# Wireless Guest Access FAQ

**Document ID: 107458**

## Questions

**Introduction**
**What is an Ethernet over IP (EoIP) tunnel to the unsecured network area?**
**How do I select the right controller to deploy as a guest anchor controller?**
**How many Ethernet over IP (EoIP) tunnels can be terminated on a guest anchor controller?**
**Can the Cisco 2000/2100 Series Wireless LAN Controller be used as a guest anchor controller in the unsecured network area?**
**Can the Cisco Wireless LAN Controller Module for Integrated Services Routers (WLCM) be used as a guest anchor controller in the unsecured network area?**
**What controllers can be used to support guest access in the unsecured network area?**
**If a guest anchor controller is used outside the firewall, what firewall ports are open for guest access to work?**
**Can guest traffic pass through a firewall with Network Address Translation (NAT) configured?**
**If guest traffic is tunneled to the unsecured network area, where do guest clients get an IP address?**
**Does the Cisco Wireless LAN Controller support web portals for guest authentication?**
**How do I customize the web portal?**
**How are guest credentials managed?**
**Is the lobby ambassador function available in the Cisco Wireless LAN Controller in addition to the Wireless Control System (WCS)?**
**Can guests be authenticated with an external authentication, authorization, and accounting (AAA) server?**
**What occurs when a guest logs on?**
**Is it possible to skip the guest user authentication and display only the web page disclaimer option?**
**Do we need to have the remote controller and guest anchor controller on the same mobility group?**
**If there is more than one guest SSID, can each WLAN (SSID) be directed to a unique web page portal?**
**Is there a deployment guide for Wireless Guest Access?**
**Is there a design guide for Wired and Wireless Guest Access?**
**NetPro Discussion Forums – Featured Conversations**
**Related Information**

## Introduction

This document provides information on the most frequently asked questions (FAQs) about the Wireless Guest Access feature, which is a part of the Cisco Unified Wireless network.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Q. What is an Ethernet over IP (EoIP) tunnel to the unsecured network area?

**A.** Cisco recommends the use of a controller dedicated to guest traffic. This controller is known as the guest anchor controller.

The guest anchor controller is usually located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN. An EoIP tunnel is established between the internal WLAN controllers and the guest anchor controller in order to ensure path isolation of guest traffic from enterprise data traffic. Path isolation is a critical security management feature for guest access. It ensures that security and quality of service (QoS) policies can be separate, and are differentiated between guest traffic and corporate or internal traffic.

An important feature of the Cisco Unified Wireless Network architecture is the ability to use an EoIP tunnel to statically map one or more provisioned WLANs (that is, SSIDs) to a specific guest anchor controller within the network. All traffic both to and from a mapped WLAN traverses a static EoIP tunnel that is established between a remote controller and the guest anchor controller.

Using this technique, all associated guest traffic can be transported transparently across the enterprise network to a guest anchor controller that resides in the unsecured network area.

## Q. How do I select the right controller to deploy as a guest anchor controller?

**A.** The selection of the guest anchor controller is a function of the amount of guest traffic as defined by the number of active guest client sessions, or as defined by the uplink interface capacity on the controller, or both.

Total throughput and client limitations per guest anchor controller are as follows:

- ♦ Cisco 4100 Series Wireless LAN Controller One 1000 Mb interface and 1500 guest clients
- ♦ Cisco 4402 Wireless LAN Controller Two 1000 Mb interfaces and 2500 guest clients
- ♦ Cisco 4404 Wireless LAN Controller Four 1000 Mb interfaces and 5000 guest clients
- ♦ Cisco Catalyst 6500 Series Wireless Services Module (WiSM) Eight 1000 Mb interfaces and 10,000 guest clients

A maximum of 2048 guest usernames and passwords can be stored on each controller s database. Therefore, if the total number of active guest credentials is in excess of this number, more than one controller will be needed. Alternatively, guest credentials can be stored in an external RADIUS server.

The number of access points in the network does not impact the selection of the guest anchor controller.

## Q. How many Ethernet over IP (EoIP) tunnels can be terminated on a guest anchor controller?

**A.** One guest anchor controller can terminate up to 40 EoIP tunnels from internal WLAN

controllers. This capacity is the same across any model of the Cisco Wireless LAN Controller. More than one guest anchor controller can be configured if additional tunnels are required.

EoIP tunnels are counted per WLAN controller, independently of the number of tunneled WLANs or Secure Set Identifiers (SSIDs) in each EoIP.

One EoIP tunnel is configured between the guest anchor controller and each internal controller that supports access points with guest client associations.

## Q. Can the Cisco 2000/2100 Series Wireless LAN Controller be used as a guest anchor controller in the unsecured network area?

**A.** No. The Cisco 2000/2100 Series Wireless LAN Controller cannot terminate guest traffic outside the firewall. The Cisco 2000 Series Wireless LAN Controller can only originate guest tunnels.

## Q. Can the Cisco Wireless LAN Controller Module for Integrated Services Routers (WLCM) be used as a guest anchor controller in the unsecured network area?

