

# Deployment Guide: Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.0

Last revised: February 1, 2008

# **Contents**

- "Overview" section on page 1
- "Configuring Guest Access on the Cisco Wireless LAN Controller" section on page 2
- "Creating Guest Access Accounts" section on page 11
- "Web Authentication Process" section on page 17
- "Troubleshooting" section on page 42
- "Related Documentation" section on page 51

# **Overview**

Today, leading companies are faced with providing network access for their customers, partners, vendors, contractors and other visitors. This expanded network access enables higher productivity, improved collaboration, and better service; however, it necessitates that a guest access policy be established to address increased network usage and security issues.

By implementing a broad-based solution to guest access, companies can control network access, eliminate ad hoc IT support requirements, track guest network usage and securely separate guest traffic from internal resources.

The need for guest access has evolved as the needs of guests have evolved. Today, with laptops, networked applications, and digital phone lines, a visiting guest is disempowered without continued access to these technologies.



Guest networks are network connections provided by an enterprise to enable their guests to gain access to the Internet, and the guests' own enterprise without compromising the security of the host enterprise. The main technical requirements for a complete guest access solution are outlined below:

- Complete integration into the enterprise network and its resources
- Logical separation (segmentation) of guest traffic from internal enterprise traffic
- Secure VPN connections to guests' own corporate networks
- Authentication and login capabilities

In this document, we have included various scenarios where the Cisco Wireless LAN Controller can be used to deploy a guest access solution over the corporate network.

### **Terms and Acronyms**

Term or Acronym	Definition
AP	Wireless access point
BBSM	Cisco Building Broadband Service Manager
Cisco WiSM	Cisco Wireless Services Module
Lightweight AP	An access point running LWAPP that makes the AP work with the WLCs
LWAPP	Lightweight Access Point Protocol—IETF draft protocol used in the Cisco Centralized WLAN Architecture implementations. LWAPP defines both control and data encapsulation formats used in the Cisco Centralized WLAN Architecture
WCS	Cisco Wireless Control System—Management software that manages WLC devices and adds advanced management like location-based services
WLC	Cisco Wireless LAN controller—Cisco devices that centrally manage lightweight access points and WLAN data traffic

#### Table 1 Key Terms Used in this Deployment Guide

# **Configuring Guest Access on the Cisco Wireless LAN Controller**

An existing enterprise wired and wireless network infrastructure can be used to implement a wireless guest network. No separate, overlay network is required to support guest access.

Therefore, the overall implementation and maintenance costs of a guest network are greatly reduced.

To successfully implement a guest network on an existing wired or wireless network, the following critical elements are required:

 A dedicated guest SSID/WLAN – Required implementation within all wireless networks in which guest access is needed.

- Guest traffic segregation or path isolation To restrict guest user traffic to distinct, independent logical traffic paths within a shared physical network infrastructure.
- Access Control To identify any user or device that logs onto the network for assignment to appropriate groups by employing an authentication process.
- Guest User Credential Management To support creation of temporary credentials for a guest by an authorized user. This function may reside within an access control platform or a component of AAA or other management system.

### **Initial Configuration**

Figure 1 shows an example of basic guest access using the Cisco wireless LAN controller. The configuration shown is applicable for Cisco controller models 2006, 410x, and 440x.

The wireless LAN controller in the remote office is connected to a WAN infrastructure.

- All the interfaces on the wireless LAN controller are mapped to physical port 1 and two WLANs are configured:
  - one for a guest user (SSID guest) and
  - one for EAP authentication (SSID secure).
- Dynamic VLAN interfaces are created for the guest SSID (VLAN 60) and the secure EAP SSID (VLAN 30).
- The management and access point (AP) manager interfaces are configured to use VLAN 50.
- All network services (AAA, DHCP, and DNS) are configured on VLAN 1.
- All access points will be connected to VLAN 50.

#### Figure 1 Configuration Example - Remote Office



#### **Connecting to the Neighbor Switch**

The WLC is connected to the neighboring Catalyst 3750 switch using only 1 port. The neighbor switch port is configured as an 802.1Q trunk, and only the appropriate VLANs in this case, specifically VLANs 30, 50 and 60 are allowed. The AP-Manager and Management interfaces are members of VLAN 50 which in this example is configured as the native VLAN in the trunk interface.

The 802.1Q switchport command-line interface (CLI) configuration is as follows:

```
interface GigabitEthernet1/1
description Trunk Port to Cisco WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 50
switchport trunk allowed vlan 30,50,60
switchport mode trunk
no ip address
```

#### **Configuring the Cisco Wireless LAN Controller**

The initial configuration of the Cisco wireless LAN controller is done through a console cable connected to the controller. The administrator can configure the system using the Configuration Wizard available on the console port.

# <u>Note</u>

After the initial configuration, the administrator can configure the Cisco wireless LAN controller using the controller command-line interface (CLI) or the controller GUI.

