WLC和NAC Guest Server(NGS)整合指南

目錄

簡介

本檔案將提供有關整合NAC訪客伺服器和無線LAN控制器的准則。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco無線LAN控制器(WLC)4.2.61.0
- 採用IOS®版本12.2(25)SEE2的Catalyst 3560
- Cisco ADU版本4.0.0.279
- NAC訪客伺服器版本1.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

Cisco NAC Guest Server是一個完整的調配和報告系統，為訪客、訪客、承包商、顧問或客戶提供臨時網路訪問。訪客伺服器與Cisco NAC裝置或思科無線LAN控制器配合使用，後者為訪客訪問提供強制網路門戶和實施點。

Cisco NAC Guest Server允許具有許可權的任何使用者輕鬆建立臨時訪客帳戶和發起訪客。Cisco NAC Guest Server對發起人（建立訪客帳戶的使用者）執行完全身份驗證，並允許發起人通過列印輸出、電子郵件或SMS向訪客提供帳戶詳細資訊。整個體驗（從使用者帳戶建立到訪客網路訪問）都儲存為稽核和報告。

建立訪客帳戶後，這些帳戶在Cisco NAC裝置管理器(Clean Access Manager)中調配，或者儲存在Cisco NAC訪客伺服器上的內建資料庫中。使用訪客伺服器的內建資料庫時，外部網路存取裝置（例如思科無線LAN控制器）可以使用遠端驗證撥入使用者服務(RADIUS)通訊協定對訪客伺服器驗證使用者身分。

Cisco NAC Guest Server會在建立帳戶時指定的時間內設定訪客帳戶。帳戶到期後，訪客伺服器會直接從Cisco NAC裝置管理器刪除帳戶，或傳送一則RADIUS消息，通知網路接入裝置(NAD)帳戶在需要刪除使用者之前的有效時間量。

Cisco NAC Guest Server通過整合從訪客帳戶建立到訪客帳戶使用的整個稽核跟蹤來提供重要的訪客網路訪問記帳，以便可以通過中央管理介面執行報告。

訪客存取概念

Cisco NAC Guest Server使用許多術語來解釋提供訪客訪問所需的元件。

訪客使用者

訪客使用者是需要使用者帳戶來訪問網路的人。

發起人

發起人是建立訪客使用者帳戶的人。此人通常是提供網路訪問的組織的員工。保證人可以是特定的— 3 — 具有特定工作角色的人員，也可以是能夠根據公司目錄(如Microsoft Active Directory(AD))進行身份驗證的任何員工。

網路執行裝置

這些裝置是提供網路訪問的網路基礎設施元件。此外，網路實施裝置會將訪客使用者推送到強制網路門戶，在該門戶中，他們可以輸入其訪客帳戶詳細資訊。當訪客輸入其臨時使用者名稱和密碼時，網路實施裝置會根據訪客伺服器建立的訪客帳戶檢查這些憑證。

