无线局域网控制器(WLC)和NAC客户服务器(NGS)集成指南

Contents

Introduction

本文档提供了集成 NAC Guest Server 和无线 LAN 控制器的指南。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco 无线 LAN 控制器 (WLC) 4.2.61.0
- 带有 IOS® 12.2(25)SEE2 版的 Catalyst 3560
- Cisco ADU 4.0.0.279 版
- NAC Guest Server 1.0 版

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.

背景信息

Cisco NAC Guest Server 是为来宾、访客、承包商、顾问或客户提供临时网络访问权的完整配置和报告系统。Guest Server 与 Cisco NAC Appliance 或 Cisco 无线 LAN 控制器配合工作，后者为访客访问提供捕获式门户和实施点。

Cisco NAC Guest Server 允许拥有权限的任何用户轻松地创建临时访客帐户和邀请访客。Cisco NAC Guest Server 对邀请人（创建访客帐户的用户）执行完整的身份验证，并允许邀请人通过打印输出、电子邮件或 SMS 将帐户详细信息提供给访客。系统会存储从创建用户帐户到访客访问网络的完整体验以进行审计和报告。

在创建访客帐户时，系统会在 Cisco NAC Appliance Manager (Clean Access Manager) 中配置它们，或将它们存储在 Cisco NAC Guest Server 上的内置数据库中。当您使用 Guest Server 的内置数据库时，外部网络接入设备（例如 Cisco 无线 LAN 控制器）可以利用远程身份验证拨入用户服务 (RADIUS) 协议根据 Guest Server 对用户进行身份验证。

在创建帐户时，Cisco NAC Guest Server 会为访客帐户配置指定的有效期。在帐户过期后，Guest Server 将直接从 Cisco NAC Appliance Manager 中删除帐户，或发送 RADIUS 消息来通知网络接入设备 (NAD) 帐户剩余的有效时间长度，在该时间长度后，NAD 必须删除用户。

Cisco NAC Guest Server 提供了重要的访客网络访问记帐，方法是合并从创建访客帐户到访客使用帐户的整个审计跟踪过程，以便可以通过中心管理界面执行报告。

访客访问概念

Cisco NAC Guest Server 利用许多术语来解释提供访客访问所需的组件。

客人身份的用户

访客用户是需要用户帐户来访问网络的人。

赞助商

邀请人是创建访客用户帐户的人。此人通常是提供网络访问的组织的员工。邀请人可以是承担某些工作职责的特定个人，也可以是可以根据企业目录（例如 Microsoft Active Directory (AD)）进行身份验证的任何员工。

网络实施设备

这些设备是提供网络访问的网络基础设施组件。另外，网络实施设备将访客用户推送到捕获式门户，他们可以在其中输入其访客帐户详细信息。当访客输入其临时用户名和密码时，网络实施设备将根据 Guest Server 所创建的访客帐户来检查这些凭证。

