

Configurazione dell'autenticazione Web esterna con i WLC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Processo di autenticazione Web esterno](#)

[Installazione della rete](#)

[Configurazione](#)

[Creazione di un'interfaccia dinamica per gli utenti guest](#)

[Creazione di un ACL di preautenticazione](#)

[Creare un database locale sul WLC per gli utenti guest](#)

[Configurare il WLC per l'autenticazione Web esterna](#)

[Configurazione della WLAN per gli utenti guest](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[I client reindirizzati al server di autenticazione Web esterno ricevono un avviso di certificato](#)

[Errore: impossibile visualizzare la pagina](#)

[Informazioni correlate](#)

[Introduzione](#)

Questo documento spiega come usare un server Web esterno per configurare un controller WLC per l'autenticazione Web.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC
- Conoscenze base di LWAPP (Lightweight Access Point Protocol) e di CAPWAP (Control and Provisioning of Wireless Access Point)
- Informazioni su come configurare un server Web esterno
- Informazioni su come configurare i server DHCP e DNS

Componenti usati

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

- Cisco 4400 WLC con firmware versione 7.0.116.0
- Cisco serie 1131AG LAP
- Cisco 802.11a/b/g Wireless Client Adapter con firmware versione 3.6
- Server Web esterno che ospita la pagina di accesso per l'autenticazione Web
- Server DNS e DHCP per la risoluzione degli indirizzi e l'allocazione degli indirizzi IP ai client wireless

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

Convenzioni

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

Premesse

L'autenticazione Web è una funzione di sicurezza di livello 3 che impedisce al controller di autorizzare il traffico IP (ad eccezione dei pacchetti relativi a DHCP e DNS) da un determinato client fino a quando il client non ha fornito correttamente un nome utente e una password validi. L'autenticazione Web è un metodo di autenticazione semplice che non richiede un'utilità supplicant o client.

L'autenticazione Web può essere eseguita utilizzando:

- Finestra di accesso predefinita sul WLC
- Versione modificata della finestra di accesso predefinita sul WLC
- Finestra di accesso personalizzata configurata su un server Web esterno (autenticazione Web esterna)
- Una finestra di accesso personalizzata da scaricare sul controller

In questo documento viene fornito un esempio di configurazione per spiegare come configurare il WLC in modo che utilizzi uno script di accesso da un server Web esterno.

Processo di autenticazione Web esterno

Con l'autenticazione Web esterna, la pagina di accesso utilizzata per l'autenticazione Web viene memorizzata su un server Web esterno. Questa è la sequenza di eventi che si verificano quando un client wireless tenta di accedere a una rete WLAN per la quale è abilitata l'autenticazione Web esterna:

1. Il client (utente finale) si connette alla WLAN e apre un browser Web e immette un URL, ad esempio www.cisco.com.
2. Il client invia una richiesta DNS a un server DNS per risolvere www.cisco.com in indirizzo IP.

3. Il WLC inoltra la richiesta al server DNS che, a sua volta, risolve `www.cisco.com` in indirizzo IP e invia una risposta DNS. Il controller inoltra la risposta al client.
4. Il client tenta di avviare una connessione TCP con l'indirizzo IP `www.cisco.com` inviando il pacchetto TCP SYN all'indirizzo IP `www.cisco.com`.
5. Il WLC ha delle regole configurate per il client e può quindi fungere da proxy per `www.cisco.com`. Invia un pacchetto TCP SYN-ACK al client con origine come indirizzo IP di `www.cisco.com`. Il client restituisce un pacchetto TCP ACK per completare l'handshake TCP a tre vie e la connessione TCP viene stabilita completamente.
6. Il client invia un pacchetto HTTP GET destinato a `www.google.com`. Il WLC intercetta questo pacchetto e lo invia per la gestione del reindirizzamento. Il gateway applicazioni HTTP prepara un corpo HTML e lo invia come risposta al comando HTTP GET richiesto dal client. Con questo codice HTML il client passa all'URL predefinito della pagina Web del WLC, ad esempio `http://<Virtual-Server-IP>/login.html`.
7. Il client avvia quindi la connessione HTTPS all'URL di reindirizzamento che lo invia alla versione 1.1.1.1. Indirizzo IP virtuale del controller. Il client deve convalidare il certificato del server o ignorarlo per attivare il tunnel SSL.
8. Poiché l'autenticazione Web esterna è abilitata, il WLC reindirizza il client al server Web esterno.
9. All'URL di accesso con autenticazione Web esterna vengono aggiunti parametri quali `AP_Mac_Address`, `client_url` (`www.cisco.com`) e `action_URL` necessari al client per contattare il server Web del controller. **Nota:** `Action_URL` indica al server Web che il nome utente e la password sono memorizzati sul controller. Le credenziali devono essere rinviate al controller per essere autenticate.
10. L'URL del server Web esterno consente all'utente di accedere a una pagina di accesso.
11. La pagina di accesso accetta l'input delle credenziali dell'utente e invia nuovamente la richiesta all'URL_azione, ad esempio `http://1.1.1.1/login.html`, del server Web WLC.
12. Il server Web WLC invia nome utente e password per l'autenticazione.
13. Il WLC avvia la richiesta del server RADIUS o utilizza il database locale sul WLC e autentica l'utente.
14. Se l'autenticazione ha esito positivo, il server Web WLC inoltra l'utente all'URL di reindirizzamento configurato o all'URL utilizzato dal client, ad esempio `www.cisco.com`.
15. Se l'autenticazione non riesce, il server Web WLC reindirizza l'utente all'URL di accesso del cliente.

Nota: per configurare l'autenticazione Web esterna per l'utilizzo di porte diverse da HTTP e HTTPS, eseguire questo comando:

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

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

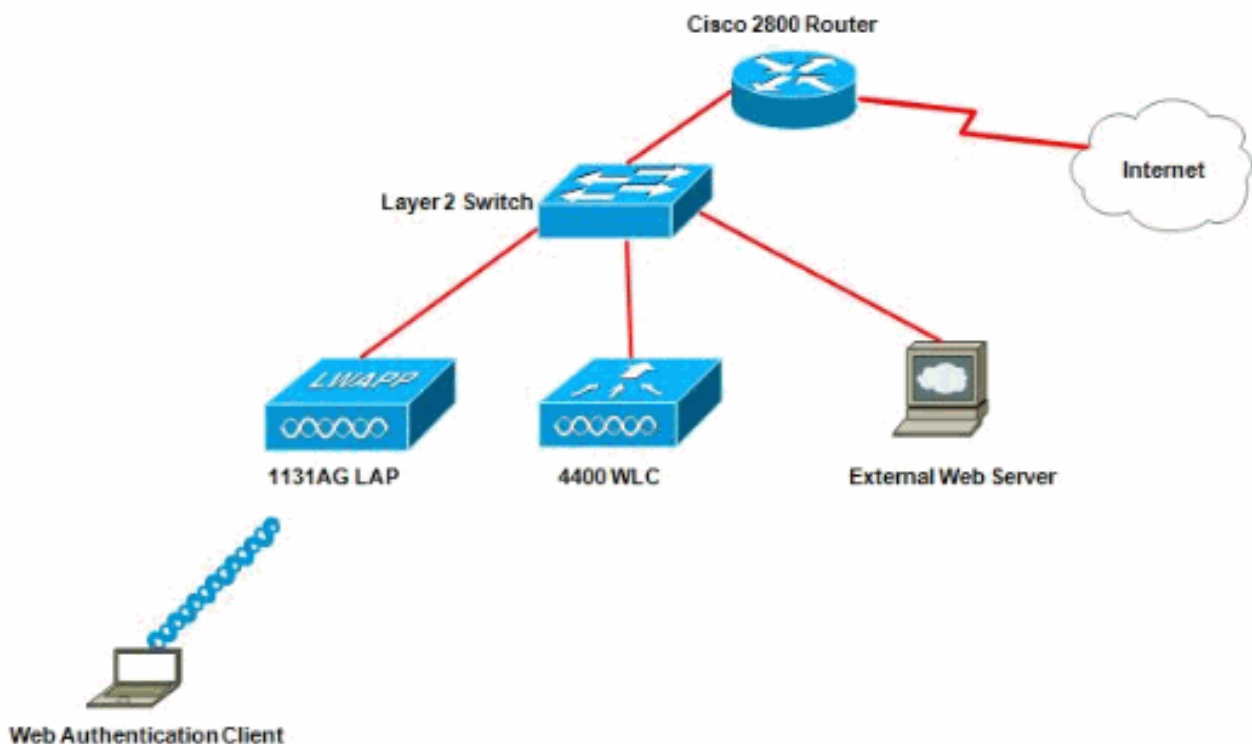
[Installazione della rete](#)

L'esempio di configurazione utilizza questa impostazione. Un LAP è registrato sul WLC. È necessario configurare un **guest** WLAN per gli utenti guest e abilitare l'autenticazione Web per gli utenti. È inoltre necessario assicurarsi che il controller reindirizzi l'utente all'URL del server Web esterno (per l'autenticazione Web esterna). Il server Web esterno ospita la pagina di accesso Web utilizzata per l'autenticazione.

Le credenziali dell'utente devono essere convalidate rispetto al database locale gestito sul

controller. Una volta completata l'autenticazione, agli utenti deve essere consentito l'accesso al guest WLAN. Per questa installazione è necessario configurare il controller e gli altri dispositivi.

Nota: è possibile utilizzare una versione personalizzata dello script di accesso, che verrà utilizzata per l'autenticazione Web. È possibile scaricare uno script di autenticazione Web di esempio dalla pagina [Download di software Cisco](#). Ad esempio, per i controller 4400, selezionare **Prodotti > Wireless > Wireless LAN Controller > Controller standalone > Cisco serie 4400 Wireless LAN Controller > Cisco 4404 Wireless LAN Controller > Software sullo chassis > Wireless Lan Controller Web Authentication Bundle-1.0.1** e scaricare il file `webauth_bundle.zip`.



Nota: il pacchetto di autenticazione Web personalizzato prevede un limite massimo di 30 caratteri per i nomi di file. Assicuratevi che i nomi di file all'interno del fascio non siano più lunghi di 30 caratteri.

Nota: in questo documento si presume che i server DHCP, DNS e Web esterni siano configurati. Per informazioni su come configurare DHCP, DNS e il server Web esterno, consultare la documentazione di terze parti appropriata.

Configurazione

Prima di configurare il WLC per l'autenticazione Web esterna, è necessario configurare il WLC per il funzionamento di base e registrare i LAP sul WLC. In questo documento si presume che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se un nuovo utente sta cercando di configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla [registrazione di un Lightweight AP \(LAP\)](#) su un Wireless LAN Controller (WLC).

Per configurare i LAP e i WLC per questa configurazione, completare la procedura seguente:

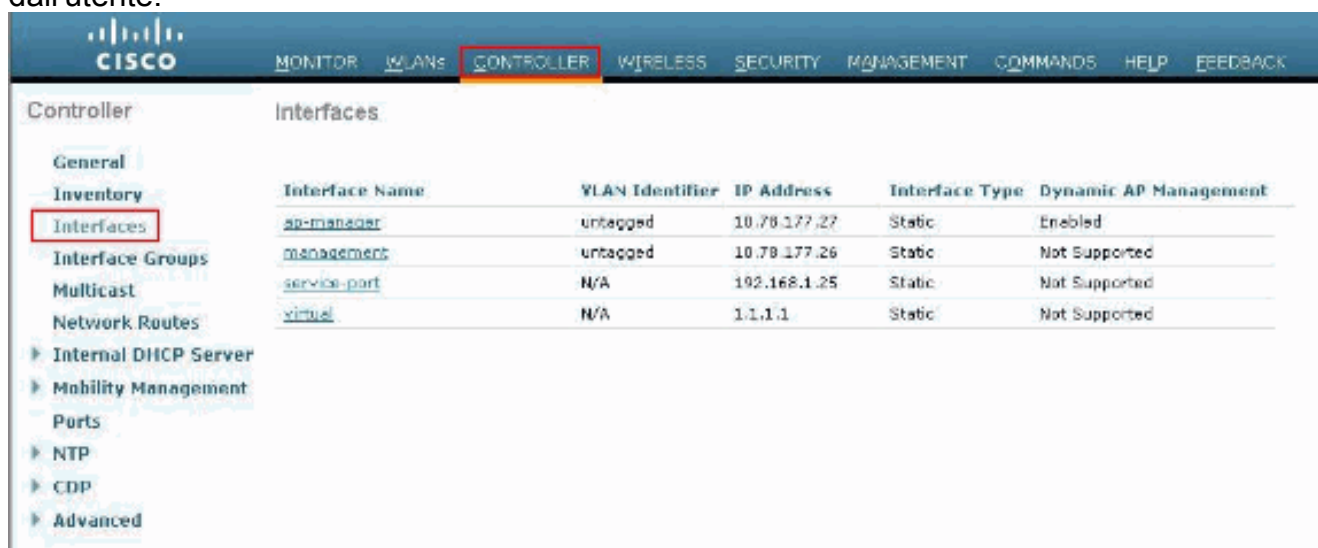
1. [Creazione di un'interfaccia dinamica per gli utenti guest](#)
2. [Creazione di un ACL di preautenticazione](#)

3. [Creare un database locale sul WLC per gli utenti guest](#)
4. [Configurare il WLC per l'autenticazione Web esterna](#)
5. [Configurazione della WLAN per gli utenti guest](#)

Creazione di un'interfaccia dinamica per gli utenti guest

Completare questi passaggi per creare un'interfaccia dinamica per gli utenti guest:

1. Dall'interfaccia utente del WLC, scegliere **Controller > Interfacce**. Viene visualizzata la finestra Interfacce. In questa finestra sono elencate le interfacce configurate sul controller. Sono incluse le interfacce predefinite, ovvero l'interfaccia di gestione, l'interfaccia ap-manager, l'interfaccia virtuale e l'interfaccia della porta di servizio e le interfacce dinamiche definite dall'utente.



