



# Deployment Guide for Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.1

---

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 10](#)

[“Web Authentication Process” section on page 15](#)

[“Client Login” section on page 31](#)

[“Troubleshooting” section on page 44](#)

[“Related Documentation” section on page 53](#)

## 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. Today, with laptops, networked applications, and digital phone lines, a visiting guest’s effectiveness is severely limited without continued access to these technologies.

Guest networks are network connections provided by a company to enable their guests to gain access to the Internet, and their own enterprise without compromising the security of the host enterprise network.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

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

This document includes various scenarios in which the Cisco Wireless LAN Controller can be used to deploy a guest access solution over the corporate network.

## Terms and Acronyms

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

Term or Acronym	Definition
Cisco WiSM	Cisco Wireless Services Module provides the functionality of the wireless LAN controller for Cisco Catalyst 3750G and Catalyst 6500 switches
Lightweight access point (LAP)	An access point running the Lightweight Access Point Protocol (LWAPP) that makes the access point work with wireless LAN controllers
LWAPP	Lightweight Access Point Protocol—An IETF draft protocol used in the Cisco Unified Wireless Network architecture, a centralized wireless LAN Architecture. LWAPP defines both control and data encapsulation formats used in the Cisco Unified Wireless Network.
WCS	Cisco Wireless Control System—Management software that manages wireless LAN controllers and adds advanced management options such as location-based services
WLAN	Wireless LAN
WLC (or controller)	Cisco wireless LAN controller—Cisco devices that centrally manage lightweight access points and wireless LAN data traffic

## 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 within all wireless networks that require guest access.
- 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 a basic guest access application using the Cisco wireless LAN controller. The configuration shown is applicable for Cisco 2000, 2100, and 4400 series wireless LAN controllers.

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

- All the interfaces on the controller are mapped to physical port 1, and two wireless LANs 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**



## Connecting to the Neighbor Switch

The controller is connected to the neighboring Catalyst 3750 switch using only one 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

Initial configuration of the Cisco wireless LAN controller is accomplished using a console cable connection to the controller. The administrator can configure the system using the automatic Configuration Wizard available on the console port.

**Note**

After the initial configuration, the administrator can configure the Cisco wireless LAN controller using the controller 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 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 ([Figure 1](#)), 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 *secure* (employee) VLAN must be modified from the configuration initially assigned during the configuration wizard process.

**Note**

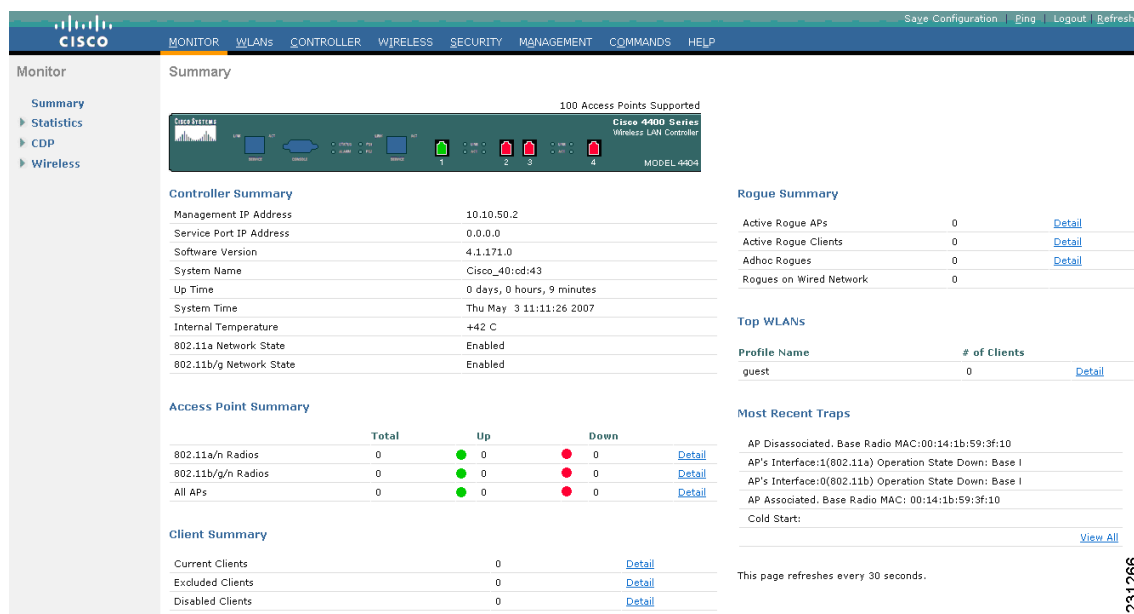
All configuration of the controller from this point forward employs the controller GUI.

To modify the *guest* and *secure* VLAN interfaces using the controller GUI, follow these steps:

- Step 1** Browse to 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.

**Figure 2** Initial Configuration of the Controller as Created by the Configuration Wizard

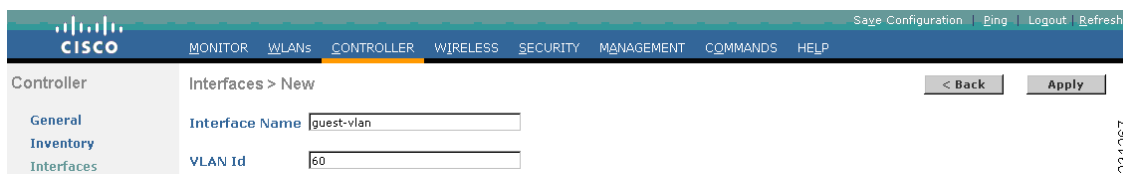


- Step 2** In the controller GUI, choose **Controller > Interfaces**.

- Step 3** Click **New...** to create a dynamic VLAN interface for the *guest* SSID.

In the window that appears, 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 (see [Figure 3](#)).

**Figure 3** Controller > Interfaces > New



- Step 4** Click **Apply**. The window seen in [Figure 4](#) displays.

**Figure 4** *Interfaces > Edit Window*

Controller

Interfaces > Edit

General Information

Interface Name: guest-vlan  
MAC Address: 00:0b:85:40:cd:40

Interface Address

VLAN Identifier: 60  
IP Address: 10.10.60.2  
Netmask: 255.255.255.0  
Gateway: 10.10.60.1

Physical Information

Port Number: 1  
Backup Port: 0  
Active Port: 0  
Enable Dynamic AP Management: ☐

Configuration

Quarantine: ☐

DHCP Information

Primary DHCP Server: 10.10.60.1  
Secondary DHCP Server:

Access Control List

ACL Name: none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

- Step 5** 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 shown in [Figure 5](#) appears and the newly added VLAN is listed.

**Figure 5** *Interface Summary Window Showing Guest and Secure VLAN*

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.10.50.3	Static	Enabled
guest-vlan	60	10.10.60.2	Dynamic	Disabled
management	untagged	10.10.50.2	Static	Not Supported
secure-vlan	30	10.10.30.2	Dynamic	Disabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

- 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.

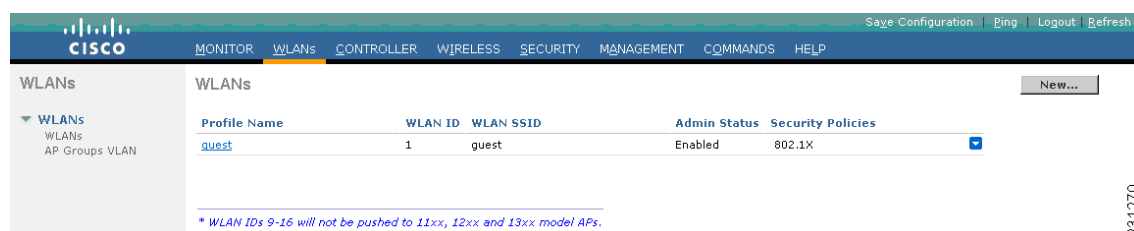
## Modifying the WLAN Instance to Define Security Policies

After configuring the IP address for the guest and secure VLAN interfaces for the wireless LAN, you can define security policies 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 WLANs, follow these steps:

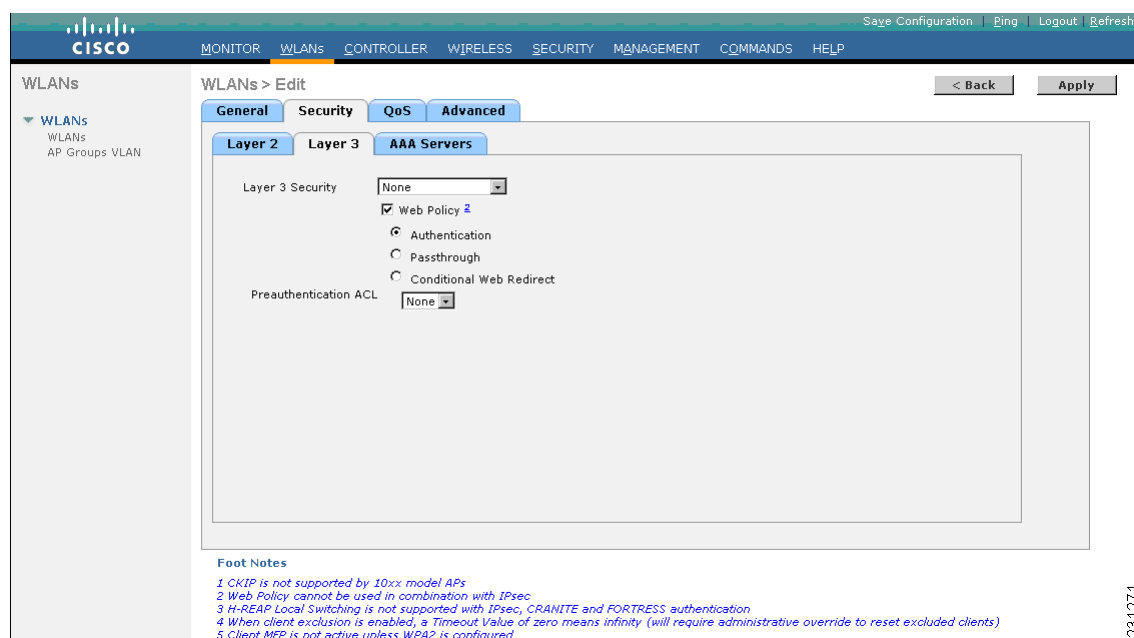
- Step 1** Click **WLANs**. The WLANs summary window appears (see [Figure 6](#)).

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



- Step 2** Click the blue drop-down arrow next to **guest WLAN** and select **Edit**. The window seen in [Figure 7](#) displays.

**Figure 7** WLANs > Edit Window for the Guest WLAN




- Step 3** At the **General Policies** tab, check the **DHCP Relay/DHCP Server IP Addr** check box to verify whether you have a valid DHCP server assigned to the WLAN.

If you have a DHCP server assigned, continue with Step 4.