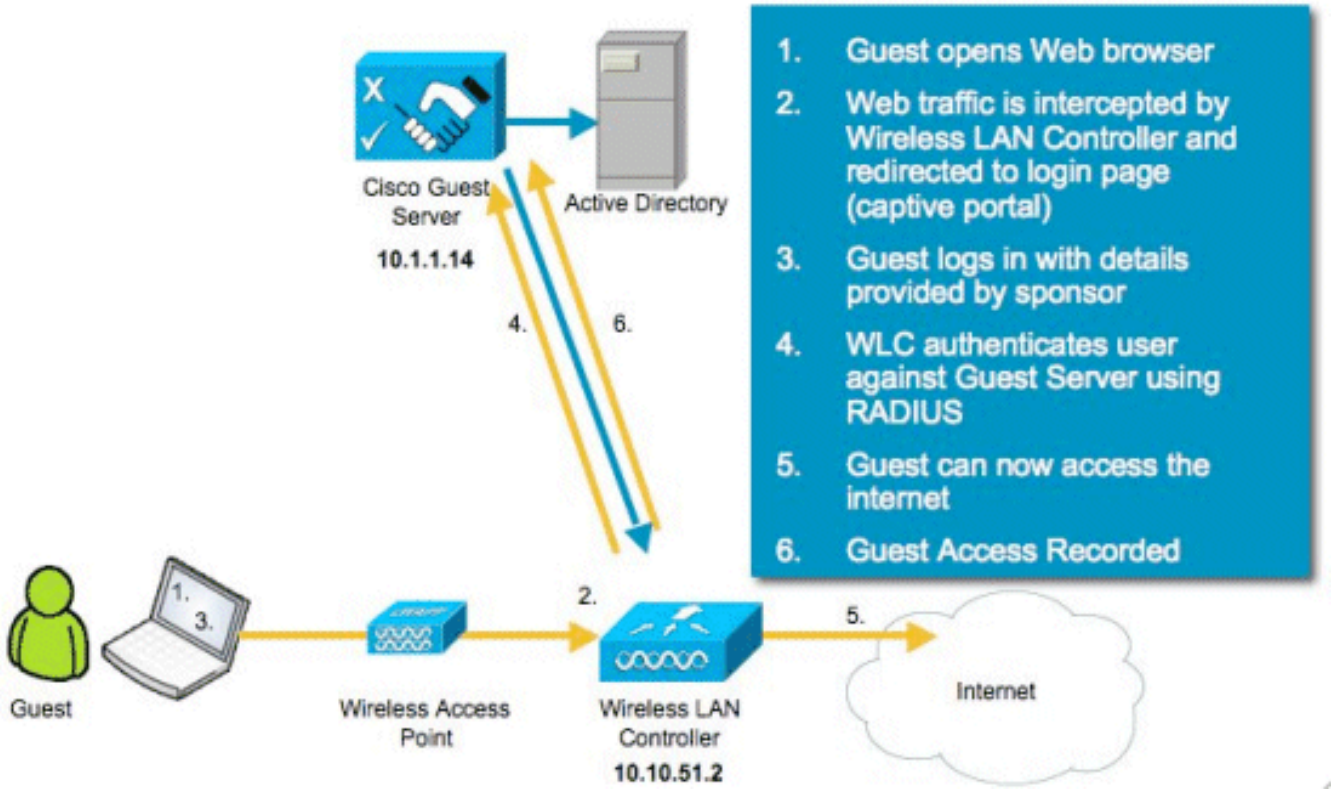
Guest Server

这是 Cisco NAC Guest Server，它将所有访客访问连接在一起。Guest Server 将以下各项链接在一起：创建访客帐户的邀请人、传递给访客的帐户详细信息、根据网络实施设备进行的访客身份验证和使用 Guest Server 进行的访客的网络实施设备验证。另外，Cisco NAC Guest Server 合并网络实施设备中的记帐信息以提供单点访客访问报告。

在 CCO 中提供了有关 NGS 的详细文档。

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

实验室拓扑概述



配置无线 LAN 控制器 (WLC)

请按照以下步骤配置 WLC：

1. 初始化控制器和接入点。
2. 配置控制器接口。
3. 配置 RADIUS。
4. 配置 WLAN 设置。

初始化

对于初始配置，请使用控制台连接（例如 HyperTerminal）并按照设置提示来填充登录和接口信息。**reset system 命令**也可启动这些提示。

```
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
```

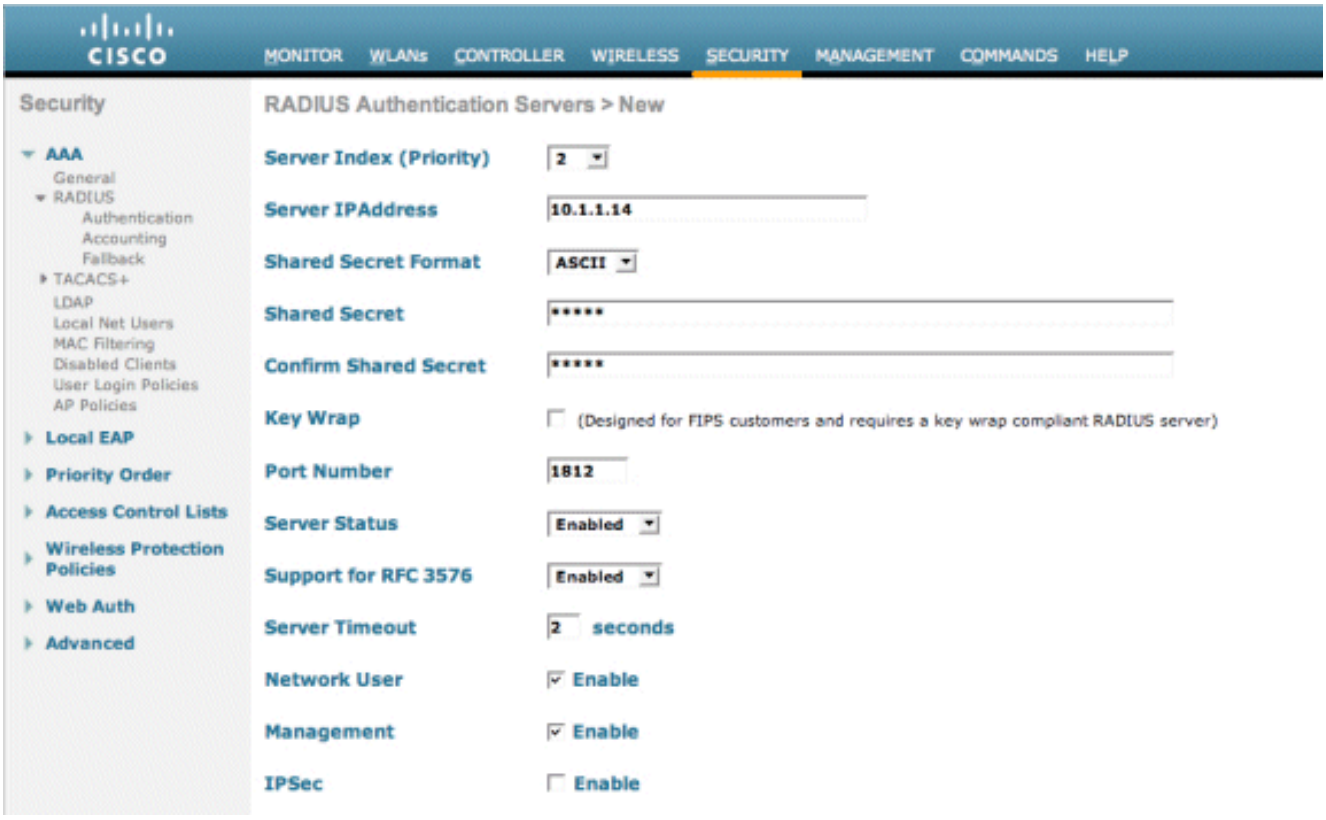
Cisco NAC Guest Server

Cisco NAC Guest Server 是为客户端（例如访客、承包商等）提供临时网络访问的配置和报告解决方案。Cisco NAC Guest Server 与 Cisco 统一无线网络或 Cisco NAC Appliance 解决方案配合工作。本文档指导您完成将 Cisco NAC Guest Server 与 Cisco WLC 集成的步骤，这将可以创建访客用户帐户并验证访客的临时网络访问。

