Wireless LAN Controller (WLC) and NAC Guest Server (NGS) Integration Guide

Document ID: 107630

Introduction

This document provides a guideline to integrate the NAC Guest Server and Wireless LAN Controllers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Wireless LAN Controller (WLC) 4.2.61.0
- Catalyst 3560 with IOS® Version 12.2(25)SEE2
- Cisco ADU Version 4.0.0.279
- NAC Guest Server Version 1.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Background Information

The Cisco NAC Guest Server is a complete provisioning and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers. The Guest Server works alongside Cisco NAC Appliance or Cisco Wireless LAN Controller, which provides the captive portal and enforcement point for guest access.

Cisco NAC Guest Server allows any user with privileges to easily create temporary guest accounts and sponsor guests. Cisco NAC Guest Server performs full authentication of sponsors, the users who create guest accounts, and allows sponsors to provide account details to the guest by printout, email, or SMS. The entire experience, from user account creation to guest network access, is stored for audit and reporting.

When guest accounts are created, they are either provisioned within the Cisco NAC Appliance Manager (Clean Access Manager) or stored within the built−in database on the Cisco NAC Guest Server. When you use the built−in database of the Guest Server, external network access devices, such as the Cisco Wireless LAN Controller, can authenticate users against the Guest Server with the Remote Authentication Dial In User Service (RADIUS) protocol.

The Cisco NAC Guest Server provisions the guest account for the amount of time specified when the account is created. Upon expiry of the account, the Guest Server either deletes the account directly from the Cisco NAC Appliance Manager or sends a RADIUS message that notifies the network access device (NAD) of the amount of valid time that remains for the account before the NAD must remove the user.

The Cisco NAC Guest Server provides vital guest network access accounting by consolidation of the entire audit trail from guest account creation to guest use of the account so that reports can be performed through a central management interface.

Guest Access Concepts

Cisco NAC Guest Server makes use of a number of terms to explain the components needed to provide guest access.

Guest User

The guest user is the person who needs a user account to access the network.

Sponsor

The Sponsor is the person who creates the guest user account. This person is often an employee of the organization that provides the network access. Sponsors can be specific − 3 − individuals with certain job roles, or can be any employee who can authenticate against a corporate directory such as Microsoft Active Directory (AD).

Network Enforcement Device

These devices are the network infrastructure components that provide the network access. Additionally, network enforcement devices push guest users to a captive portal, where they can enter their guest account details. When a guest enters his or her temporary user name and password, the network enforcement device checks those credentials against the guest accounts created by the Guest Server.

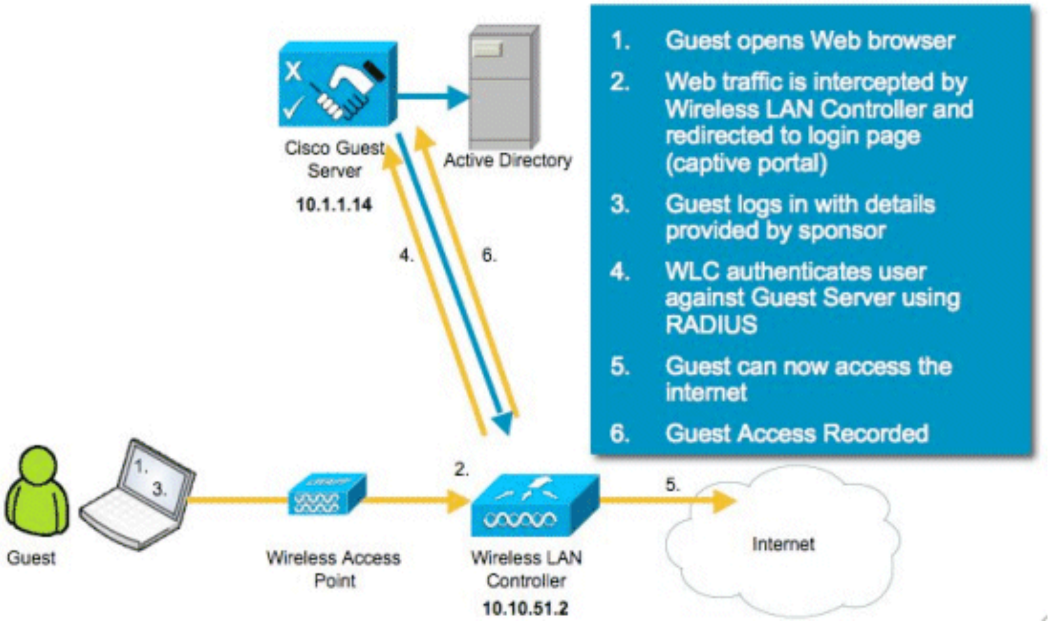
Guest Server

This is the Cisco NAC Guest Server, which ties together all the pieces of guest access. The Guest Server links these together: the sponsor that creates the guest account, the account details passed to the guest, the guest authentication against the network enforcement device, and the verification of the network enforcement device of the guest with the Guest Server. Additionally, the Cisco NAC Guest Server consolidates accounting information from network enforcement devices to provide a single point of guest access reports.

Detailed documentation on NGS is available in CCO.

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/10/nacguestserver.html

Lab Topology Overview



1. Guest opens Web browser
2. Web traffic is intercepted by Wireless LAN Controller and redirected to login page (captive portal)
3. Guest logs in with details provided by sponsor
4. WLC authenticates user against Guest Server using RADIUS
5. Guest can now access the internet
6. Guest Access Recorded

Configure the Wireless LAN Controller (WLC)

Follow these steps to configure the WLC:

1. Initialize the controller and access point.
2. Configure the controller interfaces.
3. Configure RADIUS.
4. Configure the WLAN settings.

