

# 融合接入和统一接入WLC上的集中式Web身份验证配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[拓扑 1](#)

[拓扑 2](#)

[拓扑 3](#)

[示例](#)

[拓扑1配置示例](#)

[ISE上的配置](#)

[WLC上的配置](#)

[拓扑2配置示例](#)

[ISE上的配置](#)

[WLC上的配置](#)

[拓扑3配置示例](#)

[ISE上的配置](#)

[WLC上的配置](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何在融合接入无线局域网控制器(WLC)上以及融合接入WLC和统一接入WLC ( 5760和5760和5508之间 ) 之间配置集中式Web身份验证。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco WLC 5508、5760、3850的基本知识
- 身份服务引擎(ISE)基础知识
- 无线移动性的基础知识
- 访客锚定的基础知识

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS® XE 3.3.3版的WLC 5760
- 运行Cisco Aironet OS版本7.6的WLC 5508
- 运行Cisco IOS XE版本3.3.3的交换机3850
- 运行版本1.2的思科ISE

## 配置

**注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。**

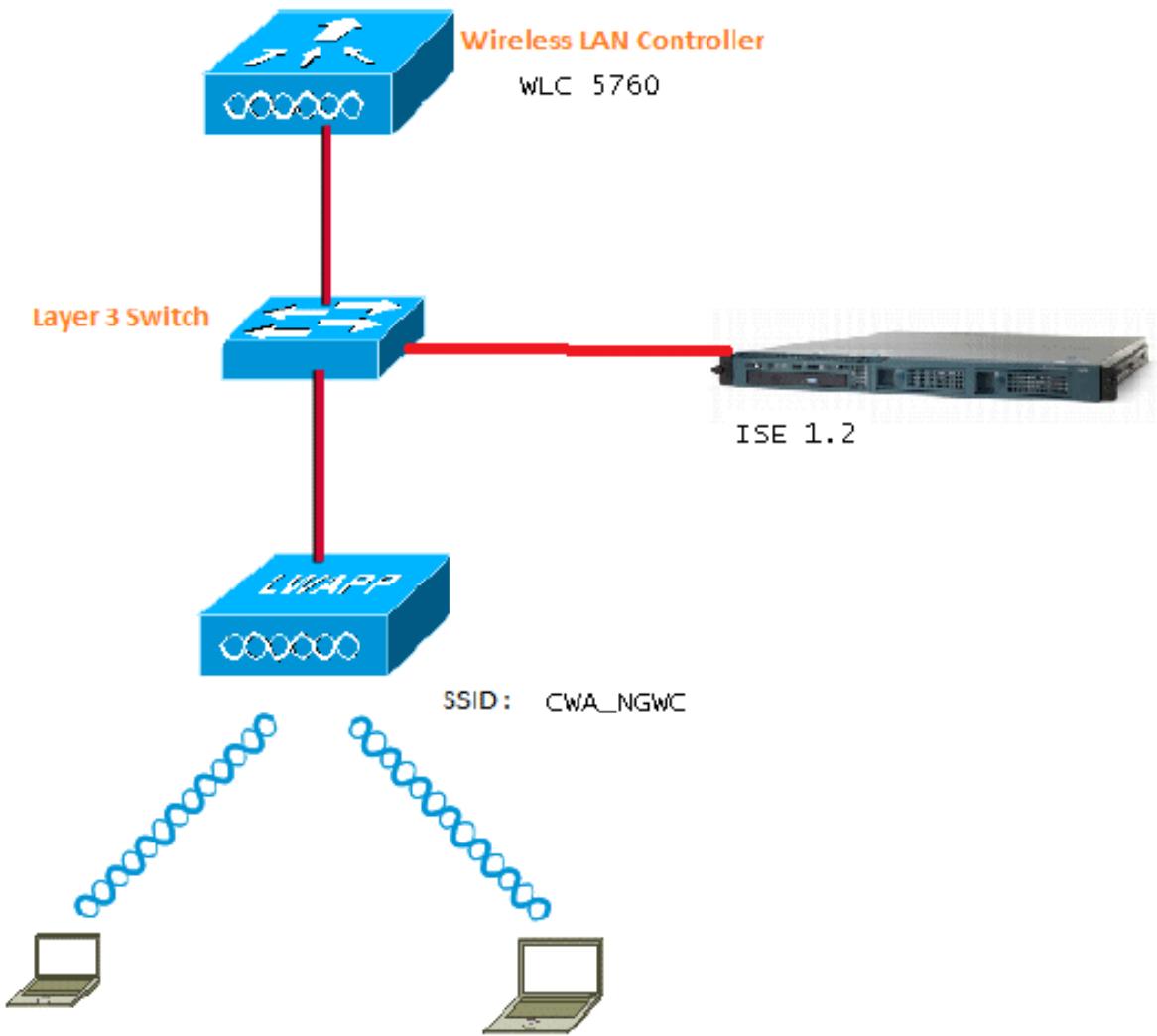
该流程包括以下步骤：

1. 用户与Web身份验证服务集标识符(SSID)关联，SSID实际上是开放式+macfiltering且无第3层安全性。
2. 用户打开浏览器。
3. WLC重定向到访客门户。
4. 用户在门户上进行身份验证。
5. ISE发送RADIUS授权更改（CoA - UDP端口1700）以向控制器指示用户有效，并最终推送RADIUS属性，例如访问控制列表(ACL)。
6. 系统将提示用户重试原始URL。

