

Guia de integração de servidor convidado (NGS) WLC e NAC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar a controladora Wireless LAN \(WLC\)](#)

[Inicialização](#)

[Servidor Convidado Cisco NAC](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento fornece uma diretriz para integrar o NAC Guest Server e os Controllers de LAN Wireless.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Controladora de LAN sem fio (WLC) 4.2.61.0 da Cisco
- Catalyst 3560 com IOS[®] versão 12.2(25)SEE2
- Cisco ADU Versão 4.0.0.279
- NAC Guest Server versão 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](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Informações de Apoio

O Cisco NAC Guest Server é um sistema completo de provisionamento e geração de relatórios que fornece acesso temporário à rede para convidados, visitantes, contratados, consultores ou clientes. O servidor convidado funciona junto com o Cisco NAC Appliance ou o Cisco Wireless LAN Controller, que fornece o portal cativo e o ponto de aplicação para acesso de convidados.

O Cisco NAC Guest Server permite que qualquer usuário com privilégios crie facilmente contas de convidado temporárias e patrocinadores convidados. O Cisco NAC Guest Server executa a autenticação completa de patrocinadores, os usuários que criam contas de convidado, e permite que os patrocinadores forneçam detalhes da conta para o convidado por impressão, e-mail ou SMS. Toda a experiência, desde a criação de contas de usuários até o acesso à rede de convidados, é armazenada para auditoria e relatórios.

Quando as contas de convidado são criadas, elas são provisionadas no Cisco NAC Appliance Manager (Clean Access Manager) ou armazenadas no banco de dados integrado no Cisco NAC Guest Server. Quando você usa o banco de dados integrado do servidor convidado, os dispositivos de acesso à rede externos, como o Cisco Wireless LAN Controller, podem autenticar usuários no servidor convidado com o protocolo RADIUS (Remote Authentication Dial In User Service).

O Cisco NAC Guest Server provisiona a conta de convidado pelo período de tempo especificado quando a conta é criada. Após a expiração da conta, o servidor convidado exclui a conta diretamente do Cisco NAC Appliance Manager ou envia uma mensagem RADIUS que notifica o dispositivo de acesso à rede (NAD) da quantidade de tempo válido restante para a conta antes que o NAD remova o usuário.

O Cisco NAC Guest Server fornece contabilidade de acesso vital à rede de convidados por meio da consolidação de toda a trilha de auditoria, desde a criação da conta de convidado até o uso da conta pelo convidado, de modo que os relatórios possam ser executados por meio de uma interface de gerenciamento central.

Conceitos de acesso para convidados

O Cisco NAC Guest Server usa vários termos para explicar os componentes necessários para fornecer acesso para convidados.

Usuário convidado

O usuário convidado é a pessoa que precisa de uma conta de usuário para acessar a rede.

Patrocinador

O Patrocinador é a pessoa que cria a conta de usuário convidado. Essa pessoa geralmente é um funcionário da organização que fornece acesso à rede. Os patrocinadores podem ser pessoas específicas, ou seja, indivíduos com determinadas funções profissionais, ou qualquer funcionário que possa se autenticar em um diretório corporativo, como o Microsoft Active Directory (AD).

Dispositivo de Imposição de Rede

Esses dispositivos são os componentes da infraestrutura de rede que fornecem o acesso à rede. Além disso, os dispositivos de aplicação da rede enviam os usuários convidados para um portal cativo, onde eles podem inserir os detalhes de suas contas de convidados. Quando um convidado insere seu nome de usuário e senha temporários, o dispositivo de imposição de rede verifica essas credenciais em relação às contas de convidado criadas pelo servidor convidado.

