# Exemplo de configuração da autenticação da Web do controlador do Wireless LAN

## Índice



## Introdução

Este documento explica como Cisco executa a autenticação da Web e mostra como configurar um controlador do Wireless LAN do Cisco 4400 Series (WLAN) (WLC) para apoiar uma autenticação do web interna.

## Pré-requisitos

### Requisitos

O documento supõe que você já possui uma configuração inicial na WLC 4400.

### Componentes Utilizados

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

- Um 4400 Series WLC que execute a versão 7.0.116.0
- A versão 4.2 do Serviço de controle de acesso Cisco Secure (ACS) instalou em um server de Microsoft® Windows 2003
- Access point do peso leve da série do Cisco Aironet 1131AG
- Adaptador Wireless de CardBus do a/b/g do 802.11 do Cisco Aironet que executa a versão 4.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Autenticação da Web

A autenticação da Web é uns recursos de segurança da camada 3 que façam com que o controlador não permita o tráfego IP (exceto o DHCP e o DNS - pacotes relacionados) de um cliente específico até que esse cliente forneça corretamente um nome de usuário válido e uma senha. É um método de autenticação simples sem a necessidade para um suplicante ou um utilitário de cliente. A autenticação da Web é usada tipicamente por clientes que desejam implantar uma rede com acesso de convidados. As implementações típicas podem incluir locais de "hot spot" tais como T-Mobile ou Starbucks.

Tenha em mente que a autenticação da Web não proporciona a criptografia de dados. A autenticação da Web é usada tipicamente como um acesso simples de convidado a um "hot spot" ou à atmosfera de campus, onde o único interesse é a conectividade.

A autenticação da Web pode ser utilização executada:

- Indicador do início de uma sessão do padrão no WLC
- Versão modificada do indicador do início de uma sessão do padrão no WLC
- Um indicador personalizado do início de uma sessão que você configure em um servidor de Web externo (autenticação do web externa)
- Um indicador personalizado do início de uma sessão que você transfira ao controlador

Neste documento, o controlador do Wireless LAN para a autenticação do web interna é configurado.

## Processo de autenticação da Web

Este é o que ocorre quando um usuário conecta a um WLAN configurado para a autenticação da Web:

- O usuário abre um navegador da Web e incorpora uma URL, por exemplo, http://www.cisco.com. O cliente manda um pedido DNS para que esta URL obtenha o IP para o destino. O WLC contorneia o pedido DNS ao servidor DNS e o servidor DNS responde para

trás com uma resposta DNS, que contenha o endereço IP de Um ou Mais Servidores Cisco ICM NT do destino www.cisco.com. Isto, é enviado por sua vez aos clientes Wireless.

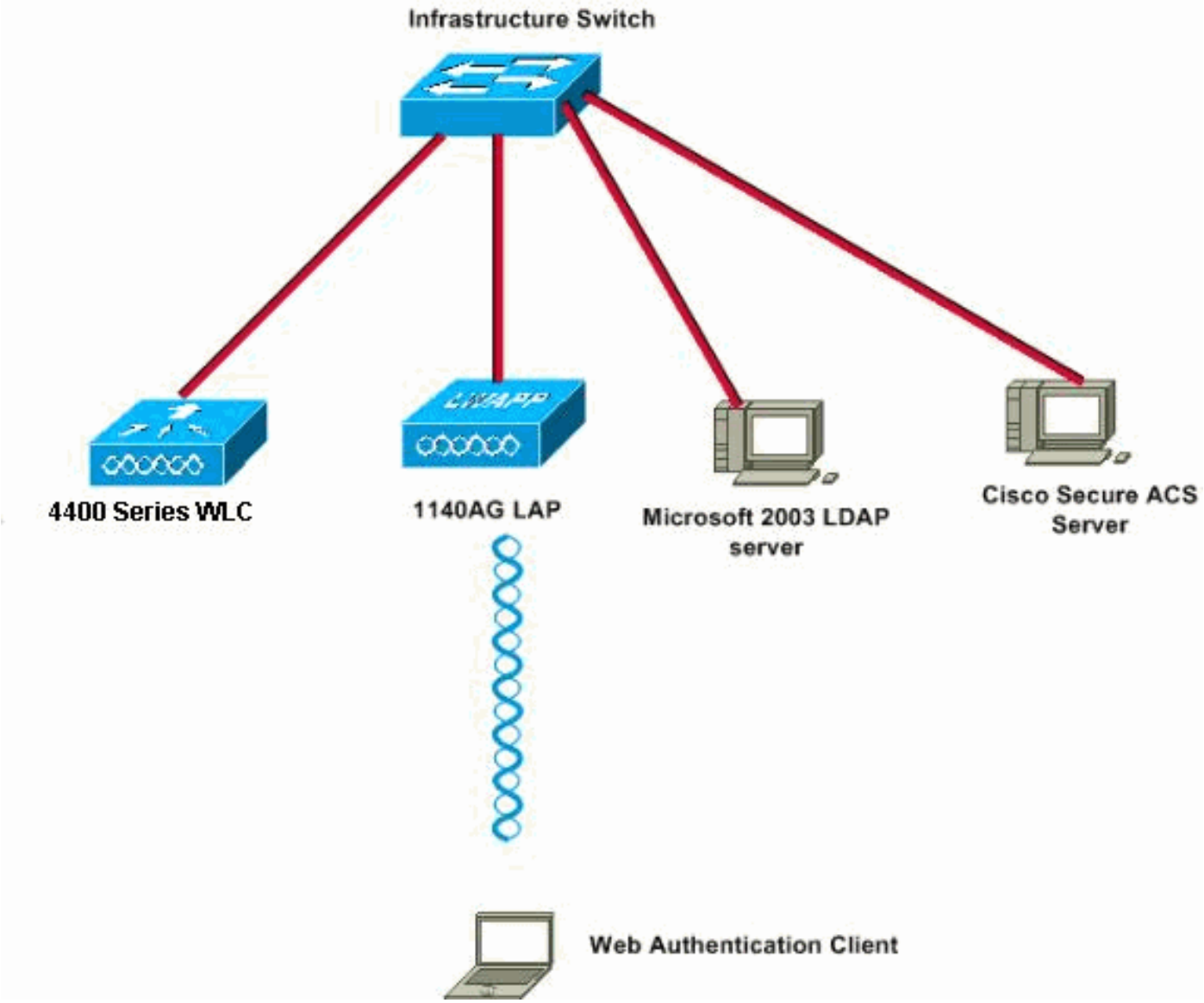
- O cliente tenta então abrir uma conexão de TCP com o endereço IP de destino. Manda um pacote SYN de TCP destinado ao endereço IP de Um ou Mais Servidores Cisco ICM NT de www.cisco.com.
- O WLC tem as regras configuradas para o cliente e daqui pode atuar como um proxy para www.cisco.com. Envia para trás um pacote TCP SYN-ACK ao cliente com fonte como o endereço IP de Um ou Mais Servidores Cisco ICM NT de www.cisco.com. O cliente envia para trás um pacote de ACK TCP a fim terminar o cumprimento de TCP de três maneiras e a conexão de TCP é estabelecida inteiramente.
- O cliente envia um pacote HTTP GET destinado a www.cisco.com. O WLC intercepta este pacote e envia-o para a manipulação da reorientação. O gateway de aplicativo HTTP prepara um corpo HTML e envia-o para trás como a resposta ao HTTP GET pedido pelo cliente. Este HTML faz o cliente ir ao Web page URL do padrão do WLC, por exemplo, http:// <Virtual-Server-IP>/login.html.
- O cliente fecha a conexão de TCP com o endereço IP de Um ou Mais Servidores Cisco ICM NT, por exemplo, www.cisco.com.
- Agora o cliente quer ir a http://1.1.1.1/login.html. Consequentemente, o cliente tenta abrir uma conexão de TCP com o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do WLC. Envia um pacote SYN de TCP para 1.1.1.1 ao WLC.
- O WLC responde para trás com um TCP SYN-ACK e o cliente envia para trás um TCP ACK ao WLC a fim terminar o aperto de mão.
- O cliente envia um HTTP GET para /login.html destinou a 1.1.1.1 a fim pedir para a página de login.
- Este pedido é permitido até o servidor de Web do WLC, e o server responde para trás com a página de login do padrão. O cliente recebe a página de login na janela de navegador onde o usuário pode ir adiante e início de uma sessão.

Está aqui um link a um vídeo na comunidade do apoio de Cisco que explica o processo de autenticação da Web:

Autenticação da Web nos controladores de LAN do Cisco Wireless (WLC)


## Instalação de rede

Este documento utiliza a seguinte configuração de rede:




# Configurar a Controladora para a Autenticação da Web

Neste documento, um WLAN é configurado para a autenticação da Web e traçado a um vlan dedicada. Estas são as etapas envolvidas para configurar um WLAN para a autenticação da Web:

- Criar uma Interface de VLAN
- Configurar o WLC para a autenticação do web interna
- Adicionar uma Instância de WLAN
- Configurar o tipo do autenticação (três maneiras de autenticar usuários na autenticação da Web)

Nesta seção, serão apresentadas as informações necessárias para a configuração da controladora para a autenticação da Web.

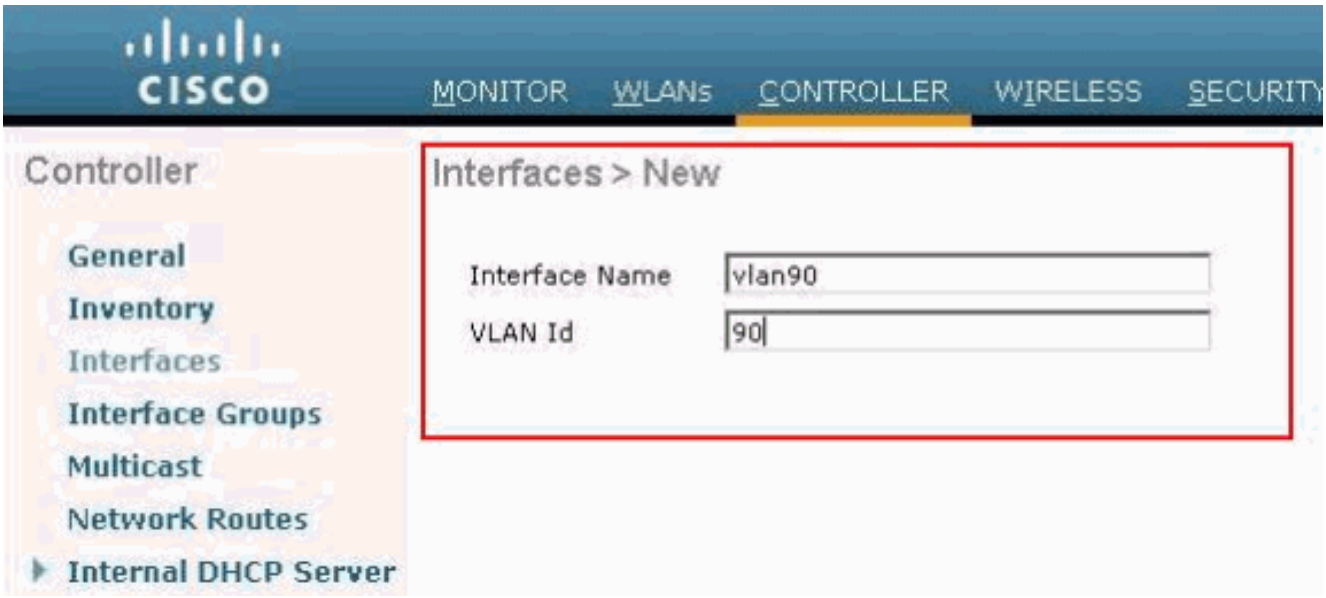
**Estes são os endereços IP usados neste documento:**

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC é 10.77.244.204.
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ACS é 10.77.244.196.

