

Regulador del Wireless LAN (WLC) y guía de integración del servidor del invitado del NAC (NG)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configure el regulador del Wireless LAN \(el WLC\)](#)

[Inicialización](#)

[Cisco NAC Guest Server](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una pauta para integrar el NAC Guest Server y los controladores de LAN inalámbricos.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador LAN de la tecnología inalámbrica de Cisco (WLC) 4.2.61.0
- Catalyst 3560 con la versión 12.2(25)SEE2 IOS®
- Versión de ADU 4.0.0.279 de Cisco
- Versión del servidor 1.0 del invitado del NAC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Antecedentes

El Cisco NAC Guest Server es un aprovisionamiento y un sistema de reporte completos que proporciona el acceso de red temporaria para los invitados, los visitantes, los contratistas, los consultores, o los clientes. El servidor del invitado funciona junto al dispositivo NAC de Cisco o al controlador LAN de la tecnología inalámbrica de Cisco, que proporcionan la punta prisionera del portal y de la aplicación para el acceso de invitado.

El Cisco NAC Guest Server permite a cualquier usuario con los privilegios de crear fácilmente las cuentas de invitado temporales y de patrocinar a los invitados. El Cisco NAC Guest Server realiza la autenticación completa de los patrocinadores, los usuarios que crean las cuentas de invitado, y permite que los patrocinadores proporcionen los detalles de la cuenta al invitado por el informe de ejecución, el correo electrónico, o SMS. La experiencia entera, de la creación de la cuenta de usuario al acceso de red del invitado, se salva para la auditoría y la información.

Cuando se crean las cuentas de invitado, son aprovisionado dentro del administrador del dispositivo NAC de Cisco (Access Manager limpio) o salvado dentro de la base de datos incorporada en el Cisco NAC Guest Server. Cuando usted utiliza la base de datos incorporada del servidor del invitado, los dispositivos de acceso de la red externa, tales como el controlador LAN de la tecnología inalámbrica de Cisco, puede autenticar a los usuarios contra el servidor del invitado con el protocolo del Remote Authentication Dial In User Service (RADIUS).

El Cisco NAC Guest Server provisions al invitado explica la cantidad de tiempo especificada cuando se crea la cuenta. Sobre el vencimiento de la cuenta, el servidor del invitado borra la cuenta directamente del administrador del dispositivo NAC de Cisco o envía un mensaje de RADIUS que notifique el dispositivo de acceso a la red (NAD) del periodo del tiempo válido que sigue habiendo para la cuenta antes de que el NAD deba quitar al usuario.

El Cisco NAC Guest Server proporciona las estadísticas vitales del acceso de red del invitado por la consolidación del rastro de auditoría entero de la creación de la cuenta de invitado al uso del invitado de la cuenta para poder realizarse los informes a través de una interfaz de administración central.

Conceptos del acceso de invitado

El Cisco NAC Guest Server hace uso de varios términos para explicar los componentes necesarios para proporcionar el acceso de invitado.

Usuario invitado

El Usuario invitado es la persona que necesita una cuenta de usuario acceder la red.

Patrocinador

El patrocinador es la persona que crea la cuenta de Usuario invitado. Esta persona es a menudo empleado de la organización que proporciona el acceso a la red. Los patrocinadores pueden ser - 3 - individuos específicos con ciertos papeles del trabajo, o pueden ser cualquier empleado que

pueda autenticar contra a Corporate Directory (Directorio corporativo) por ejemplo el Microsoft Active Directory (AD).

Dispositivo de imposición de la red

Estos dispositivos son los componentes de la infraestructura de red que proporcionan el acceso a la red. Además, los dispositivos de imposición de la red avanzan a los Usuarios invitados a un portal prisionero, en donde pueden ingresar sus detalles de la cuenta del invitado. Cuando un invitado ingresa su Nombre de usuario y contraseña temporales, el dispositivo de imposición de la red marca esas credenciales contra las cuentas del invitado creadas por el servidor del invitado.