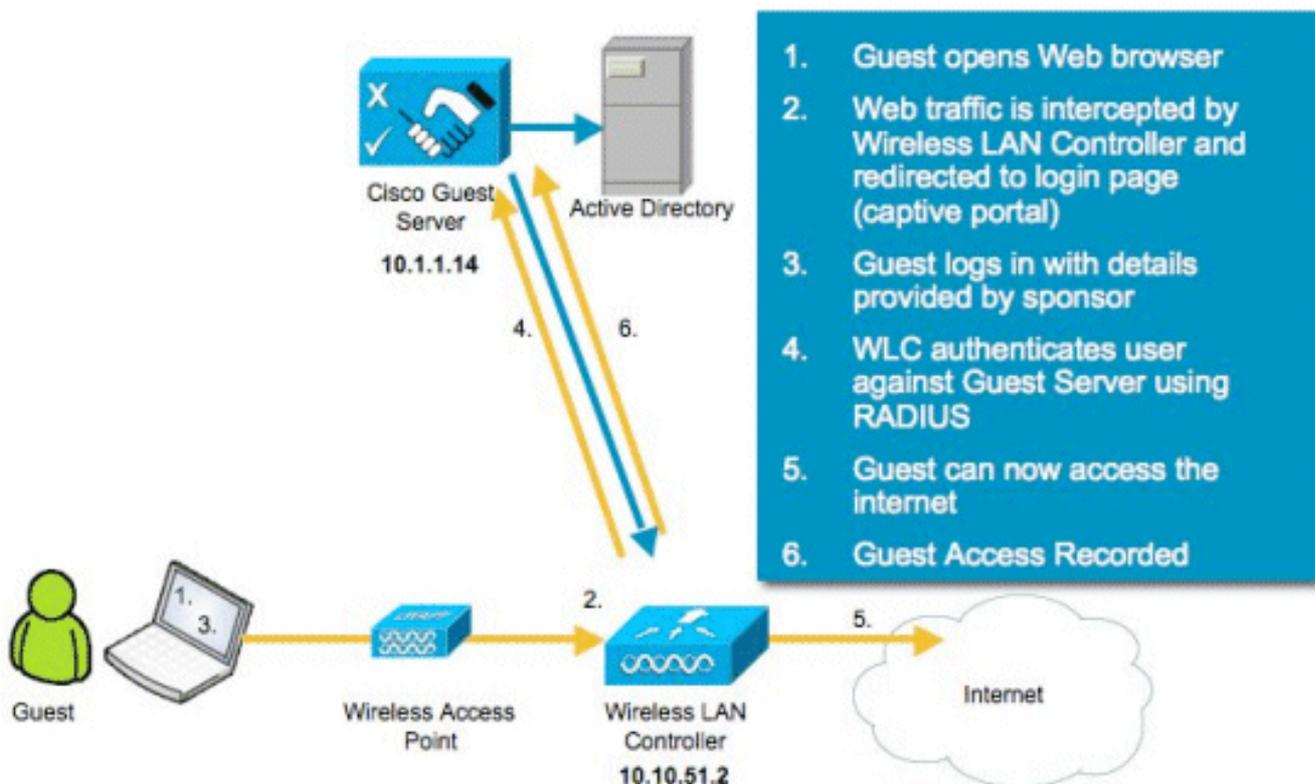
Servidor convidado

Esse é o Cisco NAC Guest Server, que une todas as partes do acesso de convidado. O Servidor Convidado vincula todos: o patrocinador que cria a conta de convidado, os detalhes da conta passados para o convidado, a autenticação de convidado em relação ao dispositivo de imposição de rede e a verificação do dispositivo de imposição de rede do convidado com o Servidor Convidado. Além disso, o Cisco NAC Guest Server consolida as informações de tarifação dos dispositivos de aplicação da rede para fornecer um único ponto de relatórios de acesso de convidados.

A documentação detalhada sobre o NGS está disponível no CCO.

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

Visão geral da topologia do laboratório



Configurar a controladora Wireless LAN (WLC)

Siga estas etapas para configurar o WLC:

1. Inicialize o controlador e o ponto de acesso.

2. Configure as interfaces do controlador.
3. Configure o RADIUS.
4. Defina as configurações da WLAN.

Inicialização

Para a configuração inicial, use uma conexão de console como o HyperTerminal e siga os prompts de configuração para preencher as informações de login e interface. O comando **reset system** também inicia esses 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
```

Servidor Convidado Cisco NAC

O Cisco NAC Guest Server é uma solução de provisionamento e geração de relatórios que fornece acesso temporário à rede para clientes, como convidados, contratados etc. O Cisco NAC Guest Server funciona com as soluções Cisco Unified Wireless Network ou Cisco NAC Appliance. Este documento orienta você durante as etapas para integrar o Cisco NAC Guest Server com um Cisco WLC, que cria uma conta de usuário convidado e verifica o acesso temporário à rede do convidado.

Siga estas etapas para concluir a integração:

1. Adicione o Cisco NAC Guest Server como um servidor de autenticação no WLC. Navegue até sua WLC (<https://10.10.51.2, admin/admin>) para configurar isso. Escolha **Security > RADIUS > Authentication**.

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'Security > RADIUS > Authentication' 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. Below this is a table listing existing 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 type="button" value="v"/>

Escolha **New**. Adicione o endereço IP (10.1.1.14) para o Cisco NAC Guest Server. Adicione o segredo compartilhado. Confirme o segredo compartilhado.

The screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The left sidebar shows the navigation menu with 'Security > RADIUS > Authentication > New' selected. The main content area contains the following configuration fields:

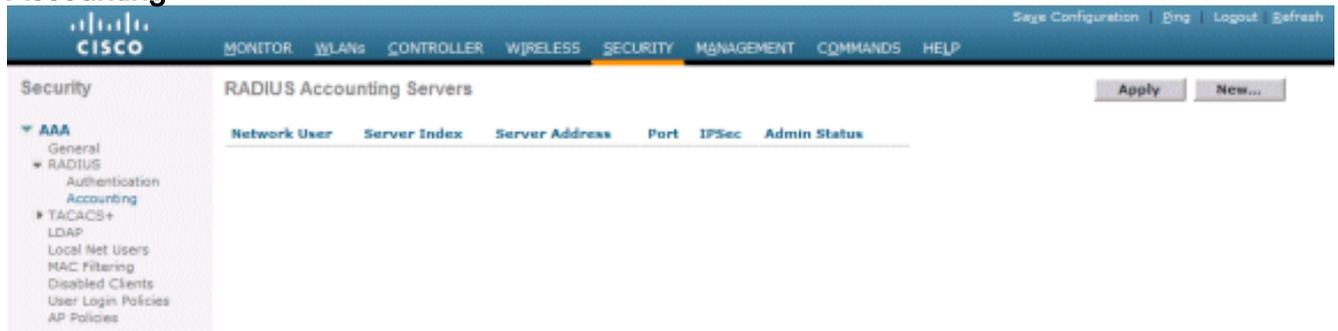
- Server Index (Priority): 2
- Server IP Address: 10.1.1.14
- Shared Secret Format: ASCII
- Shared Secret: *****
- Confirm Shared Secret: *****
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

Escolha **Aplicar**.

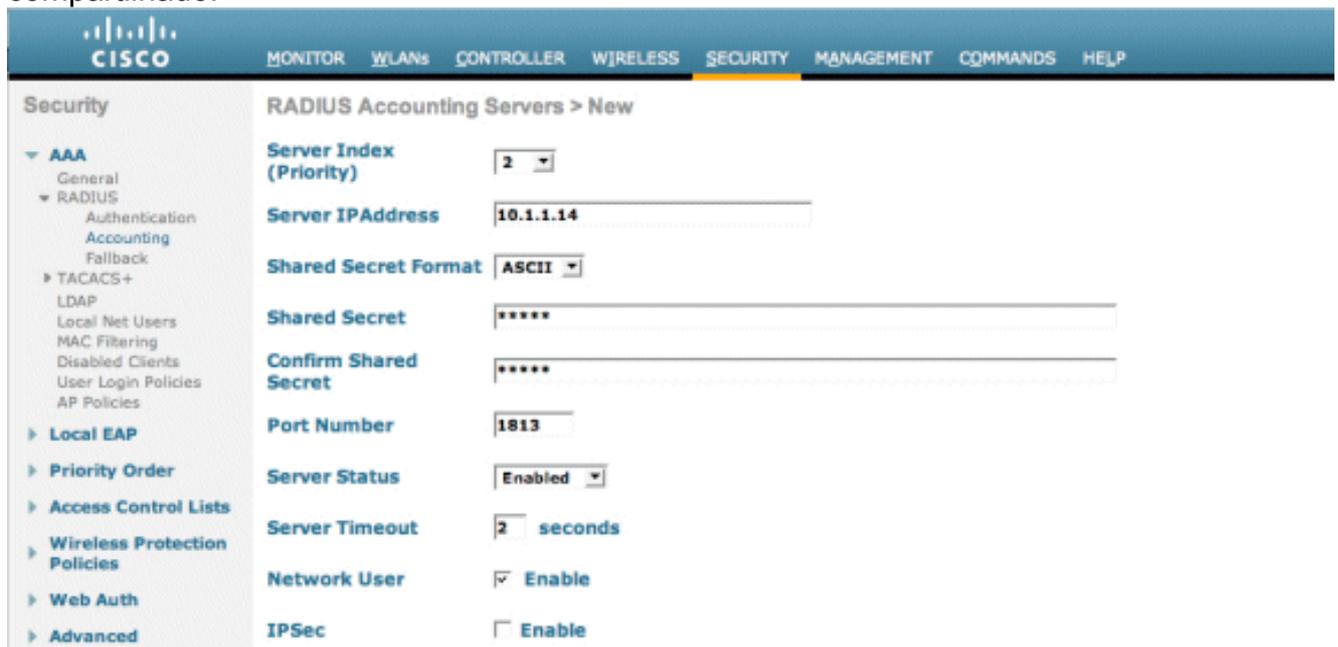
The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers after applying the changes. The left sidebar shows the navigation menu with 'Security > RADIUS > Authentication' selected. The main content area is titled 'RADIUS Authentication Servers' and includes a 'Call Station ID Type' dropdown set to 'IP Address' and a 'Use AES Key Wrap' checkbox. Below this is a table listing the updated 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 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. Adicione o Cisco NAC Guest Server como um servidor de contabilização no WLC. Escolha **Security > RADIUS > Accounting**.



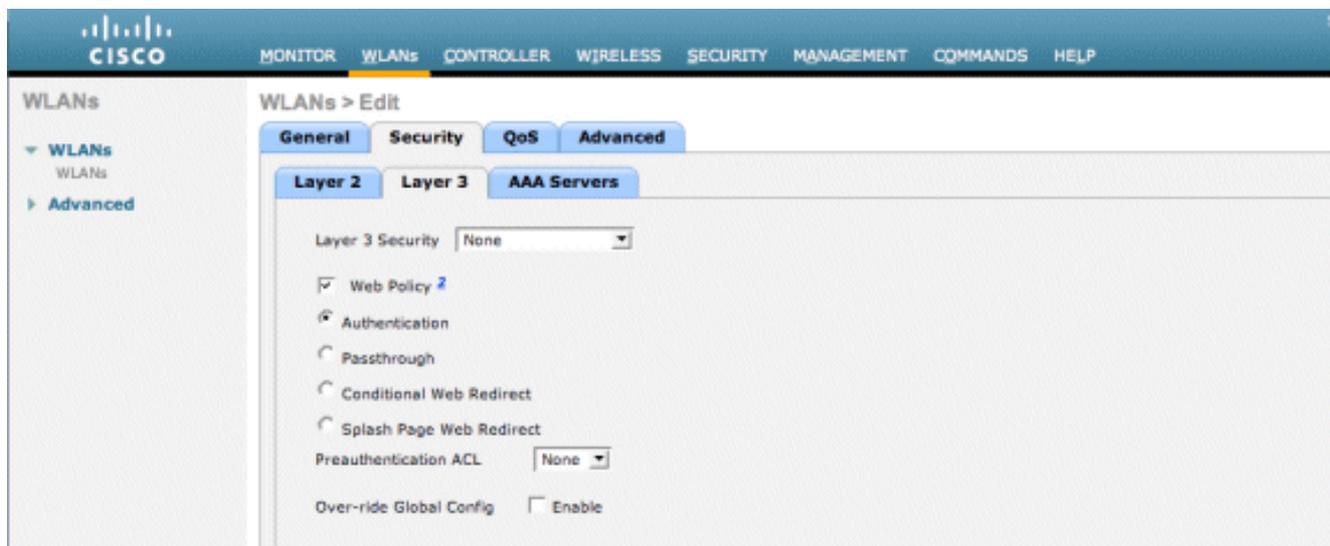
Escolha **New**. Adicione o endereço IP (10.1.1.14) para o Cisco NAC Guest Server. Adicione o segredo compartilhado. Confirme o segredo compartilhado.



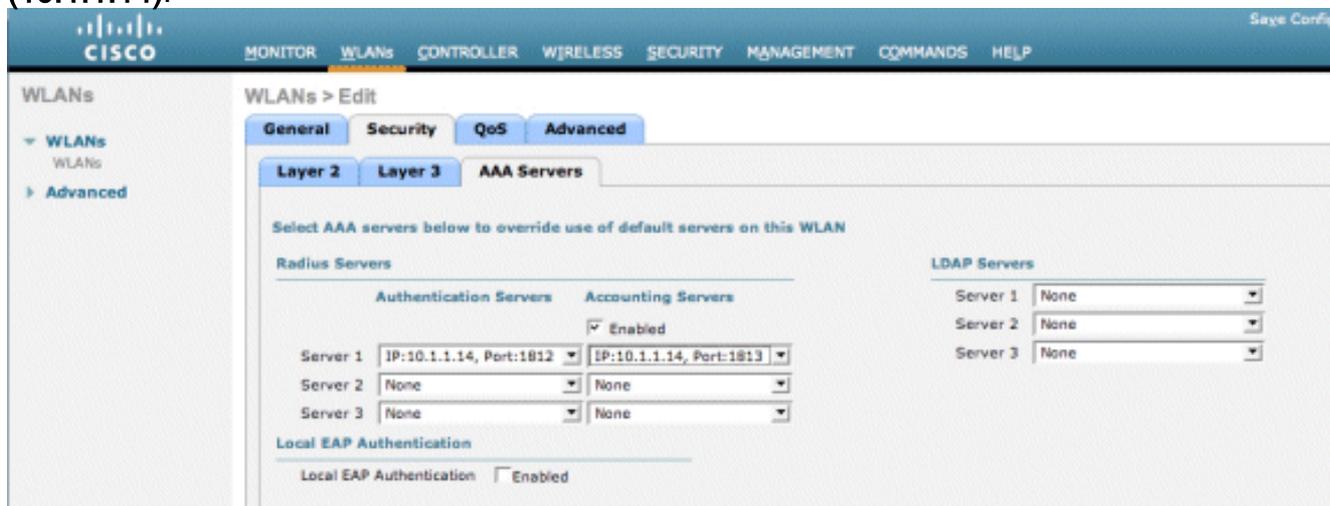
Escolha **Aplicar**.



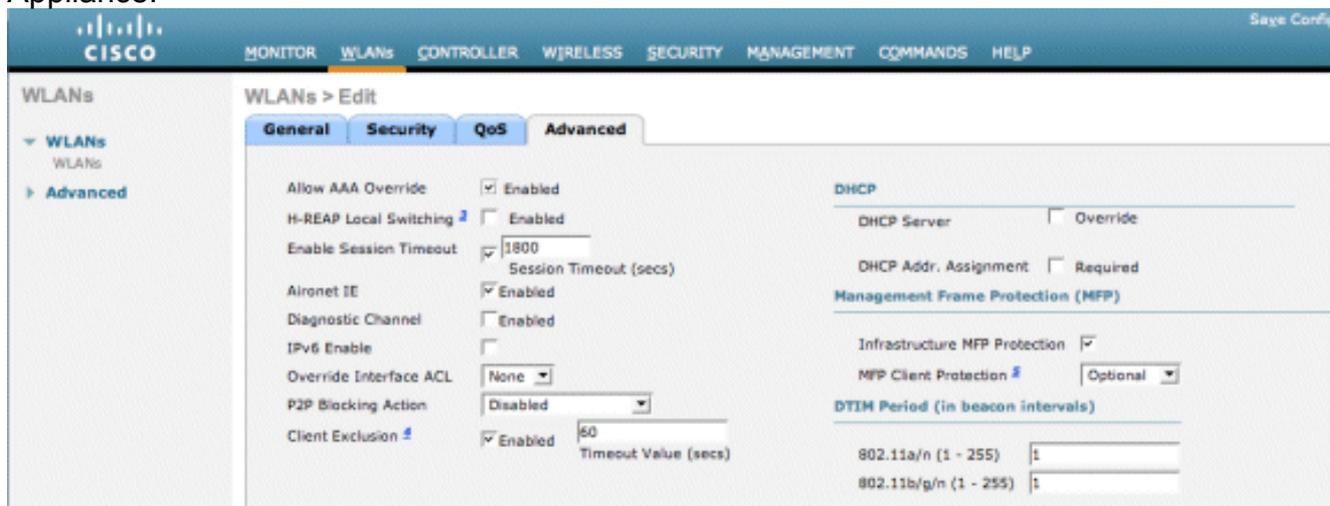