The screenshot shows the Cisco WLC Controller configuration page. The 'CONTROLLER' tab is 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. The rows listed are: 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), and virtual (N/A, 1.1.1.1, Static, Not Supported). The 'Interfaces' menu item in the left sidebar is highlighted with a red box.

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. Per creare una nuova interfaccia dinamica, fare clic su **New** (Nuovo).
3. Nella finestra **Interfacce > Nuovo**, immettere il nome dell'interfaccia e l'ID VLAN. Quindi, fare clic su **Applica**. Nell'esempio, il nome dell'interfaccia dinamica è **guest** e l'ID VLAN è assegnato **10**.

The screenshot shows the Cisco WLC configuration 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, a sidebar lists various configuration categories under the heading 'Controller'. The main 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. Nella finestra **Interfacce > Modifica**, immettere l'indirizzo IP, la subnet mask e il gateway predefinito per l'interfaccia dinamica. Assegnarla a una porta fisica sul WLC e immettere l'indirizzo IP del server DHCP. Quindi fare clic su **Apply** (Applica).

The screenshot shows the Cisco WLC configuration interface for an interface named 'guest'. The configuration is organized into 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: 0)
- Physical Information:** Port Number (input field: 2), Backup Port (input field: 0), Active Port (input field: 0), Enable Dynamic AP Management (checkbox)
- Interface Address:** VLAN Identifier (input field: 10), IP Address (input field: 172.18.1.10), Netmask (input field: 255.255.255.0), Gateway (input field: 172.18.1.20)
- DHCP Information:** Primary DHCP Server (input field: 172.18.1.20), Secondary DHCP Server (input field)
- Access Control List:** ACL Name (dropdown menu: none)

[Creazione di un ACL di preautenticazione](#)

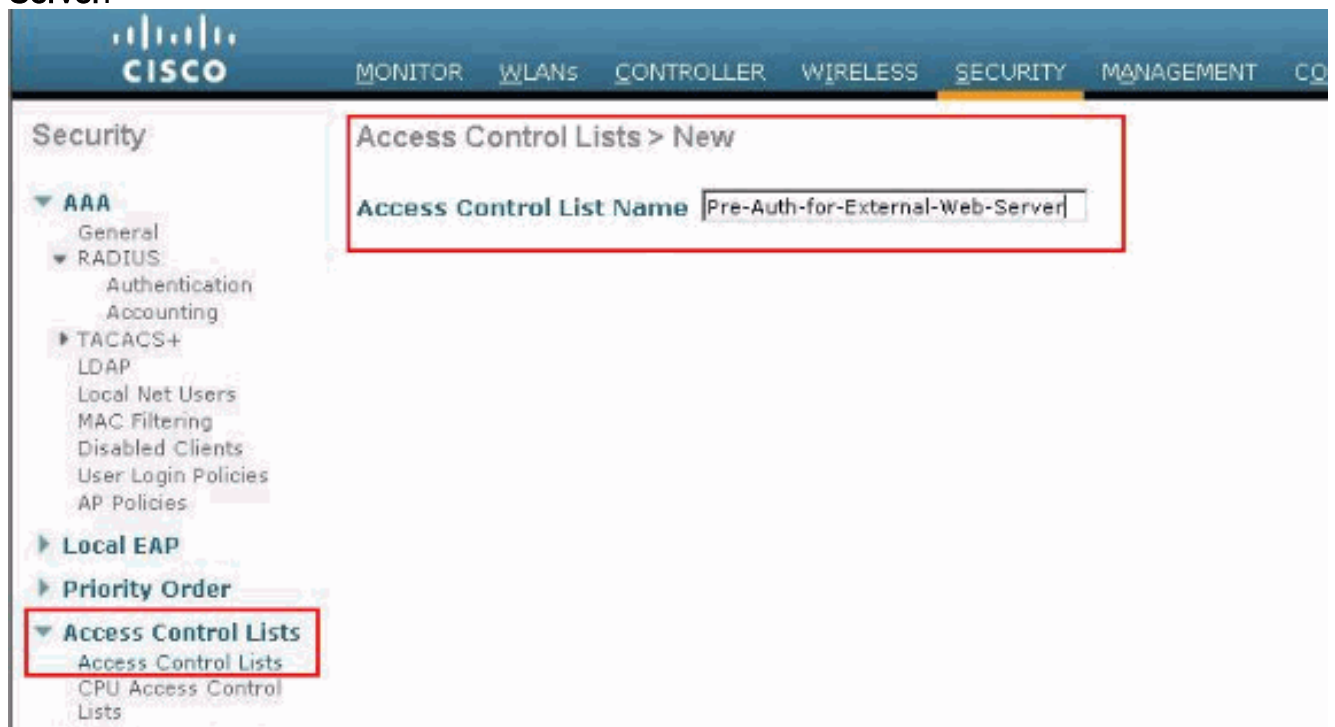
Se si usa un server Web esterno per l'autenticazione Web, alcune piattaforme WLC devono avere un ACL di preautenticazione per il server Web esterno (il controller Cisco serie 5500, un controller Cisco serie 2100, Cisco serie 2000 e il modulo di rete del controller). Per le altre piattaforme WLC, l'ACL di preautenticazione non è obbligatorio.

Tuttavia, è buona norma configurare un ACL di preautenticazione per il server Web esterno quando si utilizza l'autenticazione Web esterna.