按照以下步骤完成集成：

1. 在 WLC 中添加 Cisco NAC Guest Server 作为身份验证服务器。浏览到您的 WLC（https://10.10.51.2，admin/admin）来执行以下配置。选择 **Security > RADIUS > Authentication**。

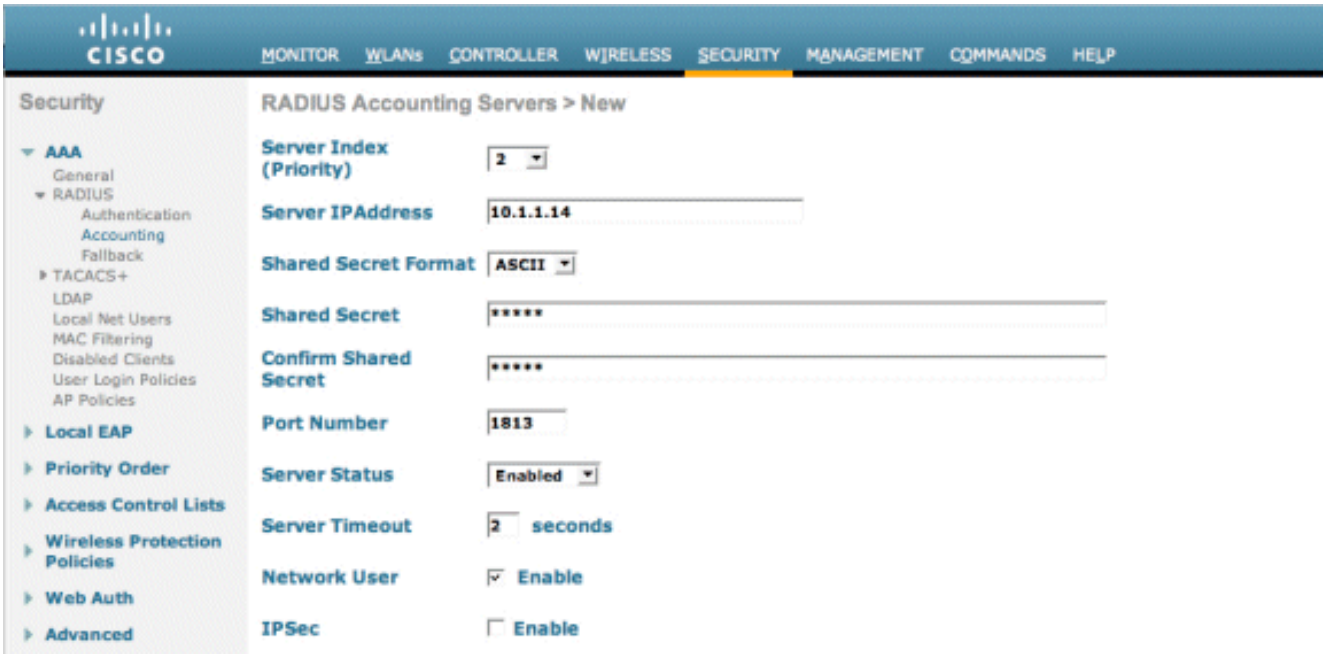
选择**新**。添加 Cisco NAC Guest Server 的 IP 地址 (10.1.1.14)。添加共享密钥。确认共享密钥。



选择 Apply。

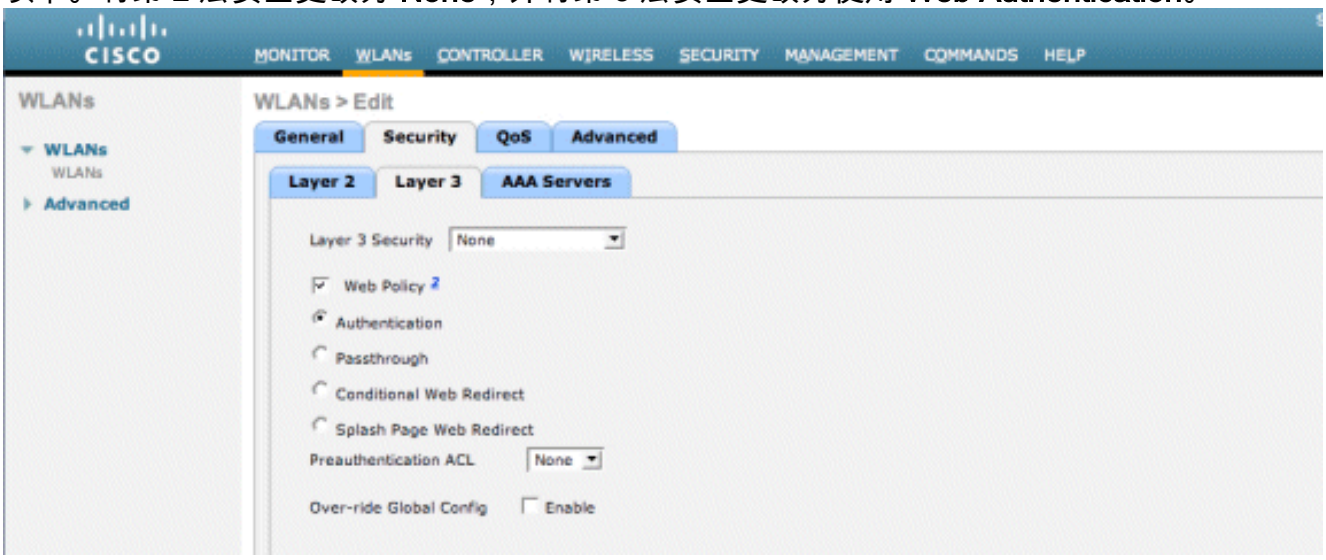
2. 在 WLC 中添加 Cisco NAC Guest Server 作为记帐服务器。选择 **Security > RADIUS >Accounting**。