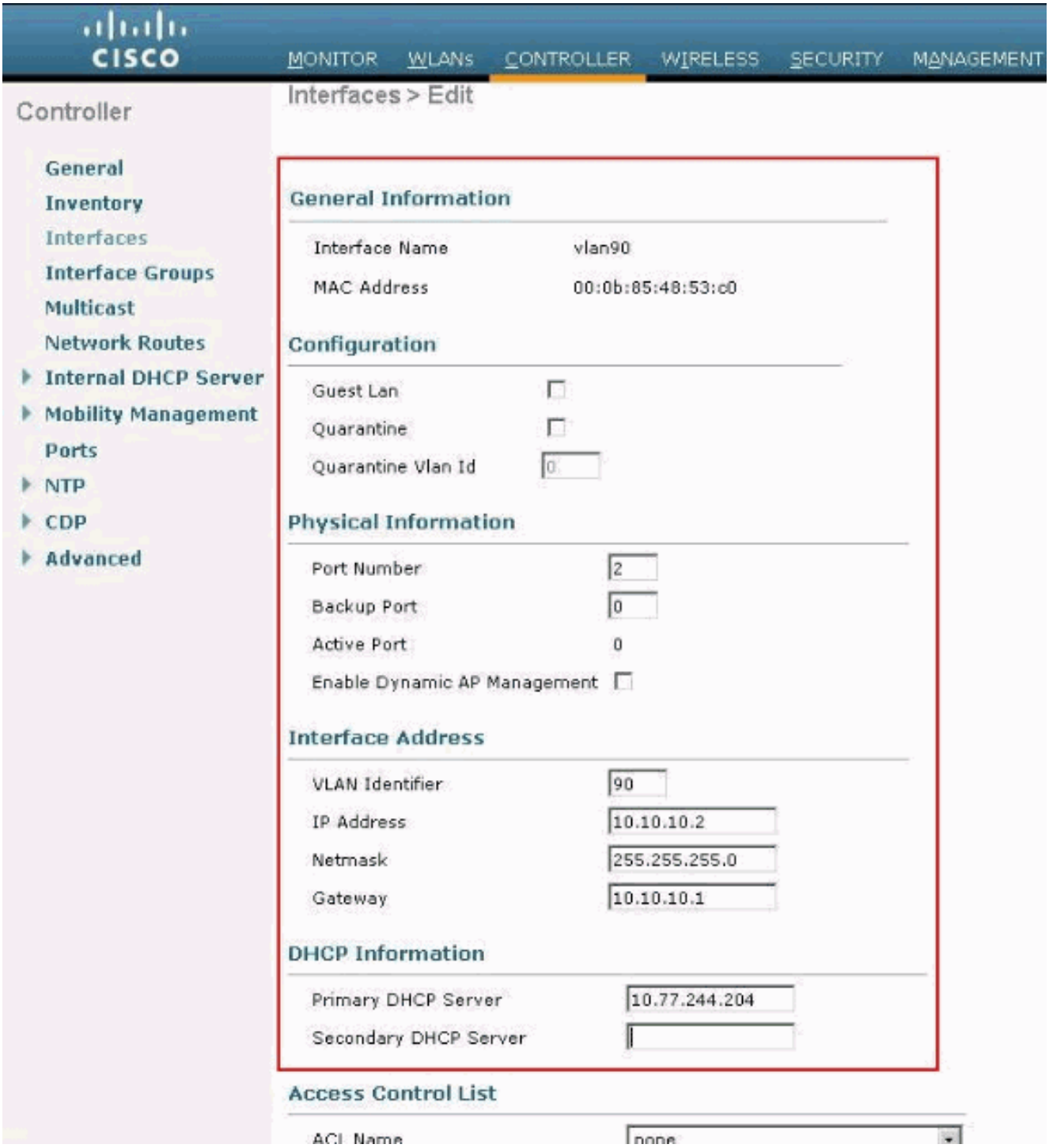
## Criar uma Interface de VLAN

Conclua estes passos:

1. Do controlador GUI do Wireless LAN, escolha o **controlador do** menu na parte superior, escolha **relações do** menu à esquerda, e clique-as **novo no** lado direito superior do indicador para criar uma interface dinâmica nova.**As relações > a nova janela** aparecem. Este exemplo usa o nome de interface *vlan90* com ID de VLAN *90*:




2. Cique em **Apply** para criar a interface de VLAN.**As relações > editam o** indicador aparecem que pede que você encha a informação do específico da relação.
3. Este documento usa estes parâmetros:Endereço IP — 10.10.10.2Máscara de rede — 255.255.255.0 (24 bits)Gateway — 10.10.10.1Número da porta — 2Servidor DHCP primário — 10.77.244.204**Note**: Este parâmetro deve ser o endereço IP do seu servidor DHCP ou RADIUS. Neste exemplo, o endereço de gerenciamento da WLC é usado como o servidor DHCP porque o escopo de DHCP interno é configurado na WLC.Servidor DHCP secundário — 0.0.0.0**Note**: O exemplo não possui um servidor DHCP secundário. Assim, use 0.0.0.0. Se sua configuração possuir um servidor DHCP secundário, adicione o endereço IP do servidor neste campo.Nome da ACL —
   Nenhum



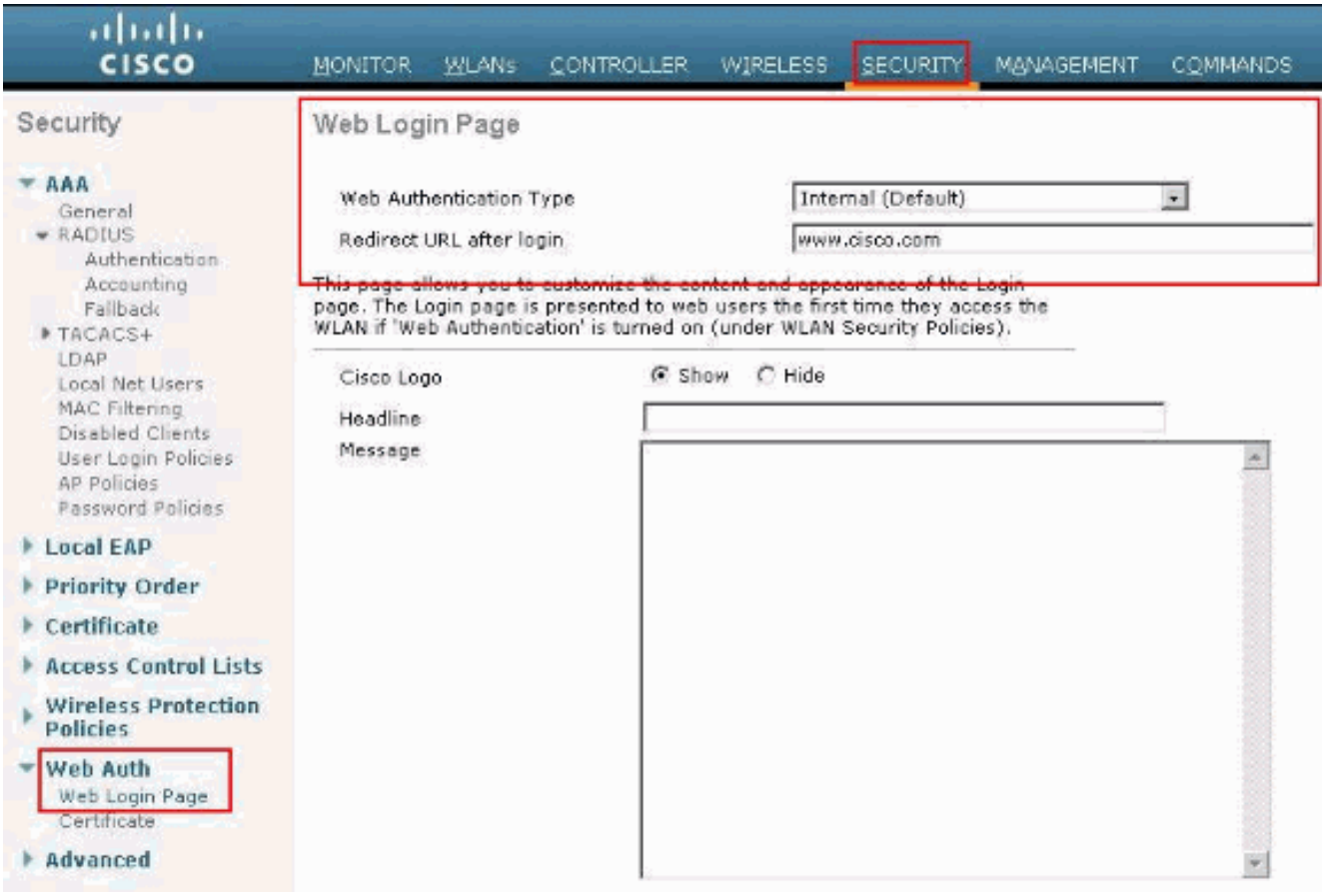

4. Clique em **Apply** para salvar as alterações.

## Configurar o WLC para a autenticação do web interna

A próxima etapa é configurar o WLC para a autenticação do web interna. A autenticação do web interna é o tipo do autenticação do web padrão em WLC. Se este parâmetro não foi mudado, nenhuma configuração está exigida para permitir a autenticação do web interna. Se o parâmetro da autenticação da Web foi mudado previamente, termine estas etapas para configurar o WLC para a autenticação do web interna:

1. Do controlador GUI, escolha o **AUTH da Segurança** > da **Web** > a **página de login da Web** a fim alcançar a página de login da Web.
2. Da autenticação da Web datilografe a caixa suspensa, escolhem a **autenticação do web interna**.

3. **Na reorientação URL depois que o** campo do **início de uma sessão**, incorpora a URL da página a que o utilizador final estará reorientado após à autenticação bem sucedida.



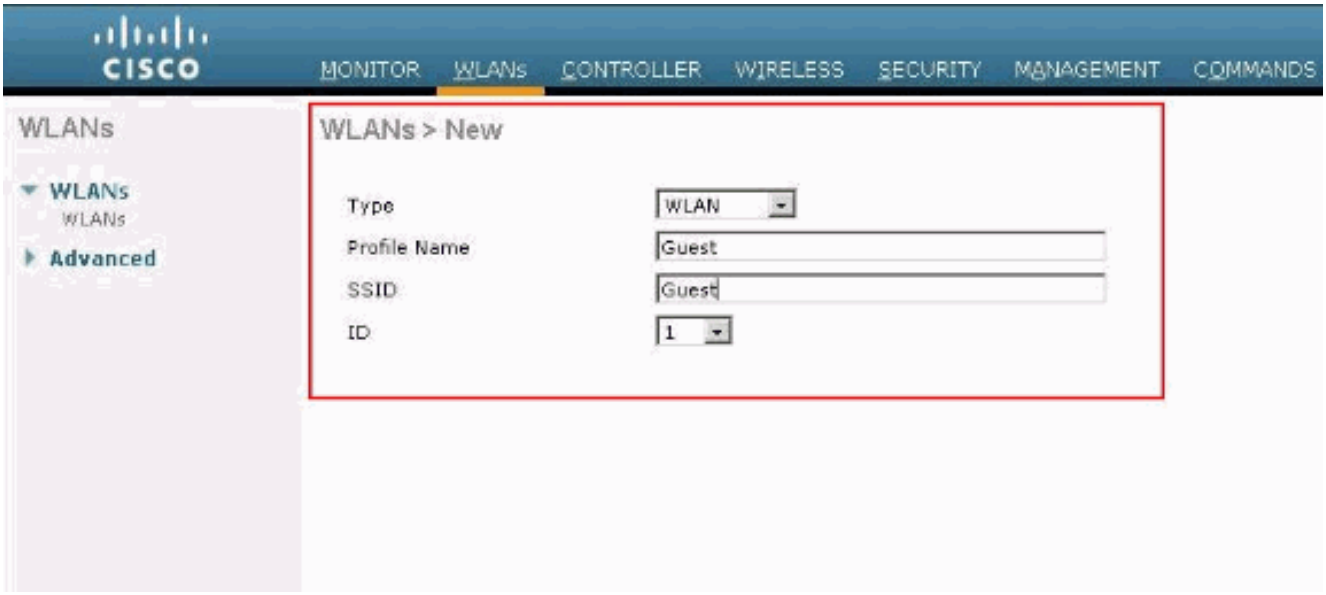

**Note**: Em versões 5.0 e mais recente WLC, a página da saída para a autenticação da Web pode igualmente ser personalizada. Refira as páginas do início de uma sessão, da falha no login e da saída da atribuição pela seção WLAN da *configuração de controle Guide,5.2 do Wireless LAN* para obter mais informações sobre de como configurar-la.