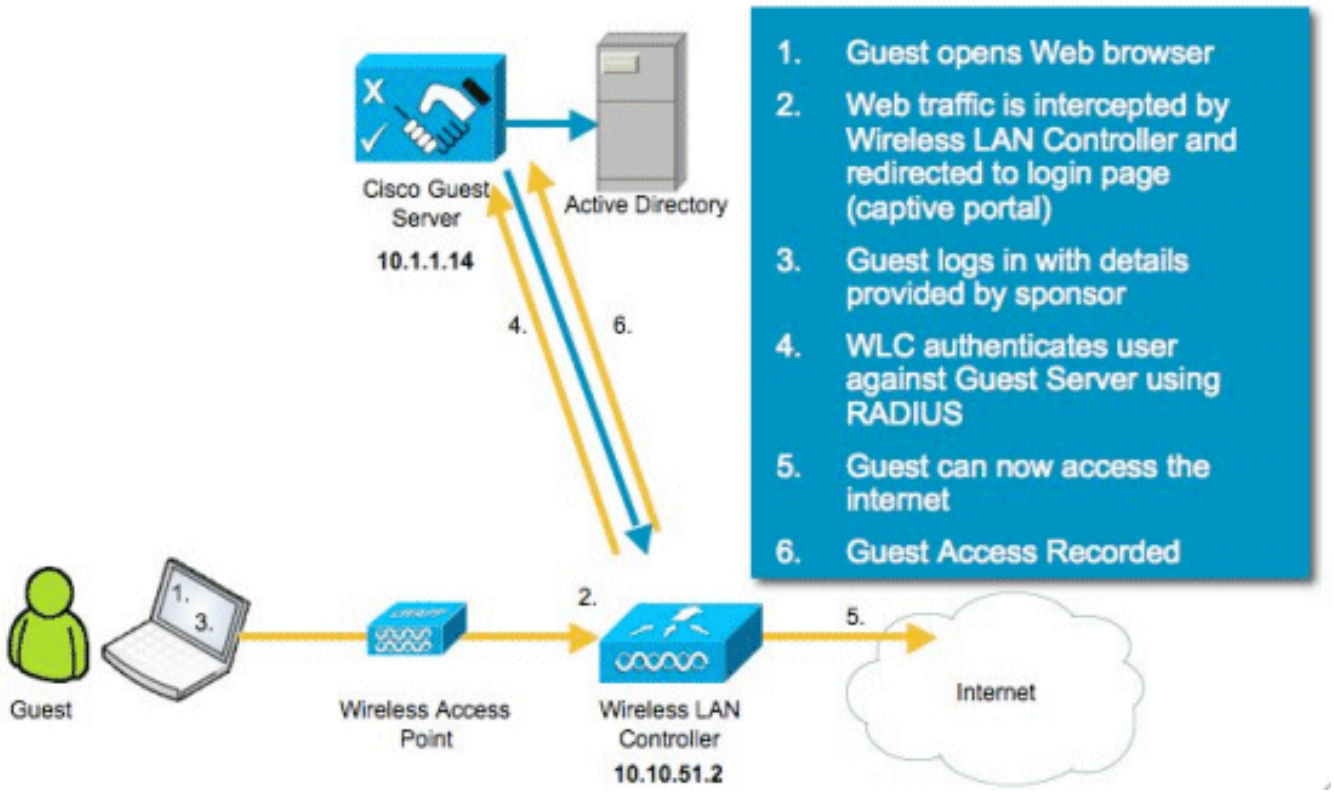
訪客伺服器

這是Cisco NAC訪客伺服器，將訪客訪問的所有部分連線在一起。訪客伺服器將這些連結在一起：建立訪客帳戶的發起人、傳遞至訪客的帳戶詳細資訊、針對網路實施裝置的訪客身份驗證，以及訪客的網路實施裝置與訪客伺服器的驗證。此外，Cisco NAC Guest Server整合來自網路實施裝置的記帳資訊，以提供單點訪客訪問報告。

CCO中提供了有關NGS的詳細文檔。

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

實驗拓撲概述



設定無線區域網路控制器(WLC)

請依照以下步驟設定WLC:

1. 初始化控制器和接入點。
2. 設定控制器介面。
3. 設定RADIUS。
4. 配置WLAN設定。

初始化

對於初始配置，請使用控制檯連線（如HyperTerminal）並按照設定提示填充登入和介面資訊。**reset system**命令也會啟動這些提示。

```
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
```

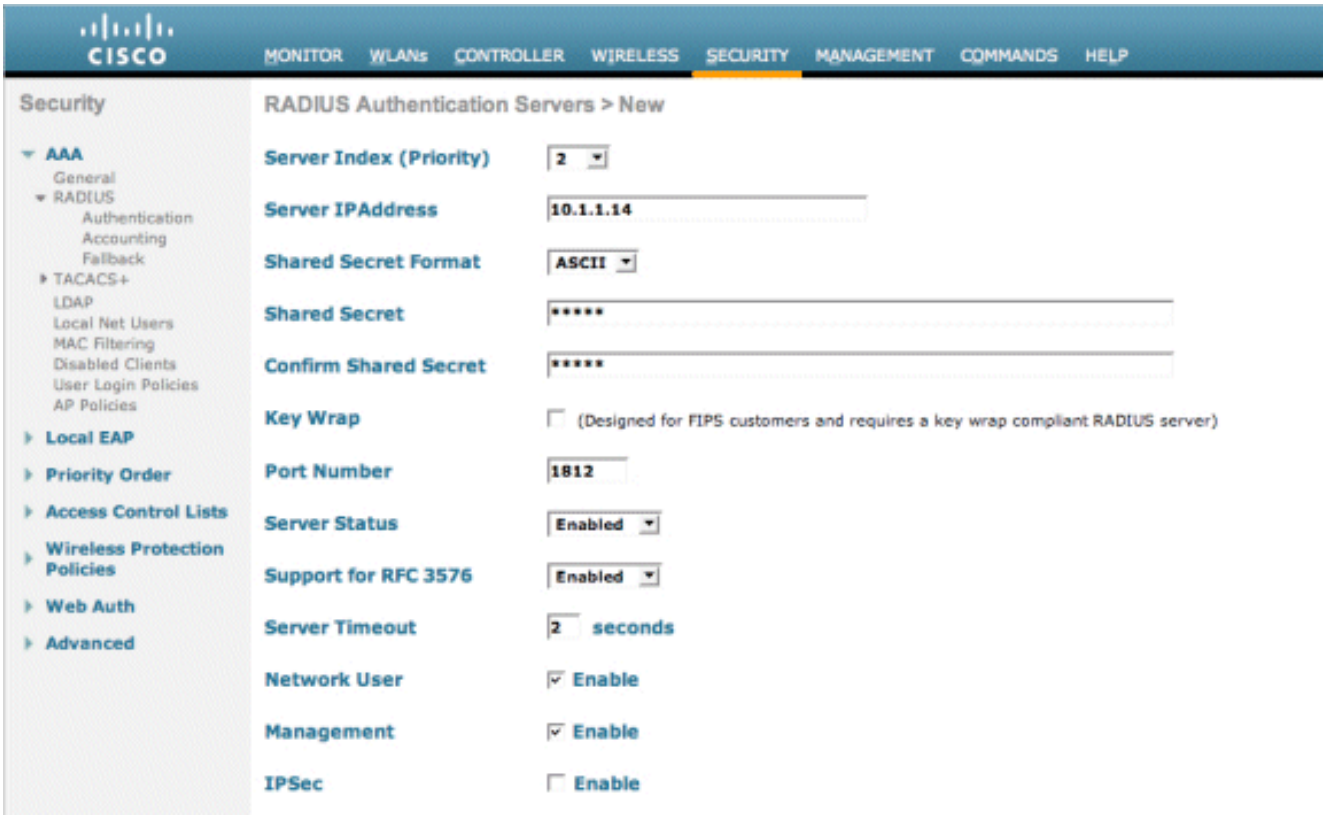
Cisco NAC訪客伺服器

Cisco NAC Guest Server是一種調配和報告解決方案，可為客戶端（如訪客、承包商等）提供臨時網路訪問。Cisco NAC訪客伺服器可與思科統一無線網路或Cisco NAC裝置解決方案配合使用。本文檔將引導您完成將Cisco NAC訪客伺服器與Cisco WLC整合的步驟，Cisco WLC會建立訪客使用者帳戶並驗證訪客的臨時網路訪問。