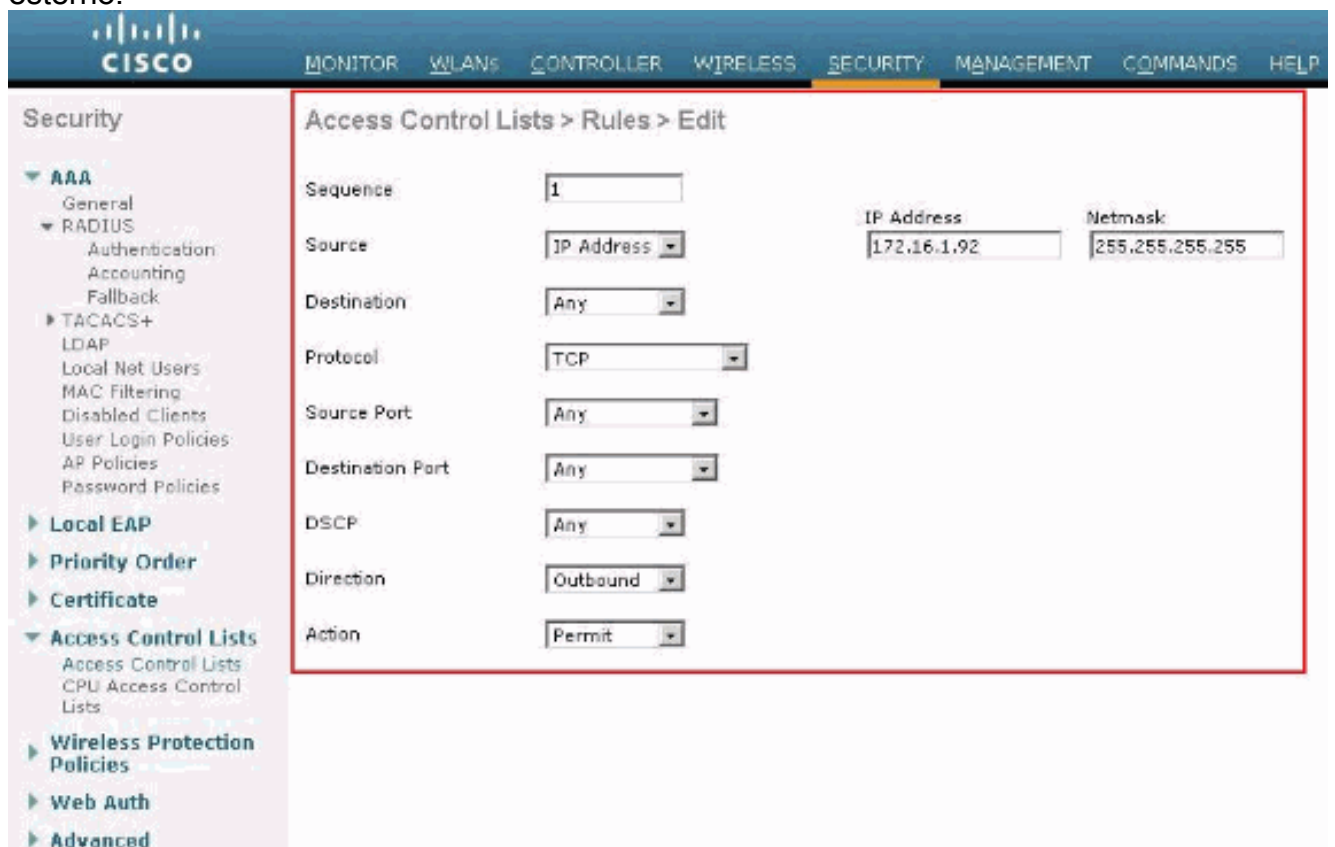
Per configurare l'ACL di preautenticazione per la WLAN, completare la procedura seguente:

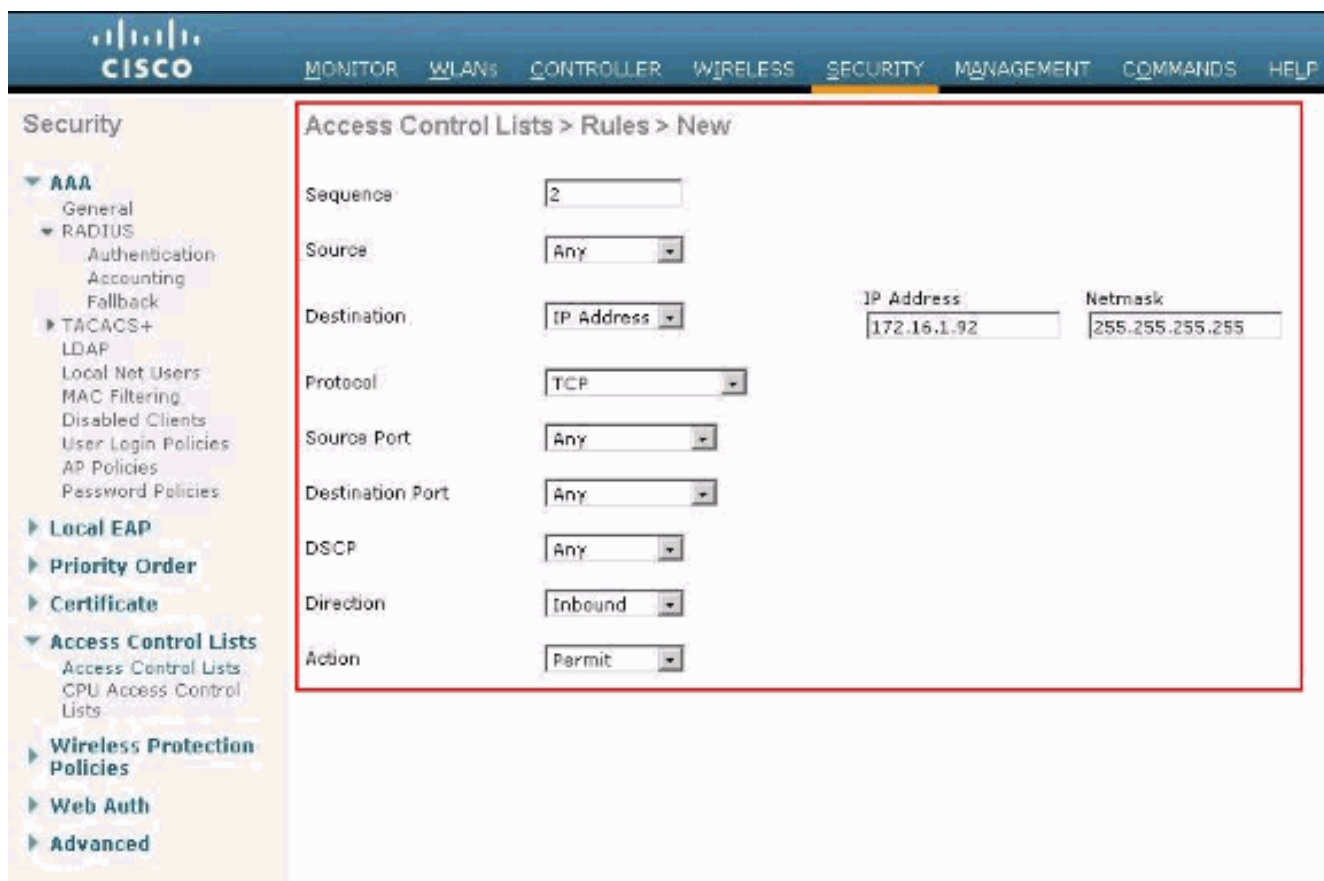
1. Dall'interfaccia utente del WLC, scegliere **Sicurezza > Access Control Lists**. Questa finestra consente di visualizzare gli ACL correnti simili agli ACL standard del firewall.
2. Per creare un nuovo ACL, fare clic su **New** (Nuovo).
3. Immettere il nome dell'ACL e fare clic su **Apply**. Nell'esempio, il nome dell'ACL è **Pre-Auth-for-External-Web-**

Server.