Initialization

For the initial configuration, use a console connection like HyperTerminal and follow the setup prompts to populate login and interface information. The **reset system** command also initiates these prompts.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_44:36:c3]: WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): admin
Service Interface IP Address Configuration [none][DHCP]: <ENTER>
Enable Link Aggregation (LAG) [yes][NO]:no
Management Interface IP Address: 10.10.51.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.51.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 10.10.51.1
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 10.10.51.3
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.10.5<X>.1):<ENTER>
Virtual Gateway IP Address: 1.1.1.1
```

```
Mobility/RF Group Name: mobile-1
Enable Symmetric Mobility Tunneling: No
Network Name (SSID): wireless-1
Allow Static IP Addresses [YES][no]:<ENTER>
Configure a RADIUS Server now? [YES][no]:<ENTER>
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:<ENTER>
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:<ENTER>
Enable 802.11b Network [YES][no]:<ENTER>
Enable 802.11a Network [YES][no]:<ENTER>
Enable 802.11g Network [YES][no]:<ENTER>
Enable Auto-RF [YES][no]:<ENTER>
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
```

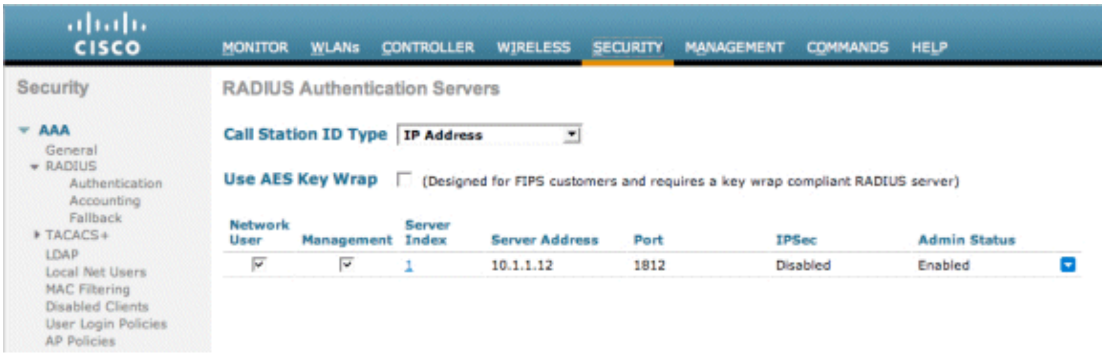
Cisco NAC Guest Server

The Cisco NAC Guest Server is a provisioning and reporting solution that provides temporary network access to clients such as guests, contractors, etc. The Cisco NAC Guest Server works with the Cisco Unified Wireless Network or Cisco NAC Appliance solutions. This document walks you through the steps to integrate the Cisco NAC Guest Server with a Cisco WLC, which creates a guest user account and verifies the temporary network access of the guest.