請按照以下步驟完成整合：

1. 將Cisco NAC訪客伺服器新增為WLC中的驗證伺服器。瀏覽到您的WLC(https://10.10.51.2, admin/admin)進行配置。選擇**Security > RADIUS > Authentication**。

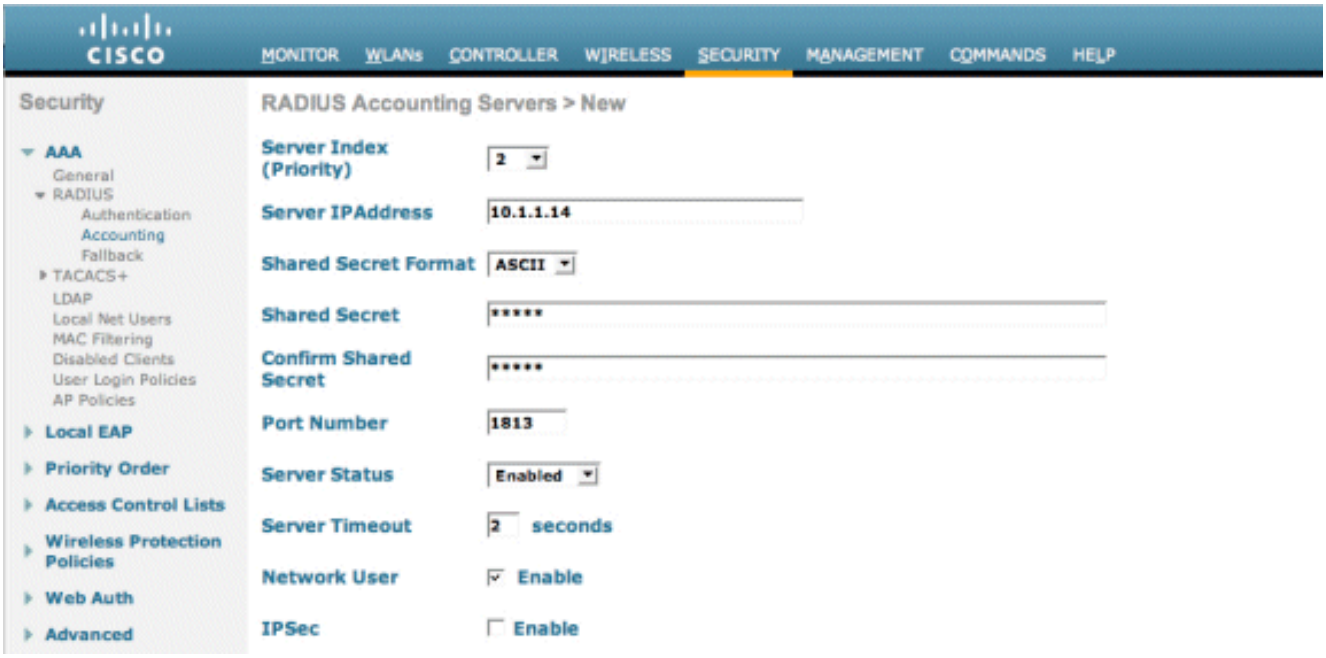
選擇**New**。為Cisco NAC Guest Server新增IP地址(10.1.1.14)。新增共用金鑰。確認共用金鑰。



選擇**Apply**。

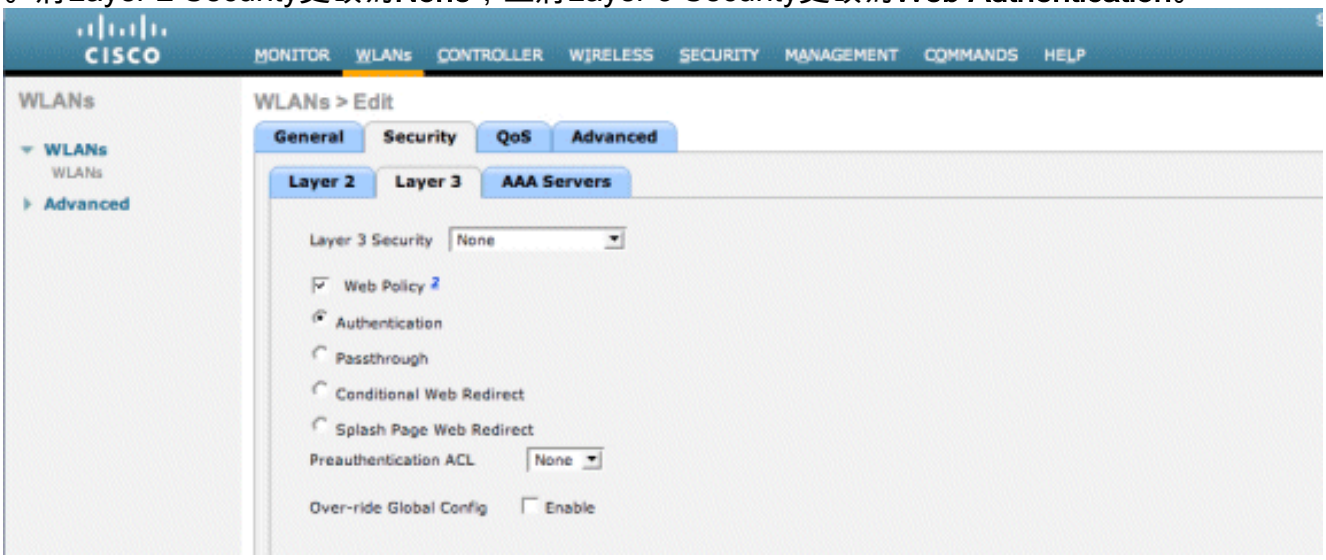
2. 將Cisco NAC Guest Server新增為WLC中的記帳伺服器。選擇**Security > RADIUS >Accounting**。