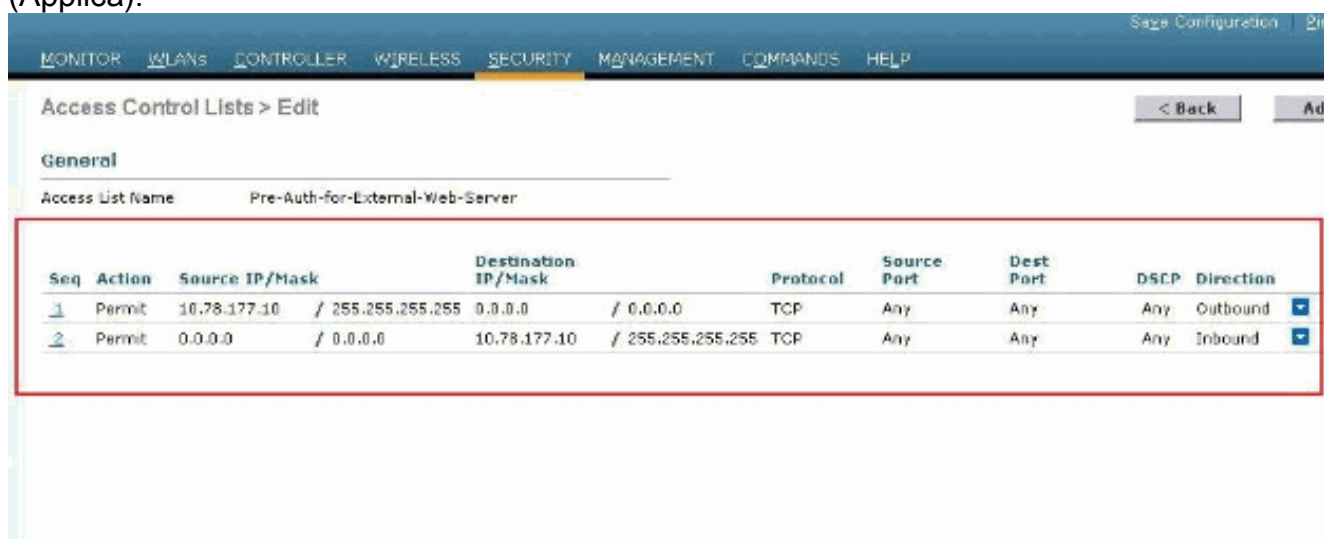


4. Per il nuovo ACL creato, fare clic su **Modifica**. Viene visualizzata la finestra ACL > Modifica. Questa finestra consente all'utente di definire nuove regole o di modificare le regole dell'ACL esistente.
5. Fare clic su **Aggiungi nuova regola**.
6. Definire una regola ACL che consenta ai clienti di accedere al server Web esterno. Nell'esempio, 172.16.1.92 è l'indirizzo IP del server Web esterno.





7. Per eseguire il commit delle modifiche, fare clic su **Apply** (Applica).



[Creare un database locale sul WLC per gli utenti guest](#)

Il database utenti per gli utenti guest può essere archiviato nel database locale del controller LAN wireless oppure può essere archiviato all'esterno del controller.

In questo documento il database locale sul controller viene utilizzato per autenticare gli utenti. È necessario creare un utente di rete locale e definire una password per l'accesso client di autenticazione Web. Per creare il database utenti sul WLC, completare i seguenti passaggi:

1. Dall'interfaccia utente del WLC, scegliere **Security**.
2. Fare clic su **Local Net Users** nel menu AAA a sinistra.

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 the following items: AAA (expanded), General, RADIUS (expanded), Authentication, Accounting, Fallback, 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 headers: User Name, WLAN Profile, Guest User, Role, and Description.

3. Per creare un nuovo utente, fare clic su **New** (Nuovo).Viene visualizzata una nuova finestra in cui vengono richiesti il nome utente e la password.
4. Immettere un Nome utente e una Password per creare un nuovo utente, quindi confermare la password che si desidera utilizzare.In questo esempio viene creato l'utente **User1**.
5. Se lo si desidera, aggiungere una descrizione.In questo esempio viene utilizzato **Guest User1**.
6. Per salvare la nuova configurazione utente, fare clic su **Apply** (Applica).

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

Below the form, a table lists the created user:

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

7. Ripetere i passaggi da 3 a 6 per aggiungere altri utenti al database.

[Configurare il WLC per l'autenticazione Web esterna](#)

Il passaggio successivo è configurare il WLC per l'autenticazione Web esterna. Attenersi alla seguente procedura:

1. Dalla GUI del controller, selezionare **Security > Web Auth > Web Login Page** (Sicurezza > Web Auth > Pagina di accesso Web) per accedere alla pagina di accesso Web.
2. Dalla casella di riepilogo a discesa Tipo di autenticazione Web, scegliere **Esterno (reindirizzamento a server esterno)**.
3. Nella sezione **Server Web esterno** aggiungere il nuovo server Web esterno.
4. Nel campo **Reindirizza URL dopo l'accesso**, immettere l'URL della pagina a cui l'utente finale verrà reindirizzato dopo l'autenticazione. Nel campo **External Web Auth URL (URL autenticazione Web esterno)**, immettere l'URL in cui la pagina di accesso è memorizzata sul server Web esterno.

Web Login Page

Web Authentication Type: (Dropdown menu open showing: 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

Cisco Logo:
 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

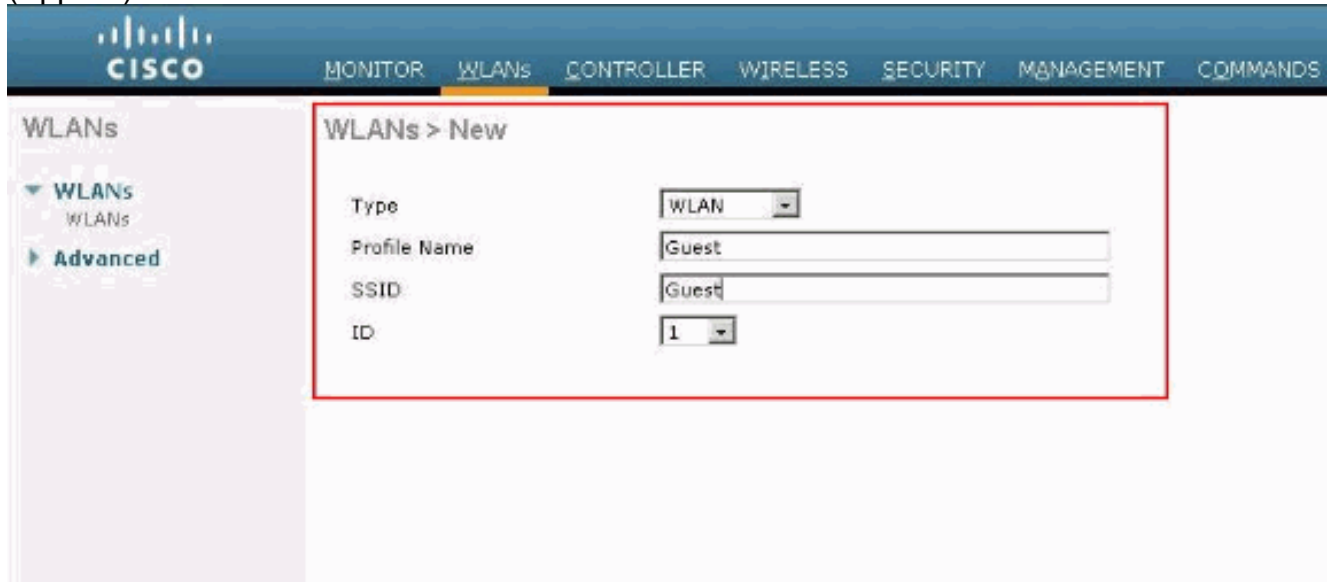
Web Server IP Address
<input type="text" value="172.16.1.92"/>