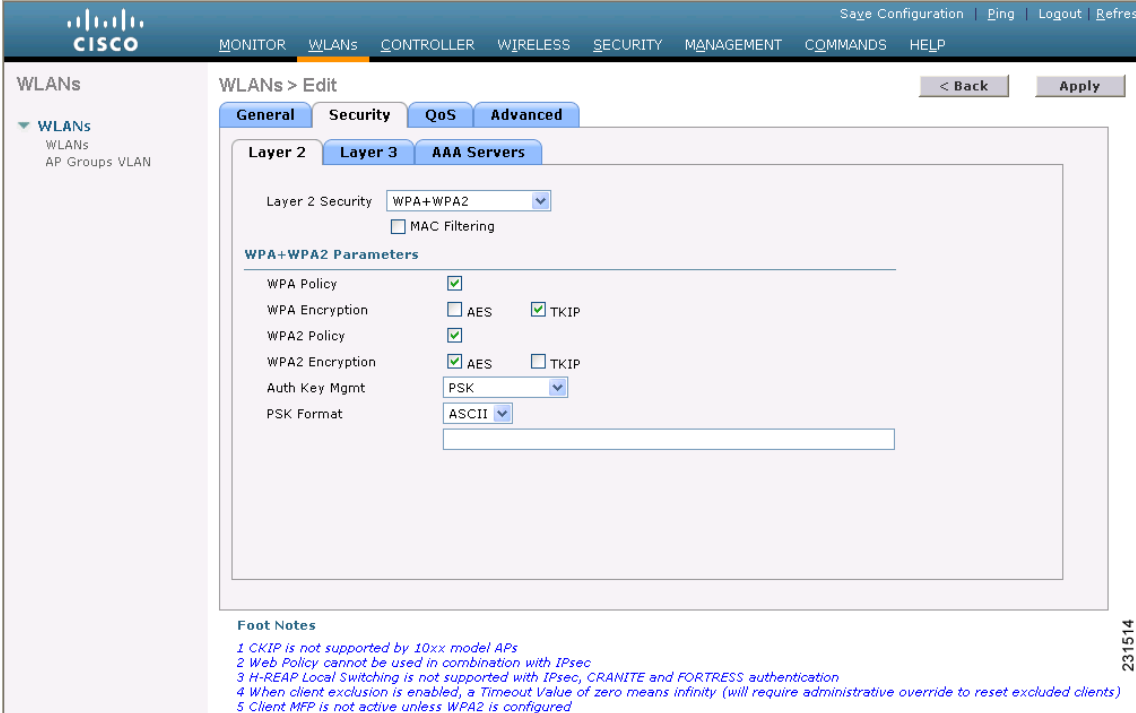
If you have no DHCP server assigned to the WLAN, follow Steps a through e below:

- a. Under **General Policies**, uncheck the **Admin Status** check box.



- b. Click **Apply** to disable the WLAN.
  - c. In the **DHCP Relay/DHCP Server IP Addr** edit box, enter a valid DHCP server IP address for this WLAN.
  - d. Under **General Policies**, check the **Admin Status** check box.
  - e. Click **Apply** to assign the DHCP server to the WLAN and to enable the WLAN. You are returned to the **WLANs** page.
- Step 4** In the upper-right corner of the **WLANs** page, click **Ping** and enter the DHCP server IP address to verify that the WLAN can communicate with the DHCP server.
- Step 5** Select the appropriate **Interface Name** from the drop-down menu located on the **General Policies** tab. 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 6** At the Layer 3 tab, 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 7** Click **Apply** to save edits for the interface on the running configuration of the WLAN switch.
- Step 8** To configure the security policy for the secure WLAN, click the blue drop-down arrow next to **secure WLAN** and select **Edit**.
- Step 9** Repeat Steps 3 through 5, listed above for the *secure* WLAN.
- Step 10** At the Layer 2 tab, select one of the higher security options from the drop-down Layer 2 Security menu such as WPA+ WPA2.

**Figure 8 Assigning Layer 2 Security Policy for the Secure WLAN**



WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

☐ MAC Filtering

**WPA+WPA2 Parameters**

WPA Policy: ☒

WPA Encryption: ☐ AES ☒ TKIP

WPA2 Policy: ☒

WPA2 Encryption: ☒ AES ☐ TKIP

Auth Key Mgmt: PSK

PSK Format: ASCII

**Foot Notes**

1 CKIP is not supported by 10xx model APs  
 2 Web Policy cannot be used in combination with IPsec  
 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication  
 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)  
 5 Client MFP is not active unless WPA2 is configured

**Note**

If you select WPA2 from the Layer 2 Security drop-down menu, you must check the check boxes of both of the WPA Encryption options (**AES** and **TKIP**) for the feature to work.

**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 10.

**Step 11** Click **Apply** to save edits for the interface on the running configuration of the WLAN switch.

## Creating Guest Access Accounts

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.

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 user accounts after logging into the controller using the lobby ambassador account. 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 Lobby Ambassador Option

A lobby ambassador account is used to assign guest access accounts. You can create a lobby ambassador account on the controller through either its GUI or the CLI.

Examples for the CLI and GUI are provided in this section.

### Creating a Lobby Ambassador Account Using the Controller GUI

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

**Step 1** Click **Management > Local Management Users**. The window seen in [Figure 9](#) displays.

**Figure 9** Local Management Users Summary Window

User Name	User Access Mode
admin	ReadWrite

**Note**

This Local Management Users window lists the names and access privileges of the current local management users. You can delete any of the user accounts from the controller by selecting the **Remove** option from the blue arrow drop-down menu next to that account. 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.

**Step 2** Click **New**. The window seen in [Figure 10](#) displays.

**Figure 10** Local Management Users > New Page

**Step 3** In the User Name field, enter a username.

**Step 4** In the Password and Confirm Password fields, enter a password.

**Note**

Passwords are case sensitive.

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

**Note**

The **ReadOnly** option in the User Access Mode menu 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 CLI

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

```
config mgmtuser add lobbyadmin_username lobbyadmin_pwd lobby-admin
```



### Note

Replacing **lobby-admin** with **read-only** in the CLI command, 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 Using the Controller GUI

Follow these steps to create guest user accounts using the controller GUI after you have created the Lobby Ambassador account:

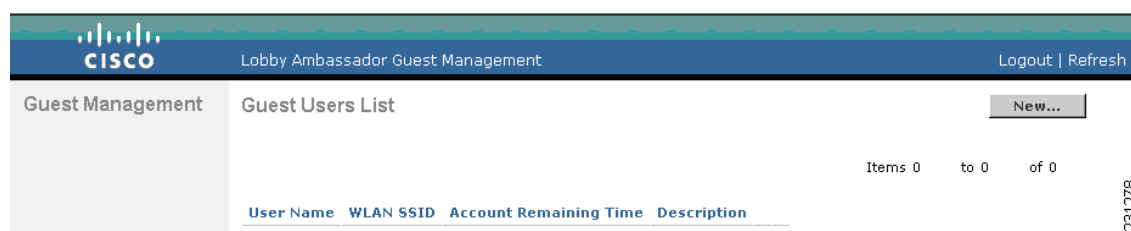


### Note

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 Lobby Ambassador Account Using the Controller GUI](#)” section above.
- The window seen in [Figure 11](#) displays.

**Figure 11** Lobby Ambassador Guest Management > Guest Users List Window



- Step 2** Click **New** to create a guest user account. The window seen in [Figure 12](#) displays.

**Figure 12**      **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.



**Note** 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.



**Note** A value of zero (0) is not valid for the lifetime parameter.

**Default:** 1 day

**Range:** 5 minutes to 30 days



**Note** 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.



**Note** 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 menu, choose the SSID to be used by the guest user. The only WLANs that are listed are those which have Layer 3 web authentication configured. (See the [“Modifying the WLAN Instance to Define Security Policies”](#) section on page 8 for details on configuring security policies).



**Note** 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 (see [Figure 13](#)).

**Figure 13** Lobby Ambassador Guest Management > Guest Users List Summary Window

User Name	WLAN SSID	Account Remaining Time	Description
guest1	guest	1 d	guest1

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.

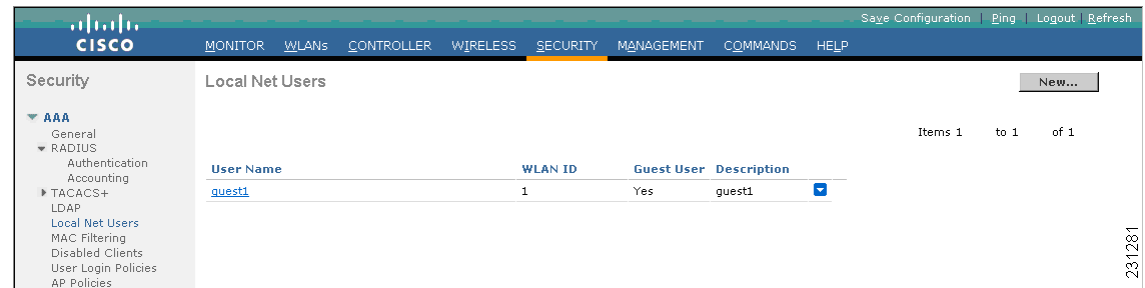
- Step 9** Repeat this procedure to create any additional guest user accounts.

## 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 as seen in [Figure 14](#).

**Figure 14**      **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.

You can edit or remove accounts by clicking the blue arrow drop-down menu and selecting the appropriate option.

## 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 enables 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, on an external web server or on an external database on a RADIUS server.

These four methods are described in the following sections:

[“Web Authentication Using Mobility Anchor Feature on Controller” section on page 16](#)

[“Web Authentication Using an External RADIUS Server” section on page 27](#)

[“Web Authentication Using an External Web Server” section on page 28](#)

[“Modifying the PC to Support Wireless Guest Access” section on page 31](#)

## Web Authentication Using Mobility Anchor Feature on Controller

Guest tunneling provides additional security for guest 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 controller on the network, a Cisco 4100 or 4400 series wireless LAN controller or Cisco WiSM can be used in the DMZ VLAN 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 access to the corporate wireless network across most controller platforms ([Table 1](#)).

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

Software Release/Platform	3.0	3.2	4.0	4.1
Cisco 4100 series wireless LAN controllers	Y	Y	N	N
Cisco 4400 series wireless LAN controllers	Y	Y	Y	Y
Cisco 2000 and 2100 series wireless LAN controllers <sup>1</sup>	N	Y	Y	Y
Cisco 6500 series (WiSM)	---	Y	Y	Y
Cisco 3750 series with integrated wireless LAN controller	---	N	Y	Y
Cisco wireless LAN controller module for Integrated Service Routers <sup>1</sup>	---	Y	Y	Y

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 a dedicated VLAN for guests.
- All user traffic is transported over an Ethernet-over-IP (EoIP) tunnel between the remote controller and the DMZ anchor controller.

Mobility is supported as a client device roams between 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 anchor controller can use the AAA-override feature to apply RADIUS Vendor Specific Attributes (VSAs) on a per-session basis.

