

Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de fundo](#)

[Processo de autenticação do web externa](#)

[Instalação de rede](#)

[Configurar](#)

[Crie uma interface dinâmica para os usuários convidado](#)

[Crie um ACL Pré-autenticação](#)

[Crie um base de dados local no WLC para os usuários convidado](#)

[Configurar o WLC para a autenticação do web externa](#)

[Configurar o WLAN para usuários convidado](#)

[Verificar](#)

[Troubleshooting](#)

[Os clientes reorientados ao Authentication Server do web externa recebem um aviso do certificado](#)

[Erro: a "página não pode ser indicada"](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento explica como usar um servidor web externo para configurar o Controller de LAN Wireless (WLC) para autenticação web.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração do Lightweight Access Points (regações) e do Cisco WLCs
- Conhecimento básico do protocolo de pouco peso do Access point (LWAPP) e o controle e o abastecimento dos pontos de acesso Wireless (CAPWAP)

- Conhecimento em como estabelecer e configurar um servidor de Web externo
- Conhecimento em como estabelecer e configurar o DHCP e os servidores DNS

Componentes Utilizados

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

- Cisco 4400 WLC que executa a versão de firmware 7.0.116.0
- REGAÇO do Cisco 1131AG Series
- Adaptador de cliente Wireless de Cisco 802.11a/b/g que executa a versão de firmware 3.6
- Servidor de Web externo que hospeda a página de login da autenticação da Web
- DNS e servidores DHCP para o address resolution e a alocação de endereço IP aos clientes Wireless

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any.

Convenções

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

Informações de fundo

A autenticação da Web é um recurso de segurança da camada 3 que faz 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. A autenticação da Web é um método de autenticação simples sem a necessidade para um suplicante ou um utilitário de cliente.

A autenticação da Web pode ser utilizada 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

Este original fornece um exemplo de configuração para explicar como configurar o WLC para usar um script do início de uma sessão de um servidor de Web externo.

Processo de autenticação do web externa

Com autenticação do web externa, a página de login usada para a autenticação da Web é armazenada em um servidor de Web externo. Esta é a sequência de evento quando um cliente Wireless tenta alcançar uma rede de WLAN que tenha a autenticação do web externa permitida:

1. O cliente (utilizador final) conecta ao WLAN e abre um web browser e incorpora uma URL,

tal como www.cisco.com.

2. O cliente envia um pedido DNS a um servidor DNS a fim resolver www.cisco.com ao IP address.
3. O WLC para a frente o pedido ao servidor DNS que, por sua vez, resolve www.cisco.com ao IP address e envia uma resposta DNS. O controlador para a frente a resposta ao cliente.
4. O cliente tenta iniciar uma conexão de TCP com o IP address de www.cisco.com enviando o pacote SYN de TCP ao IP address de www.cisco.com.
5. 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 IP address de www.cisco.com. O cliente envia para trás um pacote TCP ACK a fim terminar o cumprimento de TCP de três maneiras e a conexão de TCP é estabelecida inteiramente.
6. O cliente envia um pacote HTTP GET destinado a www.google.com. O WLC intercepta este pacote, 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.
7. O cliente liga então a conexão de HTTPS à reorientação URL que a envia a 1.1.1.1. Este é o IP address virtual do controlador. O cliente tem que validar o certificado de servidor ou ignorá-lo a fim trazer acima o túnel SSL.
8. Porque a autenticação do web externa é permitida, o WLC reorienta o cliente ao servidor de Web externo.
9. O início de uma sessão URL do AUTH do web externa é adicionado com parâmetros tais como o AP_Mac_Address, o client_url (www.cisco.com) e o action_URL que o cliente precisa de contactar o servidor de Web do controlador. **Note:** O action_URL diz ao servidor de Web que o nome de usuário e senha está armazenado no controlador. As credenciais devem ser enviadas para trás ao controlador a fim obter autenticadas.
10. O servidor de Web externo URL conduz o usuário a uma página de login.
11. A página de login toma a entrada das credenciais do usuário, e envia o pedido de volta ao action_URL, exemplo http://1.1.1.1/login.html, do servidor de Web WLC.
12. O servidor de Web WLC submete o nome de usuário e senha para a autenticação.
13. O WLC inicia o pedido do servidor Radius ou usa o base de dados local no WLC e autentica o usuário.
14. Se a autenticação é bem sucedida, o servidor de Web WLC qualquer um para a frente o usuário ao configurado reorienta a URL ou à URL o cliente começou com, como www.cisco.com.
15. Se a autenticação falha, a seguir o servidor de Web WLC reorienta o usuário de volta ao início de uma sessão URL do cliente.

Note: A fim configurar o webauthentication externo para usar portas diferentes do HTTP e do HTTPS, emita este comando:

```
(Cisco Controller) >config network web-auth-port
```

```
<port> Configures an additional port to be redirected for web authentication.
```

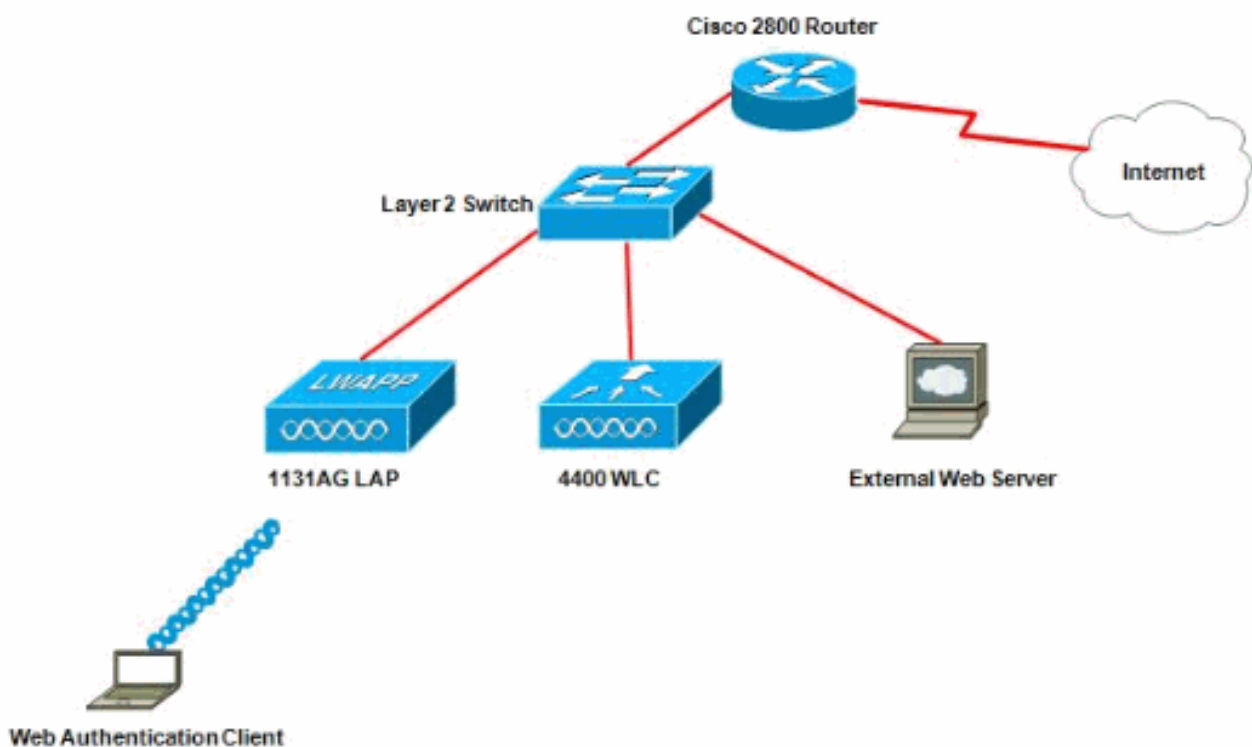
[Instalação de rede](#)

O exemplo de configuração usa esta instalação. UM REGAÇO é registrado ao WLC. Você precisa de configurar um **convidado** WLAN para os usuários convidado e tem que permitir a autenticação

da Web para os usuários. Você igualmente precisa de assegurar-se de que o controlador reoriente o usuário ao servidor de Web externo URL (para a autenticação do web externa). O servidor de Web externo hospeda a página de login da Web que é usada para a autenticação.