## Adicionar uma Instância de WLAN

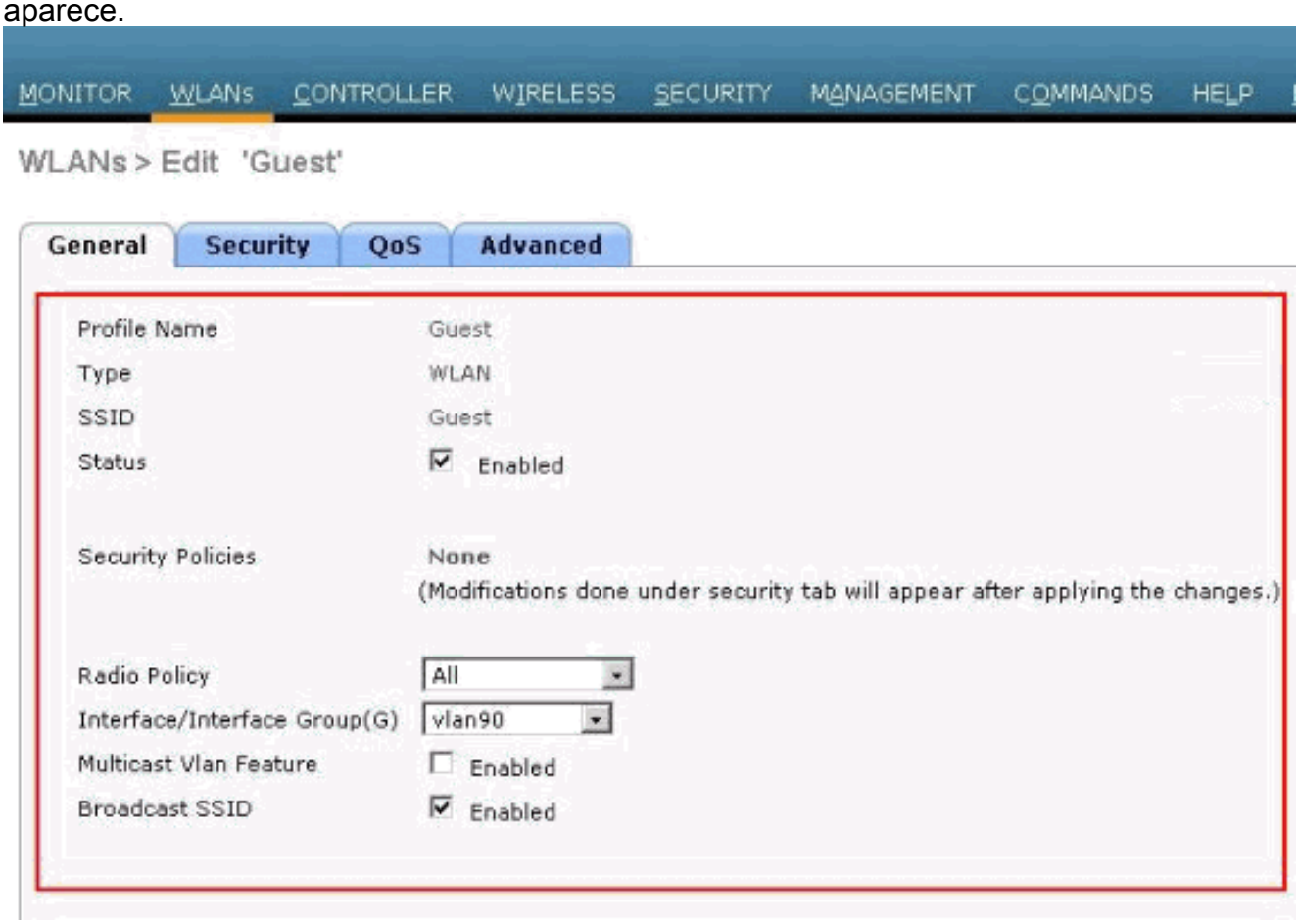
Agora que a autenticação do web interna foi permitida e há uma interface de VLAN dedicada para a autenticação da Web, você deve fornecer um WLAN/SSID novo a fim apoiar os usuários da autenticação da Web.

Conclua estes passos para criar um WLAN/SSID:

1. Do WLC GUI, clique o **WLAN no** menu na parte superior, e clique **novo no** lado direito superior.Escolha **WLAN** na opção Type. Escolha um nome de perfil e um SSID de WLAN para a autenticação da Web. Este exemplo usa o **Guest** para o nome de perfil e o SSID da WLAN.

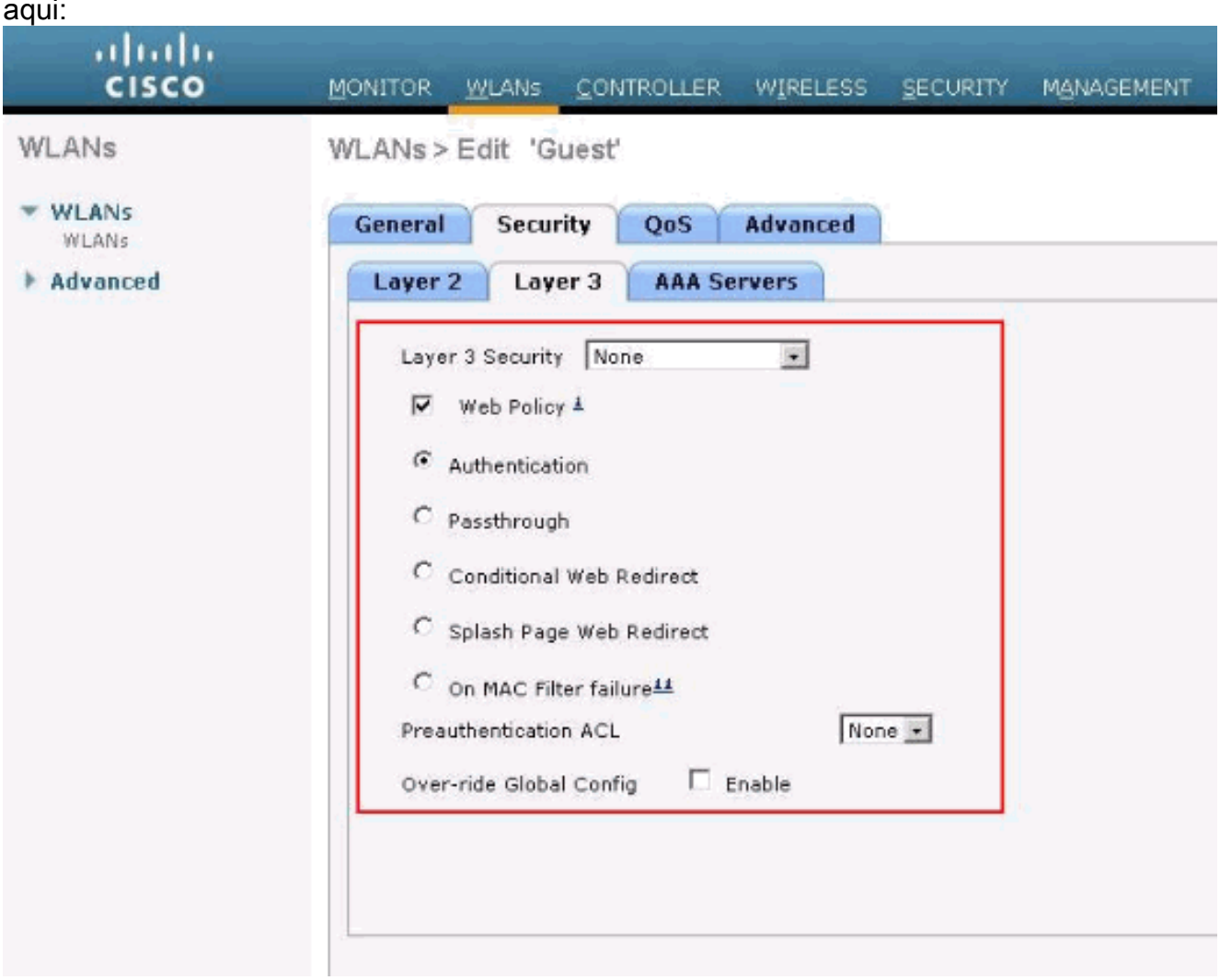



2. Clique em Apply.Um novo WLAN > edita o indicador aparece.




3. Marque a caixa de status da WLAN para habilitar a WLAN. No menu Interface, selecione o nome da interface de VLAN que você criou anteriormente. Neste exemplo, o nome da interface é *vlan90*.**Note**: Mantenha o valor padrão para os outros parâmetros nesta tela.
4. Clique na guia Security.Conclua estes passos para configurar a autenticação da Web:Clique na guia Layer 2 e defina a segurança como ***None***.**Note**: Você não pode configurar a passagem da Web como segurança da Camada 3 com 802.1x ou WPA/WPA2 como segurança da Camada 2 para uma WLAN. Consulte a Matriz de Compatibilidade da Segurança da Camada 3 e da Camada 2 da Controladora Wireless LAN para obter mais informações sobre a compatibilidade com a segurança da camada 2 e da camada 3 da controladora Wireless LAN.Clique na guia Layer 3. Verifique a caixa da **política da Web** e

escolha a ***opção de autenticação***, como mostrado aqui:




Clique em Apply para salvar a WLAN.Você voltará para a janela de resumo da WLAN. Certifique-se de que a opção Web-Auth esteja habilitada sob a coluna Security Policies da tabela WLAN para o SSID convidado.

## Três maneiras de autenticar usuários na autenticação da Web

Há três maneiras de autenticar usuários quando você usa a autenticação da Web. A autenticação local permite que você autentique o usuário na Cisco WLC. Você pode igualmente usar um servidor de raio externo ou um servidor ldap como um base de dados backend a fim autenticar os usuários.

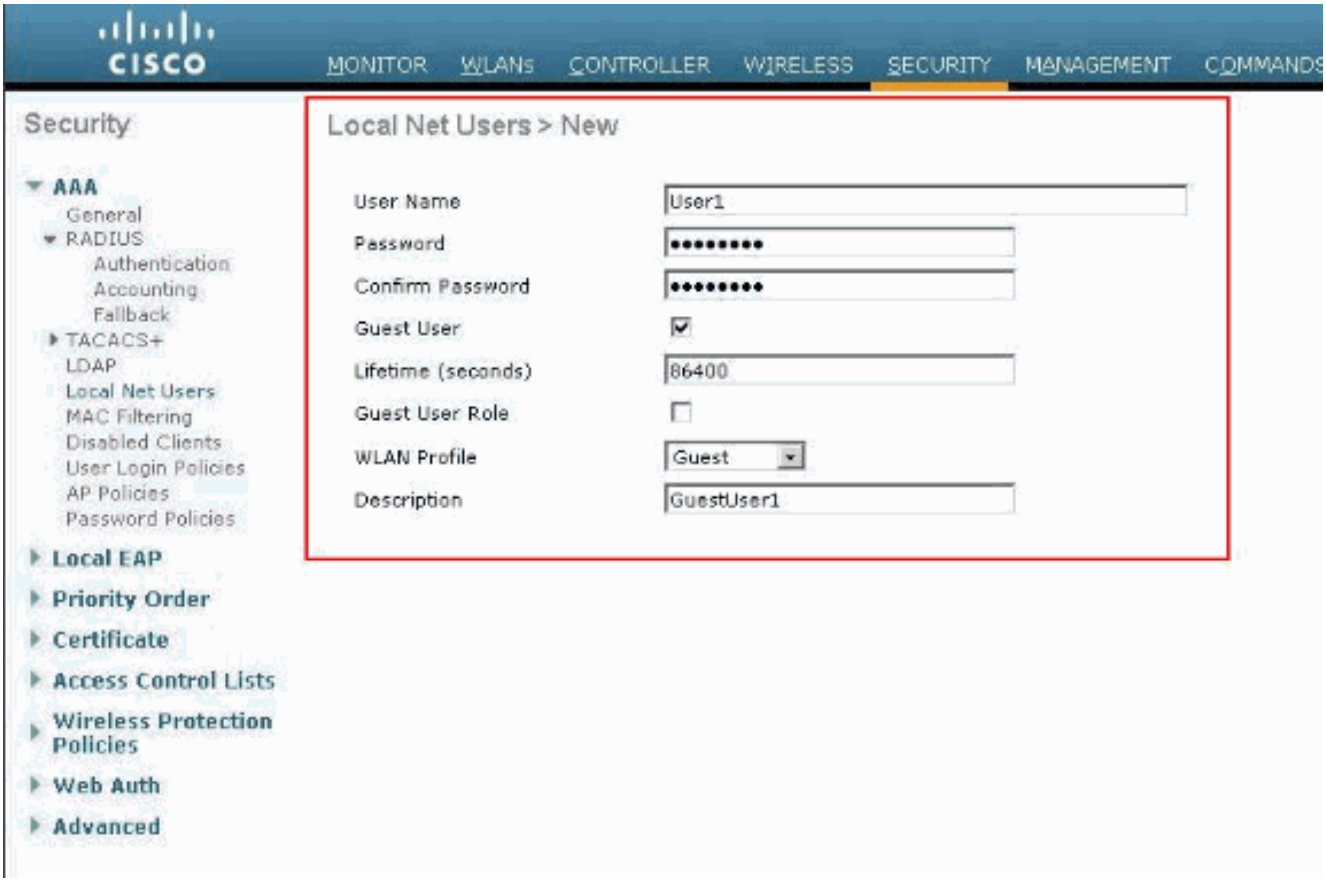
Este documento fornece um exemplo de configuração para todos os três métodos.