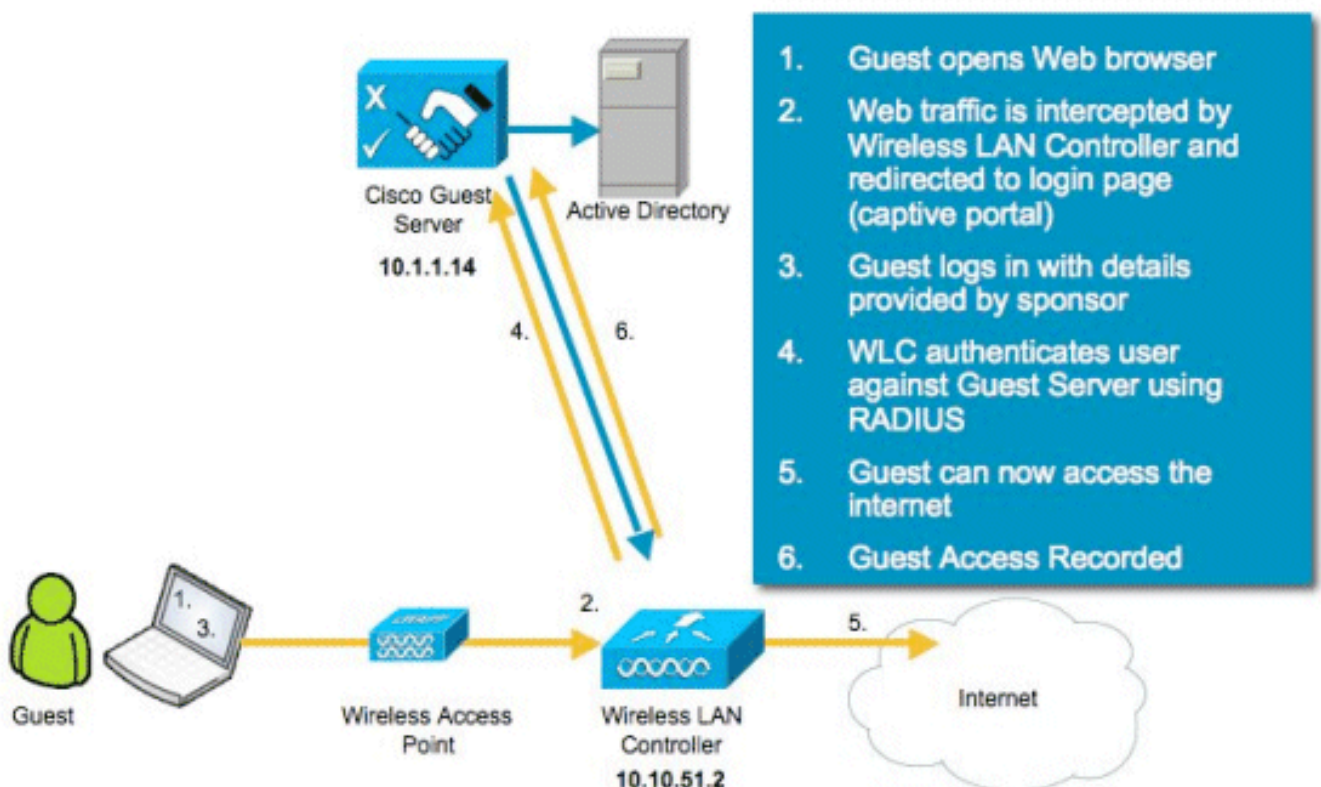
Servidor del invitado

Éste es el Cisco NAC Guest Server, que ata junto todos los pedazos de acceso de invitado. El servidor del invitado conecta éstos juntos: el patrocinador que crea la cuenta de invitado, los detalles de la cuenta pasó al invitado, a la autenticación del invitado contra el dispositivo de imposición de la red, y a la verificación del dispositivo de imposición de la red del invitado con el servidor del invitado. Además, el Cisco NAC Guest Server consolida la información de la cuenta de los dispositivos de imposición de la red para proporcionar un monopunto de los informes del acceso de invitado.

La documentación detallada en los NG está disponible en el CCO.