As credenciais do usuário devem ser validadas contra o base de dados local mantido no controlador. Após a autenticação bem sucedida, os usuários devem ser permitidos o acesso ao convidado WLAN. O controlador e os outros dispositivos precisam de ser configurados para esta instalação.

Note: Você pode usar uma versão personalizada do script do início de uma sessão, que será usado para a autenticação da Web. Você pode transferir um script da autenticação da Web da amostra da página das [transferências de software Cisco](#). Por exemplo, para os 4400 controladores, navegue ao **Produtos > ao Sem fio > ao controlador do Wireless LAN > aos Controladores autônomos > ao Controladores de LAN sem fio Cisco série 4400 > ao controlador > ao software do Wireless LAN de Cisco 4404 no chassi > na autenticação da Web Bundle-1.0.1 do controlador do Wireless LAN** e transfira o arquivo `webauth_bundle.zip`.



Note: O pacote personalizado do AUTH da Web tem um limite de até 30 caracteres para nomes de arquivo. Assegure-se de que nenhum nome de arquivo dentro do pacote esteja maior de 30 caracteres.

Note: Este original supõe que o DHCP, o DNS e os servidores de Web externos estão configurados. Refira a documentação apropriada da terceira parte para obter informações sobre de como configurar o DHCP, o DNS e o servidor de Web externo.

[Configurar](#)

Antes que você configure o WLC para a autenticação do web externa, você deve configurar o WLC para a operação básica e registrar os regaços ao WLC. Este original supõe que o WLC está configurado para a operação básica e que os regaços estão registrados ao WLC. Refira o [registro](#)

[de pouco peso AP \(REGAÇO\) a um controlador do Wireless LAN \(WLC\)](#) se você é um novo usuário que tenta estabelecer o WLC para a operação básica com regaços.

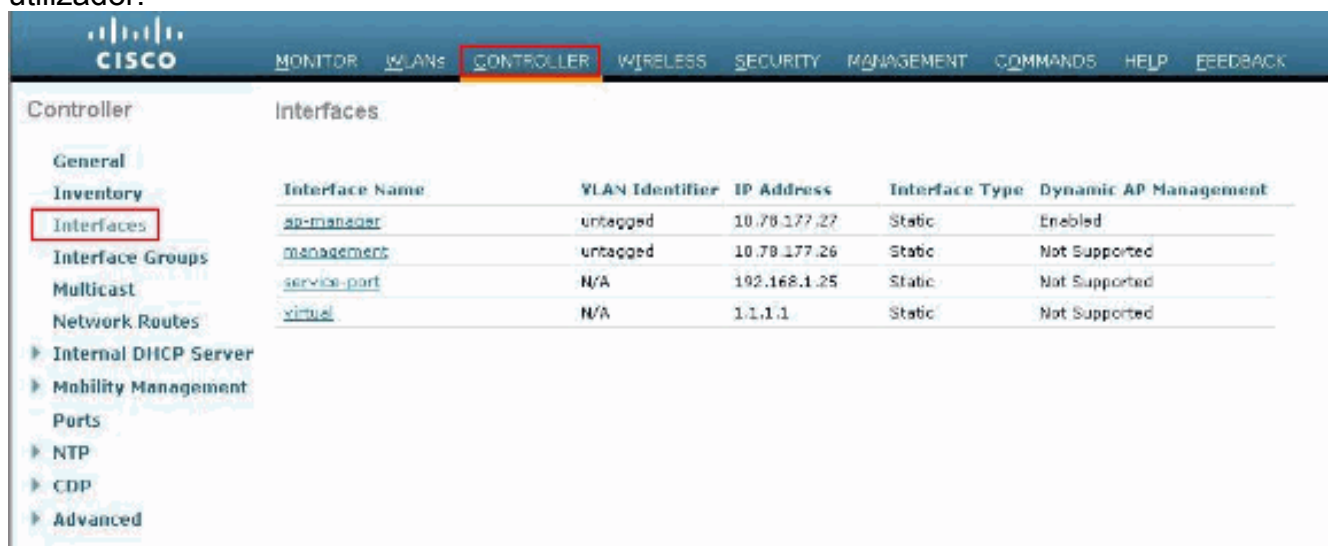
Termine estas etapas a fim configurar os regaços e o WLC para esta instalação:

1. [Crie uma interface dinâmica para os usuários convidado](#)
2. [Crie um ACL Pré-autenticação](#)
3. [Crie um base de dados local no WLC para os usuários convidado](#)
4. [Configurar o WLC para a autenticação do web externa](#)
5. [Configurar o WLAN para usuários convidado](#)

[Crie uma interface dinâmica para os usuários convidado](#)

Termine estas etapas a fim criar uma interface dinâmica para os usuários convidado:

1. Do WLC GUI, escolha **controladores > relações**. O indicador das relações aparece. Este indicador lista as relações que são configuradas no controlador. Isto inclui as interfaces padrão, que são a interface de gerenciamento, relação do ap-gerente, a interface virtual e a interface de porta do serviço, e as interfaces dinâmica definidas pelo utilizador.



The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. The 'Interfaces' section is active, displaying a table of configured interfaces. The table has the following columns: Interface Name, VLAN Identifier, IP Address, Interface Type, and Dynamic AP Management.

| Interface Name | VLAN Identifier | IP Address | Interface Type | Dynamic AP Management |
|------------------------------|-----------------|--------------|----------------|-----------------------|
| ap-manager | untagged | 10.78.177.27 | Static | Enabled |
| management | untagged | 10.78.177.26 | Static | Not Supported |
| service-port | N/A | 192.168.1.25 | Static | Not Supported |
| virtual | N/A | 1.1.1.1 | Static | Not Supported |

2. Clique **novo** a fim criar uma interface dinâmica nova.
3. **Nas relações > na nova janela**, incorpore o nome da relação e a identificação VLAN. Então, o clique **aplica-se**. Neste exemplo, a interface dinâmica é nomeada **convidado** e a identificação VLAN é atribuída o **10**.

The screenshot shows the Cisco Controller web interface. At the top, there is a navigation bar with the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The CONTROLLER tab is selected. On the left, there is a sidebar menu under the heading 'Controller' with various options: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'guest' and 'VLAN Id' with the value '10'. A red box highlights these two fields.

4. **Nas relações > edite** o indicador, para a interface dinâmica, entre no IP address, na máscara de sub-rede, e no gateway padrão. Atribua-à uma porta física no WLC, e incorpore-o o IP address do servidor DHCP. Então, o clique **aplique-se**.

The screenshot displays the Cisco WLC GUI for configuring an interface. The left sidebar shows the navigation menu with 'Interfaces' selected. The main content area is titled 'Interfaces > Edit' and contains the following configuration sections:

- General Information:** Interface Name: guest; MAC Address: 00:0b:85:48:53:c0
- Configuration:** Guest Lan: ; Quarantine: ; Quarantine Vlan Id: 0
- Physical Information:** Port Number: 2; Backup Port: 0; Active Port: 0; Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 10; IP Address: 172.18.1.10; Netmask: 255.255.255.0; Gateway: 172.18.1.20
- DHCP Information:** Primary DHCP Server: 172.18.1.20; Secondary DHCP Server: (empty)
- Access Control List:** ACL Name: none

[Crie um ACL Pré-autenticação](#)