思科使用三种不同的部署设置，涵盖所有不同的场景，以实现集中式Web身份验证(CWA)。

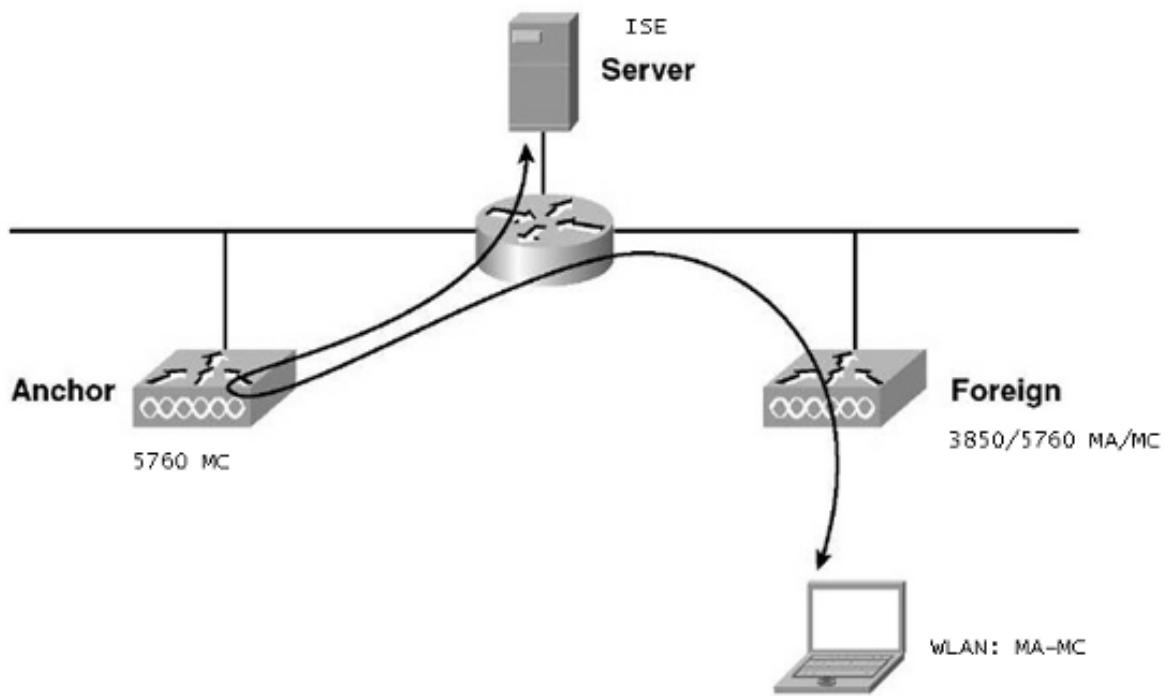
## 拓扑 1

5760 WLC充当独立WLC，接入点终止于同一5760 WLC。客户端连接到无线局域网(WLAN)，并向ISE进行身份验证。



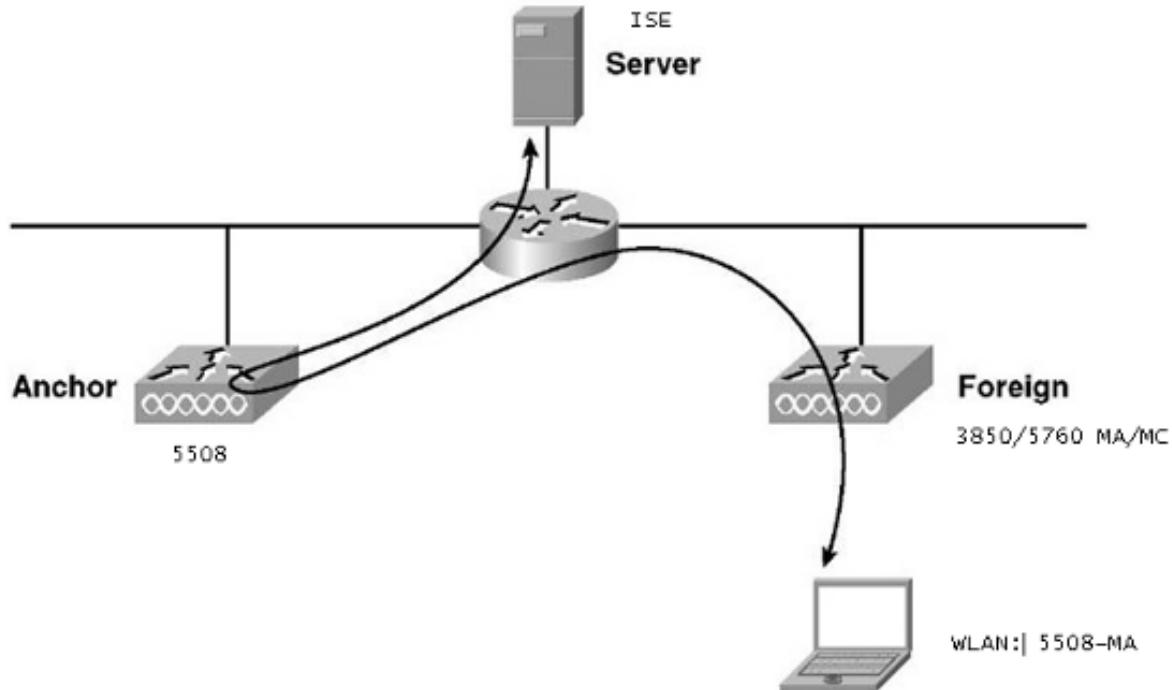
## 拓扑 2

访客锚定在融合接入WLC之间，一个充当移动控制器，另一个充当移动代理。移动代理是外部WLC，移动控制器是锚点。



### 拓扑 3

访客锚定在Cisco Unified WLC 5508和融合接入WLC 5760/3850之间，一个用作移动控制器，另一个用作移动代理。移动代理/移动控制器是外部WLC，5508移动控制器是锚点。