### Autenticação Local

A base de dados de usuário para os usuários convidado é armazenada no base de dados local do WLC. Os usuários são autenticados pelo WLC contra este base de dados.

1. Do WLC GUI, escolha a **Segurança**.
2. Clique **usuários líquidos locais do** menu AAA à esquerda.


3. Clique **novo** a fim criar um novo usuário.Indicadores de uma nova janela que pede a informação do nome de usuário e senha.
4. Incorpore um nome de usuário e uma senha a fim criar um novo usuário, a seguir confirme a senha que você quer usar.Este exemplo cria o usuário nomeado **Usuário1**.
5. Adicione uma descrição, se desejar.Este exemplo usa o **usuário1 do convidado**.
6. Clique em **Apply** para salvar a configuração do novo usuário.




7. Repita etapas 3-6 para adicionar mais usuários ao base de dados.

## Servidor RADIUS para a Autenticação da Web

Este original usa um ACS wireless no Windows 2003 Server como o servidor RADIUS. Você pode usar qualquer servidor RADIUS disponível implantado em sua rede.

**Note**: O ACS pode ser configurado no Windows NT ou no Windows 2000 Server. Para baixar o ACS de Cisco.com, consulte o Centro de Software (Downloads) - Software Seguro da Cisco (somente clientes registrados). Você precisa uma conta da Web da Cisco para baixar o software.

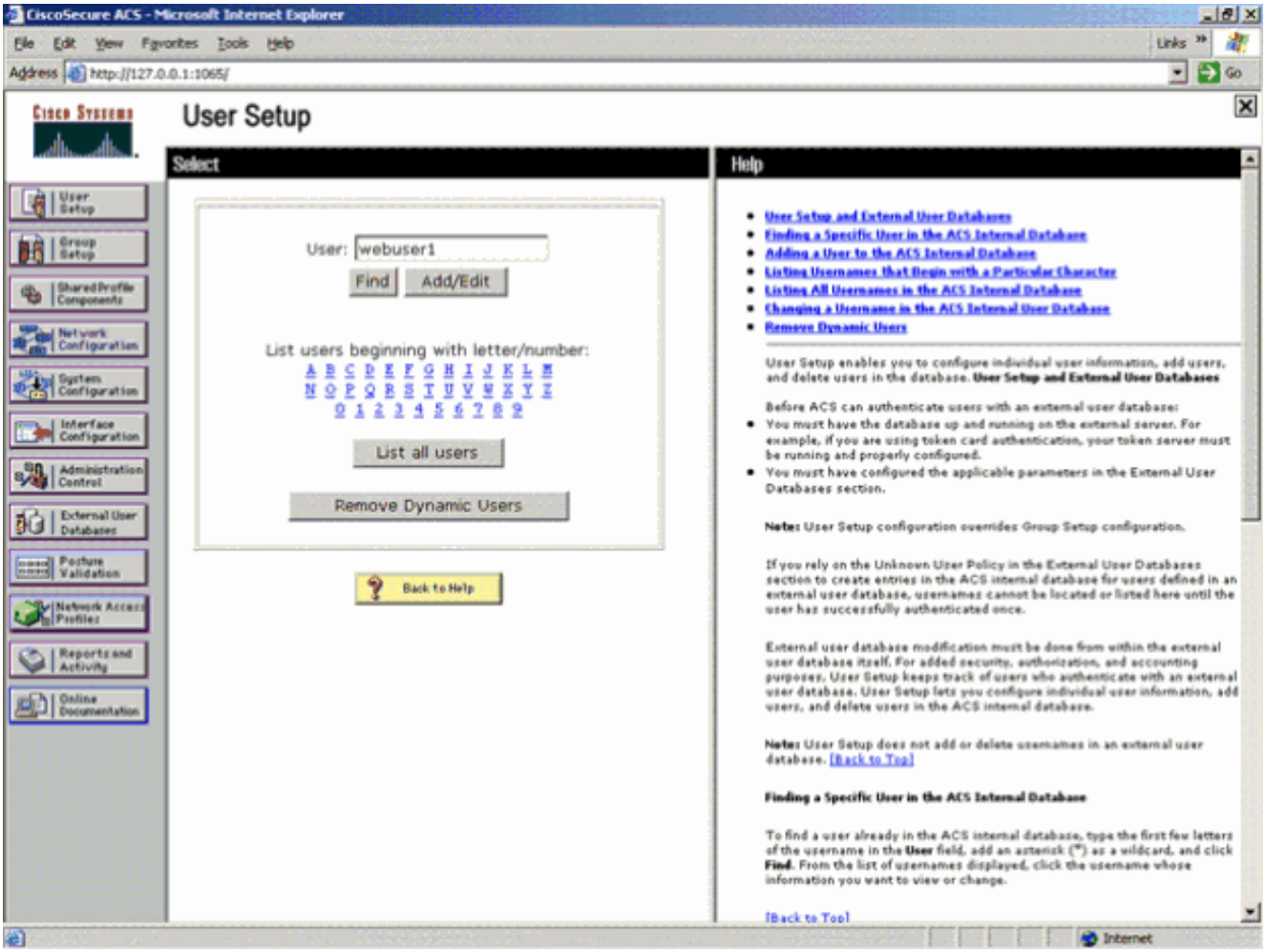
A seção Configuração do ACS mostra como configurar o ACS para o RADIUS. Você deve ter uma rede completamente funcional com um Domain Name System (DNS) e um servidor RADIUS.

## Configuração do ACS

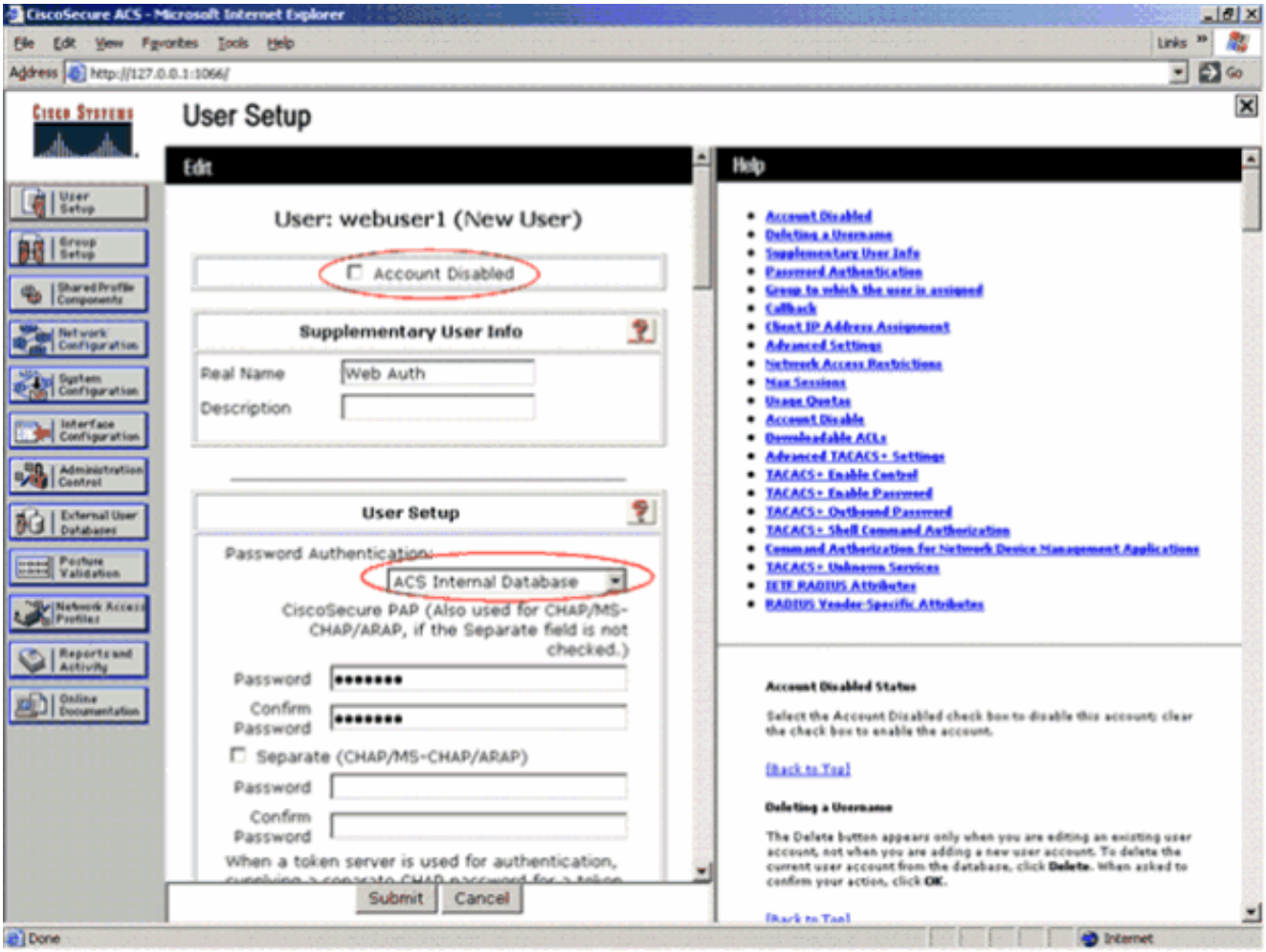
Esta seção apresenta as informações necessárias para configurar o ACS para o RADIUS.

