

Configurar a autenticação da Web externa com WLCs

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Processo de Autenticação Externa da Web](#)

[Instalação de rede](#)

[Configurar](#)

[Criar uma interface dinâmica para os usuários convidados](#)

[Criar uma ACL de pré-autenticação](#)

[Crie um banco de dados local no WLC para os usuários convidados](#)

[Configurar a WLC para autenticação externa da Web](#)

[Configurar a WLAN para usuários convidados](#)

[Verificar](#)

[Troubleshoot](#)

[Clientes Redirecionados para Servidor de Autenticação da Web Externo Recebem um Aviso de Certificado](#)

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

[Informações Relacionadas](#)

[Introduction](#)

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

[Prerequisites](#)

[Requirements](#)

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

- Conhecimento básico da configuração de Pontos de Acesso Lightweight (LAPs) e Cisco WLCs
- Conhecimento básico do Lightweight Access Point Protocol (LWAPP) e do Control and Provisioning of Wireless Access Points (CAPWAP)

- Conhecimento sobre como instalar e configurar um servidor Web externo
- Conhecimento sobre como instalar e configurar servidores DHCP e DNS

Componentes Utilizados

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

- WLC Cisco 4400 com firmware versão 7.0.116.0
- LAP Cisco 1131AG Series
- Adaptador de cliente wireless da Cisco 802.11a/b/g que executa firmware com release 3.6
- Servidor Web externo que hospeda a página de logon da autenticação da Web
- Servidores DNS e DHCP para resolução de endereços e alocação de endereços IP para clientes sem fio

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

A autenticação da Web é um recurso de segurança da Camada 3 que visa impedir que o controlador permita o tráfego IP (exceto pacotes relacionados a DHCP e DNS) de um cliente específico até que este tenha um nome de usuário e senha válidos. A autenticação da Web é um método de autenticação simples sem a necessidade de um suplicante ou utilitário cliente.

A autenticação da Web pode ser executada ao usar:

- Janela de login padrão do WLC
- Versão modificada da janela de login padrão do WLC
- Uma janela de login personalizada, configurada em um servidor externo da Web (Autenticação externa da Web)
- Uma janela de login personalizada, baixada no controlador

Este documento fornece um exemplo de configuração para explicar como configurar o WLC para usar um script de login de um servidor web externo.

Processo de Autenticação Externa da Web

Com a autenticação da Web externa, a página de logon usada para autenticação da Web é armazenada em um servidor Web externo. Esta é a sequência de eventos quando um cliente sem fio tenta acessar uma rede WLAN que tem a autenticação externa da Web habilitada:

1. O cliente (usuário final) se conecta à WLAN e abre um navegador da Web e digita uma URL, como www.cisco.com.
2. O cliente envia uma solicitação DNS a um servidor DNS para resolver www.cisco.com para

o endereço IP.

3. A WLC encaminha a solicitação ao servidor DNS que, por sua vez, resolve `www.cisco.com` para o endereço IP e envia uma resposta DNS. O controlador encaminha a resposta ao cliente.
4. O cliente tenta iniciar uma conexão TCP com o endereço IP `www.cisco.com` enviando o pacote TCP SYN para o endereço IP `www.cisco.com`.
5. O WLC tem regras configuradas para o cliente e, portanto, pode agir como um proxy para `www.cisco.com`. Ele responde enviando um pacote TCP SYN-ACK ao cliente com a fonte como o endereço IP de `www.cisco.com`. Em resposta, o cliente envia um pacote TCP ACK para concluir o handshake de três vias do TCP e, com isso, a conexão TCP é plenamente estabelecida.
6. O cliente envia um pacote HTTP GET destinado a `www.google.com`. A WLC intercepta esse pacote e o envia para tratamento de redirecionamento. O gateway de aplicativo HTTP prepara um corpo HTML e o envia de volta como resposta ao HTTP GET solicitado pelo cliente. Esse HTML leva o cliente ao URL padrão da página da Web do WLC, por exemplo, `http://<Virtual-Server-IP>/login.html`.
7. Em seguida, o cliente inicia a conexão HTTPS com a URL de redirecionamento que a envia para a `1.1.1.1`. Este é o endereço IP virtual do controlador. O cliente precisa validar o certificado do servidor ou ignorá-lo para ativar o túnel SSL.
8. Como a autenticação da Web externa está habilitada, a WLC redireciona o cliente para o servidor Web externo.
9. A URL de login de autenticação da Web externa é anexada a parâmetros como o `AP_Mac_Address`, o `client_url` (`www.cisco.com`) e o `action_URL` que o cliente precisa para entrar em contato com o servidor Web da controladora. **Observação:** O `action_URL` informa ao servidor Web que o nome de usuário e a senha estão armazenados no controlador. As credenciais devem ser enviadas de volta ao controlador para serem autenticadas.
10. A URL externa do servidor Web leva o usuário a uma página de login.
11. A página de login usa a entrada das credenciais do usuário e envia a solicitação de volta ao `action_URL`, por exemplo, `http://1.1.1.1/login.html`, do servidor Web da WLC.
12. O servidor Web da WLC envia o nome de usuário e a senha para autenticação.
13. A WLC inicia a solicitação do servidor RADIUS ou usa o banco de dados local na WLC e autentica o usuário.
14. Se a autenticação for bem-sucedida, o servidor Web da WLC encaminha o usuário para a URL de redirecionamento configurada ou para a URL com a qual o cliente iniciou, como `www.cisco.com`.
15. Se a autenticação falhar, o servidor Web da WLC redirecionará o usuário de volta ao URL de login do cliente.

Observação: para configurar a autenticação da Web externa para usar portas diferentes de HTTP e HTTPS, emita este comando:

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

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

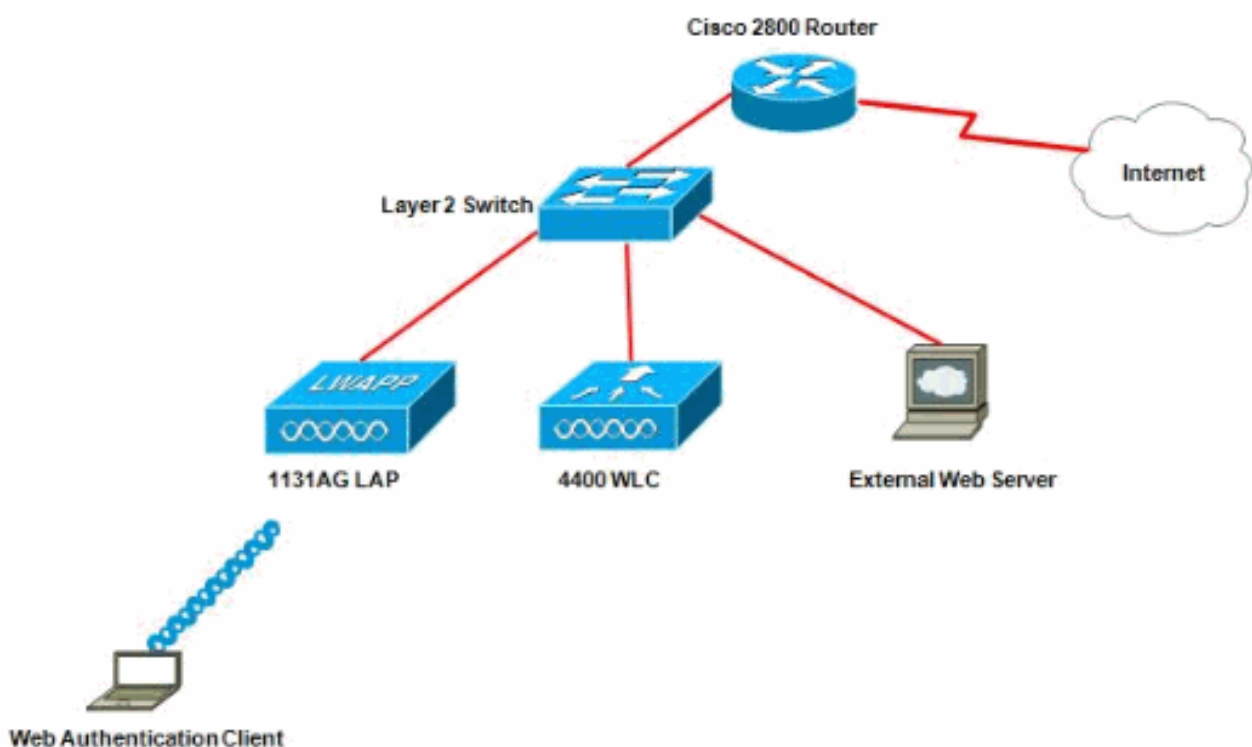
[Instalação de rede](#)

O exemplo de configuração usa essa configuração. Um LAP é registrado na WLC. Você precisa configurar um **convidado** WLAN para os usuários convidados e precisa habilitar a autenticação da

Web para os usuários. Você também precisa garantir que o controlador redirecione o usuário para a URL do servidor Web externo (para autenticação da Web externa). O servidor Web externo hospeda a página de logon da Web usada para autenticação.

As credenciais do usuário devem ser validadas em relação ao banco de dados local mantido no controlador. Após a autenticação bem-sucedida, os usuários devem ter acesso ao convidado da WLAN. O controlador e outros dispositivos precisam ser configurados para esta configuração.

Observação: você pode usar uma versão personalizada do script de logon, que será usada para autenticação da Web. Você pode fazer o download de um exemplo de script de autenticação da Web na página [Cisco Software Downloads](#). Por exemplo, para os controladores 4400, navegue para **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 4400 Series Wireless LAN Controllers > Cisco 4404 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle-1.0.1** e faça download do arquivo `webauth_bundle.zip`.



Observação: o pacote de autenticação da Web personalizado tem um limite de até 30 caracteres para nomes de arquivo. Certifique-se de que nenhum nome de arquivo dentro do pacote tenha mais de 30 caracteres.

Observação: este documento pressupõe que o DHCP, o DNS e os servidores Web externos estejam configurados. Consulte a documentação de terceiros apropriada para obter informações sobre como configurar o DHCP, o DNS e o servidor Web externo.

[Configurar](#)

Antes de configurar a WLC para autenticação externa da Web, você deve configurar a WLC para a operação básica e registrar os LAPs na WLC. Este documento pressupõe que o WLC foi configurado para operação básica e que os LAPs foram registrados no WLC. Consulte [Registro de AP Lightweight \(LAP\) em uma controladora Wireless LAN \(WLC\)](#) se você for um novo usuário tentando configurar a WLC para operação básica com LAPs.

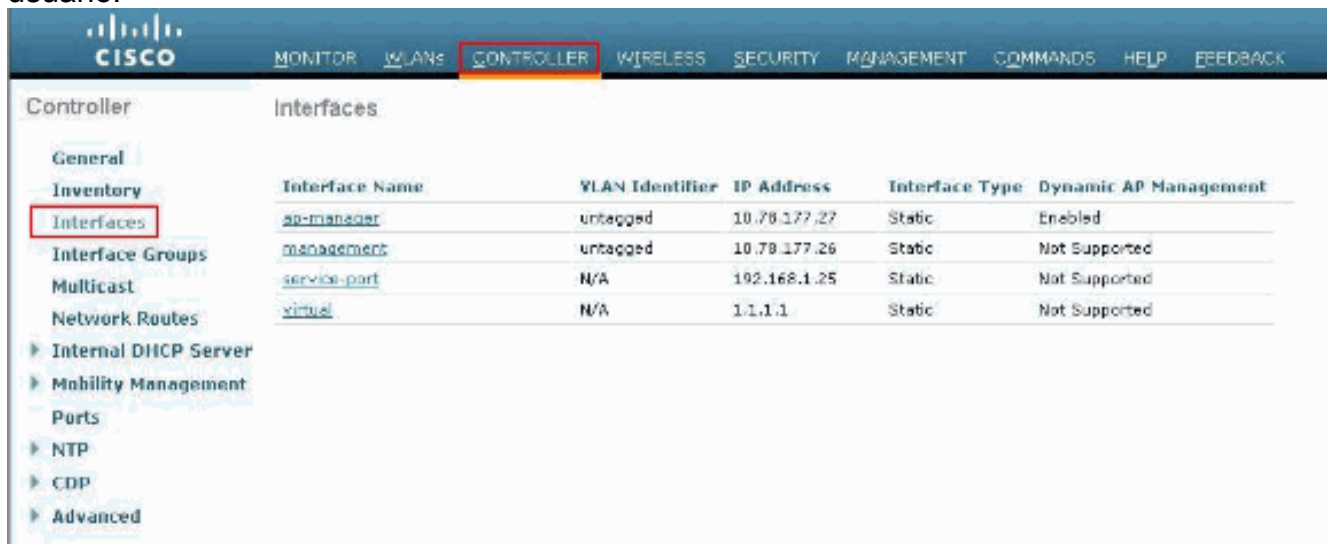
Conclua estes passos para configurar os LAPs e a WLC para esta configuração:

1. [Criar uma interface dinâmica para os usuários convidados](#)
2. [Criar uma ACL de pré-autenticação](#)
3. [Crie um banco de dados local no WLC para os usuários convidados](#)
4. [Configurar a WLC para autenticação externa da Web](#)
5. [Configurar a WLAN para usuários convidados](#)

[Criar uma interface dinâmica para os usuários convidados](#)

Conclua estas etapas para criar uma interface dinâmica para os usuários convidados:

1. Na GUI da WLC, escolha **Controllers > Interfaces**. A janela Interfaces é exibida. Essa janela lista as interfaces configuradas no controlador. Isso inclui as interfaces padrão, que são a interface de gerenciamento, a interface do gerenciador de aplicativos, a interface virtual e a interface da porta de serviço e as interfaces dinâmicas definidas pelo usuário.