选择**新**。添加 Cisco NAC Guest Server 的 IP 地址 (10.1.1.14)。添加共享密钥。确认共享密钥。

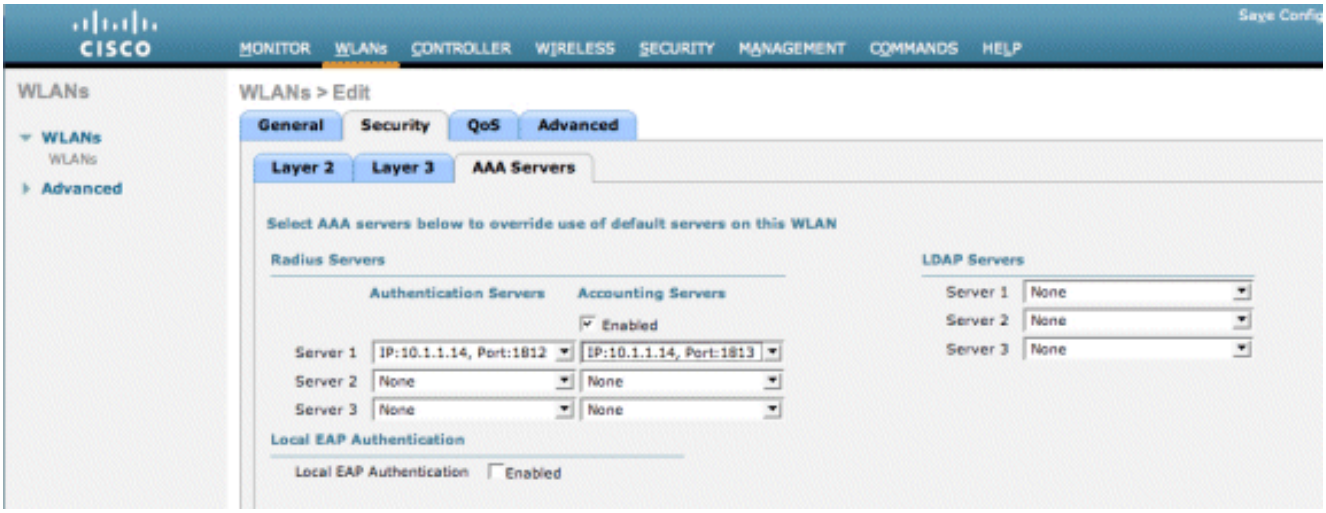


选择 Apply。

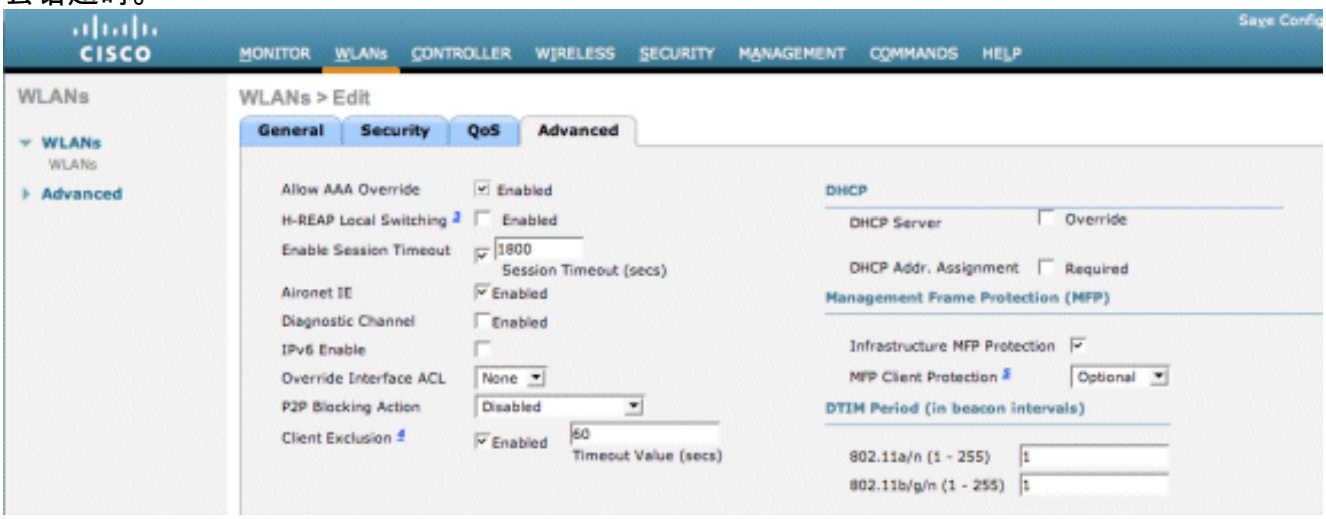
3. 修改 WLAN（无线 x）以使用 NAC Guest Server。编辑 WLAN（无线 x）。选择 **Security** 选项卡。将第 2 层安全更改为 **None**，并将第 3 层安全更改为使用 **Web Authentication**。