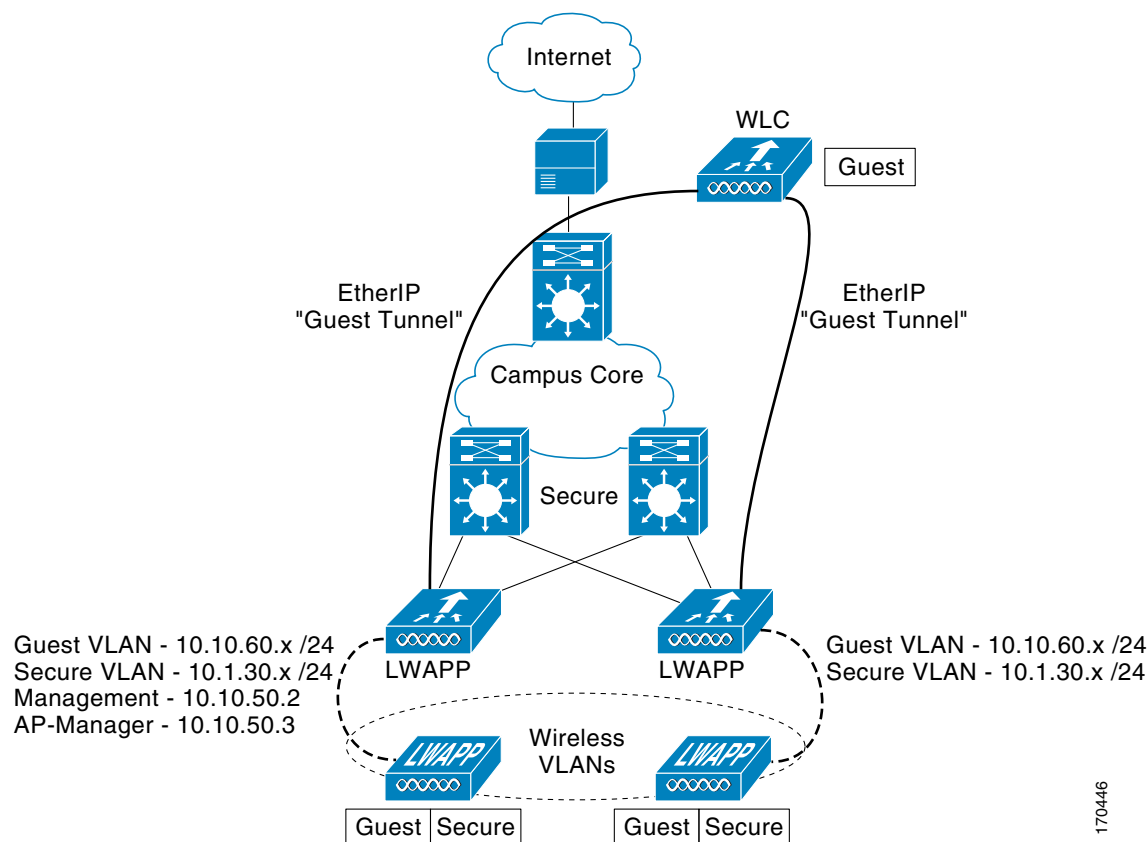
Guest tunneling provides additional security for guest access to the corporate wireless network.



**Note**

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 15** 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 interface off the firewall.

- 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 Mobility Group

To configure a mobility group, follow these steps:

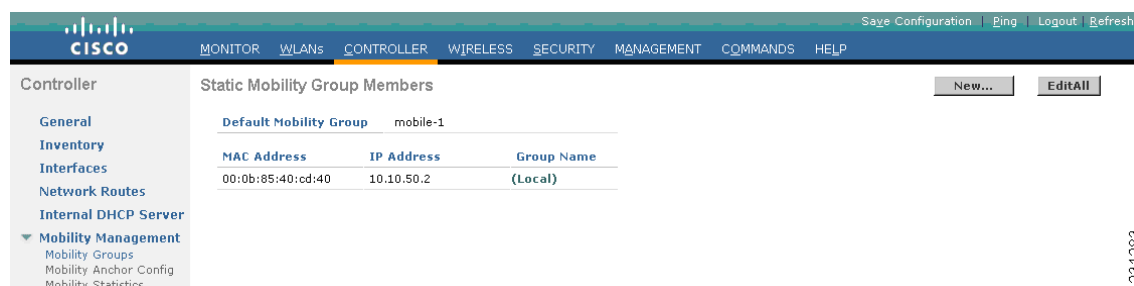
- Step 1** Create a mobility group in the remote and DMZ anchor controller. For this example, we named the mobility group for the remote controller, *mobile-1*; and, we named the mobility group on the DMZ anchor controller, *mobile-9*.



**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 window (see [Figure 16](#)).

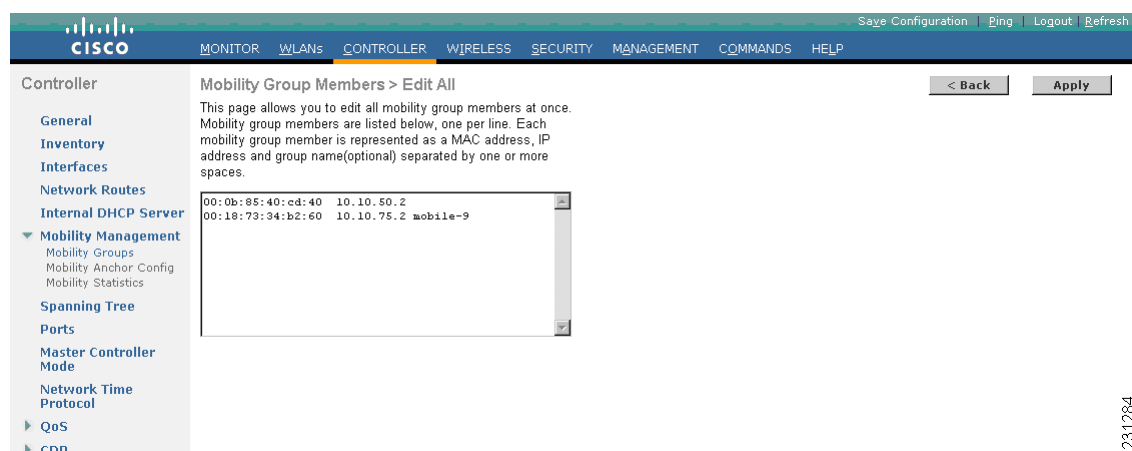
**Figure 16** *Controller > Static Mobility Group Members Window*



231283

- Step 3** Click **Edit All**. The window seen in [Figure 17](#) displays.

**Figure 17** *Mobility Group Members > Edit All*



231284

- Step 4** Enter the MAC address, IP address, and mobility group name of the DMZ anchor controller in the Edit All panel.



**Note** In this example, we use a MAC address of 00:18:73:34:b2:60, an IP address of 10.10.75.2 and a mobility group name of *mobile-9* for the DMZ anchor controller.

- Step 5** At the DMZ anchor controller, choose **Controller > Mobility Groups** to access the Static Mobility Group Members window.

- Step 6** Click **Edit All**.

- Step 7** Enter the MAC address and IP address of the remote controller in the Edit All panel.



**Note** In this example, we use a MAC address of 00:0b:85:40:cd:40 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 WLAN to a single subnet, regardless of a client's entry point into the network. Clients can then access a guest WLAN 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 centralized controllers for a WLAN. 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.

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

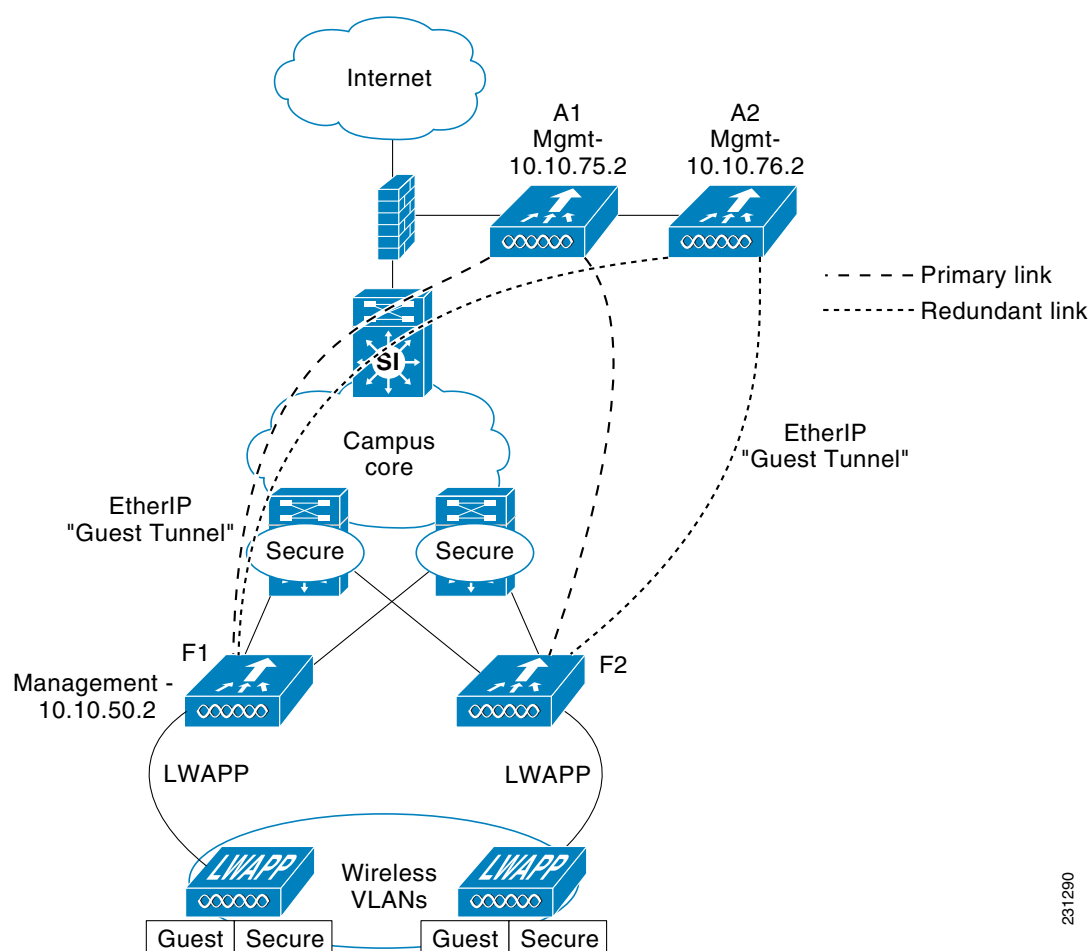
When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are de-encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller de-encapsulates the packets and forwards them to the client.

In controller software releases prior to 4.1, there is no automatic way of determining if a particular controller in a mobility group is unreachable. As a result, the foreign controller may continually send all new client requests to a failed anchor controller, and the clients remain connected to this failed controller until a session timeout occurs.

In controller software release 4.1 and later, mobility group members can send ping requests to one another to check the data and control paths among them to find failed members and reroute clients. You can configure the number and interval of ping requests sent to each anchor controller. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility.