Nota: nelle versioni WLC 5.0 e successive, è possibile personalizzare anche la pagina di disconnessione per l'autenticazione Web. Per ulteriori informazioni su come configurare il controller *Wireless LAN Controller*, consultare la sezione [Assign Login, Login failure and Logout pages per WLAN Configuration Guide, 5.2](#) (Assegna login, Login failure and Logout pages per WLAN Controller Configuration Guide, 5.2).

[Configurazione della WLAN per gli utenti guest](#)

Il passaggio finale è la creazione di WLAN per gli utenti guest. Attenersi alla seguente procedura:

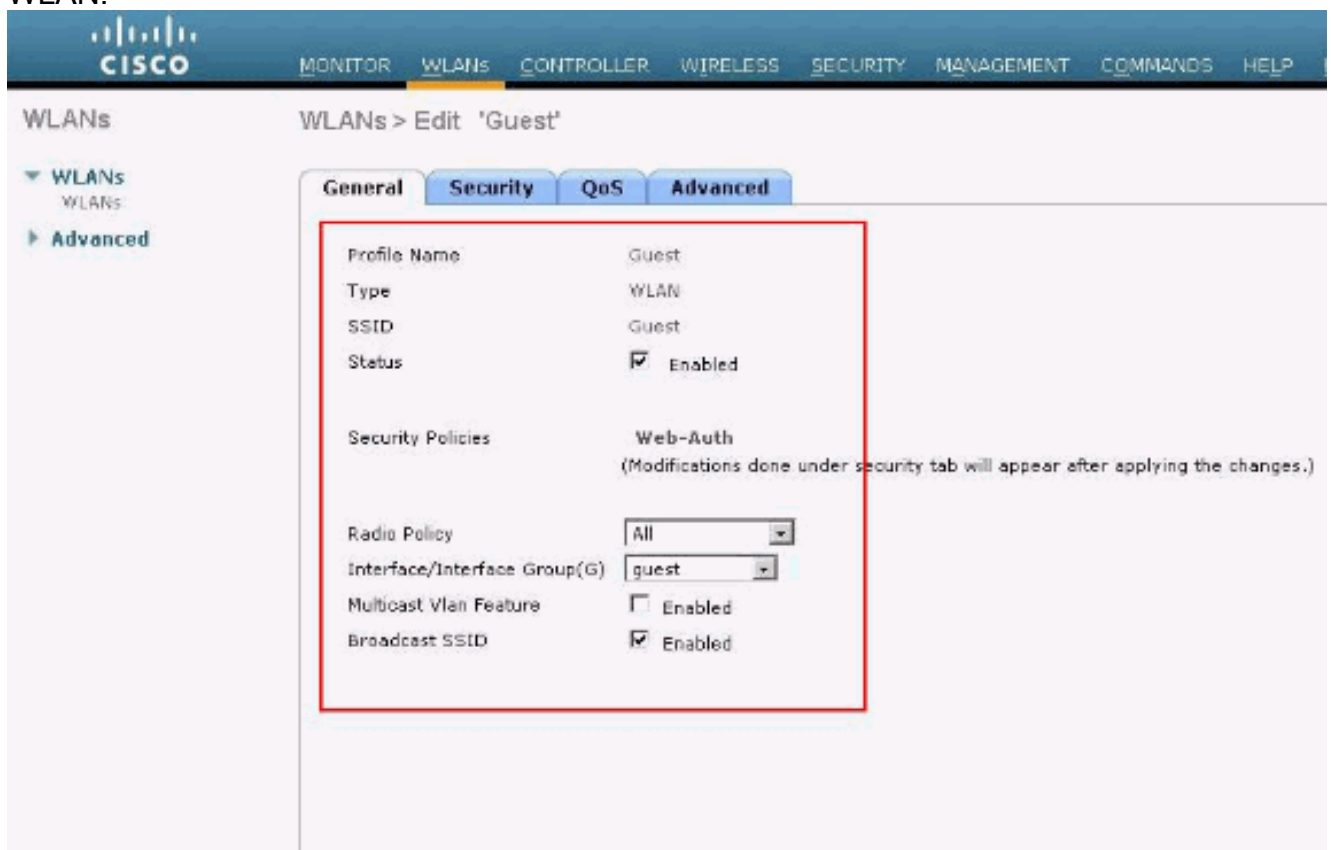
1. Per creare una WLAN, fare clic su **WLAN** dall'interfaccia utente del controller. Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.
2. Per configurare una nuova WLAN, fare clic su **New** (Nuovo). Nell'esempio, il nome della WLAN è **Guest** e l'ID della WLAN è **1**.
3. Fare clic su **Apply** (Applica).



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains a form with the following fields:

Type	WLAN
Profile Name	Guest
SSID	Guest
ID	1

4. Nella finestra WLAN > Modifica, definire i parametri specifici della WLAN. Per la WLAN guest, nella scheda Generale scegliere l'interfaccia appropriata nel campo Nome interfaccia. In questo esempio viene mappata l'interfaccia dinamica **guest** precedentemente creata al guest WLAN.