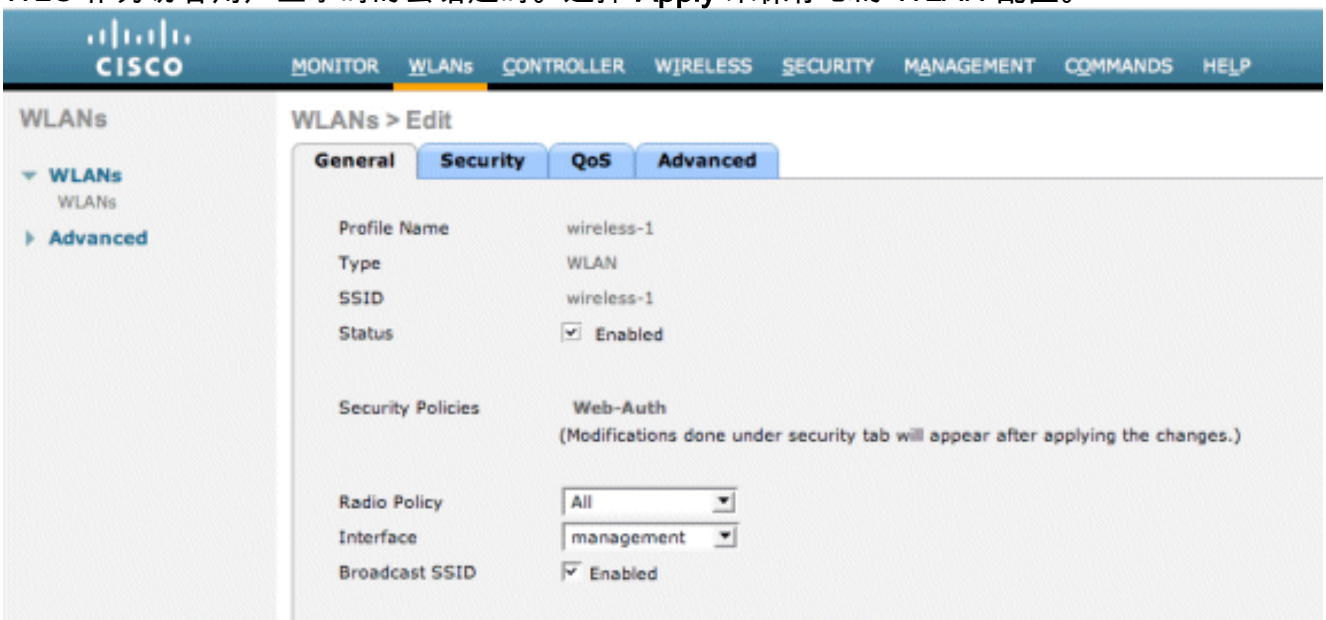
选择“Security”选项卡下的 **AAA Servers**。在“Server 1”框下，选择 **RADIUS server (10.1.1.14)**。在“Server 1”框下，选择 **Accounting Server (10.1.1.14)**。



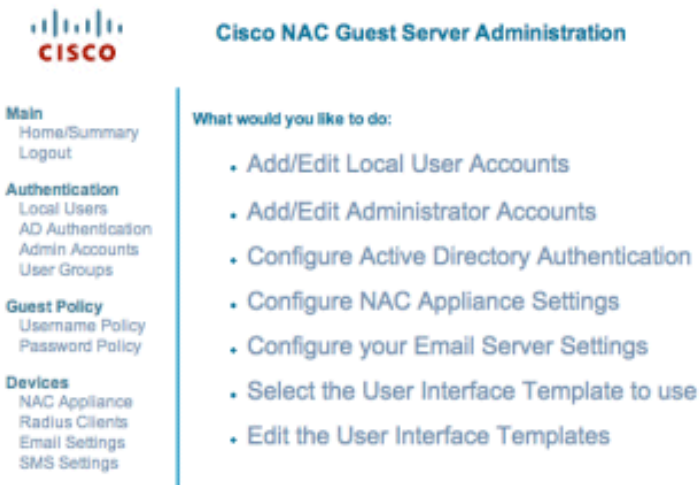
选择 **Advanced** 选项卡。启用 **Allow AAA Override**。这允许从 NAC Guest 设备设置每客户端会话超时。