Follow these steps to complete the integration:

1. Add the Cisco NAC Guest Server as an Authentication Server in the WLC.

    a. Browse to your WLC (https://10.10.51.2, admin/admin) to configure this.
    b. Choose **Security > RADIUS > Authentication**.



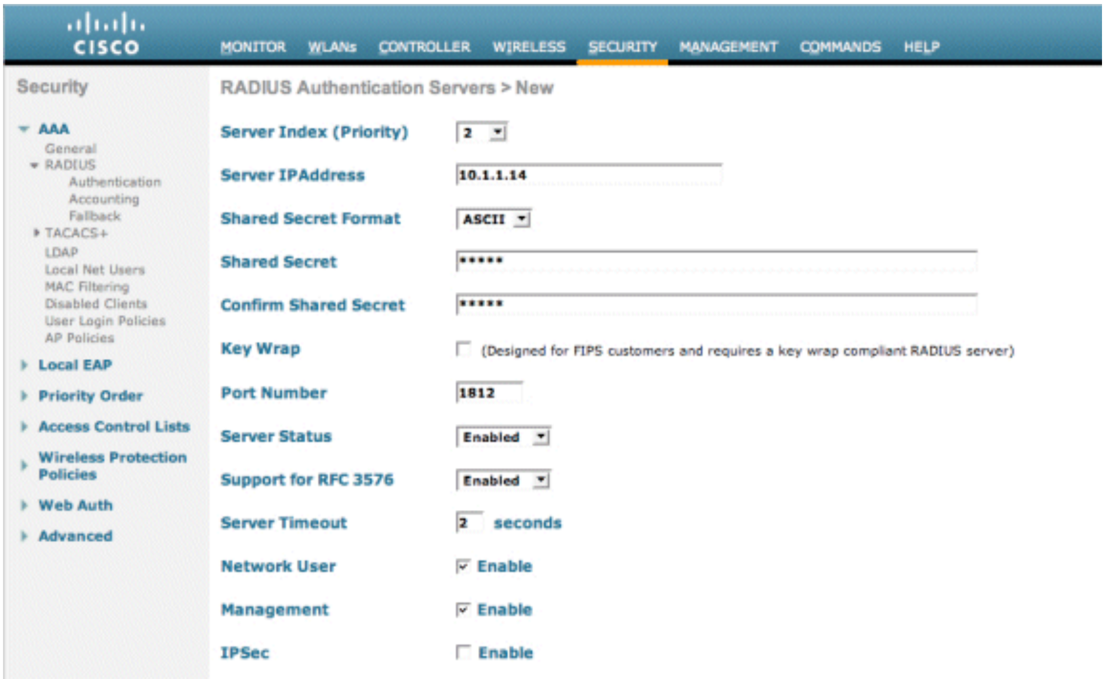
RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
☑	☑	1	10.1.1.12	1812	Disabled	Enabled

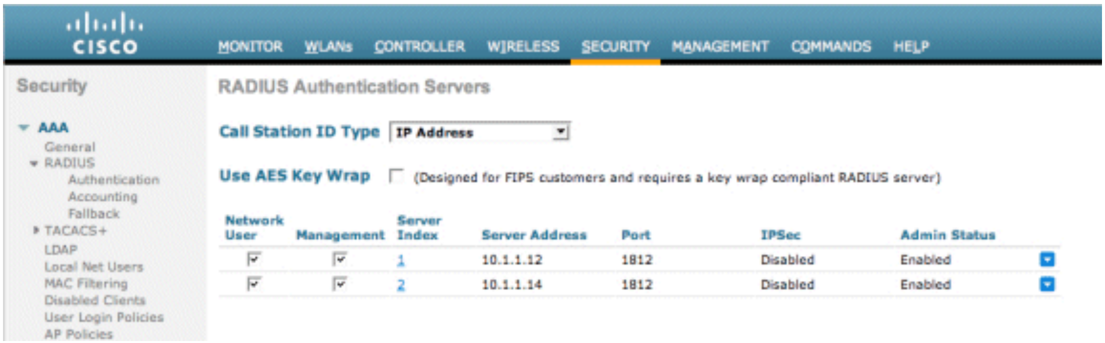
    c. Choose **New**.
    d. Add the IP Address (10.1.1.14) for the Cisco NAC Guest Server.
    e. Add the Shared Secret.
    f. Confirm the Shared Secret.



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IPAddress	10.1.1.14
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
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

g. Choose **Apply**.



RADIUS Authentication Servers

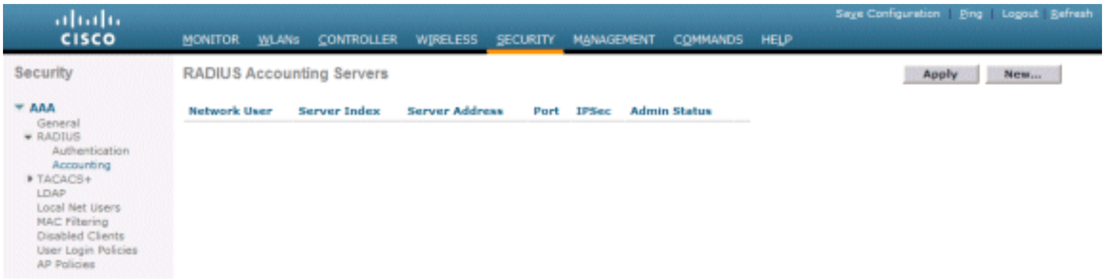
Call Station ID Type: IP Address

Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
☑	☑	1	10.1.1.12	1812	Disabled	Enabled
☑	☑	2	10.1.1.14	1812	Disabled	Enabled

2. Add the Cisco NAC Guest Server as an accounting server in the WLC.

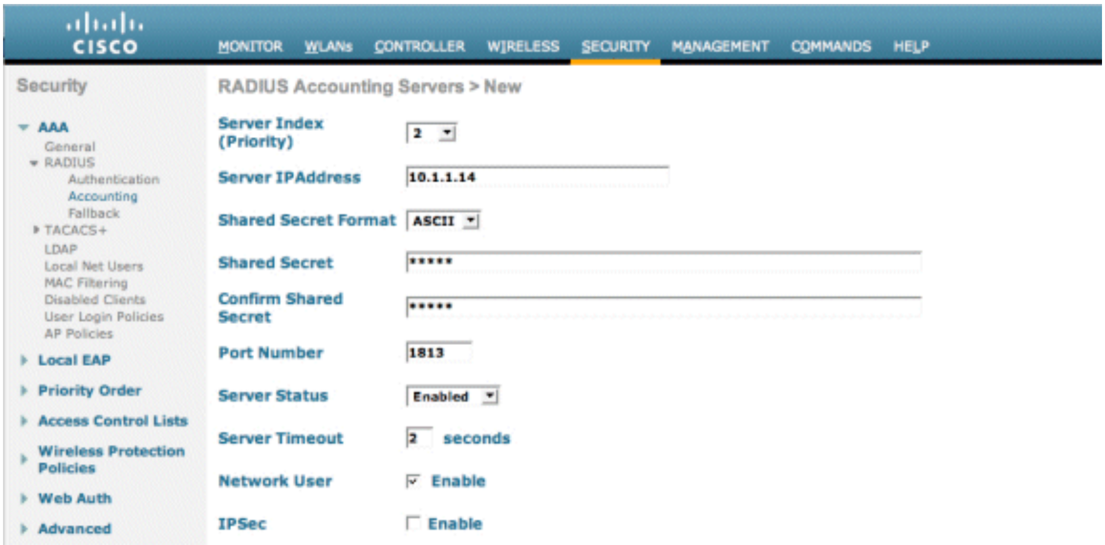
a. Choose **Security > RADIUS >Accounting**.



RADIUS Accounting Servers

Network User	Server Index	Server Address	Port	IPSec	Admin Status

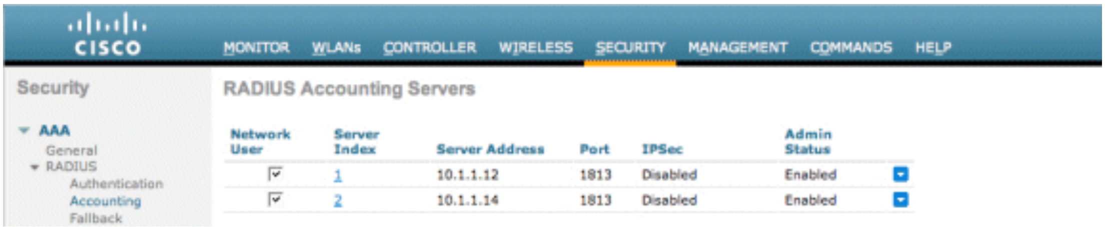
b. Choose **New**.
c. Add the IP Address (10.1.1.14) for the Cisco NAC Guest Server.
d. Add the Shared Secret.
e. Confirm the Shared Secret.



RADIUS Accounting Servers > New

Server Index (Priority)	2