選擇**New**。為Cisco NAC Guest Server新增IP地址(10.1.1.14)。新增共用金鑰。確認共用金鑰。

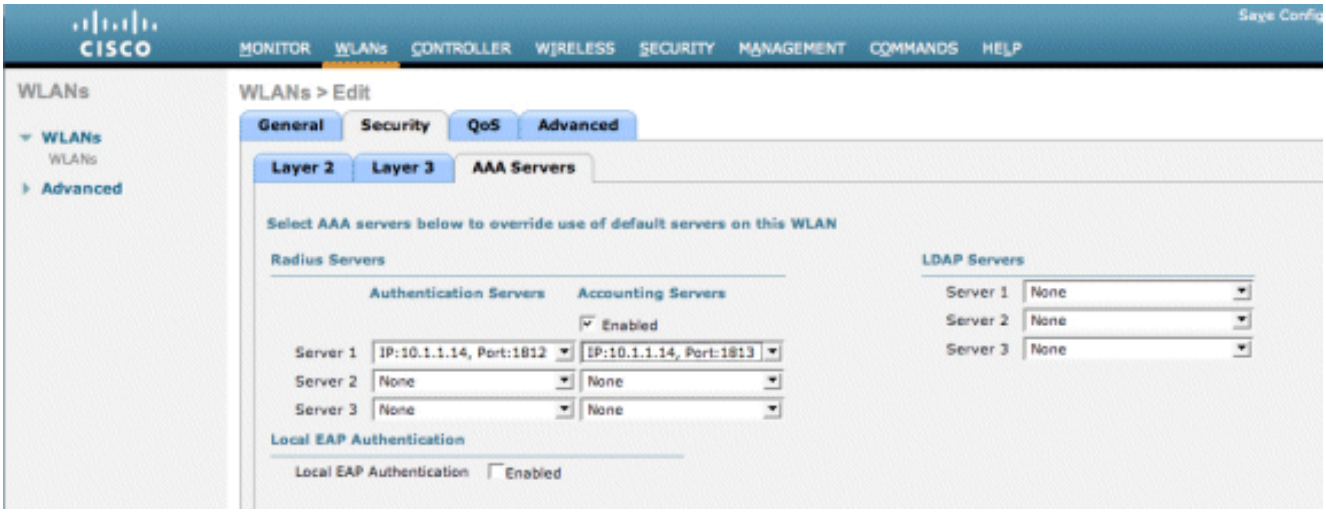


選擇**Apply**。

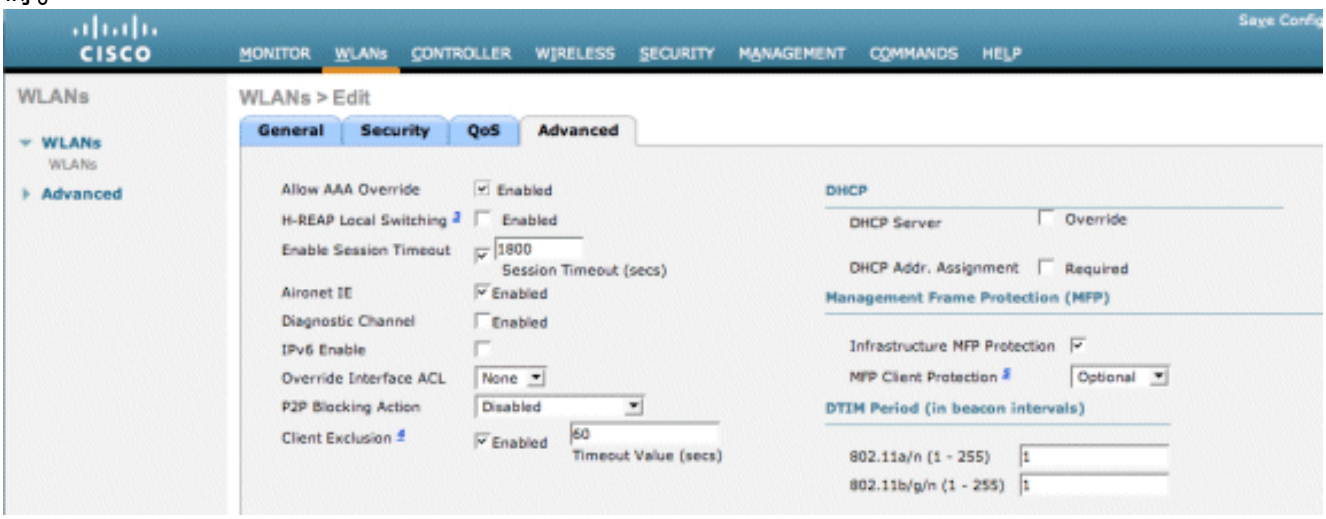
3. 修改WLAN(wireless-x)以使用NAC Guest Server。編輯WLAN(wireless-x)。選擇**Security**頁籤。將Layer 2 Security更改為**None**，並將Layer 3 Security更改為**Web Authentication**。