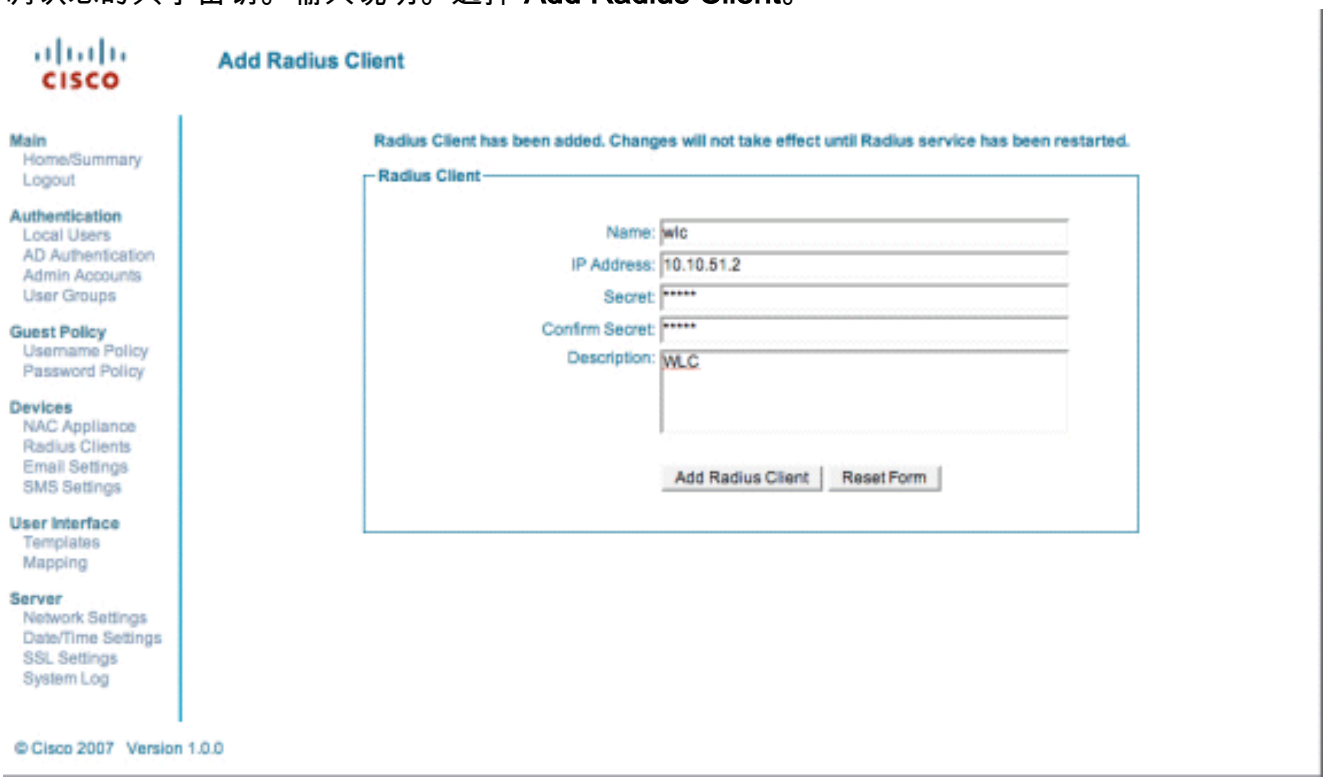
Note: 当在 SSID 上启用了 **AAA override** 后，NGS 上的访客用户帐户的剩余寿命会被推送到 WLC 作为访客用户登录时的会话超时。选择 **Apply** 来保存您的 WLAN 配置。



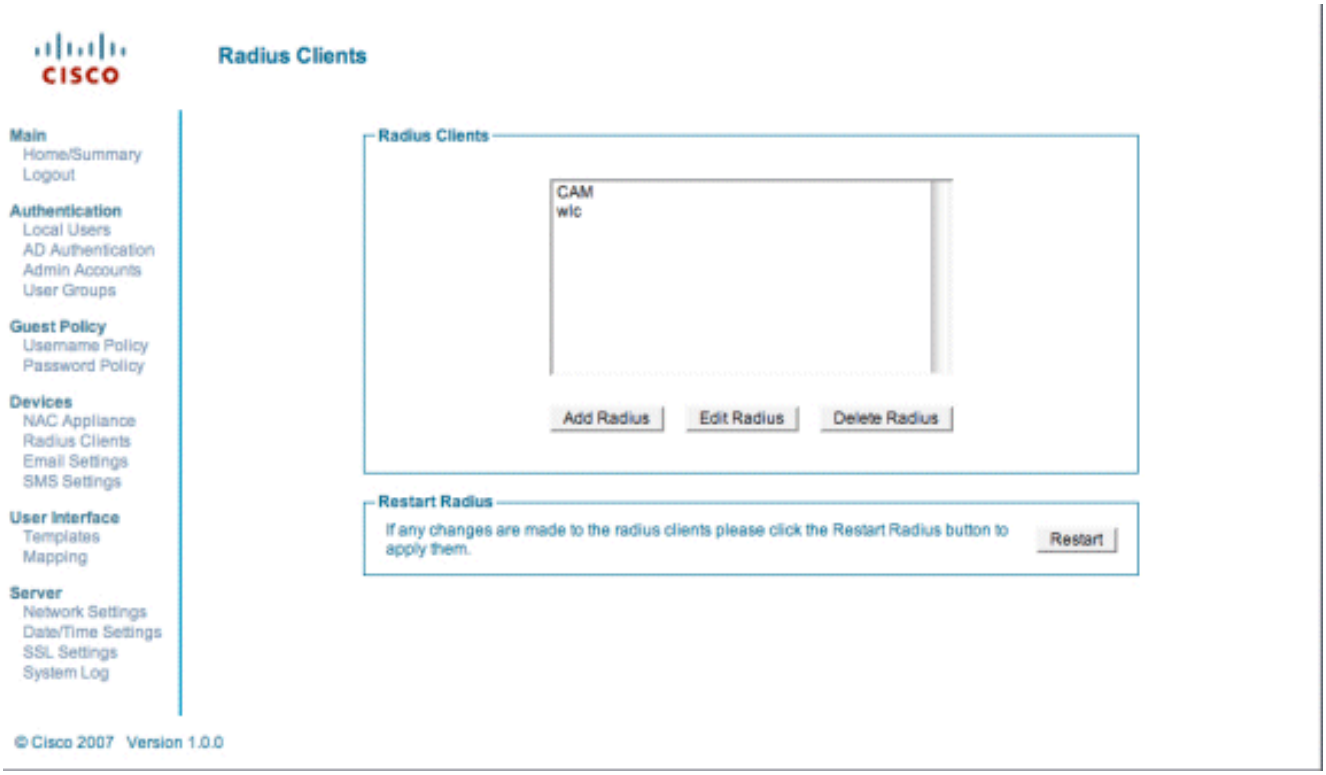
4. 验证是否在 Cisco NAC Guest Server 中将控制器添加为 Radius 客户端。浏览到 NAC Guest Server (https://10.1.1.14/admin) 来执行以下配置。**Note:** 如果您在 URL 中指定了 /admin，则将获得管理页面。