Server IPAddress	10.1.1.14
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
IPSec	□ Enable

f. Choose **Apply**.

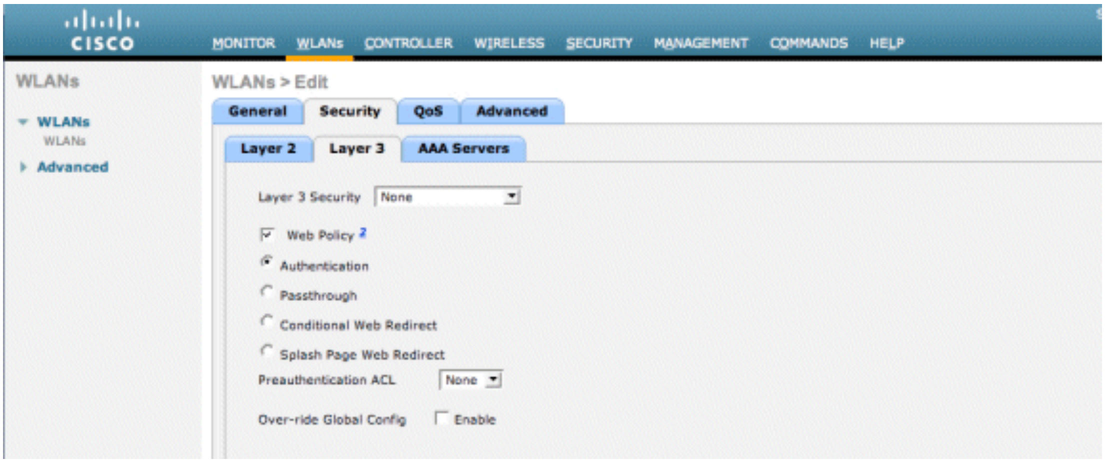

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback

RADIUS Accounting Servers

Network User	Server Index	Server Address	Port	IPSec	Admin Status
☑	1	10.1.1.12	1813	Disabled	Enabled
☑	2	10.1.1.14	1813	Disabled	Enabled

3. Modify the WLAN (wireless−x) to use the NAC Guest Server.

a. Edit the WLAN (wireless−x).
b. Choose the **Security** tab.
c. Change the Layer 2 Security to **None** and Layer 3 Security to use **Web Authentication**.



WLANs > Edit

Layer 3 Security: None

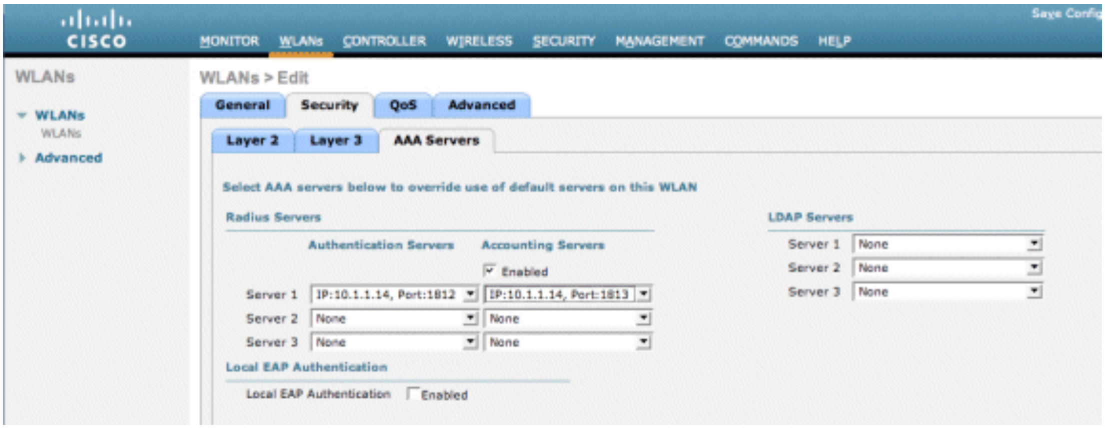
☑ Web Policy

● Authentication
○ Passthrough
○ Conditional Web Redirect
○ Splash Page Web Redirect

Preauthentication ACL: None

Over-ride Global Config: □ Enable

d. Choose the **AAA Servers** under the Security tab.
e. Under the Server 1 box, choose the **RADIUS server (10.1.1.14)**.
f. Under the Server 1 box, choose the **Accounting Server (10.1.1.14)**.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Config
WLANs
WLANs
WLANs
Advanced
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	IP:10.1.1.14, Port:1812	IP:10.1.1.14, Port:1813
Server 2	None	None
Server 3	None	None

LDAP Servers

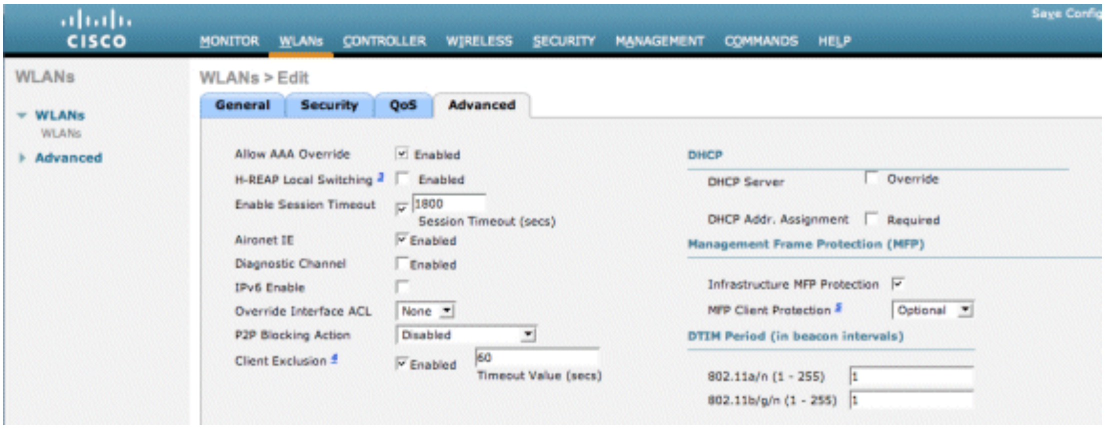
Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication □ Enabled

g. Choose the the **Advanced** tab.

h. Enable **Allow AAA Override**. This allows the per client session timeout to be set from the NAC Guest Appliance.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Config
WLANs
WLANs
WLANs
Advanced
General Security QoS Advanced

WLANs > Edit

Allow AAA Override ☑ Enabled