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

Descripción de la Topología de laboratorio



Configure el regulador del Wireless LAN (el WLC)

Siga los siguientes pasos para configurar el WLC:

1. Inicialice el regulador y el Punto de acceso.
2. Configure las interfaces del regulador.
3. Configure el RADIUS.
4. Configure las configuraciones de la red inalámbrica (WLAN).

Inicialización

Para la configuración inicial, utilice una conexión de consola como el hyperterminal y siga los prompts de la configuración para poblar la información del login y de la interfaz. El comando **reset system** también inicia estos 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

El Cisco NAC Guest Server es una solución del aprovisionamiento y de la información que proporciona el acceso de red temporaria a los clientes tales como invitados, contratistas, etc. El Cisco NAC Guest Server funciona con la red del Cisco Unified Wireless o las soluciones del

dispositivo NAC de Cisco. Este documento recorre usted con los pasos para integrar el Cisco NAC Guest Server con un WLC de Cisco, que crea una cuenta de Usuario invitado y verifica el acceso de red temporaria del invitado.

Siga los siguientes pasos para completar la integración:

1. Agregue el Cisco NAC Guest Server como servidor de autenticación en el WLC. Hojee a su WLC (https://10.10.51.2, admin/admin) para configurar esto. Elija la **Seguridad > el RADIUS > la autenticación**.

The screenshot shows the Cisco WLC interface for configuring RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS' selected. The main content area is titled 'RADIUS Authentication Servers' and includes a 'Call Station ID Type' dropdown set to 'IP Address' and a 'Use AES Key Wrap' checkbox which is unchecked. Below this is a table with the following data:

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.1.12	1812	Disabled	Enabled <input type="checkbox"/>

Elija **nuevo**. Agregue la dirección IP (10.1.1.14) para el Cisco NAC Guest Server. Agregue el secreto compartido. Confirme el secreto compartido.

The screenshot shows the 'New' configuration page for a RADIUS Authentication Server. The left sidebar is the same as the previous screenshot. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 2
- Server IP Address: 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

Elija **se aplican**.

The screenshot shows the Cisco WLC Security page with the RADIUS Authentication Servers configuration. The left sidebar shows the navigation menu with 'Security' expanded to 'RADIUS' > 'Accounting'. The main content area is titled 'RADIUS Authentication Servers' and includes a 'Call Station ID Type' dropdown set to 'IP Address' and a 'Use AES Key Wrap' checkbox which is unchecked. Below this is a table of configured servers:

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.1.12	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.1.1.14	1812	Disabled	Enabled

2. Agregue el Cisco NAC Guest Server como servidor de contabilidad en el WLC. Elija la Seguridad > el RADIUS > Accounting.

The screenshot shows the Cisco WLC Security page with the RADIUS Accounting Servers configuration. The left sidebar shows the navigation menu with 'Security' expanded to 'RADIUS' > 'Accounting'. The main content area is titled 'RADIUS Accounting Servers' and includes a table with columns for Network User, Server Index, Server Address, Port, IPSec, and Admin Status. There are 'Apply' and 'New...' buttons at the top right of the configuration area.

Elija **nuevo**. Agregue la dirección IP (10.1.1.14) para el Cisco NAC Guest Server. Agregue el secreto compartido. Confirme el secreto compartido.

