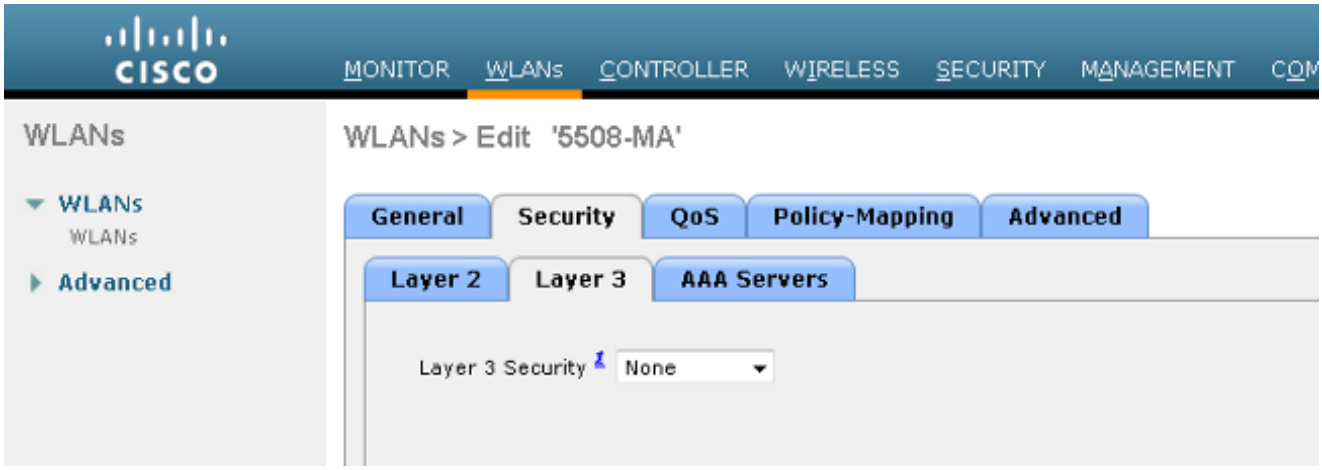
2. From the WLC 5508 GUI, choose **WLANs > New** in order to configure the Anchor 5508. Fill in the details in order to enable MAC filtering.



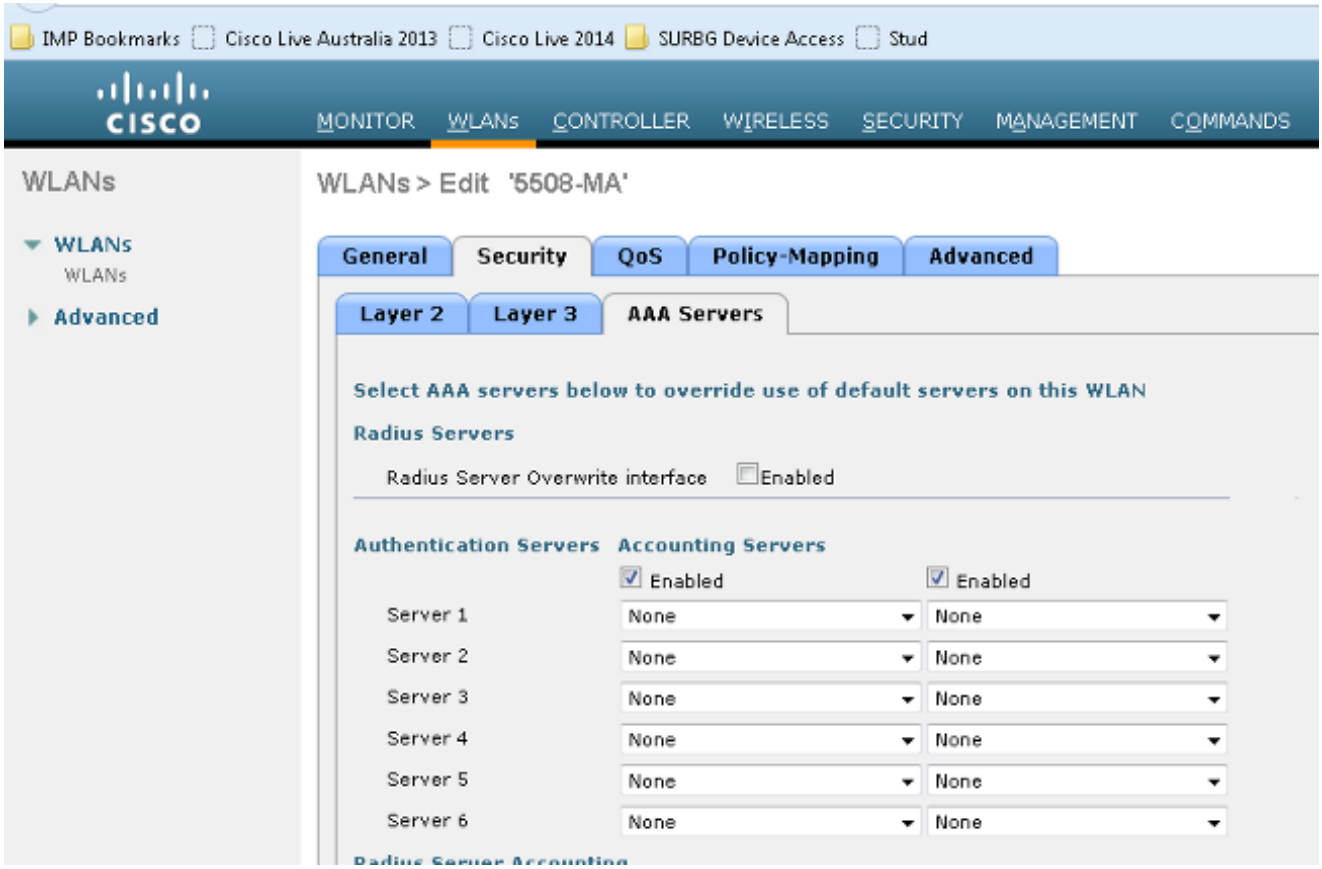
3. It is not necessary to configure Layer 2 options.



