融合接入和統一接入WLC上的中央Web身份驗證配置示例

目錄

簡介

本檔案介紹如何在融合存取無線LAN控制器(WLC)上以及融合存取WLC和整合存取WLC（5760之間以及5760和5508之間）之間設定中央Web驗證。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco WLC 5508、5760、3850基礎知識
- 身份服務引擎(ISE)基礎知識
- 無線移動的基本知識
- 訪客錨定基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS® XE 3.3.3版的WLC 5760
- 執行Cisco Aironet OS版本7.6的WLC 5508
- 執行Cisco IOS XE版本3.3.3的交換器3850
- 運行版本1.2的Cisco ISE

設定

> **註**：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

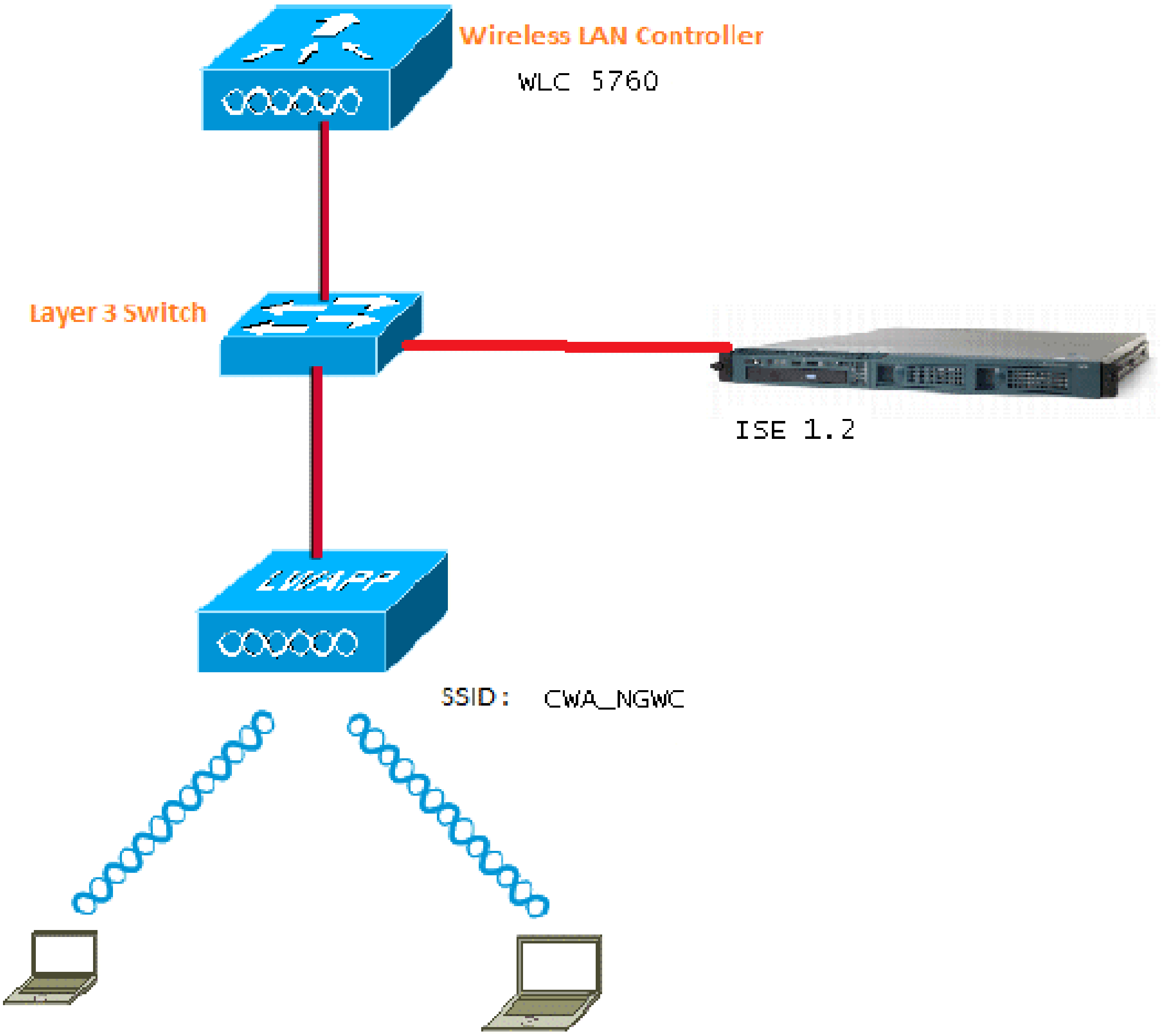
此流程包括以下步驟：

1. 使用者會連線到Web驗證服務組識別碼(SSID)，實際上是開放式+macfiltering且沒有第3層安全功能。
2. 使用者開啟瀏覽器。
3. WLC重新導向至訪客輸入網站。
4. 使用者在門戶上進行身份驗證。
5. ISE會傳送RADIUS授權變更（CoA - UDP連線埠1700）以指示控制器使用者有效，並最終推送RADIUS屬性，例如存取控制清單(ACL)。
6. 系統將提示使用者重試原始URL。

思科使用三種不同的部署設定來完成中央Web驗證(CWA)，這些設定涵蓋所有不同的方案。

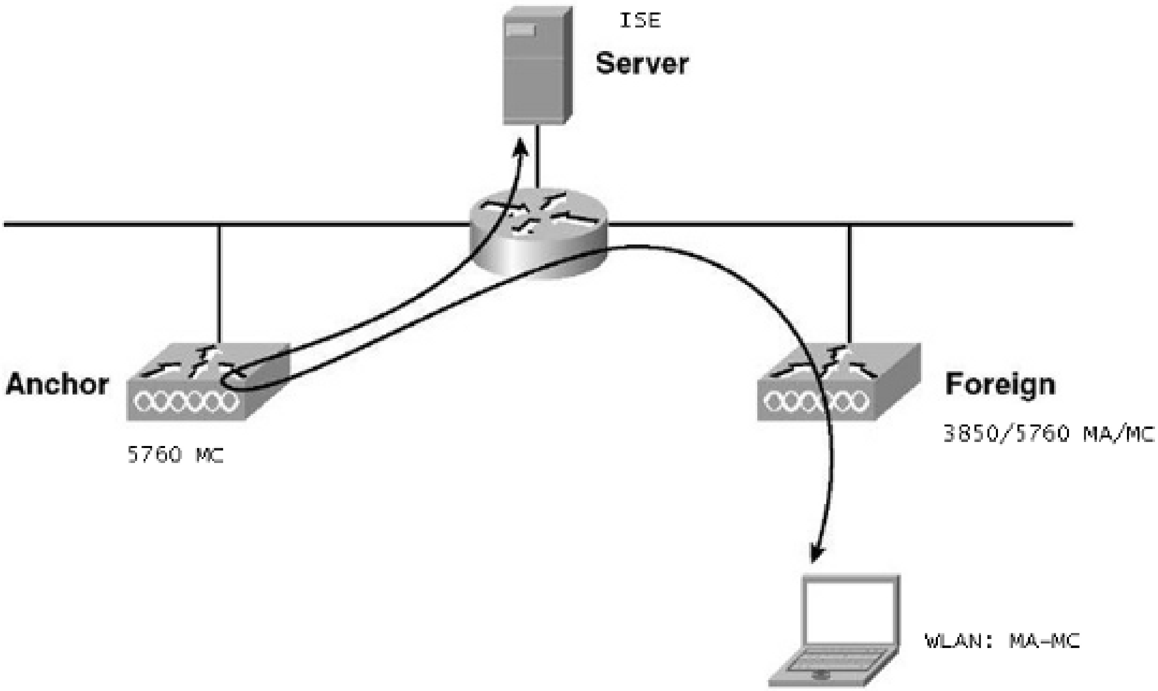
拓撲1

5760 WLC充當獨立WLC，且存取點終止於同一5760 WLC上。客戶端連線到無線LAN(WLAN)並由ISE進行身份驗證。



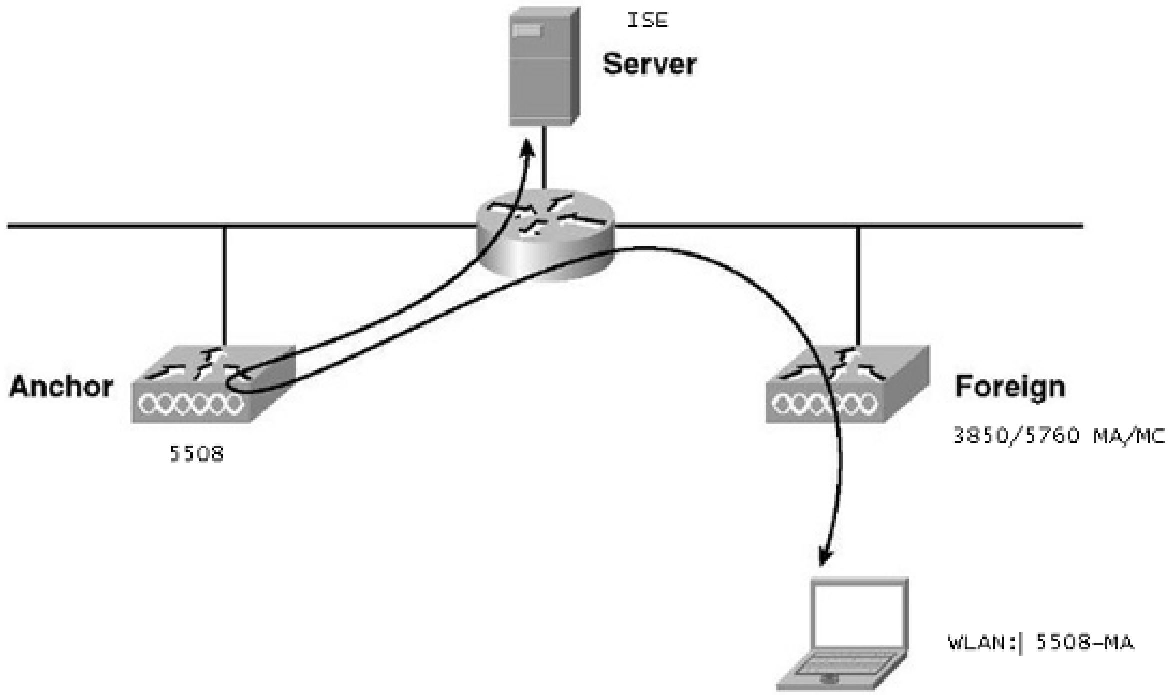
拓撲2

訪客錨定在融合接入WLC之間，其中一個充當行動控制器，另一個充當行動代理。移動代理是外部WLC，移動控制器是錨點。



拓撲3

訪客錨定在Cisco Unified WLC 5508和融合接入WLC 5760/3850之間，其中一個用作移動控制器，另一個用作移動代理。移動代理/移動控制器是外部WLC，5508移動控制器是錨點。



註：有許多部署，其中錨點是移動控制器，外部WLC是從另一個移動控制器獲取許可證的移動代理。在這種情況下，外部WLC僅有一個錨點，而該錨點是推送策略的錨點。不支援雙錨定，並且不起作用，因為預計它不會這樣工作。

範例

WLC 5508作為錨點，WLC 5760作為3850交換器（作為行動代理）的行動化控制器。對於錨點外部WLAN，WLC 5508將成為3850外部WLAN的錨點。根本無需在WLC 5760上設定該WLAN。如果將3850交換器指向5760錨點，然後從此WLC 5760到WLC 5508作為雙錨點，則它將無法運作，因為這會變成雙錨點，且原則位於5508錨點上。

如果您的設定包含作為錨點的WLC 5508、作為行動控制器的WLC 5760，以及作為行動代理和外部WLC的3850交換器，則3850交換器的錨點在任何時間都將是WLC 5760或WLC 5508。不能同時為和，並且雙錨點不起作用。

拓撲1配置示例

有關網路圖和說明，請參閱拓撲1。

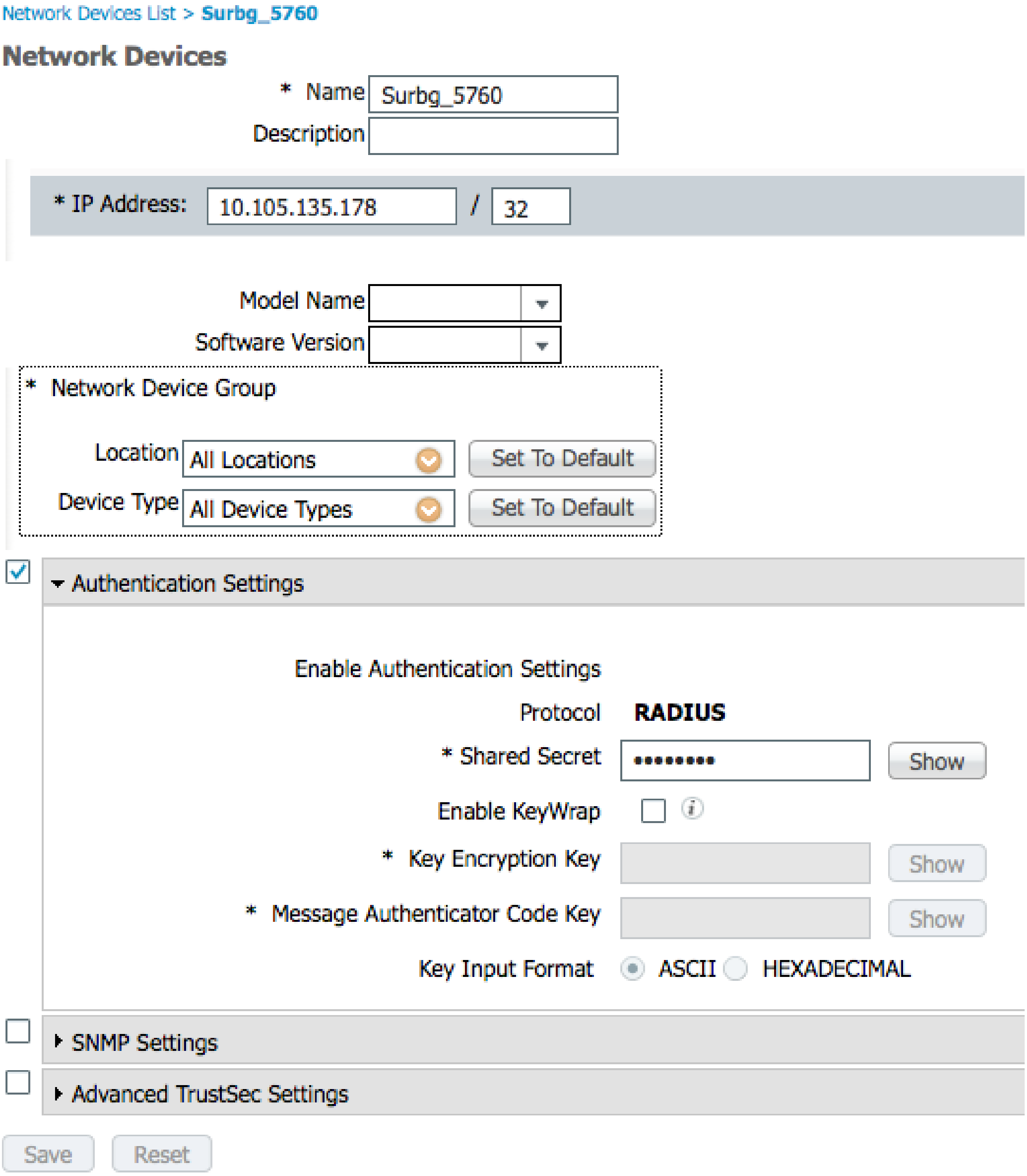
此組態分為兩個步驟：

1. ISE上的配置。
2. WLC 上的組態.

WLC 5760作為獨立WLC，使用者通過ISE驗證。

ISE上的配置

1. 選擇**ISE GUI > Administration > Network Resource > Network Devices List > Add**，以便在ISE上將WLC新增為身份驗證、授權和記帳(AAA)客戶端。確保在WLC上輸入與RADIUS伺服器上新增的共用金鑰。 **注意**：部署錨點外部時，只需新增外部WLC。無需在ISE上新增錨點WLC作為AAA客戶端。本文檔中的所有其他部署方案使用相同的ISE配置。