**注：**在许多部署中，锚点是移动控制器，外部WLC是移动代理，从另一个移动控制器获取许可证。在这种情况下，外部WLC只有一个锚点，该锚点是推送策略的锚点。不支持双锚定，并且不起作用，因为预计不会这样工作。

## 示例

WLC 5508充当锚点，WLC 5760充当充当Mobility Agent的3850交换机的移动控制器。对于锚点外部WLAN，WLC 5508将成为3850外部WLAN的锚点。根本无需在WLC 5760上配置该WLAN。如果将3850交换机指向5760锚点，然后从此WLC 5760到WLC 5508作为双锚点，它将不起作用，因为这会变成双锚点，并且策略位于5508锚点上。

如果您的设置包括作为锚点的WLC 5508、作为移动控制器的WLC 5760，以及作为移动代理和外部WLC的3850交换机，则3850交换机的锚点在任何时间都将是WLC 5760或WLC 5508。它不能同时为和，并且双锚点不起作用。

## 拓扑1配置示例

有关网络图和说明，请参阅[拓扑1](#)。

配置过程分为两步：

1. ISE上的配置。
2. WLC上的配置。

WLC 5760充当独立WLC，用户通过ISE进行身份验证。

## ISE上的配置

- 选择ISE GUI > Administration > Network Resource > Network Devices List > Add，以便在ISE上添加WLC作为身份验证、授权和记帐(AAA)客户端。确保您在WLC上输入与RADIUS服务器上添加的共享密钥。**注意**：在部署Anchor-Foreign时，只需添加外部WLC。无需在ISE上添加锚点WLC作为AAA客户端。本文档中的所有其他部署方案都使用相同的ISE配置。

Network Devices List > [Surbg\\_5760](#)

### Network Devices

\* Name

Description

\* IP Address:  /

Model Name

Software Version

\* Network Device Group

Location

Device Type

▾ Authentication Settings

Enable Authentication Settings

Protocol	<b>RADIUS</b>
* Shared Secret	<input type="text" value="*****"/> <input type="button" value="Show"/>
Enable KeyWrap	<input type="checkbox"/> <input type="button" value="i"/>
* Key Encryption Key	<input type="text"/> <input type="button" value="Show"/>
* Message Authenticator Code Key	<input type="text"/> <input type="button" value="Show"/>
Key Input Format <input type="radio"/> ASCII <input type="radio"/> HEXADECIMAL	

▾ SNMP Settings

▾ Advanced TrustSec Settings

- 在ISE GUI中，选择Policy > Authentication > MAB > Edit以创建身份验证策略。身份验证策略接受客户端的MAC地址，该地址指向内部终端。在“选项”列表中选择以下选项：从If authentication failed下拉列表中，选择Reject。从If user not found下拉列表中，选择Continue。从If process failed下拉列表中，选择Drop。当您使用这些选项进行配置时，未通过MAC授权的客户端会继续进行访客门户。

3. 从ISE GUI中，选择Policy > Authorization > Results > Authorization Profiles > Add。填写详细信息并单击Save以创建授权配置文件。此配置文件帮助客户端在MAC身份验证后重定向到重定向URL，客户端在其中输入访客用户名/密码。

Select an Item	=		-	+
----------------	---	--	---	---

4. 在ISE GUI中，选择Policy > Authorization > Results > Authorization Profiles > Add以创建另一个授权配置文件，从而允许使用正确凭证访问用户。

Authorization Profiles > PermitAccess

**Authorization Profile**

- \* Name: PermitAccess
- Description: Default Profile with access type as Access-Accept
- \* Access Type: ACCESS\_ACCEPT
- Service Template:

Common Tasks

Advanced Attributes Settings

Attributes Details

Access Type = ACCESS\_ACCEPT

Save    Reset

5. 创建授权策略。授权策略“Guest\_Wireless”将重定向URL和重定向ACL推送到客户端会话。此处推送的配置文件是之前所示的CWA。授权策略“Guest\_Wireless-Success”允许通过访客门户成功进行身份验证的访客用户具有完全访问权限。在访客门户上成功对用户进行身份验证后，WLC将发送动态授权。这将使用“Network Access:Use EQUALS Guest Flow”属性重新验证客户端会话。最终授权策略如下所示

Guest_Wireless_Success	If: Guest AND Network Access:UseCase EQUALS Guest Flow	then: PermitAccess	Edit   ▾
Guest_Wireless	If: Wireless_MAC	then: OVA	Edit   ▾

Save    Reset

6. 可选：在这种情况下，使用默认的多门户配置。根据要求，可以在GUI中更改相同内容。从ISE GUI中，选择Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal。

CISCO Identity Services Engine

Home Operations | Policy | Administration |

System Identity Management Network Resources Web Portal Management Feed Service

Sponsor Group Policy Sponsor Groups Settings

Multi-Portal Configuration List > DefaultGuestPortal

**Multi-Portal**

General Operations Customization Authentication

**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

Settings

- General
- Sponsor
- My Devices
- Guest
  - Details Policy
  - Guest Roles Configuration
  - Language Template
  - Multi-Portal Configurations
    - CWA
    - DefaultGuestPortal
    - DRW
    - Portal Policy
    - Password Policy
  - Time Profiles

创建Guest\_Portal\_sequence，允许内部、访客和AD用户。

**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

Available Actions: > < >> <<

Selected Actions: <<< <<<

▼ 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

Save Reset

7. 从ISE GUI中，选择Guest > Multi-Portal Configurations > DefaultGuestPortal。从Identity Store Sequence下拉列表中，选择Guest\_Portal\_Sequence。

## WLC上的配置

1. 在WLC 5760上定义ISE Radius服务器。
2. 使用CLI配置RADIUS服务器、服务器组和方法列表。

```
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配置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配置重定向ACL。这是ISE作为AAA覆盖返回的url-redirect-acl以及访客门户重定向的重定向URL。它是当前在统一架构上使用的直接ACL。这是一个“punt”ACL，通常用于统一架构的反向ACL。您需要阻止对DHCP、DHCP服务器、DNS、DNS服务器和ISE服务器的访问。根据需要仅允许www、443和8443。此ISE访客门户使用端口8443，并且重定向仍可使用此处显示的ACL。这里启用了ICMP，但是您可以根据安全规则拒绝或允许。