H-REAP Local Switching □ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

IPv6 Enable □

Override Interface ACL None

P2P Blocking Action Disabled

Client Exclusion ☑ Enabled 60 Timeout Value (secs)

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑

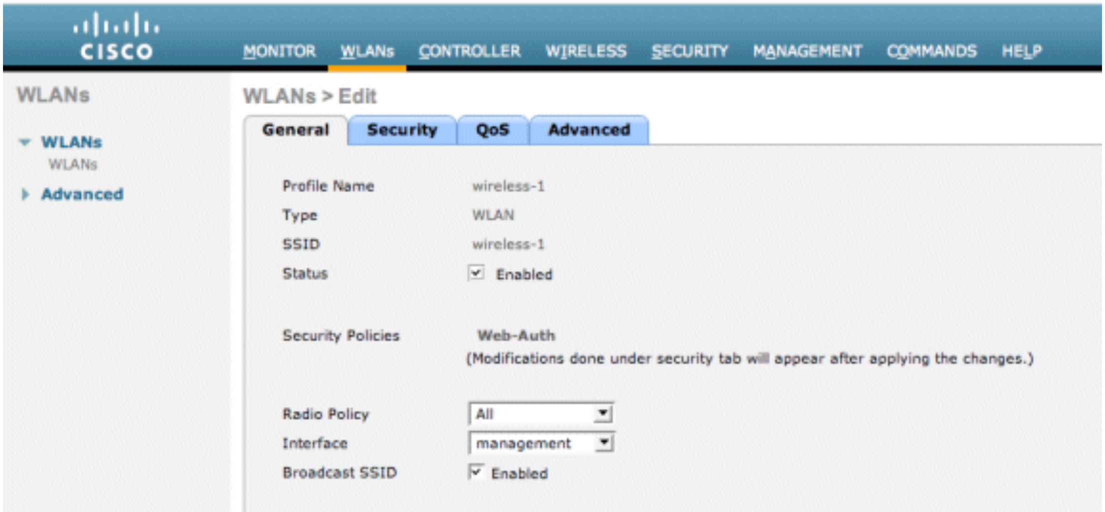
MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

i. Choose **Apply** to save your WLAN configuration.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
General Security QoS Advanced

WLANs > Edit

Profile Name wireless-1

Type WLAN

SSID wireless-1

Status ☑ Enabled

Security Policies Web-Auth

(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

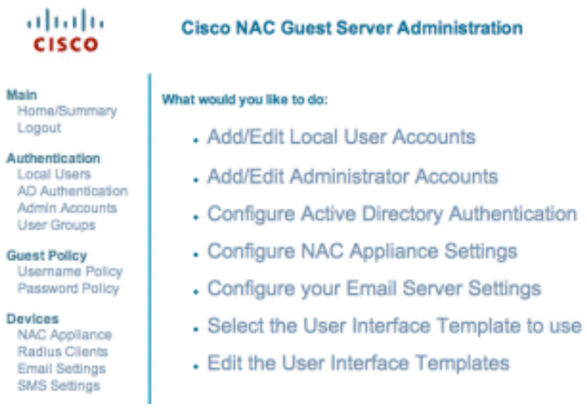
Interface management

Broadcast SSID ☑ Enabled

4. Verify whether the controller is added as a Radius Client in the Cisco NAC Guest Server.

a. Browse to the NAC Guest Server (https://10.1.1.14/admin) to configure this.

Note: You get the Administration page if you specify the /admin in the URL.

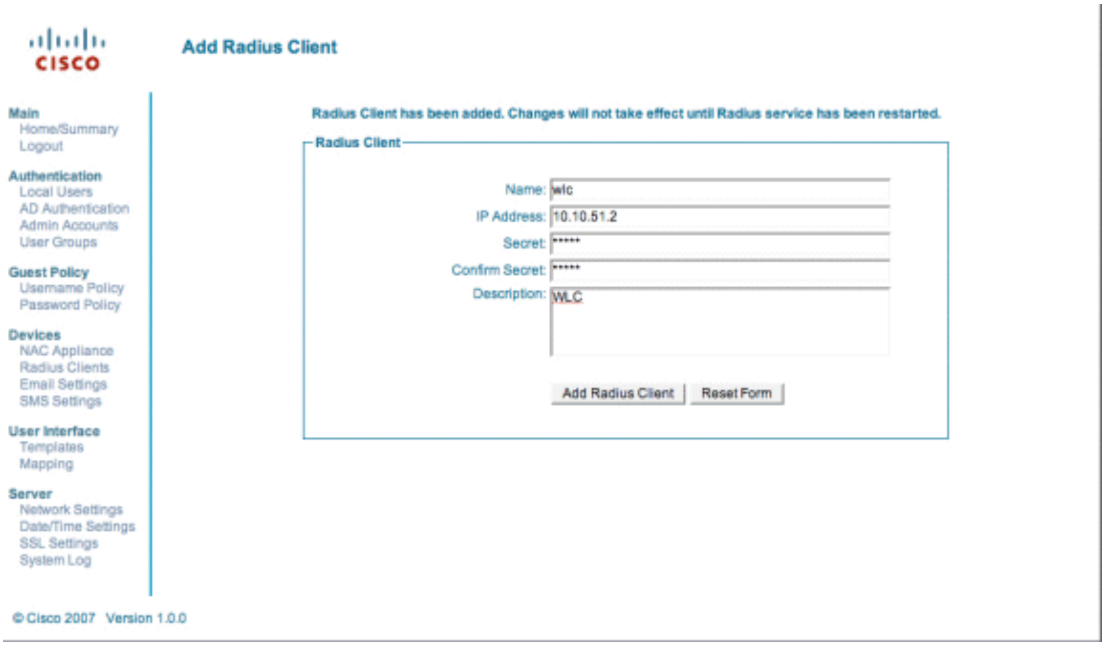

Cisco NAC Guest Server Administration
Main
Home/Summary
Logout
Authentication
Local Users
AD Authentication
Admin Accounts
User Groups
Guest Policy
Username Policy
Password Policy
Devices
NAC Appliance
Radius Clients
Email Settings
SMS Settings
What would you like to do:
Add/Edit Local User Accounts
Add/Edit Administrator Accounts
Configure Active Directory Authentication
Configure NAC Appliance Settings
Configure your Email Server Settings
Select the User Interface Template to use
Edit the User Interface Templates

b. Choose **Radius Clients**.

c. Choose **Add Radius**.

d. Enter the Radius Client information:

◊ Enter a name: WLC system name.