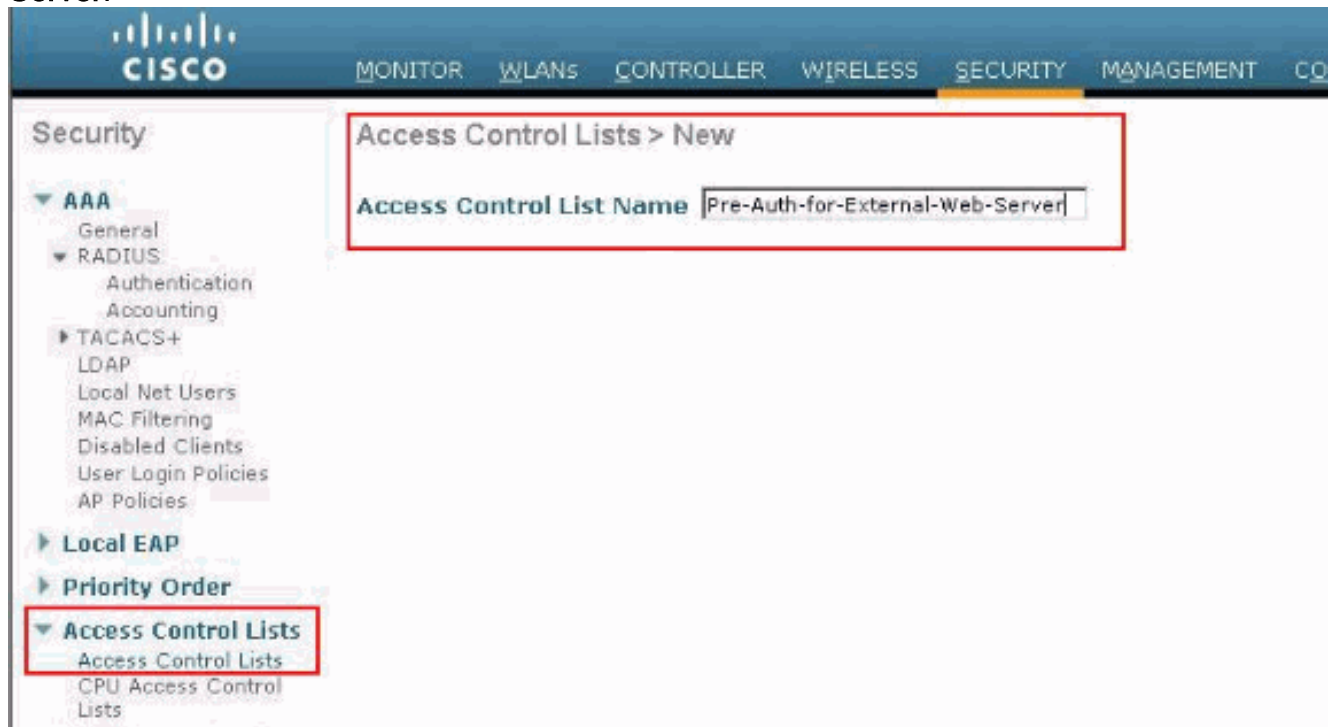
Ao usar um servidor de Web externo para a autenticação da Web, algumas das Plataformas WLC precisam uma PRE-autenticação ACL para o servidor de Web externo (o controlador do Cisco 5500 Series, um Cisco 2100 Series controlador, o Cisco 2000 Series e o módulo de rede do controlador). Para as outras Plataformas WLC a PRE-autenticação ACL não é imperativa.

Contudo, é uma boa prática configurar um ACL Pré-autenticação para o servidor de Web externo ao usar a autenticação do web externa.

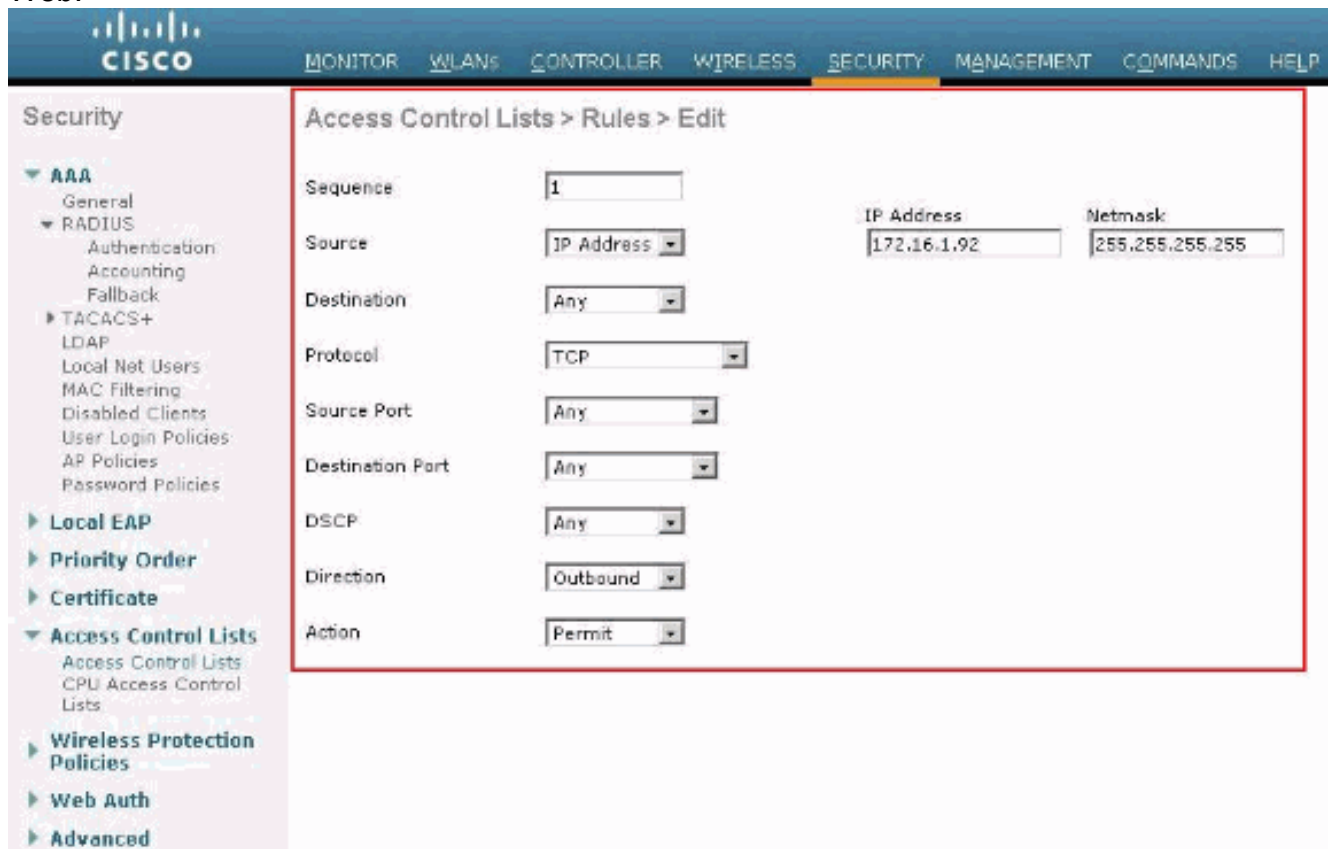
Termine estas etapas a fim configurar o ACL Pré-autenticação para o WLAN:

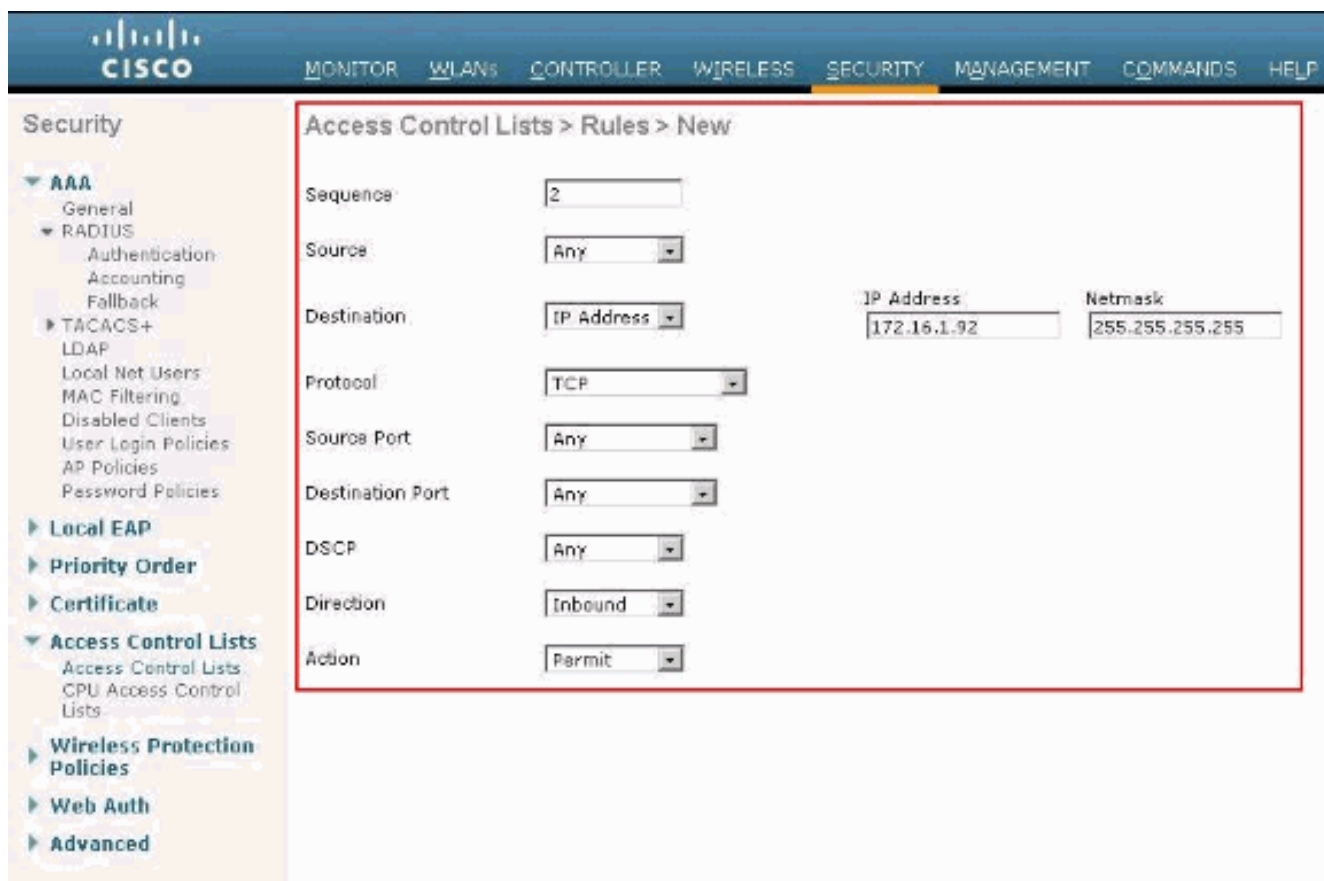
1. Do WLC GUI, escolha a **Segurança > as listas de controle de acesso**. Este indicador permite que você ver os ACL atuais que são similares ao Firewall padrão ACL.
2. Clique **novo** a fim criar um ACL novo.
3. Dê entrada com o nome do ACL e do clique **aplicam-se**. Neste exemplo, o ACL é nomeado PRE-AUTH-para-Externo-Web-