```

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

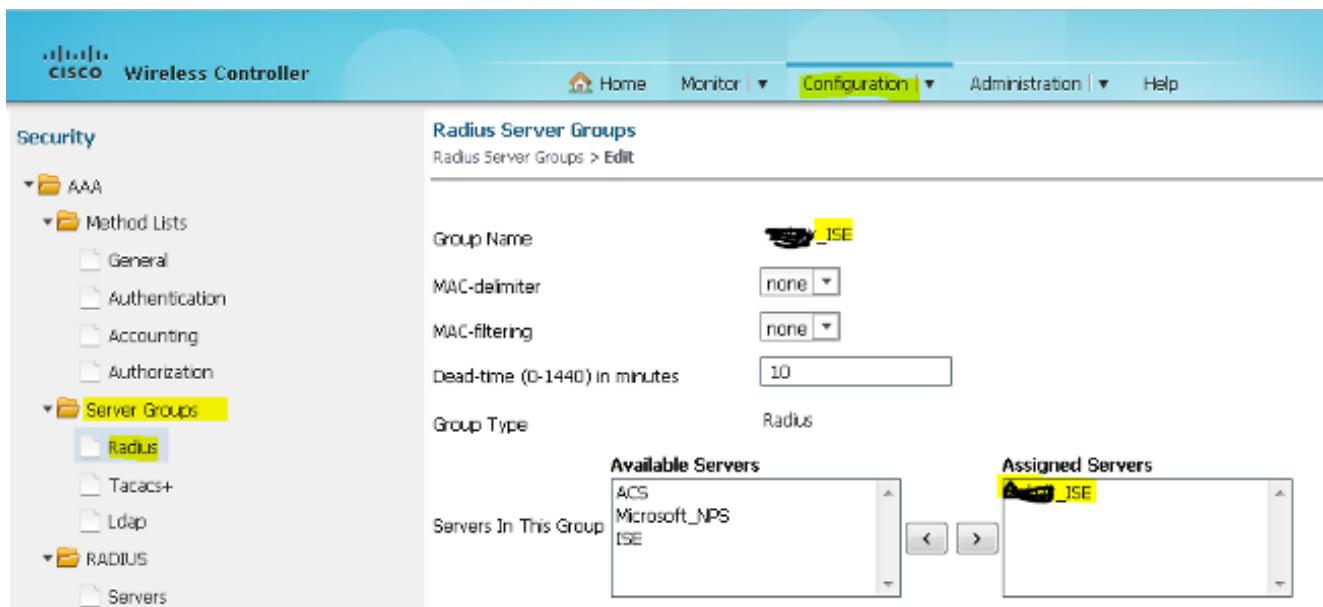
```

**注意：**启用HTTPS时，由于可扩展性，可能导致一些高CPU问题。除非思科设计团队推荐此服务，否则请勿启用此服务。

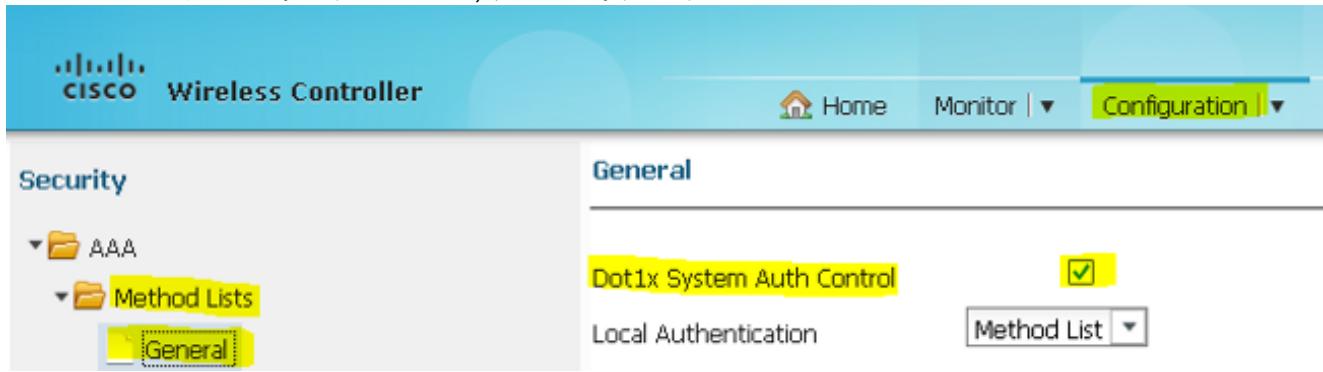
5. 从无线控制器GUI中，选择**AAA > RADIUS > Servers**。在GUI中配置RADIUS服务器、服务器组和方法列表。填写所有参数并确保此处配置的共享密钥与ISE上为此设备配置的密钥匹配。从Support for RFC 3576下拉列表中，选择**Enable**。

Radius Servers	
Radius Servers > Edit	
Server Name	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

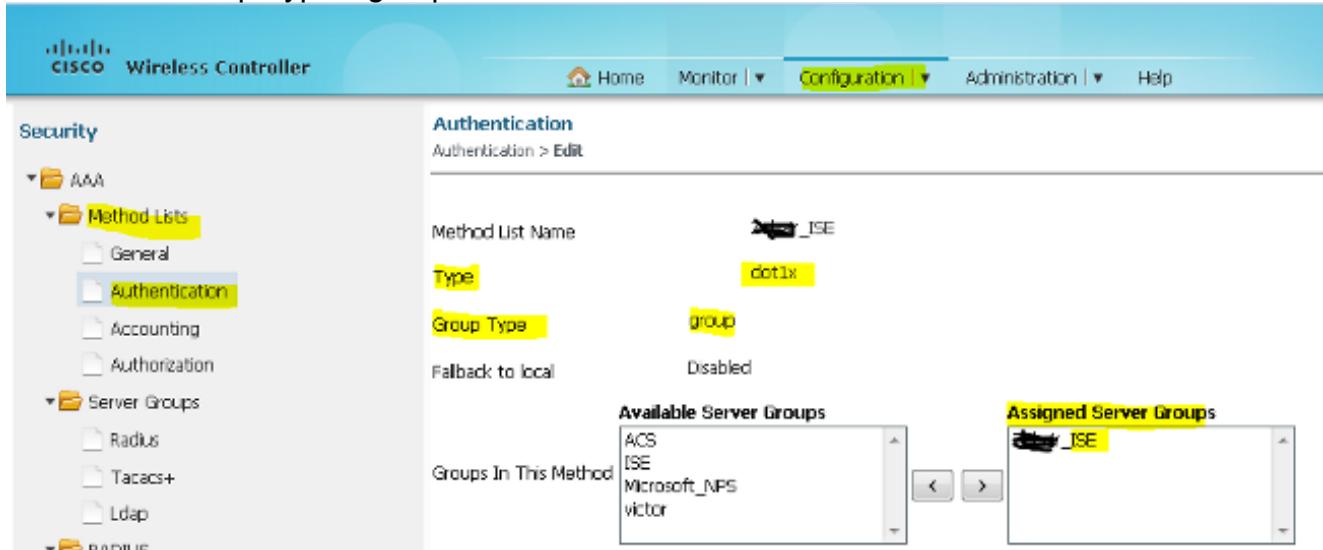
6. 从无线控制器GUI中，选择**AAA > Server Groups > Radius**。将之前创建的RADIUS服务器添加到服务器组。



7. 从无线控制器GUI中，选择AAA > Method Lists > General。选中Dot1x System Auth Control复选框。如果禁用此选项，则AAA不起作用。



8. 从无线控制器GUI中，选择AAA > Method Lists > Authentication。为dot1X类型创建身份验证方法列表。Group Type为group。将其映射到ISE。



9. 从无线控制器GUI中，选择AAA > Method Lists > Accounting。为类型标识创建记帐方法列表。将其映射到ISE。

**Accounting**  
Accounting > Edit

Method List Name: **ISE**

Type: identity

Available Server Groups:

- ACS
- ISE
- Microsoft\_NPS
- victor

Assigned Server Groups:

- ISE

10. 从无线控制器GUI中，选择AAA > Method Lists > Authorization。为Type网络创建授权方法列表。将其映射到ISE。

**Authorization**  
Authorization > Edit

Method List Name: **ISE**

Type: network

Group Type: group

Available Server Groups:

- ACS
- ISE
- Microsoft\_NPS
- victor

Assigned Server Groups:

- ISE

11. 可选，因为也有MAC故障支持。为类型网络创建授权方法列表MACFILTER。将其映射到ISE。

**Authorization**  
Authorization > Edit

Method List Name: **MACFILTER**

Type: network

Group Type: group

Available Server Groups:

- ACS
- ISE
- Microsoft\_NPS
- victor