3. Modifique a WLAN (wireless-x) para usar o NAC Guest Server. Edite a WLAN (wireless-x). Escolha a guia **Segurança**. Altere a segurança da camada 2 para **None** e a segurança da camada 3 para usar a **autenticação da Web**.



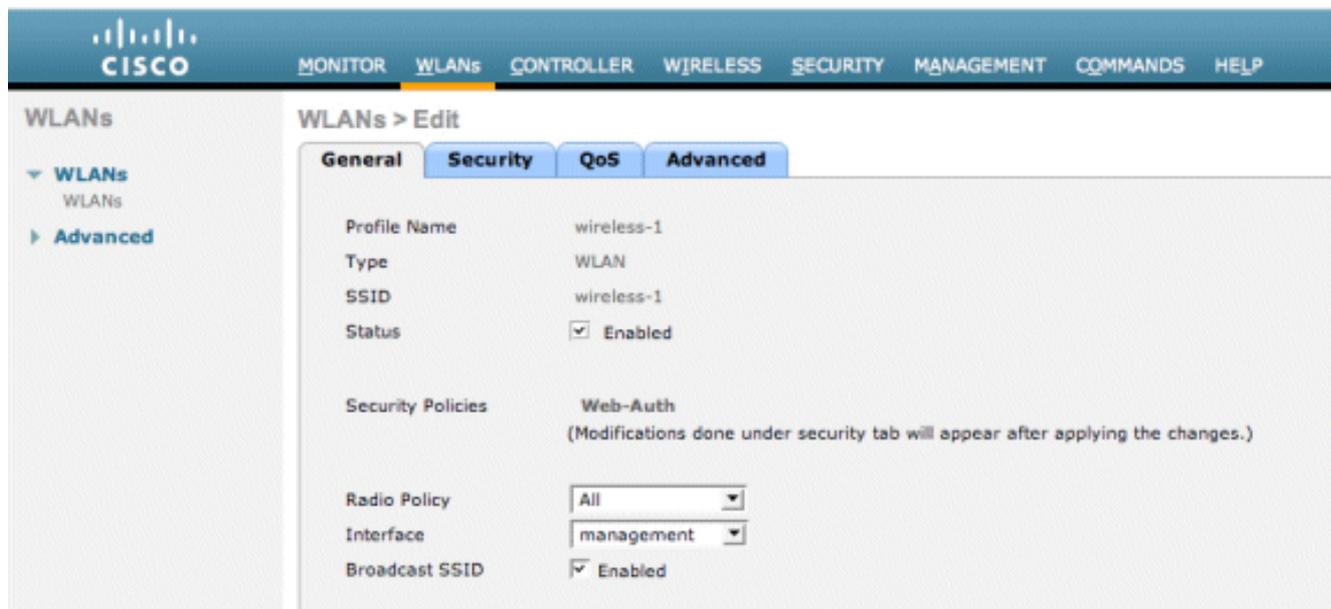
Escolha os servidores AAA na guia Security. Na caixa Server 1 (Servidor 1), escolha o servidor RADIUS (10.1.1.14). Na caixa Servidor 1, escolha o Servidor de contabilidade (10.1.1.14).



Escolha a guia Avançado. Habilite Allow AAA Override. Isso permite que o tempo limite de sessão por cliente seja definido no NAC Guest Appliance.



Observação: quando AAA override está habilitado no SSID, o tempo de vida restante do Guest User no NGS é enviado para a WLC como o tempo limite da sessão no momento do logon do usuário convidado. Escolha Apply para salvar sua configuração de WLAN.



4. Verifique se a controladora foi adicionada como um cliente Radius no servidor convidado do Cisco NAC. Navegue até o NAC Guest Server (<https://10.1.1.14/admin>) para fazer essa configuração. **Observação:** você obtém a página Administração se especificar o /admin no URL.



Selecione **Radius Clients**. Escolha **Add Radius**. Insira as informações do Radius Client: Insira um nome: nome do sistema WLC. Insira o endereço IP: IP address of WLC (10.10.51.2). Insira o mesmo segredo compartilhado que você inseriu na Etapa 1. Confirme seu segredo compartilhado. Insira uma descrição. Escolha **Add Radius Client**.