Guest N+1 redundancy (Figure 18) allows detection of failed anchors. Once a failed anchor controller is detected, all of the clients anchored to this controller are de-authenticated so that they can quickly become anchored to another controller. This same functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.

**Figure 18** Redundancy with Guest WLANs to Detect Failed Anchors



**Note**

A 2000 or 2100 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 or 2100 series controller can have a 4400 series controller as its anchor.

231290

**Note**

The IPSec and L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

## Configuration Guidelines

Keep these guidelines in mind when you configure auto-anchor mobility:

- Controllers must be added to the mobility group member list before you can designate them as mobility anchors for a WLAN.
- You can configure multiple controllers as mobility anchors for a WLAN.
- Ensure that the WLAN security configuration is the same for both the anchor and remote controller.
- Auto-anchor mobility supports web authorization but does not support other Layer 3 security types.
- The WLANs 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 controller as a mobility anchor.
- Auto-anchor mobility is not supported for use with DHCP option 82.
- When using the guest N+1 redundancy and mobility failover features with a firewall, make sure that the following ports are open:
  - UDP 16666 for tunnel control traffic
  - UDP 16667 for encrypted traffic
  - IP Protocol 97 for user data traffic
  - UDP 161 and 162 for SNMP

To configure auto-anchor mobility for a WLAN and to configure the controller to detect failed anchor controllers within a mobility group, follow these steps:

**Step 1** Follow these steps to configure the controller to detect failed anchor controllers within a mobility group:

- a. Click **Controller > Mobility Management > Mobility Anchor Config** to access the Mobility Anchor Config page (see [Figure 19](#)).

**Figure 19** *Mobility Anchor Config Page*

- b. In the Keep Alive Count field, enter the number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.

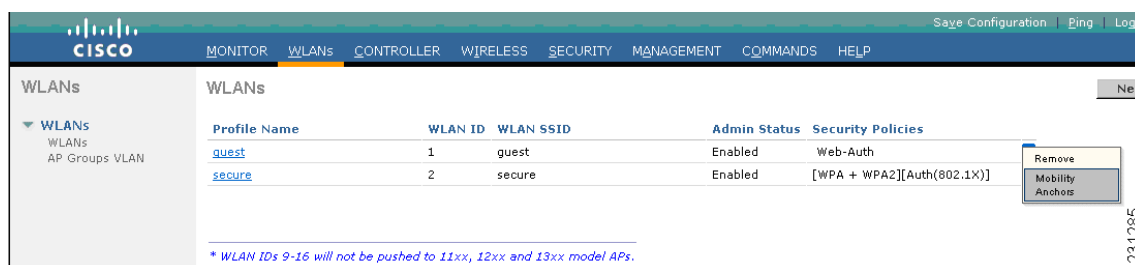
- c. In the Keep Alive Interval field, enter the amount of time (in seconds) between each ping request sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
- d. Click **Apply** to commit your changes.



**Note** You are now ready to create the auto-anchor mobility group for the WLAN.

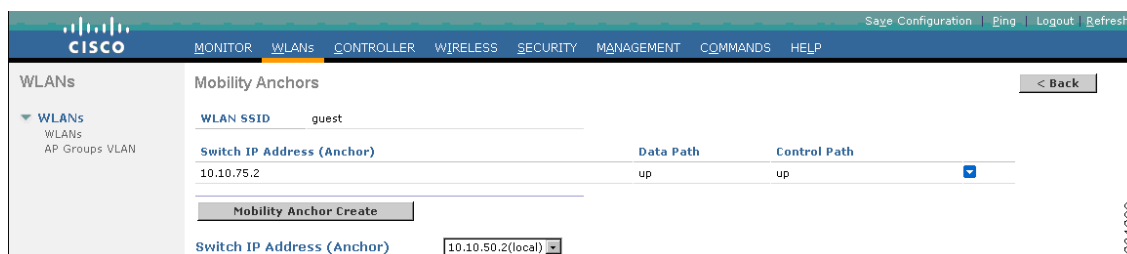
- Step 2** Click **Controller > WLANs** to access the WLANs page (see [Figure 20](#)).

**Figure 20** *Controller > WLANs Page*



- Step 3** Click the blue drop-down arrow for the desired WLAN and choose **Mobility Anchors**. The Mobility Anchors page for that WLAN appears ([Figure 21](#)).

**Figure 21** *Mobility Anchors Page*



This page lists the controllers that have already been configured as mobility anchors, if any, and shows the current state of their data and control paths. Controllers within a mobility group communicate control information among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. Specifically, they send mpings, which test mobility control packet accessibility over the management interface, over mobility UDP port 16666 and epings, which test the mobility data traffic over the management interface, over EoIP port 97. The Control Path field shows whether mpings have passed (up) or failed (down), and the Data Path field shows whether epings have passed (up) or failed (down). If the Data or Control Path field shows “down,” the mobility anchor cannot be reached and is considered failed.

- Step 4** At the Mobility Anchors page, select the IP address of the controller to be designated a mobility anchor from the Switch IP Address (Anchor) drop-down box.
- Step 5** Click **Mobility Anchor Create**. The selected controller becomes an anchor for this wireless LAN.

**Note**

Verify that both the Data and Control Paths are noted as UP for the anchor controller on the Mobility Anchors page (far-right).

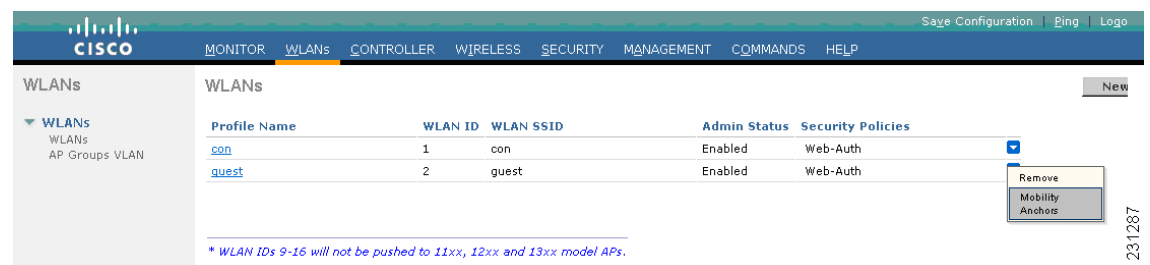
**Note**

To delete a mobility anchor for a WLAN, select the **Remove** option from the blue arrow drop-down menu to the right of the appropriate controller's IP address.

**Step 6** Click **Save Configuration** to save your changes.

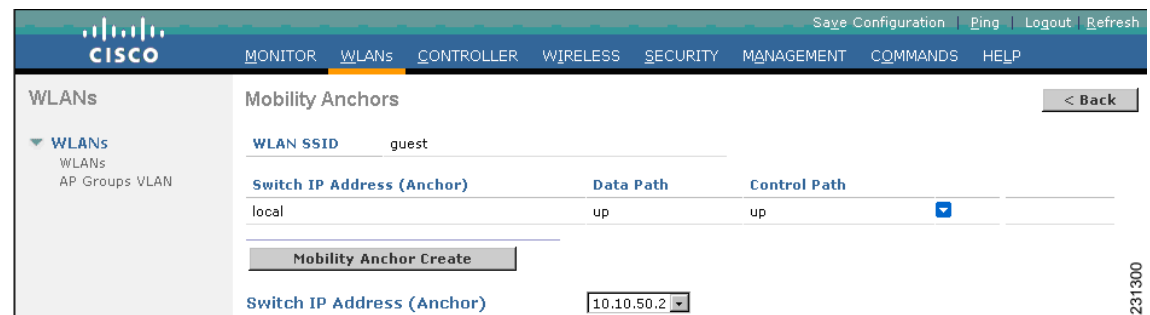
**Step 7** To configure the DMZ controller, select **Mobility Anchor** from the blue arrow drop-down menu next to the desired WLAN (see [Figure 22](#)).

**Figure 22 DMZ Controller Security Policy**



**Step 8** Select the IP address of the DMZ anchor controller, itself (see [Figure 23](#)).

**Figure 23 DMZ Anchor Controller IP Address is Selected**



**Step 9** Create a mobility anchor following Steps 4 and 5 above.

**Step 10** Verify that the data and control paths are UP.

**Note**

You 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, enter this command:

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

```
Number of WLANs..... 2
```

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
1	guest / guest	Enabled	guest-vlan
2	secure / secure	Enabled	secure-vlan

```
(Cisco Controller) >show mobility summary
```

```
Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) .... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... mobile-1
Mobility Keepalive interval..... 10
Mobility Keepalive count..... 3
Mobility Group members configured..... 2
```

```
Controllers configured in the Mobility Group
```

MAC Address	IP Address	Group Name	Status
00:0b:85:40:cd:40	10.10.50.2	<local>	Up
00:18:73:34:b2:60	10.10.75.2	mobile-9	Up mobile-1

```
(Cisco Controller) > show mobility anchor
```

```
Mobility Anchor Export List
```

WLAN ID	IP Address	Status
1	10.10.75.2	Up

To verify the configuration on the DMZ Anchor controller, enter this command:

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

```
Number of WLANs..... 2
```

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
1	con / con	Enabled	guest
2	guest / guest	Enabled	guest

```
(Cisco Controller) >show mobility summary
```

```
Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) .... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... mobile-9
Mobility Keepalive interval..... 10
Mobility Keepalive count..... 3
Mobility Group members configured..... 2
```



Controllers configured in the Mobility Group

MAC Address	IP Address	Group Name	Status
00:0b:85:40:cd:40	10.10.50.2	mobile-1	Up
00:18:73:34:b2:60	10.10.75.2	<local>	Up

(Cisco Controller) >**show mobility anchor**

Mobility Anchor Export List

WLAN ID	IP Address	Status
1	10.10.75.2	Up
2	10.10.75.2	Up



#### 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.



#### Note

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

## Enabling the Web Login Page on the Controller

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

To enable the web login, follow these steps:

**Step 1** Choose **Security** from the navigation bar at the top of the page.

**Step 2** Click **Web Auth > Web Login Page**.

The Web Login Page appears (see [Figure 24](#)).

**Figure 24** Web Login Page

231309

- Step 3** Select **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 web site) 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 2,047 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.



**Note** You must reboot the controller to commit the changes. See [“Rebooting the Wireless LAN Controller”](#) section on page 27 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 10.1.1.12.

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

- Step 1** Choose **WLANs > Edit** (see [Figure 25](#)).

**Figure 25** *WLANs > Edit Page*

The screenshot shows the Cisco Wireless LAN Controller GUI. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main navigation bar has tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the WLANs menu with sub-items for WLANs, AP Groups, and VLAN. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The Advanced tab is selected, and within it, the AAA Servers sub-tab is active. The AAA Servers section contains a form for configuring Radius and LDAP servers. The Radius Servers section has a table with columns for Server, IP, Port, and Enabled. The table has three rows: Server 1 (IP: 10.1.1.12, Port: 1812, Enabled: checked), Server 2 (IP: None, Port: None, Enabled: unchecked), and Server 3 (IP: None, Port: None, Enabled: unchecked). The LDAP Servers section has a table with columns for Server and Name. The table has three rows: Server 1 (Name: None), Server 2 (Name: None), and Server 3 (Name: None). The Local EAP Authentication section has a checkbox for Enabled, which is currently unchecked. The page also includes a Footer Notes section with five notes.