Assigned Server Groups:

- ISE

12. 从无线控制器GUI中，选择WLAN > WLANs。使用此处显示的参数创建新配置。

The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'WLAN' is expanded, and 'WLANS' is selected. On the right, the 'WLAN' configuration page is displayed with the 'General' tab selected. The configuration includes:

- Profile Name: CWA\_NGWC
- Type: WLAN
- SSID: CWA\_NGWC
- Status: Enabled (checkbox checked)
- Security Policies: MAC Filtering (checkbox checked)
- Radio Policy: AI
- Interface/Interface Group(G): VLAN0012
- Broadcast SSID: checked
- Multicast VLAN Feature: unchecked

13. 选择Security > Layer2。在MAC Filtering字段中，输入MACFILTER。

The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'WLAN' is expanded, and 'WLANS' is selected. On the right, the 'WLAN' configuration page is displayed with the 'Security' tab selected. The configuration includes:

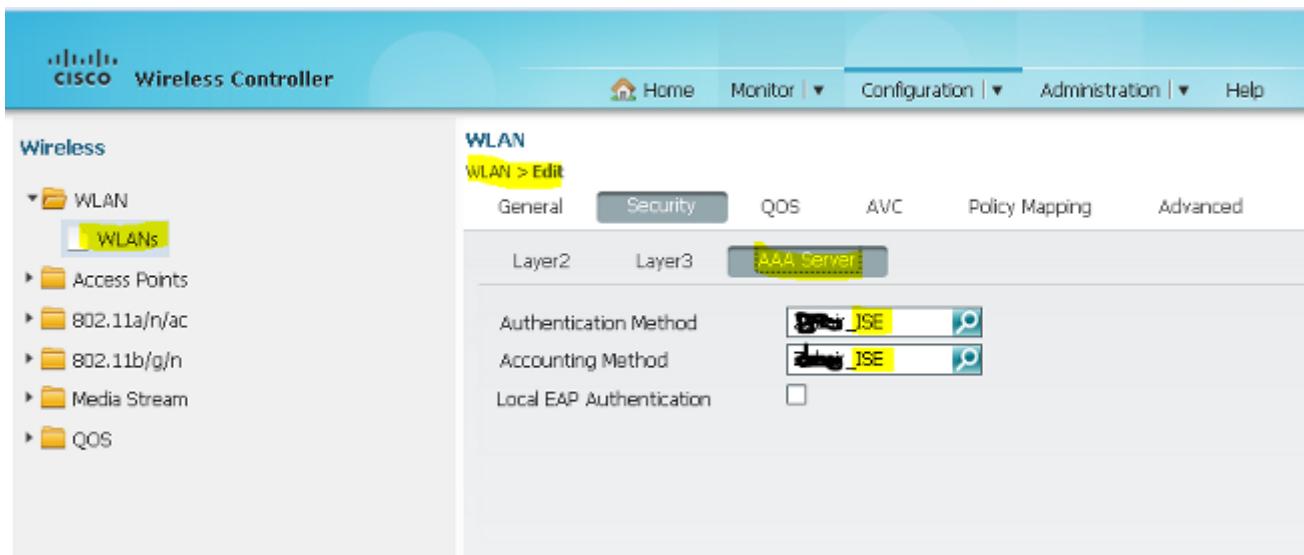
- Layer 2 Security: None
- MAC Filtering: MACFILTER (highlighted in yellow)
- Fast Transition: unchecked
- Over the DS: checked
- Reassociation Timeout: 20

14. 无需配置第3层。

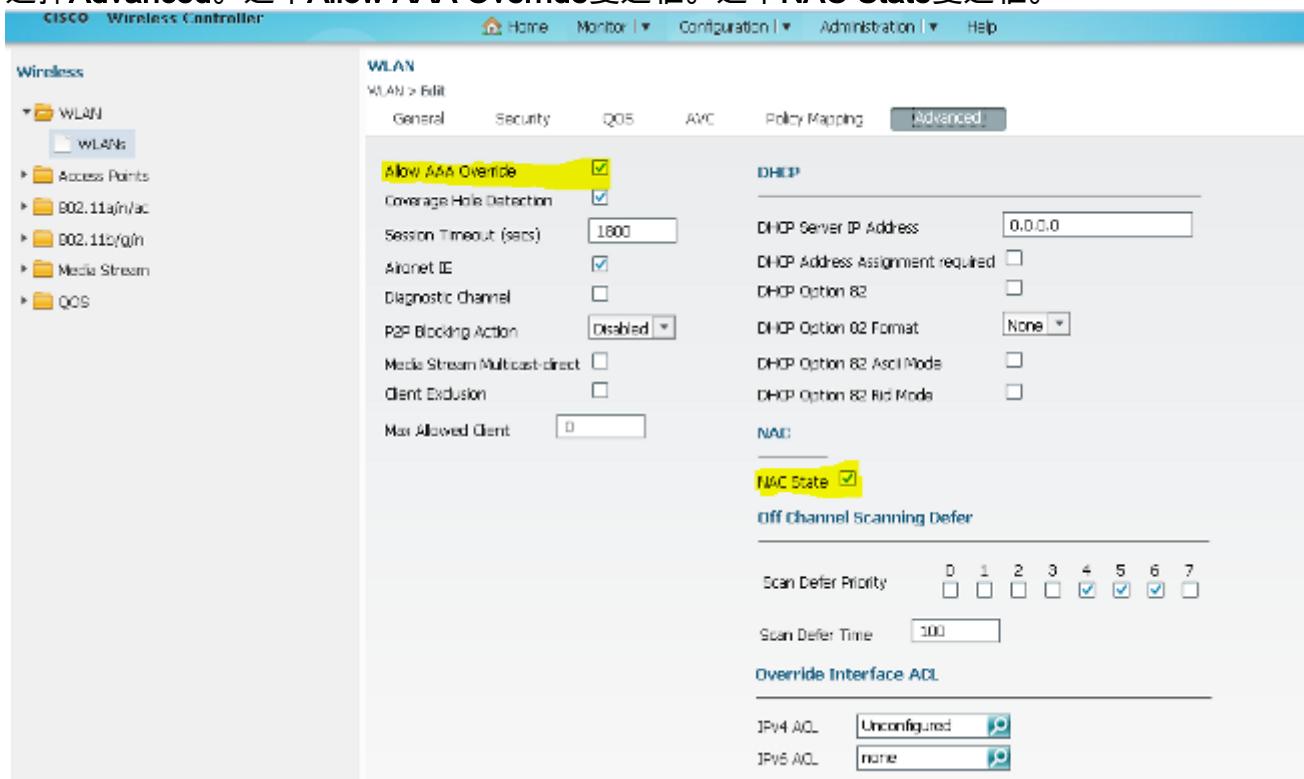
The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'WLAN' is expanded, and 'WLANS' is selected. On the right, the 'WLAN' configuration page is displayed with the 'Layer3' tab selected. The configuration includes:

- Web Policy: unchecked
- Conditional Web Redirect: unchecked
- Webauth Authentication List: Disabled
- Webauth Parameter Map: Unconfigured
- Webauth On-mac-filter Failure: unchecked
- Preattentiation IPv4 ACL: Unconfigured