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

Reinicie o Radius Service para que as alterações tenham efeito. Selecione **Radius Clients**. Escolha **Restart** na caixa 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. Crie um usuário local, ou seja, Lobby Ambassador, no servidor convidado do Cisco NAC. Escolha **Usuários locais**. Escolha **Add User**. **Observação:** você deve preencher todos os campos. Insira um Nome: **lobby**. Insira um Sobrenome: **Embaixador**. Digite Nome de usuário: **lobby**. Insira uma senha: **password**. Deixar Grupo como **Padrão**. Insira o endereço de e-mail: **lobby@xyz.com**. Escolha **Add User**.



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. Faça login como o usuário local e crie uma conta de convidado. Navegue até o NAC Guest Server (<https://10.1.1.14>), efetue login com o nome de usuário/senha que você criou na Etapa 5 e configure isso:



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](#)

Escolha **Criar** para uma conta de usuário convidado. **Observação:** você deve preencher todos os campos. Insira um nome. Digite um sobrenome. Informe a Empresa. Digite o endereço de e-mail. **Observação:** o endereço de e-mail é o nome de usuário. Informe o Fim da Conta: **Hora**. Escolha **Add User**.



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. Conecte-se à WLAN de convidado e faça login como o usuário convidado. Conecte seu cliente sem fio à WLAN de convidado (wireless-x). Abra o navegador da Web para ser redirecionado à página de login de autenticação