O ACS estabelecido em seu server e termina então estas etapas a fim criar um usuário para a autenticação:

1. Quando o ACS perguntar se você quer abrir o ACS em uma janela de navegador para configurá-lo, clique em **Yes**.**Note**: Após você configurar o ACS, um ícone será colocado em sua área de trabalho.
2. No menu à esquerda, clique em **User Setup**.Esta ação toma-o à tela de instalação de usuário como mostrado
   aqui:




3. Insira o usuário que você deseja usar para a autenticação da Web e clique em **Add/Edit**.Depois que o usuário é criado, um segundo indicador abre como mostrado aqui:

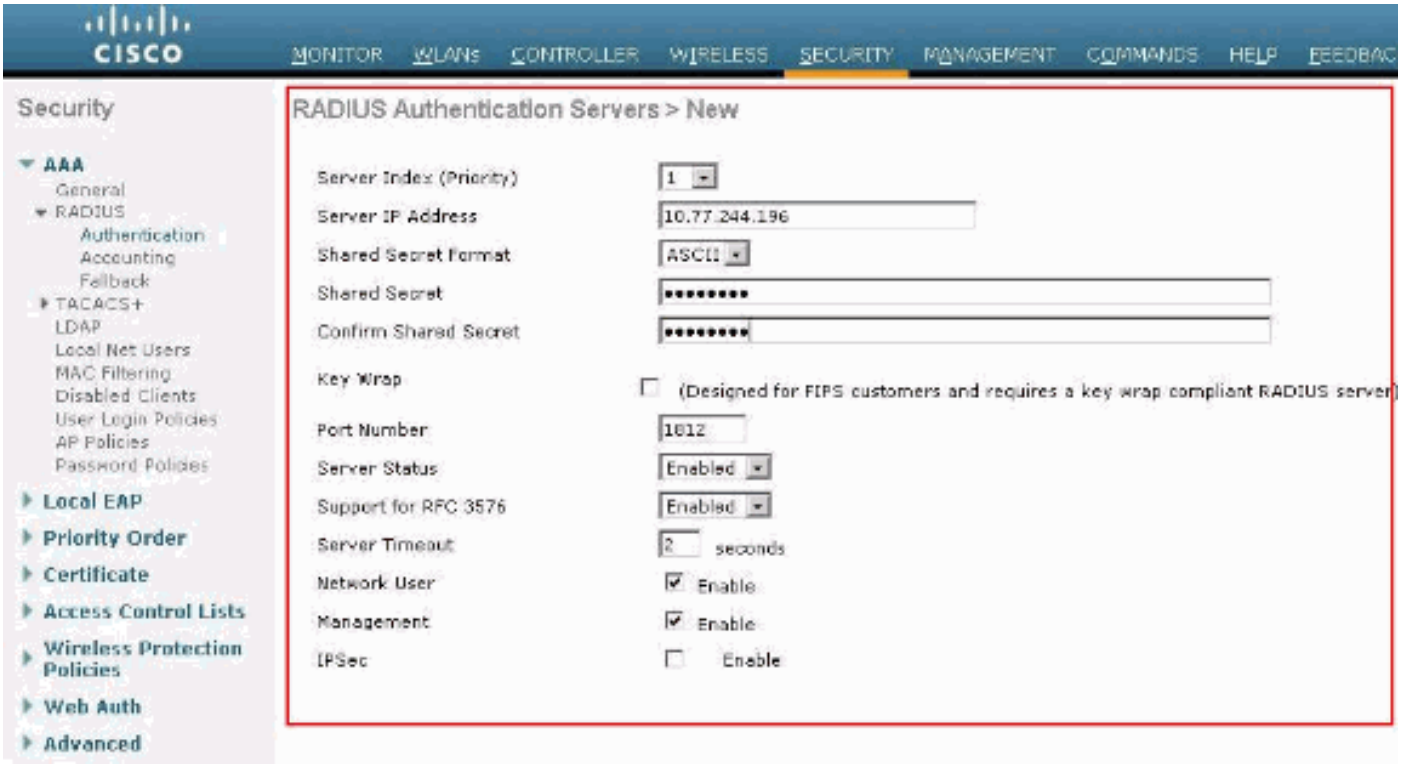



4. Assegure-se de que a caixa **desabilitada conta na** parte superior não esteja verificada.
5. Escolha o **base de dados interno ACS** para a opção da autenticação de senha.
6. Incorpore a senha. O Admin tem uma opção para configurar a autenticação PAP/CHAP ou de MD5-CHAP ao adicionar um usuário no base de dados interno ACS. O PAP é o tipo da autenticação padrão para usuários do Web-AUTH em controladores. O Admin tem a flexibilidade mudar o método de autenticação a chap/md5-chap usando este comando CLI:
   `config custom-web radiusauth <auth method>`
7. Clique em Submit.

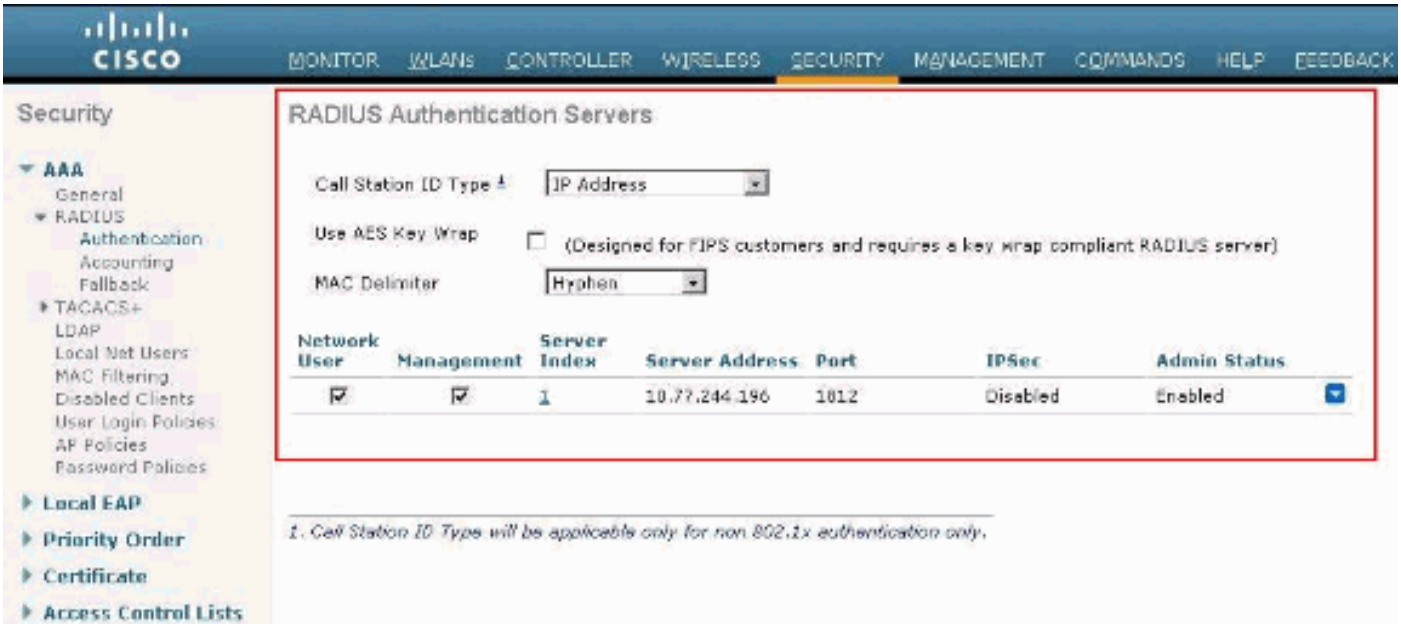
## Insira sua informações de servidor RADIUS na Cisco WLC

Conclua estes passos:

1. Clique em **Security** no menu da parte superior.
2. Clique em **Radius Authentication no** menu à esquerda.
3. Clique em **New** e insira o endereço IP do seu servidor ACS/RADIUS. Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ACS é **10.77.244.196**.
4. Insira o segredo compartilhado para o servidor Radius. Certifique-se de que esta chave secreta é a mesma que essa você entrou no servidor Radius para o WLC.
5. Mantenha o número da porta no valor padrão, 1812.
6. Certifique-se de que a opção **Server Status** esteja habilitada.
7. Verifique o **usuário de rede permitem a** caixa de modo que este servidor Radius seja usado para usuários de autenticação de sua rede Wireless.
8. Clique em Apply.



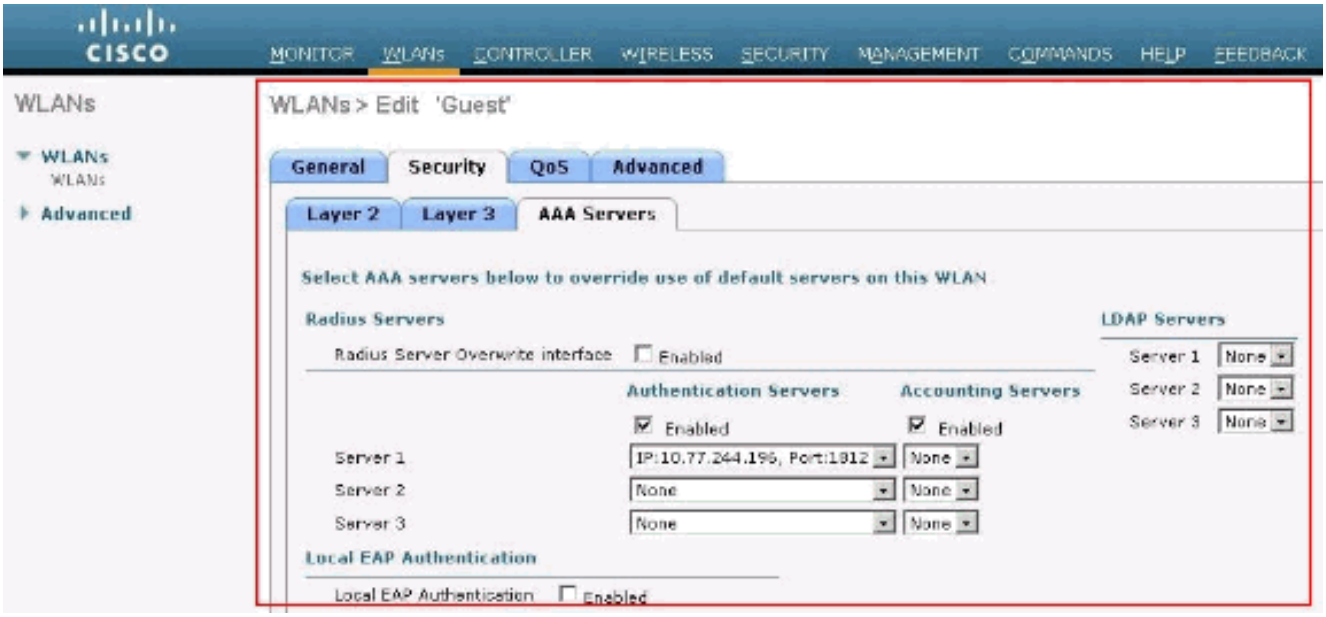

Certifique-se de que a caixa do *usuário de rede* está verificada e *status administrativo* é permitido.




## Configuração da WLAN com o Servidor RADIUS

Agora que o servidor RADIUS está configurado na WLC, você precisa configurar a WLAN para usar este servidor RADIUS para a autenticação da Web. Conclua estes passos para configurar a WLAN com o servidor RADIUS.