Foot Notes

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

- 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.



**Note** Authentication is disabled by default.

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



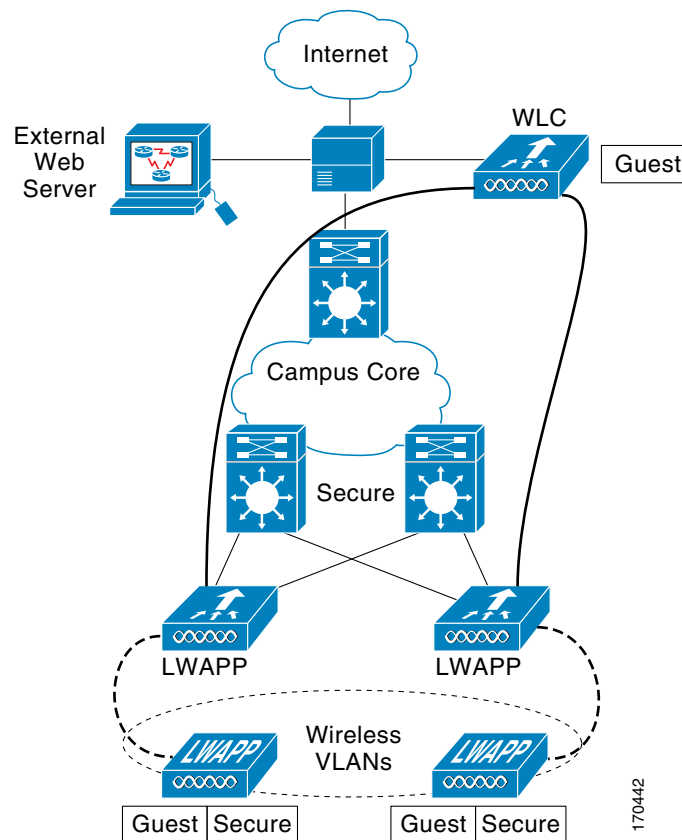
**Note** You can enter the **show radius acct statistics**, **show radius auth statistics**, and **show radius summary** commands to verify that the RADIUS settings are correctly configured.

## 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, 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 26** Using an External Web Server to Authenticate a Guest User



**Note**

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** Choose **Security > Web Login Page** (see [Figure 27](#)).

**Figure 27**      **Security > Web Login Page**

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The main heading is 'Web Login Page'. On the left, a navigation tree shows 'Security' expanded, with 'Web Auth' selected. The 'Web Authentication Type' is set to 'External (Redirect to external server)'. The 'URL' field contains 'https://192.168.10.8/pas/compat/asdf/plain'. The 'Web Server IP Address' field contains '192.168.10.8', with an 'Add Web Server' button below it. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The top right corner has links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'.

- 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**.

After it is 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 either the local user database of the controller or to an external RADIUS server for verification as determined by the wireless LAN configuration.

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

## Modifying the PC to Support Wireless Guest Access

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



### Note

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

- 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.



### Note

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 (see [Figure 28](#)).



### Note

Be sure you use secure https:// when authenticating the user with the controller's web server.

**Figure 28**      **Client Login Page**

**Login**

**Welcome to the Cisco wireless network**

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

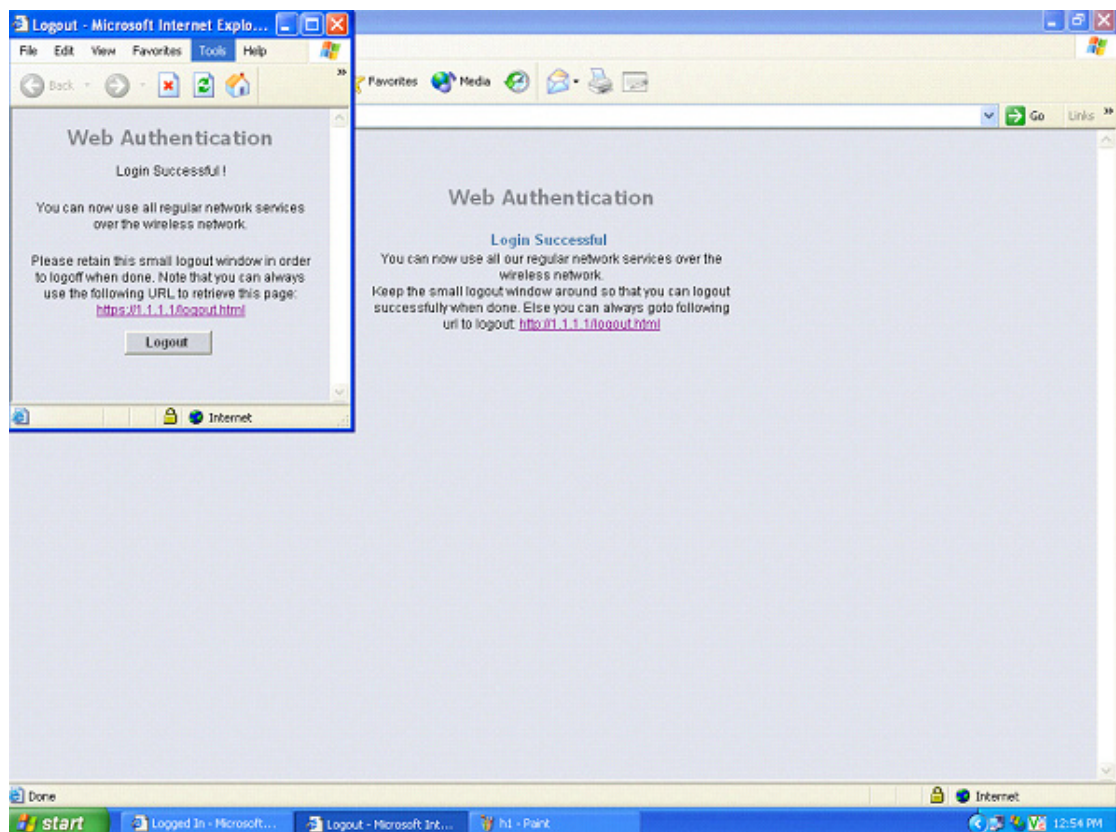
User Name

Password

231312

**Step 2** Enter the username and password provided.

**Step 3** If your login is successful, a browser window noting a successful login appears (see [Figure 29](#)).

**Figure 29**      **Successful Login Page**

170444



## Adding Guest Users Using Cisco WCS

You can use the Cisco Lobby Ambassador feature to create guest user accounts in WCS. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

The system administrator must first set up a lobby administrator account. A lobby ambassador account has limited configuration privileges and only allows access to the screens used to configure and manage guest user accounts. The lobby administrator has no access to online help.

This account allows a non-administrator to create and manage guest user accounts on WCS. The purpose of a guest user account is to provide a user account for a limited amount of time. The lobby ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. This section describes how a lobby ambassador can create and manage guest user accounts on WCS.

This section describes how to perform the following procedures:

- [Creating a Lobby Ambassador Account](#)
- [Logging in to the WCS User Interface](#)
- [Managing WCS Guest User Accounts](#)
- [Logging the Lobby Ambassador Activities](#)

## Creating a Lobby Ambassador Account

The lobby ambassador is able to create the following types of guest user accounts:

- A guest user account with a limited lifetime. The lobby ambassador is able to configure a specific end time for the guests user account to be active. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the start and end time of the valid time period.

Follow these steps to create a lobby ambassador account in WCS.



### Note

User should have SuperUser privilege (by default) to create a lobby ambassador account and not administration privileges.



### Note

A root group, which is created during installation, has only one assigned user, and no additional users can be assigned after installation. This root user cannot be changed. Also, unlike a super user, no task changes are allowed.

- Step 1** Log into the WCS user interface as an administrator.
- Step 2** Click **Administration > AAA**, then choose **Users** in the left sidebar menu.
- Step 3** From the Select a Command drop-down menu, choose **Add User** and click **GO**. The Users window displays (see [Figure 30](#)).

**Figure 30**      **Users Window**

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Help

AAA

Change Password

Local Password Policy

AAA Mode

Users

Groups

Active Sessions

TACACS+

RADIUS

Username lobby

New Password

Confirm Password

Groups Assigned to this User

- ☐ Admin
- ☐ ConfigManagers
- ☐ System Monitoring
- ☐ Users Assistant
- ☒ LobbyAmbassador
- ☐ Monitor Lite
- ☐ North Bound API
- ☐ SuperUsers
- ☐ Root
- ☐ User Defined 1
- ☐ User Defined 2
- ☐ User Defined 3
- ☐ User Defined 4

Submit Cancel

Foot Notes

1. Click [here](#) for current password policy.

2. If user belongs to 'LobbyAmbassador' or 'Monitor Lite' or 'North Bound API' or 'Users Assistant' group then he cannot belong to any other group.

3. Root group is only assignable to 'root' user and that assignment cannot be changed.

231313

- Step 4** On the Users window, follow these steps to add a new Lobby Ambassador account.
- Enter the username.
  - Enter the password. The minimum is 6 characters. Re-enter and confirm the password.
  - In the section *Groups Assigned to this User*, check the **Lobby Ambassador** check box.
  - Click **Submit**. When the lobby ambassador is added, it is part of the lobby ambassador group. The name of the new lobby ambassador account is listed and can be used immediately.

## Logging in to the WCS User Interface

When you log in as a lobby ambassador, you have access to the guest user template page in the WCS. You can then configure guest user accounts (through templates).

Follow these steps to log into the WCS user interface through a web browser.

- Step 1** Launch Internet Explorer 6.0 or later on your computer.



### Note

Some WCS features may not function properly if you use a web browser other than Internet Explorer 6.0 on a Windows workstation.

**Step 2** In the browser's address line, enter **https://wcs-ip-address** (such as <https://1.1.1.1/login.html>), where *wcs-ip-address* is the IP address of the computer on which WCS is installed. Your administrator can provide this IP address.

**Step 3** When the WCS user interface displays the Login window, enter your username and password.



**Note** All entries are case sensitive.



**Note** The lobby administrator can only define guest users templates.

**Step 4** Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The Guest Users window is displayed as seen in [Figure 31](#). This window provides a summary of all created Guest Users.

**Figure 31** *Guest Users Window*

User Name	Profile	Description	Applied To	Status
<a href="#">quest</a>	con	Wireless Network Guest Access	Controller List	Active
<a href="#">quest1</a>	con	Wireless Network Guest Access	Indoor Door Area	Active
<a href="#">g3</a>	con	Wireless Network Guest Access	Controller List	Active



**Note** To exit the WCS user interface, close the browser window or click **Logout** in the upper right corner of the window. Exiting a WCS user interface session does not shut down WCS on the server.



