

Guida all'integrazione di WLC e NAC Guest Server (NGS)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione del controller WLC](#)

[Inizializzazione](#)

[Cisco NAC Guest Server](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento vengono fornite le linee guida per l'integrazione di NAC Guest Server e Wireless LAN Controller.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Wireless LAN Controller (WLC) 4.2.61.0
- Catalyst 3560 con IOS[®] versione 12.2(25)SEE2
- Cisco ADU versione 4.0.0.279
- NAC Guest Server versione 1.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

Cisco NAC Guest Server è un sistema completo di provisioning e reporting che fornisce accesso temporaneo alla rete a ospiti, visitatori, collaboratori esterni, consulenti o clienti. Il server guest funziona insieme a Cisco NAC Appliance o Cisco Wireless LAN Controller, che fornisce il portale captive e il punto di imposizione per l'accesso guest.

Cisco NAC Guest Server consente a qualsiasi utente con privilegi di creare facilmente account guest temporanei e sponsor guest. Cisco NAC Guest Server esegue l'autenticazione completa degli sponsor, ossia gli utenti che creano account guest, e consente agli sponsor di fornire i dettagli dell'account all'guest tramite stampa, e-mail o SMS. L'intera esperienza, dalla creazione di account utente all'accesso alla rete guest, viene archiviata per il controllo e la creazione di report.

Quando si creano gli account guest, viene eseguito il provisioning in Cisco NAC Appliance Manager (Clean Access Manager) o vengono archiviati nel database incorporato in Cisco NAC Guest Server. Quando si utilizza il database incorporato del server guest, i dispositivi di accesso alla rete esterni, ad esempio Cisco Wireless LAN Controller, possono autenticare gli utenti sul server guest con il protocollo RADIUS (Remote Authentication Dial In User Service).

Cisco NAC Guest Server esegue il provisioning dell'account Guest per il periodo di tempo specificato al momento della creazione dell'account. Alla scadenza dell'account, il server guest elimina l'account direttamente da Cisco NAC Appliance Manager o invia un messaggio RADIUS per notificare al dispositivo di accesso alla rete (NAD) il periodo di validità rimanente per l'account prima che il NAD rimuova l'utente.

Cisco NAC Guest Server fornisce un'importante contabilità dell'accesso alla rete guest consolidando l'intero audit trail dalla creazione degli account guest all'utilizzo degli account guest, in modo che i report possano essere eseguiti attraverso un'interfaccia di gestione centrale.

Nozioni base sull'accesso guest

Cisco NAC Guest Server utilizza una serie di termini per spiegare i componenti necessari per fornire l'accesso guest.

Utente Guest

L'utente guest è la persona che ha bisogno di un account utente per accedere alla rete.

Sponsor

Lo sponsor è la persona che crea l'account utente guest. Questa persona è spesso un dipendente dell'organizzazione che fornisce l'accesso alla rete. Gli sponsor possono essere persone specifiche (3) con determinati ruoli di lavoro o qualsiasi dipendente in grado di eseguire l'autenticazione in una directory aziendale, ad esempio Microsoft Active Directory (AD).

Dispositivo di imposizione di rete

Questi dispositivi sono i componenti dell'infrastruttura di rete che forniscono l'accesso alla rete. Inoltre, i dispositivi di imposizione di rete spingono gli utenti guest a un portale vincolato, dove

possono immettere i dettagli dell'account guest. Quando un guest immette il proprio nome utente e la propria password temporanei, il dispositivo di imposizione di rete controlla tali credenziali rispetto agli account guest creati dal server guest.