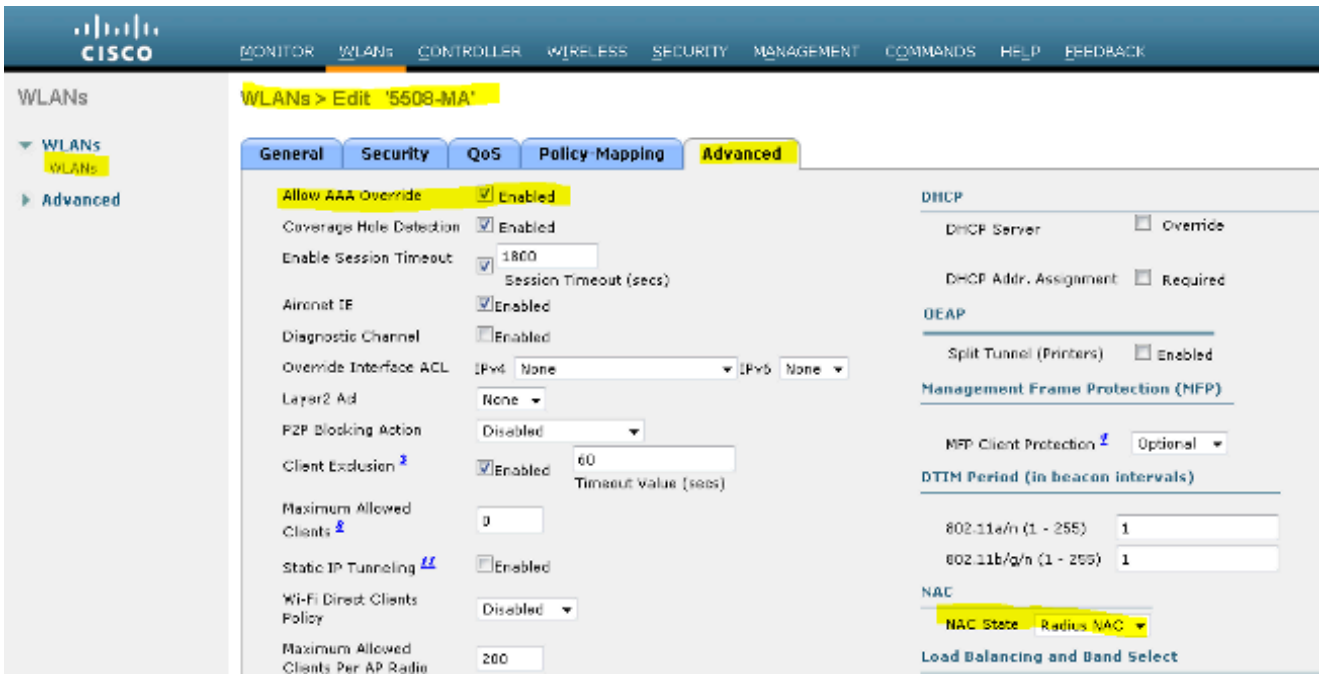
4. It is not necessary to configure Layer 3 options.



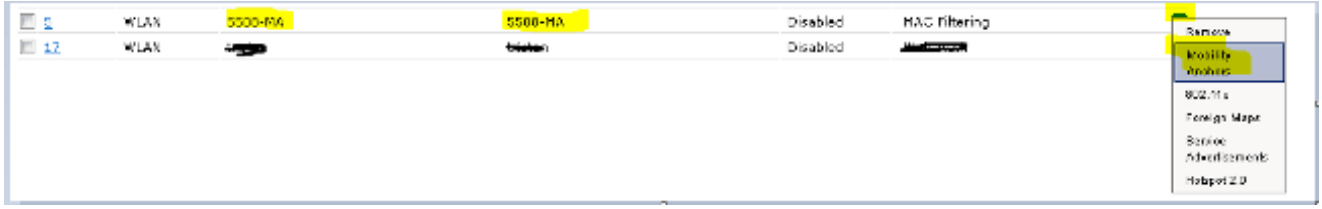
5. AAA servers should be disabled in the Anchor AireOS WLC in order for the CoA to be processed by the foreign NGWC. AAA servers can only be enabled in the Anchor WLC if there is no RADIUS servers configured under: Security > AAA > RADIUS > Authentication



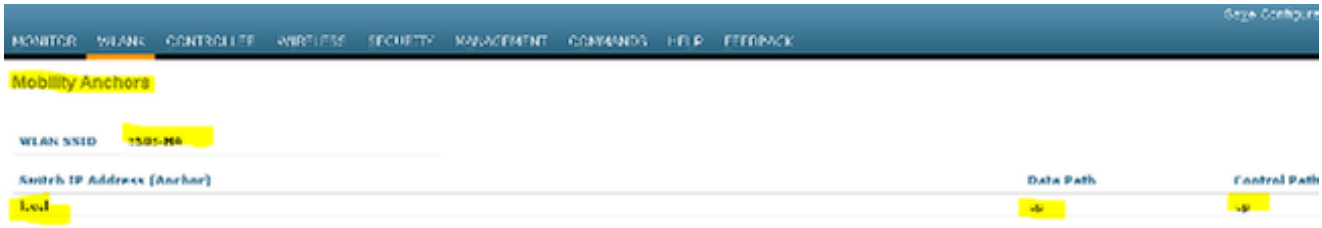
6. Choose **WLANs > WLANs > Edit > Advanced**. Check the **Allow AAA Override** check box. From the NAC State drop-down list, choose **Radius NAC**.