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 em **New** para criar uma nova interface dinâmica.
3. Na janela **Interfaces > New**, insira o nome da interface e o ID da VLAN. Em seguida, clique em **Apply**. Neste exemplo, a interface dinâmica é chamada de **convidado** e a ID da VLAN é atribuída a **10**.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- ▶ Internal DHCP Server
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ Advanced

Interfaces > New

Interface Name

VLAN Id

4. Na janela **Interfaces > Edit**, para a interface dinâmica, insira o endereço IP, a máscara de sub-rede e o gateway padrão. Atribua-o a uma porta física na WLC e insira o endereço IP do servidor DHCP. Em seguida, clique em **Apply**.

The screenshot displays the Cisco WLC GUI for configuring an interface. The left sidebar shows navigation options like General, Inventory, Interfaces, and Advanced. The main content area is titled 'Interfaces > Edit' and contains several sections:

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

[Criar uma ACL de pré-autenticação](#)

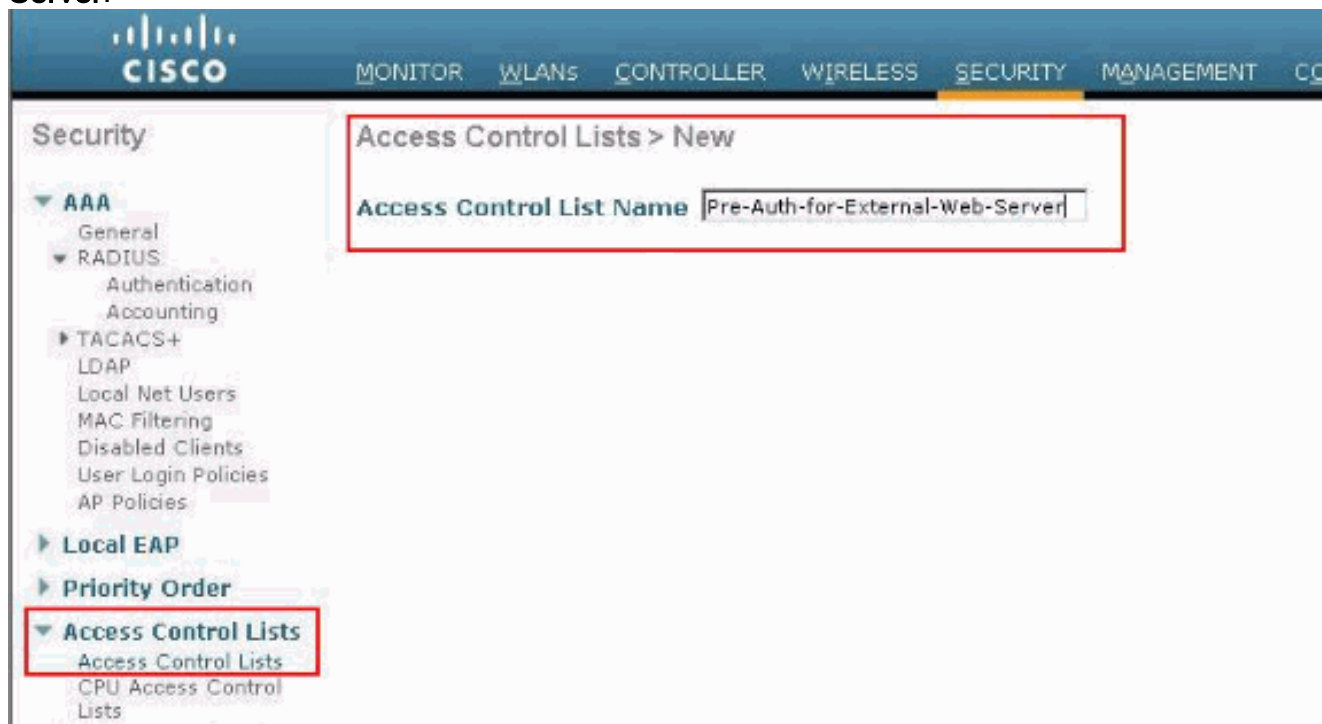
Ao usar um servidor Web externo para autenticação da Web, algumas das plataformas WLC precisam de uma ACL de pré-autenticação para o servidor Web externo (o Cisco 5500 Series Controller, um Cisco 2100 Series Controller, o Cisco 2000 Series Controller Network Module e o módulo de rede do controlador).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

No entanto, é uma boa prática configurar uma ACL de pré-autenticação para o servidor Web externo ao usar a autenticação da Web externa.

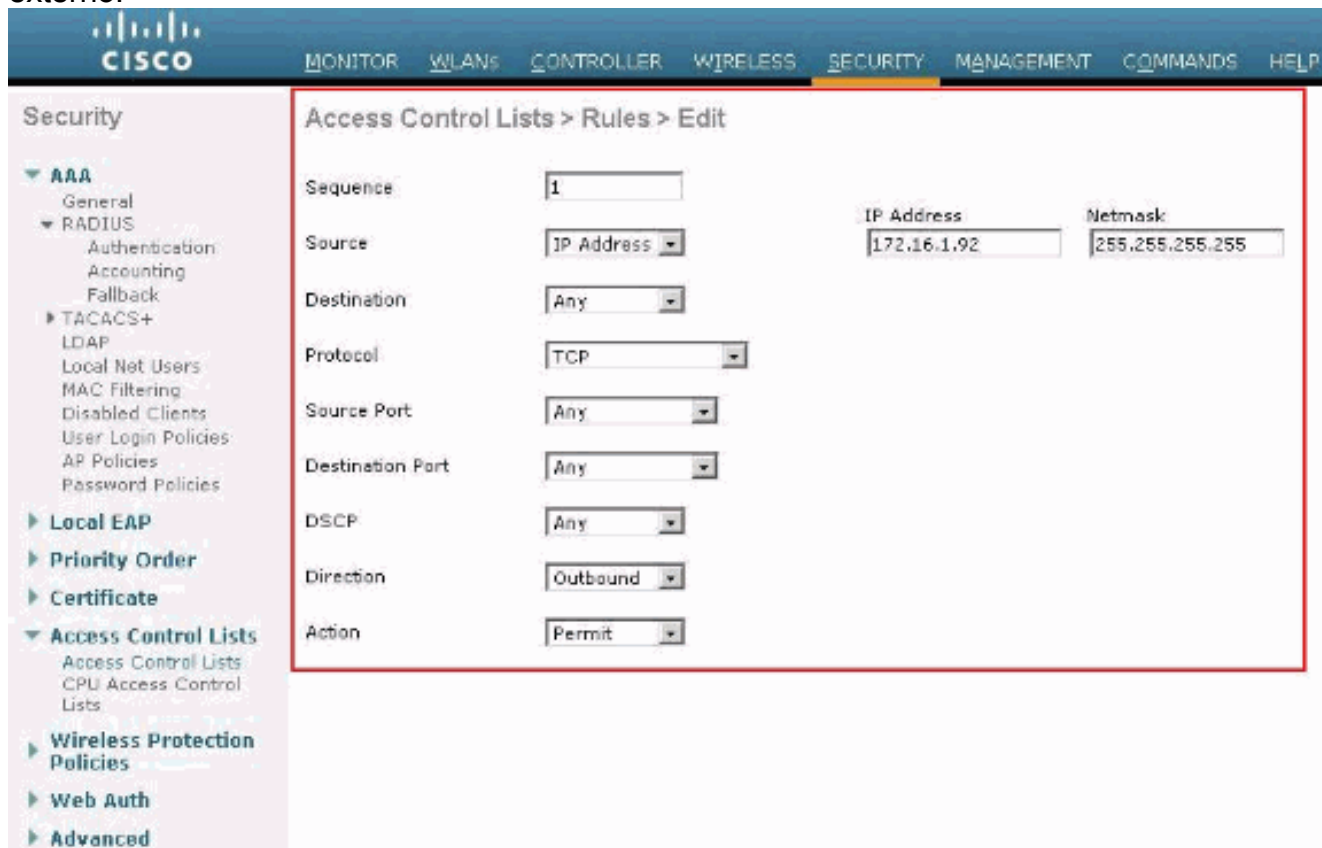
Conclua estas etapas para configurar a ACL de pré-autenticação para a WLAN:

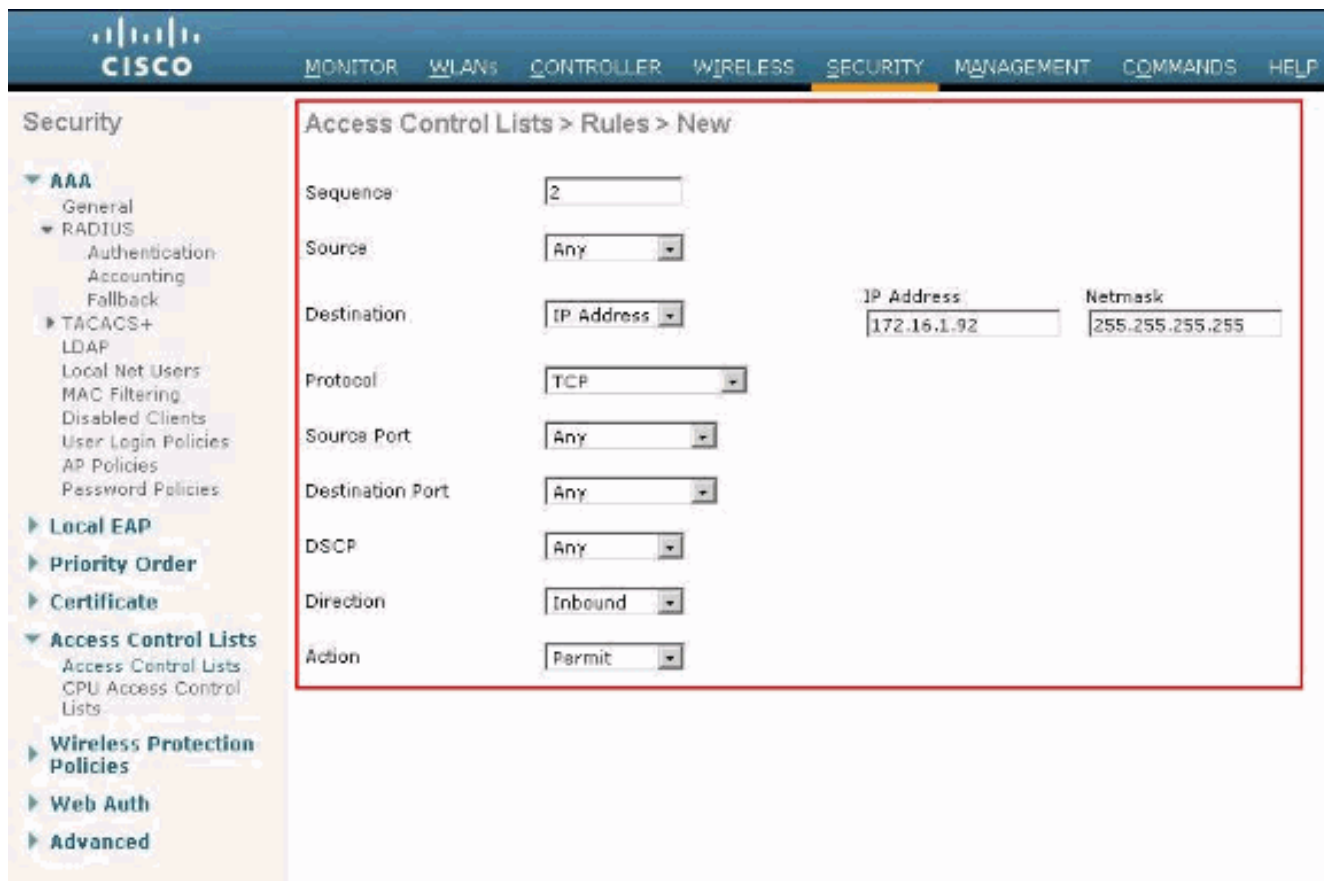
1. Na GUI da WLC, escolha **Security > Access Control Lists**. Essa janela permite exibir as ACLs atuais que são semelhantes às ACLs de firewall padrão.
2. Clique em **New** para criar uma nova ACL.
3. Insira o nome da ACL e clique em **Apply**. Neste exemplo, a ACL é chamada **Pre-Auth-for-**

External-Web-Server.