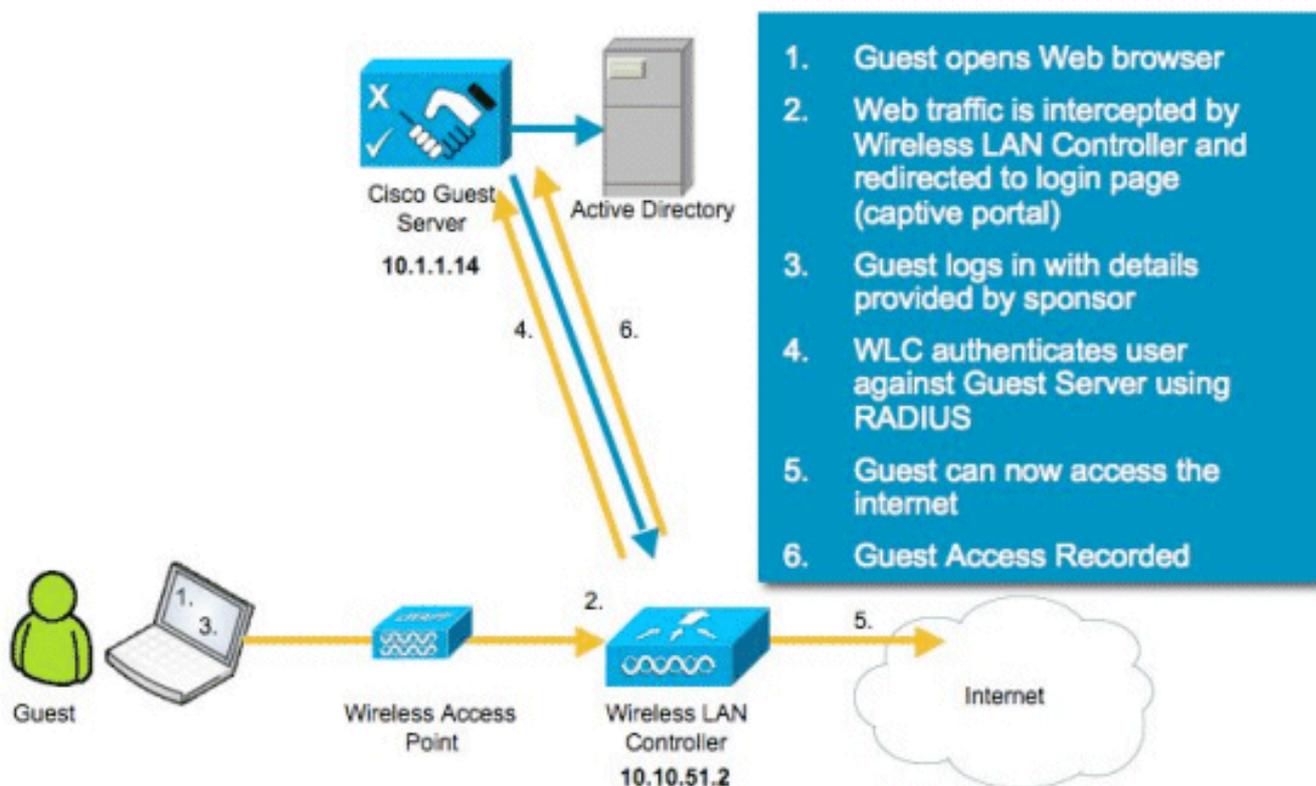
Guest Server

Questo è il Cisco NAC Guest Server, che unisce tutti i componenti dell'accesso guest. Il server guest collega tra loro: lo sponsor che crea l'account guest, i dettagli dell'account passati al guest, l'autenticazione guest rispetto al dispositivo di imposizione di rete e la verifica del dispositivo di imposizione di rete del guest con il server guest. Inoltre, Cisco NAC Guest Server consolida le informazioni di accounting provenienti dai dispositivi di imposizione di rete per fornire un singolo punto di accesso guest ai report.

La documentazione dettagliata relativa a NGS è disponibile in CCO.

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

Panoramica sulla topologia Lab



Configurazione del controller WLC

Per configurare il WLC, attenersi alla procedura seguente:

1. Inizializzare il controller e il punto di accesso.
2. Configurare le interfacce del controller.
3. Configurare RADIUS.
4. Configurare le impostazioni WLAN.