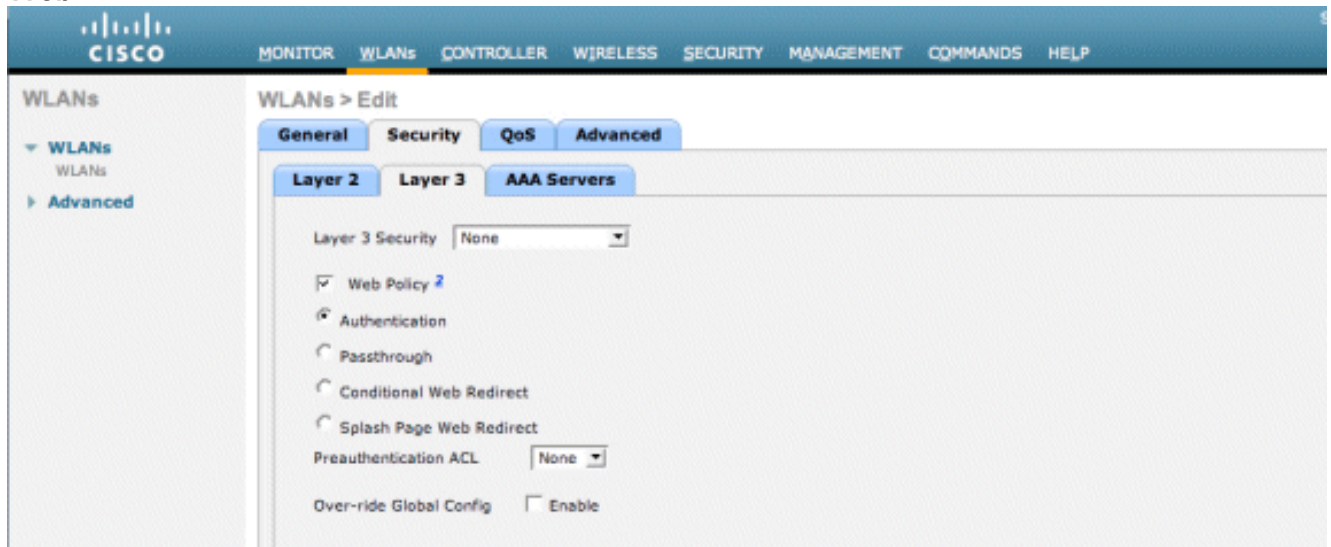
The screenshot shows the Cisco WLC Security page with the 'New' RADIUS Accounting Server configuration form. The left sidebar shows the navigation menu with 'Security' expanded to 'RADIUS' > 'Accounting'. The main content area is titled 'RADIUS Accounting Servers > New' and includes the following fields:

- Server Index (Priority): 2
- Server IP Address: 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

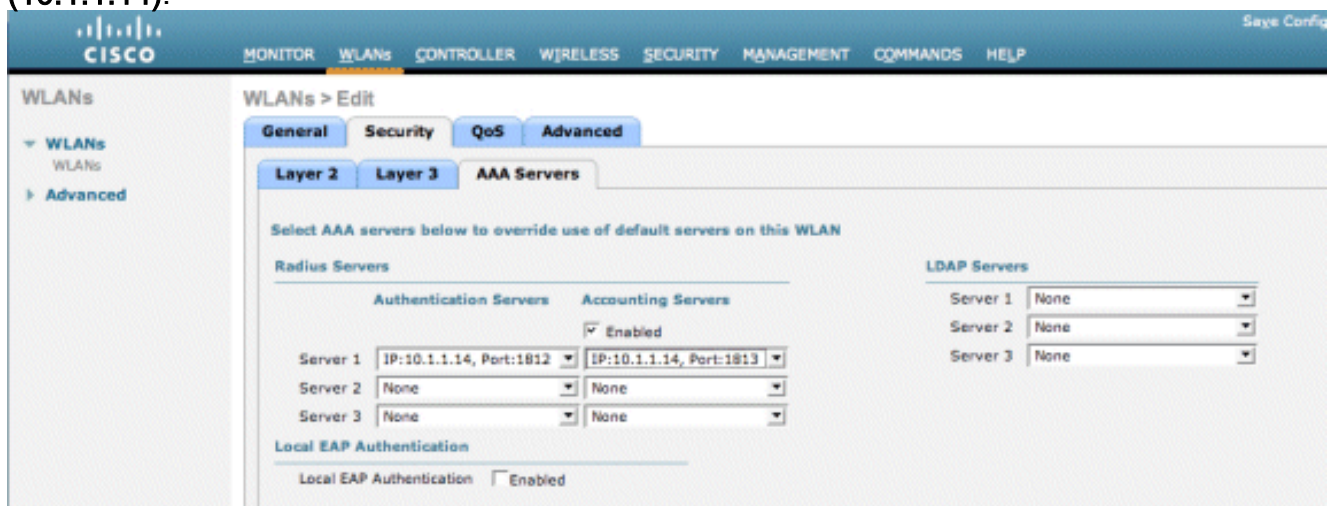
Elija se aplican.