◊ Enter the IP address: IP address of WLC **(10.10.51.2)**.
◊ Enter the same shared secret that you entered in Step 1.
◊ Confirm your shared secret.
◊ Enter a description.
◊ Choose **Add Radius Client**.



Radius Client has been added. Changes will not take effect until Radius service has been restarted.

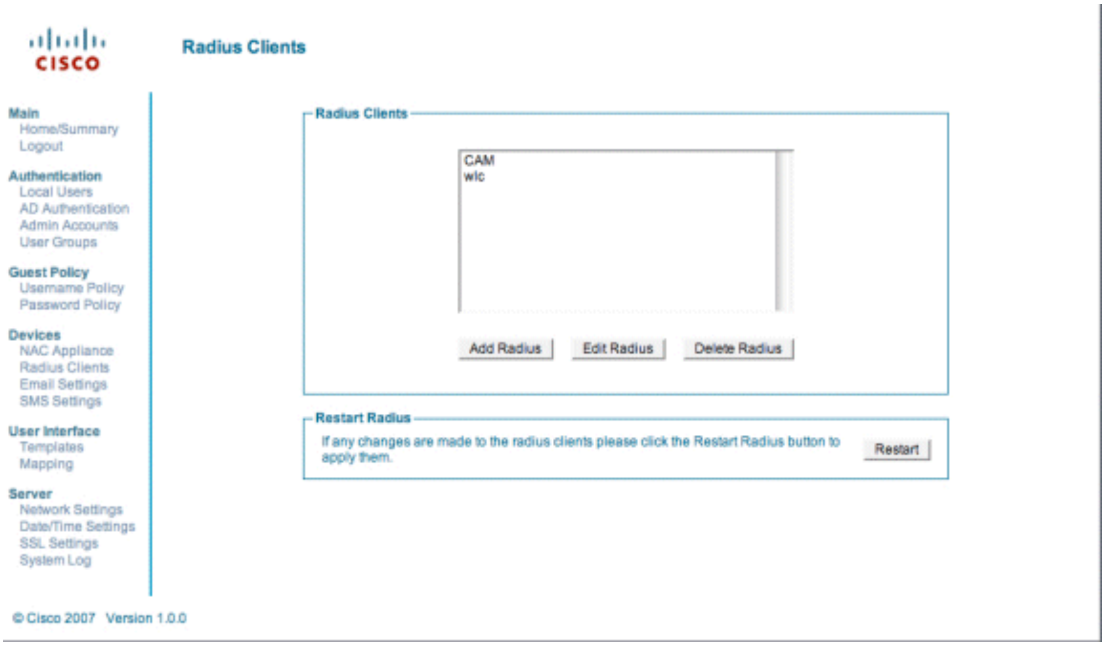
Radius Client

Name: wlc
IP Address: 10.10.51.2
Secret: *****
Confirm Secret: *****
Description: WLC

e. Restart the Radius Service in order for the changes to take effect.

f. Choose **Radius Clients**.

g. Choose **Restart** in the Restart Radius box.



Radius Clients

Radius Clients

CAM
wlc

Restart Radius

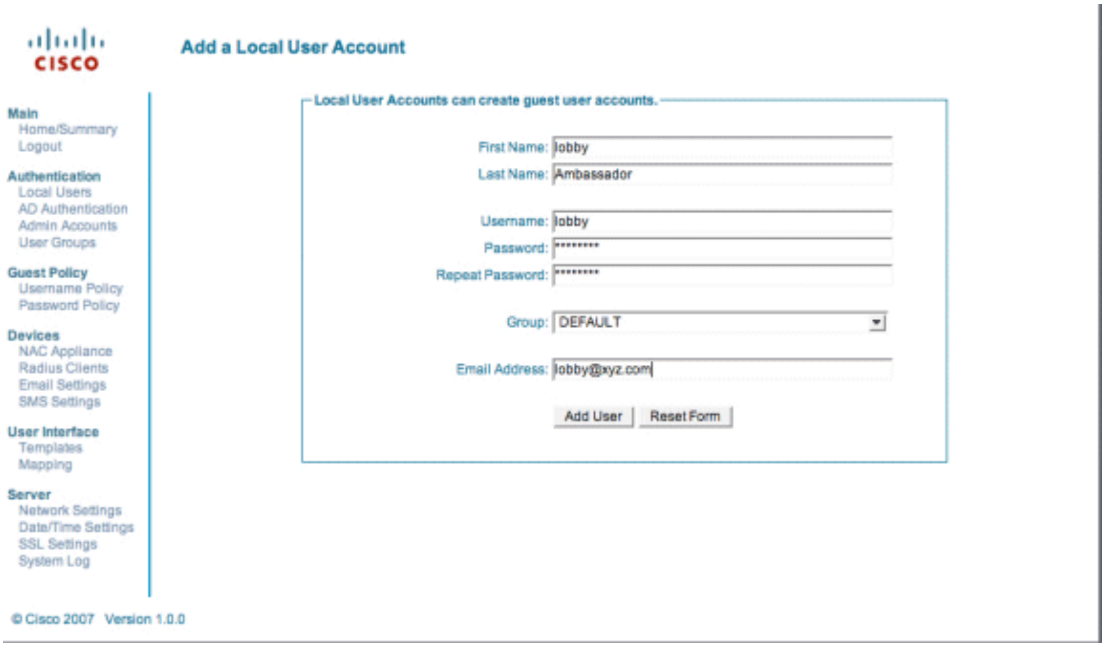
If any changes are made to the radius clients please click the Restart Radius button to apply them.

5. Create a Local User, that is, Lobby Ambassador, in the Cisco NAC Guest Server.

   a. Choose **Local Users**.
   b. Choose **Add User**.

   Note: You must fill in all fields.

   c. Enter a First Name: **lobby**.
   d. Enter a Last Name: **Ambassador**.
   e. Enter Username: **lobby**.
   f. Enter a Password: **password**.
   g. Leave Group as **Default**.
   h. Enter Email Address: **lobby@xyz.com**.
   i. Choose **Add User**.



Add a Local User Account

Local User Accounts can create guest user accounts.

First Name: lobby
Last Name: Ambassador

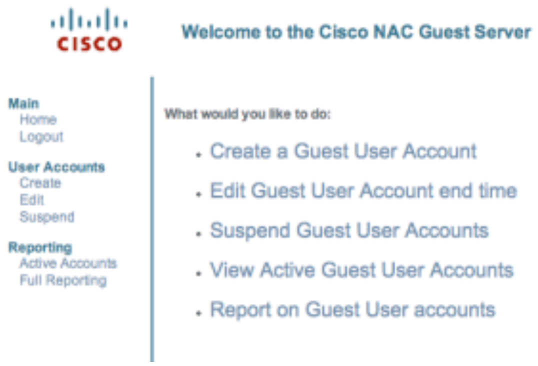
Username: lobby
Password: ********
Repeat Password: ********

Group: DEFAULT

Email Address: lobby@xyz.com

6. Login as the Local User and create a guest account.

   a. Browse to the NAC Guest Server (https://10.1.1.14), login with the user name/password you created in Step 5, and configure this:



Welcome to the Cisco NAC Guest Server

What would you like to do:

- Create a Guest User Account
- Edit Guest User Account end time
- Suspend Guest User Accounts
- View Active Guest User Accounts
- Report on Guest User accounts

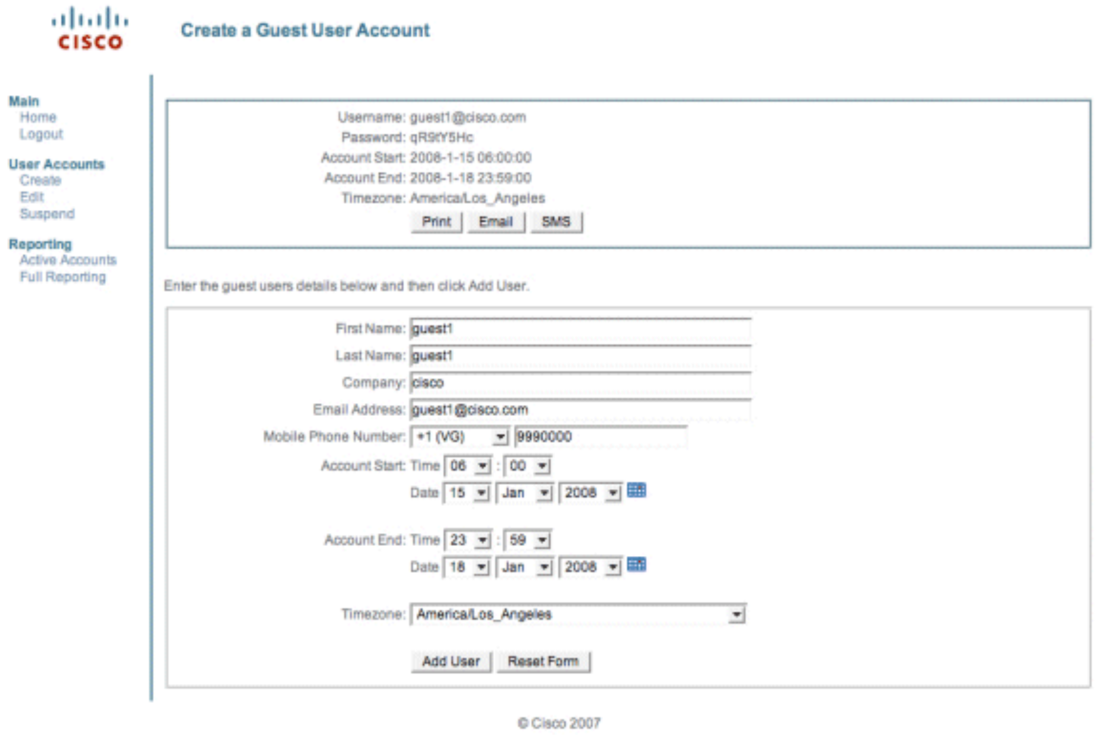
b. Choose **Create** for a guest user account.

Note: You must fill in all fields.

c. Enter a First Name.
d. Enter a Last Name.
e. Enter the Company.
f. Enter the Email Address.

Note: The email address is the Username.

g. Enter the Account End: **Time**.
h. Choose **Add User**.



Create a Guest User Account

Username: guest1@cisco.com
Password: qR9tY5Hc
Account Start: 2008-1-15 06:00:00
Account End: 2008-1-18 23:59:00
Timezone: America/Los_Angeles

Enter the guest users details below and then click Add User.

First Name: guest1
Last Name: guest1
Company: cisco
Email Address: guest1@cisco.com
Mobile Phone Number: +1 (VG) 9990000
Account Start: Time 06 : 00
Date 15 Jan 2008
Account End: Time 23 : 59
Date 18 Jan 2008
Timezone: America/Los_Angeles

© Cisco 2007

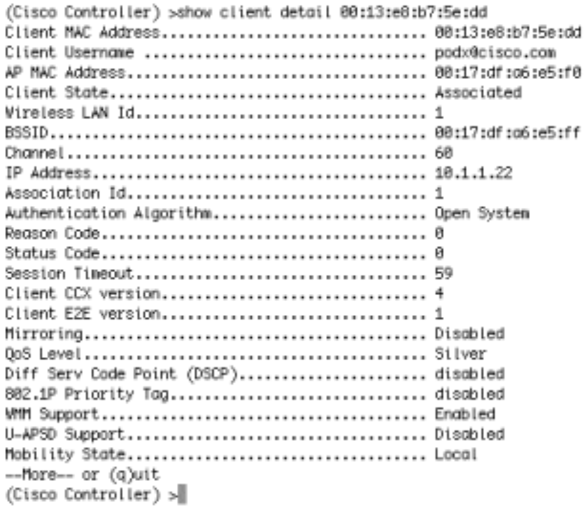
7. Connect to the guest WLAN and login as the guest user.

a. Connect your wireless client to the guest WLAN (wireless−x).
b. Open the web browser to be redirected to the Web−Auth Login page.

Note: Alternatively, type **https://1.1.1.1/login.html** to be redirected to the Login page.

c. Enter the guest User Name that you created in Step 6.
d. Enter the Password that was auto−generated in Step 6.
e. Telnet to the WLC and verify that the Session Timeout has been set with the **show client detail** command.

f. When the Session Timeout expires, the guest client is disconnected, and your ping stops.



