



## Configuring WLC

---

- [Configure the WLC for NAT, page 1](#)
- [Configuring the Time Zone, page 2](#)
- [Configuring SNMP, page 3](#)
- [Configuring Wireless User Authentication, page 7](#)

## Configure the WLC for NAT

The Internet edge firewall translates the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so Cisco Aironet 1815 Teleworker Access Point at teleworker locations can reach the WLC. However, in order for the Cisco Aironet 1815T(Teleworker) Access Point to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface.

To configure the WLC for NAT, perform the following steps:

### Procedure

---

- Step 1** In **Controller > Interfaces**, click the management interface.
- Step 2** Select **Enable NAT Address**.
- Step 3** In the **NAT IP Address** box, enter the publicly reachable IP address, and then click **Apply**. (Example: 172.16.130.20)

**Note** The NAT IP Address must be the external, globally unique IP address that the Wireless LAN Controller displays on the Internet. This allows the WLC to place this IP address into the CAPWAP discovery response packet prior to encryption. The address shown here is an RFC-1918, private IP address and is used in this guide only for documentation purposes.

The screenshot shows the Cisco WLC configuration interface for the 'management' interface. The configuration is as follows:

Section	Parameter	Value
General Information	Interface Name	management
	MAC Address	d0:d0:fd:1f:59:e0
Configuration	Quarantine	<input checked="" type="checkbox"/>
	Quarantine Vlan Id	0
NAT Address	Enable NAT Address	<input checked="" type="checkbox"/>
	NAT IP Address	172.16.130.20
Interface Address	VLAN Identifier	0
	IP Address	192.168.19.20
	Netmask	255.255.255.0
	Gateway	192.168.19.1
Physical Information	Port Number	1
	Backup Port	0
	Active Port	1
	Enable Dynamic AP Management	<input checked="" type="checkbox"/>
DHCP Information	Primary DHCP Server	10.4.48.10
	Secondary DHCP Server	0.0.0.0
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.

## Configuring the Time Zone

To configure the time zone, perform the following steps:

### Procedure

- Step 1** Navigate to **Commands > Set Time**.
- Step 2** In the Location list, choose the time zone that corresponds to the location of the WLC.
- Step 3** Click Set Timezone.

The screenshot shows the Cisco WLC configuration interface for setting time and timezone. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS (selected), HELP, and FEEDBACK. In the top right corner of the header, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. On the left side, there is a 'Commands' menu with options: Download File, Upload File, Reboot, Config Boot, Scheduled Reboot (selected), Reset to Factory Default, Set Time, and Login Banner. The main content area is titled 'Set Time' and contains two buttons: 'Set Date and Time' and 'Set Timezone'. Below these buttons, the 'Current Time' is displayed as 'Tue May 31 11:07:38 2011'. The 'Date' section includes dropdown menus for Month (May), Day (31), and Year (2011). The 'Time' section includes dropdown menus for Hour (11), Minutes (7), and Seconds (38). The 'Timezone' section includes a 'Delta' field with 'hours 0' and 'mins 0' input boxes, and a 'Location' dropdown menu set to '(GMT -8:00) Pacific Time (US and Canada)'. At the bottom, there is a 'Foot Notes' section with a single note: '1. Automatically sets daylight savings time where used.'

## Configuring SNMP

To configure SNMP, perform the following tasks:

### Procedure

- Step 1** In **Management > SNMP > Communities**, click **New**.
- Step 2** Enter the **Community Name**. (Example: cisco)
- Step 3** Enter the IP Address. (Example: 10.4.48.0)
- Step 4** Enter the IP Mask. (Example: 255.255.255.0)
- Step 5** In the **Status** list, choose **Enable**, and then click **Apply**.

Management

SNMP v1 / v2c Community > New

Community Name:

IP Address:

IP Mask:

Access Mode:

Status:

Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management
- Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

Save Configuration | Ping | Logout | Refresh

< Back | Apply

**Step 6** In **Management > SNMP > Communities**, click **New**.

**Step 7** Enter the **Community Name**. (Example: cisco123)

**Step 8** Enter the **IP Address**. (Example: 10.4.48.0)

**Step 9** Enter the **IP Mask**. (Example: 255.255.255.0)

**Step 10** In the **Access Mode** list, choose Read/Write.

**Step 11** In the **Status** list, choose **Enable**, and then click **Apply**.

Management

SNMP v1 / v2c Community > New

Community Name:

IP Address:

IP Mask:

Access Mode:

Status:

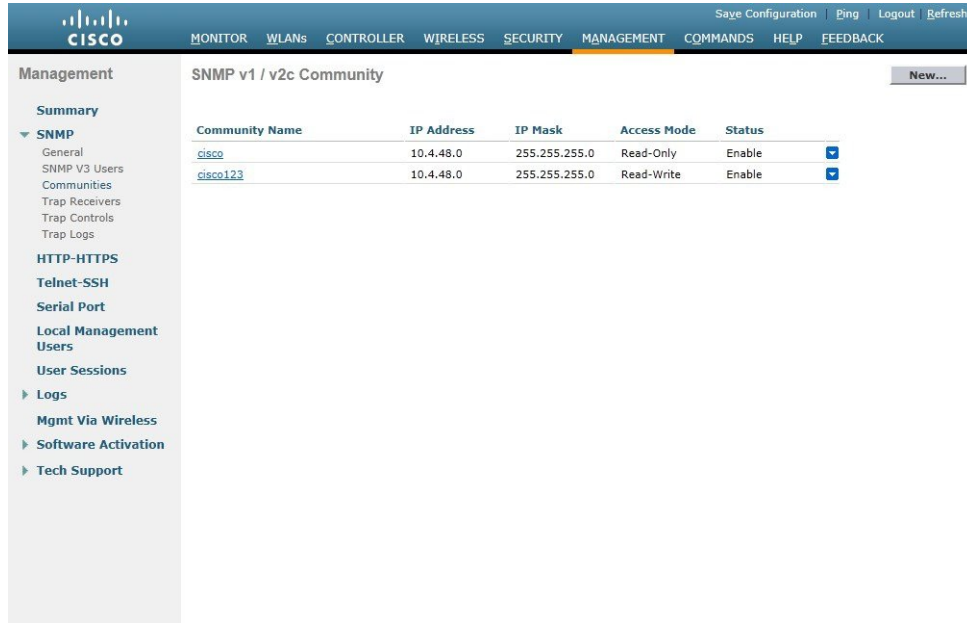
Summary

- SNMP
  - General
  - SNMP V3 Users
  - Communities
  - Trap Receivers
  - Trap Controls
  - Trap Logs
- HTTP-HTTPS
- Telnet-SSH
- Serial Port
- Local Management
- Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Software Activation
- Tech Support

Save Configuration | Ping | Logout | Refresh

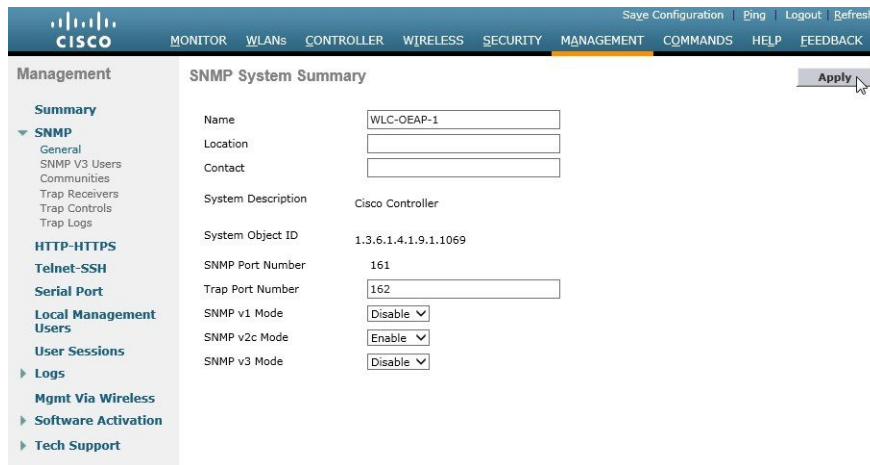
< Back | Apply

- Step 12** Navigate to **Management > SNMP > Communities**.
- Step 13** Point to the blue box for the public community, and then click **Remove**.
- Step 14** On the "Are you sure you want to delete?" message,click **OK** .
- Step 15** Repeat Step 13 and Step 14 for the private community.



- Step 16** Navigate to **Management > SNMP > General** and disable SNMP v3 Mode, and click **Apply**.

Figure 1:



- Step 17** Navigate to **Management > SNMP Communities > SNMP V3 Users**.
- Step 18** On the right side of the default **User Name**, point and click the blue down arrow, and then click **Remove**.

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'MANAGEMENT' tab is active. On the left, the 'Management' sidebar is expanded to 'SNMP'. The main content area is titled 'SNMP V3 Users' and contains a table with the following data:

User Name	Access Level	Auth Protocol	Privacy Protocol
default	Readwrite	HMAC-SHA	AES

A 'Remove' button is visible next to the 'default' user entry, and a 'New...' button is in the top right corner of the table area.

**Step 19** Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**.

This screenshot shows the same Cisco WLC Management interface as the previous one, but with a confirmation dialog box open. The dialog box is titled 'Message from webpage' and contains the question 'Are you sure you want to delete?' with 'OK' and 'Cancel' buttons. The 'default' user is still visible in the table behind the dialog.

**Note** Changes to the SNMP configuration may sometimes require that the WLC be rebooted.

# Configuring Wireless User Authentication

## Procedure

- Step 1** In **Security > AAA > Radius > Authentication**, click **New**.
- Step 2** Enter the **Server IP Address**. (Example: 10.4.48.15)
- Step 3** Enter and confirm the **Shared Secret**. (Example: SecretKey)
- Step 4** To the right of **Management**, clear **Enable**, and then click **Apply**.

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'RADIUS' expanded. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 1
- Server IP Address: 10.4.48.15
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User:  Enable
- Management:  Enable
- IPSec:  Enable

- Step 5** To the right of **Management**, clear **Enable**, and then click **Apply**.
- Step 6** Enter the **Server IP Address**. (Example: 10.4.48.15)
- Step 7** Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

Save Configuration | Bing | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security **RADIUS Accounting Servers > New** < Back Apply

AAA

- General
- ▼ RADIUS
  - Authentication
  - Accounting
  - Fallback
- ▶ TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- ▶ Local EAP
- ▶ Priority Order
- ▶ Certificate
- ▶ Access Control Lists
- ▶ Wireless Protection Policies
- ▶ Web Auth
- TrustSec SXP
- ▶ Advanced

Server Index (Priority)

Server IP Address

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout  seconds

Network User  Enable

IPSec  Enable