Network Devices List > Surbg_5760

Network Devices

* Name: Surbg_5760

Description:

* IP Address: 10.105.135.178 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations (Set To Default)

Device Type: All Device Types (Set To Default)

☑ Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: •••••••••

Enable KeyWrap: □

* Key Encryption Key:

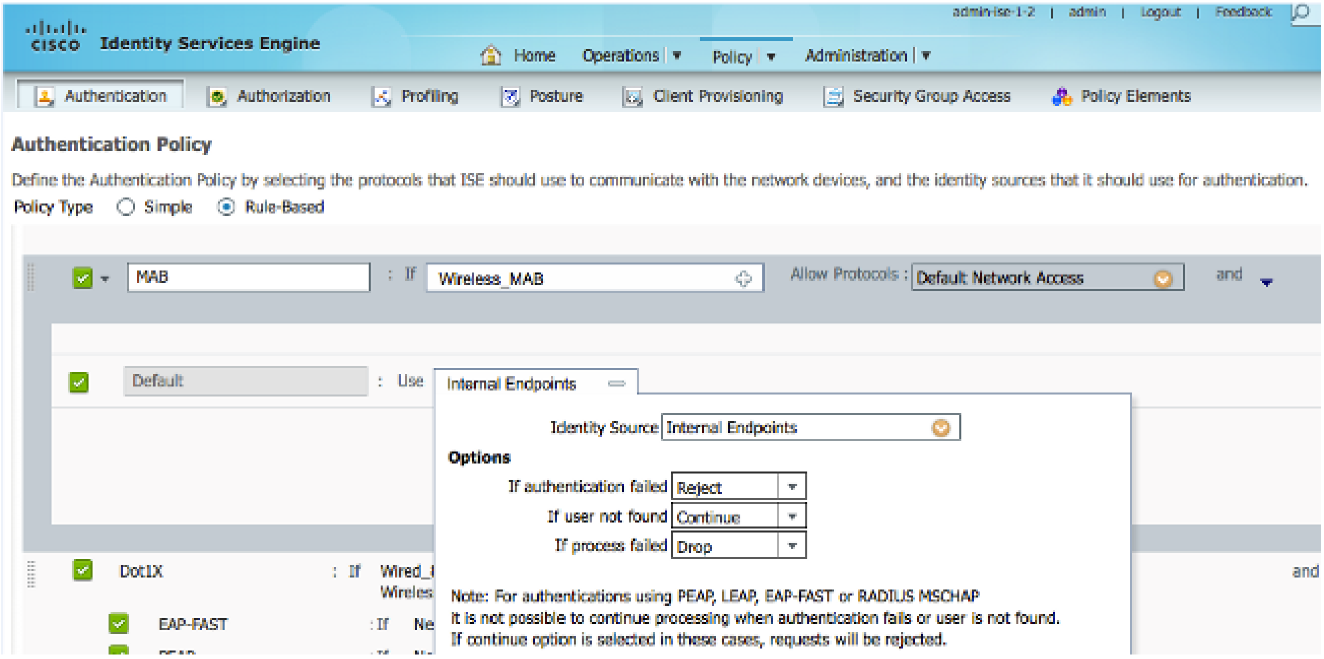
* Message Authenticator Code Key:

Key Input Format: ● ASCII ○ HEXADECIMAL

□ SNMP Settings

□ Advanced TrustSec Settings

2. 在ISE GUI中，選擇**Policy > Authentication > MAB > Edit**以建立身份驗證策略。身份驗證策略接受指向內部端點的客戶端的MAC地址。 在「選項」清單中選擇以下選項：從If authentication failed下拉選單中，選擇**Reject**。在「If user not found（未找到使用者）」下拉式清單中選擇**「Continue」**。在If process failed下拉選單中，選擇**Drop**。使用這些選項進行配置時，MAC授權失敗的客戶端會繼續訪問訪客門戶。



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use Internal Endpoints

Identity Source Internal Endpoints

Options

If authentication failed Reject

If user not found Continue

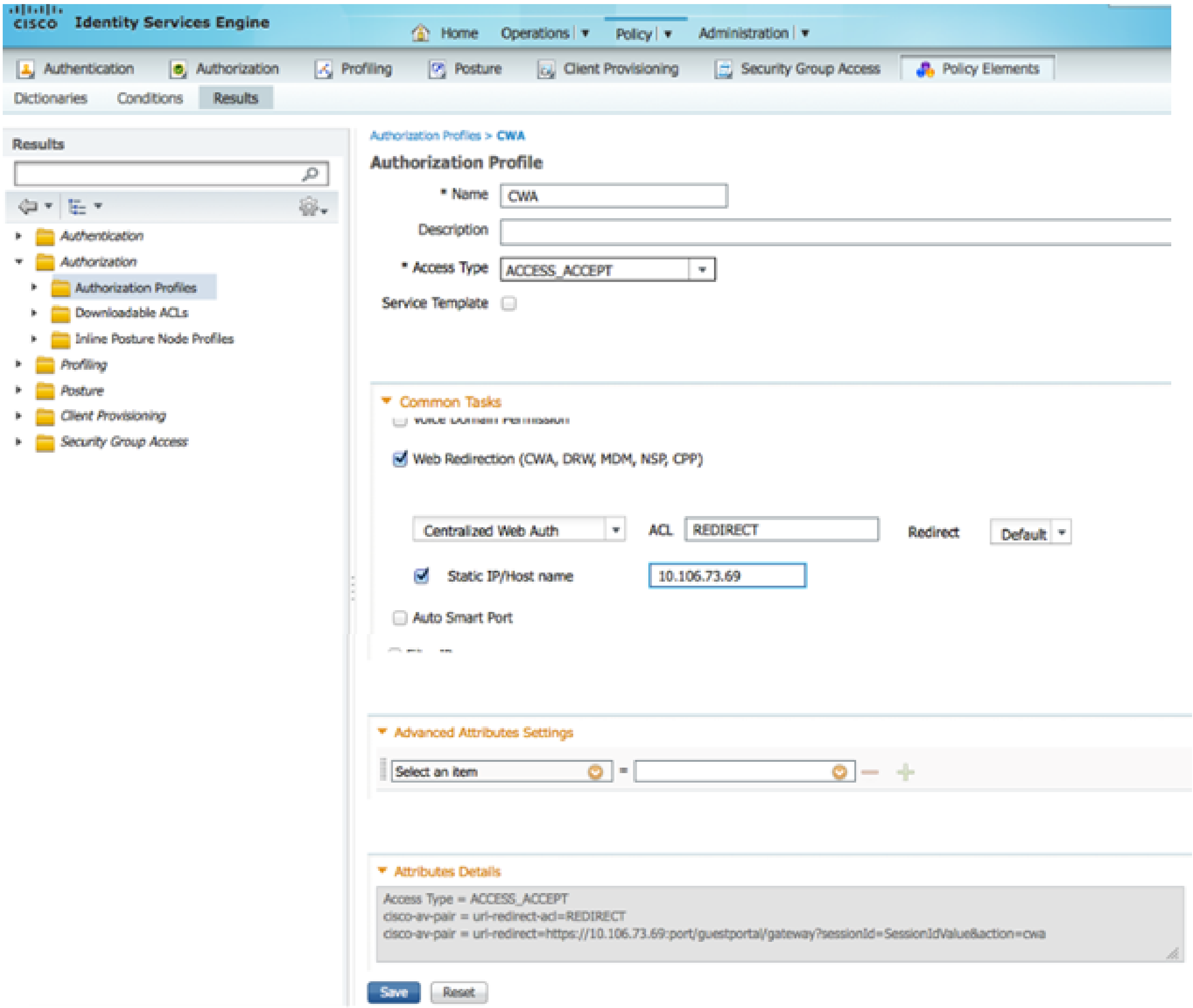
If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
it is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.

☑ Dot1X : If Wired_ Wireles and

☑ EAP-FAST : If Ne

3. 在ISE GUI中，選擇**Policy > Authorization > Results > Authorization Profiles > Add**。填寫詳細資訊並按一下**Save**以建立授權配置檔案。 此設定檔協助使用者端重新導向至MAC驗證後的重新導向URL，以便使用者端輸入訪客使用者名稱/密碼。



Authorization Profiles > CWA

Authorization Profile

* Name CWA

Description

* Access Type ACCESS_ACCEPT

Service Template □

▾ Common Tasks

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Centralized Web Auth ACL REDIRECT Redirect Default

☑ Static IP/Host name 10.106.73.69

□ Auto Smart Port

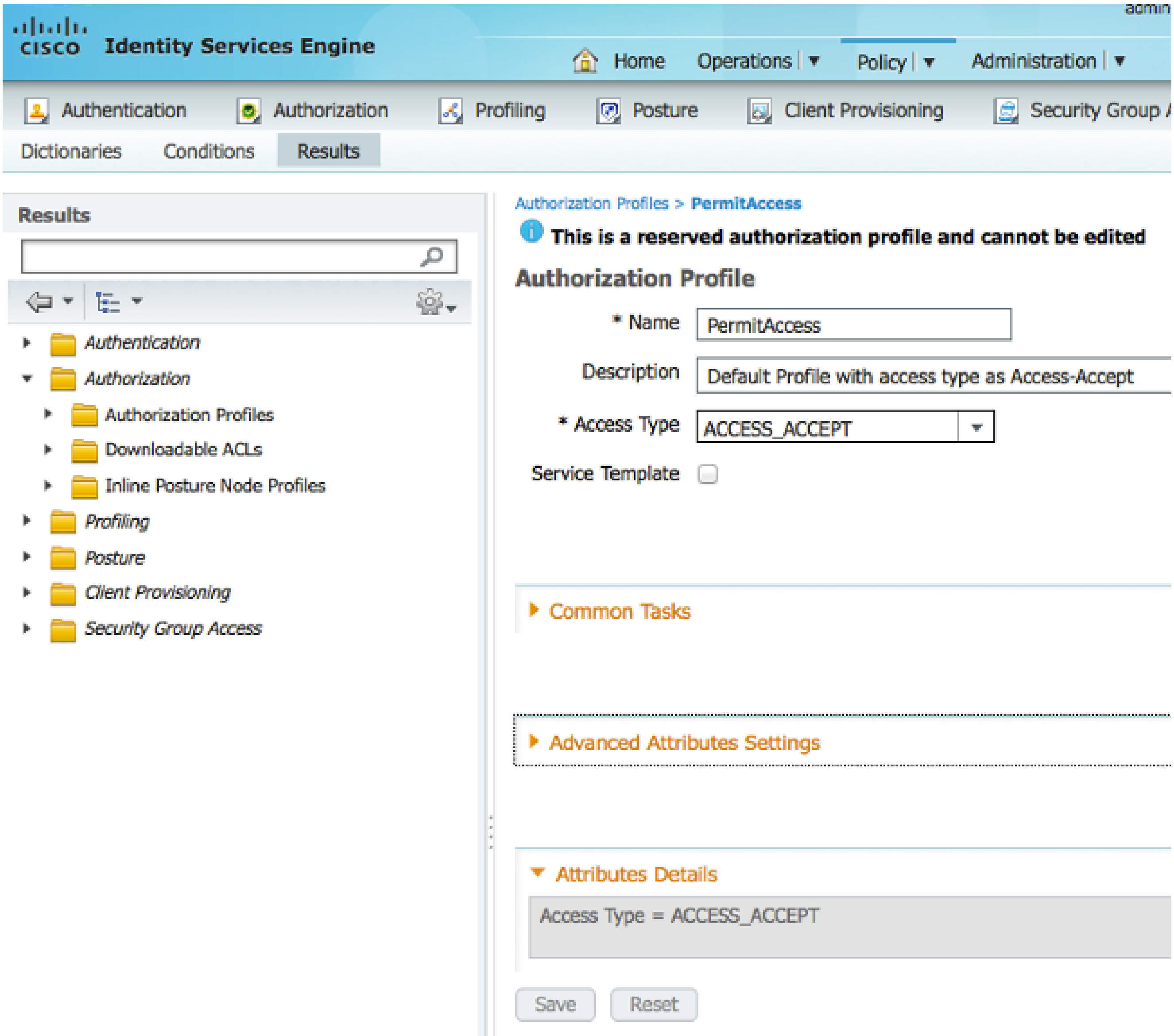
▾ Advanced Attributes Settings

Select an item =

▾ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=REDIRECT
cisco-av-pair = url-redirect=https://10.106.73.69:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

4. 在ISE GUI中，選擇**Policy > Authorization > Results > Authorization Profiles > Add**以建立另一個授權配置檔案以允許使用正確憑證訪問使用者。



Authorization Profiles > PermitAccess

This is a reserved authorization profile and cannot be edited

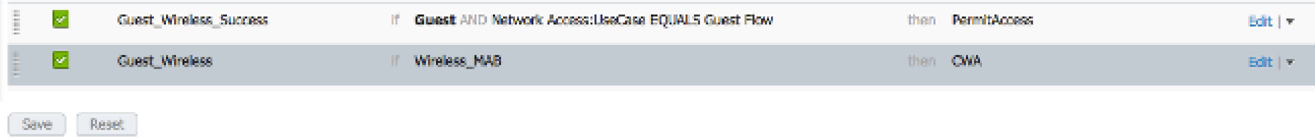
Authorization Profile

* Name	PermitAccess
Description	Default Profile with access type as Access-Accept
* Access Type	ACCESS_ACCEPT
Service Template	□