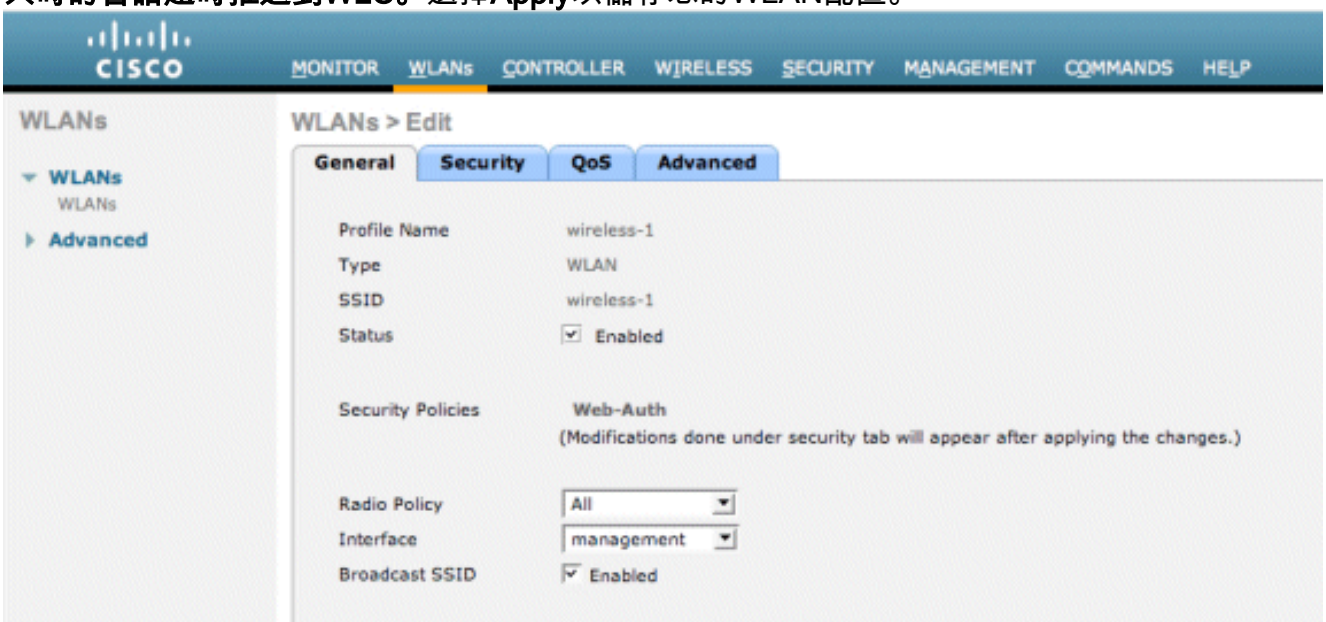
在Security頁籤下選擇**AAA Servers**。在「Server 1」框中，選擇**RADIUS伺服器(10.1.1.14)**。在Server 1框中，選擇**Accounting Server(10.1.1.14)**。



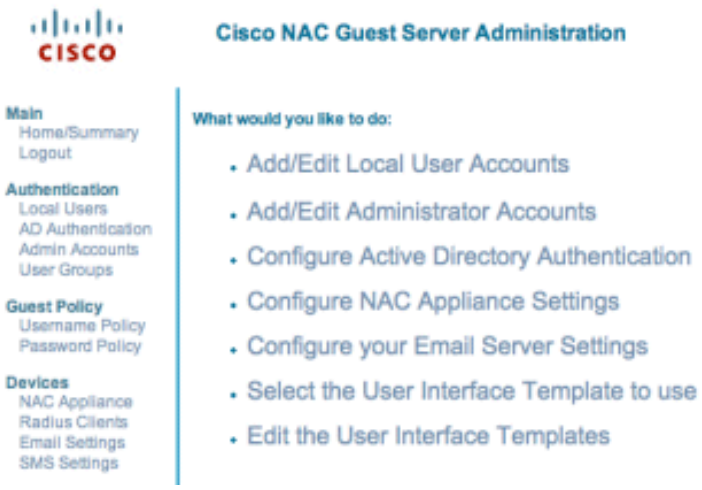
選擇Advanced頁籤。啟用Allow AAA Override。這允許從NAC訪客裝置設定每客戶端會話超時。