The Configuration Wizard is used to configure a number of items as seen in the script example below. Some of the items configured during this process include: the system name, Cisco wireless LAN controller (WLC) administrative user credentials, the Management interface, AP Manager, virtual interfaces, the mobility group name, one SSID, and a RADIUS server.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:1c:c0]:
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.50.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.50.1
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.1.1.11
AP Manager Interface IP Address: 10.10.50.3
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.1.1.11):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Network Name (SSID): guest
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: YES
Enter the RADIUS Server's Address: 10.1.1.11
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]: US
Enable 802.11b Network [YES][no]: YES
Enable 802.11a Network [YES][no]: YES
Enable 802.11g Network [YES] [no]: YES
Enable Auto-RF [YES][no]: YES
Configuration saved!
Resetting system with new configuration....
```

Note

During initial setup, the VLAN for the Management interface is untagged because it corresponds to the native VLAN on the switch trunk port. By default, an untagged VLAN is assigned the value of zero (0) but this value may not correspond to the VLAN number on the switch port. In the example in this document, the switch port's Native VLAN is VLAN 50, but on the Cisco wireless LAN controller, the Management interface is assigned to VLAN 0. The default values for all other options are accepted as assigned and noted above in the Configuration Wizard script.

#### Modifying the VLAN Interfaces for the Guest and Secure (Employee) VLAN

The guest VLAN and the employee (secure) VLAN must be modified from the configuration initially assigned during the configuration wizard process.



All configuration of the controller from this point forward is done using a web management interface.

To modify the guest and employee (secure) VLAN interfaces, follow these steps:

Step 1 Open an Internet Explorer browser window (only Internet Explorer is supported) and point it at the Management interface IP address. Only HTTPS is on by default, so the URL should be https://<management\_IP>.

The window seen in Figure 2 appears.

- **Step 2** In the web interface of the wireless LAN controller (WLC), choose **Controller > Interfaces.**
- **Step 3** Click New... to create a dynamic VLAN interface for the guest SSID.

In the window that appears (Figure 3), enter a name in the Interface Name field and assign a value to the VLAN ID field. For this example, we entered *guest-vlan* and 60, respectively.

- Step 4 Click Apply.
- **Step 5** In the window that appears (Figure 4), enter the IP address, net mask, and gateway addresses for the VLAN interface.
- **Step 6** Enter the port number of the physical port.
- **Step 7** Enter the IP address for the DHCP server.
- **Step 8** Select the Access Control List, if applicable.
- **Step 9** Click **Apply**. The window seen in Figure 5 appears.
- Step 10 Repeat steps 2 to 9 to create another dynamic interface for the EAP SSID (employee secure VLAN). For this example, we named the VLAN secure-vlan with a VLAN ID of 30.



To view the newly created *guest-VLAN* and *secure-VLAN*, choose **WLANs** from the navigation bar (Figure 5).

isco Systems								Save Configuratio	on   Ping	Logout Refi
dhi, albi	MONITOR WLAN	ls COl	VTROLLER	WIR	ELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
1onitor	Summary									
ummary tatistics	Controller Sum	nary					Rogue Summa	ary		
Controller Ports	Management IP Ad	dress	10.10.5	50.2			Active Rogue AP		0	Detail
/ireless	Software Version		3.2.78	0			Active Rogue Cli		0	Detail
Roque APs	System Name		Cisco_	33:1c:c	:0		Adhoc Rogues	encs	0	Detail
Known Rogue APs	Up Time		0 days	, 0 hour	rs, 13 n	ninutes	Rogues on Wired	Network	0	<u>Croton</u>
Rogue Clients Adhoc Rogues 802.11a Radios 802.11b/g Radios Clients	System Time		Mon Fe	b 13 22	2:23:11	2006	Rogues on whet	Network	0	
	802.11a Network S	state	Enable	d						
	802.11b/g Network State Enabled						Top WLANs			
RADIUS Servers	Loose Daint O						WLAN		# of C by SS	lients ID
	Access Point Su	mmary					guest		0	Detail
		Total	Up	D	own					
	802.11a Radios	0	• 0	• (	0	Detail	Most Recent T	raps		
	802.11b/g Radios	0	• 0	• (	0	Detail				
	All APs	0	• 0	• 0	0	Detail	Cold Start:			
							Link Up: Slot: 0			
	Client Summary	,					Link Down: Slot	t: 0 Port: 1		
										View All
	Current Clients	0				Detail				
	Excluded Clients	0				Detail	This page refresh	es every 30 seco	nds.	
	Disabled Clients	0				Detail				

#### Figure 2 Initial Configuration of the WLC as Created by the Configuration Wizard

#### Figure 3 Configuring VLAN Interface for Guest and Secure (Employee) Wireless LAN Access

Cisco Stateme			Save Configuration   Ping   Logout   Refresh
dr. dr.	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMMANDS HELP
Controller	Interfaces > New		< Back Apply
General Inventory	Interface Name guest-vlan		53
Interfaces	VLAN Id 60		170422

Cisco Systems 	MONITOR WLANS C	CONTROLLER	WIRELESS	SECURITY	S	ave Configurat	ion   Ping HELP	Logout   Re
Controller General Inventory Interfaces Internal DHCP Gerver Mobility Management Mobility Groups Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	Interfaces > Edit General Information Interface Name Interface Address VLAN Identifier IP Address Netmask Gateway Physical Information Port Number DHCP Information Primary DHCP Server Secondary DHCP Server	guest-vlan [60 [10.: [255 [10.: ] 1	10.60.2 .255.255.0 10.60.1				C Back	Apply
	Access Control List							

#### Figure 4 Entering Configuration Details for the Guest VLAN Interface

Figure 5 Summary Page Showing Guest and Secure VLAN

Cisco Sverent	MONITOR WLANS	CONTROLLER W	VIRELESS SECURITY	S MANAGEMENT	ave Configurat COMMANDS	ion Pin HELP	g Logout Refre	sh
Controller	Interfaces						New	
General 🔓	Interface Name	VLAN	Identifier IP Address	Interface	Туре			
Inventory	ap-manager	untage	ged 10.10.50.3	Static	Edit			
Interfaces	guest-vlan	60	10.10.60.2	Dynamic	Edit Re	move		
Internal DHCP Server	management	untago	ged 10.10.50.2	Static	Edit			
Mobility Management	secure-vlan	30	10.1.30.3	Dynamic	Edit Ba	move		194
Mobility Groups Mobility Statistics	virtual	N/A	1.1.1.1	Static	Edit			170660

#### Modifying the WLAN Instance to Define Security Policies

After configuring the IP address for the guest and secure VLAN interfaces for the wireless LAN, you can define security polices such as web authentication (a Layer 3 security policy) for the guest and secure (employee) wireless LAN access interfaces.

To define security policies for the VLANs, follow these steps:

- **Step 1** Click WLANs. The WLANs summary window appears (Figure 6).
- Step 2 At the WLANs window (Figure 6), click the Edit link next to the guest WLAN to access the WLANs > Edit page (Figure 7).

dry dry	MONITO	R WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANS	WLANs								Ne	w
WLANs WLANs										
WLANs	WLAN ID	WLAN SSID			Admin Status	Security Policies				
		WLAN SSID				Security Policies Web-Auth		Edit	Remove	Mobilit

#### Figure 6 WLANs Summary Page Showing Existing Defined Wireless LANs

#### Figure 7

WLANs > Edit Page for the Guest WLAN

Creek Statems	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY		ve Configuration Ping Logout Ref COMMANDS HELP	fre
WLANS	WLANs > Edit			< Back Apply	ľ
WLANS WLANS AP Groups VLAN	WLAN ID WLAN SSID	1 guest			
	General Policies		Security Policie	s	
	Radio Policy Admin Status Session Timeout (secs)	All Enabled	Layer 2 Security	None 💌	
	Quality of Service (QoS) WMM Policy	Silver (best effort) • Disabled •	Layer 3 Security	None	
	7920 Phone Support Broadcast SSID	Client CAC Limit CAP CAC Limit	Preauthenticatio	Authentication C Passthroug     Act none	gh
	Allow AAA Override External Policy Validation		* Web Policy car and L2TP.	nnot be used in combination with IPsec	
	Client Exclusion	Enabled ••• 60     Timeout Value (secs)     Override		exclusion is enabled, a timeout value of ity(will require administrative override t dients)	
	DHCP Addr. Assignment Interface Name	Required			
	Radius Servers				
	Server 1	Authentication Servers Accounting Servers none Inone			170551

**Step 3** At the WLANs > Edit page (Figure 7), check the DHCP Addr. Assignment box.

This enables dynamic IP address assignment.

**Step 4** Select the appropriate **Interface Name** from the drop-down menu.

For this example, the interface for the guest WLAN is *guest-vlan* (assigned in the "Modifying the VLAN Interfaces for the Guest and Secure (Employee) VLAN" section on page 5).

**Step 5** At the Layer 3 Security section, check the **Web Policy** box and select the circle next to **Authentication**.



**Note** Menu options for Layer 2 and Layer 3 Security remain as "None."

- **Step 6** Click **Apply** to save edits for the interface on the running configuration of the WLAN switch.
- **Step 7** Choose WLANs to verify that the edits are saved (Figure 8).

For this example, we want to verify that web authentication (Web-Auth), the assigned security policy, is enabled for the guest WLAN.

Cince Statem Save Configuration | Ping | Logout | Refres WLANS WLANS New... WLANS WLAN Admin WLAN SSID Security Policies VLAN: ID Status AP Groups VLAN Enabled Edit Remove quest Web-Auth 1

Figure 8 WLANs Page Verifying Security Policy Assigned to Guest WLAN

- **Step 8** Choose **WLANs > New** to create a secure (employee) WLAN.
- **Step 9** At the WLANs page, select the **Edit** link next to the newly created secure WLAN.
- **Step 10** At the WLANs > Edit page, check the DHCP Addr. Assignment box.
- Step 11 Select secure-vlan from the Interface Name drop-down menu.
- Step 12 From the Layer 2 Security section, select one of the higher security options.

For this example, we chose WPA2 with 802.1x authentication from a RADIUS server.

S, Note

If you select WPA2 from the Layer 2 Security menu, you must select the **TKIP and AES** option from the **WPA1/WPA2 Policy** drop-down menu (scroll to bottom of screen) for the feature to work.

S. Note

If using a RADIUS server to authenticate, select the appropriate IP address from the **Authentication Server** drop-down menu found under the Radius Servers section. For this example, we need to define this value given our Layer 2 security selection in Step 12.

- **Step 13** Click **Apply** to save edits for the interface on the running configuration of the WLAN switch.
- Step 14 Choose WLANs to verify that the edits are saved (Figure 9).

Figure 9 WLANs Page Verifying Security Policy Assigned to Secure (Employee) WLAN

cisco Svorens	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY		ave Configurati COMMANDS	on   Ping   HELP	Logout	
WLANS	WLANs								Ne	w
WLANS WLANS	WLAN N	VLAN SSID			Admin Status	Security Policies				
					Enabled	Web-Auth		Edit	Remove	Mobility
AP Groups VLAN	1 (	uest			chapted	Web-Addi		10000		Anchor

# **Creating Guest Access Accounts**

If you are using controllers running controller software release 3.2, see the "Creating a Guest Access Account Using the Local Network User Option" section on page 11.

The Local Network User option allows you to directly add users to the local database of the controller. The local user database is limited to a maximum of 2048 entries and is set to a default value of 512 entries at the **Security > General** page. This database is shared by local management users (including lobby ambassadors), net users (including guest users), MAC filter entries, and disabled clients. Together, all of these types of users cannot exceed the configured database size.

**If you are using controllers running software release 4.0 or greater,** see the "Creating a Guest Access Account Using the Lobby Ambassador Option" section on page 12.

The Lobby Ambassador option is a two-step process. The first step is to create a lobby administrator account, also known as a *lobby ambassador account*. The second step is to create guest accounts when the lobby ambassador is active. The lobby ambassador has limited configuration privileges and only has access to the web pages used to manage the guest accounts. The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

## **Creating a Guest Access Account Using the Local Network User Option**

You must create a local net user username and password to use when logging in as a Web Authentication client to the wireless LAN.

To create a username and a password, follow these steps:

- **Step 1** Choose **Security > Local Net Users** found under the AAA summary heading.
- **Step 2** On the Local Net Users page, click **New**.

The Local Net Users > New page appears (Figure 10).

er wireless securi	ITY MANAGEMENT	COMMANDS HEI	LP Sack	Apply
			< Back	Apply
LAN 🔽				
				170548
				17(
	LAN 💌	LAN 🕶	LAN 💌	

Step 3 Step 4 Step 5 Step 7 In the Lifetime field, enter the period of time (in seconds) that the user account should remain active. Note A value of zero (0) is not valid for the lifetime parameter. Step 8 Select the WLAN ID to which the user is allowed access. Note Select the WLAN which has layer 3 web authentication configured (under WLAN Security Policies). Step 9 In the Description field, enter a term for the user such as guest user. Click **Apply** to see your entries and changes. Step 10 Step 11 Click **Save Configuration** to save the information entered.

## **Creating a Guest Access Account Using the Lobby Ambassador Option**

You can create a lobby ambassador account on the controller through either its web interface or the CLI. Examples of both are provided below.

#### **Creating a Lobby Ambassador Account Using the Controller Web Interface**

To create a lobby ambassador account on the controller using the web interface, follow these steps:

Step 1

Click **Management > Local Management Users** to access the Local Management Users page (Figure 11).



This page lists the names and access privileges of the local management users. You can click **Remove** to delete any of the user accounts from the controller. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

CISCO SYSTEMS									Ping	Logout	
	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Management	Local Man	agement	Users						1	New	
Summary	User Nam	е			User Access	Mode					
SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs	doc				ReadWrite		<u>Remove</u>				
нттр											
Felnet-SSH											
Serial Port											
Local Management Users											
User Sessions											
Logs Config Message logs											
Mgmt Via Wireless											
<b>Tech Support</b> System Resource Information Controller Crash AP Log											

#### Figure 11 Local Management Users Page

#### Step 2 Click New.

The Local Management Users > New page appears (Figure 12).

Figure 12	Local Management Users > New Page	
CLEAN SVETCHE		

CISCO SYSTEMS									Save Configuration - Fing	LUGU
	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Management	Local Mana	gement	Users > New						< Back	A
Summary	User Name	)								
SNMP										
General SNMP V3 Users	Password									
Communities	Confirm Pa	seword								
Trap Receivers Trap Controls	GUIIIIIIPO	15597010								
Trap Logs	User Acces	e Modo	ReadOnly	*						
НТТР	USEI ALLES	ss moue	ReadOnly	×						
Telnet-SSH			ReadWrite LobbyAdmi							
Serial Port										6
Local Management Users										170549

- **Step 3** In the User Name field, enter a username.
- **Step 4** In the Password and Confirm Password fields, enter a password.



**Step 5** Choose LobbyAdmin from the User Access Mode drop-down menu. This option enables the lobby ambassador to create guest user accounts.

# Note

The **ReadOnly** option creates an account with read-only privileges, and the **ReadWrite** option creates an administrative account with both read and write privileges.

- **Step 6** Click **Apply** to see your changes. The new lobby ambassador account appears in the list of local management users.
- **Step 7** Click **Save Configuration** to save your changes.

#### **Creating a Lobby Ambassador Account Using the Command-Line Interface**

Enter this command to create a lobby ambassador account using the controller CLI:

config mgmtuser add lobbyadmin\_username lobbyadmin\_pwd lobby-admin



Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

#### **Creating Guest User Accounts as a Lobby Ambassador**

Follow these steps to create guest user accounts:



A lobby ambassador cannot access the controller CLI and therefore can only create guest user accounts from the controller GUI.

**Step 1** Log into the controller as the lobby ambassador, using the username and password specified in the "Creating a Guest Access Account Using the Lobby Ambassador Option" section above.

The Lobby Ambassador Guest Management > Guest Users List page appears (Figure 13).