Access Type = ACCESS_ACCEPT

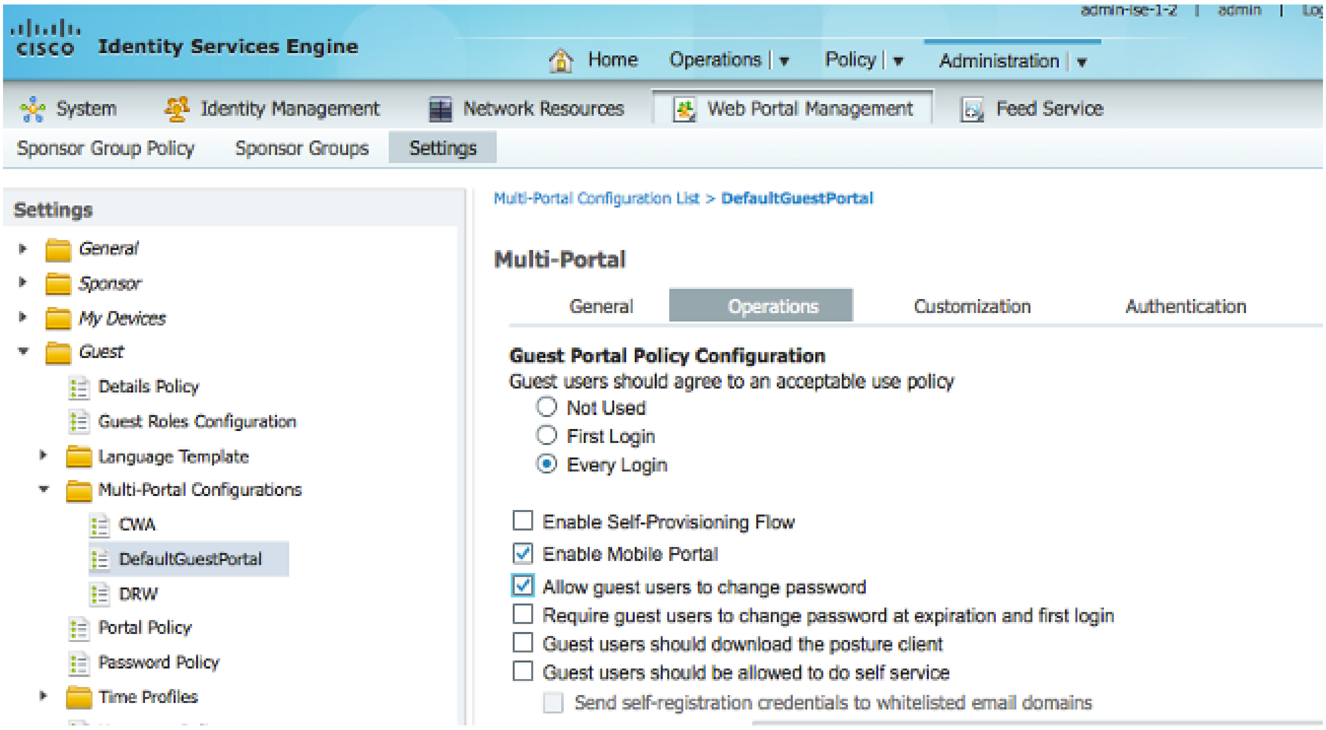
5. 建立授權策略。 授權策略「Guest_Wireless」將重定向URL和重定向ACL推送到客戶端會話。此處推入的配置檔案是CWA（如前所示）。授權策略「Guest_Wireless-Success」允許通過訪客門戶成功進行身份驗證的訪客使用者具有完全訪問許可權。使用者在訪客入口上成功通過驗證後，WLC會傳送動態授權。這將使用屬性「Network Access:Use EQUALS Guest Flow」重新驗證客戶端會話。最終授權策略如下所示

:



☑	Guest_Wireless_Success	If	Guest AND Network Access:UseCase EQUALS Guest Flow	then	PermitAccess	Edit
☑	Guest_Wireless	If	Wireless_MAB	then	CWA	Edit

6. 可選：在這種情況下，使用預設的多門戶配置。根據要求，可以在GUI中更改相同內容。 在ISE GUI中選擇**Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal**。



Guest Portal Policy Configuration

Guest users should agree to an acceptable use policy

○ Not Used

○ First Login

● Every Login

□ Enable Self-Provisioning Flow

☑ Enable Mobile Portal

☑ Allow guest users to change password

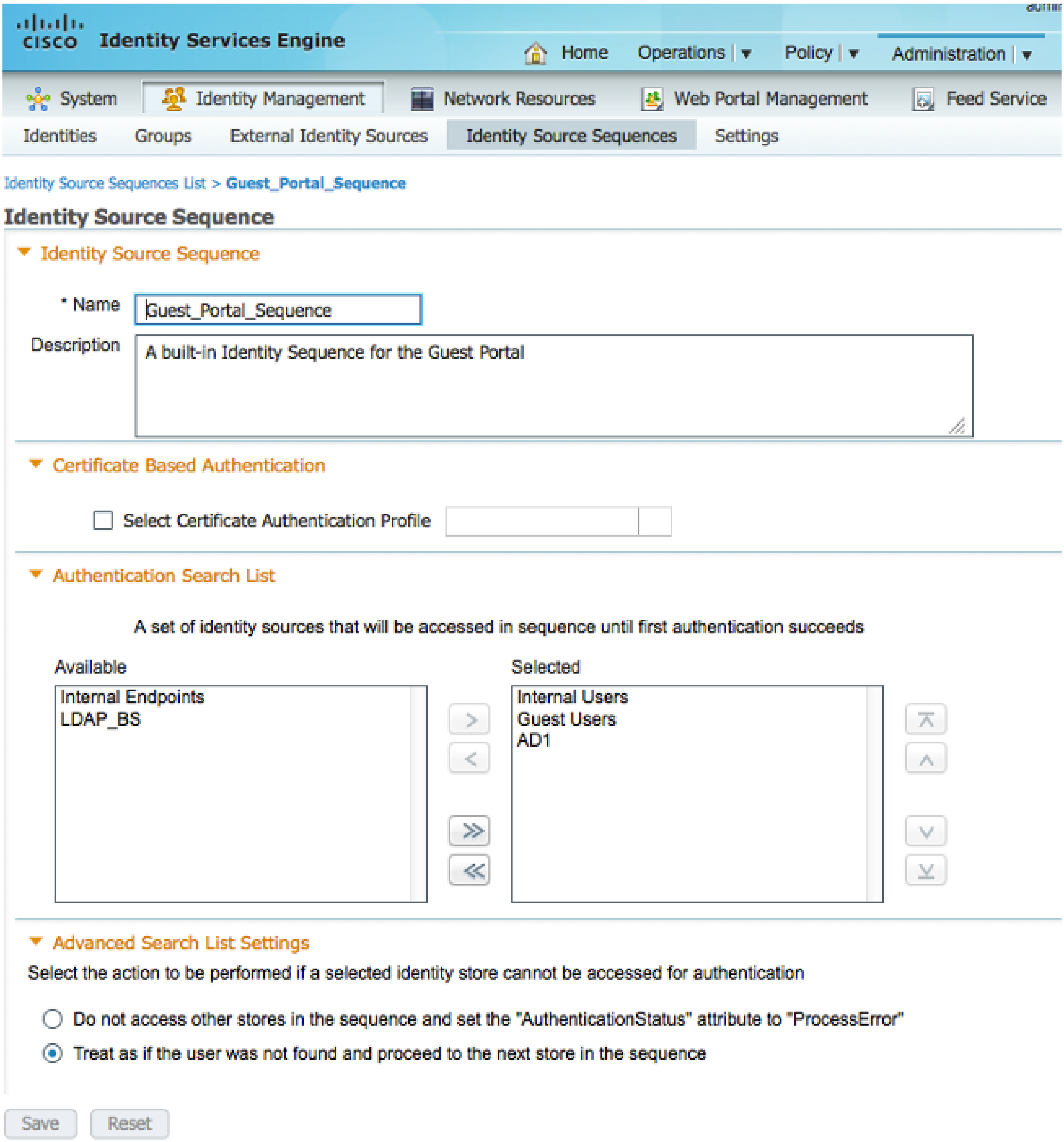
□ Require guest users to change password at expiration and first login

□ Guest users should download the posture client

□ Guest users should be allowed to do self service

□ Send self-registration credentials to whitelisted email domains

建立Guest_Portal_sequence，允許內部、訪客和AD使用者。



cisco Identity Services Engine
Home
Operations
Policy
Administration
System
Identity Management
Network Resources
Web Portal Management
Feed Service
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Source Sequences List > Guest_Portal_Sequence

Identity Source Sequence

Identity Source Sequence

* Name: Guest_Portal_Sequence

Description: A built-in Identity Sequence for the Guest Portal

Certificate Based Authentication

□ Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints LDAP_BS	Internal Users Guest Users AD1

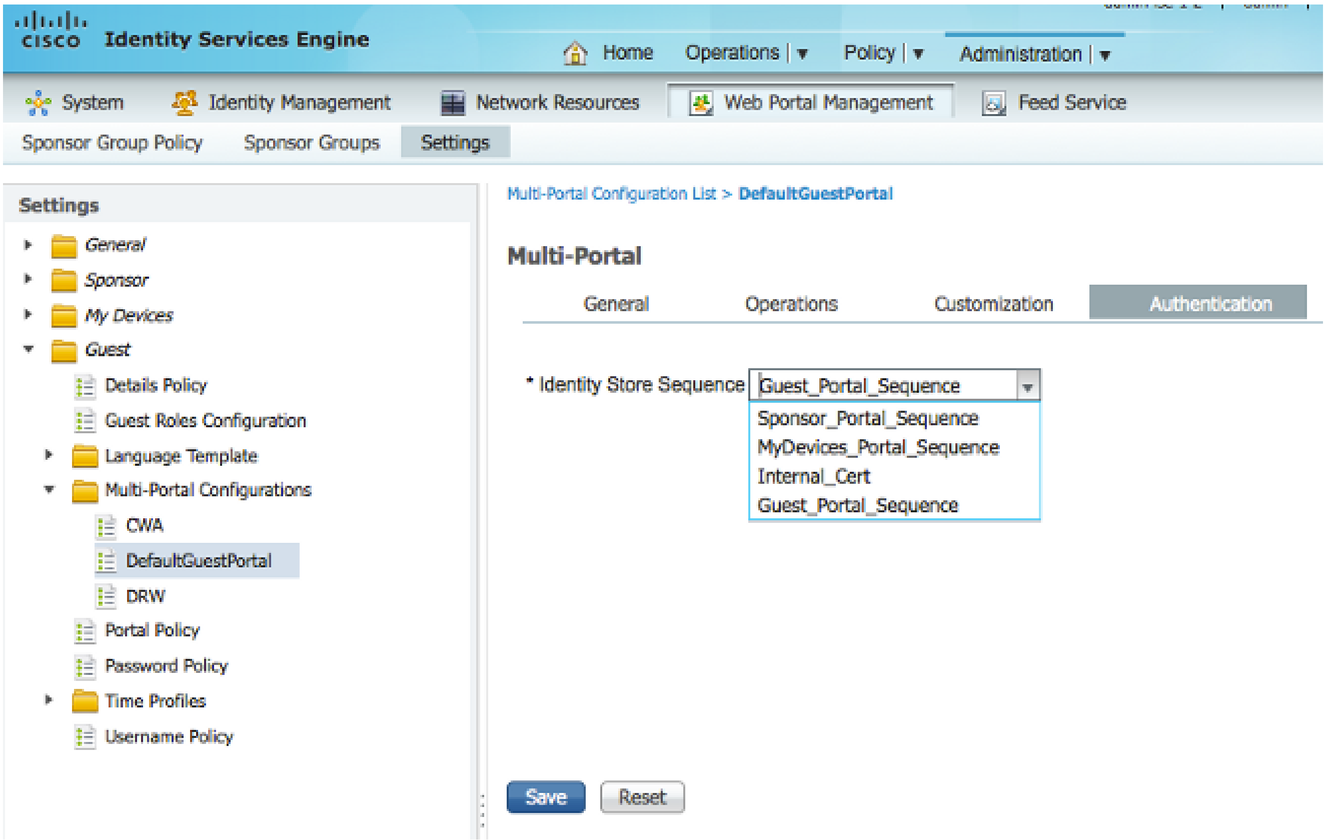
Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

7. 在ISE GUI中，選擇**Guest > Multi-Portal Configurations > DefaultGuestPortal**。從Identify Store Sequence下拉選單中選擇**Guest_Portal_Sequence**。



* Identity Store Sequence: Guest_Portal_Sequence

WLC 上的組態

1. 在WLC 5760上定義ISE Radius伺服器。
2. 使用CLI配置RADIUS伺服器、伺服器組和方法清單。

```
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. 使用CLI設定WLAN。

```
wlan CWA_NGWC 10 CWA_NGWC
 aaa-override
accounting-list ISE
client vlan VLAN0012
no exclusionlist
mac-filtering MACFILTER
nac
```

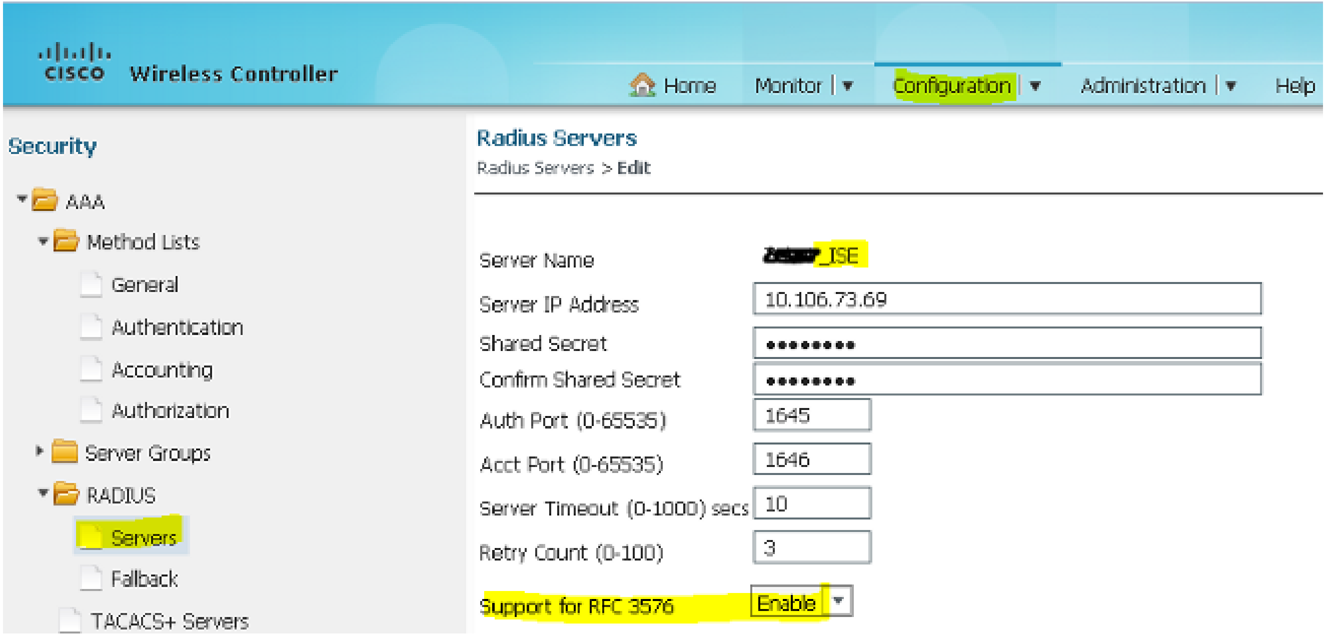
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

4. 使用CLI設定重新導向ACL。 這是ISE作為AAA覆蓋返回的url-redirect-acl，以及訪客門戶重定向的重定向URL。它是當前在統一架構上使用的直接ACL。這是一個「punt」ACL，也就是通常用於統一架構的反向ACL。您需要阻止對DHCP、DHCP伺服器、DNS、DNS伺服器和ISE伺服器的訪問。根據需要僅允許www、443和8443。此ISE訪客門戶使用埠8443，重定向仍可使用此處顯示的ACL。此處啟用了ICMP，但根據安全規則，您可以拒絕或允許。