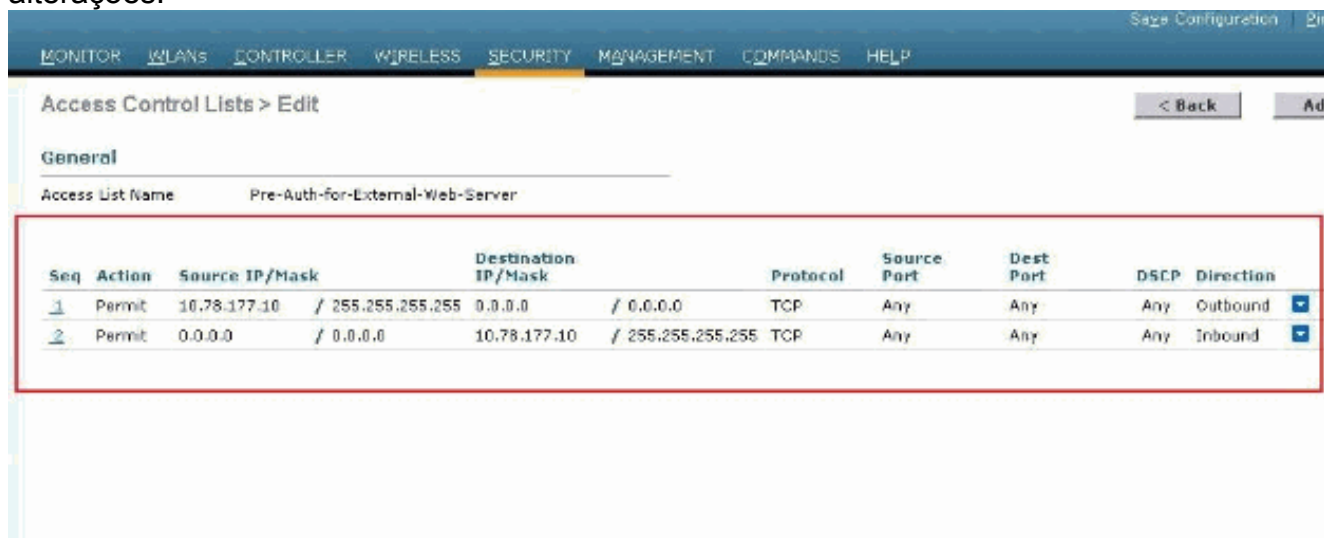


4. Para a nova ACL criada, clique em **Edit**. A janela ACL > Edit é exibida. Essa janela permite que o usuário defina novas regras ou modifique as regras da ACL existente.
5. Clique em **Adicionar nova regra**.
6. Defina uma regra de ACL que permita o acesso dos clientes ao servidor Web externo. Neste exemplo, 172.16.1.92 é o endereço IP do servidor Web externo.





7. Clique em **Apply** para confirmar as alterações.



[Crie um banco de dados local no WLC para os usuários convidados](#)

O banco de dados de usuários convidados pode ser armazenado no banco de dados local do Controlador de LAN sem fio ou pode ser armazenado fora do controlador.

Neste documento, o banco de dados local no controlador é usado para autenticar usuários. Você deve criar um usuário de rede local e definir uma senha para o login do cliente de autenticação da Web. Conclua estes passos para criar o banco de dados do usuário no WLC:

1. Na GUI do WLC, selecione **Security (Segurança)**.
2. Clique em **Local Net Users (Usuários da rede local)** no menu AAA à esquerda.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the Security menu with options like AAA, RADIUS, TACACS+, LDAP, Local Net Users (highlighted with 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 contains a table with the following header: 'User Name', 'WLAN Profile', 'Guest User', 'Role', and 'Description'.

3. Clique em **New (Novo)** para criar um novo usuário. É exibida uma nova janela, que solicita o nome de usuário e a senha.
4. Digite um User Name (Nome de usuário) e uma Password (Senha) para criar um novo usuário e, em seguida, confirme a senha que deseja usar. Neste exemplo, é criado o usuário nomeado **User1 (Usuário1)**.
5. Adicione uma descrição, se desejar. Neste exemplo, é usada a descrição **Guest User1 (Usuário1 convidado)**.
6. Clique em **Apply** para salvar a configuração do novo usuário.

The screenshot shows the Cisco WLC GUI with the 'Security' tab selected. The left sidebar shows the navigation menu with 'Local Net Users' highlighted. The main content area displays the 'Local Net Users > New' configuration form. The form fields are as follows:

- User Name: User1
- Password: [masked]
- Confirm Password: [masked]
- Guest User:
- Lifetime (seconds): 86400
- Guest User Role:
- WLAN Profile: Guest
- Description: GuestUser1

Below the configuration page, a table lists the created user:

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

7. Repita as etapas 3 a 6 para adicionar outros usuários ao banco de dados.

[Configurar a WLC para autenticação externa da Web](#)

A próxima etapa é configurar a WLC para a autenticação da Web externa. Conclua estes passos:

1. Na GUI do controlador, selecione **Security (Segurança) > Autorização da Web > Web Login Page (Página de login da Web)** para acessar a Página de login da Web.
2. Na caixa suspensa Tipo de autenticação da Web, escolha **Externo (Redirecionar para servidor externo)**.
3. Na seção **Servidor Web externo**, adicione o novo servidor Web externo.
4. No campo **Redirect URL after login**, digite o URL da página para a qual o usuário final será redirecionado após a autenticação bem-sucedida. No campo **URL de autenticação da Web externa**, insira a URL onde a página de logon está armazenada no servidor Web externo.

Web Login Page

Web Authentication Type: (Dropdown menu open with options: Internal (Default), 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).

Show Hide

Headline:

Message:

External Web Servers

Web Server IP Address
<input type="text"/>

Web Login Page

Web Authentication Type: (Dropdown menu)

Redirect URL after login:

External Webauth URL:

External Web Servers

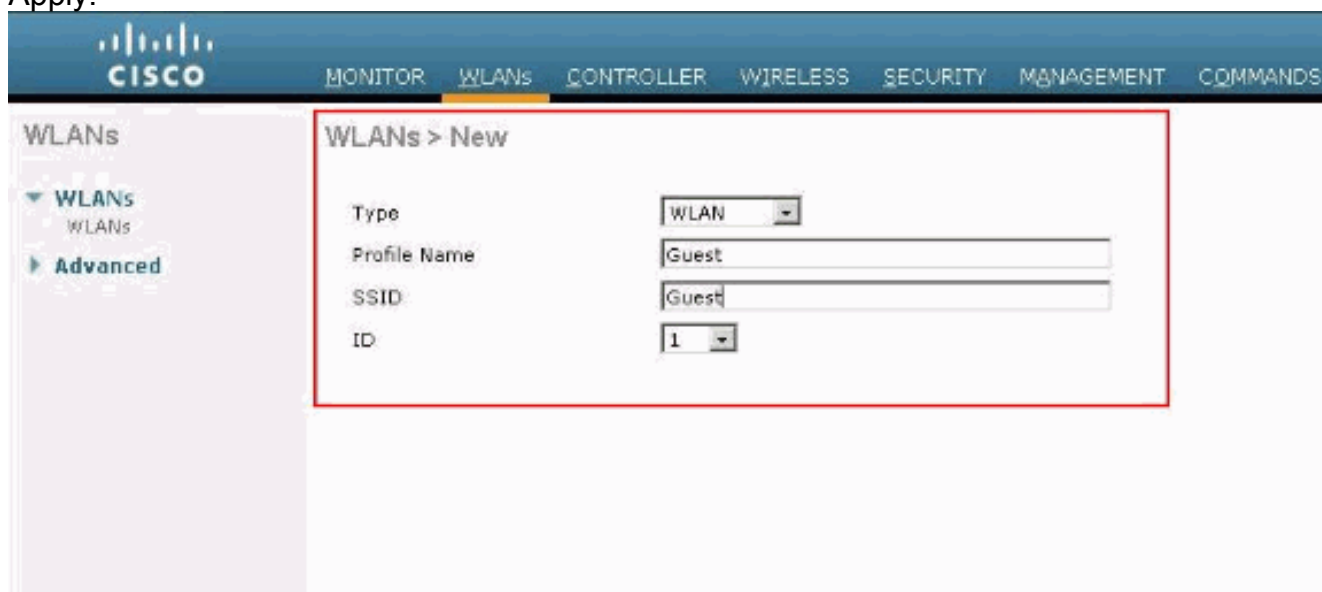
Web Server IP Address
<input type="text" value="172.16.1.92"/>

Observação: nas versões 5.0 e posteriores da WLC, a página de logout para autenticação da Web também pode ser personalizada. Consulte a seção [Atribuir páginas de login, falha de login e logout por WLAN](#) do *Guia de Configuração da Controladora Wireless LAN, 5.2* para obter mais informações sobre como configurá-la.