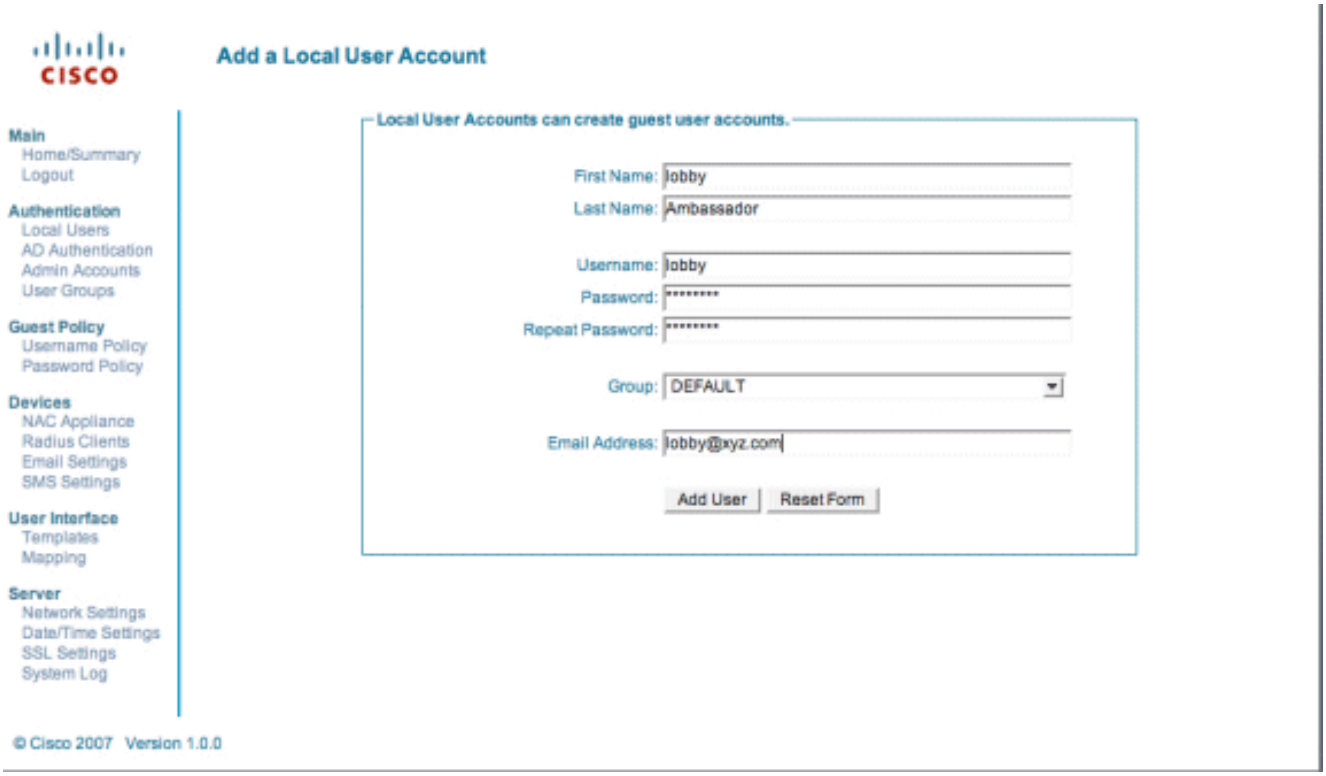
选择 **Radius Clients**。选择 **Add Radius**。输入 Radius 客户端信息：输入名称：WLC 系统名称。输入 IP 地址：WLC 的 IP 地址 **(10.10.51.2)**。输入您在步骤 1 中输入的同一共享密钥。确认您的共享密钥。输入说明。选择 **Add Radius Client**。