```
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
```

注意：啟用HTTPS時，由於可擴充性，可能會造成一些高CPU問題。除非思科設計團隊推薦此功能，否則請不要啟用它。

5. 在無線控制器GUI中選擇**AAA > RADIUS > Servers**。在GUI中配置RADIUS伺服器、伺服器組和方法清單。 填寫所有引數並確保此處配置的共用金鑰與ISE上為此裝置配置的共用金鑰匹配。在「RFC 3576支援」下拉選單中，選擇**啟用**。



Radius Servers

Radius Servers > Edit

Server Name [redacted]_ISE

Server IP Address 10.106.73.69

Shared Secret ••••••••

Confirm Shared Secret ••••••••

Auth Port (0-65535) 1645

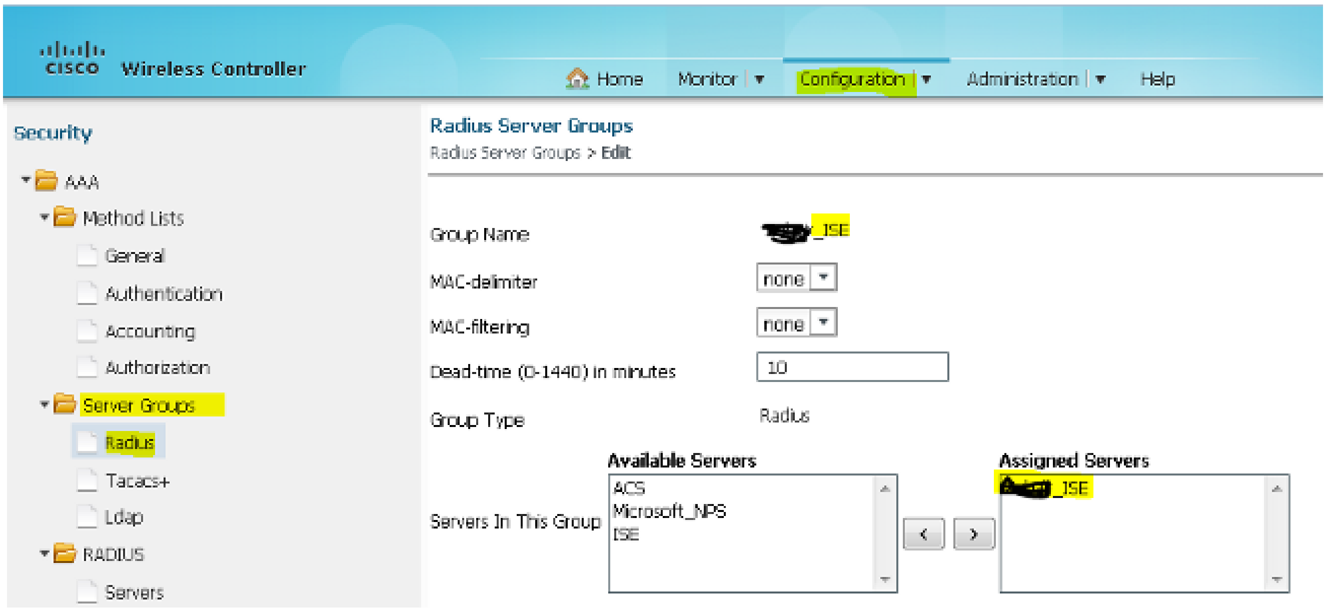
Acct Port (0-65535) 1646

Server Timeout (0-1000) secs 10

Retry Count (0-100) 3

Support for RFC 3576 Enable

6. 在無線控制器GUI中選擇**AAA > Server Groups > Radius**。將先前建立的RADIUS伺服器新增到伺服器組。

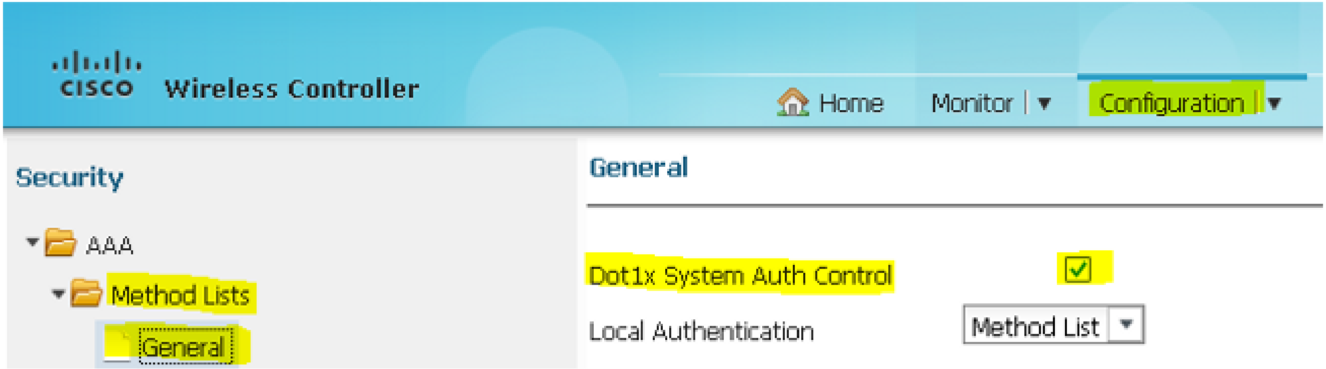


Radius Server Groups
Radius Server Groups > Edit

Group Name [redacted]_ISE
MAC-delimiter none
MAC-filtering none
Dead-time (0-1440) in minutes 10
Group Type Radius

Servers In This Group
Available Servers: ACS, Microsoft_NPS, ISE
Assigned Servers: [redacted]_ISE

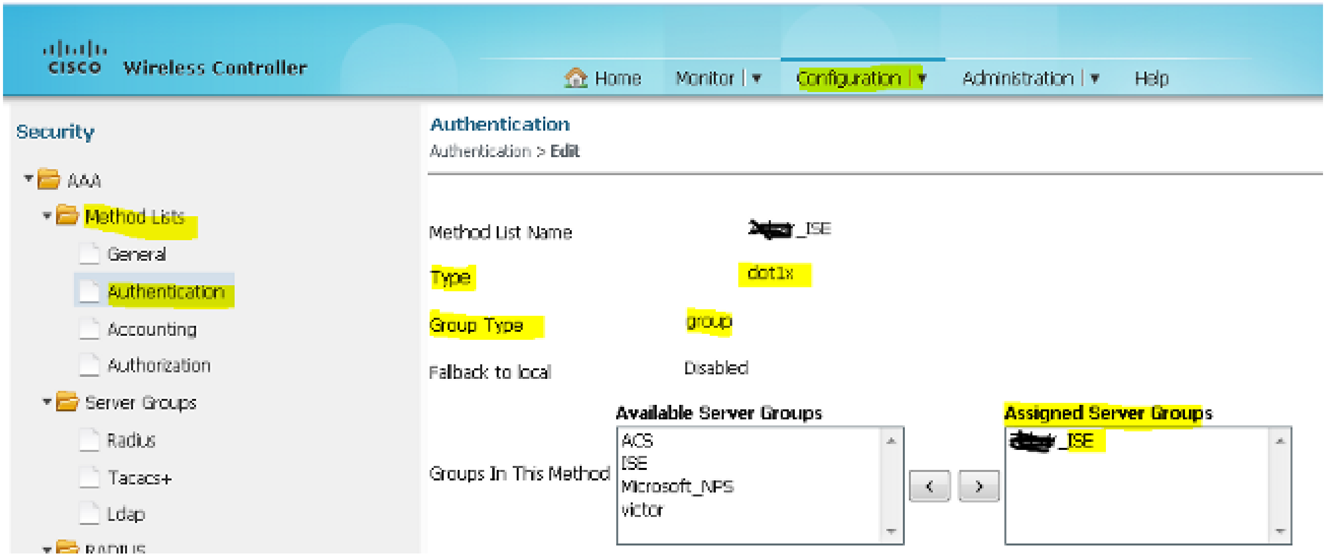
7. 從無線控制器GUI中選擇**AAA > Method Lists > General**。選中**Dot1x System Auth Control**覈取方塊。如果禁用此選項，則AAA不起作用。



General

Dot1x System Auth Control ☑
Local Authentication Method List

8. 在無線控制器GUI中選擇**AAA > Method Lists > Authentication**。為dot1X型別建立身份驗證方法清單。組型別為組。將其對映到ISE。

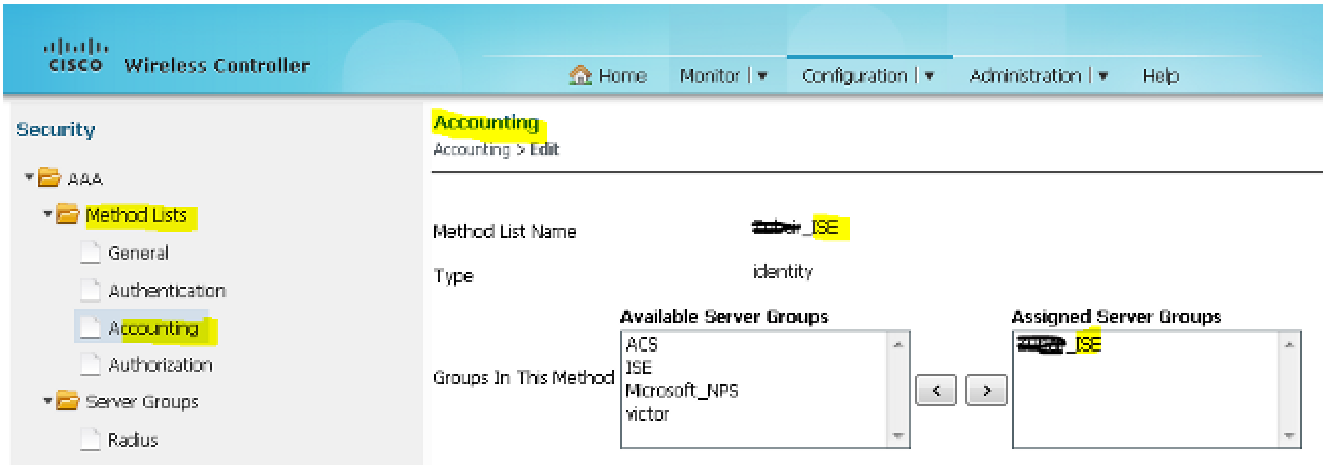


Authentication
Authentication > Edit

Method List Name [redacted]_ISE
Type dot1x
Group Type group
Fallback to local Disabled

Groups In This Method
Available Server Groups: ACS, ISE, Microsoft_NPS, victor
Assigned Server Groups: [redacted]_ISE

9. 從無線控制器GUI中選擇**AAA > Method Lists > Accounting**。為型別標識建立記帳方法清單。將其對映到ISE。



Accounting

Accounting > Edit

Method List Name [redacted]_ISE

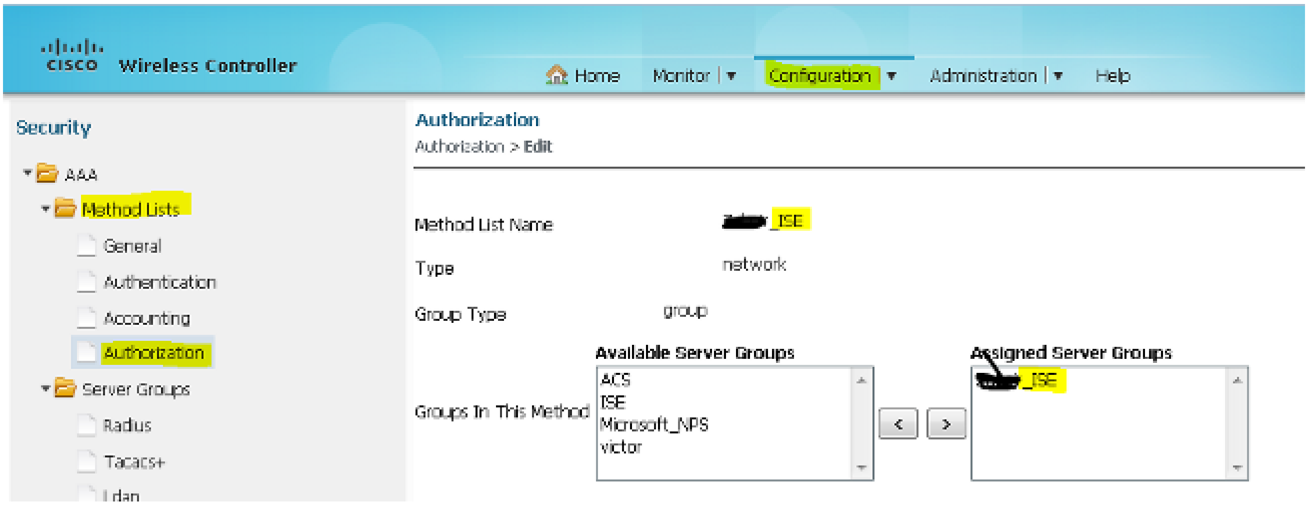
Type identity

Groups In This Method

Available Server Groups: ACS, ISE, Microsoft_NPS, victor

Assigned Server Groups: [redacted]_ISE

10. 在無線控制器GUI中選擇**AAA > Method Lists > Authorization**。為Type網路建立授權方法清單。將其對映到ISE。



Authorization

Authorization > Edit

Method List Name [redacted]_ISE

Type network

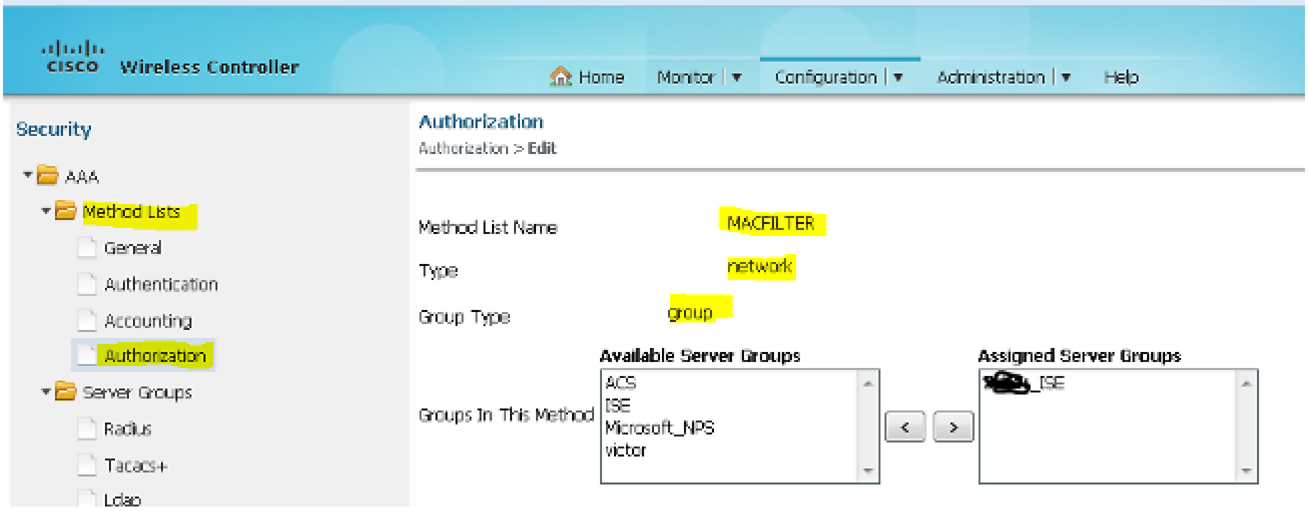
Group Type group

Groups In This Method

Available Server Groups: ACS, ISE, Microsoft_NPS, victor

Assigned Server Groups: [redacted]_ISE

11. 可選，因為還支援MAC故障。為型別網路建立授權方法清單MACFILTER。將其對映到ISE。



Authorization

Authorization > Edit

Method List Name MACFILTER

Type network

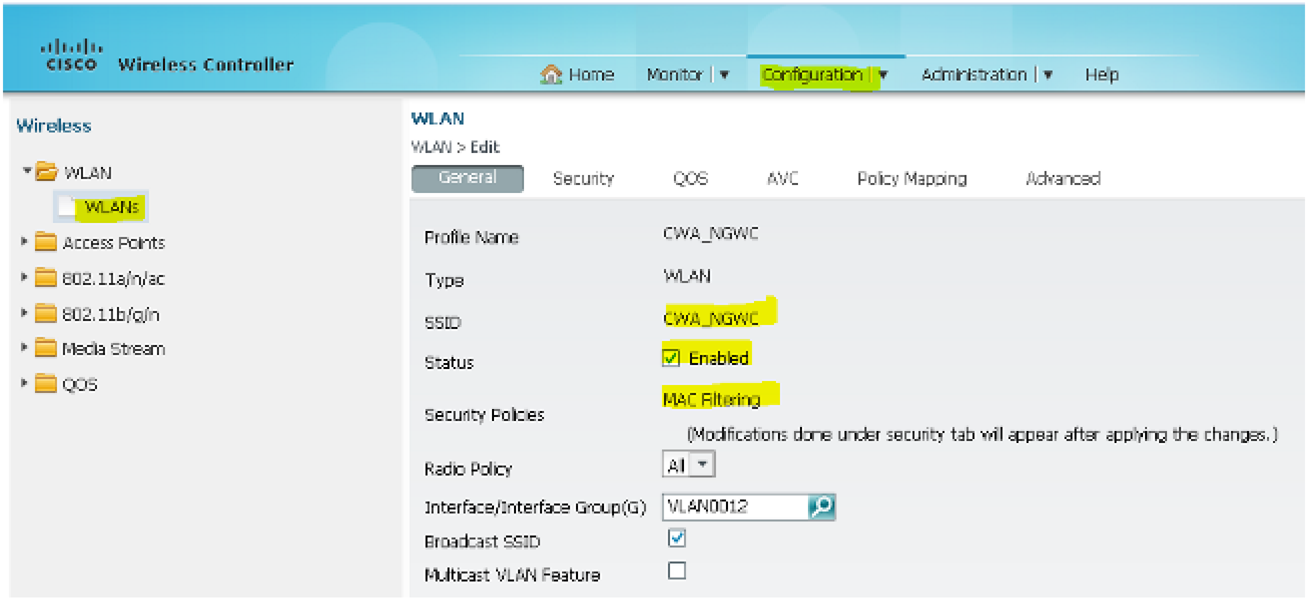
Group Type group

Groups In This Method