da Web. **Observação:** como alternativa, digite <https://1.1.1.1/login.html> para ser redirecionado à página Login. Digite o Nome de usuário convidado que você criou na Etapa 6. Insira a senha que foi gerada automaticamente na etapa 6. Faça Telnet para o WLC e verifique se o Session Timeout foi definido com o comando **show client detail**. Quando o tempo limite da sessão expira, o cliente convidado é desconectado e o ping é interrompido.

```
(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..... 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) >
```

Observação: para configurar a autenticação da Web a partir do Wireless LAN Controller, WLC para o NAC Guest Server (NGS), você precisa usar a autenticação do modo PAP nas propriedades de autenticação da Web. Se a política de autenticação da Web estiver definida

como CHAP, a autenticação falhará porque não há suporte para CHAP com NGS.

Informações Relacionadas

- [Cisco NAC Appliance - Guia de Instalação e Configuração do Clean Access Manager, Versão 4.1\(3\)](#)
- [Suporte ao switch do dispositivo Cisco NAC e ao controlador de LAN sem fio](#)
- [Guia de configuração do Cisco Wireless LAN Controller Release 7.0.116.0](#)
- [\(Vídeo\) Integração do Cisco Identity Services Engine \(ISE\) com o Wireless LAN Controller \(WLC\)](#)
- [NAC \(Clean Access\): configurar acesso de convidado](#)
- [Guia de implantação: Cisco Guest Access usando o Cisco Wireless LAN Controller, versão 4.1](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.