```
(Cisco Controller) >show client detail 00:13:e8:b7:5e:dd
Client MAC Address........................ 00:13:e8:b7:5e:dd
Client Username .......................... podx@cisco.com
AP MAC Address............................ 00:17:df:a6:e5:f0
Client State.............................. Associated
Wireless LAN Id........................... 1
BSSID..................................... 00:17:df:a6:e5:ff
Channel................................... 60
IP Address................................ 10.1.1.22
Association Id............................ 1
Authentication Algorithm.................. Open System
Reason Code............................... 0
Status Code............................... 0
Session Timeout........................... 59
Client CCX version........................ 4
Client E2E version........................ 1
Mirroring................................. Disabled
QoS Level................................. Silver
Diff Serv Code Point (DSCP)............... disabled
802.1P Priority Tag....................... disabled
WMM Support............................... Enabled
U-APSD Support............................ Disabled
Mobility State............................ Local
--More-- or (q)uit
(Cisco Controller) >
```

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

- **Cisco NAC Appliance − Clean Access Manager Installation and Configuration Guide, Release 4.1(3)**
- **Cisco Wireless LAN Controller Configuration Guide, Release 5.1**
- **NAC (Clean Access): Configure Guest Access**
- **Deployment Guide: Cisco Guest Access Using the Cisco Wireless LAN Controller, Release 4.1**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 01, 2008 Document ID: 107630