Server.

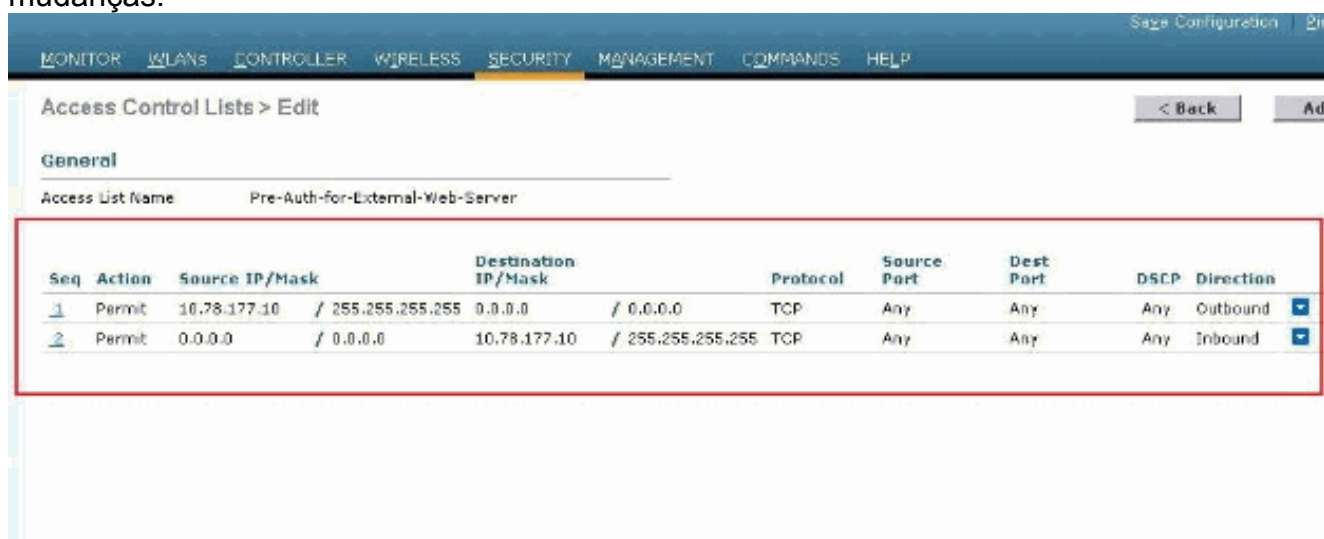


4. Para o ACL novo criado, o clique **edita**. O ACL > edita o indicador aparece. Este indicador deixa o usuário definir regras novas ou alterar as regras do ACL que existem.
5. O clique **adiciona a regra nova**.
6. Defina uma regra ACL que permita o acesso para os clientes ao servidor de Web externo. Neste exemplo, 172.16.1.92 é o IP address externo do servidor de Web.





7. O clique **aplica-se** a fim comprometer as mudanças.



[Crie um base de dados local no WLC para os usuários convidado](#)

A base de dados de usuário para os usuários convidado pode ser armazenada no base de dados local do controlador do Wireless LAN, ou pôde ser externo armazenado do controlador.

Neste original o base de dados local no controlador é usado para autenticar usuários. Você deve criar um usuário líquido local e definir uma senha para o login do cliente da autenticação da Web. Termine estas etapas a fim criar a base de dados de usuário no WLC:

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

The image shows the Cisco SCA interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar is titled 'Security' and contains a tree view with the following items: AAA (General, RADIUS (Authentication, Accounting, Fallback), TACACS+, LDAP, Local Net Users (highlighted in a red box), MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies), Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The main content area is titled 'Local Net Users' and displays a table with the following columns: User Name, WLAN Profile, Guest User, Role, and Description.

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 **User1**.
5. Adicione uma descrição, se desejar. Este exemplo usa o **convidado User1**.
6. Clique em **Apply** para salvar a configuração do novo usuário.

The image shows the 'Local Net Users > New' configuration form in the Cisco SCA. The form fields are: User Name (User1), Password (masked), Confirm Password (masked), Guest User (checked), Lifetime (seconds) (86400), Guest User Role (unchecked), WLAN Profile (Guest), and Description (GuestUser1). The entire form area is highlighted with a red box.

The screenshot shows the Cisco WLC Security configuration page. The left sidebar is expanded to 'Local Net Users'. The main content area displays a table with the following data:

| User Name | WLAN Profile | Guest User | Role | Description |
|-----------|--------------|------------|------|-------------|
| User1 | Guest | Yes | | GuestUser1 |

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

Configurar o WLC para a autenticação do web externa

A próxima etapa é configurar o WLC para a autenticação do web externa. Conclua estes passos:

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 **externo (reoriente ao servidor interno)**.
3. Na seção **externo do servidor de Web**, adicionar o servidor de Web externo novo.
4. **Na reorientação URL depois que o campo do início de uma sessão**, incorpora a URL da página a que o utilizador final estará reorientado em cima da autenticação bem sucedida. No campo **URL do AUTH do web externa**, incorpore a URL onde a página de login é armazenada no servidor de Web externo.

The screenshot shows the Cisco WLC Security configuration page for the Web Login Page. The left sidebar is expanded to 'Web Auth > Web Login Page'. The main content area displays the following settings:

Web Login Page

Web Authentication Type: (Dropdown menu options: Internal (Default), Customized (Downloaded), External (Redirect to external server) ...)

Redirect URL after login:

This page allows you to customize the content and appearance of the login page. The Login page is presented to web users the first time they access the WLAN if "Web Authentication" is turned on (under WLAN Security Policies).