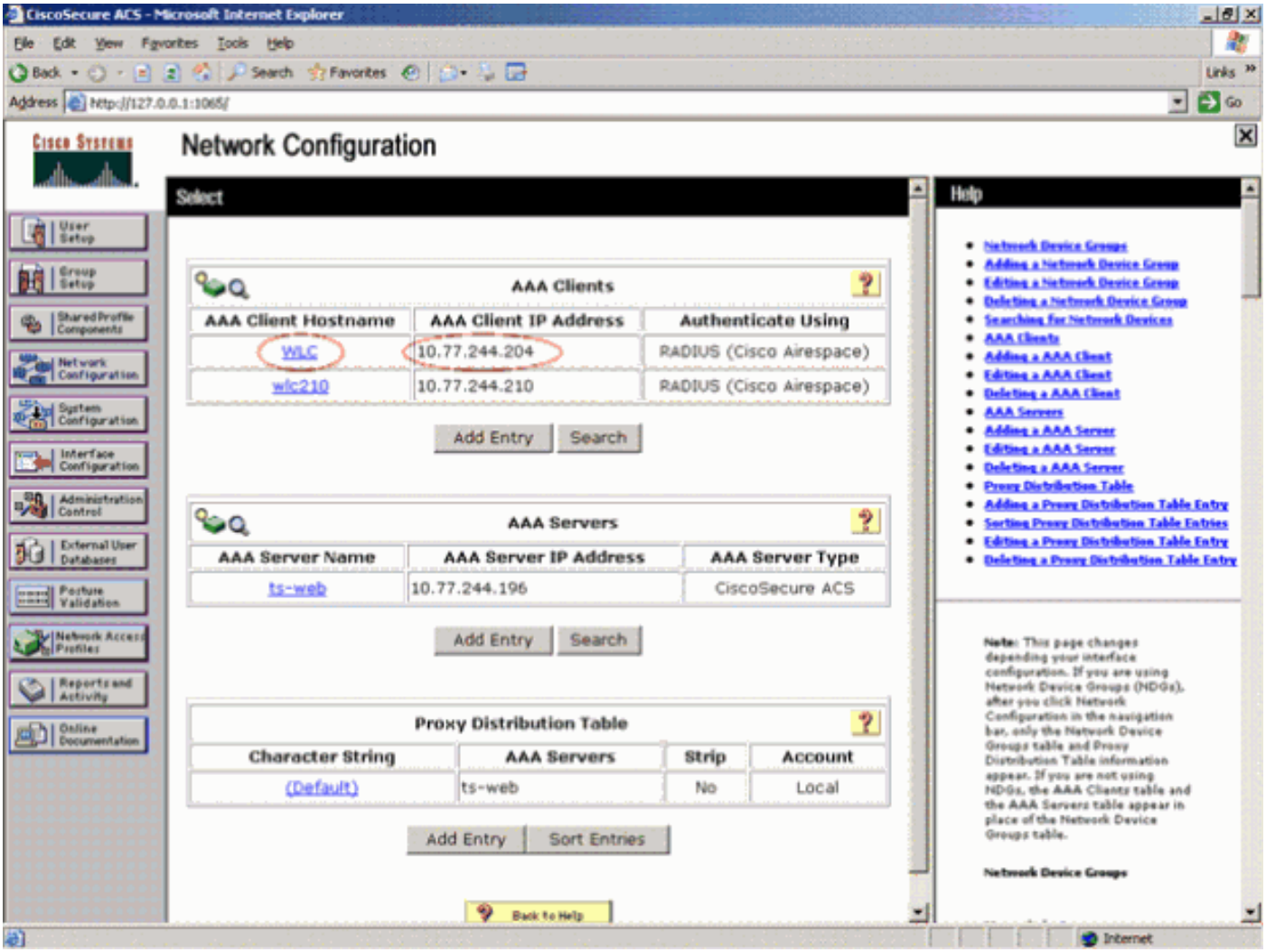
1. Abra seu navegador WLC e clique em **WLANs**. Isto indica a lista de WLAN configurados no WLC. Clique o **convidado** WLAN que foi criado para a autenticação da Web.
2. No os **WLAN > editam o** clique da página o **menu Segurança**. Clique a aba dos **servidores AAA** sob a Segurança. Então, escolha o servidor Radius que é 10.77.244.196 neste exemplo:



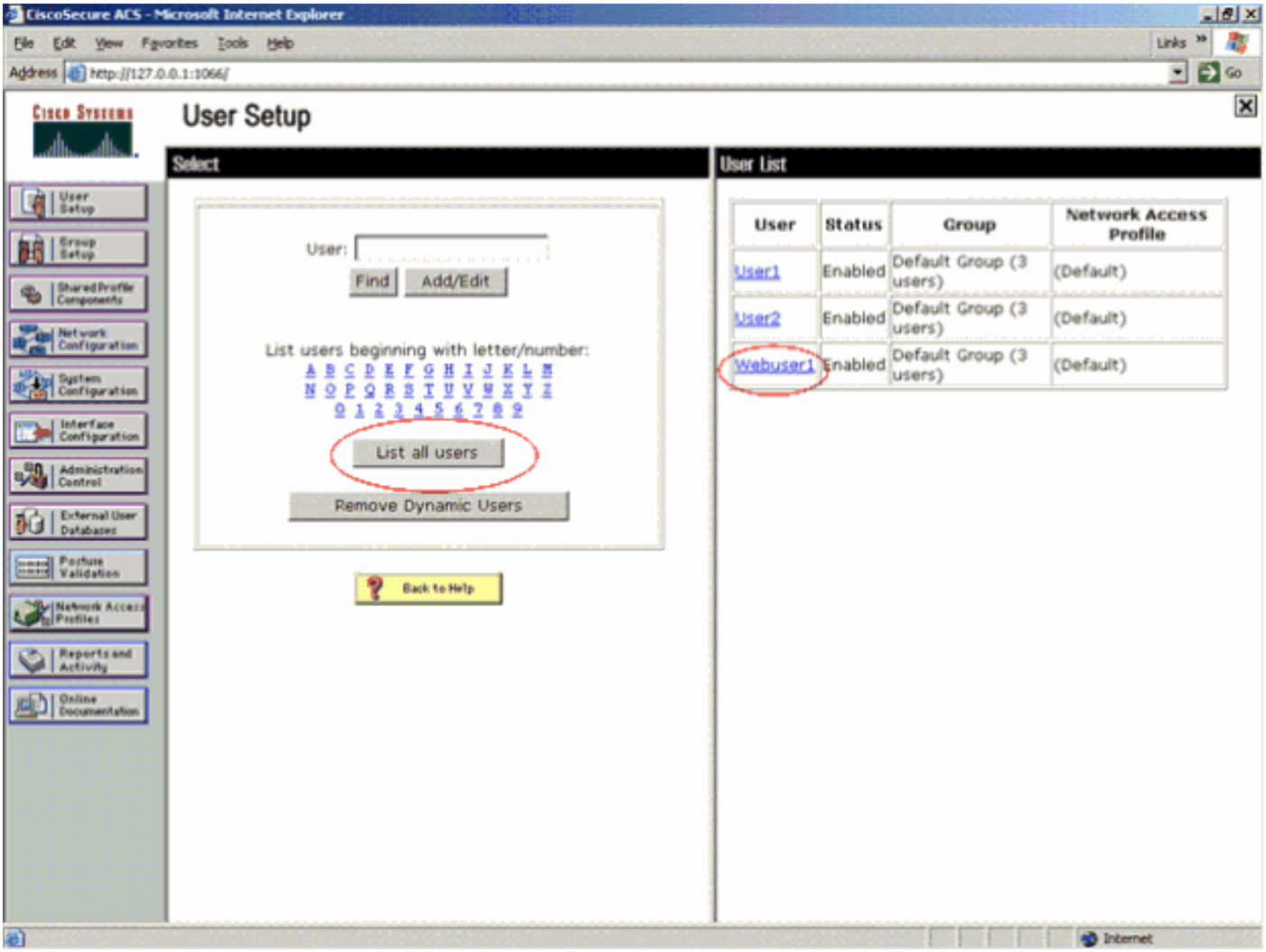

3. Clique em Apply.

## Verificar o ACS

Quando você estabelece o ACS, recorde transferir todas as correções de programa atuais e código o mais atrasado. Isso deve resolver problemas iminentes. Caso que você está usando a autenticação RADIUS certifique-se de que seu WLC está alistado como um dos clientes de AAA. Clique o menu da **configuração de rede no** lado esquerdo para verificar isto. Clique o cliente de AAA, a seguir verifique a senha e o tipo do autenticação configurados. Consulte a seção Configuração dos Clientes AAA do Guia do Usuário do Cisco Secure Access Control Server 4.2 para obter mais informações sobre como configurar um cliente AAA.




Quando você escolhe a instalação de usuário, verifique outra vez que seus usuários existem realmente. Clique a **lista todos os usuários**. Um indicador aparece como mostrado. Certifique-se que o usuário que foi criado exista na lista.

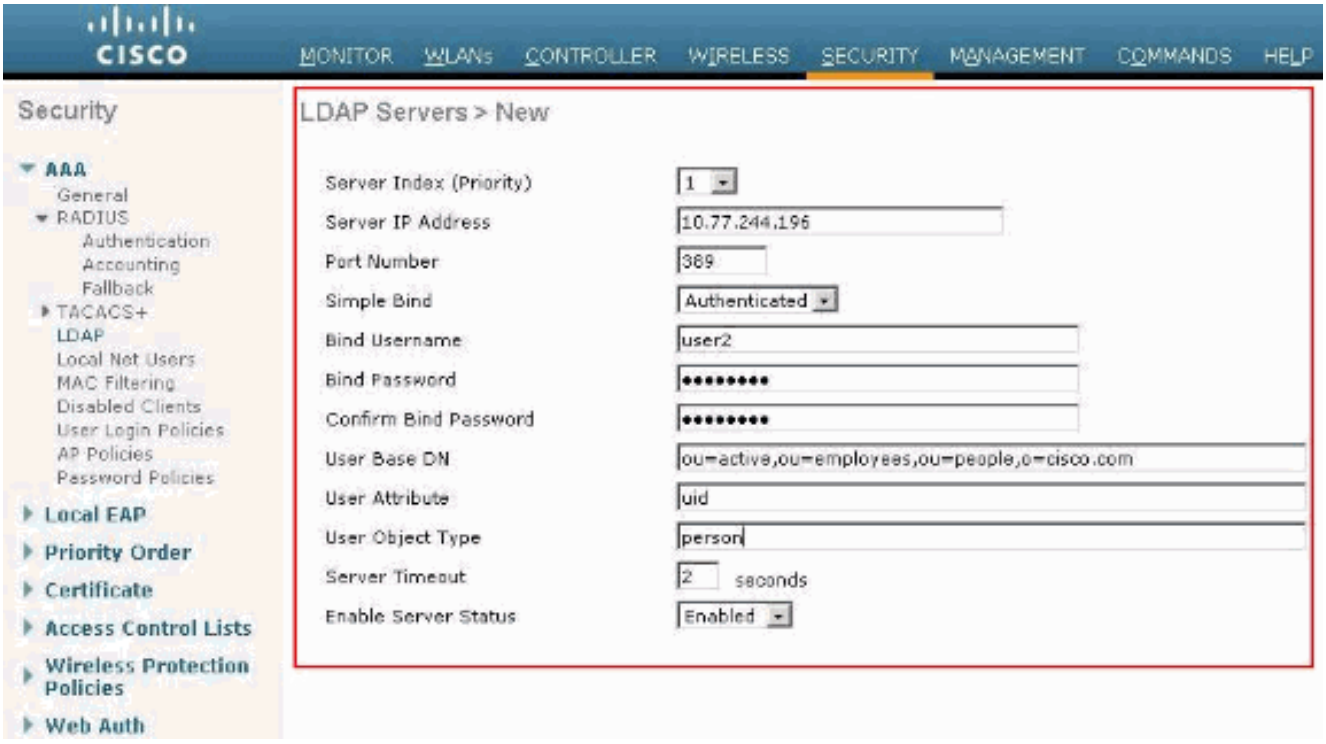



## Servidor ldap

Esta seção explica como configurar um server do Lightweight Directory Access Protocol (LDAP) como um base de dados backend, similar a um RAIO ou a uma base de dados de usuário local. Um base de dados da parte posterior LDAP permite que o controlador pergunte um servidor ldap para as credenciais (nome de usuário e senha) de um usuário particular. Estas credenciais são usadas então para autenticar o usuário.

Termine estas etapas para configurar o LDAP usando o controlador GUI:

1. Clique a **Segurança** > o **AAA** > o **LDAP** a fim abrir os servidores ldap.Esta página alista todos os servidores ldap que forem configurados já.Se você quer suprimir de um servidor ldap existente, mova seu cursor sobre a seta azul da gota-para baixo para esse server e escolha-o **removem**.Se você quer se certificar de que o controlador pode alcançar um servidor particular, paira seu cursor sobre a seta azul da gota-para baixo para esse server e escolhe o **sibilo**.
2. Execute um do seguinte:Para editar um servidor ldap existente, clique o número do índice para esse server. Os servidores ldap > editam a página aparecem.Para adicionar um servidor ldap, clique **novo**. Os servidores ldap > página nova aparecem.