#### Figure 13 Lobby Ambassador Guest Management > Guest Users List Page

CISCO SYSTEMS	Lobby Ambassador Guest Management	Logout   Refresh
Guest Management	Guest Users List	New
	User Name WLAN SSID Account Remaining Time Description	
		155939

Step 2 Click New to create a guest user account. The Guest Users List > New page appears (Figure 14).

Cisco Systems matthematthem	Lobby Ambassador Guest	Management		Logout   Refresh
Guest Management	Guest Users List > New		< Back	Apply
	User Name			
	Generate Password			
	Password			
	Confirm Password			
	Lifetime	1 days 0 hours 0 mins secs 0		
	WLAN SSID	guest 💌		
	Description			155941

Figure 14 Guest Users List > New Page

- **Step 3** In the User Name field, enter a name for the guest user. You can enter up to 24 characters.
- **Step 4** Perform one of the following:
  - If you want to generate an automatic password for this guest user, check the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password fields.
  - If you want to create a password for this guest user, leave the **Generate Password** check box unchecked and enter a password in both the Password and Confirm Password fields.



Passwords can contain up to 24 characters and are case sensitive.

Step 5 From the Lifetime drop-down boxes, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four fields creates a permanent account.

Default: 1 day

Range: 5 minutes to 30 days



The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires re-authentication.



You can change a guest user account with a non-zero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent or to change a permanent account to a guest account, you must delete the account and create it again.

Step 6 From the WLAN SSID drop-down box, choose the SSID that will be used by the guest user. The only WLANs that are listed are those for which Layer 3 web authentication has been configured (under WLAN Security Policies).

Cisco recommends that the system administrator create a specific guest WLAN to prevent any
potential conflicts. If a guest account expires and it has a name conflict with an account on the
RADIUS server and both are on the same WLAN, the users associated with both accounts are
disassociated before the guest account is deleted.

- Step 7 In the Description field, enter a description of the guest user account. You can enter up to 32 characters.
- Step 8 Click Apply to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page (Figure 15).

Figure 15 Lobby Ambassador Guest Management > Guest Users List Page

Cisco Systems	Lobby Ambassador Gu	iest Management		Logout   Refresh	
Guest Management	Guest Users List			l	
	User Name	WLAN SSID	Account Remaining Time	Description	
	guest1	guest	23 h 54 m 43 s	Guest1 user account	E o
					15594(

From this page, you can see all of the guest user accounts, their WLAN SSIDs, and their lifetimes. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

**Step 9** Repeat this procedure to create any additional guest user accounts.

### **Viewing Guest User Accounts**

After a lobby ambassador creates the guest user accounts, the system administrator can view them from the controller GUI or CLI.

#### Using the GUI to View Guest Accounts

To view guest user accounts using the controller GUI, click **Security** and then **Local Net Users** under AAA. The Local Net Users page appears (Figure 16).

Cisco Systems	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Save Co COMMANDS	nfiguration HELP	Ping   Loo	gout   Refre:
Security	Local Net	Users							Ne	
AAA General	User Nam	е		WLAN ID	Guest	User Descripti	on			
ADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies	guest1			2	Yes	Guest1 us	er account		Edit	<u>Remove</u>
AP Policies Access Control Lists										

Figure 16 Local Net Users Page

From the Local Net Users page, the system administrator can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using that guest WLAN and are logged in using that account's username are deleted.

#### Using the CLI to View Guest Accounts

To view all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command: **show netuser summary** 

# Web Authentication Process

Web authentication is a Layer 3 security feature that causes the controller to block IP traffic (except DHCP-related packets) until the client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. Then when the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login window.

Using the Web Authentication feature on a Cisco wireless LAN controller, we can authenticate a guest user on the wireless LAN controller, an external web server, an external database on a RADIUS server or via the Cisco Building Broadband Service Manager (BBSM).

These four methods are described in the following sections:

"Web Authentication Using Mobility Anchor Feature on Controller" section on page 17

"Web Authentication Using an External RADIUS Server" section on page 26

"Web Authentication Using an External Web Server" section on page 28

"Web Authentication Using Cisco Building Broadband Service Manager" section on page 30

### Web Authentication Using Mobility Anchor Feature on Controller

Guest tunneling provides additional security for guest-user access to the corporate wireless network, ensuring that guest users are unable to access the corporate network without first passing through the corporate firewall. Instead of extending the DMZ virtual LAN (VLAN) to each wireless LAN controller on the network, a Cisco 4100 or 4400 series wireless LAN controller or Cisco WiSM can be used in the DMZ as an anchor controller to terminate traffic from remote controllers.

Internal employee user traffic is segregated from guest user traffic using Ethernet over IP (EoIP) tunnels and VLANs between the remote controllers and the DMZ controller.

#### **Guest Tunneling Support on Cisco Products**

Guest Tunneling provides additional security for guest-user access to the corporate wireless network across most wireless LAN controller platforms (Table 2).

Software Release/Platform	3.0	3.2	4.0
Cisco 4100 series wireless LAN controllers	Y	Y	Ν
Cisco 4400 series wireless LAN controllers	Y	Y	Y
Cisco 2000 series wireless LAN controllers <sup>1</sup>	N	Y	Y
Cisco 6500 series (WiSM)		Y	Y
Cisco 3750 series with integrated wireless LAN controller		N	Y
Cisco wireless LAN controller module for Integrated Service Routers <sup>1</sup>		Y	Y

#### Table 2 Guest Tunneling Support on Wireless LAN Controller Platforms

1. Cannot be used for anchor functions (tunnel termination, web authentication and access control); however, origination of guest controller tunnels is supported. When a user associates with a service set identifier (SSID) that is designated as the guest SSID, the user's traffic is tunneled to the DMZ Anchor controller which can route the traffic to the DMZ network outside of the corporate firewall.

In guest tunneling scenarios:

- The user's IP address is administered from the DMZ anchor controller, which has dedicated VLAN for guest users.
- All user traffic is transported over an Ethernet-over-IP (EoIP) tunnel between the remote wireless LAN controller and the DMZ anchor wireless LAN controller.

Mobility is supported as a client device roams between wireless LAN controllers.

Each DMZ anchor controller can support 40 tunnels from various inside controllers. These tunnels are established from each controller for each SSID using the mobility anchor feature, meaning that many wireless clients can ride the tunnel.

For a customer with many remote sites, it is now possible to forward different types of guest traffic from different sites to different DMZ Anchor controllers, or to the same DMZ Anchor controller with different wireless LANs. Any user getting placed on the DMZ can use the AAA-override feature to apply RADIUS Vendor Specific Attributes (VSAs) on a per-session basis.

Guest tunneling provides additional security for guest-user access to the corporate wireless network.



For the example in this deployment guide, the remote and the DMZ anchor controllers are assigned to the same mobility group. Generally, implementing the guest tunneling feature does not require that the remote and DMZ anchor controllers be in the same mobility group.



#### Figure 17 Web Authentication Using the Mobility Anchor Controller Feature

#### **Anchor Controller Selection**

The anchor function on a controller includes tunnel termination, web authentication, and access control.

A Cisco 4400 series controller is the most cost effective controller that can be used as an Anchor controller in the DMZ.

- If the controller is used for guest access and tunnel termination functions only, a Cisco 4402 with 12 access point support is sufficient as it is not used to manage LWAPP access points in the network. Additionally, the Cisco 4400 supports up to 2,500 simultaneous users and has a forwarding capacity of 2 Gbps.
- If your guest access network deployment requires more than 2 Gbps throughput, you can use a Cisco 4404 or Cisco WiSM as an Anchor controller.
  - A single Cisco 4400 series controller or Cisco Catalyst 3750G Integrated wireless LAN controller can support EoIP tunnels from up to 40 other controllers.
  - A Cisco WiSM, which consists of two independent controllers, can support up to 80 EoIP tunnels.

#### **Creating and Adding Controllers to the Same Mobility Group**

To configure a mobility group, follow these steps:

**Step 1** Create a mobility group in the remote and DMZ anchor controller. For this example, we named the mobility group, *mobile-1*.

٩, Note

The mobility group name is generally set at deployment time through the Startup Wizard. However, you can change it if necessary through the Default Mobility Domain Name field on the **Controller** > **General** page. The mobility group name is case sensitive.

Step 2 From the remote controller, choose Controller > Mobility Groups to access the Static Mobility Group Members page (Figure 18).

Figure 18 Controller > Static Mobility Group Members Page

CISCO SYSTEMS						ave Configurati	on   Ping	Logout   Rel	fresh
allowed by	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Controller	Static Mobility Grou	p Members				N	lew	EditAll	
General	Default Mobility G	roup mobile-	1						
Inventory Interfaces	MAC Address	IP Address		iroup Name					37
Internal DHCP Server	00:0b:85:33:1c:c0	10.10.50.2	(1	.ocal)					1704

- **Step 3** Click **Edit All**. The window seen in Figure 19 appears.
  - Figure 19 Mobility Group Members > Edit All

Cisco Systems						S	Save Configuration   Ping	Logout   Refres
	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS HELP	
Controller	Mobility G	roup Men	nbers > Edit All				< Back	Apply
General			o edit all mobility ( s are listed below					
Inventory	mobility grou	up member	is represented as	a MAC addres	ss, IP			
Interfaces	address and spaces.	group nan	ne(optional) separ	ated by one or	more			
Internal DHCP Server								
Mobility Management Mobility Groups Mobility Statistics			10.10.50.2 40.1.3.10 mob	ile-l	<u>^</u>			
Ports								
Master Controller Mode								
Network Time Protocol								
QoS Profiles					Ŧ			

**Step 4** Enter the MAC address and IP address of the DMZ anchor controller in the window of the Edit All page.

In this example, we use a MAC address of 00:11:92:ff:87:20 and an IP address of 40.1.3.10 for the DMZ anchor controller.

- **Step 5** From the DMZ anchor controller, choose **Controller > Mobility Groups** to access the Static Mobility Group Members page.
- Step 6 Click Edit All.
- Step 7 Enter the MAC address and IP address of the remote controller in the window of the Edit All page.

Note

# <u>Note</u>

In this example, we use a MAC address of 00:0b:85:33:1c:c0 and an IP address of 10.10.50.2 for the remote controller.

**Step 8** After adding the two controllers to the mobility group, click **Apply** and **Save Configuration**.

You are now ready to create the mobility anchor between the remote and DMZ controllers.

#### **Configuring Auto-Anchor Mobility**

You can use auto-anchor mobility (or guest WLAN mobility) to improve load balancing and security for roaming clients on your wireless LANs. Under normal roaming conditions, client devices join a wireless LAN and are anchored to the first controller that they contact. If a client roams to a different subnet, the controller to which the client roamed sets up a foreign session for the client with the anchor controller.

However, using the auto-anchor mobility feature, you can specify a controller or set of controllers as the anchor points for clients on a wireless LAN. In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a wireless LAN. You can use this feature to restrict a wireless LAN to a single subnet, regardless of a client's entry point into the network. Clients can then access a guest wireless LAN throughout an enterprise but still be restricted to a specific subnet.

Auto-anchor mobility can also provide geographic load balancing because the wireless LANs can represent a particular section of a building (such as a lobby, a restaurant, and so on), effectively creating a set of home controllers for a wireless LAN. Instead of being anchored to the first controller that they happen to contact, mobile clients can be anchored to controllers that control access points in a particular vicinity.

#### **Configuration Guidelines**

Keep these guidelines in mind when configuring auto-anchor mobility:

- Add Controllers to the mobility group member list before you designate them as mobility anchors for a wireless LAN.
- You can configure multiple controllers as mobility anchors for a wireless LAN.
- The wireless LANs on both the foreign controller and the anchor controller must be configured with mobility anchors. On the anchor controller, configure the anchor controller itself as a mobility anchor. On the foreign controller, configure the anchor as a mobility anchor.

To configure auto-anchor mobility, follow these steps:

Step 1 Click Controller > WLANs to access the WLANs page (Figure 20).

Figure 20 Controller > WLANs Page

Cisco Systems						S	ave Configurati	on   Ping	Logout	Refresh
Also alles	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANS	WLANs		-						Ne	w
WLANS WLANS	WLAN W	LAN SSID			Admin Status	Security Policies				
AP Groups VLAN	1 9	uest			Enabled	Web-Auth		Edit	Remove	Mobility Anchors
	2 se	ecure			Enabled	RSN (802.1x)		Edit	Remove	Advanta Difference

**Step 2** On the WLANs page, click the **Mobility Anchors** link for the desired wireless LAN. The Mobility Anchors page for that wireless LAN appears (Figure 21).

Figure 21 Mobility Anchors Page

CISCO SYSTEMS		Save Configuration   Ping   Logout   Refresh
Abrah	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP
WLANS	Mobility Anchors	< Back
WLANS WLANS AP Groups VLAN	WLAN SSID guest Switch IP Address (Anchor)	
	Mobility Anchor Create Switch IP Address (Anchor) 40.1.3.10 •	170440

- **Step 3** At the Mobility Anchors page, select the IP address of the controller to be designated a mobility anchor in the Switch IP Address (Anchor) drop-down box.
- Step 4 Click Mobility Anchor Create. The selected controller becomes an anchor for this WLAN.
- Note
   To delete a mobility anchor for a WLAN, click Remove to the right of the controller's IP address.

   Step 5
   Click Save Configuration to save your changes.

   Step 6
   Repeat steps 3 to 5 to set any other controllers as mobility anchors for this WLAN.

   Step 7
   Configure the same set of anchor controllers on every controller in the mobility group.

#### Verifying Mobility Anchor Configuration

You can use the CLI to verify the configuration of the mobility anchor configuration for the remote and DMZ anchor controller.

To verify the configuration on the remote controller, follow these steps:

(Cisco Controller) >**show wlan summary** 

Default Mobility Domain..... mobile-1 Mobility Group members configured...... 2

Switches configured	in the Mobili	ty Group
MAC Address	IP Address	Group Name
00:0b:85:33:1c:c0	10.10.50.2	<local></local>
00:11:92:ff:87:20	40.1.3.10	mobile-1

(Cisco Controller) >show mobility anchor Mobility Anchor Export List WLAN ID IP Address 1 40.1.3.10 2 40.1.3.10

To verify the configuration on the DMZ controller, follow these steps:

(Cisco Controller) >show wlan summary Number of WLANs..... 2 WLAN ID WLAN Name Status Interface Name \_\_\_\_\_ \_\_\_\_ secure-1 Enabled management 1 Enabled guest-vlan 2 guest (Cisco Controller) >show mobility summary Mobility Protocol Port..... 16666 Mobility Security Mode..... Disabled Default Mobility Domain..... mobile-1 Mobility Group members configured..... 2 Switches configured in the Mobility Group MAC Address IP Address Group Name 00:0b:85:33:1c:c0 10.10.50.2 mobile-1 00:11:92:ff:87:20 40.1.3.10 <local> (Cisco Controller) >show mobility anchor Mobility Anchor Export List WLAN ID IP Address 40.1.3.10 1

Note