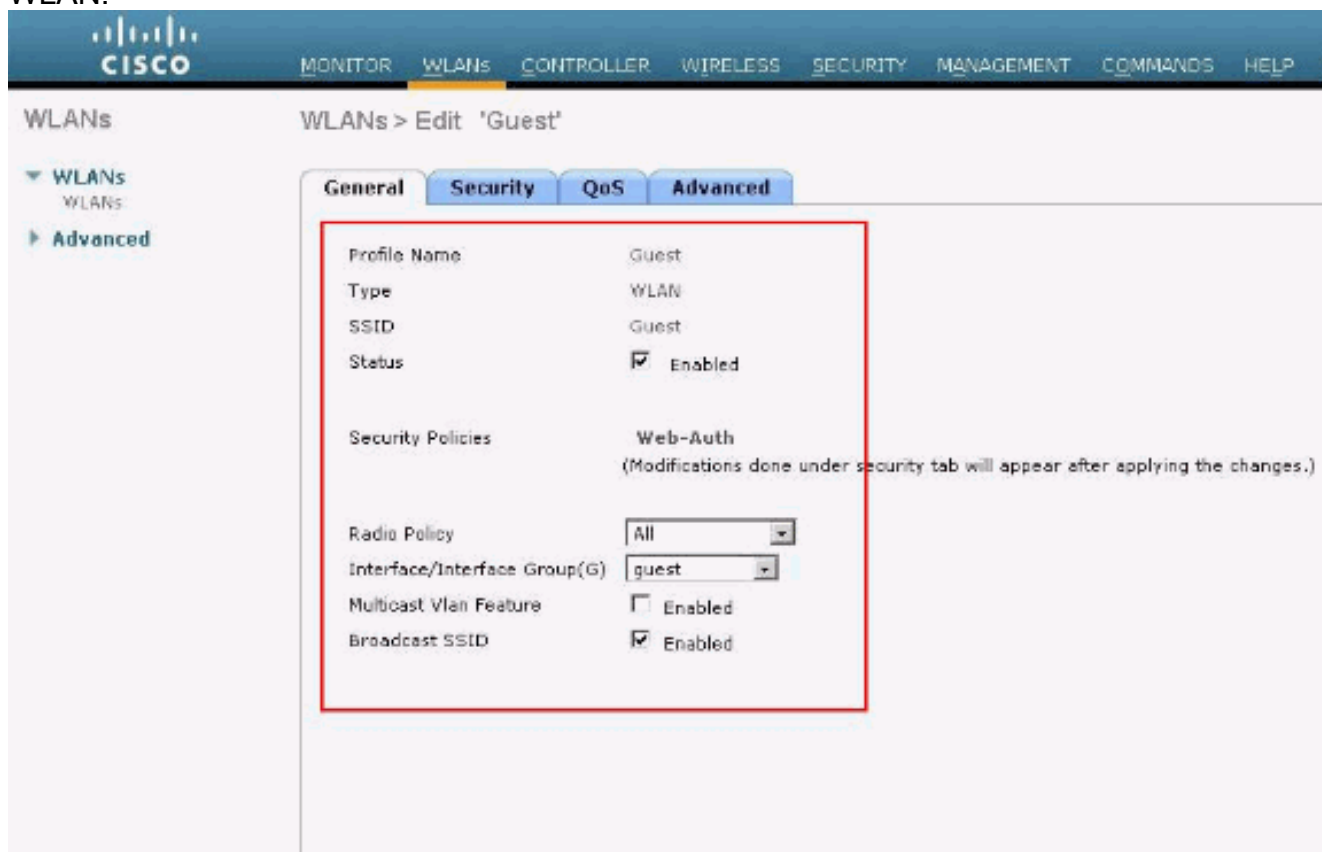
[Configurar a WLAN para usuários convidados](#)

A etapa final é criar WLANs para os usuários convidados. Conclua estes passos:

1. Clique em **WLANs** na GUI do controlador para criar uma WLAN. A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.
2. Clique em **Novo** para configurar uma nova WLAN. Neste exemplo, a WLAN é chamada de **Guest** e o ID da WLAN é 1.
3. Clique em **Apply**.