Inizializzazione

Per la configurazione iniziale, utilizzare una connessione console come HyperTerminal e seguire le istruzioni di installazione per popolare le informazioni di accesso e interfaccia. Anche il comando **reset system** avvia questi prompt.

```
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 è una soluzione di provisioning e reporting che fornisce accesso temporaneo alla rete a client quali guest, collaboratori esterni, ecc. Cisco NAC Guest Server funziona con le soluzioni Cisco Unified Wireless Network o Cisco NAC Appliance. In questo documento viene descritta la procedura per integrare Cisco NAC Guest Server con un Cisco WLC, che crea un account utente guest e verifica l'accesso temporaneo alla rete del guest.

Per completare l'integrazione, procedere come segue:

1. Aggiungere Cisco NAC Guest Server come server di autenticazione nel WLC. Accedere al WLC (<https://10.10.51.2>, admin/admin) per configurare questa opzione. Scegliere **Sicurezza > RADIUS > Autenticazione**.

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies

RADIUS Authentication Servers

Call Station ID Type:

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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.1.12	1812	Disabled	Enabled <input type="button" value="v"/>

Scegliere **Nuovo**. Aggiungere l'indirizzo IP (10.1.1.14) per Cisco NAC Guest Server. Aggiungere il segreto condiviso. Confermare il segreto condiviso.

Security

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