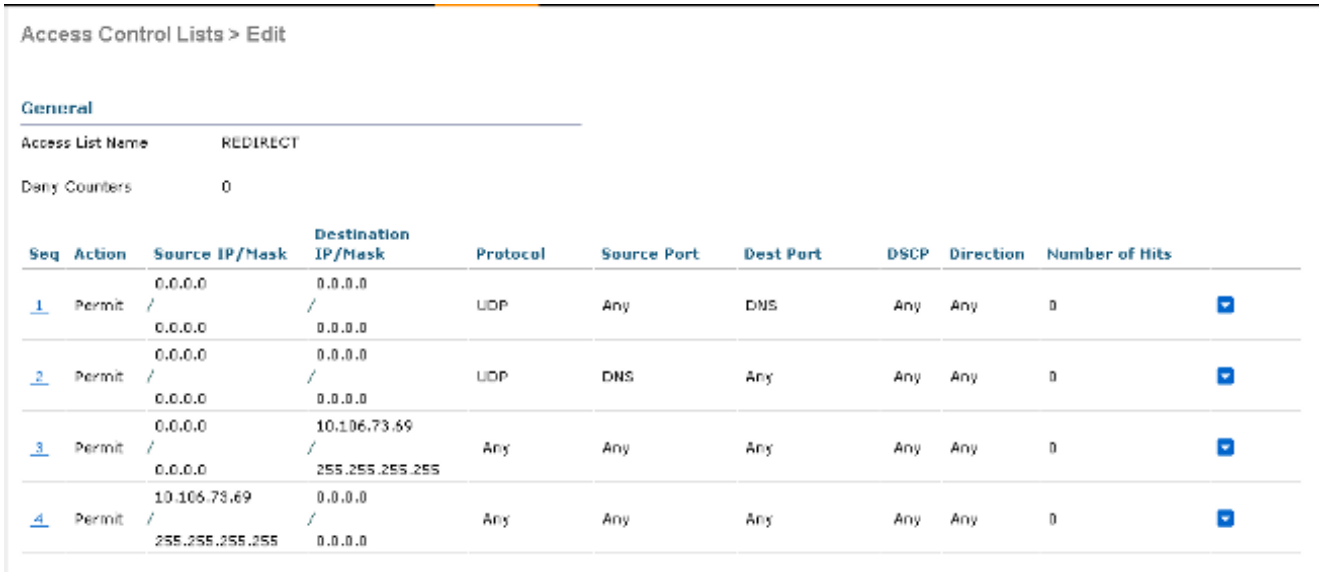
7. Add this as the Anchor for the WLAN.



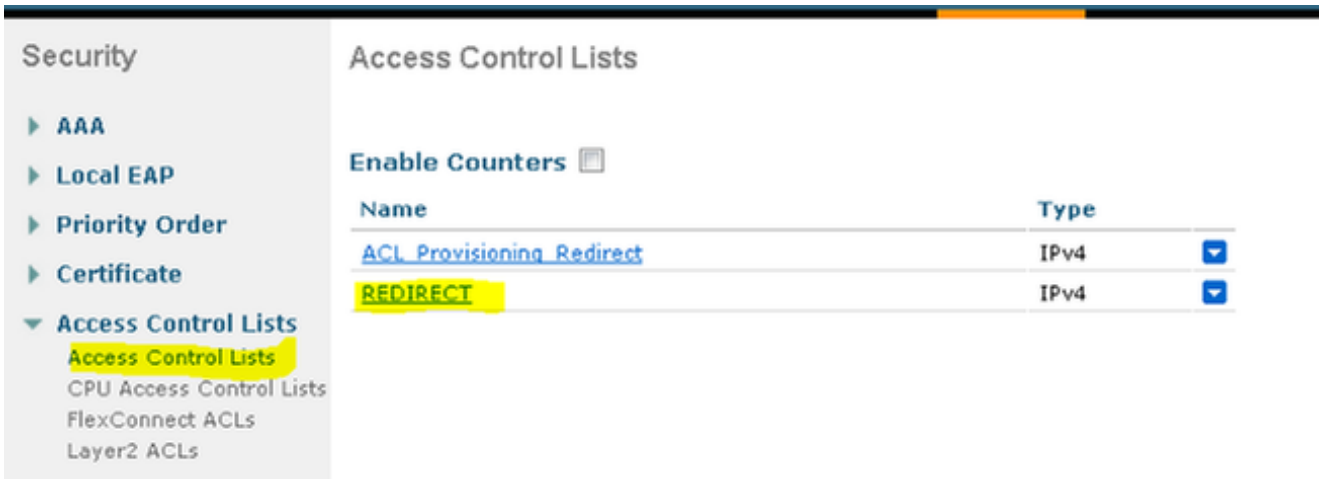
8. After it is pointed to local, it should look this with Control and Data Path UP/UP.



9. Create the Redirect ACL on the WLC. This denies DHCP and DNS. It allows HTTP/HTTPs.



This is how it looks after the ACL is created.