Available Server Groups: ACS, ISE, Microsoft_NPS, victor

Assigned Server Groups: [redacted]_ISE

12. 在無線控制器GUI中選擇**WLAN > WLANs**。使用此處顯示的引數建立新配置。



Profile Name CWA_NGWC

Type WLAN

SSID CWA_NGWC

Status ☑ Enabled

Security Policies MAC Filtering

(Modifications done under security tab will appear after applying the changes.)

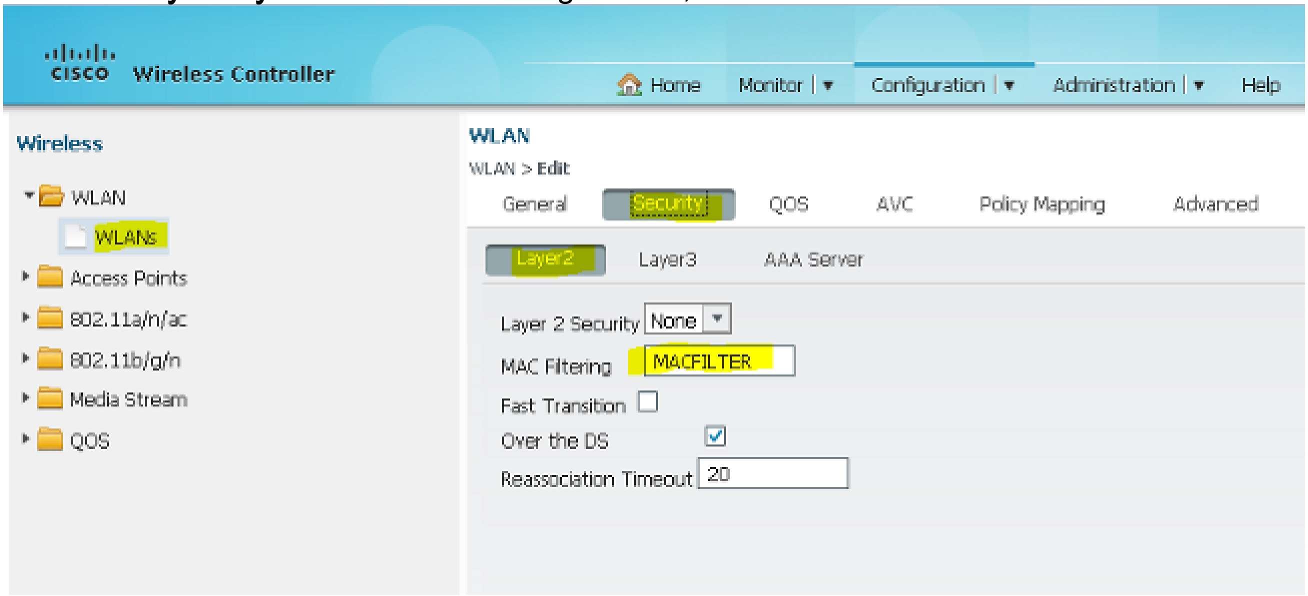
Radio Policy All

Interface/Interface Group(G) VLAN0012

Broadcast SSID ☑

Multicast VLAN Feature □

13. 選擇**Security > Layer2**。在MAC Filtering欄位中，輸入**MACFILTER**。



Layer 2 Security None

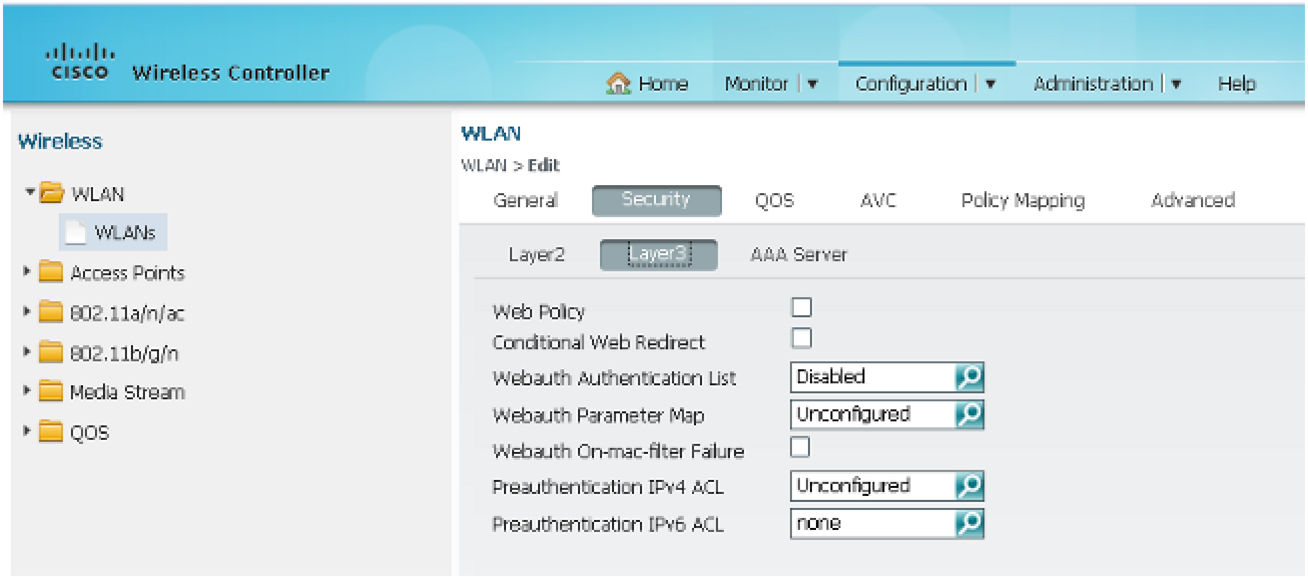
MAC Filtering MACFILTER

Fast Transition □

Over the DS ☑

Reassociation Timeout 20

14. 無需配置第3層。



Web Policy □

Conditional Web Redirect □

Webauth Authentication List Disabled

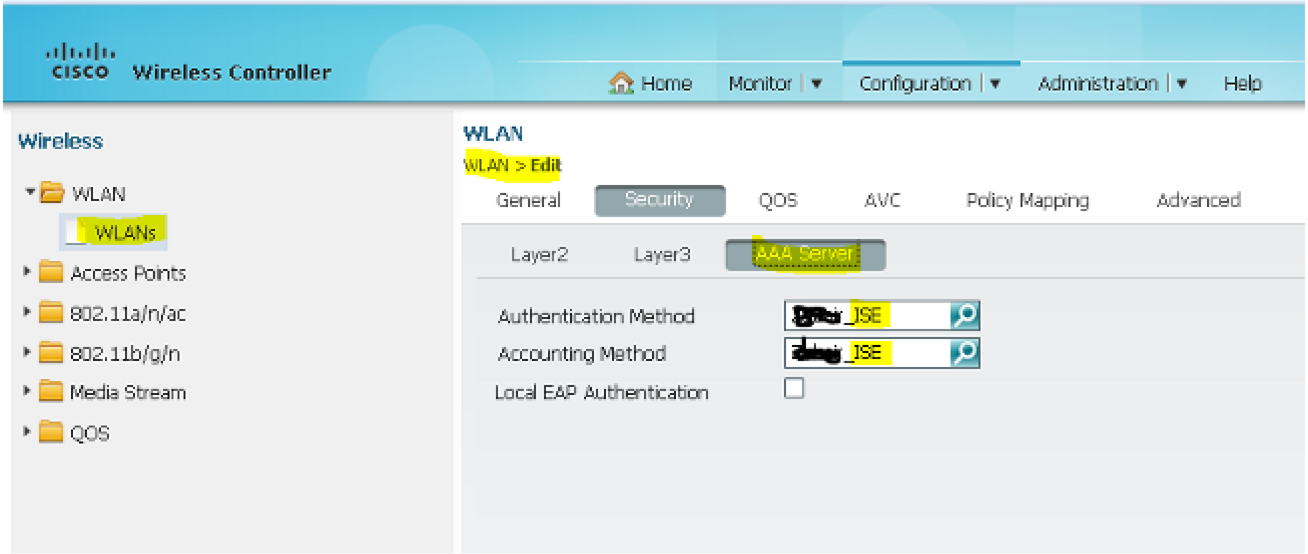
Webauth Parameter Map Unconfigured

Webauth On-mac-filter Failure □

Preauthentication IPv4 ACL Unconfigured

Preauthentication IPv6 ACL none

15. 選擇**Security > AAA Server**。在Authentication Method下拉選單中，選擇**ISE**。從Accounting Method下拉選單中，選擇**ISE**。

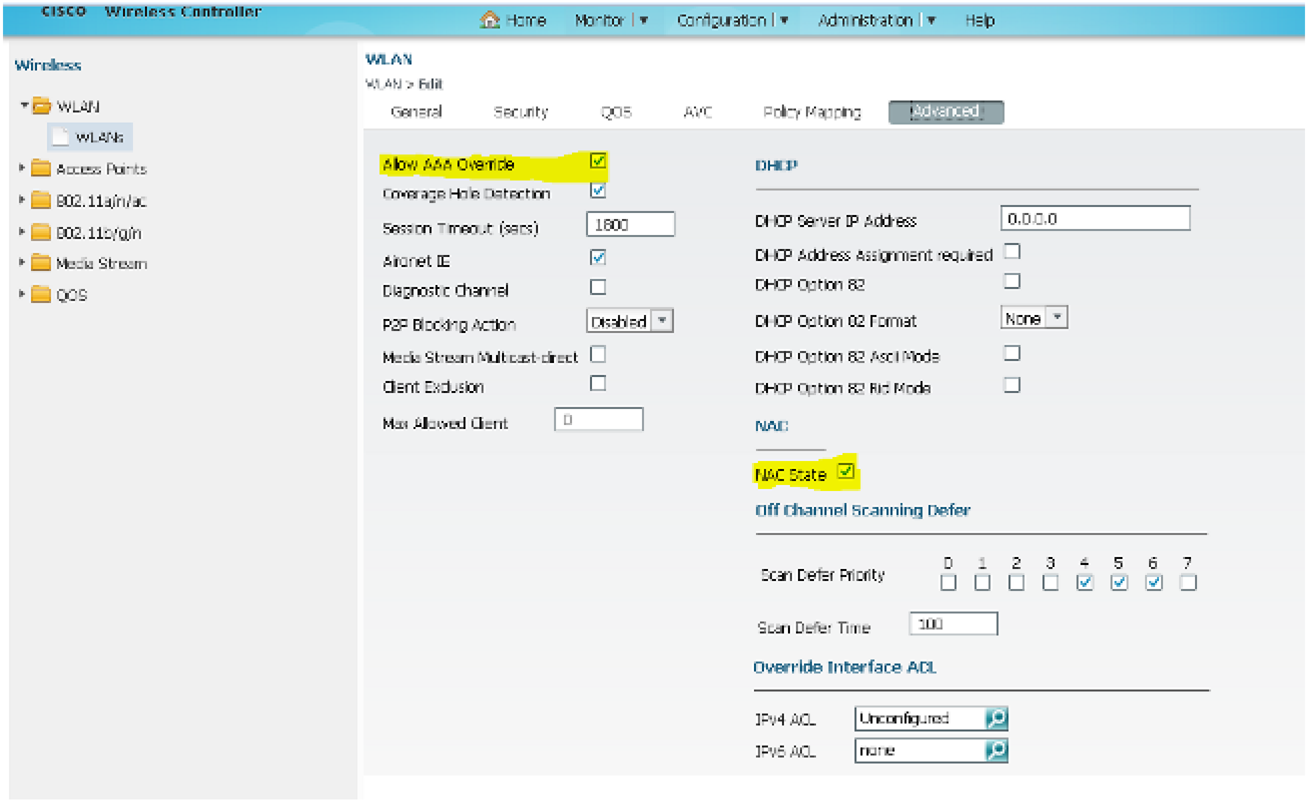


Authentication Method [redacted]_ISE

Accounting Method [redacted]_ISE

Local EAP Authentication □

16. 選擇**Advanced**。選中**Allow AAA Override**覈取方塊。選中**NAC狀態**覈取方塊。



Allow AAA Override ☑

Coverage Hole Detection ☑

Session Timeout (secs) 1800

Aironet IE ☑

Diagnostic Channel □

P2P Blocking Action Disabled

Media Stream Multicast-direct □

Client Exclusion □

Max Allowed Client 0

DHCP

DHCP Server IP Address 0.0.0.0

DHCP Address Assignment required □

DHCP Option 82 □

DHCP Option 82 Format None

DHCP Option 82 Ascii Mode □

DHCP Option 82 Rid Mode □

NAC

NAC State ☑

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □

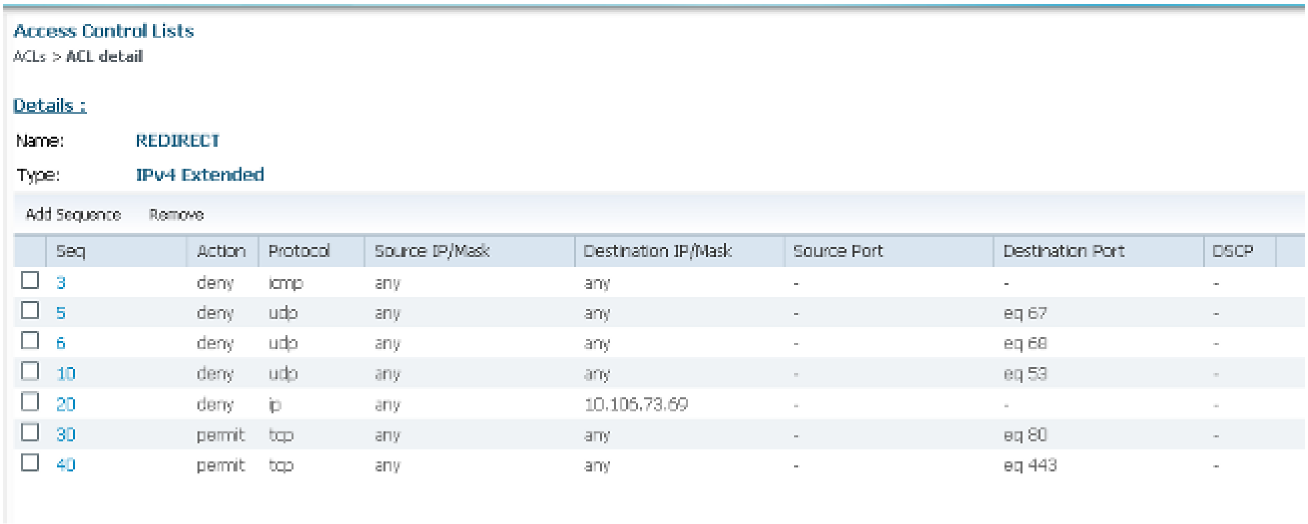
Scan Defer Time 100

Override Interface ACL

IPv4 ACL Unconfigured

IPv6 ACL none

17. 在GUI中設定WLC上的重新導向ACL。


Access Control Lists

ACLs > ACL detail

Details :

Name: REDIRECT

Type: IPv4 Extended

	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	-

拓撲2配置示例

有關網路圖和說明，請參閱拓撲2。

此配置也是分兩步進行的。

ISE上的配置

ISE上的配置與拓撲1的配置相同。

無需在ISE上新增錨點控制器。您只需在ISE上新增外部WLC，在外部WLC上定義RADIUS伺服器，並在WLAN下對映授權策略。在錨點上，您只需啟用MAC過濾。

在此組態範例中，有兩個WLC 5760擔任外部錨點。如果您想要使用WLC 5760作為錨點，使用3850交換器作為外部錨點（也就是行動代理）連線到另一個行動控制器，則相同的設定是正確的。但是，無需在3850交換器從其獲得許可證的第二個行動控制器上設定WLAN。您只需將3850交換器指向充當錨點的WLC 5760。

WLC 上的組態

1. 在外部，使用AAA的AAA方法清單配置ISE伺服器，並將WLAN對映到MAC過濾器授權。 **注意**：在錨點和外部以及MAC過濾上配置重定向ACL。