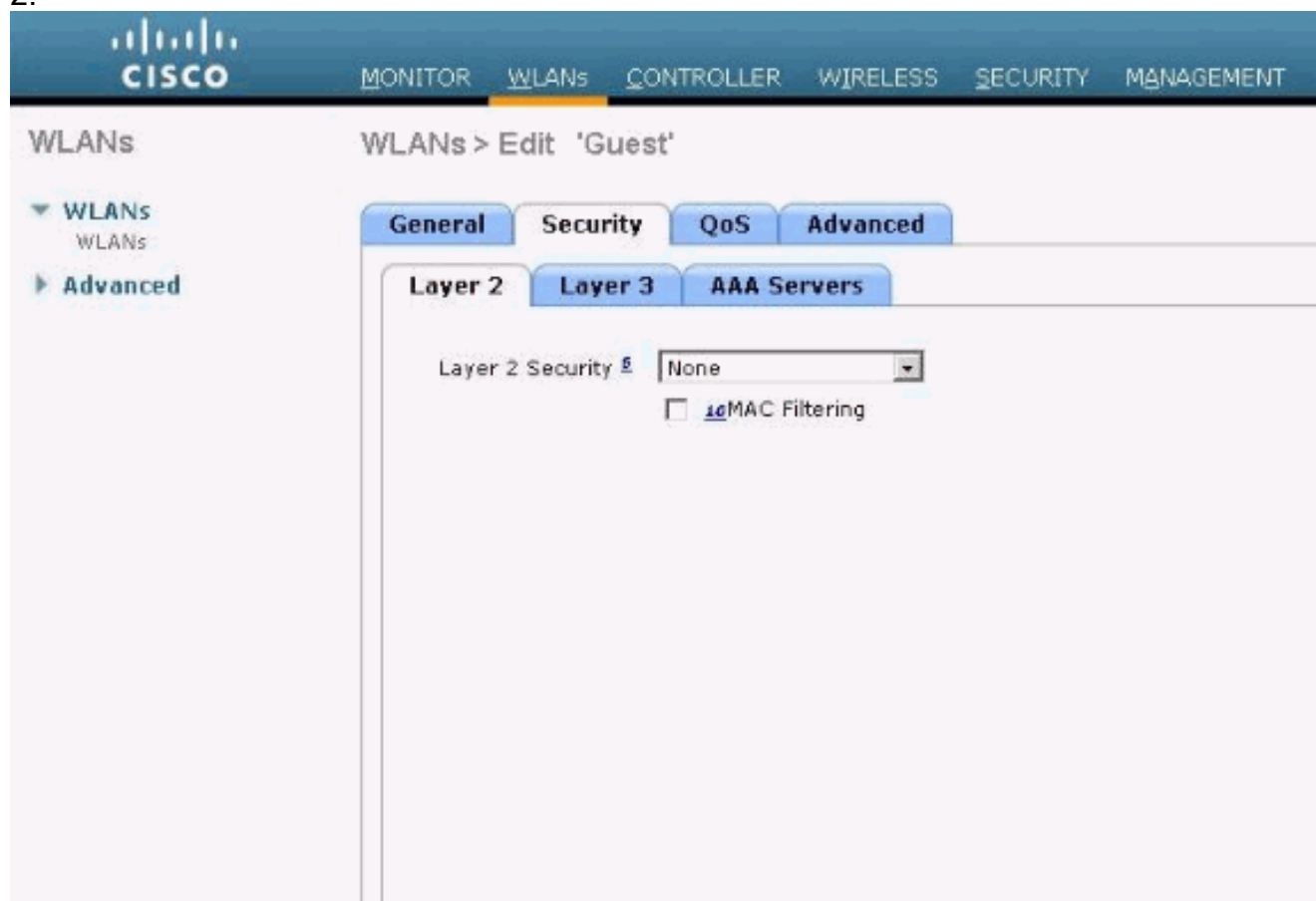


4. Na janela WLAN > Editar, defina os parâmetros específicos para a WLAN. Para a WLAN convidada, na guia Geral, escolha a interface apropriada no campo Nome da Interface. Este exemplo mapeia a interface dinâmica **guest** que foi criada anteriormente para o convidado da WLAN.

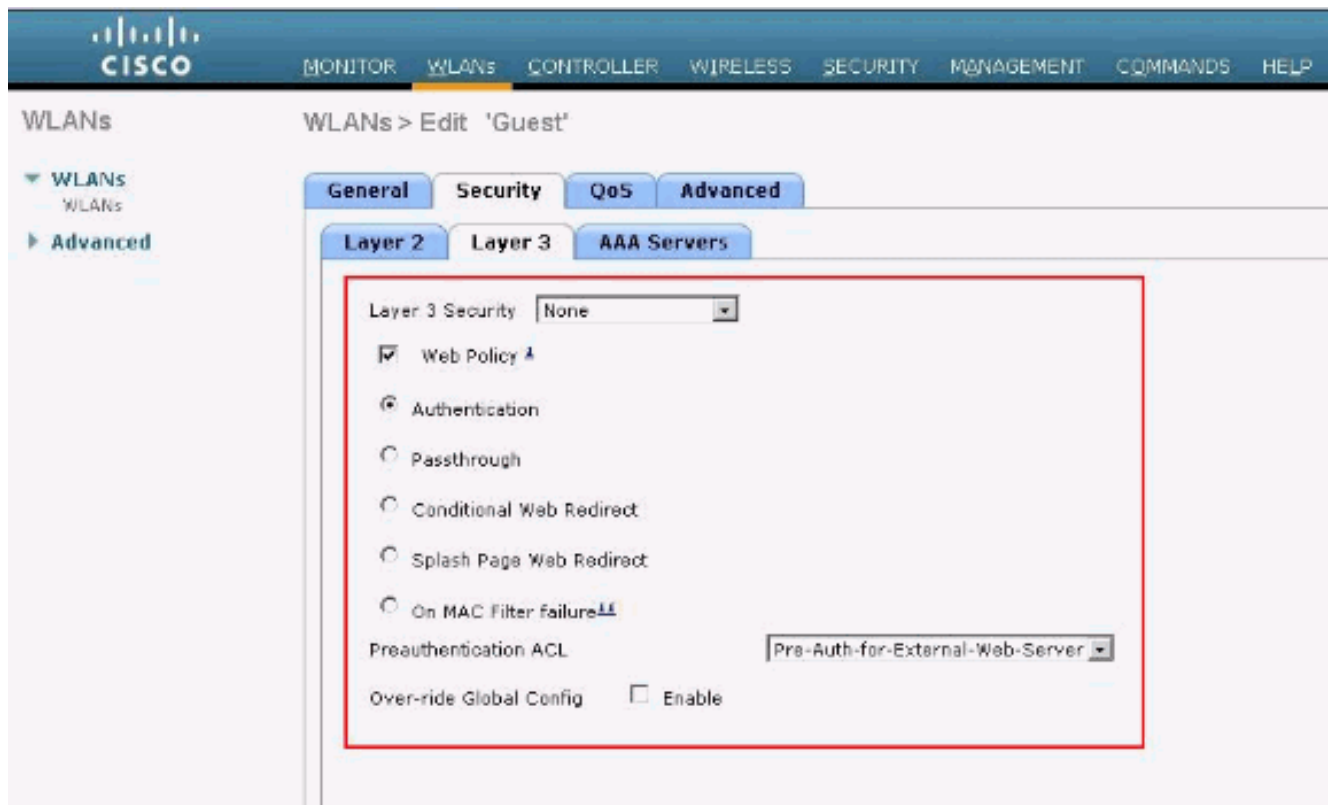


Vá até a guia Segurança. Em Layer 2 Security, **None** é selecionado neste exemplo. **Observação:** a autenticação da Web não é suportada com a autenticação 802.1x. Isso significa que você não pode escolher 802.1x ou um WPA/WPA2 com 802.1x como a

segurança de Camada 2 quando usar a autenticação da Web. A autenticação da Web é suportada com todos os outros parâmetros de segurança de Camada 2.



No campo Layer 3 Security, marque a caixa de seleção **Web Policy** e escolha a opção **Authentication**. Esta opção é escolhida porque a autenticação da Web é usada para autenticar os clientes convidados sem fio. Escolha a ACL de pré-autenticação apropriada no menu suspenso. Neste exemplo, a ACL de pré-autenticação criada anteriormente é usada. Clique em Apply.



Verificar

O cliente sem fio é ativado e o usuário digita o URL, como www.cisco.com, no navegador da Web. Como o usuário não foi autenticado, a WLC redireciona o usuário para a URL de login da Web externa.

O usuário é solicitado a fornecer as credenciais de usuário. Depois que o usuário envia o nome de usuário e a senha, a página de login insere as credenciais do usuário e, ao enviar, envia a solicitação de volta ao exemplo `action_URL`, `http://1.1.1.1/login.html`, do servidor Web da WLC. Isso é fornecido como um parâmetro de entrada para o URL de redirecionamento do cliente, onde 1.1.1.1 é o endereço de interface virtual no switch.

A WLC autentica o usuário com base no banco de dados local configurado na WLC. Após a autenticação bem-sucedida, o servidor Web da WLC encaminha o usuário para a URL de redirecionamento configurada ou para a URL com a qual o cliente iniciou, como www.cisco.com.