- Preattentiation IPv6 ACL: none

15. 选择Security > AAA Server。从Authentication Method下拉列表中，选择ISE。从Accounting Method下拉列表中，选择ISE。



16. 选择Advanced。选中Allow AAA Override复选框。选中NAC State复选框。



17. 在GUI中的WLC上配置重定向ACL。

**Access Control Lists**  
ACLs > ACL detail

**Details :**

Name: **REDIRECT**  
Type: **IPv4 Extended**

Add Sequence	Remove								
<input type="checkbox"/>	Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP	
<input type="checkbox"/>	3	deny	icmp	any	any	-	-	-	
<input type="checkbox"/>	5	deny	udp	any	any	-	eq 67	-	
<input type="checkbox"/>	6	deny	udp	any	any	-	eq 68	-	
<input type="checkbox"/>	10	deny	udp	any	any	-	eq 53	-	
<input type="checkbox"/>	20	deny	ip	any	10.105.73.69	-	-	-	
<input type="checkbox"/>	30	permit	tcp	any	any	-	eq 80	-	
<input type="checkbox"/>	40	permit	tcp	any	any	-	eq 443	-	

有关网络图和说明，请参阅[拓扑2](#)。

此配置也是分两步进行的。

## ISE上的配置

ISE的配置与拓扑1的配置相同。

无需在ISE上添加锚点控制器。您只需要在ISE上添加外部WLC，在外部WLC上定义RADIUS服务器，并在WLAN下映射授权策略。在锚点上，您只需启用MAC过滤。

在此配置示例中，有两个用作外部锚点的WLC 5760。如果您要将WLC 5760用作锚点，将3850交换机用作另一个移动控制器的锚点外部（即移动代理），则相同的配置是正确的。但是，无需在3850交换机从中获取许可证的第二个移动控制器上配置WLAN。您只需将3850交换机指向用作锚点的WLC 5760。

## WLC上的配置

1. 在外部，使用AAA的AAA方法列表配置ISE服务器，并将WLAN映射到MAC过滤器授权。**注意**：在锚点(Anchor)和外部(Foreign)以及MAC过滤上配置重定向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配置重定向ACL。这是ISE作为AAA覆盖返回的url-redirect-acl以及访客门户重定向的重定向URL。它是当前在统一架构上使用的直接ACL。这是一个“punt”ACL，通常用于统一架构的反向ACL。您需要阻止对DHCP、DHCP服务器、DNS、DNS服务器和ISE服务器的访问。根据需要仅允许www、443和8443。此ISE访客门户使用端口8443，并且重定向仍可使用此处显示的ACL。这里启用了ICMP，但是您可以根据安全规则拒绝或允许。