**A.** No. The WLCM cannot terminate guest tunnels. The WLCM can only originate guest tunnels.

## Q. What controllers can be used to support guest access in the unsecured network area?

**A.** The guest tunnel anchor function, which includes EoIP tunnel termination, Web authentication, and access control of guest clients, is supported in these Cisco Wireless LAN Controller platforms with Version 4.0 and later software images:

- Cisco 4400 Series Wireless LAN Controller (either the 4402 or the 4404)
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750G Integrated Wireless LAN Controller

## Q. If a guest anchor controller is used outside the firewall, what firewall ports are open for guest access to work?

**A.** On any firewall between the guest anchor controller and the remote controllers, these ports need to be open:

- IP Protocol 97 for user data traffic
- UDP Port 16666 (or 16667, if encrypted) for tunnel control traffic

For optional management, these firewall ports need to be open:

- SSH/Telnet TCP Port 22/23
- TFTP UDP Port 69
- NTP UDP Port 123
- SNMP UDP Ports 161 (gets and sets) and 162 (traps)
- HTTPS/HTTP TCP Port 443/80
- Syslog TCP Port 514

## Q. Can guest traffic pass through a firewall with Network Address Translation (NAT) configured?

**A.** One to one NAT must be used on the EoIP tunnel going through a firewall.

## Q. If guest traffic is tunneled to the unsecured network area, where do guest clients get an IP address?

**A.** Guest traffic is transported within the enterprise at Layer 3 via EoIP. Therefore, the first point at which Dynamic Host Configuration Protocol (DHCP) services can be implemented is locally on the guest anchor controller, or the guest anchor controller can relay client DHCP requests to an external server. This is also the method by which Domain Name System (DNS) address resolution is handled.

## Q. Does the Cisco Wireless LAN Controller support web portals for guest authentication?

**A.** Cisco Wireless LAN Controllers, software Version 3.2 or later, provide a built–in web portal that captures guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer and acceptable use policy information.

## Q. How do I customize the web portal?

**A.** For information on how to customize a web portal, refer to Choosing the Web Authentication Login Page.

## Q. How are guest credentials managed?

**A.** Guest credentials can be created and managed centrally using the Cisco Wireless Control System (WCS) Version 4.0 and later. A network administrator can establish a limited–privilege administrative account within WCS that permits  lobby ambassador access for the purpose of creating guest credentials. In WCS, the person with a lobby ambassador account is able to create, assign, monitor, and delete guest credentials for the controller serving as a guest anchor controller.

The lobby ambassador can enter the guest username (or user ID) and password, or the credentials can be autogenerated. There is also a global configuration parameter that enables the use of one username and password for all guests, or a unique username and password for each guest.

In order to configure the lobby ambassador account on the WCS, refer to the Creating Guest User Accounts section of Cisco Wireless Control System Configuration Guide, Release 5.0.

## Q. Is the lobby ambassador function available in the Cisco Wireless LAN Controller in addition to the Wireless Control System (WCS)?

**A.** Yes. If the WCS is not deployed, a network administrator can establish a lobby ambassador account on the guest anchor controller. A person who logs into the guest anchor controller using the lobby ambassador account will have access only to guest user management functions.

If there are multiple guest anchor controllers, a WCS must be used to simultaneously configure usernames on multiple guest anchor controllers.

For information on how to create lobby ambassador accounts using Wireless LAN Controllers, refer to the Creating a Lobby Ambassador Account section of Cisco Wireless LAN Controller Configuration Guide, Release 5.0.

## Q. Can guests be authenticated with an external authentication, authorization, and accounting (AAA) server?

**A.** Yes. Guest authentication requests can be relayed to an external RADIUS server.

## Q. What occurs when a guest logs on?

**A.** When a wireless guest logs in through the web portal, the guest anchor controller handles the authentication by performing these steps:

1. The guest anchor controller checks its local database for username and password, and if they are present, grants access.
2. If no user credentials are present locally on the guest anchor controller, the guest anchor controller checks WLAN configuration settings to see if an external RADIUS server(s) has been configured for the guest WLAN. If so, the controller creates a RADIUS access−request packet with the username and password and forwards it to the selected RADIUS server for authentication.
3. If no specific RADIUS servers have been configured for the WLAN, the controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate  network user  will be queried with the guest user s credentials. Otherwise, if no servers have  network user  selected, and the user has not been authenticated through steps 1 or 2, the authentication will fail.

## Q. Is it possible to skip the guest user authentication and display only the web page disclaimer option?

**A.** Yes. Another configuration option of wireless guest access is to bypass user authentication altogether and allow open access. However, there might be a need to present an acceptable−use policy and disclaimer page to guests before granting access. In order to do this, a guest WLAN can be configured for web policy passthrough. In this scenario, a guest user is redirected to a web portal page which contains disclaimer information. In order to enable identification of the guest user, passthrough mode also has an option for a user to enter an email address before connecting.

## Q. Do we need to have the remote controller and guest anchor controller on the same mobility group?

**A.** No. The guest anchor controller and the remote controller can be on separate mobility groups.

## Q. If there is more than one guest SSID, can each WLAN (SSID) be directed to a unique web page portal?

**A.** Yes. All guest traffic, either on a single or multiple WLANs are redirected to one web page. Starting from WLC version 4.2 or later, each WLAN can be directed to a unique web portal page. Refer to the Assigning Login, Login Failure, and Logout Pages per WLAN section of Cisco Wireless LAN Controller Configuration Guide, Release 5.0.

## Q. Is there a deployment guide for Wireless Guest Access?

**A.** Here is the link to the deployment guide:

Deployment Guide: Cisco Guest Access Using the Cisco Wireless LAN Controller

## Q. Is there a design guide for Wired and Wireless Guest Access?

**A.** Here is the link to the design guides:

Network Virtualization

# NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

| NetPro Discussion Forums – Featured Conversations for Wireless |
| --- |
| Wireless – Mobility: WLAN Radio Standards |
| Wireless – Mobility: Security and Network Management |
| Wireless – Mobility: Getting Started with Wireless |
| Wireless – Mobility: General |

# Related Information

- **Wired Guest Access using Cisco WLAN Controllers Configuration Example**
- **Deployment Guide: Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.1**
- **Technical Support & Documentation – Cisco Systems**

Updated: Jun 26, 2008                                    Document ID: 107458