RADIUS Authentication Servers > New

Server Index (Priority):

Server IP Address:

Shared Secret Format:

Shared Secret:

Confirm Shared Secret:

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

Port Number:

Server Status:

Support for RFC 3576:

Server Timeout: seconds

Network User: Enable

Management: Enable

IPSec: Enable

Scegliere **Applica**.

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies

RADIUS Authentication Servers

Call Station ID Type:

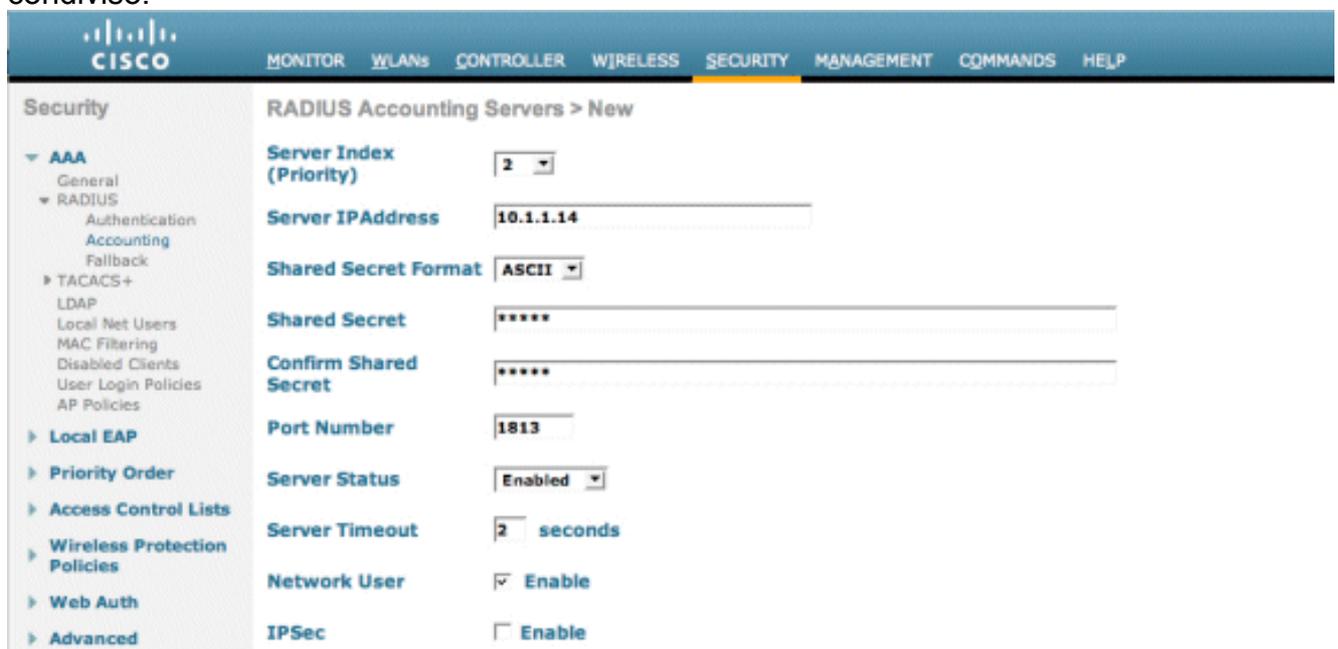
Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

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

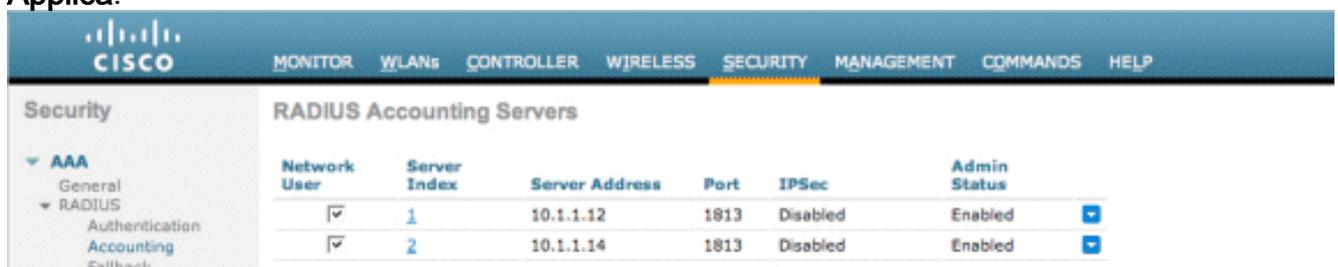
2. Aggiungere Cisco NAC Guest Server come server di accounting nel WLC. Scegliere **Sicurezza > RADIUS > Accounting**.



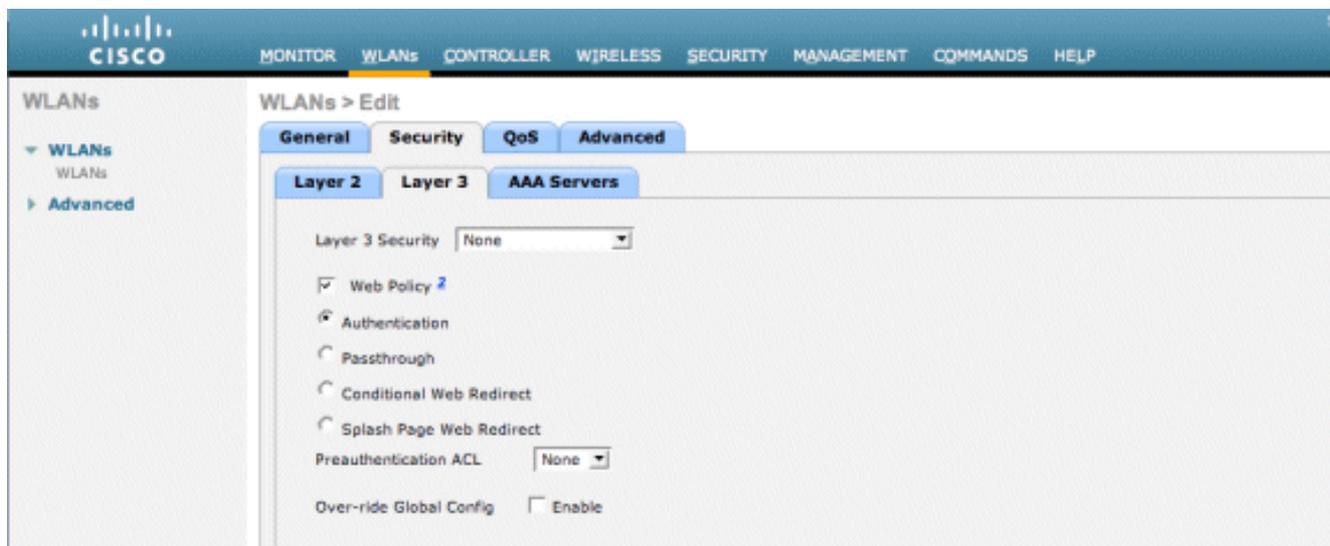
Scegliere **Nuovo**. Aggiungere l'indirizzo IP (10.1.1.14) per Cisco NAC Guest Server. Aggiungere il segreto condiviso. Confermare il segreto condiviso.



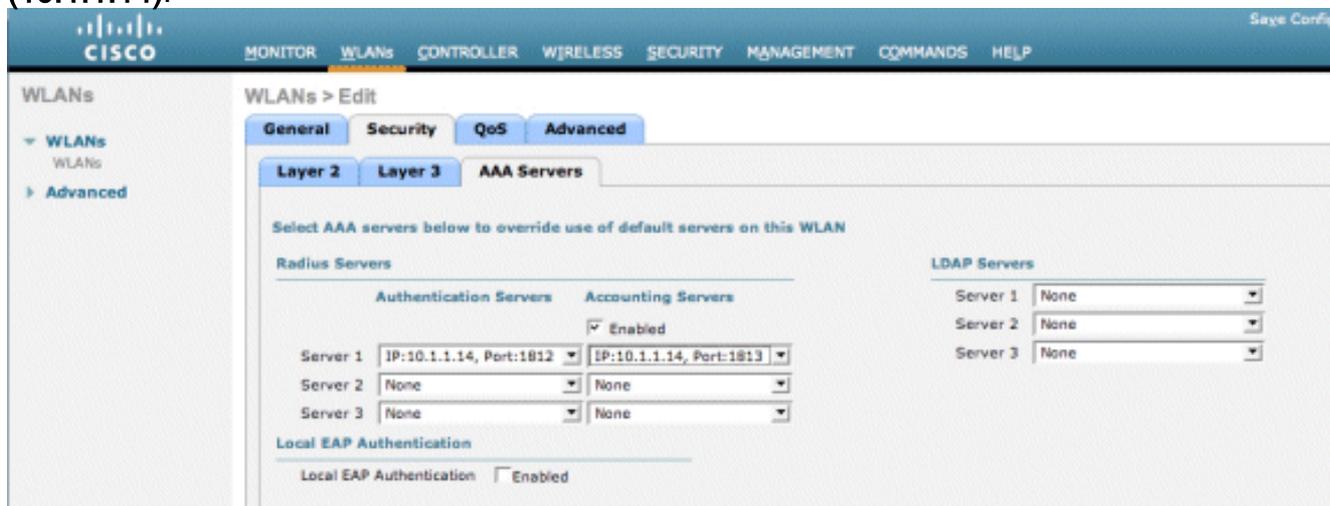
Scegliere **Applica**.



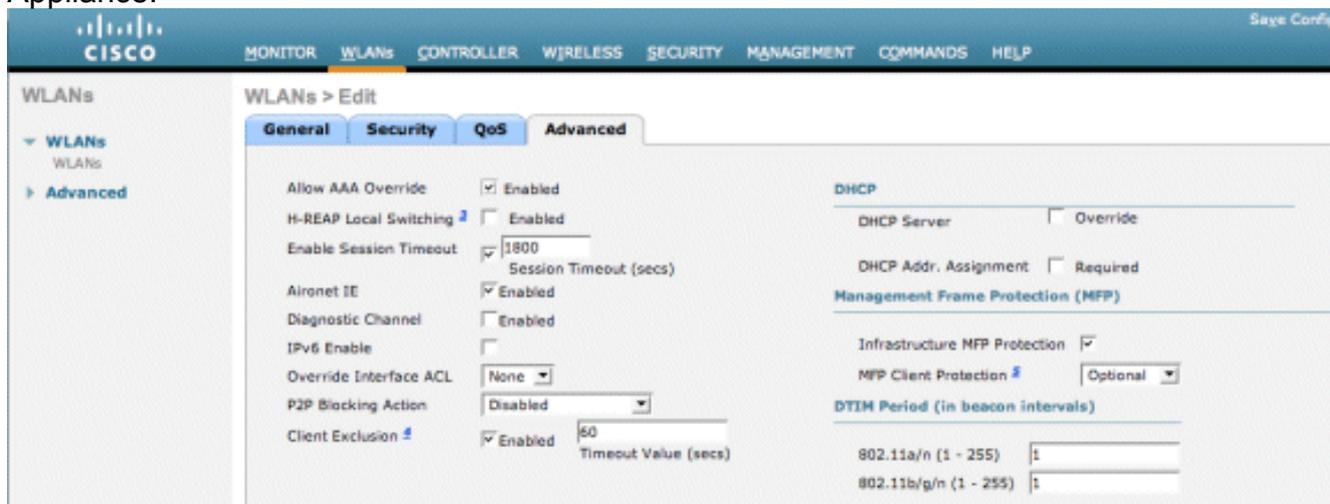
3. Modificare la WLAN (wireless-x) in modo da utilizzare il NAC Guest Server. Modificare la WLAN (wireless-x). Scegliere la scheda **Protezione**. Impostare Protezione di livello 2 su **Nessuna** e Protezione di livello 3 per utilizzare l'**autenticazione Web**.



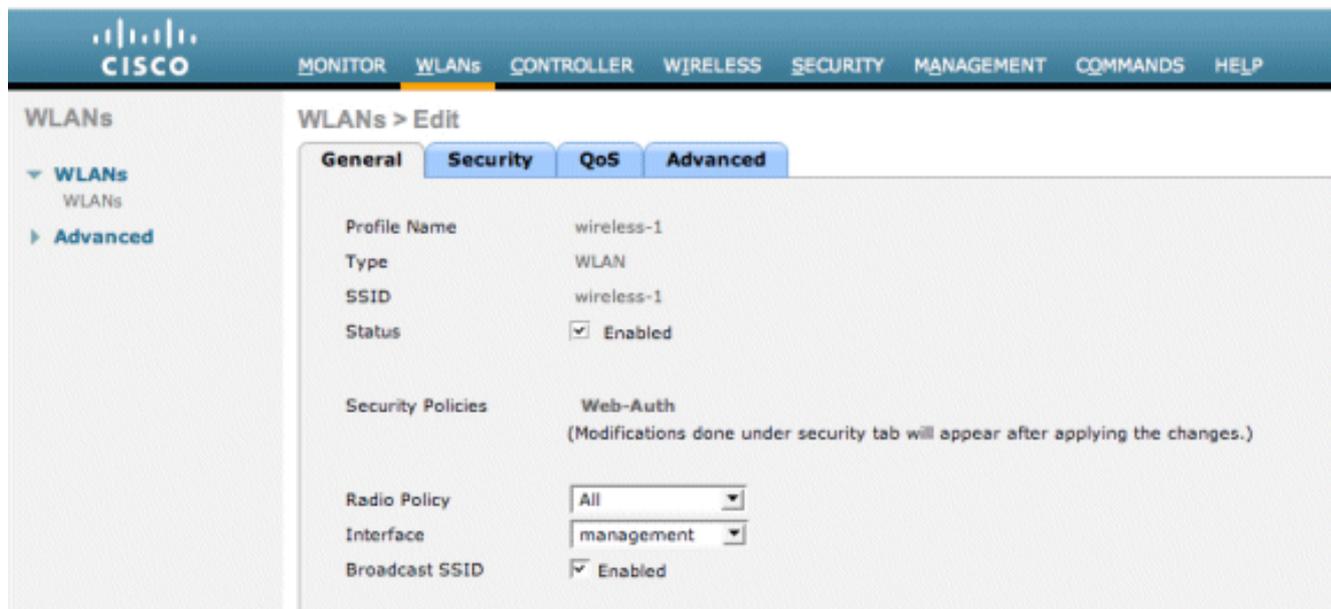
Selezionare i **server AAA** nella scheda Security (Sicurezza). Nella casella Server 1 scegliere il **server RADIUS (10.1.1.14)**. Nella casella Server 1 scegliere **Accounting Server (10.1.1.14)**.