3. Se você está adicionando um server novo, escolha um número da caixa suspensa do deslocamento predeterminado do server (prioridade) especificar a ordem da prioridade deste server com relação a todos os outros servidores ldap configurados. Você pode configurar até dezessete server. Se o controlador não pode alcançar o primeiro server, a seguir tenta segundo da lista e assim por diante.
4. Se você está adicionando um server novo, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ldap ao campo de endereço IP do servidor.
5. Se você está adicionando um server novo, inscreva o número de porta de TCP do servidor ldap no campo de número de porta. O intervalo válido é 1 a 65535, e o valor padrão é 389.
6. Verifique a caixa de verificação do **status de servidor da possibilidade** para permitir este servidor ldap, ou desmarcar-la para desabilitá-la. O valor padrão é desabilitado.
7. Da caixa suspensa simples do ligamento, escolha **anônimo** ou **autenticado** para especificar o método do ligamento da autenticação local para o servidor ldap. O método anônimo permite o acesso anônimo ao servidor ldap, visto que o método autenticado exige que um nome de usuário e senha esteja incorporado ao acesso seguro. O valor padrão é anônimo.
8. Se você escolheu autenticado na etapa 7, termine estas etapas:No campo de nome de usuário do ligamento, incorpore um username a ser usado para a autenticação local ao servidor ldap.Na senha do ligamento e confirme campos de senha do ligamento, incorporam uma senha a ser usada para a autenticação local ao servidor ldap.
9. No campo da base do usuário DN, dê entrada com o nome destacado (DN) do subtree no servidor ldap que contém uma lista de todos os usuários. Por exemplo, unidade do ou=organizational, unidade organizacional .ou=next, e o=corporation.com. Se a árvore que contém usuários é a base DN, datilografe o=corporation.com ou dc=corporation, dc=com.
10. No campo do atributo de usuário, dê entrada com o nome do atributo no registro de usuário que contém o username. Você pode obter este atributo de seu servidor de diretório.
11. No tipo de objeto do usuário campo, incorpore o valor do atributo do objectType LDAP que identifica o registro como um usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo do objectType, alguns de que são originais ao usuário e alguns de que são compartilhados com outros tipos de objeto.
12. No campo do timeout de servidor, incorpore o número de segundos entre retransmissões.

O intervalo válido é 2 a 30 segundos, e o valor padrão é 2 segundos.

13. O clique **aplica-se** para comprometer suas mudanças.
14. **Configuração da salvaguarda do** clique para salvar suas mudanças.
15. Termine estas etapas se você deseja atribuir servidores ldap específicos a um WLAN:Clique **WLAN** para abrir a página WLAN.Clique o número de ID do WLAN desejado.Quando os WLAN > editam a página publica-se, clica-se as abas da **Segurança** > dos **servidores AAA** para abrir WLAN > edita (Segurança > servidores AAA) a página.


Das caixas suspensas dos servidores ldap, escolha os server LDAP que você quer usar com este WLAN. Você pode escolher até três servidores ldap, que são tentados na ordem da prioridade.O clique **aplica-se** para comprometer suas mudanças.**Configuração da salvaguarda do** clique para salvar suas mudanças.

## Configurar seu cliente de WLAN para usar a autenticação da Web

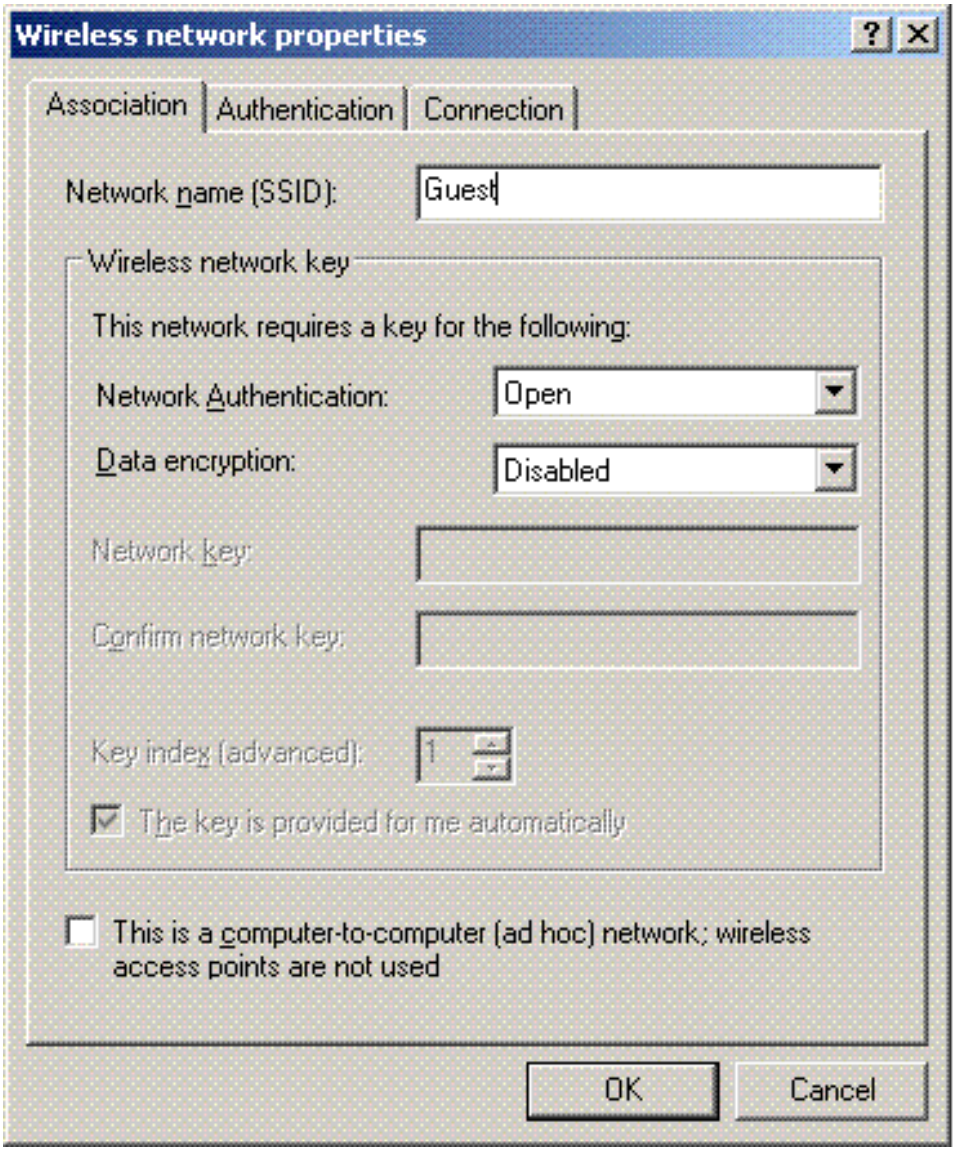
Uma vez que o WLC é configurado, o cliente deve ser configurado apropriadamente para a autenticação da Web. Nesta seção, serão apresentadas as informações necessárias para a configuração do sistema Windows para a autenticação da Web.

### Configuração do Cliente

A configuração do cliente wireless da Microsoft permanece praticamente inalterada para este assinante. Você precisa somente adicionar as informações de configuração da WLAN/SSID apropriada. Conclua estes passos:

1. No menu Start do Windows, escolha **Settings > Control Panel > Network and Internet Connections**.
2. Clique no ícone **Network Connections**.
3. Clique com o botão direito no ícone **LAN Connection** e escolha **Disable**.
4. Clique com o botão direito no ícone **Wireless Connection** e escolha **Enable**.
5. Clique com o botão direito no ícone **Wireless Connection** novamente e escolha **Properties**.
6. Na janela Wireless Network Connection Properties, clique na guia **Wireless Networks**.

7. Sob as redes preferidas, clique em **Add** para configurar o SSID da autenticação da Web.
8. Sob a guia Associação, insira o valor de Network Name (WLAN/SSID) que deseja usar para a autenticação da
   Web.




   **Note**: O valor de Data Encryption é, por padrão, Wired Equivalent Privacy (WEP). Desabilite a criptografia de dados para que a autenticação da Web funcione.
9. Clique em **OK** na parte inferior da janela para salvar a configuração.Ao se comunicar com a WLAN, você verá um ícone de sinalização na caixa Preferred Network.

Isto mostra uma conexão Wireless bem sucedida à autenticação da Web. A WLC forneceu ao seu cliente Windows wireless um endereço IP.


**Note**: Se seu cliente Wireless é igualmente um ponto final VPN e você tem a autenticação da Web configurada como uns recursos de segurança para o WLAN, a seguir o túnel VPN não está estabelecido até que você atravesse o processo de autenticação da Web explicado aqui. A fim estabelecer um túnel VPN, o cliente deve primeiramente atravessar o processo de autenticação da Web com sucesso. Somente então a criação de um túnel de VPN será bem-sucedida.

**Note**: Após um login bem-sucedido, se os clientes Wireless são quietude e não se comunicam com os alguns dos outros dispositivos, o cliente de-é autenticado após um período do idle timeout. O período de timeout é 300 segundos à revelia e pode ser mudado usando este comando CLI: `<seconds> do usertimeout da rede da configuração`. Quando isto ocorre, a entrada de cliente está removida do controlador. Se o cliente associa outra vez, mover-se-á de volta a um estado de Webauth_Reqd.

**Note**: Se os clientes são ativos após o login bem-sucedido, obterão de-autenticados e a entrada pode ainda ser removida do controlador após o período de timeout de sessão configurado nesse WLAN (pelos segundos example,1800 à revelia e pode ser mudado usando este comando CLI: `<seconds> wlan do sessão-intervalo <WLAN ID> da configuração`). Quando isto ocorre, a entrada de cliente está removida do controlador. Se o cliente associa outra vez, moverá em um estado de Webauth_Reqd.

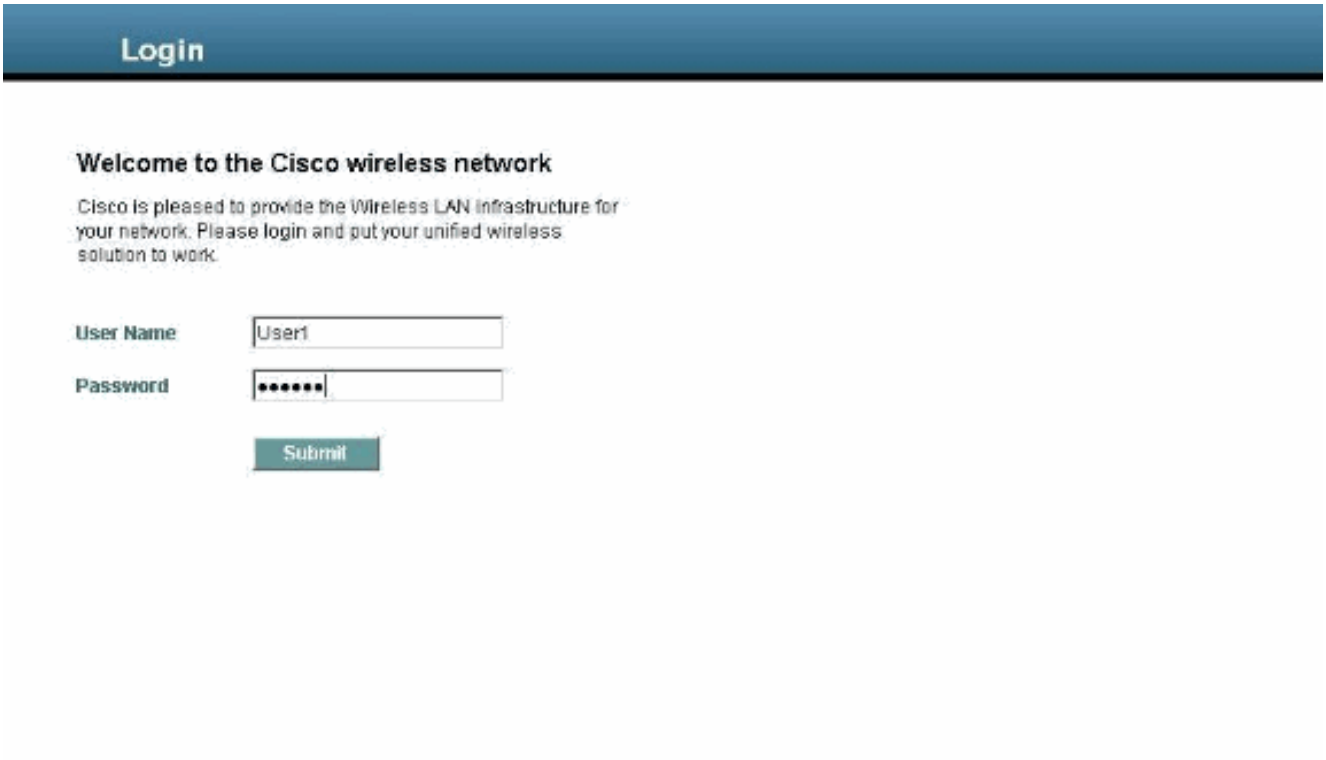
Se os clientes estão no estado de Webauth_Reqd, nenhuma matéria se são ativos ou inativos, os clientes obterão de-autenticados depois que um Web-**AUTH exigiu o período de timeout** (por exemplo, 300 segundos e esta vez são não utilizador configurável). Todo o tráfego do cliente (permitido através do PRE-AUTH ACL) será interrompido. Se o cliente associa outra vez, mover-se-á de volta ao estado de Webauth_Reqd.