On any firewalls between the two controllers, the following ports need to be open: (1) UDP 16666 (or 16667, if encryption is enabled) for tunnel control traffic, (2) IP protocol 97 for user data traffic, (3) UDP 161 and 162 for SNMP, (4) UDP 69 for TFTP and (5) TCP port 80/443 for management.



For details on debugging the Mobility Anchor feature, please see the "Troubleshooting" section at the end of this deployment guide.

#### **Running Mobility Ping Tests (Release 4.0 and later)**

Controllers belonging to the same mobility group communicate with each other by controlling information over a well-known UDP port and exchanging data traffic through an Ethernet-over-IP (EoIP) tunnel. Because UDP and EoIP are not reliable transport mechanisms, there is no guarantee that a mobility control packet or data packet will be delivered to a mobility peer. Mobility packets may be lost in transit due to a firewall filtering the UDP port or EoIP packets or due to routing issues.

Controller software release 4.0 enables you to test the mobility communication environment by performing mobility ping tests. These tests may be used to validate connectivity between members of a mobility group (including guest controllers).

Note

You must have release 4.0 installed in the anchor and remote controller for this feature to work.

Two ping tests are available:

- **Mobility ping over UDP**—This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.
- Mobility ping over EoIP—This test runs over EoIP. It tests the mobility data traffic over the management interface.

Only one mobility ping test per controller can be run at a time.

Note

These ping tests are not Internet Control Message Protocol (ICMP) based. The term "ping" is used to indicate an echo request and an echo reply message.

Use these commands to run mobility ping tests from the controller CLI.

**1.** To test the mobility UDP control packet communication between two controllers, enter this command:

**mping** *mobility\_peer\_IP\_address* 

The *mobility\_peer\_IP\_address* parameter must be the IP address of a controller that belongs to a mobility group.

2. To test the mobility EoIP data packet communication between two controllers, enter this command:

eping mobility\_peer\_IP\_address

The *mobility\_peer\_IP\_address* parameter must be the IP address of a controller that belongs to a mobility group.

3. To troubleshoot your controller for mobility ping, enter these commands:

#### config msglog level verbose

#### show msglog

To troubleshoot your controller for mobility ping over UDP, enter this command to display the mobility control packet:

#### debug mobility handoff enable

Note

Cisco recommends using an ethereal trace capture when troubleshooting.

#### Enabling the Web Login Page on the Controller

After defining the security policies for the guest and secure VLAN interfaces, you need to enable the web login on the controller.

To enable the web login, follow these steps:

- **Step 1** Choose **Controllers** from the navigation bar at the top of the page.
- Step 2 Click Web Login Page from the option summary on the left.

The Web Login Page appears (Figure 22).

#### Figure 22 Configuring Web Login Page on Controller

ullandlin.	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Save Co COMMANDS	nfiguration Ping HELP	Logout   Refre
Security	Web Logir	n Page						Preview	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering	page. The L	llows you to ogin page is	n Type customize the co presented to we ation' is turned o	b users the firs	arance of the	cess the			
Disabled Clients User Login Policies AP Policies	Cisco Log	ю	Show	C Hide					
Access Control Lists	Redirect L login	URL after							
Network Access Control	-								
IPSec Certificates	Headline								
CA Certificate ID Certificate	Message						14		
Web Auth Certificate									
Wireless Protection Policies Trusted AP Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection									
Web Login Page									
CIDS Sensors Shunned Clients							<b>_</b>		

Step 3 Choose Internal (Default) from the Web Authentication Type drop-down menu.

# Note

If you want to customize the Web Login Page display, continue with Step 4. If you want to keep the Cisco defaults, go to Step 8.

- **Step 4** Click **Hide** if you do not want the Cisco logo to appear on the log on page.
- Step 5 To direct the user to a specific URL (such as your company) after log in, enter the appropriate URL in the Redirect URL after login field. Format of entry is: www.companyname.com. Up to 254 characters can be entered.
- Step 6 To display summary or headline information on the web login page, enter that information in the Headline field. Up to 127 characters can be entered. The default headline is "Welcome to the Cisco wireless network."
- Step 7 To display a message on the Web login page, enter the desired text in the Message field. Up to 2047 characters can be entered. The default message is "Cisco is pleased to provide the wireless LAN infrastructure for your network. Please login and put your air space to work."
- **Step 8** Click **Apply** to save changes.



You must reboot the controller to commit the changes. See "Rebooting the Wireless LAN Controller" section on page 26 for detailed steps.

#### **Rebooting the Wireless LAN Controller**

To commit the web authentication changes entered in the previous steps, you must reboot the controller. To reboot the controller, follow these steps:

- **Step 1** Choose **Commands** from the navigation bar at the top of the page.
- **Step 2** Choose Reboot and then click **Reboot**.
- Step 3 If there are any unsaved changes in your configuration, click Save and Reboot.

## Web Authentication Using an External RADIUS Server

We can configure the wireless LAN used for guest traffic to authenticate the user from an external RADIUS server; in this example it is 10.1.1.11.

To enable an external RADIUS server to authenticate traffic using the GUI, follow these steps:

**Step 1** Choose WLANs > Edit (Figure 23).

WLANS AP Groups VLAN	Admin Status Session Timeout (secs) Quality of Service (QoS) WMM Policy	2 guest All Enabled 1800 Silver (best effort)	Security Policies IPv6 Enable Layer 2 Security	None	
AP Groups VLAN	Radio Policy Admin Status Session Timeout (secs) Quality of Service (QoS) WMM Policy	All  Enabled  Silver (best effort)  Disabled	IPv6 Enable Layer 2 Security	None	
G	Radio Policy Admin Status Session Timeout (secs) Quality of Service (QoS) WMM Policy	Enabled 1800 Silver (best effort) • Disabled •	IPv6 Enable Layer 2 Security	None 🔹	
	Admin Status Session Timeout (secs) Quality of Service (QoS) WMM Policy	Enabled 1800 Silver (best effort) • Disabled •	Layer 2 Security	None   MAC Filtering	
	Session Timeout (secs) Quality of Service (QoS) WMM Policy	1800 Silver (best effort) • Disabled •		MAC Filtering	
	Quality of Service (QoS) WMM Policy	Silver (best effort)		MAC Filtering	
	WMM Policy	Disabled 💌			
	7020 Phone Support		Layer 3 Security	None +	
	7920 Phone Support	Client CAC Limit 🔲 AP CAC Limit	,	Web Policy *	
	Broadcast SSID	Enabled		Authentication C Passthrou	
	Allow AAA Override	Enabled	Preauthentication ACL		
	External Policy Validation	Enabled			
	Client Exclusion	Enabled ** 60 Timeout Value (secs)	* Web Policy cannot be and L2TP.	e used in combination with IPsec	
	DHCP Server	C Override	** When client exclusion is enabled, a timeout valu zero means infinity(will require administrative over		
	DHCP Addr. Assignment	Required	reset excluded clients)		
	Interface Name	guest-vlan			
R	adius Servers				

#### Figure 23 WLANs > Edit Page

**Step 2** Select the appropriate IP address from the Radius Servers drop-down menu.

**Note** The IP address for the RADIUS server is entered during initial setup of the controller using the configuration wizard.

Step 3 Click Save Configuration.

To enable an external RADIUS server to authenticate traffic using CLI, follow these steps:

- **Step 1** Enter **config radius auth** *ip-address* to configure a RADIUS server for authentication.
- Step 2 Enter config radius auth *port* to specify the UDP port for authentication.
- **Step 3** Enter **config radius auth** *secret* to configure the shared secret.
- **Step 4** Enter **config radius auth** *enable* to enable authentication.



• Authentication is disabled by default.

**Step 5** Enter **config radius acct** *disable* to disable authentication.



You can enter the **show radius acct statistics**, **show radius auth statistics**, and **show radius summary** commands to verify that the RADIUS settings are correctly configured.

## Web Authentication Using an External Web Server

To use a custom web authentication login window configured on an external web server rather than the default web login window of Cisco's wireless LAN controller or the Cisco Building Broadband Service Manager (BBSM), follow the instructions in the GUI or CLI procedure below.

When you enable this feature, the user is automatically directed to your custom login window on the external web server.



Figure 24 Using an External Web Server to Authenticate a Guest User

<u>Note</u>

You must configure a pre-authentication access control list (ACL) on the wireless LAN for the external web server and then choose this ACL as the wireless LAN pre-authentication ACL under **Security Policies > Web Policy** on the **WLANs > Edit** page. Once this information is entered, the Cisco wireless LAN controller web server will automatically redirect the guest to the web address entered as part of the ACL configuration.



Web authentication through external servers is supported on controllers that are integrated into Cisco switches and routers, including those in the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Cisco 28/37/38xx Series Integrated Services Router.

# Using the GUI to Choose a Customized Web Authentication Login Window from an External Web Server

To use an external web server for authentication, follow these steps:

**Step 1** Click **Security > Web Login Page** to access the Web Login page (Figure 25).



CISCO SYSTEMS	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Security	Web Logir	n Page				
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients			10.8/pas/compat/a		Redirect to ex	ternal server) 💌
User Login Policies AP Policies	192.168.10	0.8	Rer	nove		
Access Control Lists Network Access Control	Web Serv	er IP Add		Add Web Ser	]	
IPSec Certificates CA Certificate ID Certificate				Add web ser	ver	
Web Auth Certificate						
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection						
Web Login Page						
CIDS Sensors Shunned Clients						

- **Step 2** From the Web Authentication Type drop-down box, choose **External (Redirect to external server)**.
- **Step 3** In the URL field, enter the URL of the customized web authentication login window on your web server. You can enter up to 252 characters.
- **Step 4** In the Web Server IP Address field, enter the IP address of your web server. Your web server should be on a different network from the controller service port network. Click **Add Web Server**.

This server now appears in the list of external web servers.

**Step 5** Click **Apply** to see your changes.

**Step 6** If you are satisfied with the content and appearance of the login window, click **Save Configuration**.

Once authenticated at the external login page of the external web server, a request is sent back to the controller. The controller then submits the username and password for authentication to an external RADIUS server for verification.

If verification at the RADIUS server is successful, the controller web server either forwards the user to the configured redirect URL or to the user's original opening web page.

If verification at the RADIUS server fails, then the controller web server redirects the user back to the customer login URL.

## Web Authentication Using Cisco Building Broadband Service Manager

Cisco Building Broadband Service Manager (BBSM) works with Cisco access-layer LAN and wireless LAN products (Figure 26) to provide a complete solution that enables businesses, venues and service providers to create, market and operate broadband access services in markets such as public hotspots, enterprise, health care and retail. The Enterprise can securely offer their guest's access to the Internet over existing networks.

For more details on configuring BBSM for Web Authentication, please refer to the *Cisco BBSM 5.3 Configuration Guide*.



#### Figure 26 Guest Access Deployment Using BBSM.

#### **Configuring the BBSM Server to Authenticate Guest Traffic**

Using the address change wizard, follow these steps to configure the BBSM server to authenticate guest traffic:

- Step 1 Choose IP Addresses. Figure 27 appears.
- Step 2 Enter the range of DHCP Start and End addresses to which guest access is allowed.

These IP addresses should be served by the BBSM or external DHCP server.

**Step 3** Enter the Management Start and End addresses.

The management addresses define the range of IP addresses that will pass through BBSM and will not require redirection for external web authentication. Examples of these devices are routers, switches, and access points.

**Step 4** Enter a starting and ending range of static IP addresses in the Foreign Static fields.

Users assigned these addresses will not be able to request dynamic (DHCP) IP address assignment.

Step 5 Click Save.

#### . 🗗 🗡 🎒 IP Addresses - WebConfig - Micros File Edit View Favorites Tools Help 🗘 Back 🔹 🤿 🖌 🙆 🖄 🔹 🐼 Back 🐨 Favorites 🛞 Media 🍏 🖏 🗸 ▪ ⊘Go Links × Address 💩 http://localhost:9488/webconfig/portip.asp Dashboard | Help | Logout 🔺 Building Broadband Service Manager WEBconfig BBSM Server Settings CISCO SYSTEMS IP Addresses **IP Addresses** սին Sites Routers Network Elements BBSM Internal Network Address Ranges • Port Test Settings The BBSM TCP/IP properties cannot be changed or updated in the IP Addresses web page. Use the BBSM Address 🗉 Billing 10.193.193.20 DHCP Start Security/SSL DHCP End 10.193.193.200 • Bandwidth Reservation Management Start 10.193.193.4 Change Wizard to make any Custom Page Sets changes. Management End 10.193.193.5 Walled Garden Foreign (Static) Start CAUTION: Do not use the Network and Dial-up Connections feature in Windows to change IP 10.193.193.201 Port Hopping Foreign (Static) End 10.193.193.254 • WEB Printing Alerts **BBSM TCP/IP Properties** addresses. Internal NIC IP Address 10.193.193.3 Subnet Mask 255.255.255.0 External NIC IP Address 192,168,1.9 Subnet Mask 255.255.255.0 Default Gateway 192.168.1.1 Requery Save - 0 🔐 Local intranet 🙆 Done 🏽 🔀 Start 🛛 🍝 😂 🖉 🖉 IP Addresses - WebCo... 🔩 🎫 🔥 🛛 11:53 AM

Figure 27 Entering Internal Network Addresses for BBSM Server to Support Authentication

#### **Enabling DNS Forwarding**

After entering the appropriate internal IP addresses for the BBSM server, enable DNS forwarding on the server.

Domain Name System (DNS) forwarding allows DNS requests to be relayed to a remote DNS server.

BBSM is not configured as a DNS server; instead it acts as a DNS forwarder for its clients and its own DNS requests. These DNS requests, such as a request for www.cisco.com, are mapped with their IP addresses so that the Internet routers can locate the web server with the content.



If BBSM cannot locate an IP address, it responds with its own internal IP address when the server is pinged. If the IP address that the browser requests cannot be located, BBSM displays a Network Error page or the browser displays a DNS fail page.

You must obtain an IP addresses for your DNS server from your ISP before you can perform this procedure.

To enable DNS forwarding on your server, follow these steps:

- **Step 1** Choose **Start > Programs > Administrative Tools > DNS**. The DNS window appears.
- Step 2 From the left pane, right-click your BBSM server name and choose Properties. The BBSM Properties dialog box for that server appears (Figure 28).

Figure 28 Configuring DNS Forwarding in the Server Properties Window

1 DNS	BBSM53 Properties
Action       Yew       Image: Console       Yew       Yew       Image: Console       Yew       Yew </td <td>Poinalodes help reduce any DNS quelles not antivered by this servel.  To add a forwarder; type is IP address, and then click Add.  IP address:  Add  IP 20 169 189  Emove  Dewn  Eorward time-out (seconds):  Do got use recursion</td>	Poinalodes help reduce any DNS quelles not antivered by this servel.  To add a forwarder; type is IP address, and then click Add.  IP address:  Add  IP 20 169 189  Emove  Dewn  Eorward time-out (seconds):  Do got use recursion
	OK Cancel Apply

- Step 3 Click the Forwarders tab.
- **Step 4** Check the **Enable forwarders** box.

<sup>&</sup>lt;u>Note</u>