**Note** When a system administrator stops the WCS server during your WCS session, your session ends, and the web browser displays this message: “The page cannot be displayed.” Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

## Managing WCS Guest User Accounts

WCS guest user accounts are managed with the use of templates. This section describes how to manage WCS user accounts. It includes the following:

- [Adding Guest User Accounts](#)
- [Viewing and Editing Guest Users](#)
- [Deleting Guest User Templates](#)
- [Scheduling WCS Guest User Accounts](#)
- [Print or Email WCS Guest User Details](#)

## Adding Guest User Accounts

A template is used to create guest user account in Cisco WCS that can be applied to all controllers that the guest user or users are allowed access. Follow these steps to add a new guest user account to WCS.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Guest Users**.
- Step 3** Select **Add Guest User** from the Select a command drop-down menu and click **GO**. The window seen in [Figure 32](#) displays.

**Figure 32** *Guest Users > New Users Window*

231315

- Step 4** Enter the guest user name. The maximum is 24 characters.
- Step 5** Check the Generate Password check box to auto-generate a password.



### Note

If you choose to auto generate, the password field will get populated. If you choose to enter a password manually, enter it twice to confirm.




---

**Note** Passwords are case sensitive.

---




---

**Note** The lobby administrator can only define guest user templates.

---

**Step 6** Select an SSID from the Profile drop-down menu.

This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 web authentication policy configured. Your administrator can advise you which SSID to use.

**Step 7** Enter a description of the guest user account.

**Step 8** Choose **limited** or **unlimited**.

- Limited —From the drop-down menus, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
- Unlimited —This user account never expires.

**Step 9** Click **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can also restrict the guest user to a specific listed controller or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the drop-down menus, choose one of the following:

- Controller List: Check the check box for the controller(s) for which the guest user account applies. The selected controller is usually the DMZ anchor controller or controller where web authentication is enabled.
- Indoor Area: Choose the applicable campus, building, and floor.
- Outdoor Area: Choose the applicable campus and outdoor area.
- Config Group: Choose the config group to which the guest user account is assigned.

**Step 10** **Review the disclaimer information. Use the scroll bar to move up and down.**




---

**Note** The Account Expiry displays the controller(s) to which the guest user account was applied to and the seconds remaining before the guest user account expires. If you need to update the lifetime parameter for this account, see the [“Viewing and Editing Guest Users” section on page 38](#).

---

**Step 11** Click the check box if you want to set new default disclaimer text for all future guest user accounts.

**Step 12** Click **Save** to save your changes or **Cancel** to leave the settings unchanged. The Guest User Credentials window appears (see [Figure 33](#)).

**Figure 33**      **Guest Users Credentials Window**

Wireless Control System      Username: lobby | Logout | Refresh | Print View

Help ▾

Guest Users

Guest User Account application result to the Selected controllers

IP Address	Controller Name	Operation Status	Reason
10.10.75.2	ANCHOR-1	Success	-

Guest User Credentials

Guest User Name	guest123
Password	Cisco@123
Profile	guest
Start Time	13: 16: 05/03/2007
End Time	13: 15: 05/04/2007
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

[Print/Email Guest User Credentials](#)

23/3/16

**Note**

- After the guest user credentials are created, you can either email or print the details and forward them to the guest.
- If you choose to email the credentials, an SMTP Mail Server must be defined prior to entry of the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.
- For more details on emailing the credentials, refer to the [“Print or Email WCS Guest User Details” section on page 41.](#)

**Viewing and Editing Guest Users**

Follow these steps to view the current WCS guest users.

- Step 1** Log into the WCS user interface as described in the “Logging into the WCS User Interface” section of the *Cisco Wireless Control System Configuration Guide*.
- Step 2** On the Guest User window, click an item number under the User Name column that you would like to view or edit.
- Step 3** On the **Guest Users > Users** window, you can edit the following items:
- Profile ID: Select an Profile ID from the drop-down menu. This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 web authentication policy configured. Your administrator can advise which Profile ID to use.
  - Description: Enter a description of the guest user account.
  - Limited or Unlimited:
    - Limited: From the drop-down menus, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 30 days.
    - Unlimited: This user account never expires.

- Choose **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can also restrict the guest user to specific listed controllers or a config group, which is a group of controllers that has been preconfigured by the administrator. From the drop-down menus, choose one of the following:
  - Controller List: Check the check box for the controller(s) to which the guest user account applies.
  - Indoor Area: Choose the applicable campus, building, and floor.
  - Outdoor Area: Choose the applicable campus and outdoor area.
  - Config Group: Choose the Config Group to which the guest user account applies.

**Step 4** Click **Save** to save your changes or **Cancel** to leave the settings unchanged. When you click **Save**, the screen refreshes.



**Note** The account expiry displays the controller(s) to which the guest user account was applied to and the seconds remaining before the guest user account expires.

## Deleting Guest User Templates

During deletion of the guest account, all client stations logged in and using the guest WLAN username will be deleted. Follow these steps to delete a WCS guest user template.

- Step 1** Log into the WCS user interface as described in the “Logging into the WCS User Interface” section of the *Cisco Wireless Control System Configuration Guide*.
- Step 2** On the Guest Users window, check the check box to the left of the guest user account(s) to be deleted.
- Step 3** From the Select a Command drop-down menu, choose **Delete Guest User** and click **GO**.
- Step 4** When prompted, click **OK** to confirm your decision.



**Note** The IP address and controller name to which the guest user account was applied to displays, and you are prompted to confirm the removal of the template from the controller.

The controller sends a notification of a guest account expiry and deletion by invoking a trap. WCS processes the trap and deletes the user account expired from the configuration of that controller. If that guest account is not applied to other controllers, it can be deleted from the templates as well. A notice appears in the event logs also.

- Step 5** Click **OK** to delete the guest user template from the controller or **Cancel** to leave the settings unchanged. When you delete the guest user template from the controller, you delete the specified guest user account.

## Scheduling WCS Guest User Accounts

A lobby ambassador is able to schedule automatic creation of a guest user account. The validity and recurrence of the account can be defined. The generation of a new username on every schedule is optional and is enabled using a check box. For scheduled users, the password is automatically generated and is automatically sent by email to the host of the guest. The email address for the host is configured on the New User window. After clicking Save, the Guest User Details window displays the password. From this window, you can email or printer the account credentials.

Follow these steps to schedule a recurring guest user account in WCS.

- Step 1** Log in to the WCS user interface as lobby ambassador.
- Step 2** On the Guest User window, choose **Schedule Guest User** from the Select a command drop-down menu and click **GO**. The window seen in [Figure 35](#) displays.

**Figure 34** *Guest Users > Scheduling*

The screenshot shows the 'Guest Users > Scheduling' configuration page in the Cisco Wireless Control System (WCS) interface. The page is divided into several sections:

- Guest Information:**
  - User Name:
  - ☐ Generate new on every schedule
- Account Configuration:**
  - Profile:
  - Life Time: ☒ Limited ☐ Unlimited
  - Start Time:  (Hours)  (Minutes)
  - End Time:  (Hours)  (Minutes)
  - Days of the week: ☐ Sun ☐ Mon ☐ Tues
  - Controller List:  (selected),  (unselected)
  - Apply to:
  - Description:
  - Disclaimer:
  - ☐ Make this Disclaimer default

At the bottom, there are 'Save' and 'Cancel' buttons. A calendar for May 2007 is visible on the right side of the page.

- Step 3** On the Guest Users > Scheduling window, enter the guest user name. The maximum is 24 characters.
- Step 4** Check the check box to generate a username and password on every schedule. The generation of a new username and password on every schedule is optional.
- Step 5** Select a Profile ID from the drop-down menu. This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 authentication policy configured. Your administrator can advise which Profile ID to use.
- Step 6** Enter a description of the guest user account.



**Step 7** Choose **limited** or **unlimited**.

- **Limited:** From the drop-down menu, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 30 days.
  - **Start time:** Date and time when the guest user account begins.
  - **End time:** Date and time when the guest user account expires.
- **Unlimited:** This user account never expires.
- **Days of the week:** Check the check box for the days of the week that apply to this guest user account.

**Step 8** Choose **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can also restrict the guest user to specific listed controllers or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the drop-down menus, choose one of the following:

- **Controller List:** check the check box for the controller(s) to which the guest user account applies.
- **Indoor Area:** choose the applicable campus, building, and floor.
- **Outdoor Area:** choose the applicable campus and outdoor area.
- **Config group:** choose the configuration group to which the guest user account is member.

**Step 9** Enter the email address to send the guest user account credentials. Each time the scheduled time comes up, the guest user account credentials are emailed to the specified email address.**Step 10** Review the disclaimer information. Use the scroll bar to move up and down.**Step 11** Click **Save** to save your changes or **Cancel** to leave the settings unchanged.

If you selected **Save**, the window seen in [Figure 35](#) displays.

**Figure 35** *Scheduled Guest User Account Summary Window*

The screenshot shows the 'Wireless Control System' interface. On the left is a sidebar with the Cisco logo and a 'Guest Users' menu item. The main content area is titled 'Guest User Account Scheduled on the selected controllers'. It contains a table with the following information:

Guest User Credentials	
Guest User Name	guest122
Password	C6xDyxnW
Profile	guest
Start Time	15: 20: 05/03/2007
End Time	13: 20: 05/04/2007
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

At the bottom of the table, there is a link: [Print/Email Guest User Credentials](#). The top right of the window shows the username 'lobby' and links for 'Logout', 'Refresh', and 'Print View'.

231319

## Print or Email WCS Guest User Details

The lobby ambassador can print or email the guest user account details to the host or person who will be welcoming the guest.

The email and print copy shows the following details:

- **Username:** Guest user account name.
- **Password:** Password for the guest user account.
- **Start time:** Data and time when the guest user account begins.
- **End time:** Date and time when the guest user account expires.

- **Profile ID:** Profile ID to which this guest user applies. Your administrator can advise which Profile ID to use.
- **Disclaimer:** Disclaimer information for the guest user.

When creating the guest user account and applying the account to a list of controllers, area, or configuration group, a link is provided to email or print the guest user account details. You can also print guest user account details from the Guest Users List window.

Follow these steps to print guest user details from the Guest Users List window:

- Step 1** Log into the WCS user interface as lobby ambassador.
- Step 2** On the Guest User window, check the check box next to User Name and choose **Print/Email User Details** from the Select a command drop-down menu and click **GO**. The window seen in [Figure 36](#) appears.

**Figure 36** Guest User Credentials Print or Email Window

**Guest Users Details**

Email To   
 Subject

*Credentials for Guest User **guest123***

Guest User Name	guest123
Password	Cisco@123
Profile	guest
Start Time	13: 16: 05/03/2007
End Time	13: 15: 05/04/2007
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

231317

If printing, click **Print** button and from the print window, select a printer and click **Print** or **Cancel**.

- If emailing, click **Email** button and from the email window, enter the subject text and the recipient's email address. Click **Send** or **Cancel**.



**Note**

If you select to email the credentials, an SMTP Mail Server must be defined prior to entry of the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.