10. Define the ISE RADIUS server on the WLC 5760.
11. Configure the RADIUS Server, Server group, and Method List with the CLI.
<#root>

```
dot1x system-auth-control
```

```
radius server ISE
```

```
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646

 timeout 10

 retransmit 3

 key Cisco123


aaa group server radius ISE

 server name ISE

 deadtime 10


aaa authentication dot1x ISE group ISE


aaa authorization network ISE group ISE


aaa authorization network MACFILTER group ISE


aaa accounting identity ISE start-stop group ISE


!


aaa server radius dynamic-author

 client 10.106.73.69 server-key Cisco123

 auth-type any
```

12. Configure the WLAN from the CLI.
<#root>

```
wlan 5508-MA 15 5508-MA

 aaa-override

 accounting-list ISE

 client vlan VLAN0012

 mac-filtering MACFILTER

 mobility anchor 10.105.135.151

 nac

 no security wpa

 no security wpa akm dot1x

 no security wpa wpa2

 no security wpa wpa2 ciphers aes

 security dot1x authentication-list ISE

 session-timeout 1800

 shutdown
```

13. Define the other WLC as the Mobility member on this WLC.
<#root>

```
wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1
```

> **Note**: If you configure the same with the WLC 3850 as the Foreign, then ensure you define the Switch peer group on the Mobility Controller and vice-versa on the Mobility Controller. Then configure the previous CWA configurations on the WLC 3850.

14. Configure Redirect ACLs with the CLI.

This is the url-redirect-acl that ISE returns as an AAA override along with the redirect URL for the guest portal redirection. It is a direct ACL which is used currently on the Unified architecture. This is a 'punt' ACL which is sort of a reverse ACL that you would normally use for Unified architecture. You need to block access to DHCP, the DHCP server, DNS, the DNS server, and the ISE server. Only allow www, 443, and 8443 as needed. This ISE guest portal uses port 8443 and the redirection still works with the ACL shown here. Here ICMP is enabled, but based on the security rules you can either deny or permit.

<#root>

```
ip access-list extended REDIRECT


 deny icmp any any


 deny udp any any eq bootps


 deny udp any any eq bootpc


 deny udp any any eq domain


 deny ip any host 10.106.73.69


 permit tcp any any eq www


 permit tcp any any eq 443
```

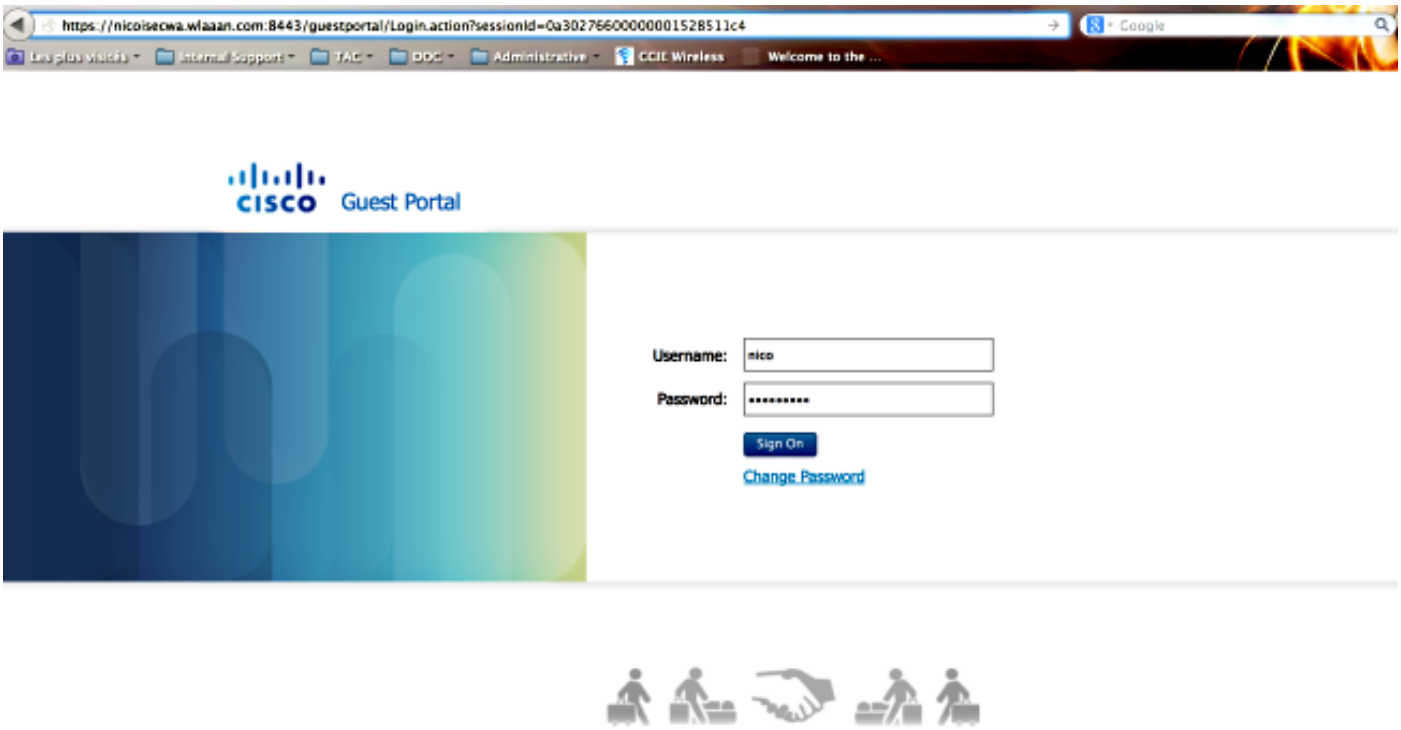
⚠ **Caution**: When you enable HTTPS, it might cause some high CPU issues due to scalability. Do not enable this unless it is recommemded by the Cisco design team.