```
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. 使用CLI設定重新導向ACL。 這是ISE作為AAA覆蓋返回的url-redirect-acl，以及訪客門戶重定向的重定向URL。它是當前在統一架構上使用的直接ACL。這是一個「punt」ACL，也就是通常用於統一架構的反向ACL。您需要阻止對DHCP、DHCP伺服器、DNS、DNS伺服器和ISE伺服器的訪問。根據需要僅允許www、443和8443。此ISE訪客門戶使用埠8443，重定向仍可使用此處顯示的ACL。此處啟用了ICMP，但根據安全規則，您可以拒絕或允許。
   ```
   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
   ```
   注意：啟用HTTPS時，由於可擴充性，可能會造成一些高CPU問題。除非思科設計團隊推薦此功能，否則請不要啟用它。
3. 在錨點上配置移動性。
   ```
   wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
   ```
   註：如果將3850交換器設定為外部，則請確保在行動控制器上定義交換器對等群組，並在行動控制器上定義交換器對等群組。然後在3850交換機上配置上述CWA配置。
4. 錨點上的配置。 在錨點上，無需配置任何ISE配置。您只需要配置WLAN。
   ```
   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. 在錨點上配置移動性。 將另一個WLC定義為此WLC上的行動成員。
   ```
   wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
   ```
6. 使用CLI設定重新導向ACL。 這是ISE作為AAA覆蓋返回的url-redirect-acl，以及訪客門戶重定向的重定向URL。它是當前在統一架構上使用的直接ACL。這是一個「punt」ACL，也就是通常用於統一架構的反向ACL。您需要阻止對DHCP、DHCP伺服器、DNS、DNS伺服器和ISE伺服器的訪問。根據需要僅允許www、443和8443。此ISE訪客門戶使用埠8443，重定向仍可使用此處顯示的ACL。此處啟用了ICMP，但根據安全規則，您可以拒絕或允許。
   ```
   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
   ```
   注意：啟用HTTPS時，由於可擴充性，可能會造成一些高CPU問題。除非思科設計團隊推薦此功能，否則請不要啟用它。

拓撲3配置示例

有關網路圖和說明，請參閱拓撲3。

這也是一個兩步過程。

ISE上的配置

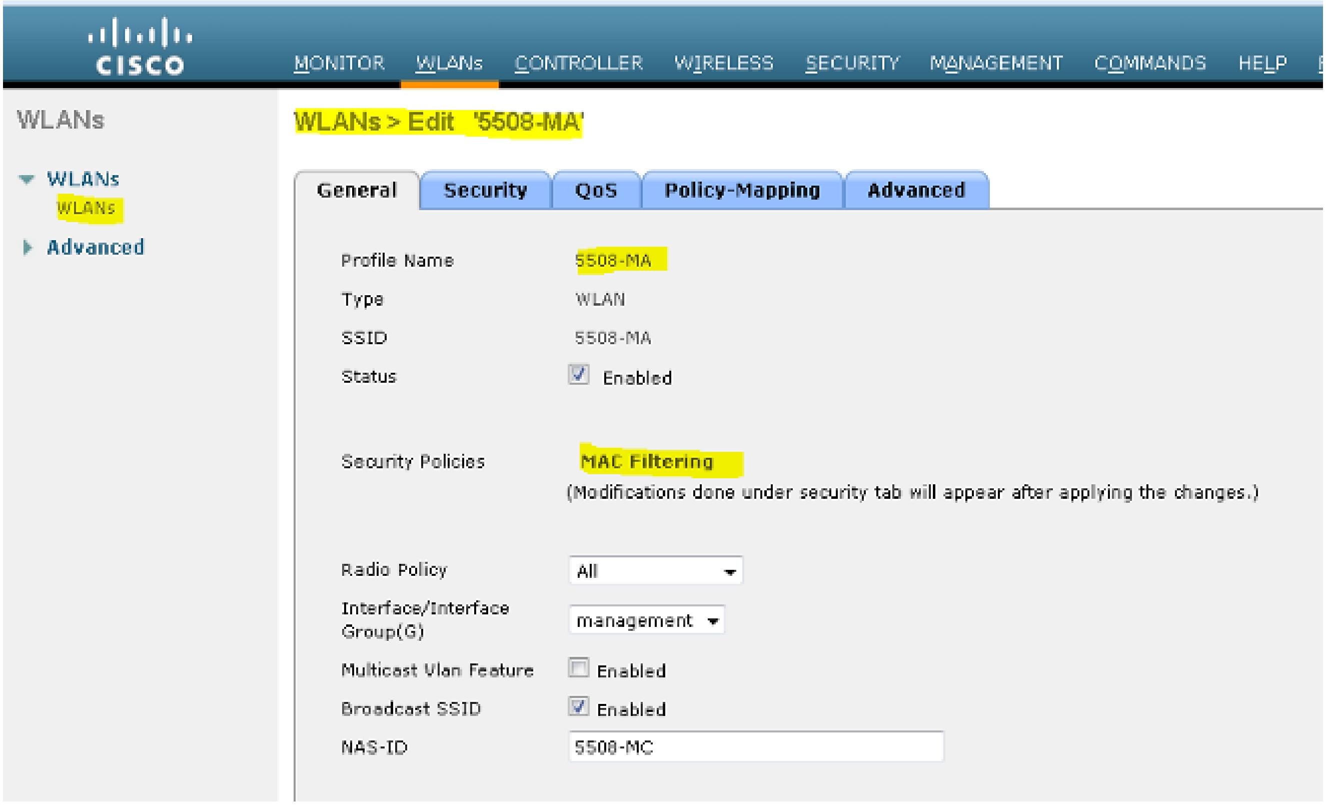
ISE上的配置與拓撲1的配置相同。

無需在ISE上新增錨點控制器。您只需在ISE上新增外部WLC，在外部WLC上定義RADIUS伺服器，並在WLAN下對映授權策略。在錨點上，您只需啟用MAC過濾。

在本範例中，有一種WLC 5508擔任錨點，而一種WLC 5760擔任外部WLC。如果要將WLC 5508用作錨點，並使用3850交換機和外部WLC（一種行動代理）連線到另一個行動控制器，則相同的設定是正確的。但是，無需在3850交換器從其獲得許可證的第二個行動控制器上設定WLAN。您只需將3850交換器指向用作錨點的5508 WLC。

WLC 上的組態

1. 在外部WLC上，使用AAA的AAA方法清單配置ISE伺服器，並將WLAN對映到MAC過濾器授權。錨點上不需要此操作。 **注意**：在錨點WLC和外部WLC上以及MAC過濾上配置重定向ACL。
2. 在WLC 5508 GUI中，選擇**WLANs > New**以設定錨點5508。填寫詳細資訊以啟用MAC過濾。



cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced

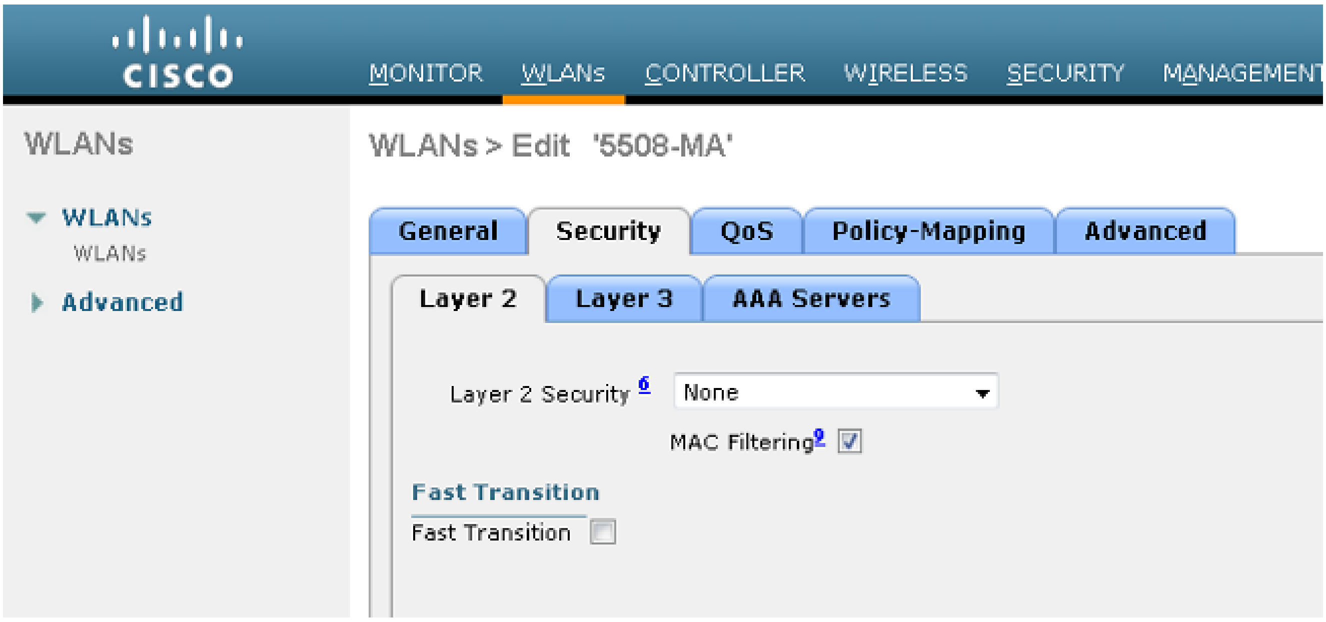
WLANs > Edit '5508-MA'

Profile Name: 5508-MA
Type: WLAN
SSID: 5508-MA
Status: ☑ Enabled

Security Policies: MAC Filtering
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): management
Multicast Vlan Feature: □ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: 5508-MC

3. 無需配置第2層選項。



WLANs > Edit '5508-MA'

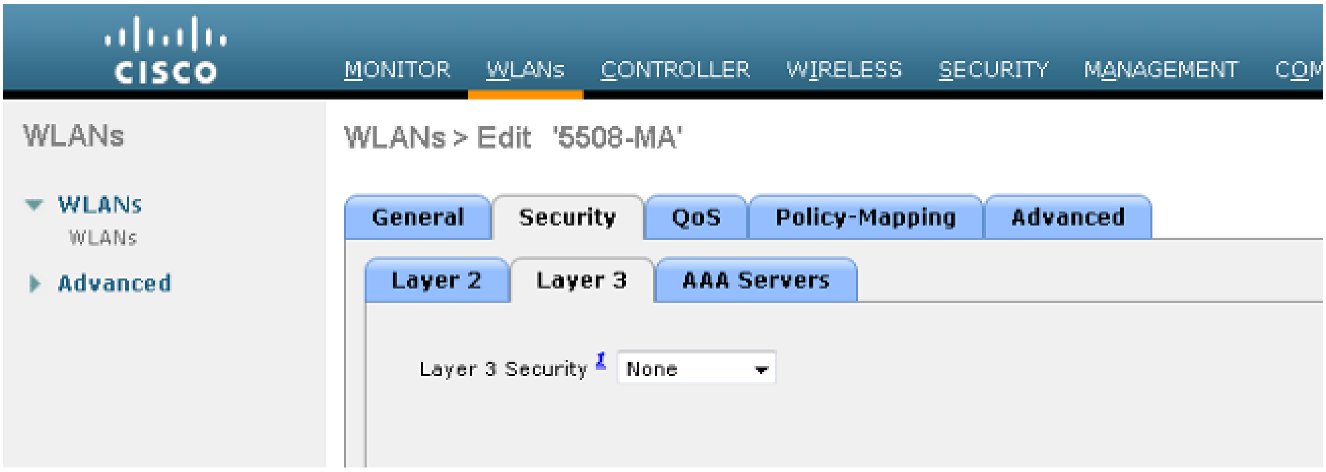
Layer 2 Security [6] None

MAC Filtering[9] ☑

Fast Transition

Fast Transition □

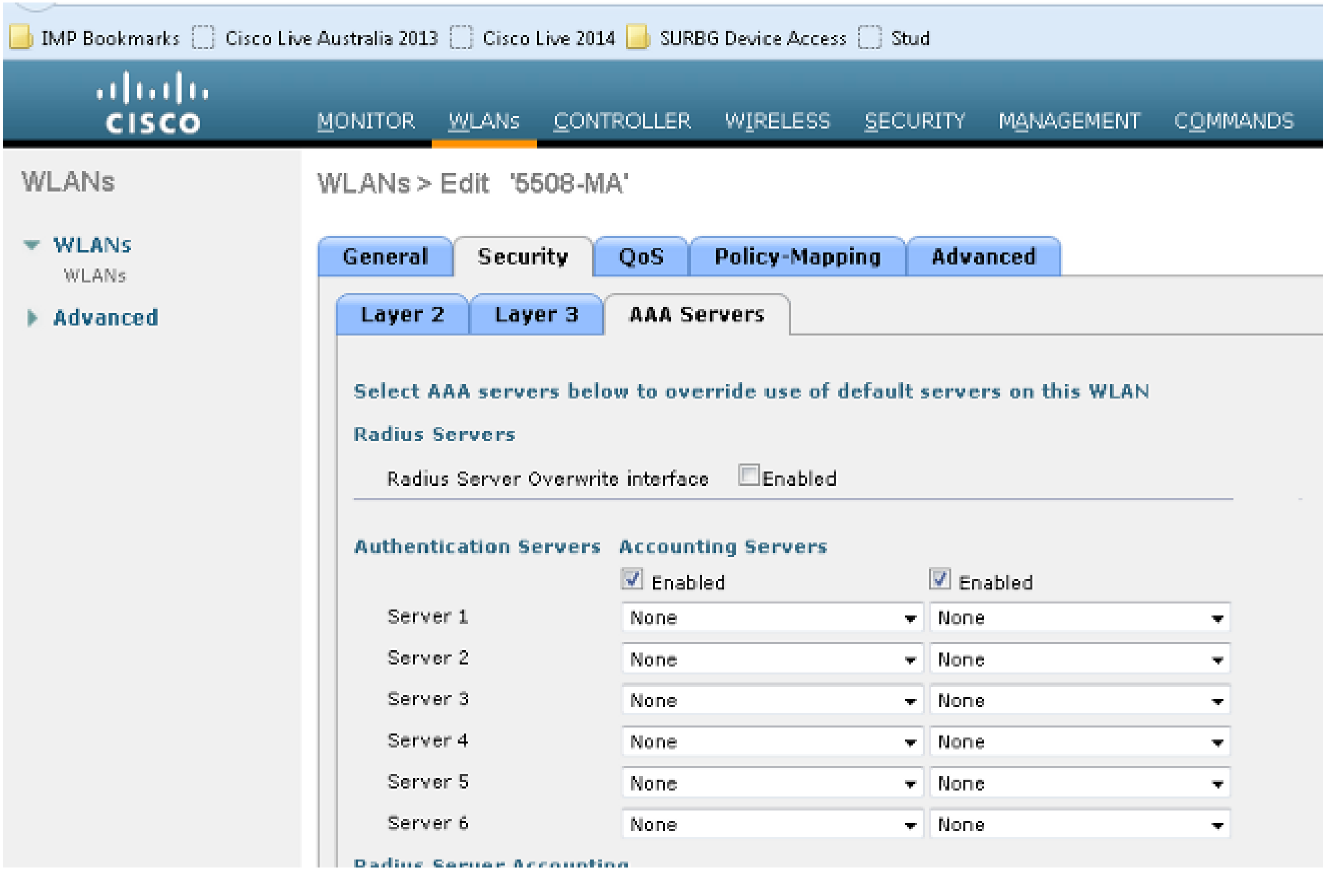
4. 無需配置第3層選項。



WLANs > Edit '5508-MA'

Layer 3 Security [1] None

5. 應該在Anchor AireOS WLC中禁用AAA伺服器，以便外部NGWC處理CoA。僅當在Security > AAA > RADIUS > Authentication下未配置RADIUS伺服器時，才能在錨點WLC中啟用AAA伺服器



WLANs > Edit '5508-MA'

Select AAA servers below to override use of default servers on this WLAN

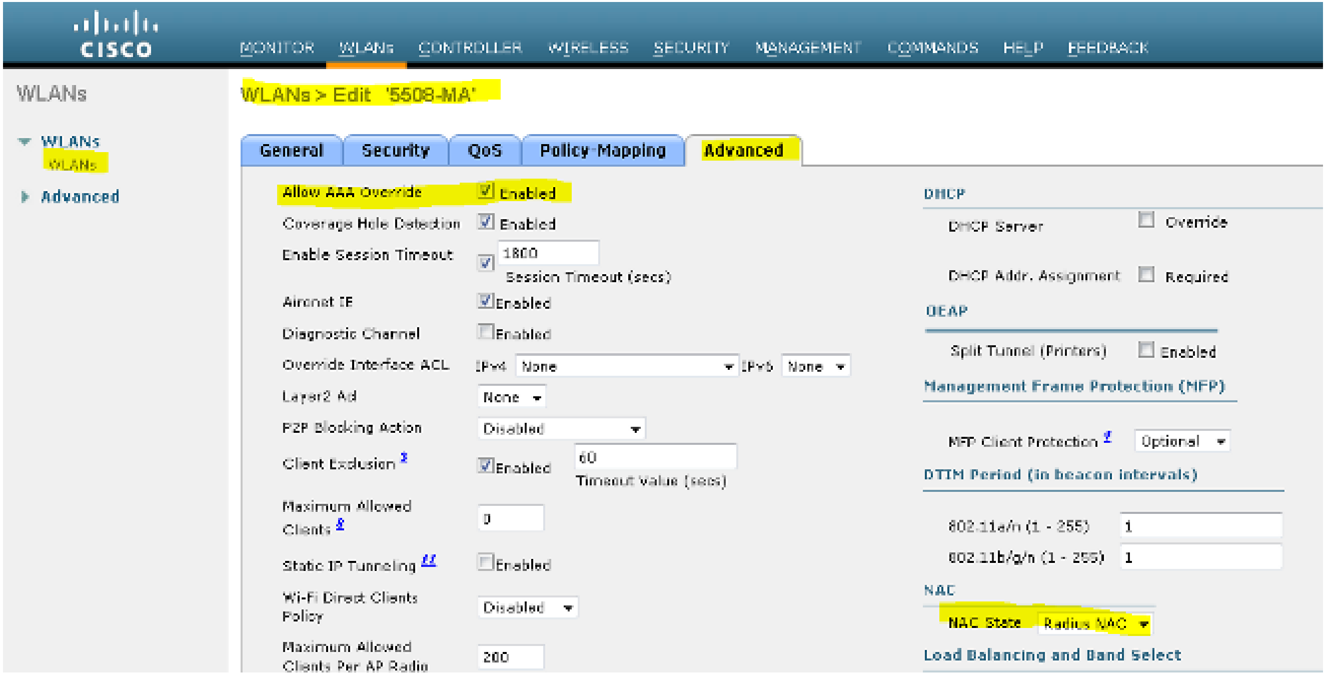
Radius Servers

Radius Server Overwrite interface □Enabled

Authentication Servers		Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

6. 選擇**WLANs > WLANs > Edit > Advanced**。選中**Allow AAA Override**覈取方塊。在NAC State下拉選單中，選擇**Radius NAC**。



WLANs > Edit '5508-MA'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑Enabled

Diagnostic Channel □Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion [3] ☑Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8] 0

Static IP Tunneling [11] □Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

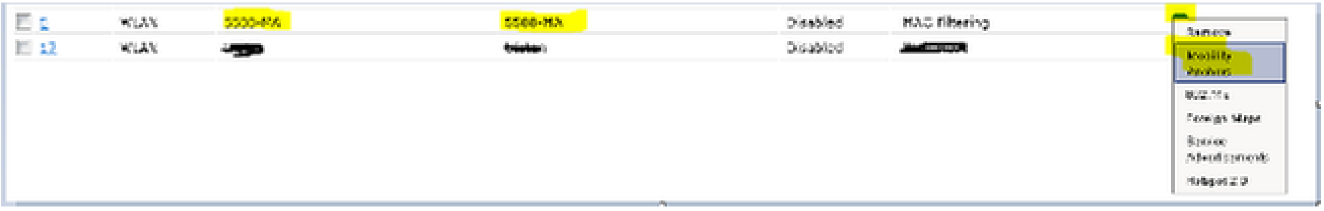
802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

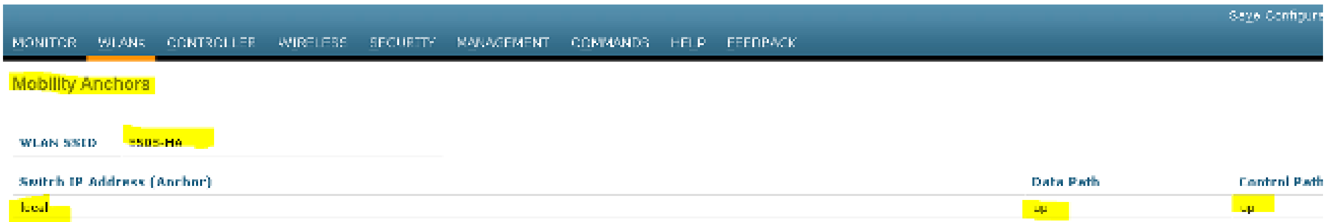
Load Balancing and Band Select

7. 將此錨點新增為WLAN的錨點。



□ 1	WLAN	5500-MA	5508-MA	Disabled	MAC filtering
□ 12	WLAN	[redacted]	[redacted]	Disabled	[redacted]

8. 將其指向本地後，應使用Control and Data Path UP/UP檢視此資訊。

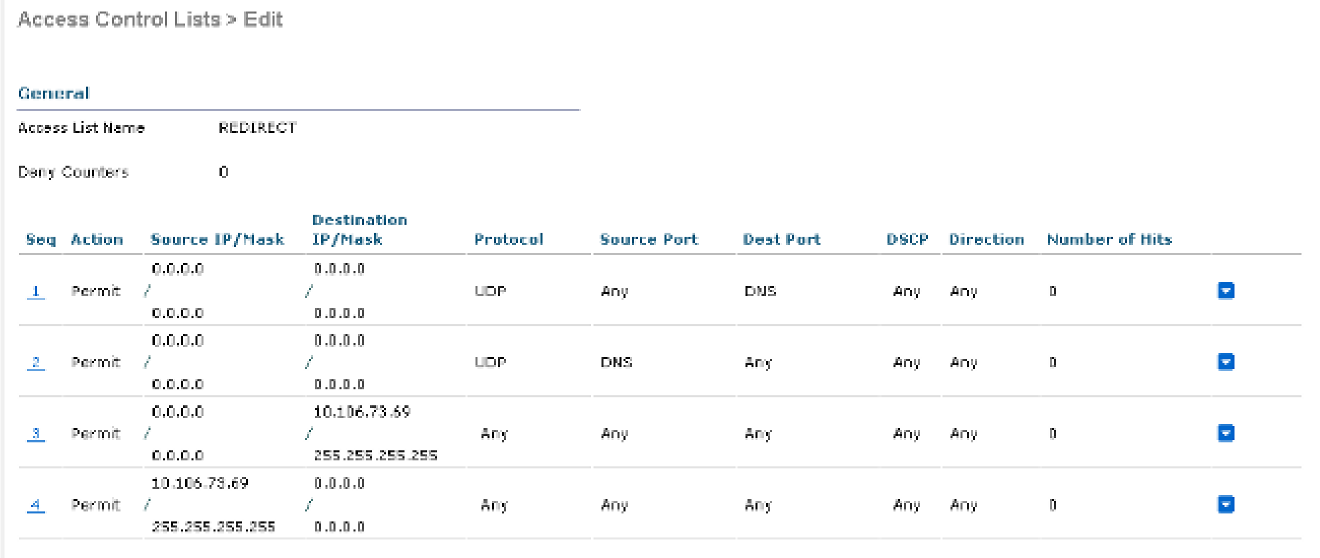


Mobility Anchors

WLAN SSID 5508-HA

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up

9. 在WLC上建立重新導向ACL。這將拒絕DHCP和DNS。它允許HTTP/HTTP。



Access Control Lists > Edit

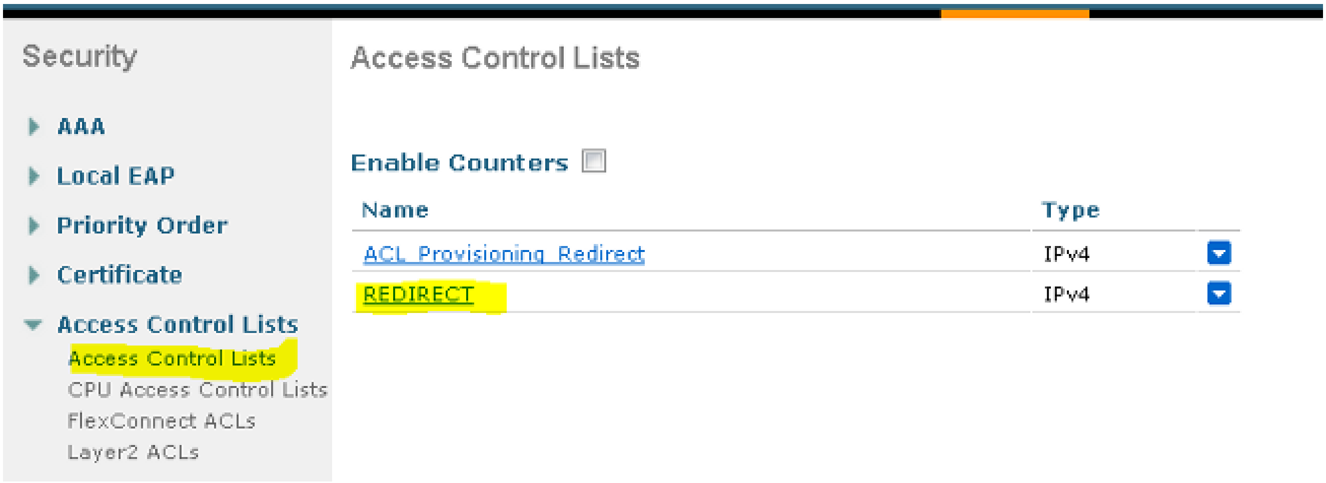
General

Access List Name REDIRECT

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0	▾
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0	▾
3	Permit	0.0.0.0 / 0.0.0.0	10.106.73.69 / 255.255.255.255	Any	Any	Any	Any	Any	0	▾
4	Permit	10.106.73.69 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	▾

這是建立ACL後的樣子。



Access Control Lists

Enable Counters □

Name	Type	
ACL_Provisioning_Redirect	IPv4	▾
REDIRECT	IPv4	▾

10. 在WLC 5760上定義ISE RADIUS伺服器。
11. 使用CLI配置RADIUS伺服器、伺服器組和方法清單。