**Step 5** In the IP address field, enter the DNS server IP address provided by your ISP and click **Add**.

If you have more than one DNS server IP address, continue to enter them and click **Add** until they are all in the list. Enter the primary DNS server first. It will appear first in the list. Enter the secondary DNS server second.

Step 6 Click OK. Close the DNS window.

#### **Defining an Access Interface**

After enabling DNS forwarding, an access interface is defined on a Layer 3 switch or router interface.



A router is configured if all users are on the same network. In this example, the router address is used as a loopback address. If the end users are on a different subnet, define the router that is closest to the end users. The router should be configured in advance.

Note

If in Layer 3 mode, SNMP communication to the router is used to track MAC addresses of end users and to define the SNMP string that is used for communication between the BBSM and the router.

To define an access interface on either a switch or router, follow these steps:

- Step 1 From the Dashboard, choose WebConfig > Network Elements > Site > Switch.
- **Step 2** Select the **Null:Clients connect to router switch** option from the Switch Type drop-down menu (Figure 29).

By selecting this option, BBSM will not try to discover the hosts behind this switch to track their MAC addresses.

Network Elements - Switches	- WEBconfig - Microsoft Internet Exploi	rer	
File Edit View Favorites Tools	s Help		100 A
🕁 Back 🔹 🤿 🖌 🙆 🔂	Search 💽 Favorites 🛞 Media 🎯	B- 3	
Address 🕘 http://localhost:9488/web	config/switches.asp?nChild=5&type=Switche	es&site=1	▼ 🖓 Go Links ≫
Buildi WEBco	ng Broadband Service <sup>nfig</sup>	Manager	🛓 Dashboard   Help   Logout 🔺
BBSM Server Settings IP Addresses Sites Routers	Cisco Systems illitictillitic	Nets	work Elements - Switches
Robuers Network Elements Site 1 — Site Access Points CMTS Switches Port Test Settings Billing Security/SSL Bandwidth Reservation Custom Page Sets Walled Garden	Site Information Cluster Number Cluster Member No. Switch Type Cluster/Switch IP Address SNMP Password Router	1 Site 1 Go 1 NULL: Clients connect to router 199.199.199.199 Aging Period 300 seconds private Packet Inactivity Period Seconds 127.0.0.1 No. of Client Ports 23	No. of Client Ports: Enter the number of ports on the switch that can be used by clients. Cluster/Switch IP Addr: Enter the unique IP address from the management address range assigned to this switch. Aging Period: Enter the number of seconds the switch waits before deactivating inactive clients.
walled Garoen	Disable Switch	Port Settings	Port Settings: Use this button to configure all ports on the selected switch. Note: For details about packet inactivity period and switch clusters, refer to the online documentation.
	New	Cluster/Switch New Cluster Member	•
🙆 Done			Local intranet
🏽 🕄 🈹 🎼 🕅 🛃 🛃 🛃 🛃	work Elements Ybbsm-1 - Paint		Local Intranet

Figure 29 Network Elements Page

- **Step 3** Leave the default values for the remaining fields and click **Save**.

**Note** Details for each switch field is provided in Table 3 below.

The **Network Elements Port Settings** page appears. This page is used to define the web page that will be displayed to visiting guests.

Note

If port configuration records already exist, the **Network Element Port Settings** window does not pop up automatically. Click **Port Settings**.

Step 4 Enter the applicable information in the Network Element Port Settings window based on the information in Table 4 and click Submit. A dialog box appears, asking you to verify your changes. Click OK.

You are returned to the Switches web page.

Field	Description				
Site Information	Displays the site number and name associated with the switch to be configured.				
Cluster Number	Displays the cluster number and cluster member number associated with the				
Cluster Member No.	switch to be configured.				
Go	Click <b>Go</b> to advance to another previously configured switch.				
Switch Type	Choose a switch type. For this example, we select <i>Null:Clients connect to router switch</i> .				
Cluster/Switch	Enter a unique IP address in the management range assigned to the cluster or				
IP Address	switch. Check with the person installing your clusters and switches if you are unsure of this IP address.				
SNMP Password	Enter the SNMP read-write community string (password) that is used when				
	communicating with switches. (Non-Cisco stackable switches, which share				
	the same stack, are installed with the same password.) The default is <i>public</i> .				
	<b>Note</b> Cisco strongly recommends that the default password on the switches and on BBSM be changed because the default password is well known and could compromise network security.				
Router	From the drop-down menu, choose the IP address of the router to which this site and cluster are connected. If the site and cluster are directly connected to the BBSM server, use the default IP address for the BBSM server, which is <i>127.0.0.1</i> .				
Disable Switch	Check this check box if you do not want BBSM to look for clients on the cluster ports. Use when troubleshooting.				
	Even if you disable a switch, its IP address remains reserved. If you need to reuse the IP address for a different switch, change the IP address of the disabled switch temporarily. If you do not change the IP address, you will not be able to update WEBconfig.				
Aging Period (in seconds)	Enter a time period, in seconds, that the network device will wait before eliminating inactive clients from its internal tables. This period also indicates at what interval BBSM automatically signs off the client. The default time period is 300 (5 minutes).				
Packet Inactivity					
Period (in seconds)	<b>Note</b> This field is disabled unless your switch type supports packet inactivity.				
	Enter a time, in seconds, that a user can be idle before being automatically signed off by BBSM. If needed, refer to the <i>Cisco BBSM Products Network Device Compatibility Guide</i> to verify the switches that monitor for packet inactivity.				
No. of Client Ports	Enter the number of ports that can be used as clients on switch 1 of the cluster. The default is 23.				
VLANs (Apply to	Clients VLAN ID: Displays the client VLAN ID.				
dual VLANs only)	Mgmt VLAN ID: Displays the management VLAN ID.				

#### Table 3 Switch Fields and Descriptions

Field	Description			
Туре	Displays the network device type.			
Location Prefix	Enter a location prefix (optional). You can enter up to 40 characters.			
Page Set	Choose a Page Set from the drop-down menu. For more details on the initial system defaults for this option, refer to Chapter 18 of the <i>Cisco BBSM 5.3 Configuration Guide</i> .			
	Caution You cannot use an SSL page set if your SSL certificate is not installed. Choose the <i>Clear</i> version of the page set until you install the certificate, and then change your page set to the SSL page set. For example, select <b>RADIUSClear</b> until the certificate is installed, then after installing the certificate, change the page set to <b>RADIUS</b> . If you install the SSL page set before installing the certificate, the Start page will not display.			
	Note For CMTSs, the page set that you choose is the default page set that will be applied to the CMTS dynamic port-room configuration. For more details refer to Chapter 13 of the <i>Cisco BBSM 5.3 Configuration Guide</i> .			
Start Page	BBSM automatically enters the starting page for the network device based on the page set; however, you can enter a different starting page.			
Bandwidth	Enter a bandwidth throttling value in kbps for clients connected to this network device. Bandwidth management must be turned on for this option to be effective. For more details, please refer to Chapter 9 of the <i>Cisco BBSM 5.3 Configuration Guide</i> . If the end user selects a bandwidth from the Connect page, that selection overrides this default bandwidth.			
Enable Port Hopping	Check this option box to enable port hopping.			
Client IP Address	This field appears only if you are using multinet.			
Range (DHCP)	If you are using multiple networks, click the default multinet number for clients connected to this network device: Multinet 1 or Multinet 2.			
	<b>Note</b> The Connect page overrides this setting if the end user selects a public or private IP address.			

 Table 4
 Port Setting Fields and Descriptions
### **Defining Access Codes (Temporary Credentials)**

After defining the access interface, you are ready to define the Internet access code for the guests. With BBSM, Internet access is defined (purchased) in one of two ways:

- **Specified date range (start and end date and time)**—A specified time period is purchased when the reservation is made for the access code or at the time the access code is used.
- **Specified duration (in minutes, hours, days, or weeks)**—Access codes are based on the duration of usage instead of a specific time period. Bandwidth throttling (instead of bandwidth reservation) is used because BBSM has no way of preventing oversubscription. When the user logs onto the Internet using access codes by duration, a disconnect window displays the time remaining.



Before creating and configuring access codes, you must choose a bandwidth management option on the BBSM Server Settings web page and, if you are using bandwidth reservation, configure reservation on the Bandwidth Reservation web pages. For more details, please refer to the "Configuring Bandwidth Reservation" section in Chapter 17 of the *Cisco BBSM 5.3 Configuration Guide*.

To define guest access authentication parameters, follow these steps:

- Step 1 From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.
- **Step 2** In the Bandwidth Management area, verify that you chose *Throttling* or *Reservation* in the Access Code Bandwidth field. This option enables bandwidth throttling or reservation for access codes.
- **Step 3** Click **Dashboard** in the upper right-hand corner and then click **Access Code Management**. The Codes by Date web page appears. This web page is used to create access codes based on date range. The page differs depending on the access codes bandwidth options that you configured on BBSM Server Settings web page in WEBconfig:
  - **None**—If you chose *None* from the Access Codes Bandwidth drop-down menu, the bandwidth defaults to Full Speed and that displays in the Manage Codes web page.
  - **Throttle**—If you chose *Throttle* from the Access Codes Bandwidth drop-down menu, the Manage Codes web page appears without the Bandwidth Class of Service options.
  - **Reservation**—If you chose *Reservation* from the Access Codes Bandwidth drop-down menu, the Manage Codes web page appears with Bandwidth Class of Service options.
- **Step 4** Option 1: To create Access Codes by date, select the Codes by Date tab (Figure 30).

Option 2: To create Access Codes by duration, select the Codes by Duration tab.

Enter the appropriate values to define access for the guest given the assignment option chosen.

odes by	y Date - Mic	rosoft Int	ernet Expl	orer			<u>[8]</u>
Edit	View Fav						
Back 🝷	⇒ • 🖄	2 4	Q Search	🗼 Favori	tes 🌒	1edia 🎯 🛙	3- <b>3</b>
ress	http://localh	nost:9488/a	ccesscodes1	/ManageCo	des.asp		▼ (∂Go Links
À.		Build Access	ing Br Code N	<b>oadb</b> Ianage	and S ment	ervice	Manager         Dashboard   Help   Logout           Codes by Date           Codes by Duration   Find Access Codes   View by Year
ISCO ST	.1.						Access Codes by Date
alenda << <	May 2	:005 >			-All Custo	_	Customers Access Codes
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Site 1 Click calendar at left to choose a start date.
1	2	3	4	5	6	7	Name sujit Set Start Date 5/14/2005
8	9	10	11	12	13	14	Time 12 • : 00 • AM •
U	3	10		12	13	14	Click calendar at left to choose an end date.
15	16	17	18	19	20	21	Click customer name for details. Set End Date 5/31/2005
							Names that cannot be dicked belong to another site.
22	23	24	25	26	27	28	Access Code Price USD ea
29	30	31					Length of Codes 5 J digits
							Bandwidth Full-Speed
Res	servations					Today	
No	Reservatio	ns					View Access Codes New Requery Save Delete
							new Requery Dave Delete
10							Cocal intranet
itart	🗹 🥭 🕻	ji  ] (€) Ci	odes by Da	ate - Micro	)		💐 🦉 🔂 🐁 12:14 PM

Figure 30 Access Code Management > Codes by Date Page

Step 5 Click Save.

۵,

**Note** If you modify a reservation while guests defined for that reservation are connected, bandwidth changes are not applied.

Step 6 Click View Access Codes button to verify configuration. The window seen in Figure 31 appears.

File Edit View F	=avorites Tools He	lp					<u>8</u>
🕁 Back 🔹 🔿 👻 🙆	🕽 😰 🖓 🧔 Searc	:h 📓 Favorites 🌒	Media 🧭 🖧 🎒				
Address 🕘 http://loc	alhost:9488/accesscode	es1/ViewEditCodes.asp?	'instID=3&viewType=date				💌 🤗 Go Links
	Building E	Broadband \$	Service Manage	ər		Da	shboard   Help   Logout
Alt.	Access Code	Management					
			Codes by D	ate   Codes by I	Duration	Find Access Co	des   View by Year
CISCO SYSTEMS						View Acces	s Codes - <u>Codes by Date</u>
Միսմիս							
	115 Marca 1	and the design of the dd					
Click Edit to	o modify the valu	es displayed in tr	ie table.				
Customer	Price	Bandwidth	Start Date	End Date	Class of Service	Access Codes	Edit Printable
iest-new	0.00 USD	Full-Speed	May 14 2005 12:00AM	May 31 2005 12:00AM	None	33385	
						75509 55309	
						89342	
						97108	
						65187 37177	
						71401	
						40615 79102	
						/9102	
							- Mart
Done							🔠 Local intranet

#### Figure 31 View Access Codes Page



You can find access codes and reservations by customer name by selecting the Find Access Codes tab.



To find reservations by date, choose Access Code Management > View by Year.

## **Modifying PC to Support Wireless Guest Access**

After you have defined the access codes using BBSM, you need to make changes to the client on the guest user's PC to support guest access.

The Microsoft Wireless Client on your PC requires minimal changes to support guest access.

To support guest access on your PC, follow these steps:

- **Step 1** From your Windows Start button, launch the **Settings > Control Panel**.
- Step 2 Click the Network and Internet Connections icon.
- Step 3 Click the Network Connections icon.
- Step 4 Right click the LAN Connection icon and select Disable.
- Step 5 Right click the Wireless Connection icon and select Enable.
- Step 6 Right click the Wireless Connection icon again and select Properties.

- Step 7 From the Wireless Network Connection Properties window, select the Wireless Networks tab.
- **Step 8** Change the Network Name in the **Preferred Network** area. Remove the old SSID and then click on the **Add...** button.
- **Step 9** In the Association tab, type in the Network Name (SSID) value you will be using for Web Authentication.



Notice that WEP is enabled. You must disable WEP for Web authentication to work.

**Step 10** Select **OK** to save the configuration.

When you are actively communicating with the wireless LAN you will see a beacon icon in the preferred network box.

# **Client Login**

Once the web authentication method is defined and the client changes are made to the guest user's PC, the user can log on.

To log on as a guest user, follow these steps:

Step 1 Open a browser window and enter the IP address of the authenticating server (Figure 32).



Figure 32 Client Login Page

leb Authenticati	on - Microsoft Internet Explorer		
Edit View Fav	orites Tools Help	Reflection Company and a second second	
Back + 🕤 -	💌 😰 🏠 🔎 Search 🤶 Pavor	ntes 🚷 Media 🔗 🍰 🍶 🗔	
📾 🙋 https://1.1.)	.1/login.html		💌 🛃 Go Unite
_ogin			Cisco Systems
Welcome to t	he Cisco wireless network		
	to provide the Wireless LAN infrastructure Please login and put your air space to wor		
for your network.	Prease login and putyour air space to wor	ĸ	
User Name	cisco123		
Password	•••••		
	Submit		
one			🔒 😨 Internet
			🔦 🖉 🍢 🔯 1254P

- **Step 2** Enter the username and password provided.
- **Step 3** If your login is successful, a browser window noting a successful login appears (Figure 33).





# Troubleshooting

This section provides debugging tips for specific features.



CLI commands and key sections of the debugging script are highlighted in bold.

## **Debugging Mobility Anchor**

Mobility hand off and mobility directory debug commands display the guest-tunnel or AnchorExport debugging information in addition to the traditional mobility debugging information.

You will see mobility exchanges [MobileAnchorExport messages (on Foreign) & MobileAnchorExportAck (on Anchor)] when enabling mobility hand off and mobility directory debugs.

Debugging guest tunneling and the Ethernet over IP are both included in the regular mobility debugs:

debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable

While the data source port is being diagnosed, look for UDP packets with Source/Destination Port=16666. Any EoIP packets can be filtered by using the display filter *etherip* in the capture taken.

#### **Debug Scripts from the Foreign Controller**