## Logging the Lobby Ambassador Activities

The following activities will be logged for each lobby ambassador account:

- Lobby ambassador login: WCS logs the authentication operation results for all users.
- Guest user creation: When a lobby ambassador creates a guest user account, WCS logs the guest user name.
- Guest user deletion: When a lobby ambassador deletes the guest user account, WCS logs the deleted guest user name.
- Account updates: WCS logs the details of any updates made to the guest user account. For example, increasing the life time.

Follow these steps to view the lobby ambassador activities.



### Note

You must have superuser status to open this window.

- 
- Step 1** Log into the Navigator or WCS user interface as an administrator.
- Step 2** Click **Administration > AAA**, then click **Groups** in the left sidebar menu to display the All Groups window.
- Step 3** On the All Groups windows, click the Audit Trail icon for the lobby ambassador account you want to view. The Audit Trail window for the lobby ambassador displays.
- This window enables you to view a list of lobby ambassador activities over time.
- User: User login name
  - Operation: Type of operation audited
  - Time: Time operation was audited
  - Status: Success or failure
- Step 4** To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down menu and click **GO**.
-

# Troubleshooting

This section provides debugging tips for specific features.



**Note**

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**

MAC address ..... 00:40:96:ad:0d:1b

```
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.
```

```
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b Association received from mobile
00:40:96:ad:0d:1b on AP 00:14:1b:59:3f:10
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b STA: 00:40:96:ad:0d:1b - rates (8): 12 18
24 36 48 72 96 108 0 0 0 0 0 0 0
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Applied RADIUS override
policy
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Plumbing duplex mobility
tunnel to 10.10.75.2 as Export Foreign (VLAN 60)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Replacing Fast Path rule
type = Airespace AP Client on AP 00:14:1b:59:3f:10, slot 1, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20)
```

```

Card = 0 (slot 1), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Successfully plumbed
mobile rule (ACL ID 255)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Plumbed mobile LWAPP rule
on AP 00:14:1b:59:3f:10
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b apfPemAddUser2 (apf_policy.c:205) Changing
state for mobile 00:40:96:ad:0d:1b on AP 00:14:1b:59:3f:10 from As
sociated to Associated
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b Session Timeout is 0 - not starting
session timer for STA 00:40:96:ad:0d:1b
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b Stopping deletion of Mobile Station:
00:40:96:ad:0d:1b (callerId: 48)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b Sending Assoc Response to station
00:40:96:ad:0d:1b on BSSID 00:14:1b:59:3f:10 (status 0)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b apfProcessAssocReq (apf_80211.c:3741)
Changing state for mobile 00:40:96:ad:0d:1b on AP 00:14:1b:59:3f:10 fro
m Associated to Associated
Tue May  8 13:34:12 2007: Mobility query, Mobile: 00:40:96:ad:0d:1b PEM State: RUN
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) State Update from
Mobility-Complete to Mobility-Incomplete
Tue May  8 13:34:12 2007: Anchor Export: Client: 00:40:96:ad:0d:1b
Client IP: 0.0.0.0, Anchor IP: 10.10.75.2
Tue May  8 13:34:12 2007: Mobility packet sent to:
Tue May  8 13:34:12 2007: 10.10.75.2, port 16666, Switch IP: 10.10.50.2
Tue May  8 13:34:12 2007: type: 16(MobileAnchorExport) subtype: 0 version: 1 xid:
19583 seq: 20500 len 244 flags 0
Tue May  8 13:34:12 2007: group id: 66c18089 22dc11a 56ca50a2 62b7c749
Tue May  8 13:34:12 2007: mobile MAC: 00:40:96:ad:0d:1b, IP: 0.0.0.0, instance: 0
Tue May  8 13:34:12 2007: VLAN IP: 10.10.60.2, netmask: 255.255.255.0
Tue May  8 13:34:12 2007: Mobility packet received from:
Tue May  8 13:34:12 2007: 10.10.75.2, port 16666, Switch IP: 10.10.75.2
Tue May  8 13:34:12 2007: type: 17(MobileAnchorExportAck) subtype: 0 version: 1
xid: 19583 seq: 16358 len 272 flags 0
Tue May  8 13:34:12 2007: group id: 27aeb903 faa89081 6f281b16 f68e7671
Tue May  8 13:34:12 2007: mobile MAC: 00:40:96:ad:0d:1b, IP: 10.10.77.48, instance:
1
Tue May  8 13:34:12 2007: VLAN IP: 10.10.77.2, netmask: 255.255.255.0
Tue May  8 13:34:12 2007: Received Anchor Export Ack: 00:40:96:ad:0d:1b from Switch
IP: 10.10.75.2
Tue May  8 13:34:12 2007: Anchor IP: 10.10.75.2 Old Foreign IP: 10.10.50.2 New
Foreign IP: 10.10.50.2
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) mobility role update
request from Export Foreign to Export Foreign
Peer = 10.10.75.2, Old Anchor = 10.10.75.2, New Anchor = 10.10.75.2
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=ExpForeign
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Change state to RUN (20)
last state RUN (20)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Reached PLUMBFASTPATH:
from line 3978
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Plumbing duplex mobility
tunnel to 10.10.75.2
as Export Foreign (VLAN 60)
Tue May  8 13:34:12 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Replacing Fast Path rule
type = Airespace AP Client
on AP 00:14:1b:59:3f:10, slot 1, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May  8 13:34:16 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20)
Card = 0 (slot 1), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May  8 13:34:16 2007: 00:40:96:ad:0d:1b 0.0.0.0 RUN (20) Successfully plumbed
mobile rule (ACL ID 255)

```

```
Tue May 8 13:34:16 2007: 00:40:96:ad:0d:1b Mobility Response: IP 0.0.0.0 code 4,
reason 4, PEM State RUN, Role Export Foreign(5)
Tue May 8 13:34:16 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Foreign role
Tue May 8 13:34:16 2007: 00:40:96:ad:0d:1b 0.0.0.0 Added NPU entry of type 1
Tue May 8 13:34:16 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Foreign role
Tue May 8 13:34:16 2007: 00:40:96:ad:0d:1b 0.0.0.0 Added NPU entry of type 1
```

The details about the client can be seen with the command **show client detail mac-address**.

Look for the following entries in the script, noted in bold: **Mobility State = Export Foreign, Security Policy Completed = Yes and Policy Manager State = RUN**.

```
(Cisco Controller) >show client detail 00:40:96:ad:0d:1b
Client MAC Address..... 00:40:96:ad:0d:1b
Client Username ..... N/A
AP MAC Address..... 00:14:1b:59:3f:10
Client State..... Associated
Wireless LAN Id..... 1
BSSID..... 00:14:1b:59:3f:1f
Channel..... 64
IP Address..... Unknown
Association Id..... 1
Authentication Algorithm..... Open System
Reason Code..... 0
Status Code..... 0
Session Timeout..... 0
Client CCX version..... 5
Client E2E version..... No E2E support
Mirroring..... Disabled
QoS Level..... Silver
Diff Serv Code Point (DSCP)..... disabled
802.1P Priority Tag..... disabled
WMM Support..... Disabled
Mobility State..... Export Foreign
Mobility Anchor IP Address..... 10.10.75.2
Mobility Move Count..... 0
Security Policy Completed..... Yes
Policy Manager State..... RUN
Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Policy Type..... N/A
Encryption Cipher..... None
Management Frame Protection..... No
EAP Type..... Unknown
Interface..... guest-vlan
VLAN..... 60
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..... 12766445
  Number of Bytes Sent..... 6213712
  Number of Packets Received..... 339110
  Number of Packets Sent..... 67131
  Number of Policy Errors..... 0
  Radio Signal Strength Indicator..... -50 dBm
  Signal to Noise Ratio..... 47 dB
```

```

Nearby AP Statistics:
    TxExcessiveRetries: 0
    TxRetries: 0
    RtsSuccessCnt: 0
    RtsFailCnt: 0
    TxFiltered: 0
    TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
    AP0014.1ced.48e8(slot 0) .....
antenna0: 57 seconds ago -80 dBm..... antenna1: 1810269 seconds ago -128
dBm
    AP0014.1ced.48e8(slot 1) .....
antenna0: 56 seconds ago -51 dBm..... antenna1: 1810269 seconds ago -128
dBm

```

## Debugging Script from the Anchor Controller

```

(Cisco Controller) >show debug
MAC address ..... 00:40:96:ad:0d:1b

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) >Tue May  8 13:31:49 2007: Mobility packet received from:
Tue May  8 13:31:49 2007:  10.10.50.2, port 16666, Switch IP: 10.10.50.2
Tue May  8 13:31:49 2007:  type: 3(MobileAnnounce) subtype: 0 version: 1 xid:
19608 seq: 20526 len 120 flags 0
Tue May  8 13:31:49 2007:  group id: 66c18089 22dc11a 56ca50a2 62b7c749
Tue May  8 13:31:49 2007:  mobile MAC: 00:40:96:ad:0d:1b, IP: 0.0.0.0, instance: 0
Tue May  8 13:31:49 2007:  VLAN IP: 10.10.60.2, netmask: 255.255.255.0
Tue May  8 13:31:49 2007: Ignoring Announce, client record for 00:40:96:ad:0d:1b not
found
Tue May  8 13:31:50 2007: Mobility packet received from:
Tue May  8 13:31:50 2007:  10.10.50.2, port 16666, Switch IP: 10.10.50.2
Tue May  8 13:31:50 2007:  type: 3(MobileAnnounce) subtype: 0 version: 1 xid:
19608 seq: 20526 len 120 flags 0
Tue May  8 13:31:50 2007:  group id: 66c18089 22dc11a 56ca50a2 62b7c749
Tue May  8 13:31:50 2007:  mobile MAC: 00:40:96:ad:0d:1b, IP: 0.0.0.0, instance: 0
Tue May  8 13:31:50 2007:  VLAN IP: 10.10.60.2, netmask: 255.255.255.0
Tue May  8 13:31:50 2007: Ignoring Announce, client record for 00:40:96:ad:0d:1b not
found
Tue May  8 13:31:51 2007: Mobility packet received from:
Tue May  8 13:31:51 2007:  10.10.50.2, port 16666, Switch IP: 10.10.50.2
Tue May  8 13:31:51 2007:  type: 16(MobileAnchorExport) subtype: 0 version: 1 xid:
19609 seq: 20527 len 244 flags 0
Tue May  8 13:31:51 2007:  group id: 66c18089 22dc11a 56ca50a2 62b7c749
Tue May  8 13:31:51 2007:  mobile MAC: 00:40:96:ad:0d:1b, IP: 0.0.0.0, instance: 0
Tue May  8 13:31:51 2007:  VLAN IP: 10.10.60.2, netmask: 255.255.255.0
Tue May  8 13:31:51 2007: 00:40:96:ad:0d:1b Received Anchor Export request: from
Switch IP: 10.10.50.2
Tue May  8 13:31:51 2007: 00:40:96:ad:0d:1b Adding mobile 00:40:96:ad:0d:1b on Remote
AP 00:00:00:00:00:00(0)
Tue May  8 13:31:51 2007: mmAnchorExportRcv: 00:40:96:ad:0d:1b, Mobility role is
Unassoc