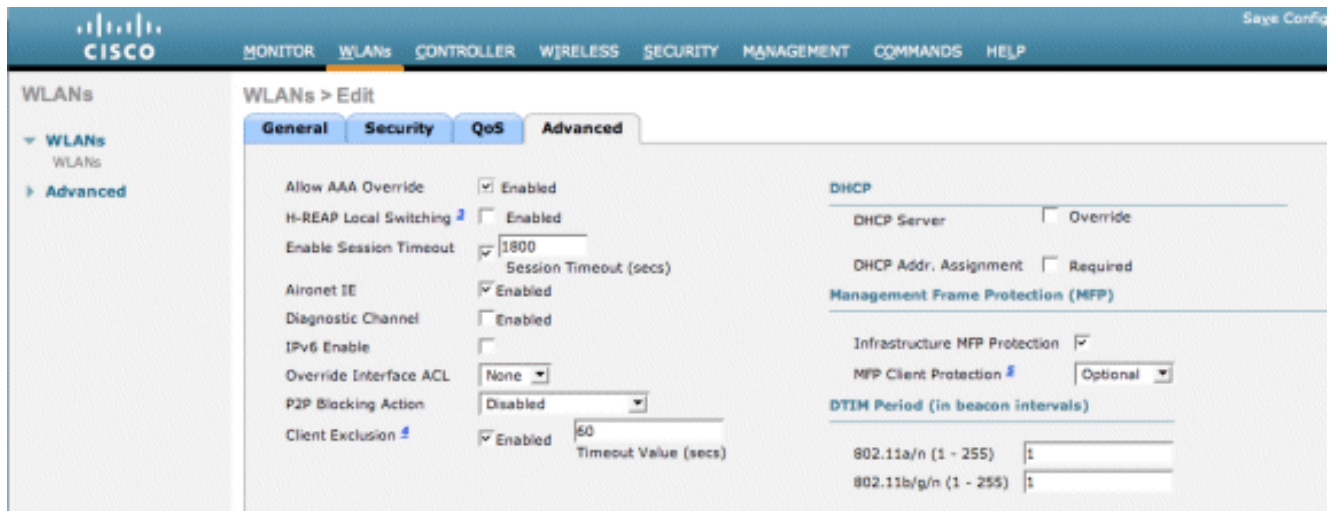
3. Modifique la red inalámbrica (WLAN) (Tecnología inalámbrica-x) para utilizar el servidor del invitado del NAC. Edite la red inalámbrica (WLAN) (Tecnología inalámbrica-x). Elija la **ficha de seguridad**. Cambie la Seguridad de la capa 2 a **ningunos** y acode la Seguridad 3 para utilizar la **autenticación Web**.