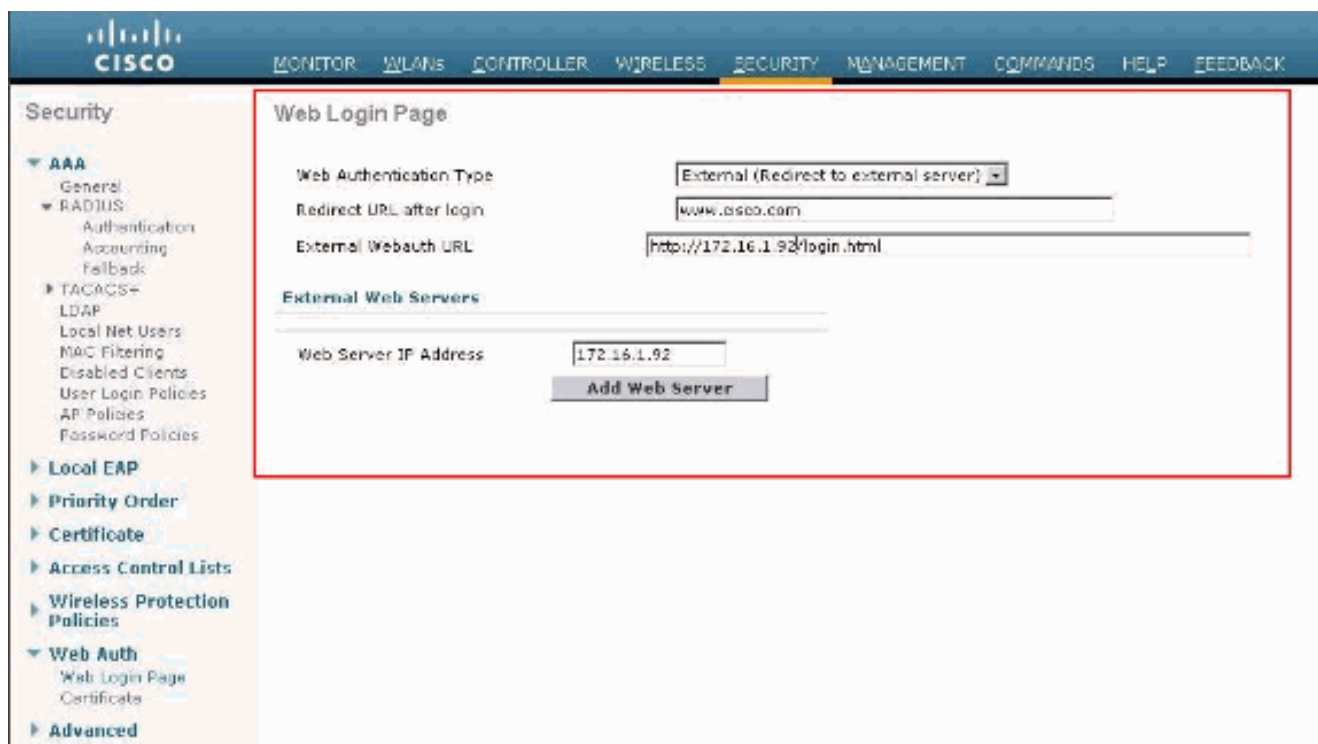
Cisco Logo: Show Hide

Headline:

Message:

External Web Servers

Web Server IP Address:

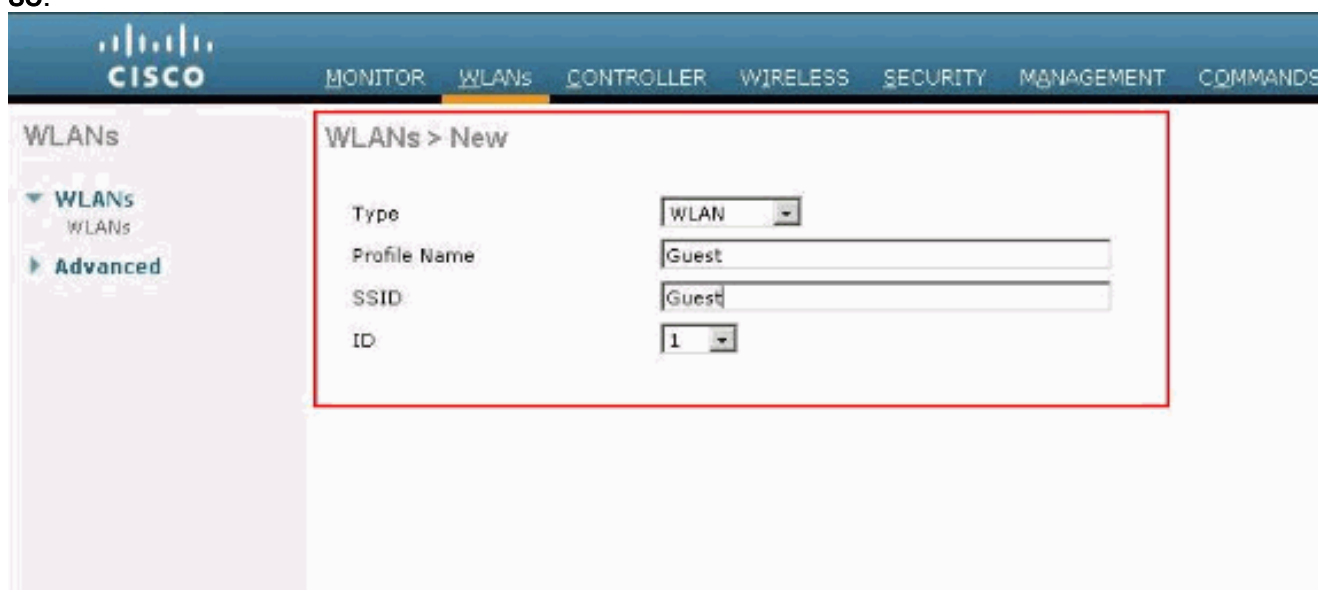


Note: Em versões 5.0 e mais recente WLC, a página da saída para a autenticação da Web pode igualmente ser personalizada. Refira as [páginas do início de uma sessão, da falha no login e da saída da atribuição pela](#) seção [WLAN da configuração de controle](#) *Guide, 5.2 do Wireless LAN* para obter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

[Configurar o WLAN para usuários convidado](#)

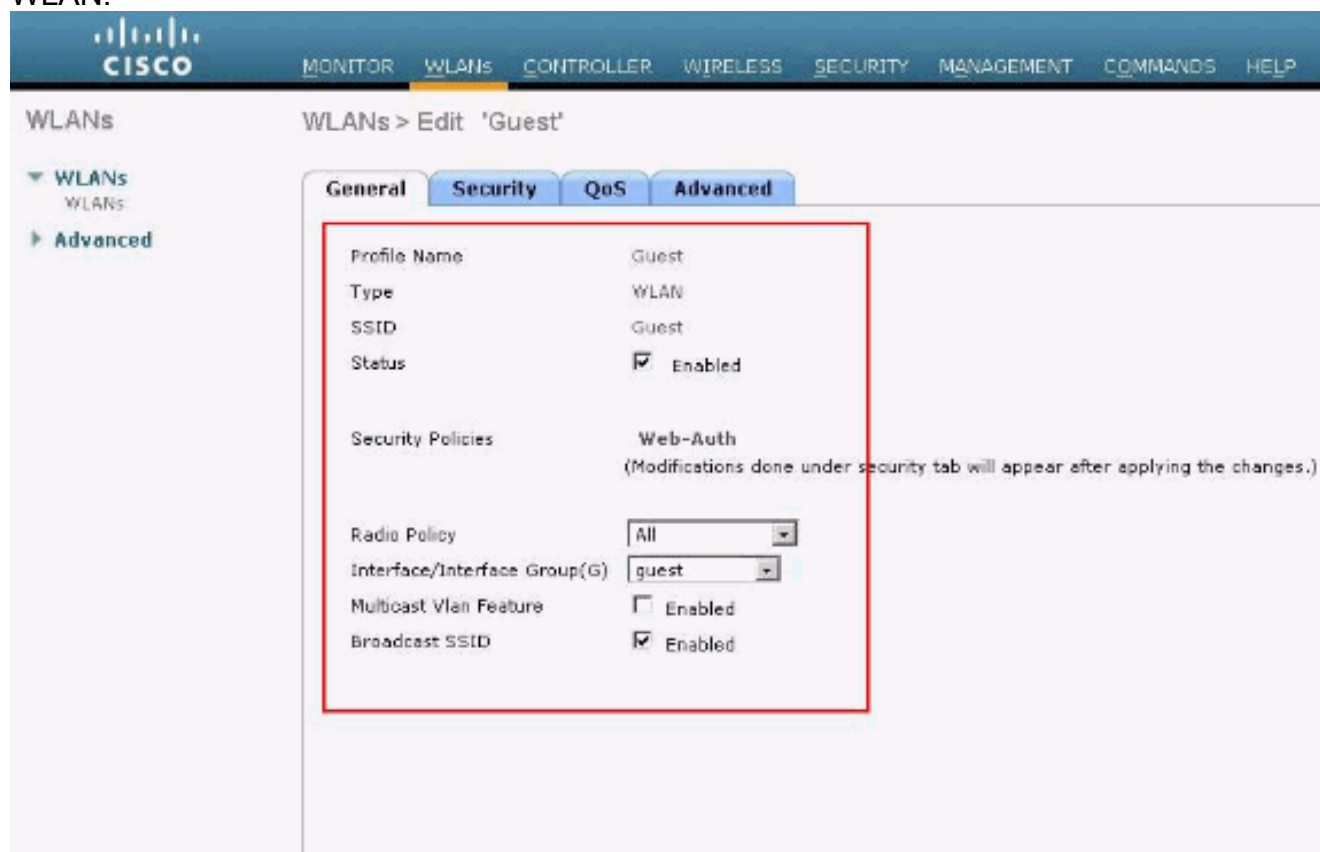
A etapa final é criar WLAN para os usuários convidado. Conclua estes passos:

1. Clique **WLAN** do controlador GUI a fim criar um WLAN. A janela WLANs aparece. Este indicador alista os WLAN configurados no controlador.
2. Clique **novo** a fim configurar um WLAN novo. Neste exemplo, o WLAN é nomeado **Convidado** e o ID de WLAN é 1.
3. O clique **aplica-se**.