Verify

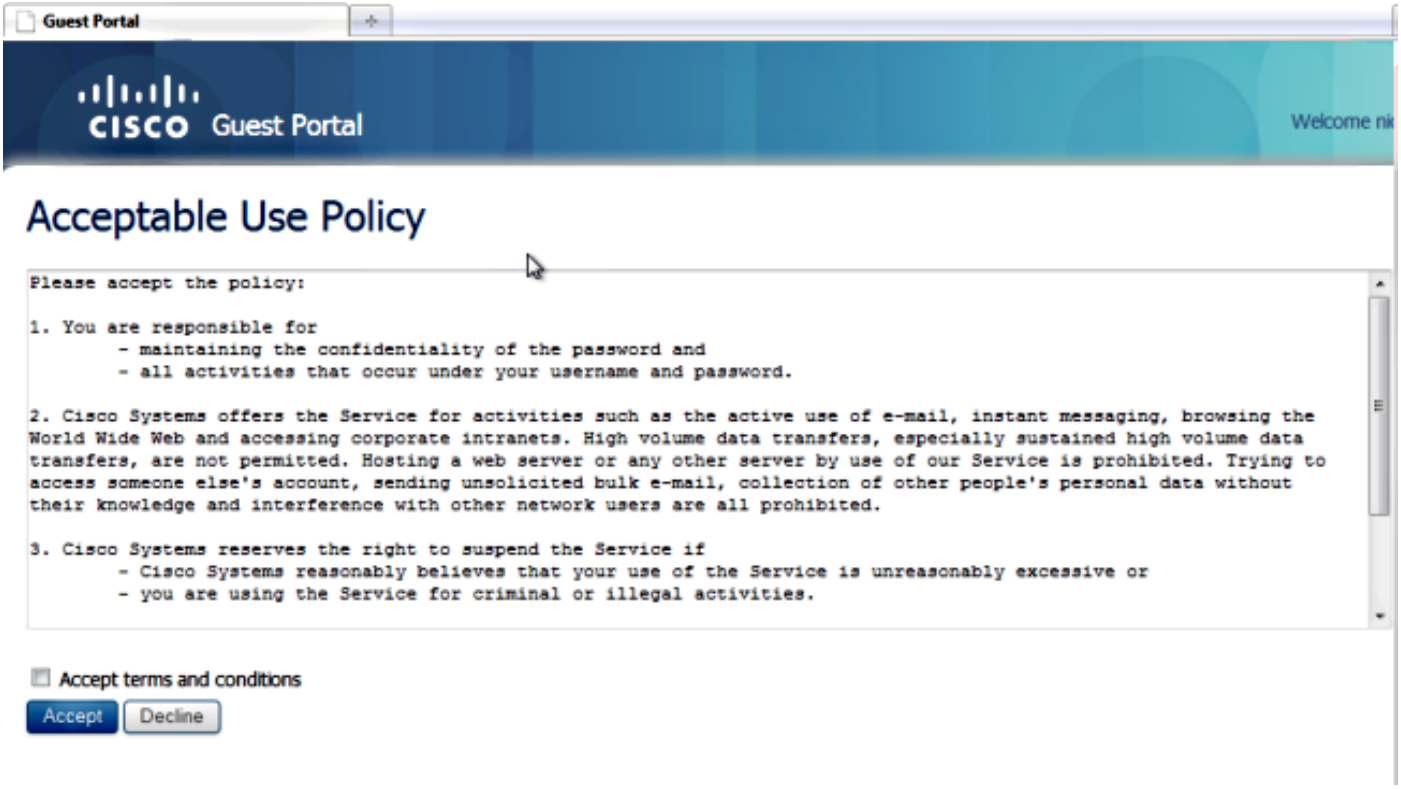
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Connect the client to the configured SSID. Once you receive the IP address and when the client goes to the Web auth Required state, open the browser. Enter your client credentials in the portal.



After successful authentication, check the **Accept terms and conditions** check box. Click **Accept**.

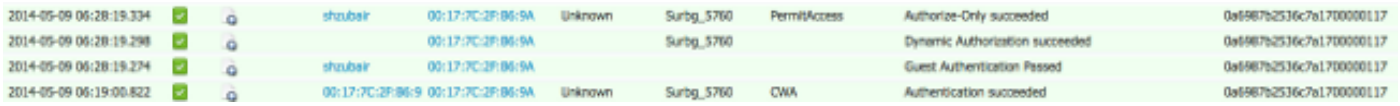


You will receive a confirmation message and will now be able to browse to the Internet.



You can now type in the original URL in the browser's address bar.

On the ISE, the client flow looks like this:



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

On the Converged Access WLC, it is recommended to run traces instead of debugs. On the Aironet OS 5508 WLC you just need to enter **debug client <client mac>** and **debug web-auth redirect enable mac <client mac>**.

```
set trace group-wireless-client level debug
set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a
set trace group-wireless-secure filter mac 0017.7c2f.b69a
```

Some known defects on the Cisco IOS-XE and the Aironet OS are included in Cisco bug ID CSCun38344.