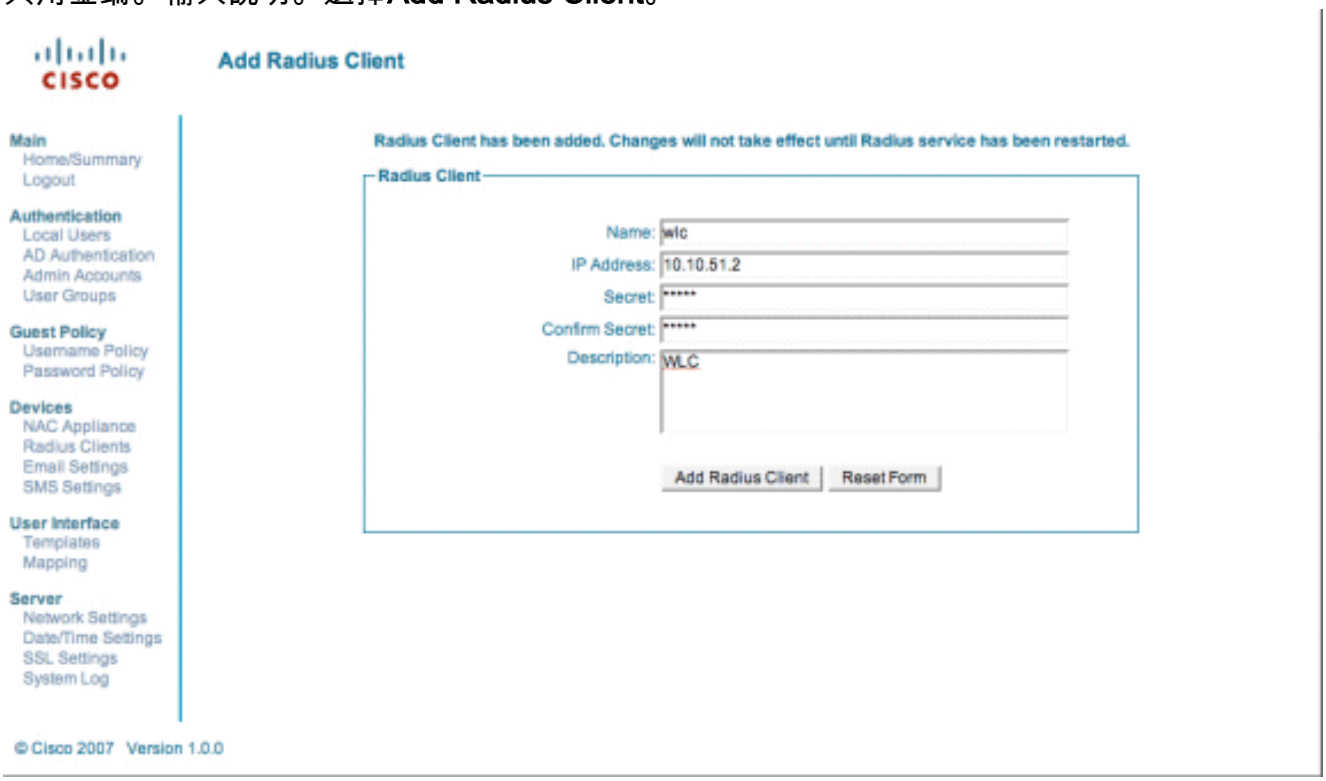
注意：在SSID上啟用AAA override時，NGS上訪客使用者的剩餘生存期將作為訪客使用者登入時的會話超時推送到WLC。選擇Apply以儲存您的WLAN配置。



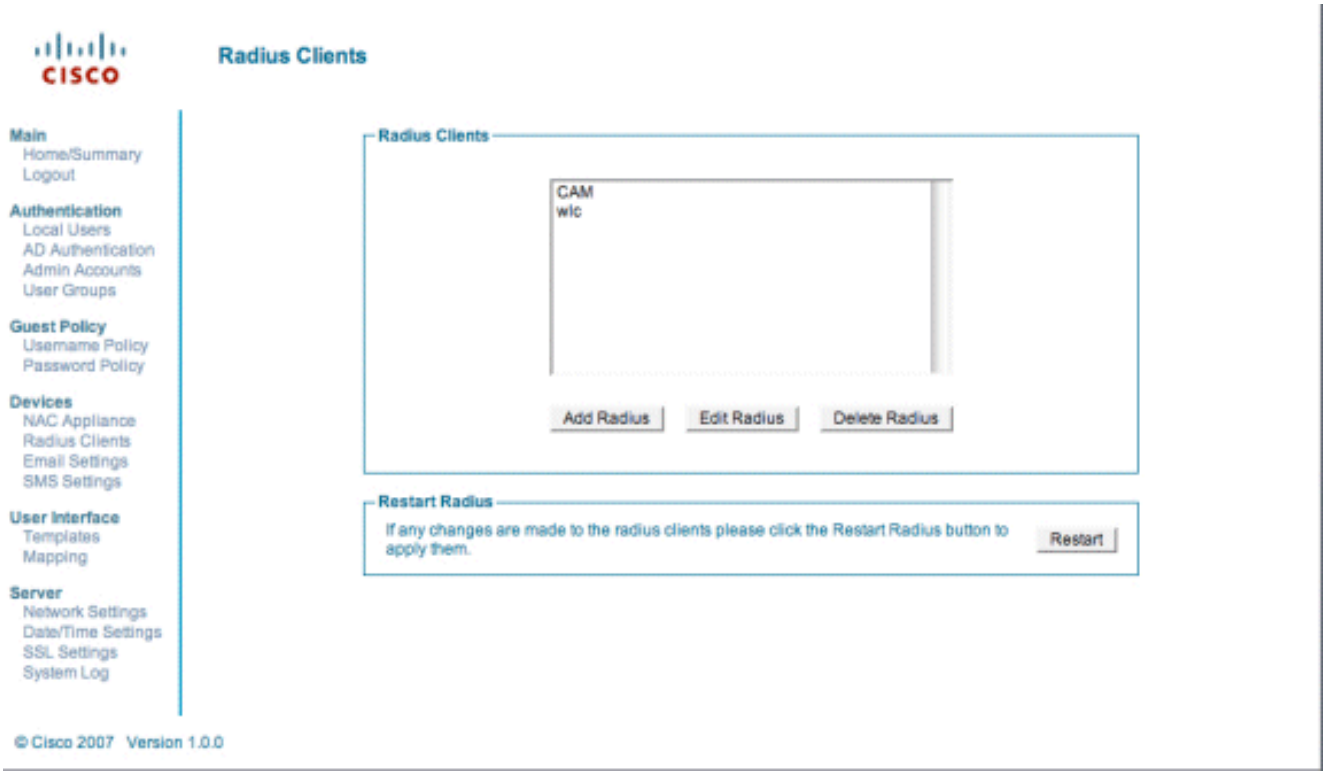
4. 驗證控制器是否已作為Radius使用者端新增到Cisco NAC Guest Server中。瀏覽到NAC Guest Server(https://10.1.1.14/admin)以配置此項。**註：如**果您在URL中指定了/admin，則您將獲得「管理」(Administration)頁面。