```
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. 從CLI配置WLAN。

```
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. 將另一個WLC定義為此WLC上的行動成員。

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

註：如果將WLC 3850設定為外部，則請確保在行動控制器上定義交換器對等群組，而在行動控制器上定義交換器對等群組。然後在WLC 3850上配置以前的CWA配置。

14. 使用CLI設定重新導向ACL。 這是ISE作為AAA覆蓋返回的url-redirect-acl，以及訪客門戶重定向的重定向URL。它是當前在統一架構上使用的直接ACL。這是一個「punt」ACL，也就是通常用於統一架構的反向ACL。您需要阻止對DHCP、DHCP伺服器、DNS、DNS伺服器和ISE伺服器的訪問。根據需要僅允許www、443和8443。此ISE訪客門戶使用埠8443，重定向仍可使用此處顯示的ACL。此處啟用了ICMP，但根據安全規則，您可以拒絕或允許。

```
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
```

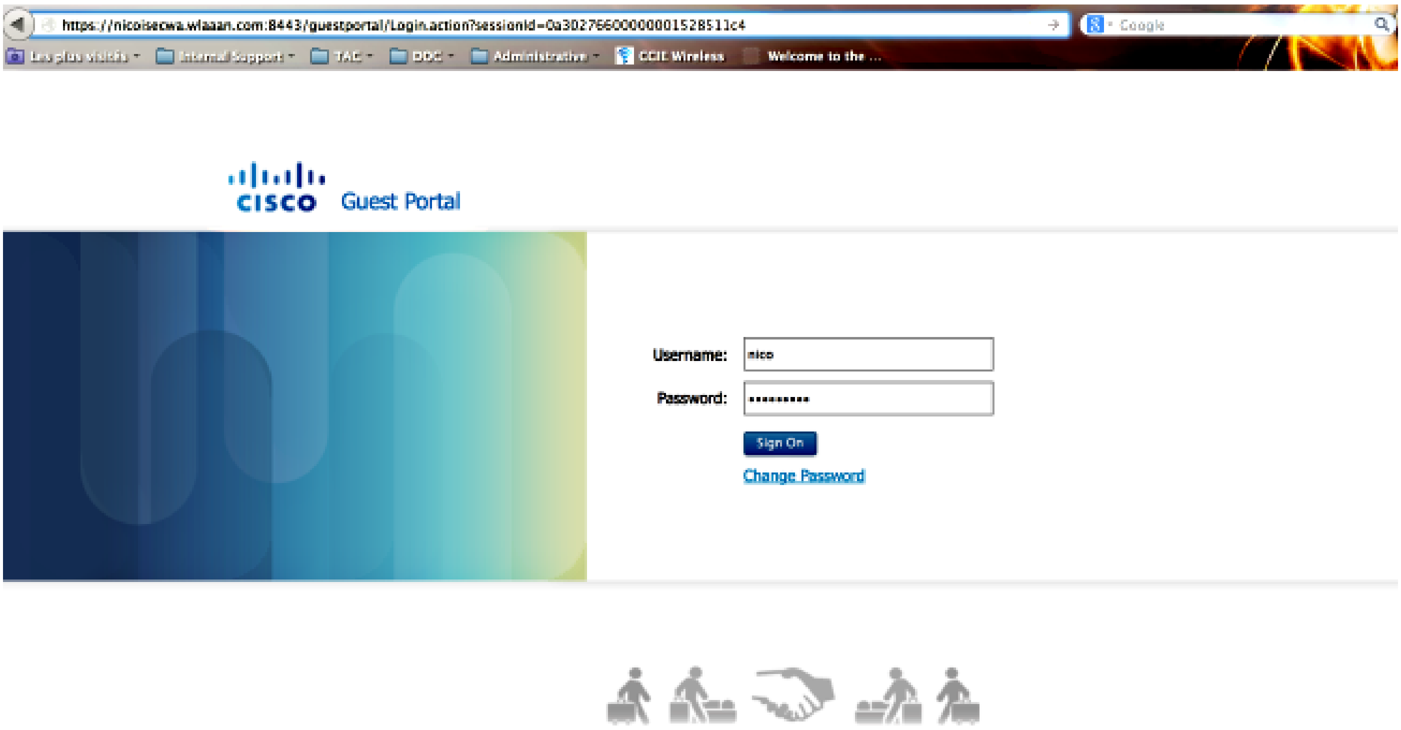
注意：啟用HTTPS時，由於可擴充性，可能會造成一些高CPU問題。除非思科設計團隊推薦此功能，否則請不要啟用它。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

將客戶端連線到配置的SSID。收到IP位址後，當使用者端進入Web auth Required狀態時，請開啟瀏覽器。在門戶中輸入您的客戶端憑據。

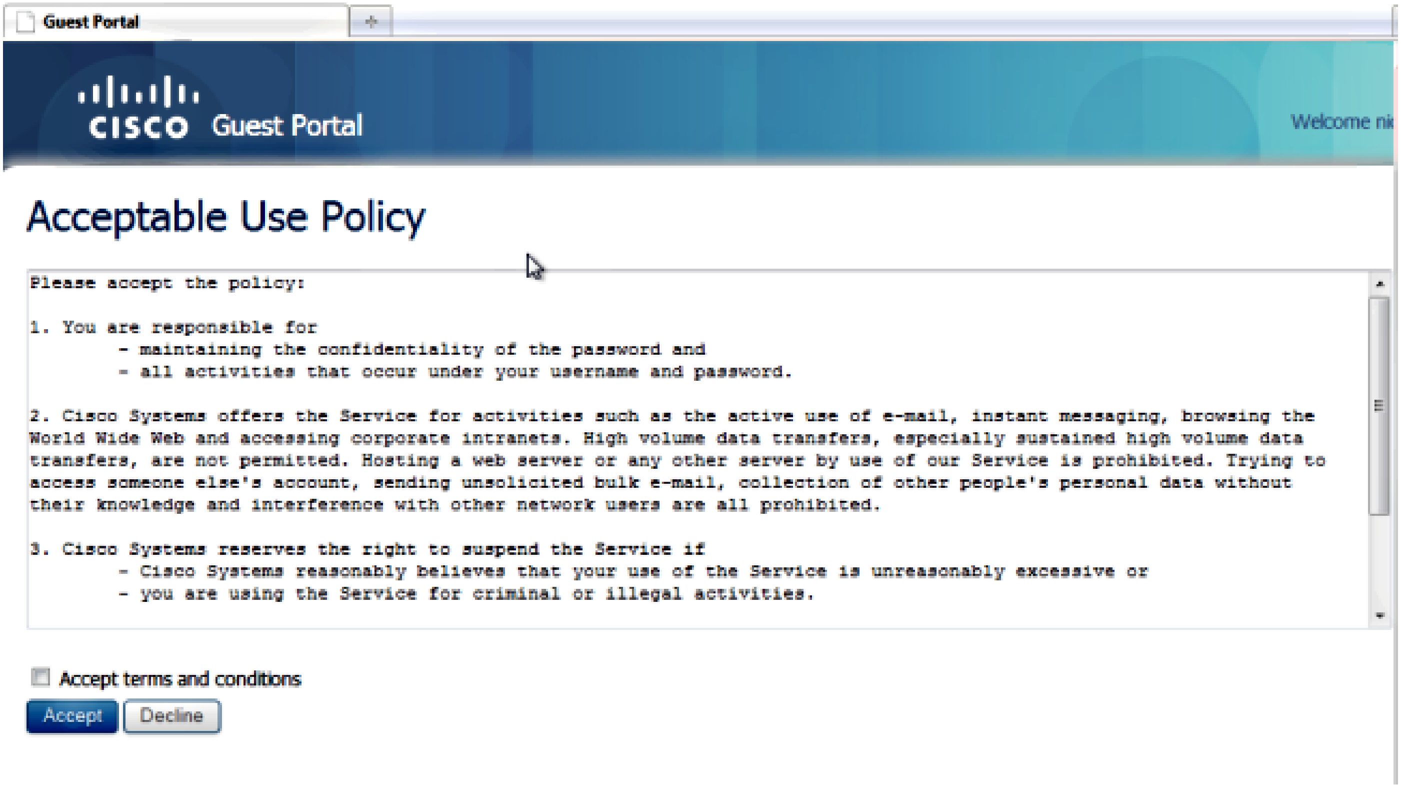


https://nicoisecwa.wlaaan.com:8443/guestportal/Login.action?sessionId=0a302766000000152851 1c4

Username: nico

Password: ••••••••••

身份驗證成功後，選中Accept terms and conditions覈取方塊。按一下「Accept」。

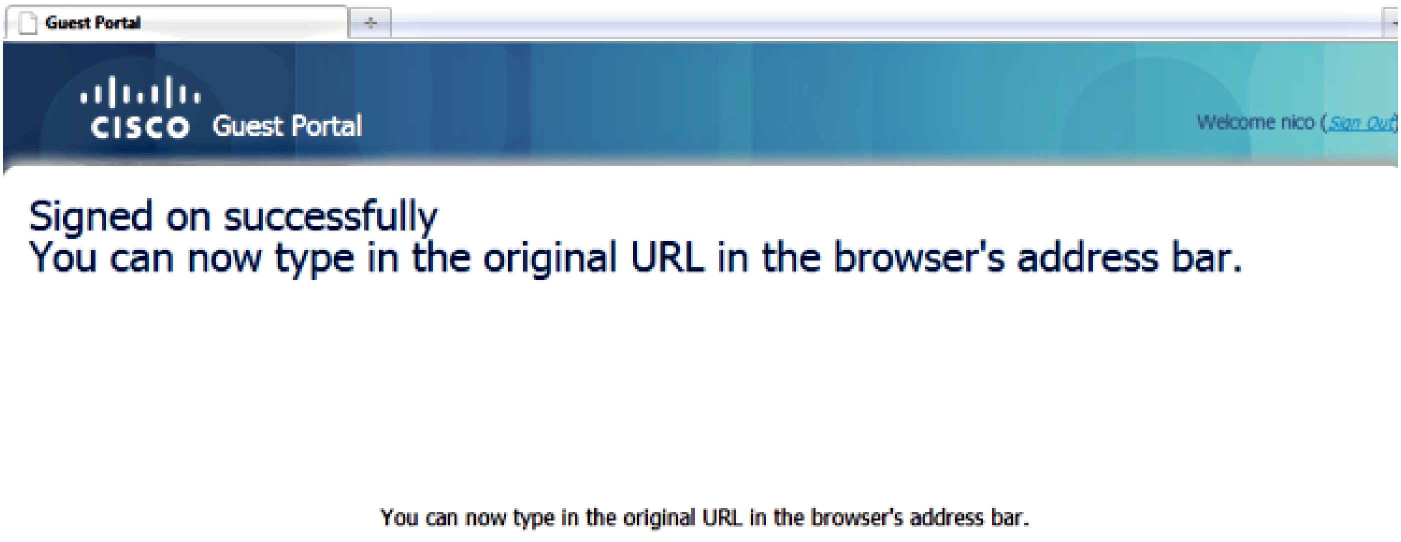


Acceptable Use Policy