Scegliere la scheda **Avanzate**. Abilitare **Consenti sostituzione AAA**. In questo modo, è possibile impostare il timeout della sessione per client da NAC Guest Appliance.



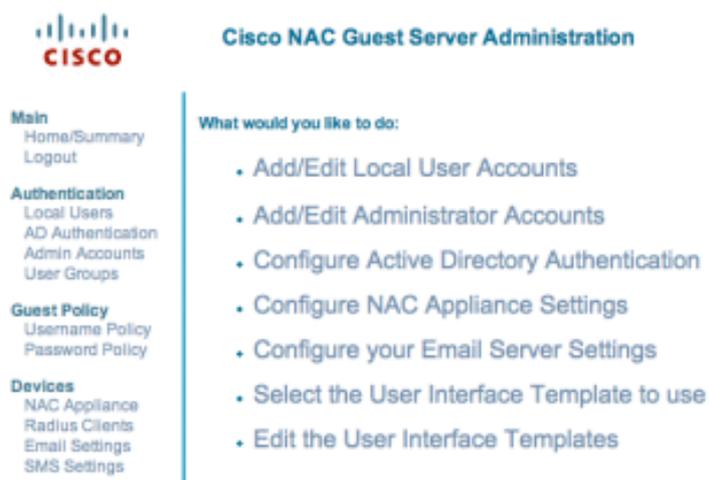
Nota: quando la **sostituzione AAA** è abilitata sull'SSID, la durata rimanente dell'utente guest su NGS viene trasferita sul WLC come timeout della sessione al momento dell'accesso dell'utente guest. Scegliere **Apply** (Applica) per salvare la configurazione WLAN.



The screenshot shows the Cisco NAC Guest Server Administration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the WLANs menu with options for WLANs and Advanced. The main content area is titled 'WLANs > Edit' and has four tabs: General, Security, QoS, and Advanced. The Security tab is active, displaying the following configuration:

Profile Name	wireless-1
Type	WLAN
SSID	wireless-1
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

4. Verificare se il controller è stato aggiunto come client Radius in Cisco NAC Guest Server. Selezionare NAC Guest Server (<https://10.1.1.14/admin>) per configurare questa opzione. **Nota:** se si specifica l'opzione /admin nell'URL, viene visualizzata la pagina Amministrazione.



The screenshot shows the Cisco NAC Guest Server Administration interface. The top navigation bar includes the Cisco logo and the title 'Cisco NAC Guest Server Administration'. The left sidebar shows the main menu with options for Main, Authentication, Guest Policy, and Devices. The main content area is titled 'What would you like to do:' and lists the following actions:

- 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

Selezionate **Client raggio**. Selezionate **Agg raggio (Add Radius)**. Immettere le informazioni sul client Radius: Immettere un nome: nome sistema WLC. Immettere l'indirizzo IP: indirizzo IP del WLC (10.10.51.2). Immettere lo stesso segreto condiviso immesso al passaggio 1. Conferma il tuo segreto condiviso. Immettere una descrizione. Scegliere **Aggiungi client Radius**.



Add Radius Client

- 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
- Server
 - Network Settings
 - Date/Time Settings
 - SSL Settings
 - System Log

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

© Cisco 2007 Version 1.0.0

Riavviare il servizio Radius per rendere effettive le modifiche. Selezionate **Client raggio**. Selezionate **Riavvia (Restart)** nella casella Raggio riavvio (Restart Radius).



Radius Clients

- 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
- Server
 - Network Settings
 - Date/Time Settings
 - SSL Settings
 - System Log

Radius Clients

CAM
wlc

Restart Radius

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

© Cisco 2007 Version 1.0.0

5. Creare un utente locale, ovvero Lobby Ambassador, nel Cisco NAC Guest Server. Scegliere **Utenti locali**. Scegliere **Aggiungi utente**. **Nota:** è necessario compilare tutti i campi. Immettere un nome: **lobby**. Immettere un cognome: **Ambasciatore**. Immettere Nome utente: **sala di attesa**. Immettere una password: **password**. Lasciare Gruppo come **predefinito**. Immettere L'Indirizzo Di Posta Elettronica: **lobby@xyz.com**. Scegliere **Aggiungi utente**.