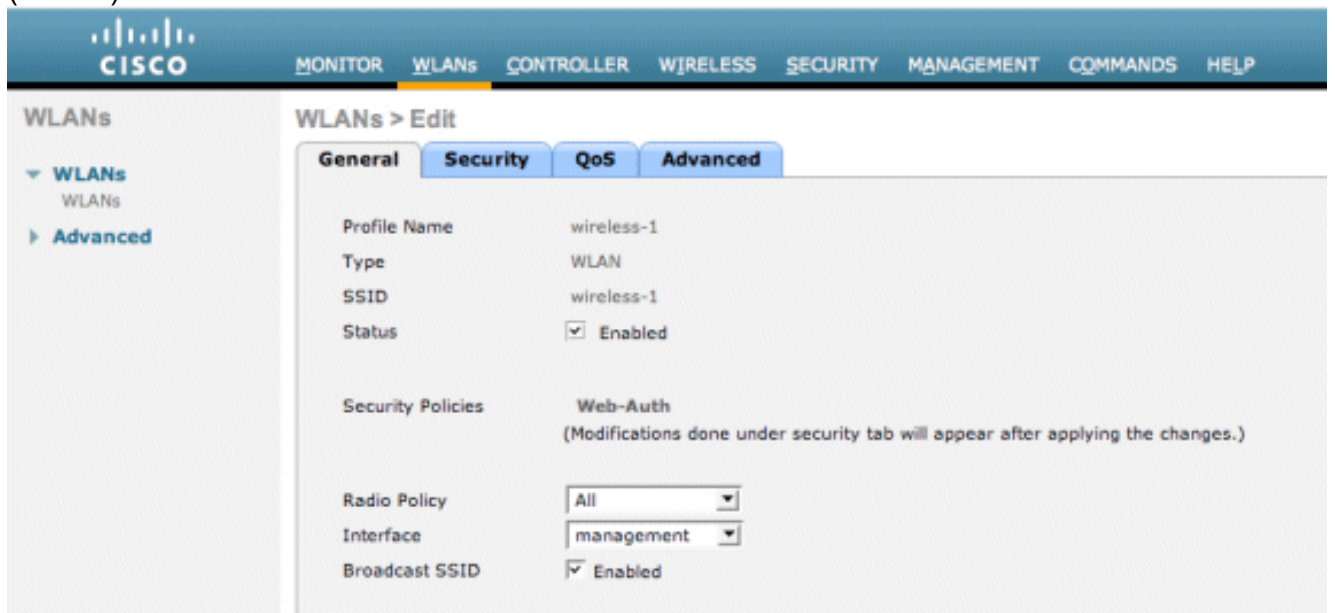
Elija a los **servidores de AAA** conforme a la ficha de seguridad. Bajo el cuadro del server1, elija al **servidor de RADIUS (10.1.1.14)**. Bajo el cuadro del server1, elija al **servidor de contabilidad (10.1.1.14)**.



Elija el **ficha Avanzadas**. El permiso **permite la invalidación AAA**. Esto permite por el **descanso de sesión de cliente** ser fijada del dispositivo del invitado del NAC.



Nota: Cuando la invalidación AAA se habilita en el SSID, el tiempo de vida restante del Usuario invitado en los NG se avanza al WLC como tiempo de espera de la sesión a la hora del login del Usuario invitado. Elija **se aplican** para salvar su configuración de la red inalámbrica (WLAN).



4. Verifique si el regulador esté agregado como cliente RADIUS en el Cisco NAC Guest Server. Hojee al servidor del invitado del NAC (<https://10.1.1.14/admin>) para configurar esto. **Nota:** Usted consigue la página de administración si usted especifica /admin en el URL.



Elija a los **clientes RADIUS**. Elija **agregar el radio**. Ingrese la información del cliente RADIUS: Ingrese un nombre: Nombre del sistema del WLC. Ingrese el IP Address: Dirección IP del WLC (10.10.51.2). Ingrese el mismo secreto compartido que usted ingresó en el paso 1. Confirme su secreto compartido. Ingrese una descripción. Elija **agregar al cliente RADIUS**.

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

Add Radius Client Reset Form

© Cisco 2007 Version 1.0.0

Recomiende el servicio RADIUS para que los cambios tomen el efecto. Elija a los **clientes RADIUS**. Elija el **reinicio** en el cuadro del radio del reinicio.