```
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：**启用HTTPS时，由于可扩展性，可能导致一些高CPU问题。除非思科设计团队推荐此服务，否则请勿启用此服务。

3. 在锚点上配置移动性。

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

**注：**如果将3850交换机配置为外部，则请确保在移动控制器上定义交换机对等组，在移动控制器上定义交换机对等组。然后在3850交换机上配置上述CWA配置。

4. 锚点上的配置。在锚点上，无需配置任何ISE配置。您只需要WLAN配置。

```
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. 在锚点上配置移动性。将另一个WLC定义为此WLC上的移动成员。

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

6. 使用CLI配置重定向ACL。这是ISE作为AAA覆盖返回的url-redirect-acl以及访客门户重定向的重定向URL。它是当前在统一架构上使用的直接ACL。这是一个“punt”ACL，通常用于统一架构的反向ACL。您需要阻止对DHCP、DHCP服务器、DNS、DNS服务器和ISE服务器的访问。根据需要仅允许www、443和8443。此ISE访客门户使用端口8443，并且重定向仍可使用此处显示的ACL。这里启用了ICMP，但是您可以根据安全规则拒绝或允许。

```
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：**启用HTTPS时，由于可扩展性，可能导致一些高CPU问题。除非思科设计团队推荐此服务，否则请勿启用此服务。

## 拓扑3配置示例

有关网络图和说明，请参阅[拓扑3](#)。

此过程也分为两步。

## ISE上的配置

ISE的配置与拓扑1的配置相同。

无需在ISE上添加锚点控制器。您只需要在ISE上添加外部WLC，在外部WLC上定义RADIUS服务器，并在WLAN下映射授权策略。在锚点上，您只需启用MAC过滤。

在本示例中，有一个用作锚点的WLC 5508和一个用作外部WLC的WLC 5760。如果要将WLC 5508用作锚点，并将3850交换机和外部WLC（移动代理）用于另一个移动控制器，则相同配置是正确的。但是，无需在3850交换机从中获取许可证的第二个移动控制器上配置WLAN。您只需将3850交换机指向用作锚点的5508 WLC。

## WLC上的配置

1. 在外部WLC上，使用AAA的AAA方法列表配置ISE服务器，并将WLAN映射到MAC过滤器授权。锚点上不需要此项。**注意**：在锚点WLC和外部WLC上以及MAC过滤上配置重定向ACL。
2. 从WLC 5508 GUI中，选择WLANs > New以配置锚点5508。填写详细信息以启用MAC过滤。

The screenshot shows the Cisco Wireless LAN Controller (WLC) 5508 GUI. The top navigation bar includes MONITOR, WLANs (which is highlighted), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. Below the navigation bar, the left sidebar shows a tree structure with WLANS expanded, and WLANs selected. The main content area is titled "WLANs > Edit '5508-MA'". The configuration tabs at the top are General, Security (highlighted in yellow), QoS, Policy-Mapping, and Advanced. The General tab displays the following settings:

- Profile Name: 5508-MA
- Type: WLAN
- SSID: 5508-MA
- Status: Enabled (checkbox checked)

Under the Security tab, the "Security Policies" section is set to "MAC Filtering". A note below states: "(Modifications done under security tab will appear after applying the changes.)". Other security policy options include Radio Policy (set to All), Interface/Interface Group(G) (set to management), Multicast Vlan Feature (checkbox unchecked), Broadcast SSID (checkbox checked), and NAS-ID (set to 5508-MC). The Advanced tab is also visible at the bottom.

3. 无需配置第2层选项。

The screenshot shows the Cisco AireOS Web Interface. The top navigation bar includes MONITOR, WLANs (highlighted in orange), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COM. The left sidebar under WLANs has options for WLANS (selected) and Advanced. The main content area is titled 'WLANs > Edit '5508-MA''. It features tabs for General, Security, QoS, Policy-Mapping, and Advanced, with Policy-Mapping selected. Within Policy-Mapping, there are sub-tabs for Layer 2, Layer 3 (selected), and AAA Servers. Under Layer 3, the 'Layer 3 Security' dropdown is set to 'None'. Below it, the 'MAC Filtering' checkbox is checked. A 'Fast Transition' section contains a 'Fast Transition' checkbox, which is unchecked.

4. 无需配置第3层选项。

This screenshot is identical to the one above, showing the same configuration for WLAN '5508-MA'. The 'Layer 3 Security' dropdown is still set to 'None', and the 'Fast Transition' checkbox is also unchecked.