```
(Cisco Controller) > show debug
Debug Flags Enabled:
arp error enabled.
bcast error enabled.
dhcp packet enabled.
dot11 mobile enabled.
dot11 state enabled
mobility directory enabled.
mobility handoff enabled.
pem events enabled.
pem state enabled.
(Cisco Controller) > show time
Time..... Tue Feb 14 13:47:31 2006
Timezone delta..... 0:0
Daylight savings..... disabled
NTP Servers
  NTP Polling Interval.....
                                     86400
                NTP Server
   Index
    _____
```

(Cisco Controller) > Tue Feb 14 13:47:40 2006: Scheduling deletion of Mobile Station: 00:40:96:a9:fa: a0 (callerId: 24) in 5 seconds Tue Feb 14 13:47:40 2006: Updated location for station 00:40:96:a9:fa:a0 - old AP 00:00:00:00:00:00-0, new AP 00:0b:85:23:cc:50-0 Tue Feb 14 13:47:40 2006: Association received from mobile 00:40:96:a9:fa:a0 on AP 00:0b:85:23:cc:50 Tue Feb 14 13:47:40 2006: Initializing policy for mobile 00:40:96:a9:fa:a0 Tue Feb 14 13:47:40 2006: pem\_api.c:1785 - State Update 00:40:96:a9:fa:a0 from START (0) to AUTHCHECK (2) Tue Feb 14 13:47:40 2006: pem\_api.c:1873 - State Update 00:40:96:a9:fa:a0 from AUTHCHECK (2) to L2AUTHCOMPLETE (4) Tue Feb 14 13:47:40 2006: Plumbed mobile LWAPP rule on AP 00:0b:85:23:cc:50 for mobile 00:40:96:a9:fa:a0 Tue Feb 14 13:47:40 2006: pem\_api.c:2006 - State Update 00:40:96:a9:fa:a0 from L 2AUTHCOMPLETE (4) to DHCP\_REQD (7) Tue Feb 14 13:47:40 2006: Changing state for mobile 00:40:96:a9:fa:a0 on AP 00:0b:85:23:cc:50 from Probe to Associated Tue Feb 14 13:47:40 2006: Session Timeout is 1800 - starting session timer for STA 00:40:96:a9:fa:a0 Tue Feb 14 13:47:40 2006: Scheduling deletion of Mobile Station: 00:40:96:a9:fa:a0 (callerId: 49) in 1800 seconds Tue Feb 14 13:47:40 2006: Sending Assoc Response to station 00:40:96:a9:fa:a0 on BSSID 00:0b:85:23:cc:50 (status 0) Tue Feb 14 13:47:40 2006: Changing state for mobile 00:40:96:a9:fa:a0 on AP 00:0b:85:23:cc:50 from Associated to Associated Tue Feb 14 13:47:40 2006: Mobility query, Mobile: 00:40:96:a9:fa:a0 PEM State: DHCP\_REQD Tue Feb 14 13:47:40 2006: Mobility packet sent to: Tue Feb 14 13:47:40 2006: 40.1.3.10, port 16666, Switch IP: 10.10.50.2 Tue Feb 14 13:47:40 2006: type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 20 seq: 21 len 120 Tue Feb 14 13:47:40 2006: group id: 8980c166 1ac12d02 a250ca56 49c7b762 Tue Feb 14 13:47:40 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 13:47:40 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 13:47:41 2006: Mobility packet sent to: Tue Feb 14 13:47:41 2006: 40.1.3.10, port 16666, Switch IP: 10.10.50.2 Tue Feb 14 13:47:41 2006: type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 20 seq: 21 len 120 Tue Feb 14 13:47:41 2006: group id: 8980c166 1ac12d02 a250ca56 49c7b762 Tue Feb 14 13:47:41 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 13:47:41 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 13:47:41 2006: Mobility packet retry:, Client: 00:40:96:a9:fa:a0 Peer IP: Groupcast, Anchor IP: 0.0.0.0 Tue Feb 14 13:47:43 2006: DHCP proxy received packet, src: 0.0.0.0, len = 300 Tue Feb 14 13:47:43 2006: dhcpProxy(): dhcp request, client: 00:40:96:a9:fa:a0: dhcp op: 1, port: 1, encap 0xec03, old mscb port number: 1 Tue Feb 14 13:47:43 2006: Dropping DHCP during mobility, chaddr: 00:40:96:a9:fa:a0 siaddr: 0.0.0.0 Tue Feb 14 13:47:43 2006: Attempting anchor export for mobile 00:40:96:a9:fa:a0 Tue Feb 14 13:47:43 2006: Anchor Export: Client: 00:40:96:a9:fa:a0 Client IP: 0.0.0.0, Anchor IP: 40.1.3.10 Tue Feb 14 13:47:43 2006: Mobility packet sent to: Tue Feb 14 13:47:43 2006: 40.1.3.10, port 16666, Switch IP: 10.10.50.2 Tue Feb 14 13:47:43 2006: type: 16(MobileAnchorExport) subtype: 0 version: 1 xid: 21 seg: 22 len 244 Tue Feb 14 13:47:43 2006: group id: 8980c166 1ac12d02 a250ca56 49c7b762 Tue Feb 14 13:47:43 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 13:47:43 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 13:47:43 2006: Mobility Response: mobile 00:40:96:a9:fa:a0IP 0.0.0.0 code 1, reason 6, PEM State DHCP\_REQD, Role Unassociated(0) Tue Feb 14 13:47:43 2006: Mobility packet received from: Tue Feb 14 13:47:43 2006: 40.1.3.10, port 16666, Switch IP: 40.1.3.10 Tue Feb 14 13:47:43 2006: type: 17(MobileAnchorExportAck) subtype: 0 version: 1 xid: 21 seq: 15 len 272

Tue Feb 14 13:47:43 2006: group id: 8980c166 1ac12d02 a250ca56 49c7b762 Tue Feb 14 13:47:43 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 1 Tue Feb 14 13:47:43 2006: VLAN IP: 10.10.60.3, netmask: 255.255.255.0 Tue Feb 14 13:47:43 2006: Received Anchor Export Ack: 00:40:96:a9:fa:a0 from Switch IP: 40.1.3.10 Tue Feb 14 13:47:43 2006: Anchor IP: 40.1.3.10 Old Foreign IP: 10.10.50.2 New Foreign IP: 10.10.50.2 Tue Feb 14 13:47:43 2006: mobility role update request from Unassociated to Export Foreign for mobile 00:40:96:a9:fa:a0 Peer = 40.1.3.10, Old Anchor = 40.1.3.10, New Anchor = 40.1.3.10 Tue Feb 14 13:47:43 2006: pemAdvanceState: State Update 00:40:96:a9:fa:a0, mscb state: DHCP\_REQD from Mobility-Incomplete to Mobility-Complete Tue Feb 14 13:47:43 2006: pem\_api.c:3541 - State Update 00:40:96:a9:fa:a0 from DHCP\_REQD (7) to RUN 20) Tue Feb 14 13:47:43 2006: Plumbing duplex mobility tunnel to 40.1.3.10, as Export Foreign, (VLAN 60) for mobile 00:40:96:a9:fa:a0 Tue Feb 14 13:47:43 2006: Adding Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP: 0.0.0.0 type = Airespace AP Client on AP 00:0B:85:23:CC:50, slot 0 InHandle = 0, ACL Id = 255, Jumbo Frames = NO, interface = 1 802.1P = 0, DSCP = 0, OutHandle = 0 TokenID = Tue Feb 14 13:47:43 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0 (ACL ID 255) Tue Feb 14 13:47:43 2006: Mobility Response: mobile 00:40:96:a9:fa:a0IP 0.0.0.0 code 4, reason 4, PEM State RUN, Role Export Foreign(5) Tue Feb 14 13:47:43 2006: pemAddScb: not sending gratuitous ARP MAC 0:40:96:a9:fa:a0, IP 0.0.0.0, VLAN Id 60

The details about the client can be seen with the command **show client detail** *<mac-address>* and look for the following entries in the script **Mobility State = Export Foreign, Security Policy Completed = Yes** and **Policy Manager State = RUN**.

(Cisco Controller) >show client detail 00:40:96:a9:fa:a0
Client MAC Address
Client UsernameN/A
AP MAC Address
Client State Associated
Wireless LAN Id 1
BSSID 00:0b:85:23:cc:50
Channel
IP Address Unknown
Association Id 1
Authentication Algorithm Open System
Reason Code 0
Status Code 0
Session Timeout 1800
Re-Authentication Timeout 1800
Remaining Re-Authentication Time 1790
QoS Level Silver
Diff Serv Code Point (DSCP) disabled
802.1P Priority Tag disabled
Mobility State Export Foreign
Mobility Anchor IP Address 40.1.3.10
Mobility Move Count 0
Security Policy Completed Yes
Policy Manager State RUN
Policy Manager Rule Created No
Policy TypeN/A
Encryption Cipher None
EAP Type Unknown
Interface guest-vlan
VLAN