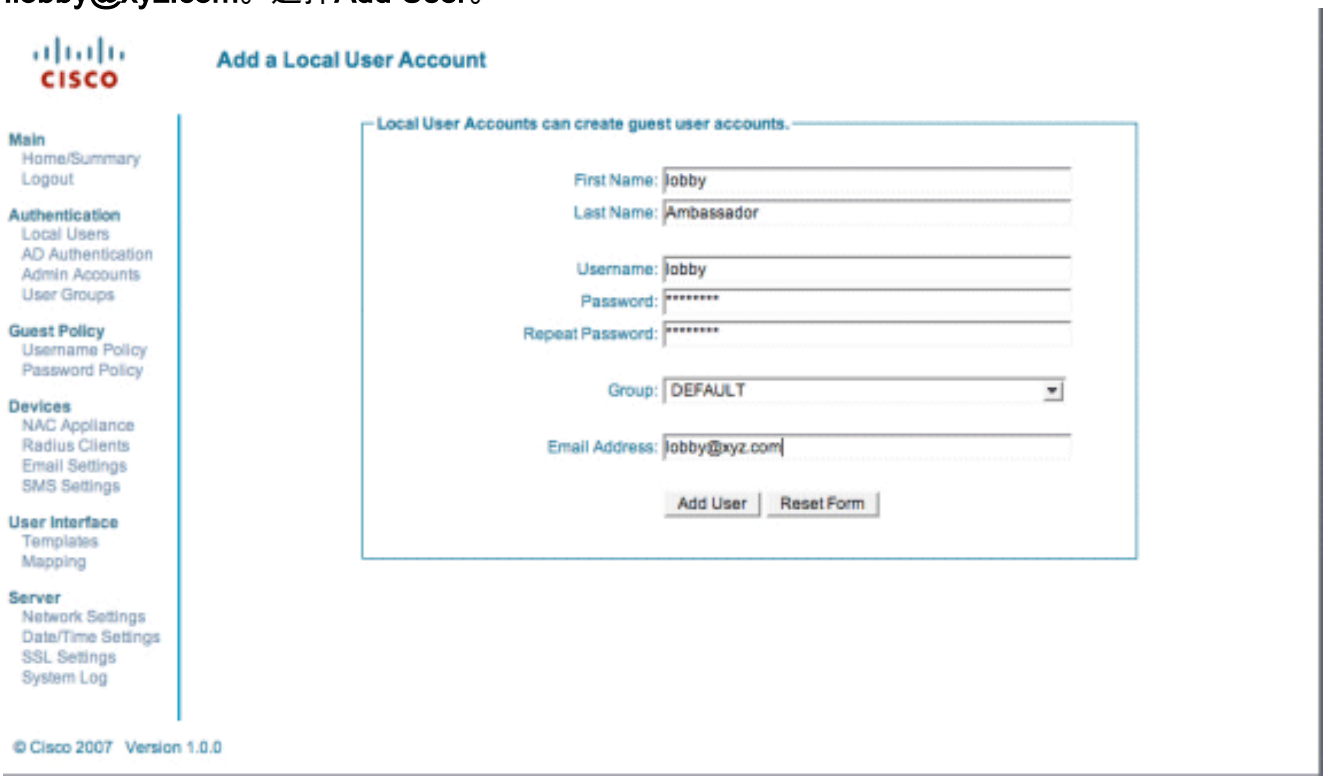
選擇**Radius Clients**。選擇**Add Radius**。輸入Radius使用者端資訊：輸入名稱：WLC系統名稱。輸入IP地址：WLC的IP**地址(10.10.51.2)**。輸入您在步驟1中輸入的相同共用金鑰。確認您的共用金鑰。輸入說明。選擇**Add Radius Client**。



重新啟動Radius服務以使更改生效。選擇**Radius Clients**。在「Restart Radius（重新啟動RADIUS）」框中選擇**Restart**。