This is how the successful CWA flow looks like on the traces:

<#root>

```
[05/09/14 13:13:15.951 IST 63d7 8151]
```

0017.7c2f.b69a Association received from mobile

on AP c8f9.f983.4260

[05/09/14 13:13:15.951 IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown and downstream policy is unknown

[05/09/14 13:13:15.951 IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6 override for station 0017.7c2f.b69a - vapId 15, site 'default-group', interface 'VLAN0012'

[05/09/14 13:13:15.951 IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012'
[05/09/14 13:13:15.951 IST 63e2 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:15.951 IST 63e3 8151] 0017.7c2f.b69a ***

Client State = START

instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1
deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

[05/09/14 13:13:15.951 IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER

[05/09/14 13:13:15.951 IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent

05/09/14 13:13:15.951 IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq (apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Idle to AAA Pending

[05/09/14 13:13:15.951 IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:15.951 IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 20) in 10 seconds
[05/09/14 13:13:15.951 IST 63f0 211]

Parsed CLID MAC Address = 0:23:124:47:182:154

[05/09/14 13:13:15.951 IST 63f1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:15.951 IST 63f2 211]

AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE

[05/09/14 13:13:16.015 IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization
[05/09/14 13:13:16.015 IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS
[05/09/14 13:13:16.015 IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266
[05/09/14 13:13:16.015 IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266
[05/09/14 13:13:16.015 IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet.
[05/09/14 13:13:16.015 IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:16.015 IST 63f9 8151] 0017.7c2f.b69a
client incoming attribute size are 193

[05/09/14 13:13:16.015 IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280

[05/09/14 13:13:16.015 IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect 'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa' set

[05/09/14 13:13:16.015 IST 63fc 8151]

0017.7c2f.b69a Redirect URL received for client from RADIUS. for redirection.

[05/09/14 13:13:16.015 IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State START