```
Client Capabilities:
    CF Pollable..... Not implemented
    CF Poll Request..... Not implemented
    Short Preamble..... Not implemented
    PBCC..... Not implemented
    Channel Agility..... Not implemented
    Listen Interval..... 0
Client Statistics:
    Number of Bytes Received...... 0
    Number of Bytes Sent..... 0
    Number of Packets Received..... 0
    Number of Packets Sent..... 0
    Number of Policy Errors..... 0
    Radio Signal Strength Indicator..... Unavailable
    Signal to Noise Ratio..... Unavailable
Nearby AP Statistics:
               --More-- or (q)uit
     TxExcessiveRetries: 0
                       TxRetries: 0
                                   RtsSuccessCnt: 0
                                                     RtsFailC
nt: 0
      TxFiltered: 0
                 TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
    AP1-cc:50(slot 0) 11 seconds ago..... -29 dBm
    AP1-cc:50(slot 1) 11 seconds ago..... -33 dBm
```

#### **Debugging Script from the Anchor Controller.**

```
(Cisco Controller) > show debug
MAC address...... 00:40:96:a9:fa:a0
Debug Flags Enabled:
    arp error enabled.
    bcast error enabled.
    dot1 mobile enabled.
    dot11 mobile enabled.
    dot11 state enabled
    mobility directory enabled.
    mobility handoff enabled.
    pem events enabled.
    pem state enabled.
```

#### (Cisco Controller) > show time

len 120

Time Tue Feb 14 14:48:03 2006
Timezone delta0:0 Daylight savings disabled
NTP Servers NTP Polling Interval
Index NTP Server
Tue Feb 14 14:48:18 2006: Mobility packet received from:
Tue Feb 14 14:48:18 2006: 10.10.50.2, port 16666, Switch IP: 10.10.50.2
Tue Feb 14 14:48:18 2006: type: 3 (MobileAnnounce) subtype: 0 version: 1 xid: 20 seq: 21

Tue Feb 14 14:48:18 2006: group id: 66c18089 22dc11a 56ca50a2 62b7c749 mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 14:48:18 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 14:48:18 2006: Tue Feb 14 14:48:19 2006: Mobility packet received from: Tue Feb 14 14:48:19 2006: 10.10.50.2, port 16666, Switch IP: 10.10.50.2 Tue Feb 14 14:48:19 2006: type: 3(MobileAnnounce) subtype: 0 version: 1 xid: 20 seq: 21 len 120 Tue Feb 14 14:48:19 2006: group id: 66c18089 22dc11a 56ca50a2 62b7c749 Tue Feb 14 14:48:19 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 14:48:19 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 14:48:21 2006: Mobility packet received from: 10.10.50.2, port 16666, Switch IP: 10.10.50.2 Tue Feb 14 14:48:21 2006: Tue Feb 14 14:48:21 2006: type: 16(MobileAnchorExport) subtype: 0 version: 1 xid: 21 seq: 22 len 244 Tue Feb 14 14:48:21 2006: group id: 66c18089 22dc11a 56ca50a2 62b7c749 Tue Feb 14 14:48:21 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 0 Tue Feb 14 14:48:21 2006: VLAN IP: 10.10.60.2, netmask: 255.255.255.0 Tue Feb 14 14:48:21 2006: Received Anchor Export request: 00:40:96:a9:fa:a0 from Switch IP: 10.10.50.2 Tue Feb 14 14:48:21 2006: Adding mobile 00:40:96:a9:fa:a0 on Remote AP 00:00:00:00:00:00(0)Tue Feb 14 14:48:21 2006: mobility role update request from Unassociated to Export Anchor for mobile 00:40:96:a9:fa:a0 Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 40.1.3.10 Tue Feb 14 14:48:21 2006: Initializing policy for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:48:21 2006: pem\_api.c:1785 - State Update 00:40:96:a9:fa:a0 from START (0) to AUTHCHECK (2) Tue Feb 14 14:48:21 2006: pem\_api.c:1873 - State Update 00:40:96:a9:fa:a0 from AUTHCHECK (2) to L2AUTHCOMPLETE (4) Tue Feb 14 14:48:21 2006: pem\_api.c:2006 - State Update 00:40:96:a9:fa:a0 from L2AUTHCOMPLETE (4) to DHCP\_REQD (7) Tue Feb 14 14:48:21 2006: Received Anchor Export policy update, valid mask 0x0: Qos Level: 0. DSCP: 0. dot1p: 0 Interface Name:, ACL Name: Tue Feb 14 14:48:21 2006: Stopping deletion of Mobile Station: 00:40:96:a9:fa:a0 (callerId: 53) Tue Feb 14 14:48:21 2006: Mobility packet sent to: Tue Feb 14 14:48:21 2006: 10.10.50.2, port 16666, Switch IP: 40.1.3.10 Tue Feb 14 14:48:21 2006: type: 17 (MobileAnchorExportAck) subtype: 0 version: 1 xid: 21 seg: 15 len 272 Tue Feb 14 14:48:21 2006: group id: 66c18089 22dc11a 56ca50a2 62b7c749 Tue Feb 14 14:48:21 2006: mobile MAC: 00:40:96:a9:fa:a0, IP: 0.0.0.0, instance: 1 Tue Feb 14 14:48:21 2006: VLAN IP: 10.10.60.3, netmask: 255.255.255.0 Tue Feb 14 14:48:21 2006: pemAdvanceState: State Update 00:40:96:a9:fa:a0, ms cab state: DHCP\_REQD from Mobility-Incomplete to Mobility-Complete Tue Feb 14 14:48:21 2006: pem\_api.c:3549 - State Update 00:40:96:a9:fa:a0 from DHCP\_REQD (7) to DHCP\_REQD (7) Tue Feb 14 14:48:21 2006: pemAdvanceState:3559 - Adding TMP rule for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:48:21 2006: Plumbing duplex mobility tunnel to 10.10.50.2, as Export Anchor (VLAN 60) for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:48:21 2006: Adding Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP: 0.0.0.0 type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00, slot 0 InHandle = 0, OutHandle = 0 ACL Id = 255, Jumbo Frames = NO, interface = 29 802.1P = 0, DSCP = Tue Feb 14 14:48:21 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0 (ACL ID 255) Tue Feb 14 14:48:21 2006: pemAddScb: Added NPU entry of type 9 for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:48:21 2006: pemAddScb: not sending gratuitous ARP MAC 0:40:96:a9:fa:a0, IP 0.0.0.0, VLAN Id 60 Tue Feb 14 14:48:24 2006: DHCP proxy received packet, src: 0.0.0.0, len = 300 Tue Feb 14 14:48:24 2006: dhcpProxy(): dhcp request, client: 00:40:96:a9:fa:a0: dhcp op: 1, port: 29, encap 0xec05, old mscb port number: 29 Tue Feb 14 14:48:24 2006: mscb->dhcp Server: 0.0.0.0, mscb->dhcpNetmask: 0.0.0.0, mscb->dhcpGateway: 0.0.0.0, mscb->dhcpRelay: 10.10.60.3 VLAN: 60 Tue Feb 14 14:48:24 2006: Local Address: 10.10.60.3, DHCP Server: 10.1.1.11, Gateway Addr: 10.10.60.1, VLAN: 60, port: 29 Tue Feb 14 14:48:24 2006: DHCP Message Type received: DHCP DISCOVER msg