Add a Local User Account

- 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
- Server**
 - Network Settings
 - Date/Time Settings
 - SSL Settings
 - System Log

Local User Accounts can create guest user accounts.

First Name:

Last Name:

Username:

Password:

Repeat Password:

Group:

Email Address:

© Cisco 2007 Version 1.0.0

6. Eseguire il login come utente locale e creare un account guest. Accedere al NAC Guest Server (<https://10.1.1.14>) con il nome utente e la password creati al punto 5 e configurare quanto segue:



Welcome to the Cisco NAC Guest Server

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

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](#)

Scegliere **Crea** per un account utente guest. **Nota:** è necessario compilare tutti i campi. Immettere un nome. Immettere un cognome. Inserire la società. Immettere l'indirizzo di posta elettronica. **Nota:** l'indirizzo e-mail è il nome utente. Inserire il campo Fine conto: **ora.** Scegliere **Aggiungi utente.**



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

7. Connettersi alla WLAN guest e accedere come utente guest. Collegare il client wireless alla rete WLAN guest (wireless-x). Aprire il browser Web da reindirizzare alla pagina Accesso Web-Auth. **Nota:** in alternativa, digitare <https://1.1.1.1/login.html> per essere reindirizzati alla pagina Accesso. Immettere il nome utente guest creato nel passo 6. Immettere la password generata automaticamente al passaggio 6. Telnet su WLC e verificare che il timeout della sessione sia stato impostato con il comando **show client detail**. Alla scadenza del timeout della sessione, il client guest viene disconnesso e il ping viene interrotto.

```
(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
VMH Support..... Enabled
U-APSD Support..... Disabled
Mobility State..... Local
--More-- or (q)uit
(Cisco Controller) >
```

Nota: per configurare l'autenticazione Web dal controller LAN Wireless, dal WLC al server guest NAC (NGS), è necessario usare l'autenticazione in modalità PAP sulle proprietà di autenticazione Web. Se il criterio di autenticazione Web è impostato su CHAP, l'autenticazione ha esito negativo perché CHAP non è supportato con NGS.

Informazioni correlate

- [Appliance Cisco NAC - Guida all'installazione e alla configurazione di Clean Access Manager, versione 4.1\(3\)](#)
- [Supporto switch appliance Cisco NAC e controller LAN wireless](#)
- [Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0](#)
- [\(Video\) Integrazione di Cisco Identity Services Engine \(ISE\) e Wireless LAN Controller \(WLC\)](#)
- [NAC \(Clean Access\): configurazione dell'accesso guest](#)
- [Guida all'installazione: Cisco Guest Access Using the Cisco Wireless LAN Controller, release 4.1](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).