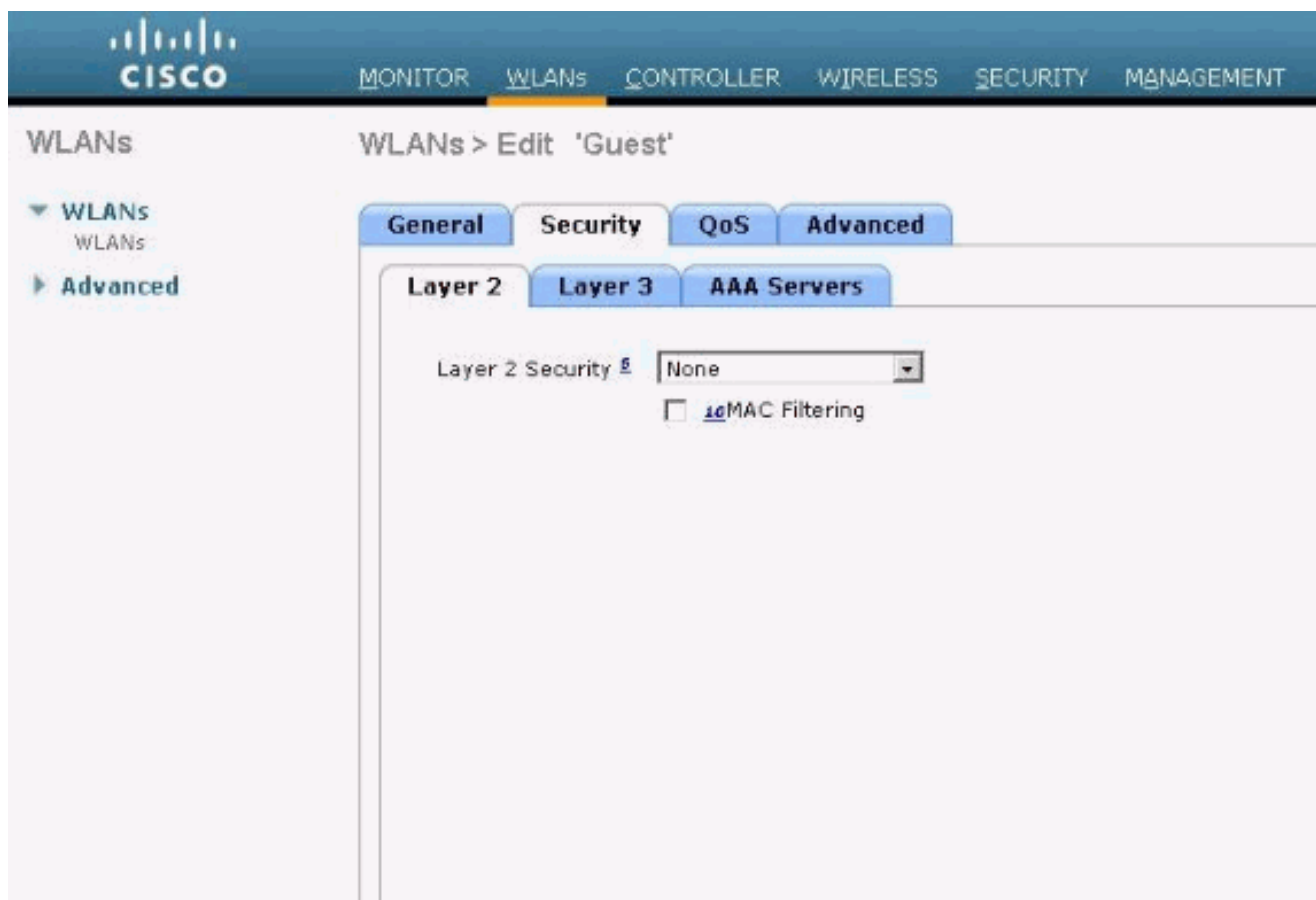


4. No o WLAN > edita o indicador, define os parâmetros específicos ao WLAN. Para o

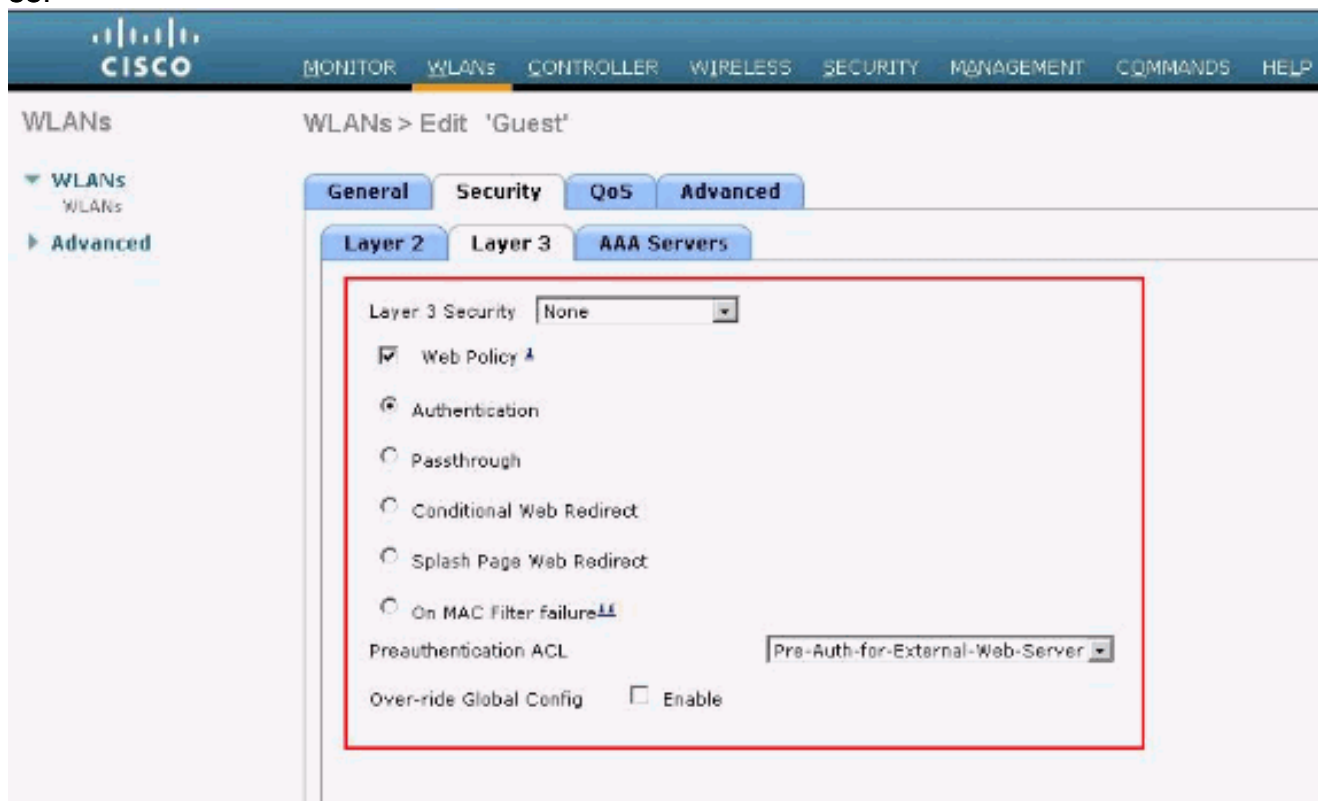
convidado WLAN, no tab geral, escolha a relação apropriada do campo de nome da relação. Este exemplo traça o **convidado da** interface dinâmica que foi criado previamente ao convidado WLAN.