```
Tue Feb 14 14:48:24 2006:
                           op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Feb 14 14:48:24 2006:
                           xid: 729520998, secs: 32774, flags: 0
Tue Feb 14 14:48:24 2006:
                           chaddr: 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006:
                           ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Tue Feb 14 14:48:24 2006: siaddr: 0.0.0.0, giaddr: 10.10.60.3
Tue Feb 14 14:48:24 2006: DHCP request to 10.10.60.1, len 350, switchport 29, vlan 60
Tue Feb 14 14:48:24 2006: mscb->dhcpServer: 0.0.0.0, mscb->dhcpNetmask: 0.0.0.0,
mscb->dhcpGateway: 0.0.0.0, mscb->dhcpRelay: 10.10.60.3 VLAN: 60
Tue Feb 14 14:48:24 2006: DHCP proxy received packet, src: 10.1.1.11, len = 300
Tue Feb 14 14:48:24 2006: DhcpProxy(): Setting dhcp server from OFFER server: 10.1.1.11
    client mac: 00:40:96:a9:fa:a0 offer ip: 0.0.0.0
Tue Feb 14 14:48:24 2006: DHCP EoIP tunnel to foreign 10.10.50.2 client 00:40:96:a9:fa:a0,
len 346
Tue Feb 14 14:48:24 2006: DHCP Message Type received: DHCP OFFER msg
Tue Feb 14 14:48:24 2006: op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Feb 14 14:48:24 2006: xid: 729520998, secs: 0, flags: 0
Tue Feb 14 14:48:24 2006: chaddr: 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: ciaddr: 0.0.0.0, yiaddr: 10.10.60.23
Tue Feb 14 14:48:24 2006:
                           siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Feb 14 14:48:24 2006:
                            server id: 1.1.1.1 rcvd server id: 10.1.1.11
Tue Feb 14 14:48:24 2006: DHCP proxy received packet, src: 0.0.0.0, len = 326
Tue Feb 14 14:48:24 2006: dhcpProxy(): dhcp request, client: 00:40:96:a9:fa:a0:
    dhcp op: 1, port: 29, encap 0xec05, old mscb port number: 29
Tue Feb 14 14:48:24 2006: mscb->dhcpServer: 10.1.1.11, mscb->dhcpNetmask: 0.0.0.0,
mscb->dhcpGateway: 0.0.0.0, mscb->dhcpRelay: 10.10.60.3 VLAN: 60
Tue Feb 14 14:48:24 2006: Local Address: 10.10.60.3, DHCP Server: 10.1.1.11, Gateway Addr:
10.10.60.1, VLAN: 60, port: 29
Tue Feb 14 14:48:24 2006: DHCP Message Type received: DHCP REQUEST msg
Tue Feb 14 14:48:24 2006: op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Feb 14 14:48:24 2006:
                           xid: 729520998, secs: 32774, flags: 0
Tue Feb 14 14:48:24 2006:
                           chaddr: 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
Tue Feb 14 14:48:24 2006:
                           siaddr: 0.0.0.0, giaddr: 10.10.60.3
Tue Feb 14 14:48:24 2006:
                            server id: 10.1.1.11 rcvd server id: 1.1.1.1
Tue Feb 14 14:48:24 2006: DHCP request to 10.10.60.1, len 374, switchport 29, vlan 60
Tue Feb 14 14:48:24 2006: DHCP proxy received packet, src: 10.1.1.11, len = 300
Tue Feb 14 14:48:24 2006: pem_api.c:4284 - State Update 00:40:96:a9:fa:a0 from DHCP_REQD
(7) to WEBAUTH_REQD (8)
Tue Feb 14 14:48:24 2006: pemAdvanceState:4287 - Adding TMP rule for STA 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: Plumbing duplex mobility tunnel to 10.10.50.2, as Export Anchor
(VLAN 60) for mobile 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: Replacing Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP:
10.10.60.23 type = Airespace AP Client - ACL passthru on AP 00:00:00:00:00:00, slot 0
InHandle = 0, OutHandle = 0 ACL Id = 255, Jumbo Frames = NO, interface = 29 802.1P =
Tue Feb 14 14:48:24 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0
(ACL ID 255)
Tue Feb 14 14:48:24 2006: Plumbing web-auth redirect rule due to user logout for
00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: Adding Web RuleID 14 for mobile 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: Assigning Address 10.10.60.23 to mobile 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: DHCP EoIP tunnel to foreign 10.10.50.2
                                                                    client
00:40:96:a9:fa:a0, len 346
Tue Feb 14 14:48:24 2006: DHCP Message Type received: DHCP ACK msg
Tue Feb 14 14:48:24 2006: op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
                          xid: 729520998, secs: 0, flags: 0
Tue Feb 14 14:48:24 2006:
Tue Feb 14 14:48:24 2006:
                           chaddr: 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006:
                           ciaddr: 0.0.0.0, yiaddr: 10.10.60.23
Tue Feb 14 14:48:24 2006:
                           siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Feb 14 14:48:24 2006:
                           server id: 1.1.1.1 rcvd server id: 10.1.1.11
Tue Feb 14 14:48:24 2006: pemAddScb: Added NPU entry of type 2 for STA 00:40:96:a9:fa:a0
Tue Feb 14 14:48:24 2006: Sent an XID frame for mobile 00:40:96:a9:fa:a0
```

At this stage the client is connected and has received a DHCP address from the server. The user now opens the web browser and enters the username *cisco1* and password and completes the web authentication.

Tue Feb 14 14:48:58 2006: Username entry (ciscol) created for mobile 00:40:96:a9:fa:a0
Tue Feb 14 14:48:58 2006: pem\_api.c:4178 - State Update 00:40:96:a9:fa:a0 from
WEBAUTH\_REQD (8) to WEBAUTH\_NOL3SEC (14)
Tue Feb 14 14:48:58 2006: pem\_api.c:4215 - State Update 00:40:96:a9:fa:a0 from
WEBAUTH\_NOL3SEC (14) to RUN (20)
Tue Feb 14 14:48:58 2006: Plumbing duplex mobility tunnel to 10.10.50.2, as Export Anchor
(VLAN 60) for mobile 00:40:96:a9:fa:a0
Tue Feb 14 14:48:58 2006: Replacing Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP:
10.10.60.23 type = Airespace AP Client on AP 00:00:00:00:00:00, slot 0 InHandle = 0,
OutHandle = 0 ACL Id = 255, Jumbo Frames = NO, interface = 29 802.1P = 0, DSCP = 0, To
Tue Feb 14 14:48:58 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0
(ACL ID 255)
Tue Feb 14 14:48:58 2006: pemAddScb: Added NPU entry of type 1 for STA 00:40:96:a9:fa:a0, IP
Address 10.10.60.23, 1Q TAG=0x003c

#### Client logs out of the web authentication session and closes the browser.

Tue Feb 14 14:49:24 2006: Deleting policy rule for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: pem\_api.c:3423 - State Update 00:40:96:a9:fa:a0 from RUN (20) to L2AUTHCOMPLETE (4) Tue Feb 14 14:49:24 2006: pem\_api.c:4401 - State Update 00:40:96:a9:fa:a0 from L2AUTHCOMPLETE (4) to DHCP REOD (7) Tue Feb 14 14:49:24 2006: pemAdvanceState:4405 - Adding TMP rule for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Plumbing duplex mobility tunnel to 10.10.50.2, as Export Anchor (VLAN 60) for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Adding Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP: 10.10.60.23 type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00, slot 0 InHandle = 0, OutHandle = 0 ACL Id = 255, Jumbo Frames = NO, interface = 29 802.1P = 0, DSC Tue Feb 14 14:49:24 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0 (ACL TD 255) Tue Feb 14 14:49:24 2006: pem\_api.c:4420 - State Update 00:40:96:a9:fa:a0 from DHCP\_REQD (7) to WEBAUTH\_REQD (8) Tue Feb 14 14:49:24 2006: pemAdvanceState:4423 - Adding TMP rule for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Plumbing duplex mobility tunnel to 10.10.50.2, as Export Anchor (VLAN 60) for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Replacing Fast Path rule for mobile Mac: 00:40:96:a9:fa:a0, IP: 10.10.60.23 type = Airespace AP Client - ACL passthru on AP 00:00:00:00:00:00, slot 0 InHandle = 0, OutHandle = 0 ACL Id = 255, Jumbo Frames = NO, interface = 29 802.1P = Tue Feb 14 14:49:24 2006: Successfully plumbed mobile rule for mobile00:40:96:a9:fa:a0 (ACL ID 255) Tue Feb 14 14:49:24 2006: Plumbing web-auth redirect rule due to user logout for 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Deleting mobile policy rule -570425345 for 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Adding Web RuleID 15 for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Username entry delete for mobile 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: pemDelScb: removed NPU entry for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: pemAddScb: Added NPU entry of type 9 for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: pemAddScb: Added NPU entry of type 2 for STA 00:40:96:a9:fa:a0 Tue Feb 14 14:49:24 2006: Sent an XID frame for mobile 00:40:96:a9:fa:a0

For details on the client on the anchor controller, enter **show client detail** *(mac-address)* and look for the following information: **Mobility State = Export Anchor, Security Policy Completed = Yes** and **Policy Manager State = WEBAUTH\_REQD** as the user has not completed the web authentication.

Number of Clients	(Cisco Controller		-	1			
00:40:96:92:fs:a0 10.10.50.2       Associated       2       No Mobile 29         Clace Controller) >show client detail 00:40:96:a9:fs:a0.         Client Versamme.       NA         AP MAC Address       00:00:00:00:00:00:00.00.00.00.00.00.00.0	MAC Address	AP Name	Status	WLAN Au			
Client MAC Address							
Client Username	(Cisco Controller	) >show client d	etail 00:40:96:a	9:fa:a0			
AP MAC Address. 00:00:00:00:0000 Client State. Associated Wireless LAN Id. 2 BSSID. 00:00:00:00:00:00:01 Channel. N/A IP Address. 10:10:60.23 Association Id. 0 Authentication Algorithm Open System Reason Code. 0 Session Timeout. 1800 Remaining Re-Authentication Time. 1800 Remaining Re-Authentication Time. 1800 Remaining Re-Authentication Time. 1800 Cos Level. Sliver Diff Serv Code Point (DSCP). disabled Mobility State. Export Anchor Mobility State. 10:10:50.2 Mobility Manager State. 10:10:50.2 Mobility Move Count. 1 Security Policy Completed. No Policy Manager State. Ves NFO Fast Fast Notified. Yes NFO Fast Fast Notified. Yes NFO Fast Fast Notified. Yes NFO Fast Fast Notified. Not implemented CF Pollable. Not implemented Short Preamble. 0 Client Statistics: Number of Bytes Sect. 0 Number of Patcks Received. 0 Number of Patcks Received. 0 Number of Patcks Sect. 0 Number of Patcks Sect. 0 Number of Patcks Received. 0 Number of Patcks Sect. 0 Number of Patck	Client MAC Addres	s		00:40:96:a	9:fa:a0		
Client State	Client Username			N/A			
<pre>Wireless LAN Id</pre>	AP MAC Address			00:00:00:0	0:00:00		
BSID	Client State			Associated	l		
Channel.       N/A         IP Address.       10.10.60.23         Association Id.       0         Authentication Algorithm.       Open System         Reason Code.       0         Status Code.       0         Session Timeout.       1800         Re-Authentication Timeout.       1800         Re-Authentication Timeout.       Biol         Re-Authentication Timeout.       Silver         Diff Serv Code Point (DSCP)       disabled         Mobility State.       Export Anchor         Mobility Move Count.       1         Security Policy Completed       No         Policy Manager Rule Created.       Yes         NPU Fast Fast Notified.       Yes         Policy Type.       N/A         Encryption Cipher       NoA         Encryption Cipher       NoA         Encryption Cipher       Not implemented         CP Pollable       Not implemented         CP Pollable       Not implemented         CP Pollable       Not implemented         CP Poll Request       Not implemented         Short Preamble       0         Number of Bytes Received       0         Number of Packets Received       0	Wireless LAN Id			2			
IP Address.       10.10.60.23         Association Id.       0         Authentication Algorithm.       Open System         Reason Code.       0         Session Timeout.       1800         Remaining Re-Authentication Time       Timer is not running         Mirroring.       Disabled         QoS Level.       Silver         Diff Serv Code Point (DSCP)       disabled         R00.119 Yate       Basoled         R0119 Yate       Basoled         R02.1P Priority Tag.       disabled         R02.1P Yriority Tag.       disabled         R02.1P Yorigin IP Address.       No         Policy Manager State.       WEBAUTH_REQD         Policy Manager State.       No         Recryption Cipher       No         Recryption Cipher       No         CP Policy Presence       Not implemented         CF Poll Request       Not implemented         Short Preamble.       Not implemented         PEC       Not implemented	BSSID			00:00:00:0	0:00:01		
Association Id	Channel			N/A			
Authentication Algorithm	IP Address			10.10.60.2	3		
Reason Code.       0         Status Code.       0         Session Timeout.       1800         Remaining Re-Authentication Time.       Timer is not running         Mirroring.       Disabled         QOS Level.       Silver         Diff Serv Code Point (DSCP).       disabled         802.1P Priority Tag.       disabled         Mobility State.       Export Anchor         Mobility Move Count.       1         Security Policy Completed.       No         Policy Manager Rule Created.       Yes         Policy Manager Rule Created.       Yes         Policy Type.       N/A         Encryption Cipher.       None         EAP Type.       Unknown         Interface.       guest-vlan         VLAN.       60         Client Capabilities:       CF Pollable.         CF Pollable.       Not implemented         Channel Agility.       Not implemented         Dister Interval.       0         Client Statistics:       0         Number of Bytes Received.       0         Number of Packets Sent.       0         Number of Packets Received.       0         Number of Packets Received.       0      N	Association Id			0			
Reason Code.       0         Status Code.       0         Session Timeout.       1800         Remaining Re-Authentication Time.       Timer is not running         Mirroring.       Disabled         QOS Level.       Silver         Diff Serv Code Point (DSCP).       disabled         802.1P Priority Tag.       disabled         Mobility State.       Export Anchor         Mobility Move Count.       1         Security Policy Completed.       No         Policy Manager Rule Created.       Yes         Policy Manager Rule Created.       Yes         Policy Type.       N/A         Encryption Cipher.       None         EAP Type.       Unknown         Interface.       guest-vlan         VLAN.       60         Client Capabilities:       CF Pollable.         CF Pollable.       Not implemented         Channel Agility.       Not implemented         Dister Interval.       0         Client Statistics:       0         Number of Bytes Received.       0         Number of Packets Sent.       0         Number of Packets Received.       0         Number of Packets Received.       0      N	Authentication Al	gorithm		Open Syste	m		
Session Timeout							
Session Timeout	Status Code			0			
Re-Authentication Timeout							
Remaining Re-Authentication Time.       Timer is not running         Mirroring.       Disabled         QOS Level.       Silver         Diff Serv Code Point (DSCP)       disabled         802.1P Priority Tag.       disabled         Mobility State.       Export Anchor         Mobility Foreign IP Address       10.10.50.2         Mobility Move Count.       1         Security Policy Completed.       No         Policy Manager State       WEBAUTH_REQD         Policy Manager State       Yes         NPU Fast Fast Notified.       Yes         Policy Type.       N/A         Encryption Cipher.       None         EAP Type.       Unknown         Interface.       guest-vlan         VLAN.       60         Client Capabilities:       Not implemented         CF Pollable.       Not implemented         Abstring Move of Explose Sectived.       0         Number of Explose Sectived.       0         Number of Packets Received.       0         Number of Packets Sectived.       0         Number of Packets Sective.       0         Number of Packets Sective.       0         Number of Packets Sective.       0         Nu							
Mirroring					ot runn	ina	
QoS Level.SilverDiff Serv Code Point (DSCP)disabledMobility State.Export AnchorMobility State.10.10.50.2Mobility Foreign IP Address10.10.50.2Mobility Move Count.1Security Policy Completed.NoPolicy Manager State.WEBAUTH_REQDPolicy Manager Rule Created.YesPolicy Type.N/AEncryption CipherNoneEAP Type.UnknownInterface.guest-vlanVLAN.60Client Capabilities:60CF PollableNot implementedShort PreambleNot implementedPBCC.Not implementedListen Interval.0Client Statistics:0Number of Bytes Received.0Number of Packets Sent.0Number of Packets Sent.0Number of Packets Sent.0Number of Packets Received.0Number of Packets Received.0Retries 1TxExcessiveRetries 0Retries 2TxExcessiveRetries 1Resources 1TxExteress 1Signal to Noise Ratio.UnavailableNearby AP Statistics:TxExteress 2 <td>-</td> <td></td> <td></td> <td></td> <td>oc raim.</td> <td>1119</td> <td></td>	-				oc raim.	1119	
Diff Serv Code Point (DSCP)	-						
<pre>802.1P Priority Tag</pre>							
Mobility State							
<pre>Mobility Foreign IP Address</pre>	-				hom		
Mobility Move Count.       1         Security Policy Completed.       No         Policy Manager State.       WEBAUTH_REQD         Policy Manager Rule Created.       Yes         NPU Fast Fast Notified.       Yes         Policy Type.       N/A         Encryption Cipher.       None         EAP Type.       Unknown         Interface.       guest-vlan         VLAN.       60         Client Capabilities:       0         CF Pollable.       Not implemented         Short Preamble.       Not implemented         DEC.       Not implemented         Listen Interval.       0         Client Statistics:       0         Number of Bytes Sect.       0         Number of Packets Received.       0         Number of Packets Sectived.       0         Number of Packets Received.       0         Radio Signal Strength Indicator.       Unavailable         Signal to Noise Ratio.       Unavailabl							
Security Policy Completed.       No         Policy Manager State.       WEBAUTH_REQD         Policy Manager Rule Created.       Yes         Policy Type.       Yes         Policy Type.       N/A         Encryption Cipher       None         EAP Type.       Unknown         Interface.       guest-vlan         VLAN.       60         Client Capabilities:       For Pollable.         CF Pollable.       Not implemented         Short Preamble.       Not implemented         PBCC.       Not implemented         DECC.       Not implemented         Listen Interval.       0         Client Statistics:       0         Number of Bytes Received.       0         Number of Packets Sent.       0         Number of Policy Errors.       0         Nearby AP Statistics:       TxExcessiveRetries: 0         R					i		
Policy Manager State							
Policy Manager Rule Created		=					
NPU Fast Fast Notified					ΩD		
Policy Type							
Encryption Cipher							
EAP Type							
Interface							
VLAN							
Client Capabilities: CF PollableNot implemented CF Poll RequestNot implemented Short PreambleNot implemented PBCCNot implemented Channel AgilityNot implemented Listen Interval				-			
CF Pollable			•••••	60			
CF Poll Request	-						
Short Preamble				-			
PBCCNot implemented Channel Agility	-			-			
Channel Agility							
Listen Interval 0 Client Statistics: Number of Bytes Received 0 Number of Bytes Sent 0 Number of Packets Received 0 Number of Packets Sent 0 Number of Policy Errors 0 Radio Signal Strength Indicator Unavailable Signal to Noise Ratio Unavailable Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsFailCnt: 0 TxFiltered: 0				-			
Client Statistics: Number of Bytes Received		-		-	ented		
Number of Bytes Received	Listen Inte	rval		0			
Number of Bytes Sent	Client Statistics	:					
Number of Packets Received 0 Number of Packets Sent		-					
Number of Packets Sent		-					
Number of Policy Errors 0 Radio Signal Strength Indicator Unavailable Signal to Noise Ratio Unavailable Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0	Number of P	ackets Received.		0			
Radio Signal Strength Indicator Unavailable Signal to Noise Ratio Unavailable Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0	Number of P	ackets Sent		0			
Signal to Noise Ratio Unavailable Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0	Number of P	olicy Errors		0			
Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 TxFiltered: 0	Radio Signa	l Strength Indic	ator	Unavailabl	e		
TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0	Signal to N	oise Ratio		Unavailabl	е		
TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0	Nearby AP Statist	ics:					
RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0		TxExcessi	veRetries: 0				
RtsFailCnt: 0 TxFiltered: 0			Т	xRetries: 0			
TxFiltered: 0					Rts	SuccessCnt	: 0
	RtsFailCn						
		TxFiltere					

TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]

# <u>Note</u>

Client details for the anchor controller details have changed and web authentication is complete (see bold text in script below). New values display when the **show client detail** *(mac-address)* is entered for the following values: **Mobility State = Export Anchor, Security Policy Completed = Yes** and **Policy Manager State = RUN.** 

		Status WLAN		otocol Po:	rt
0:40:96:a9:fa:a0				Mobile	29
(Cisco Controller)	> show client d	letail 00:40:96:a	a9:fa:a0		
Client MAC Address	3		00:40:96	:a9:fa:a0	
Client Username			cisco1		
AP MAC Address					
Client State			Associat	ed	
Wireless LAN Id					
BSSID				:00:00:01	
Channel					
IP Address				.23	
Association Id					
Authentication Alg				tem	
Reason Code					
Status Code Session Timeout					
Re-Authentication					
Remaining Re-Authe				not runniu	na
Mirroring					.19
QoS Level					
Diff Serv Code Poi					
802.1P Priority Ta					
Mobility State				nchor	
Mobility Foreign I			-		
Mobility Move Cour					
Security Policy Co	mpleted		Yes		
Policy Manager Sta	ate		RUN		
Policy Manager Rul	le Created		Yes		
NPU Fast Fast Noti	lfied		Yes		
Policy Type			N/A		
Encryption Cipher					
ЕАР Туре				an	
EAP Type Interface			-		
EAP Type Interface VLAN			-		
EAP Type Interface VLAN Client Capabilitie			60		
EAP Type Interface VLAN Client Capabilitie CF Pollable.	es:		60 Not impl	emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ	es: uest		60 Not impl Not impl	emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamb	es: lest		60 Not impl Not impl Not impl	emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC	es: lest		60 Not impl Not impl Not impl Not impl	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil	es: lest ple lity		60 Not impl Not impl Not impl Not impl Not impl	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter	es: uest ple lity		60 Not impl Not impl Not impl Not impl Not impl	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics:	es: uest ble lity cval		60 Not impl Not impl Not impl Not impl 0	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics: Number of By	es: uest ble lity cval ytes Received		60 Not impl Not impl Not impl Not impl 0 0	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics: Number of By Number of By	es: uest ble lity cval		60 Not impl Not impl Not impl Not impl 0 0	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics: Number of By Number of Pa	es: Dest Dle Lity cval ytes Received ytes Sent		60 Not impl Not impl Not impl Not impl 0 0 0 0	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics: Number of By Number of Pa Number of Pa	est ole lity cval ytes Received ytes Sent ackets Received		60 Not impl Not impl Not impl Not impl 0 0 0 0 0	emented emented emented emented	
EAP Type Interface VLAN Client Capabilitie CF Pollable. CF Poll Requ Short Preamk PBCC Channel Agil Listen Inter Client Statistics: Number of By Number of Pa Number of Pa Number of Pa	est ole lity cval ytes Received ytes Sent ackets Received ackets Sent		60 Not impl Not impl Not impl Not impl 0 0 0 0 0 0 0 0	emented emented emented emented	

## **Related Documentation**

The following Cisco documents can provide additional information on the wireless LAN controller:

- Cisco Wireless LAN Controller Configuration Guide, Software Release 4.0, June 2006, Part Number OL-9141-01
- Cisco BBSM 5.3 Configuration Guide, June 2006, Part Number 78-15807-01

This document is to be used in conjunction with the documents listed in the Related Documentation section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