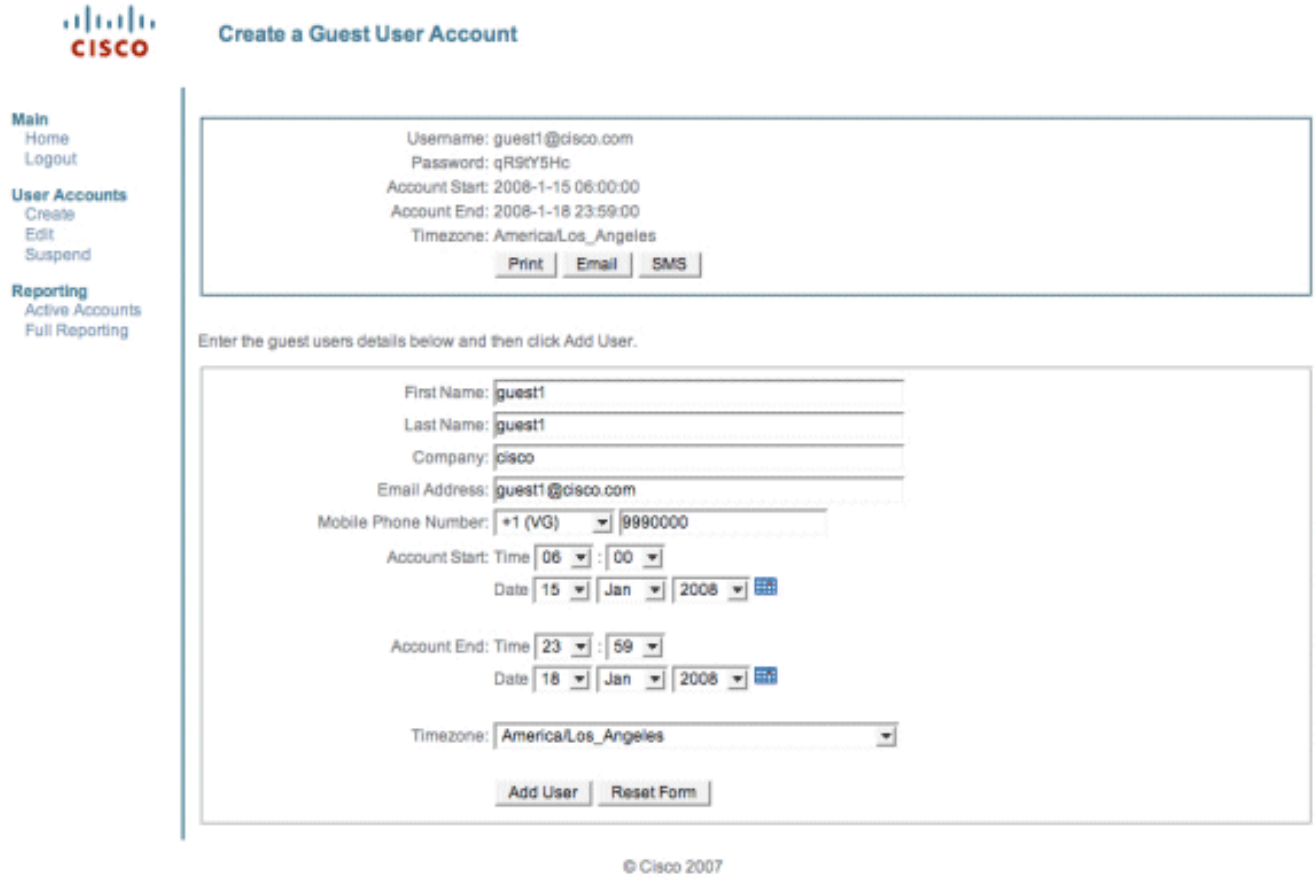


5. 在Cisco NAC Guest Server中建立本地使用者，即Lobby Ambassador。選擇**Local Users**。選擇**Add User**。**注意：**必須填寫所有欄位。輸入名字：**lobby**。輸入姓氏：**Ambassador**。輸入使用者名稱：**大廳**。輸入密碼：**密碼**。將組保留為**預設值**。輸入電子郵件地址**:lobby@xyz.com**。選擇**Add User**。



6. 以本地使用者身份登入並建立訪客帳戶。瀏覽到NAC Guest Server(https://10.1.1.14)，使用您在第5步中建立的使用者名稱/密碼登入，然後配置以下內容
：

為訪客使用者帳戶選擇**Create**。**注意**：必須填寫所有欄位。輸入名字。輸入姓氏。輸入公司。輸入電子郵件地址。**注意**：電子郵件地址是使用者名稱。輸入帳戶結束：**時間**。選擇**Add User**。



7. 連線到訪客WLAN並以訪客使用者身份登入。將您的無線客戶端連線到訪客WLAN(wireless-x)。開啟Web瀏覽器以重新導向至Web-Auth登入頁面。**注意**：或者，輸入**https://1.1.1.1/login.html**以重新導向至登入頁面。輸入您在步驟6中建立的訪客使用者名稱。輸入在步驟6中自動生成的密碼。Telnet至WLC並使用**show client detail**指令驗證是否已設定作業階段逾時。當會話超時過期時，訪客客戶端將斷開連線，您的ping將停止。

```
(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) >
```

注意：若要從Wireless LAN Controller(WLC)到NAC Guest Server(NGS)設定Web驗證，需要對Web-auth屬性使用PAP模式驗證。如果Web身份驗證策略設定為CHAP，身份驗證將失敗，因為NGS不支援CHAP。

相關資訊

- Cisco NAC裝置 — Clean Access Manager安裝及設定指南，版本4.1(3)
- Cisco NAC裝置交換器與無線LAN控制器支援
- 思科無線LAN控制器配置指南7.0.116.0版
- （影片）思科身份服務引擎(ISE)和無線區域網控制器(WLC)的整合
- NAC（清除存取）：設定訪客存取
- 部署指南：使用思科無線LAN控制器的思科訪客接入，版本4.1
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。