Radius Clients

Radius Clients

CAM wlc

Add Radius Edit Radius Delete Radius

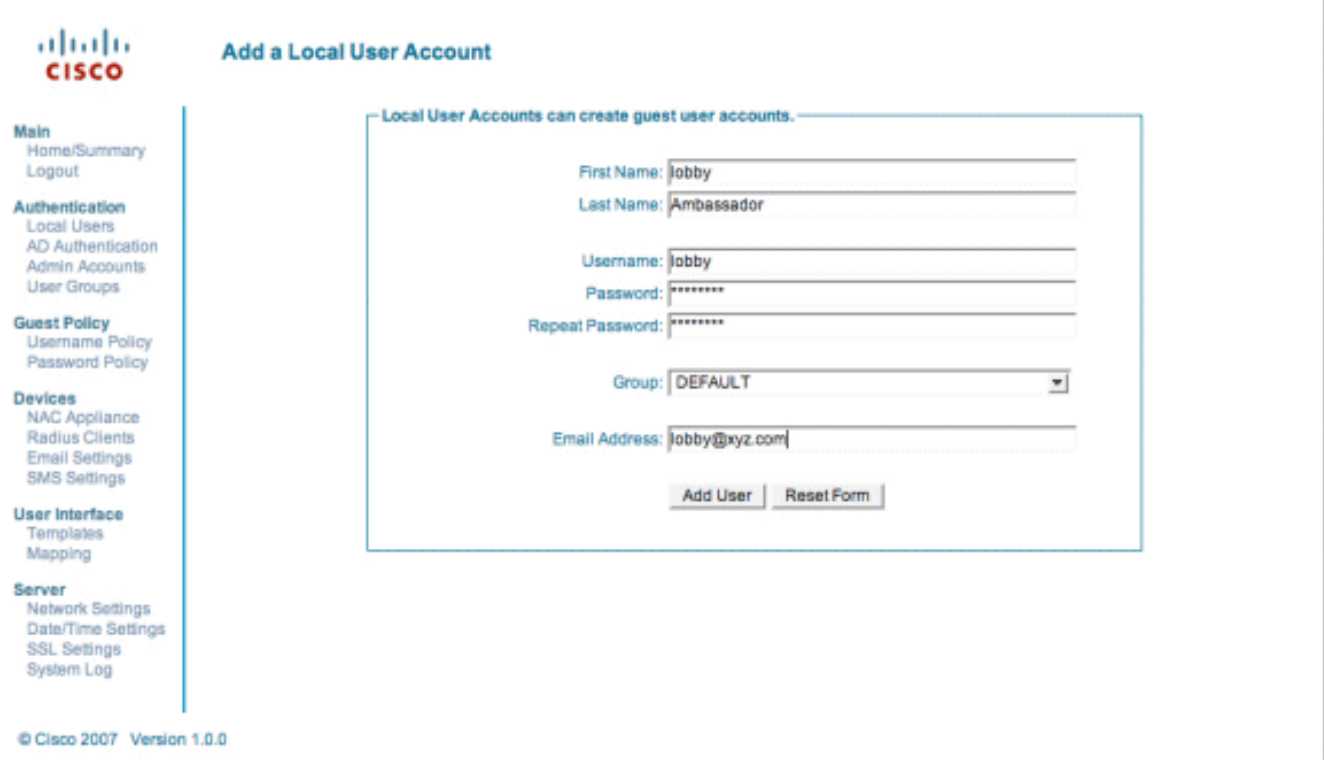
Restart Radius

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

© Cisco 2007 Version 1.0.0

5. Cree a un usuario local, es decir, embajador del pasillo, en el Cisco NAC Guest Server. Elija a los **usuarios locales**. Elija **agregar al usuario**. **Nota:** Usted debe completar todos los campos. Ingrese un primer nombre: **pasillo**. Ingrese un último nombre: **Embajador**. Ingrese el

nombre de usuario: **pasillo**. Ingrese una contraseña: contraseña. Deje al grupo como **valor por defecto**. Ingrese la dirección email: **lobby@xyz.com**. Elija **agregar al usuario**.



The screenshot displays the Cisco NAC Guest Server interface for adding a local user account. The page title is "Add a Local User Account". On the left, there is a navigation menu with categories: 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), User Interface (Templates, Mapping), and Server (Network Settings, Date/Time Settings, SSL Settings, System Log). The main content area is titled "Local User Accounts can create guest user accounts." and contains a form with the following fields: First Name (Jobby), Last Name (Ambassador), Username (Jobby), Password (masked), Repeat Password (masked), Group (DEFAULT), and Email Address (lobby@xyz.com). At the bottom of the form are two buttons: "Add User" and "Reset Form". The footer of the page reads "© Cisco 2007 Version 1.0.0".