[05/09/14 13:13:16.015 IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:16.015 IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:16.015 IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:16.015 IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:16.015 IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:16.015 IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:16.015 IST 6406 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:16.015 IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:16.015 IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:16.015 IST 640a 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC)
[05/09/14 13:13:16.015 IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:16.015 IST 640c 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform ID allocated successfully ID:259
[05/09/14 13:13:16.015 IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid 5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0) wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0 m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145

```
 glob rsc id 259dhcpsrv  0.0.0
[05/09/14 13:13:16.015 IST 641d 8151] 0017.7c2f.b69a Change state to
 AUTHCHECK (2) last state START (0)


[05/09/14 13:13:16.015 IST 641e 8151] 0017.7c2f.b69a Change state to
 L2AUTHCOMPLETE (4) last state AUTHCHECK (2)



[05/09/14 13:13:16.015 IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0,
 Curr Mob 0 llmReq 1, return False
[05/09/14 13:13:16.015 IST 6421 207] [WCDB] ==Add event: type Regular Wireless client
 (0017.7c2f.b69a) client id (0x47ad4000000145) client index (259) vlan (12)
 auth_state (ASSOCIATION) mob_state (INIT)
[05/09/14 13:13:16.015 IST 6422 207] [WCDB] ===intf src/dst (0x506c800000000f)/(0x0)
 radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0)
[05/09/14 13:13:16.015 IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1)
 vlan 12 radio 0 client_id 0x47ad4000000145 mobility=Unassoc(0) src_int
 0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip  0.0.0.0
 ip_learn_type 0
[05/09/14 13:13:16.015 IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth
 but l2ack waiting lfag not set,so set
[05/09/14 13:13:16.015 IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code
 qosCap 00
[05/09/14 13:13:16.016 IST 6426 8151] 0017.7c2f.b69a

Change state to DHCP_REQD (7)
 last state L2AUTHCOMPLETE (4)



[05/09/14 13:13:16.016 IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to
 station on BSSID  c8f9.f983.4260  (status 0) ApVapId 15 Slot 0
[05/09/14 13:13:16.016 IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp
 (apf_80211.c:2316) Changing state for mobile  0017.7c2f.b69a  on AP
 c8f9.f983.4260  from Associated to Associated

[05/09/14 13:13:16.016 IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for
 Non-dot1x wireless client
[05/09/14 13:13:16.016 IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
 to Push wireless session for client  47ad4000000145 uid 280
[05/09/14 13:13:16.016 IST 6438 8151] 0017.7c2f.b69a Session Push for
 wireless client

[05/09/14 13:13:16.016 IST 6439 8151] 0017.7c2f.b69a Session Manager Call
 Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session
 ID 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:16.016 IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca2] Session start request from Client[1] for
 0017.7c2f.b69a (method: No method, method list: none, aaa id:
 0x00000118) - session-push,  policy
[05/09/14 13:13:16.016 IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca2]  - client iif_id: 47AD4000000145, session ID:
 0a6987b2536c871300000118 for 0017.7c2f.b69a
[05/09/14 13:13:16.016 IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR:
 [0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method
```

```
[05/09/14 13:13:16.017 IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of
 dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF:
 [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for
 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a)
 client (0x47ad4000000145): FFCP operation (CREATE) return code (0)
[05/09/14 13:13:16.017 IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event:
 Notifying other features about client add
[05/09/14 13:13:16.017 IST 6446 22] [WCDB] wcdb_sisf_client_add_notify:
 Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6447 22] [WCDB] wcdb_sisf_client_add_notify:
 Notifying SISF of new Association for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler
 client code 0 mob state 0
[05/09/14 13:13:16.017 IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK
 from WCDB
[05/09/14 13:13:16.017 IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag
 updated
[05/09/14 13:13:16.017 IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.017 IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI
 (Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id
 0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1
[05/09/14 13:13:18.796 IST 644d 8151] 0017.7c2f.b69a Local Policy:
 apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:18.802 IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy
 for station  0017.7c2f.b69a  - valid mask 0x0

[05/09/14 13:13:18.802 IST 644f 8151] 0017.7c2f.b69a     QOS Level: -1, DSCP: -1,
 dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
 --More--

[05/09/14 13:13:18.802 IST 6450 8151] 0017.7c2f.b69a     Session: -1,
 User session: -1, User elapsed -1
    Interface: N/A ACL: N/A Qos Pol Down   Qos Pol Up

[05/09/14 13:13:18.802 IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of
 apfApplyOverride2. Client State DHCP_REQD

[05/09/14 13:13:18.802 IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for
 station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA
 override for station
[05/09/14 13:13:18.802 IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16,
 valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
 sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
 dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying
```

```
 override policy
[05/09/14 13:13:18.802 IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for
 station  ---
[05/09/14 13:13:18.802 IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying
 WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface
 name e VLAN0012

[05/09/14 13:13:18.802 IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0012 and VLAN ID  12

[05/09/14 13:13:18.802 IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[05/09/14 13:13:18.802 IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[05/09/14 13:13:18.802 IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy:
 Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:18.802 IST 645e 8151] 0017.7c2f.b69a Local Policy: After
 Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
 apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying
 Site Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and
 apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct
 for mobile MAC:  0017.7c2f.b69a , source 16

[05/09/14 13:13:18.802 IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override
 into chain for station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16,
 valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
 sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
 dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr
 check continuation
[05/09/14 13:13:18.802 IST 6465 8151] 0017.7c2f.b69a Local Policy:
 apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from
 apfMsSumOverride
[05/09/14 13:13:18.802 IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling
 applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:18.802 IST 6467 8151] 0017.7c2f.b69a
  **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:18.802 IST 6468 8151] 0017.7c2f.b69a *** Client State =
 DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH,
 OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0,
 userRole=(null)

[05/09/14 13:13:18.802 IST 6469 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
  sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:18.802 IST 646a 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:18.802 IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End
 AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc
[05/09/14 13:13:18.802 IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client
```

```
[05/09/14 13:13:18.802 IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x
 wireless client
[05/09/14 13:13:18.802 IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push
 wireless session for client  47ad4000000145 uid 280
 --More--
[05/09/14 13:13:18.802 IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions

[05/09/14 13:13:18.802 IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client
 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 0 Audit-Session ID
 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:18.802 IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last
 state DHCP_REQD (7)

[05/09/14 13:13:18.802 IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr
 Mob State 3 llReq flag 1
[05/09/14 13:13:18.802 IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0
 currMob State 3 afd action 1
[05/09/14 13:13:18.802 IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id
 12 auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f
 dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id
 0 wgbid 0000.0000.0000
[05/09/14 13:13:18.802 IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan
 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
 dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip  0.0.0.0
 ip_learn_type 0
[05/09/14 13:13:18.802 IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a,
 ID list 0x00000000, policy
[05/09/14 13:13:18.802 IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3
 curr Mob State 3 llReq flag 0
[05/09/14 13:13:18.802 IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4)
 vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int
 0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0
 ip  0.0.0.0 ip_learn_type 0
[05/09/14 13:13:18.802 IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start
 record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:18.802 IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting
 start request, uid=280 passthrough=1
[05/09/14 13:13:18.802 IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:18.803 IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
 client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state
 (L2_AUTH_DONE->RUN) mob_st<truncated>
[05/09/14 13:13:18.803 IST 6480 207] [WCDB] ===intf src/dst
 (0x506c800000000f->0x506c800000000f)/(0x0->0x75e18000000143)
 radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
 (<truncated>
[05/09/14 13:13:18.803 IST 6481 207] [WCDB] Foreign client add. Final llm
 notified = false
[05/09/14 13:13:18.803 IST 6482 207] [WCDB] wcdb_client_mcast_update_notify:
 No mcast action reqd
[05/09/14 13:13:18.803 IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
 client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6484 207] [WCDB] wcdb_client_state_change_notify:
 update flags = 0x3
[05/09/14 13:13:18.803 IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79
[05/09/14 13:13:18.803 IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a]
 WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6487 8151] 0017.7c2f.b69a Sending SPI
```

```
 spi_epm_epm_session_create successfull
[05/09/14 13:13:18.803 IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20
 mmRole ExpForeign !!!
[05/09/14 13:13:18.803 IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole
 ExpForeign, updating wcdb not needed
[05/09/14 13:13:18.803 IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:18.803 IST 648b 207] [WCDB] wcdb_sisf_client_update_notify:
 Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
 client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
 mob_st<truncated>
[05/09/14 13:13:18.803 IST 648d 207] [WCDB] ===intf src/dst
 (0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143)
 radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false)
 addr v4/v6 (<truncated>
[05/09/14 13:13:18.803 IST 648e 207] [WCDB] wcdb_client_mcast_update_notify:
 No mcast action reqd
[05/09/14 13:13:18.803 IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
 client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6490 207] [WCDB] wcdb_client_state_change_notify:
 update flags = 0x2
[05/09/14 13:13:18.803 IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
 [0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6492 207] [WCDB] wcdb_sisf_client_update_notify:
 Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
 client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
 client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
 Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
 Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6497 8151] 0017.7c2f.b69a Received session_create_response
 for client handle 20175213735969093
[05/09/14 13:13:18.803 IST 6498 8151] 0017.7c2f.b69a Received session_create_response
 with EPM session handle 4261413136
[05/09/14 13:13:18.803 IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client
 or posture client
 --More--
[05/09/14 13:13:18.803 IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the
 attribute list
[05/09/14 13:13:18.803 IST 649b 8151] 0017.7c2f.b69a Setting AAA Override
 Url-Redirect-Acl 'REDIRECT'

[05/09/14 13:13:18.803 IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl
'REDIRECT'



[05/09/14 13:13:18.803 IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
 set


[05/09/14 13:13:18.803 IST 649e 8151] 0017.7c2f.b69a  Wireless Client mobility role
is not ExportAnchor/Local. Hence we are not sending request to EPM
[05/09/14 13:13:20.445 IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0
 ip_learn_type 0 deleted ipv4 0.0.0.0
[05/09/14 13:13:20.446 IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update:
 Foreign client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.446 IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0] :
 fe80::6c1a:b253:d711:c7f
```