5. 为了让外部NGWC处理CoA，应在Anchor AireOS WLC中禁用AAA服务器。只有在以下位置未配置RADIUS服务器的情况下，才可以在锚点WLC中启用AAA服务器：Security > AAA > RADIUS > Authentication

The screenshot shows the Cisco WLC Web Interface under the 'WLANS' tab. In the 'Advanced' section, the 'AAA Servers' tab is selected. It contains fields for 'Radius Server Overwrite interface' (disabled) and tables for 'Authentication Servers' and 'Accounting Servers' across six servers, all of which have 'Enabled' checked.

6. 选择WLANs > WLANs > Edit > Advanced。选中Allow AAA Override复选框。从NAC State下拉列表中，选择Radius NAC。

The screenshot shows the 'Advanced' tab of the 'Edit WLAN' screen. The 'Allow AAA Override' checkbox is checked. In the 'NAC' section, the 'NAC State' dropdown is set to 'Radius NAC'.

7. 将此项添加为WLAN的锚点。

The screenshot shows the 'MAC Filtering' tab of the 'Edit WLAN' screen. The 'Radius NAC' anchor point is highlighted in yellow.

8. 在将其指向本地后，它应使用Control and Data Path UP/UP查看此信息。

## Mobility Anchors

WLAN SSID	6505-M9	Data Path	Control Path
Local		Up	Up

9. 在WLC上创建重定向ACL。这将拒绝DHCP和DNS。它允许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	UDP	Any	DNS	Any	Any	0
2	Permit	/0.0.0.0	/0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	/0.0.0.0	10.106.73.69	Any	Any	Any	Any	Any	0
4	Permit	/0.0.0.0	255.255.255.255	Any	Any	Any	Any	Any	0
5	Permit	10.106.73.69	0.0.0.0	Any	Any	Any	Any	Any	0
6	Permit	255.255.255.255	0.0.0.0	Any	Any	Any	Any	Any	0

这就是创建ACL后的情况。

Name	Type
ACL_Provisioning_Redirect	IPv4
<b>REDIRECT</b>	IPv4

10. 在WLC 5760上定义ISE RADIUS服务器。

11. 使用CLI配置RADIUS服务器、服务器组和方法列表。

```
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. 从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. 将另一个WLC定义为此WLC上的移动成员。

```
wireless mobility group member ip 10.105.135.151 public-ip 10.105.135.151 group Mobile-1
注：如果将WLC 3850配置为外部，则请确保在移动控制器上定义交换机对等组，在移动控制器上定义交换机对等组。然后在WLC 3850上配置以前的CWA配置。
```

14. 使用CLI配置重定向ACL。这是ISE作为AAA覆盖返回的url-redirect-acl以及访客门户重定向的重定向URL。它是当前在统一架构上使用的直接ACL。这是一个“punt”ACL，通常用于统一架构的反向ACL。您需要阻止对DHCP、DHCP服务器、DNS、DNS服务器和ISE服务器的访问。根据需要仅允许www、443和8443。此ISE访客门户使用端口8443，并且重定向仍可使用此处显示的ACL。这里启用了ICMP，但是您可以根据安全规则拒绝或允许。

```
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：**启用HTTPS时，由于可扩展性，可能导致一些高CPU问题。除非思科设计团队推荐此服务，否则请勿启用此服务。

## 验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序工具（仅限注册用户）支持某些 show 命令](#)。使用输出解释器工具来查看 show 命令输出的分析。

将客户端连接到已配置的SSID。收到IP地址后，当客户端进入Web auth Required状态时，请打开浏览器。在门户中输入您的客户端凭证。

**CISCO Guest Portal**

Username: nico

Password: .....  
[Sign On](#) [Change Password](#)



身份验证成功后，选中Accept terms and conditions复选框。单击Accept。

**Guest Portal**

**CISCO Guest Portal**

Welcome nico

## 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

[Accept](#) [Decline](#)

您将收到一条确认消息，现在可以浏览到Internet。



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

在ISE上，客户端流如下所示：

2014-05-09 06:28:19.334	<input checked="" type="checkbox"/>	<input type="radio"/>	shubair	00:17:7C:2F:B6:9A	Unknown	Surbg_5760	PermitAccess	Authorize-Only succeeded	0af987b2536c7a1700000117
2014-05-09 06:28:19.298	<input checked="" type="checkbox"/>	<input type="radio"/>		00:17:7C:2F:B6:9A		Surbg_5760		Dynamic Authorization succeeded	0af987b2536c7a1700000117
2014-05-09 06:28:19.274	<input checked="" type="checkbox"/>	<input type="radio"/>	shubair	00:17:7C:2F:B6:9A				Guest Authentication Passed	0af987b2536c7a1700000117
2014-05-09 06:19:00.822	<input checked="" type="checkbox"/>	<input type="radio"/>		00:17:7C:2F:B6:9A	00:17:7C:2F:B6:9A	Unknown	CWA	Authentication succeeded	0af987b2536c7a1700000117

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

[命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。](#)

**注意：**使用[debug命令之前，请参阅有关Debug命令的重要信息。](#)

在融合接入WLC上，建议运行跟踪而不是调试。在Aironet OS 5508 WLC上，您只需输入**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
```

Cisco Bug ID [CSCun3834](#) 包含Cisco IOS-XE和Aironet OS上的一些已知缺陷。

下面是跟踪中成功的CWA流的样子：

```
[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, wlanIfName: , 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 received 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:  
0x000000118) - 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 / 0xFE0000110

[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 / 0xFE0000110

[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 / 0xFE0000110

[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 / 0xFE0000110

[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 / 0xFE0000110

[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 / 0xFE0000110

[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 / 0xFE0000110

[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 received 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, unique 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 received 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 l1m_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) l1m_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

```

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。