```
Please accept the policy:

1. You are responsible for
        - maintaining the confidentiality of the password and
        - all activities that occur under your username and password.

2. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the
World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data
transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to
access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without
their knowledge and interference with other network users are all prohibited.

3. Cisco Systems reserves the right to suspend the Service if
        - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
        - you are using the Service for criminal or illegal activities.
```

□ Accept terms and conditions

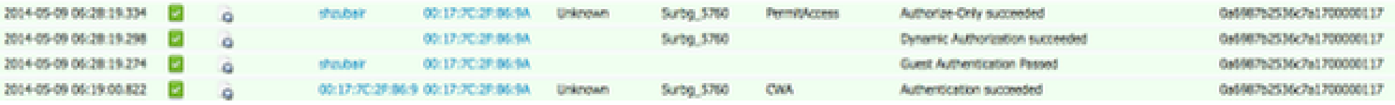
您將收到一條確認消息，現在將能夠瀏覽到Internet。



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

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

在ISE上，客戶端流如下所示：



2014-05-09 06:28:19.334	☑	🔍	shzubair	00:17:7C:2F:B6:9A	Unknown	Surbg_5760	PermitAccess	Authorize-Only succeeded	0a6987b2536c7a1700000117
2014-05-09 06:28:19.298	☑	🔍		00:17:7C:2F:B6:9A		Surbg_5760		Dynamic Authorization succeeded	0a6987b2536c7a1700000117
2014-05-09 06:28:19.274	☑	🔍	shzubair	00:17:7C:2F:B6:9A				Guest Authentication Passed	0a6987b2536c7a1700000117
2014-05-09 06:19:00.822	☑	🔍	00:17:7C:2F:B6:9	00:17:7C:2F:B6:9A	Unknown	Surbg_5760	CWA	Authentication succeeded	0a6987b2536c7a1700000117

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

在融合接入WLC上，建議運行跟蹤而不是調試。在Aironet OS 5508 WLC上，您只需輸入**debug client <client mac>**和**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
```

思科錯誤ID CSCun3834中包括Cisco IOS-XE和Aironet OS上的一些已知缺陷。

下面是成功的CWA流在跟蹤上的樣子：

```
[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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。