6. Inicie sesión como el usuario local y cree una cuenta de invitado. Hojee al servidor del invitado del NAC (<https://10.1.1.14>), login con el Nombre de usuario/la contraseña que usted creó en el paso 5, y configura esto:



The screenshot displays the Cisco NAC Guest Server interface for managing guest user accounts. The page title is "Welcome to the Cisco NAC Guest Server". On the left, there is a navigation menu with categories: Main (Home, Logout), User Accounts (Create, Edit, Suspend), and Reporting (Active Accounts, Full Reporting). The main content area is titled "What would you like to do:" and contains a list of actions: "Create a Guest User Account", "Edit Guest User Account end time", "Suspend Guest User Accounts", "View Active Guest User Accounts", and "Report on Guest User accounts".

Elija **crean** para una cuenta de Usuario invitado. **Nota:** Usted debe completar todos los campos. Ingrese un primer nombre. Ingrese un último nombre. Ingrese a la compañía. Ingrese la dirección email. **Nota:** La dirección de correo electrónico es el nombre de usuario. Ingrese el extremo de cuenta: **hora**. Elija **agregar al usuario**.



Create a Guest User Account

- Main
 - Home
 - Logout
- User Accounts
 - Create
 - Edit
 - Suspend
- Reporting
 - Active Accounts
 - Full Reporting

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
<input type="button" value="Print"/> <input type="button" value="Email"/> <input type="button" value="SMS"/>	

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

First Name:	<input type="text" value="guest1"/>
Last Name:	<input type="text" value="guest1"/>
Company:	<input type="text" value="cisco"/>
Email Address:	<input type="text" value="guest1@cisco.com"/>
Mobile Phone Number:	<input type="text" value="+1 (VG) 9990000"/>
Account Start: Time	<input type="text" value="06"/> : <input type="text" value="00"/>
Date	<input type="text" value="15"/> / <input type="text" value="Jan"/> / <input type="text" value="2008"/>
Account End: Time	<input type="text" value="23"/> : <input type="text" value="59"/>
Date	<input type="text" value="18"/> / <input type="text" value="Jan"/> / <input type="text" value="2008"/>
Timezone:	<input type="text" value="America/Los_Angeles"/>
<input type="button" value="Add User"/> <input type="button" value="Reset Form"/>	

© Cisco 2007

- Conecte con la red inalámbrica (WLAN) del invitado y inicie sesión como el Usuario invitado. Conecte a su cliente de red inalámbrica con la red inalámbrica (WLAN) del invitado (Tecnología inalámbrica-x). Abra el buscador Web que se reorientará a la página de registro del Red-auth. **Nota:** Alternativamente, tipo <https://1.1.1.1/login.html> que se reorientará a la página de registro. Ingrese el nombre de Usuario invitado que usted creó en el paso 6. Ingrese la contraseña que auto-fue generada en el paso 6. Telnet al WLC y verifica que el tiempo de espera de la sesión se haya fijado con el **comando detail del cliente de la demostración**. Cuando expira el tiempo de espera de la sesión, el cliente del invitado es sus del ping paradas disconnected, y.

```
(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:f8
Client State..... Associated
Wireless LAN Id..... 1
BSSID..... 00:17:df:a6:e5:ff
Channel..... 68
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) >
```

Nota: Para configurar la autenticación Web del controlador LAN de Wireleass, WLC al servidor del invitado del NAC (NG), usted necesita utilizar la autenticación del modo PAP en las propiedades

del red-auth. Si la directiva de la autenticación Web se fija PARA AGRIETAR, la autenticación falla porque la GRIETA no se soporta con los NG.

[Información Relacionada](#)

- [Dispositivo NAC de Cisco - Guía de instalación y configuración limpia del Access Manager, versión 4.1\(3\)](#)
- [Soporte del Switch del dispositivo NAC de Cisco y del regulador del Wireless LAN](#)
- [Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0](#)
- [Integración \(video\) del Cisco Identity Services Engine \(ISE\) y del regulador del Wireless LAN \(WLC\)](#)
- [NAC \(limpie el acceso\): Configure el acceso de invitado](#)
- [Guía de despliegue: Acceso de invitado de Cisco usando el controlador LAN de la tecnología inalámbrica de Cisco, versión 4.1](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)