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

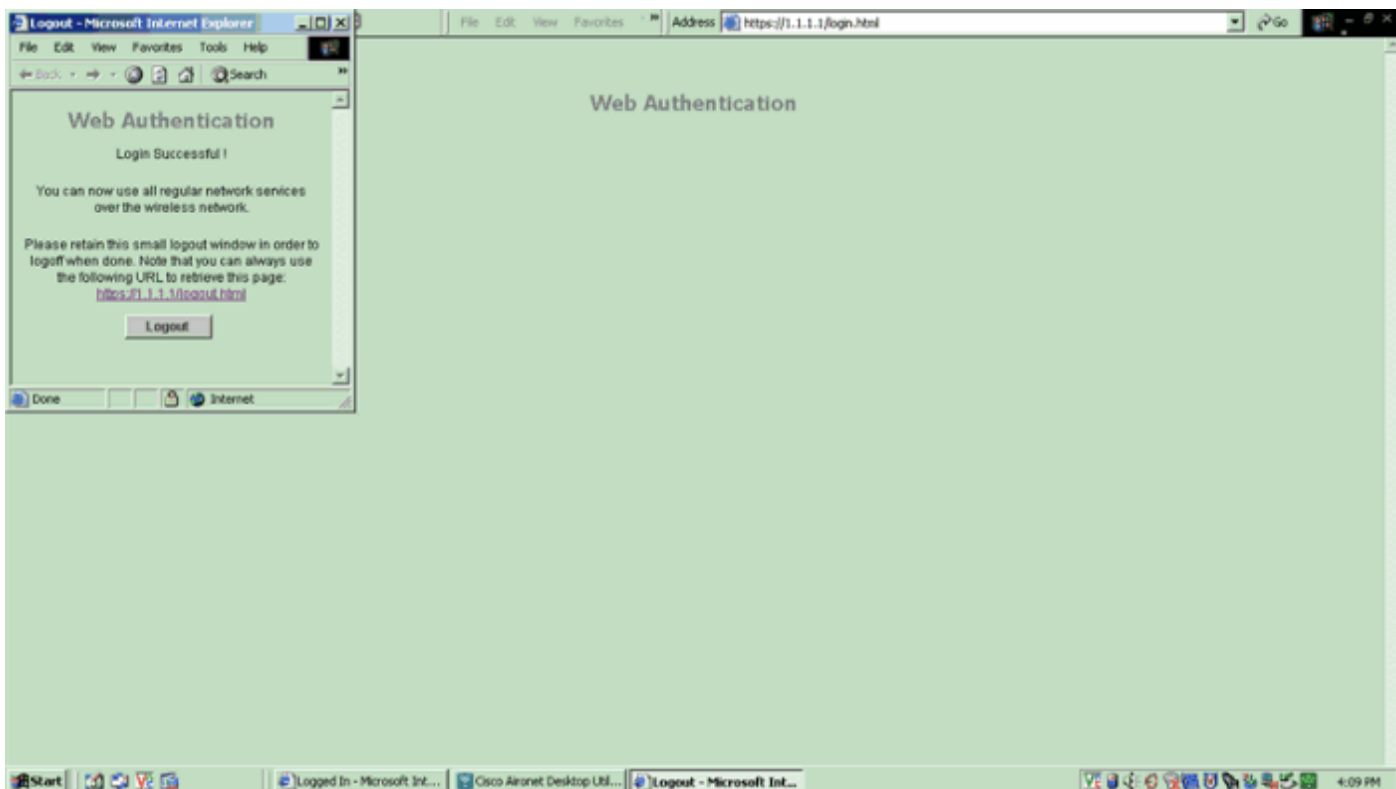
- ⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- ✔ The security certificate date is valid.
- ✔ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Web Authentication

User Name

Password



Troubleshoot

Use estes comandos debug para fazer o troubleshooting da sua configuração.

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

Use esta seção para resolver problemas de configuração.

Cientes Redirecionados para Servidor de Autenticação da Web Externo Recebem um Aviso de Certificado

Problema: quando os clientes são redirecionados para o servidor de autenticação da Web externo da Cisco, eles recebem um aviso de certificado. Há um certificado válido no servidor e, se você se conectar ao servidor de autenticação da Web externo diretamente, o aviso do certificado não será recebido. Isso ocorre porque o endereço IP virtual (1.1.1.1) da WLC é apresentado ao cliente em vez do endereço IP real do servidor de autenticação da Web externo que está associado ao certificado?

Solução: Sim. Se você executar ou não a autenticação da Web local ou externa, você ainda pressionará o servidor da Web interno no controlador. Quando você redireciona para um servidor Web externo, ainda recebe o aviso de certificado do controlador, a menos que tenha um certificado válido no próprio controlador. Se o redirecionamento for enviado para https, você receberá o aviso de certificado do controlador e do servidor Web externo, a menos que ambos

tenham um certificado válido.

Para se livrar dos avisos de certificado, você precisa ter um certificado de nível raiz emitido e baixado em seu controlador. O certificado é emitido para um nome de host e você coloca esse nome de host na caixa Nome de host DNS sob a interface virtual no controlador. Você também precisa adicionar o nome do host ao servidor DNS local e apontá-lo para o endereço IP virtual (1.1.1.1) do WLC.

Consulte [Geração de CSR \(Certificate Signing Request\) para um Certificado de Terceiros em uma WLC \(WLAN Controller\)](#) para obter mais informações.

Erro: "a página não pode ser exibida"

Problema: Depois que o controlador é atualizado para 4.2.61.0, a mensagem de erro "a página não pode ser exibida " é exibida quando você usa uma página da Web baixada para autenticação da Web. Isso funcionou bem antes da atualização. A página da Web interna padrão é carregada sem nenhum problema .

Solução: a partir da versão 4.2 e posterior da WLC, um novo recurso é introduzido onde você pode ter várias páginas de login personalizadas para autenticação da Web.

Para que a página da Web seja carregada corretamente, não é suficiente definir o tipo de autenticação da Web como **personalizado** globalmente na página **Segurança > Autenticação da Web > Logon na Web**. Ele também deve ser configurado em uma WLAN específica . Para isso, conclua essas etapas:

1. Faça login na GUI do WLC.
2. Clique na guia **WLANs** e acesse o perfil da WLAN configurada para autenticação na Web.
3. Na página WLAN > Edit, clique na guia **Security**. Em seguida, escolha **Layer 3**.
4. Nesta página, escolha **None** como a Segurança de Camada 3.
5. Marque a caixa **Web Policy** e escolha a opção **Authentication**.
6. Marque a caixa Over-ride Global Config **Enable**, escolha **Customized (Downloaded)** como o Web Auth Type e selecione a página de login desejada no menu suspenso **Login Pagepull**. Clique em Apply.

Informações Relacionadas

- [Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio](#)
- [Vídeo: Autenticação da Web em Cisco Wireless LAN Controllers \(WLCs\)](#)
- [VLANs no exemplo de configuração de Wireless LAN Controllers](#)
- [Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight](#)
- [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.

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.