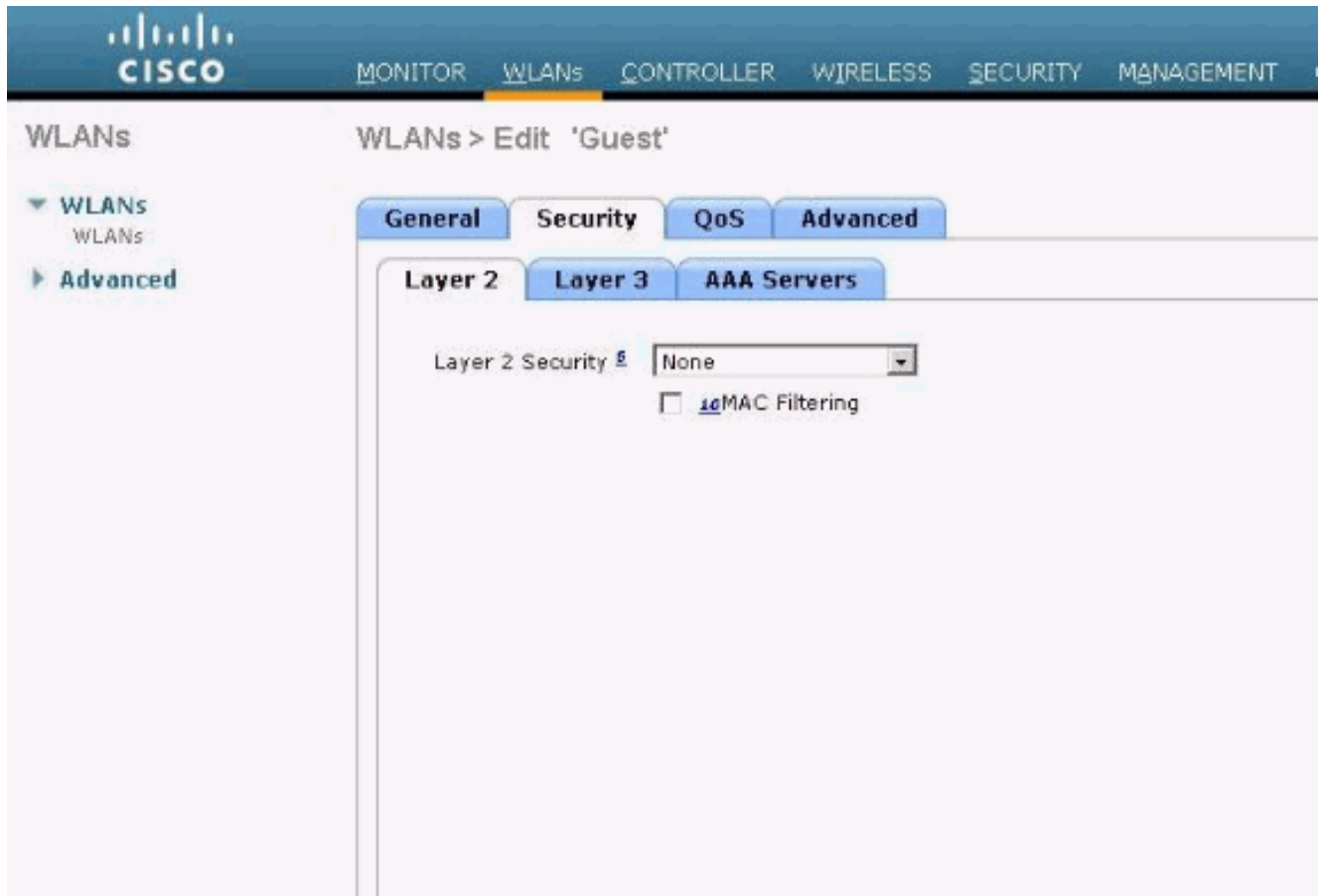


The screenshot shows the Cisco WLAN configuration interface for editing the 'Guest' WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Guest'' and contains a form with the following fields:

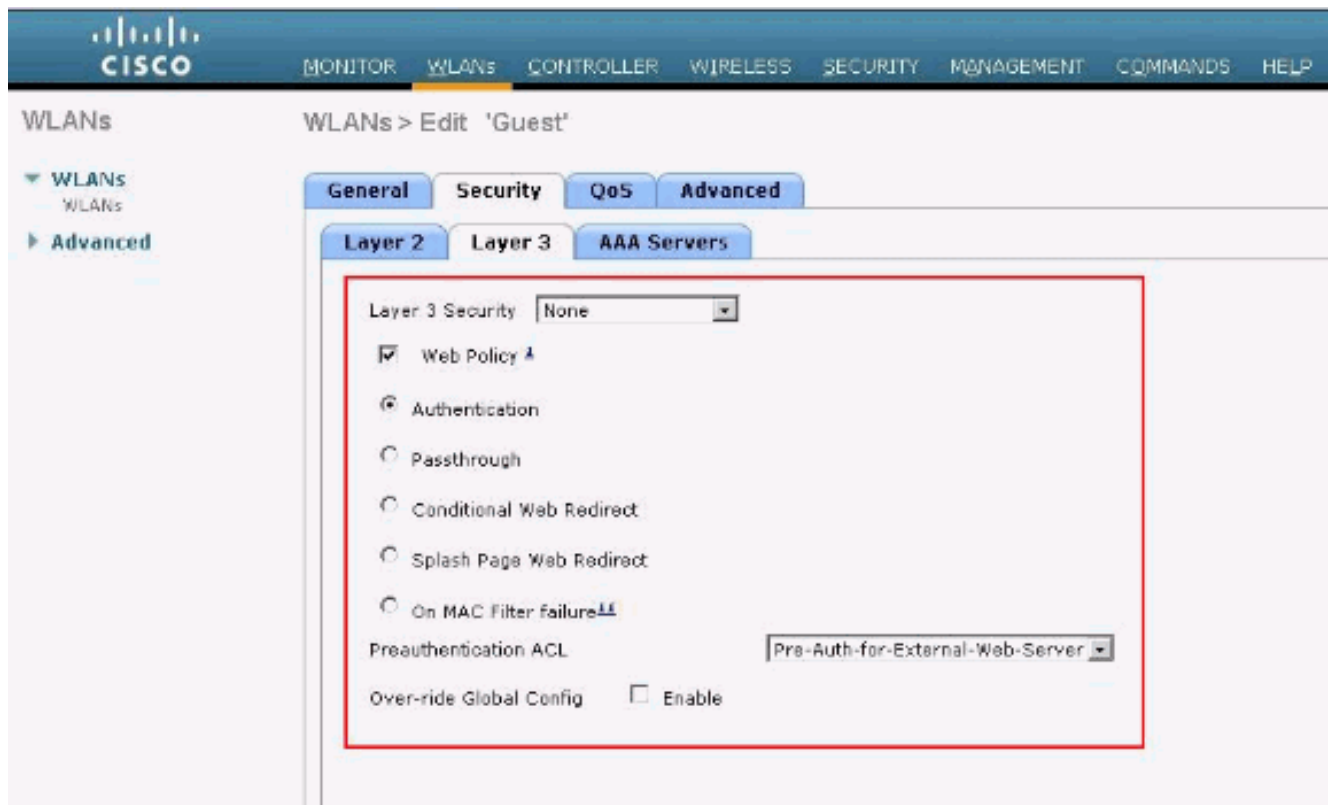
Profile Name	Guest
Type	WLAN
SSID	Guest
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled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

Andare alla scheda Protezione. In Protezione di livello 2 in questo esempio è selezionato **Nessuno**. **Nota:** l'autenticazione Web non è supportata con l'autenticazione 802.1x. Ciò significa che non è possibile scegliere 802.1x o WPA/WPA2 con 802.1x come protezione di

livello 2 quando si utilizza l'autenticazione Web.L'autenticazione Web è supportata con tutti gli altri parametri di protezione di livello 2.