Vá à ABA de segurança. Sob a Segurança da camada 2, **nenhum** é selecionado neste exemplo. **Note:** A autenticação da Web não é apoiada com autenticação do 802.1x. Isto significa que você não pode escolher o 802.1x ou um WPA/WPA2 com o 802.1x como a Segurança da camada 2 quando você usa a autenticação da Web. A autenticação da Web é apoiada com todos parâmetros de segurança restantes da camada 2.



No campo de Segurança da camada 3, verifique a **caixa de verificação de Política da web** e escolha a **opção de autenticação**. Esta opção é escolhida porque a autenticação da Web é usada para autenticar os clientes sem fio do convidado. Escolha o ACL Pré-autenticação apropriado do menu suspenso. Neste exemplo, o ACL Pré-autenticação que foi criado previamente é usado. O clique **aplica-se**.

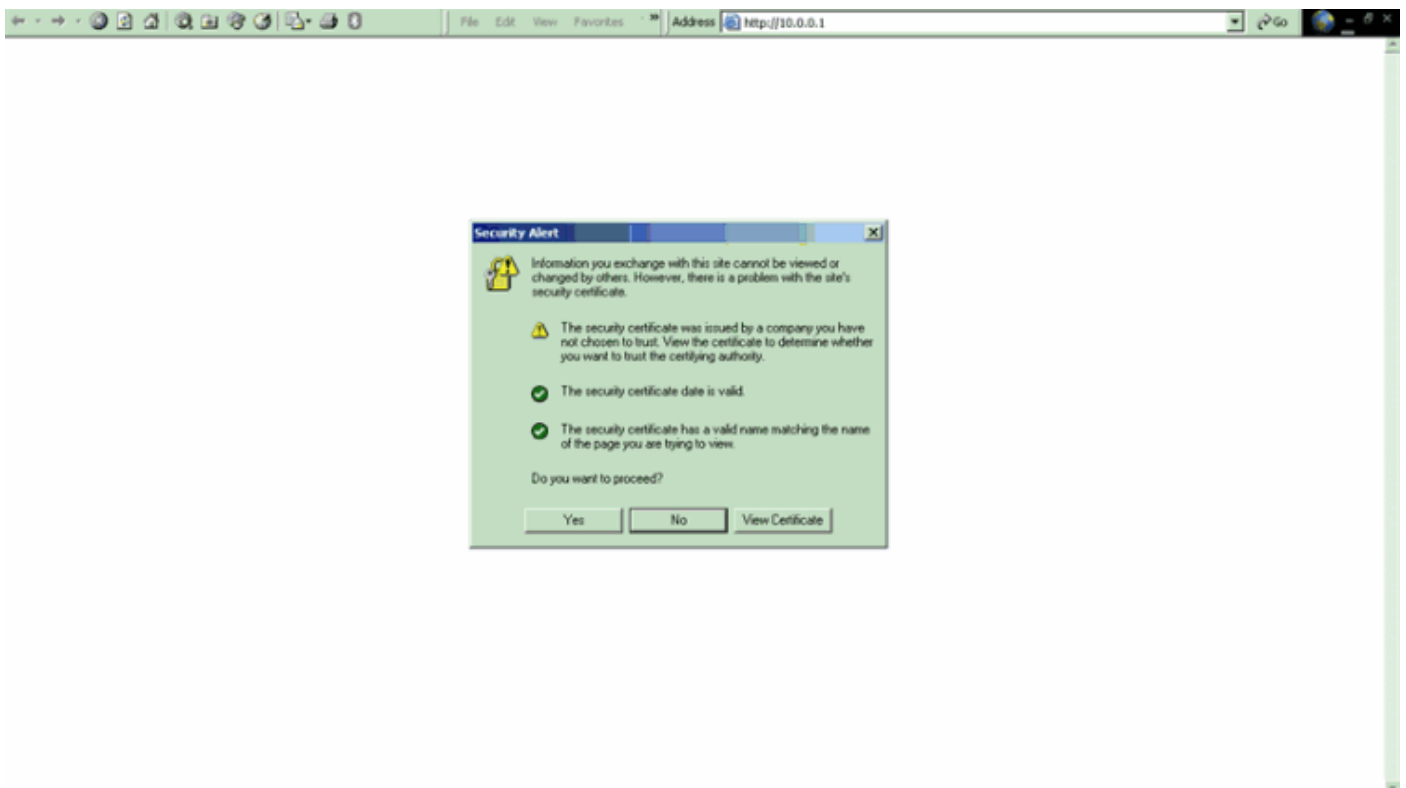


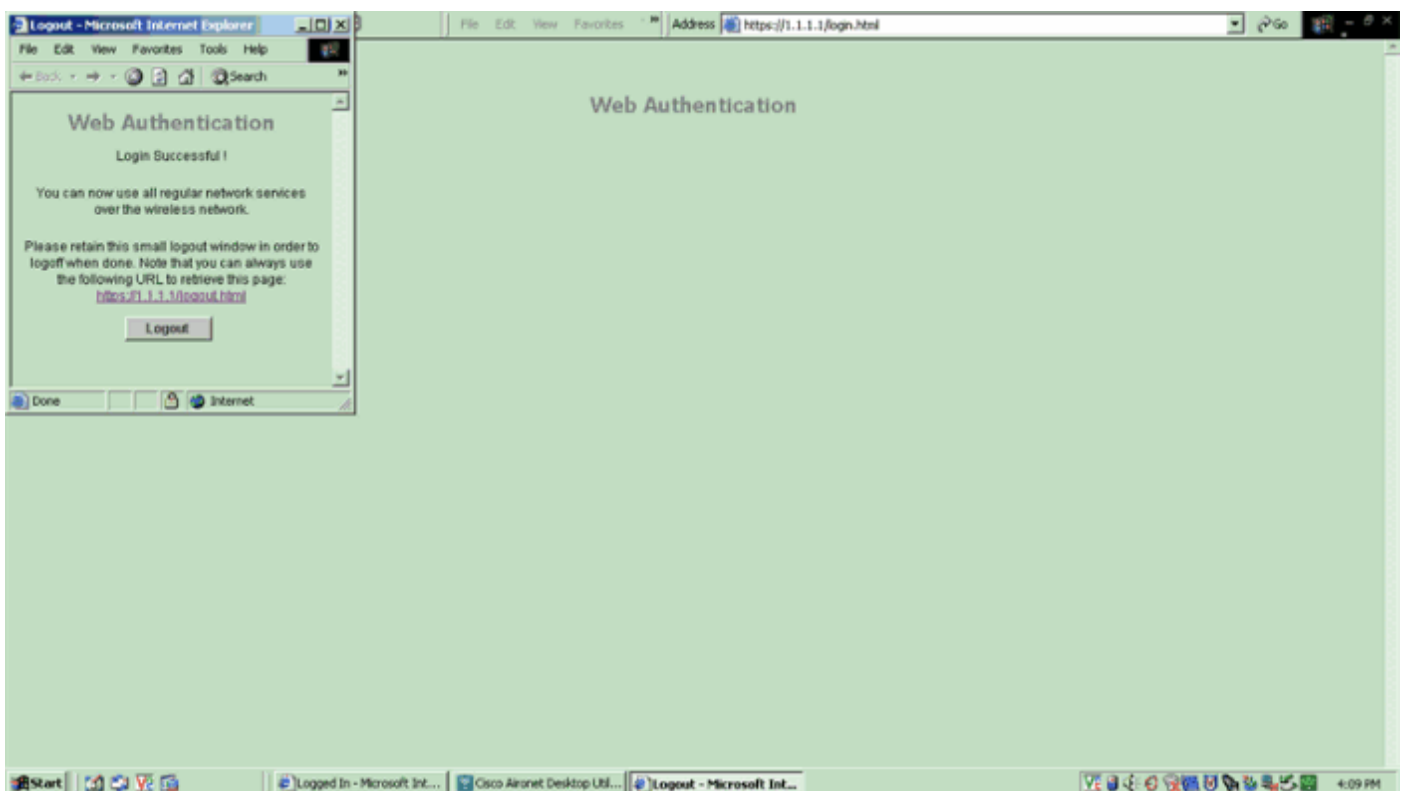
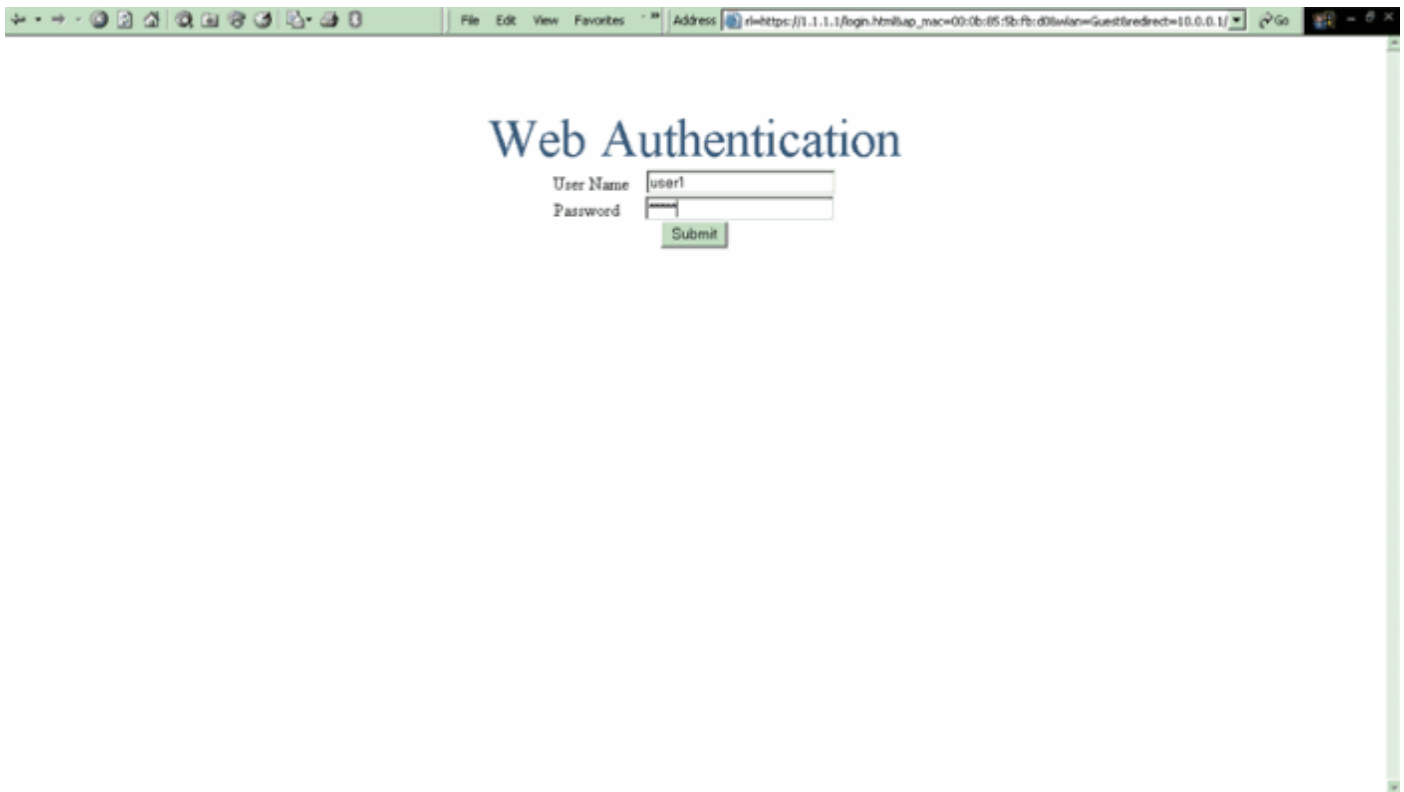
Verificar

O cliente Wireless vem acima e o usuário incorpora a URL, tal como www.cisco.com, ao web browser. Porque o usuário não foi autenticado, o WLC reorienta o usuário ao início de uma sessão URL do web externa.

O usuário é alertado para as credenciais do usuário. Uma vez que o usuário submete o nome de usuário e senha, a página de login toma a entrada das credenciais do usuário e submete-se sobre envia o pedido de volta ao exemplo do `action_URL`, `http://1.1.1.1/login.html`, do servidor de Web WLC. Isto é fornecido enquanto um parâmetro de entrada ao cliente reorienta a URL, onde 1.1.1.1 é o endereço da interface virtual no interruptor.

O WLC autentica o usuário contra o base de dados local configurado no WLC. Após a autenticação bem sucedida, o servidor de Web WLC qualquer um para a frente o usuário ao configurado reorienta a URL ou à URL o cliente começou com, como www.cisco.com.





Troubleshooting

Use estes comandos debug a fim pesquisar defeitos sua configuração.

- debug o <client-MAC-endereço xx do ADDR do Mac: xx: xx: xx: xx: xx>
- debug aaa all enable
- debug o estado PEM permitem
- debug eventos PEM permitem
- debug o mensagem DHCP permitem

- debugar o pacote DHCP permitem
- debugar pm SSH-appgw permitem
- debugar pm SSH-TCP permitem

Use esta seção para resolver problemas de configuração.

Os clientes reorientados ao Authentication Server do web externa recebem um aviso do certificado

Problema: Quando os clientes são reorientados ao Authentication Server do web externa de Cisco, recebem um aviso do certificado. Há um certificado válido no server, e se você conecta ao Authentication Server do web externa diretamente o aviso do certificado não é recebido. É isto porque o IP address virtual (1.1.1.1) do WLC é apresentado ao cliente em vez do IP address real do Authentication Server do web externa que é associado com o certificado?