重新启动 Radius 服务以使更改生效。选择 **Radius Clients**。选择“Restart Radius”框中的 **Restart**。

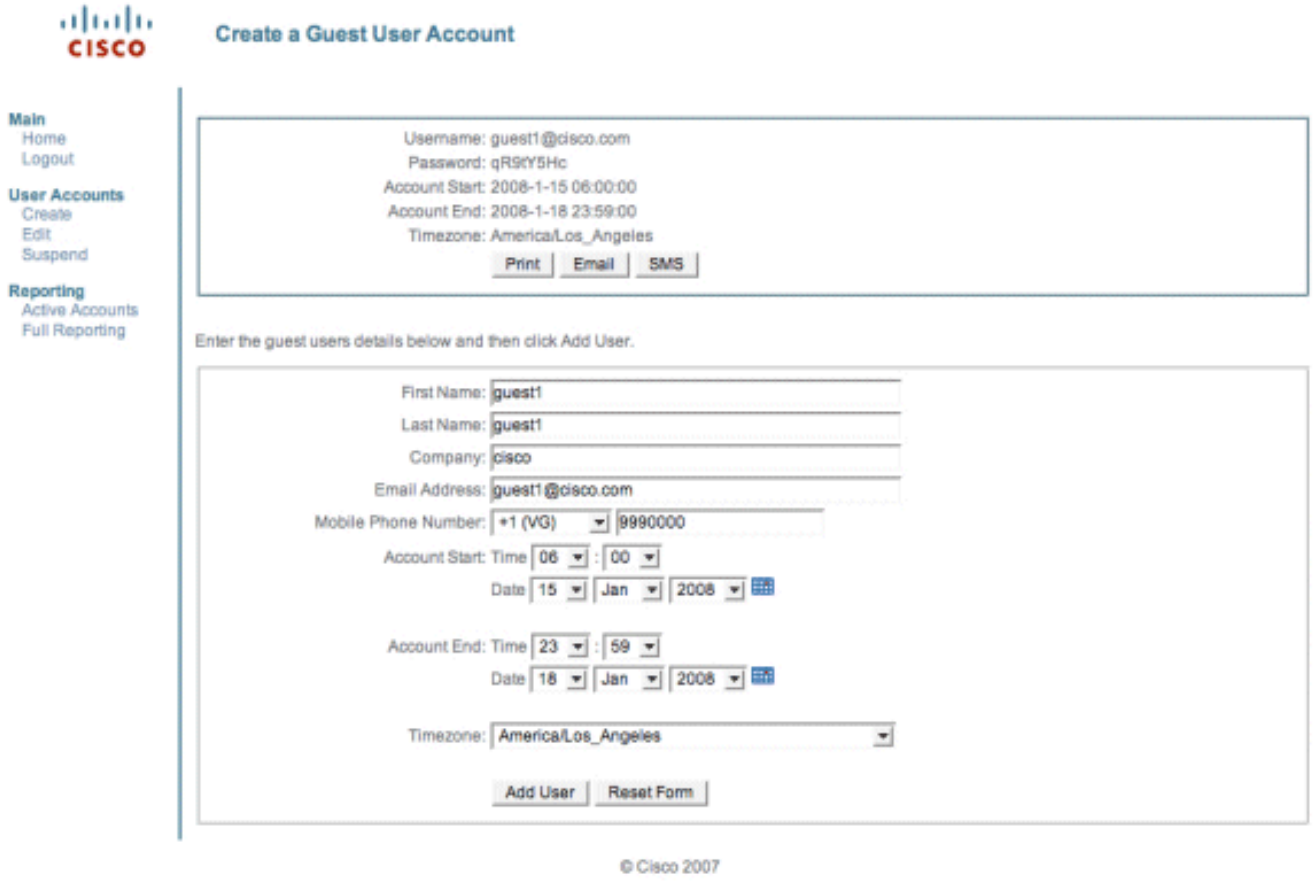


5. 在 Cisco NAC Guest Server 中创建本地用户，即，Lobby Ambassador。选择 **Local Users**。选择 **Add User**。**Note:** 您必须填写所有字段。输入名字：**大厅**。输入姓氏：**大使**。输入用户名：**大厅**。输入密码：**密码**。保留组为 **Default**。输入电子邮件地址：**lobby@xyz.com**。选择 **Add User**。



6. 作为本地用户登录并创建访客帐户。浏览到 NAC Guest Server (https://10.1.1.14)，使用您在步骤 5 中创建的用户名/密码登录，然后执行以下配置：

为访客用户帐户选择 **Create**。**Note:** 您必须填写所有字段。输入名字。输入姓氏。输入公司。输入电子邮件地址。**Note:** 电子邮件地址是用户名。输入帐户结束：时间。选择 **Add User**。



7. 连接到访客 WLAN 并作为访客用户登录。将您的无线客户端连接到访客 WLAN（无线 x）。打开 Web 浏览器以重定向到 Web-Auth 登录页。**Note:** 或者，键入 **https://1.1.1.1/login.html** 以重定向到登录页。输入您在步骤 6 中创建的访客用户名。输入在步骤 6 中自动生成的密码。通过 Telnet 登录到 WLC 并使用 **show client detail 命令**验证是否设置了会话超时。当会话超时到期时，访客客户端将断开连接，并且您的 ping 将停止。

```
(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) >
```

Note: 要设置从无线 LAN 控制器 (WLC) 到 NAC Guest Server (NGS) 的 Web 身份验证，您需要使用 web-auth 属性上的 PAP 模式身份验证。如果 Web 身份验证策略设置为 CHAP，则身份验证将失败，因为 NGS 不支持 CHAP。

Related Information

- Cisco NAC Appliance - Clean Access Manager 安装和配置指南，4.1(3) 版
- Cisco NAC Appliance 交换机和无线 LAN 控制器支持
- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- （视频）Cisco 身份服务引擎 (ISE) 和无线 LAN 控制器 (WLC) 的集成
- NAC (Clean Access) ：配置访客访问
- 部署指南：使用 Cisco 无线局域网控制器 4.1 版的 Cisco 访客接入
- Technical Support & Documentation - Cisco Systems