```

```

Tue May 8 13:31:51 2007: mmAnchorExportRcv: 00:40:96:ad:0d:1b Ssid=guest Security
Policy=0x2010
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 START (0) mobility role update
request from Unassociated to Export Anchor
    Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 10.10.75.2
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 START (0) Initializing policy
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state AUTHCHECK (2)
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to
DHCP_REQD (7) last state DHCP_REQD (7)
Tue May 8 13:31:51 2007: Received Anchor Export policy update, valid mask 0x0:
    Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , ACL Name:
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b Stopping deletion of Mobile Station:
00:40:96:ad:0d:1b (callerId: 53)
Tue May 8 13:31:51 2007: Mobility packet sent to:
Tue May 8 13:31:51 2007: 10.10.50.2, port 16666, Switch IP: 10.10.75.2
Tue May 8 13:31:51 2007: type: 17(MobileAnchorExportAck) subtype: 0 version: 1
xid: 19609 seq: 16372 len 272 flags 0
Tue May 8 13:31:51 2007: group id: 27aeb903 faa89081 6f281b16 f68e7671
Tue May 8 13:31:51 2007: mobile MAC: 00:40:96:ad:0d:1b, IP: 0.0.0.0, instance: 1
Tue May 8 13:31:51 2007: VLAN IP: 10.10.77.2, netmask: 255.255.255.0
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) Change state to
DHCP_REQD (7) last state DHCP_REQD (7)
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
3908, Adding TMP rule
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) Plumbing duplex
mobility tunnel to 10.10.50.2
    as Export Anchor (VLAN 77)
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) Adding Fast Path
rule
    type = Airespace AP - Learn IP address
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7)
    Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 DHCP_REQD (7) Successfully plumbed
mobile rule (ACL ID 255)
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Anchor role
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b 0.0.0.0 Added NPU entry of type 9
Tue May 8 13:31:51 2007: 00:40:96:ad:0d:1b Sent an XID frame
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b dhcpProxy: Received packet: Client
00:40:96:ad:0d:1b
DHCP Op: BOOTREQUEST(1), IP len: 320, switchport: 1, encap:
0xec05
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b dhcpProxy: dhcp request, client:
00:40:96:ad:0d:1b:
    dhcp op: 1, port: 1, encap 0xec05, old mscb port number: 1
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b Determing relay for 00:40:96:ad:0d:1b
    dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.77.2 VLAN: 77
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b Relay settings for 00:40:96:ad:0d:1b
    Local Address: 10.10.77.2, DHCP Server: 10.10.77.1,
    Gateway Addr: 10.10.77.1, VLAN: 77, port: 1
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b DHCP Message Type received: DHCP REQUEST
msg
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b op: BOOTREQUEST, htype: Ethernet, hlen:
6, hops: 1
Tue May 8 13:31:53 2007: 00:40:96:ad:0d:1b xid: 640661134, secs: 0, flags: 0

```



```

Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b  chaddr: 00:40:96:ad:0d:1b
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b  ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b  siaddr: 0.0.0.0,  giaddr: 10.10.77.2
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b DHCP request to 10.10.77.1, len 366,
switchport 1, vlan 77
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b Determining relay for 00:40:96:ad:0d:1b
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.77.2  VLAN: 77
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b dhcpProxy: Received packet: Client
00:40:96:ad:0d:1b
DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 1, encap: 0xec00
Tue May  8 13:31:53 2007: DhcpProxy(): Setting dhcp server from ACK, server:
10.10.77.1
        client mac: 00:40:96:ad:0d:1b offer ip: 10.10.77.48
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) Change state to
WEBAUTH_REQD (8) last state WEBAUTH_REQD (8)
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8)
pemAdvanceState2 4648, Adding TMP rule
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Plumbing
duplex mobility tunnel to 10.10.50.2
        as Export Anchor (VLAN 77)
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Replacing
Fast Path rule
        type = Airespace AP Client - ACL passthru
        on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
        ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May  8 13:31:53 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8)
        Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Successfully
plumbed mobile rule (ACL ID 255)
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b Plumbing web-auth redirect rule due to
user logout for 00:40:96:ad:0d:1b
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b Adding Web RuleID 928 for mobile
00:40:96:ad:0d:1b
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b Assigning Address 10.10.77.48 to mobile
00:40:96:ad:0d:1b
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) DHCP EoIP
tunnel to foreign 10.10.50.2 len 346
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b DHCP Message Type received: DHCP ACK msg
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  op: BOOTREPLY, htype: Ethernet, hlen: 6,
hops: 0
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  xid: 640661134, secs: 0, flags: 0
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  chaddr: 00:40:96:ad:0d:1b
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  ciaddr: 0.0.0.0,  yiaddr: 10.10.77.48
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b  server id: 1.1.1.1  rcvd server id:
10.10.77.1
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Anchor role
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b 10.10.77.48 Added NPU entry of type 2
Tue May  8 13:31:57 2007: 00:40:96:ad:0d:1b Sent an XID frame

```

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 *guest1* and password and completes the web authentication.

```

(Cisco Controller) >Tue May  8 13:34:14 2007: 00:40:96:ad:0d:1b Username entry
(guest1) created for mobile 00:40:96:ad:0d:1b
Tue May  8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Change state
to WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue May  8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state RUN (20)
Tue May  8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20) Reached
PLUMBFASPATH: from line 4568

```

```
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20) Plumbing duplex
mobility tunnel to 10.10.50.2
    as Export Anchor (VLAN 77)
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20) Replacing Fast Path
rule
    type = Airespace AP Client
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20)
    Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20) Successfully plumbed
mobile rule (ACL ID 255)
User logged inTue May 8 13:34:14 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Anchor role
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b 10.10.77.48 Added NPU entry of type 1
Tue May 8 13:34:14 2007: 00:40:96:ad:0d:1b Sending a gratuitous ARP for 10.10.77.48,
VLAN Id 77
```

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

```
(Cisco Controller) >Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20)
Deleting policy rule
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 RUN (20) Change state to
L2AUTHCOMPLETE (4) last state RUN (20)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 L2AUTHCOMPLETE (4) Change
state to DHCP_REQD (7) last state RUN (20)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) pemAdvanceState2
4770, Adding TMP rule
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) Plumbing duplex
mobility tunnel to 10.10.50.2
    as Export Anchor (VLAN 77)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) Adding Fast Path
rule
    type = Airespace AP - Learn IP address
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7)
    Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) Successfully
plumbed mobile rule (ACL ID 255)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 DHCP_REQD (7) Change state to
WEBAUTH_REQD (8) last state RUN (20)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8)
pemAdvanceState2 4787, Adding TMP rule
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Plumbing
duplex mobility tunnel to 10.10.50.2
    as Export Anchor (VLAN 77)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Replacing
Fast Path rule
    type = Airespace AP Client - ACL passthru
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8)
    Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag =
0x0000
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 WEBAUTH_REQD (8) Successfully
plumbed mobile rule (ACL ID 255)
Tue May 8 13:34:50 2007: 00:40:96:ad:0d:1b Plumbing web-auth redirect rule due to
user logout for 00:40:96:ad:0d:1b
```

```

Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b Adding Web RuleID 929 for mobile
00:40:96:ad:0d:1b
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b Username entry delete for mobile
00:40:96:ad:0d:1b
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 Removed NPU entry.
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Anchor role
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 Added NPU entry of type 9
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b Set bi-dir guest tunnel for
00:40:96:ad:0d:1b as in Export Anchor role
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b 10.10.77.48 Added NPU entry of type 2
Tue May  8 13:34:50 2007: 00:40:96:ad:0d:1b Sent an XID frame

```

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.

```
(Cisco Controller) >show client summary
```

```
Number of Clients..... 1
```

MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
00:40:96:ad:0d:1b	10.10.50.2	Associated	2	No	Mobile	1

```
(Cisco Controller) >
```

```
(Cisco Controller) >
```

```
(Cisco Controller) >show client detail 00:40:96:ad:0d:1b
```

```

Client MAC Address..... 00:40:96:ad:0d:1b
Client Username ..... guest1
AP MAC Address..... 00:00:00:00:00:00
Client State..... Associated
Wireless LAN Id..... 2
BSSID..... 00:00:00:00:00:01
Channel..... N/A
IP Address..... 10.10.77.48
Association Id..... 0
Authentication Algorithm..... Open System
Reason Code..... 0
Status Code..... 0
Session Timeout..... 0
Client CCX version..... No CCX support
Mirroring..... Disabled
QoS Level..... Silver
Diff Serv Code Point (DSCP)..... disabled
802.1P Priority Tag..... disabled
WMM Support..... 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 Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Policy Type..... N/A
Encryption Cipher..... None
Management Frame Protection..... No
EAP Type..... Unknown
Interface..... guest
  VLAN..... 77
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:
  TxExcessiveRetries: 0
  TxRetries: 0
  RtsSuccessCnt: 0
  RtsFailCnt: 0
  TxFiltered: 0
  TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]

```

The 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.**

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

```

Number of Clients..... 1

MAC Address      AP Name      Status      WLAN  Auth  Protocol  Port
-----
00:40:96:ad:0d:1b 10.10.50.2   Associated   2     Yes  Mobile    1

```

(Cisco Controller) > **show client detail 00:40:96:ad:0d:1b**

```

Client MAC Address..... 00:40:96:ad:0d:1b
Client Username ..... guest1
AP MAC Address..... 00:00:00:00:00:00
Client State..... Associated
Wireless LAN Id..... 2
BSSID..... 00:00:00:00:00:01
Channel..... N/A
IP Address..... 10.10.77.48
Association Id..... 0
Authentication Algorithm..... Open System
Reason Code..... 0
Status Code..... 0
Session Timeout..... 0
Client CCX version..... No CCX support
Mirroring..... Disabled
QoS Level..... Silver
Diff Serv Code Point (DSCP)..... disabled
802.1P Priority Tag..... disabled
WMM Support..... Disabled
Mobility State..... Export Anchor
Mobility Foreign IP Address..... 10.10.50.2
Mobility Move Count..... 1
Security Policy Completed..... Yes
Policy Manager State..... RUN

```

```

Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Policy Type..... N/A
Encryption Cipher..... None
Management Frame Protection..... No
EAP Type..... Unknown
Interface..... guest
VLAN..... 77
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:
    TxExcessiveRetries: 0
    TxRetries: 0
    RtsSuccessCnt: 0
    RtsFailCnt: 0
    TxFiltered: 0
    TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]

```

## Related Documentation

- *Cisco Wireless LAN Controller Configuration Guide*, Software Release 4.1, Part number OL-11336-01.

This document is found online at the following link:

[http://www.cisco.com/en/US/products/ps6366/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html)

- *Cisco Wireless Control System Configuration Guide*, Software Release 4.1, Part number OL-12623-01

This document is found online at the following link:

[http://www.cisco.com/en/US/products/ps6305/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html)

---

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 © 2007 Cisco Systems, Inc. All rights reserved

---