Solução: Sim. Mesmo se você executa o local ou a autenticação do web externa, você ainda bate o servidor de Web interno no controlador. Quando você reorienta a um servidor de Web externo, você ainda recebe o aviso do certificado do controlador a menos que você tiver um certificado válido no controlador próprio. Se a reorientação é enviada aos https, você recebe o aviso do certificado do controlador e do servidor de Web externo, a menos que ambos tiverem um certificado válido.

A fim obter livrou todos do certificado dos avisos junto, você precisa de ter um certificado do nível da raiz emitido e transferido em seu controlador. O certificado é emitido para um nome de host e você põe que nome de host na caixa de nome do host DNS sob a interface virtual sobre o controlador. Você igualmente precisa de adicionar o nome de host a seu servidor DNS local e de apontá-lo ao IP address virtual (1.1.1.1) do WLC.

Refira a [geração da solicitação de assinatura de certificado \(CSR\) para um certificado da terceira em um controlador de WLAN \(WLC\)](#) para mais informação.

Erro: a “página não pode ser indicada”

Problema: Depois que o controlador é promovido a 4.2.61.0, a “página não pode ser” Mensagem de Erro indicado aparece quando você usa um página da web transferido para a autenticação da Web. Isto trabalhado bem antes da elevação. O página da web interno do padrão carrega sem nenhum problema.

Solução: Da versão 4.2 e mais recente WLC uns novos recursos são introduzidos onde você pode ter páginas de login customized múltiplo para a autenticação da Web.

A fim ter a carga do página da web corretamente, não é suficiente ajustar o tipo da autenticação da Web como **personalizado** globalmente na **página de login do AUTH da Segurança > da Web > da Web**. Deve igualmente ser configurado em um WLAN particular. Para isso, conclua essas etapas:

1. Log no GUI do WLC.
2. Clique sobre a aba **WLAN**, e alcance o perfil do WLAN configurado para a autenticação da Web.
3. No o WLAN > edita a página, clica a **ABA de segurança**. Então, escolha a **camada 3**.
4. Nesta página, não escolha **nenhuns** como a Segurança da camada 3.
5. Verifique a caixa da **política da Web**, e escolha a **opção de autenticação**.

6. Verifique o config global da ultrapassagem **permitted** a caixa, escolhem-na **personalized** (**transferido**) como o tipo do AUTH da Web, e seleccionam-nos a página de login desejada do menu de **Pagepull** do início de uma sessão para baixo. O clique **aplica-se**.

Informações Relacionadas

- [Exemplo de configuração da autenticação da Web do controlador do Wireless LAN](#)
- [Vídeo: Autenticação da Web em controladores de LAN do Cisco Wireless \(WLCs\)](#)
- [VLAN no exemplo de configuração dos controladores do Wireless LAN](#)
- [Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight](#)
- [Suporte técnico & documentação - Cisco Systems](#)