## Login do Cliente

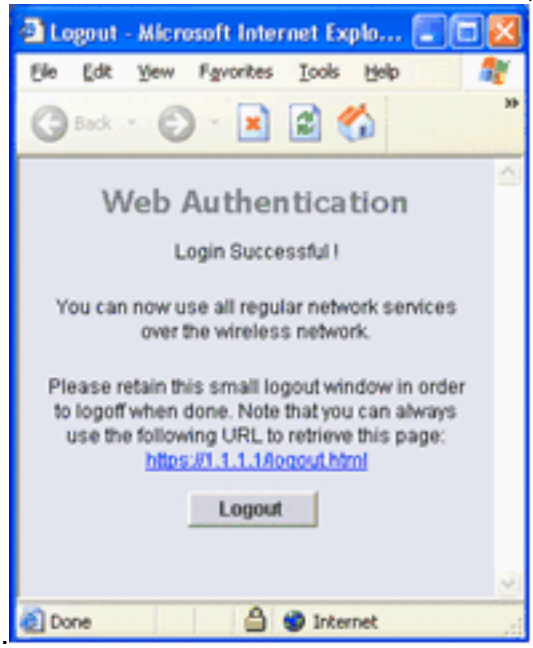
Conclua estes passos:

1. Abra uma janela de navegador e incorpore toda a URL ou endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto traz a página da autenticação da Web ao cliente.Se o controlador está executando qualquer liberação mais cedo do que o 3.0, o usuário tem que entrar em https://1.1.1.1/login.html para trazer acima a página da autenticação da Web.Uma janela de alerta de segurança é exibida.

2. Clique **Yes** para continuar.
3. Quando o indicador do início de uma sessão aparece, incorpore o nome de usuário e senha do usuário líquido local que você
criou.




Se o login for bem-sucedido, você verá duas janelas de navegador. O indicador maior indica que o login bem-sucedido e você podem este indicador consultar o Internet. Use a janela menor para encerrar a sessão quando seu uso da rede guest estiver concluído.O tiro de tela mostra que um bem sucedido reorienta para a autenticação da Web.O tiro de tela seguinte mostra ao início de uma sessão o indicador bem sucedido, que indica quando a




autenticação ocorreu.

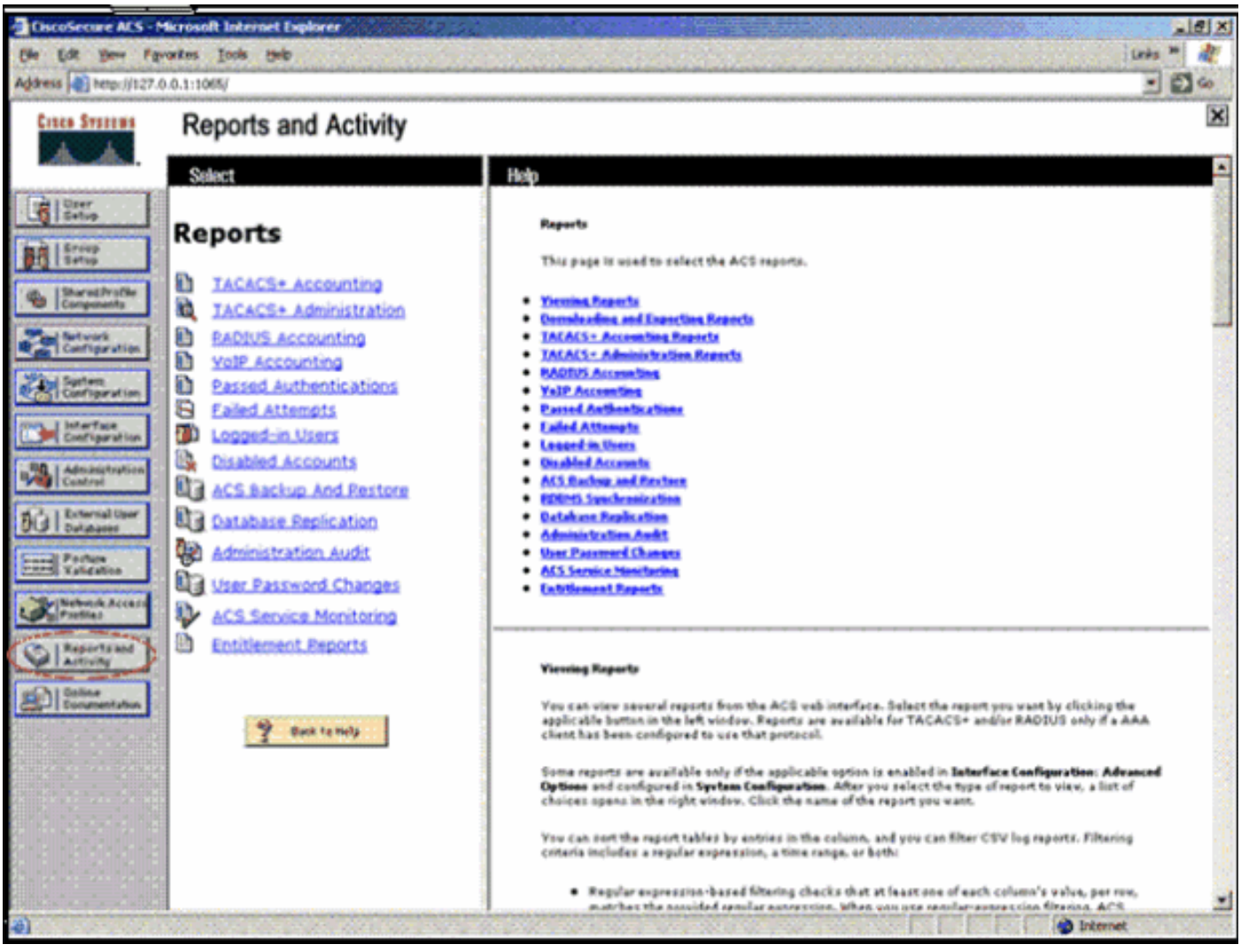
Os controladores de Cisco 4404/WiSM podem apoiar 125 inícios de uma sessão simultâneos dos usuários do AUTH da Web, e escalam até 5000 clientes do AUTH da Web.

Cisco 5500 controladores pode apoiar 150 inícios de uma sessão simultâneos dos usuários do AUTH da Web.

# Pesquise defeitos a autenticação da Web

## Troubleshooting do ACS

Se você enfrentar problemas com a autenticação de senha, clique em **Reports and Activity** no lado esquerdo inferior do ACS a fim de abrir todos os relatórios disponíveis. Depois que você abrir a janela de relatórios, você terá a opção de abrir a contabilidade do RADIUS, as falhas de tentativa de início de sessão, autenticações passadas, usuários conectados e outros relatórios. Esses relatórios são arquivos .CSV, e você pode abri-los localmente em seu computador. Os relatórios ajudam a descobrir problemas de autenticação, como nome de usuário e/ou senha incorretos. O ACS também possui documentação on-line. Se você não estiver conectado a uma rede ativa e não definiu a porta de serviço, o ACS usará o endereço IP da sua porta Ethernet como a porta de serviço. Se sua rede não estiver conectada, você provavelmente terminará com o endereço IP padrão do Windows 169.254.x.x.



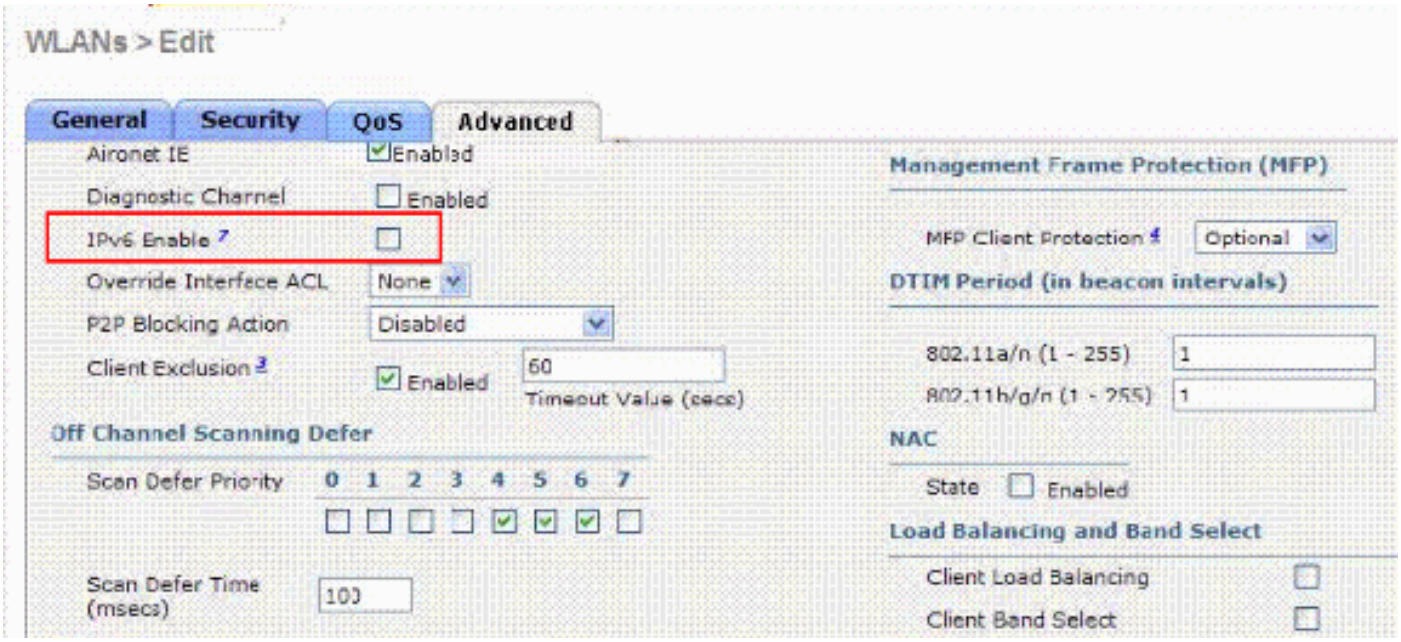

**Note**: Se você digitar algum URL externo, a WLC conectará você automaticamente à página da autenticação da Web interna. Se a conexão automática não funciona, você pode incorporar o endereço IP de gerenciamento do WLC à barra URL a fim pesquisar defeitos. Observe a parte superior do navegador em busca da mensagem sobre redirecionamento para a autenticação da Web.

Refira pesquisando defeitos a autenticação da Web em um controlador do Wireless LAN (WLC) para obter mais informações sobre da autenticação da Web do Troubleshooting.

# AUTH da Web com construção de uma ponte sobre do IPv6

A fim configurar um WLAN para o IPv6 que constrói uma ponte sobre, do controlador GUI, navegue aos **WLAN**. Então, selecione o WLAN desejado e escolha **avançado do WLAN > editam a** página.

Selecione o **IPv6 permitem a** caixa de verificação se você quer permitir os clientes que conectam a este WLAN para aceitar pacotes do IPv6. Se não, deixe a caixa de verificação unselected, que é o valor padrão. Se você desabilita (ou desmarcar) a caixa de verificação do IPv6, o IPv6 estará permitido somente após a autenticação. Permitir o IPv6 significa que o controlador pode passar o tráfego do IPv6 sem authenticação do cliente.




Para informações mais detalhadas sobre da construção de uma ponte sobre do IPv6 e das **diretrizes para usar esta característica**, refira o IPv6 configurando que constrói uma ponte sobre a seção do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 7.0.

# Informações Relacionadas

- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Pesquisar defeitos a autenticação da Web em um controlador do Wireless LAN (WLC)
- Cisco Wireless LAN
- Exemplo de Configuração de Acesso Convidado com Fio usando Cisco WLAN Controllers
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0 - Controlando contas de usuário
- Autenticação do Administrador do Lobby de Controladoras Wireless LAN via servidor RADIUS
- Suporte Técnico e Documentação - Cisco Systems