[05/09/14 13:13:20.446 IST 64a2 207] [WCDB] SISF Update : Binding delete status
for V6: = 0
[05/09/14 13:13:20.446 IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:20.448 IST 64a4 8151] 0017.7c2f.b69a MS got the IP,
resetting the Reassociation Count 0 for client
[05/09/14 13:13:20.448 IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280 passthrough=1
[05/09/14 13:13:20.449 IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address
(10.105.135.190)
[05/09/14 13:13:20.449 IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190
to mobile
[05/09/14 13:13:20.449 IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4
10.105.135.190 ip_learn_type DHCP deleted ipv4 0.0.0.0
[05/09/14 13:13:20.449 IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting
interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280

passthrough=1

[05/09/14 13:13:20.449 IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent

**[05/09/14 13:13:20.449 IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign !!!**

**[05/09/14 13:13:20.449 IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign
client (0017.7c2f.b69a) ip addr update received.**

**[05/09/14 13:13:20.449 IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign, updating wcdb not needed**

[05/09/14 13:13:20.449 IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:20.449 IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0] :
fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.449 IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0
[05/09/14 13:13:20.449 IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF
to remove assoc in Foreign
[05/09/14 13:13:20.449 IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay
add/update sync of addr for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:49.429 IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1]
[05/09/14 13:13:49.430 IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update request sent to Client[1]
[05/09/14 13:13:49.430 IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from
dot1x. COA type 5
[05/09/14 13:13:49.430 IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280,
context=268
[05/09/14 13:13:49.430 IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request,
uinque id=280, context id = 268, context reqHandle 0xfefc172c
[05/09/14 13:13:49.430 IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request
for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:49.430 IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent

```
[05/09/14 13:13:49.430 IST 64bd 8151] 0017.7c2f.b69a processing COA type 5
  was successful
[05/09/14 13:13:49.430 IST 64be 8151] 0017.7c2f.b69a processing COA type 5
  was successful
[05/09/14 13:13:49.430 IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
 Session authz update response received for Client[1]
[05/09/14 13:13:49.430 IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:49.430 IST 64c2 211] AAA SRV(00000118):

Author method=SERVER_GROUP
 Zubair_ISE


[05/09/14 13:13:49.430 IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c4 211]  AAA SRV(00000000): process response req
[05/09/14 13:13:49.469 IST 64c5 220]

 AAA SRV(00000118): protocol reply PASS for
 Authorization


[05/09/14 13:13:49.469 IST 64c6 220]

 AAA SRV(00000118): Return Authorization status=PASS


[05/09/14 13:13:49.469 IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268
[05/09/14 13:13:49.469 IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268
[05/09/14 13:13:49.469 IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs
 have not been sent yet.
[05/09/14 13:13:49.469 IST 64ca 8151] 0017.7c2f.b69a Final flag values are,
 epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:49.469 IST 64cb 8151] 0017.7c2f.b69a
client incoming attribute size are 77
 --More--

[05/09/14 13:13:49.469 IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0
 uniqueId=280



[05/09/14 13:13:49.469 IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of
 apfApplyOverride2. Client State RUN



[05/09/14 13:13:49.469 IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for
 station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA
 override for station
[05/09/14 13:13:49.469 IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2,
 valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC:
 -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:49.469 IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station  ---
[05/09/14 13:13:49.469 IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN
 policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name
 e VLAN0012

[05/09/14 13:13:49.469 IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging
 VLAN  name VLAN0012 and VLAN ID  12
```

```
[05/09/14 13:13:49.469 IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:49.469 IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless
 client in WCM(NGWC)
[05/09/14 13:13:49.469 IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the
 ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:49.469 IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN
 policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site
 Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile
    MAC:  0017.7c2f.b69a , source 2

[05/09/14 13:13:49.469 IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into
 chain for station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits:
 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC:
 -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check
 continuation
[05/09/14 13:13:49.469 IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c
 apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:49.469 IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling
 applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:49.469 IST 64e3 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:49.469 IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2
 instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0,
 deviceType=(null), userRoleLen=0, userRole=(null)

[05/09/14 13:13:49.469 IST 64e5 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
  sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:49.469 IST 64e6 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:49.469 IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN
 = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station
 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim
 record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:49.469 IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim
 request, uid=280 passthrough=1
[05/09/14 13:13:49.469 IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:49.469 IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00
[05/09/14 13:13:49.469 IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE
 for station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:49.469 IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob
 State 3 llReq flag 0
[05/09/14 13:13:49.469 IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12
 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
 dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip  10.105.135.190
 ip_learn_type DHCP
 --More--
[05/09/14 13:13:49.469 IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc
```

[05/09/14 13:13:49.469 IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from AAA Pending to Associated

[05/09/14 13:13:49.469 IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:49.469 IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 49) in 1800 seconds
[05/09/14 13:13:49.469 IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800, Session Timeout = 1800

[05/09/14 13:13:49.469 IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a) client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN) mob_st<truncated>
[05/09/14 13:13:49.469 IST 64f7 207] [WCDB] ===intf src/dst (0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated>
[05/09/14 13:13:49.469 IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast action reqd
[05/09/14 13:13:49.469 IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0

[05/09/14 13:15:47.411 IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for station 0017.7c2f.b69a

[05/09/14 13:16:38.431 IST 650b 8151] 0017.7c2f.b69a

Client stats update: Time now in sec 1399621598, Last Acct Msg Sent at 1399621547 sec