Nel campo Sicurezza di layer 3, selezionare la casella di controllo **Criteri Web** e scegliere l'opzione **Autenticazione**. Questa opzione è selezionata perché per autenticare i client guest wireless viene utilizzata l'autenticazione Web. Selezionare l'ACL di preautenticazione appropriato dal menu a discesa. Nell'esempio, viene usato l'ACL di preautenticazione creato in precedenza. Fare clic su **Apply** (Applica).



Verifica

Il client wireless si accende e l'utente immette l'URL, ad esempio www.cisco.com, nel browser Web. Poiché l'utente non è stato autenticato, il WLC reindirizza l'utente all'URL di accesso Web esterno.

All'utente vengono richieste le credenziali dell'utente. Una volta che l'utente ha inviato il nome utente e la password, la pagina di accesso accetta le credenziali dell'utente e, al momento dell'invio, invia nuovamente la richiesta all'esempio `action_URL`, `http://1.1.1.1/login.html`, del server Web WLC. Viene fornito come parametro di input per l'URL di reindirizzamento del cliente, dove `1.1.1.1` è l'indirizzo dell'interfaccia virtuale sullo switch.

Il WLC autentica l'utente rispetto al database locale configurato sul WLC. Una volta completata l'autenticazione, il server Web WLC inoltra l'utente all'URL di reindirizzamento configurato o all'URL utilizzato dal client, ad esempio 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.

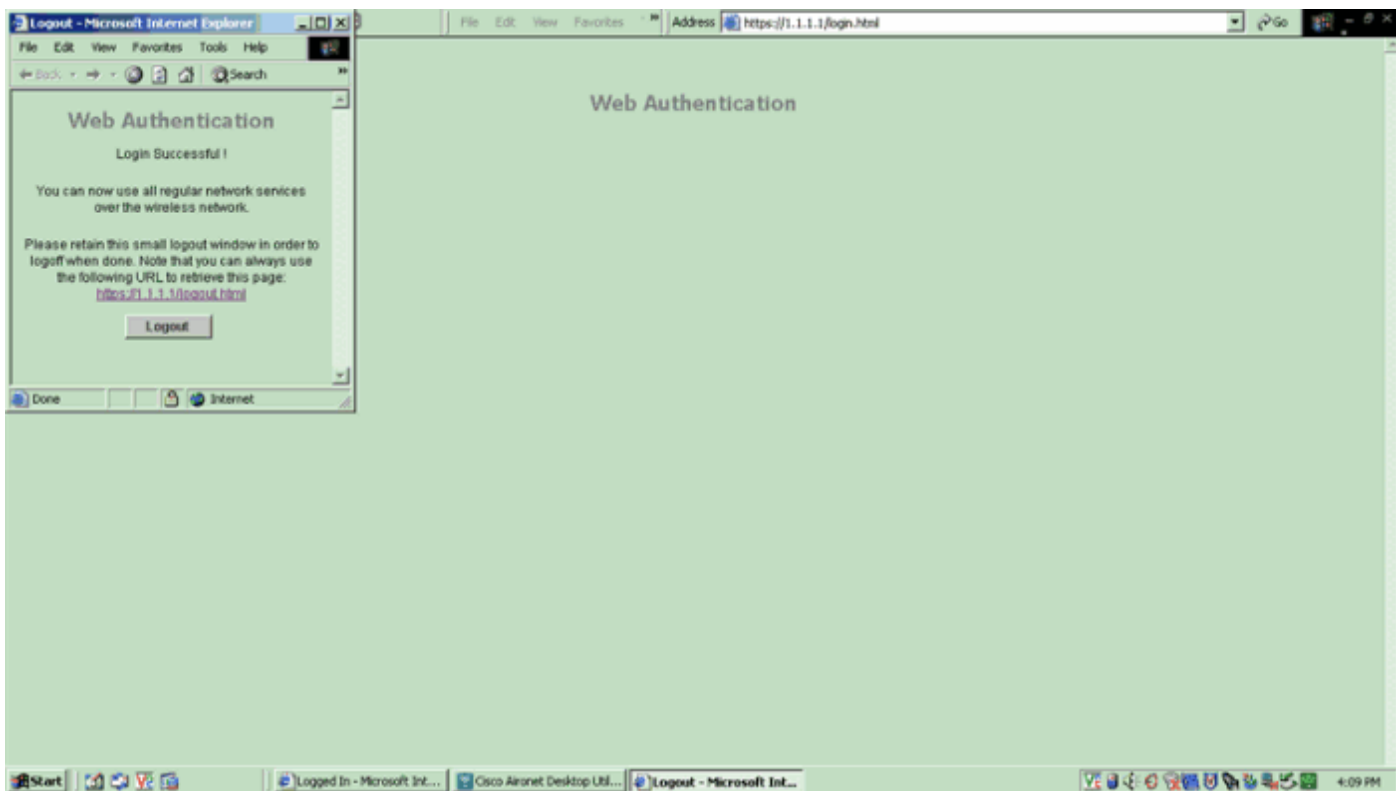
- ⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- ✔ The security certificate date is valid.
- ✔ The security certificate has a valid name matching the name of the page you are trying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

Do you want to proceed?

Web Authentication

User Name

Password



Risoluzione dei problemi

Usare questi comandi di debug per risolvere i problemi relativi alla configurazione.

- debug mac addr <indirizzo-MAC-client: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

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

I client reindirizzati al server di autenticazione Web esterno ricevono un avviso di certificato

Problema: quando i client vengono reindirizzati al server di autenticazione Web esterno di Cisco, ricevono un avviso di certificato. Nel server è presente un certificato valido e se ci si connette direttamente al server di autenticazione Web esterno, l'avviso del certificato non verrà ricevuto. Il problema è dovuto al fatto che l'indirizzo IP virtuale (1.1.1.1) del WLC viene presentato al client anziché l'indirizzo IP effettivo del server di autenticazione Web esterno associato al certificato?

Soluzione: sì. Indipendentemente dal fatto che si esegua o meno l'autenticazione Web locale o esterna, si accede comunque al server Web interno sul controller. Quando si esegue il reindirizzamento a un server Web esterno, si riceve comunque l'avviso di certificato dal controller, a meno che non si disponga di un certificato valido sul controller stesso. Se il reindirizzamento viene inviato a https, l'utente riceve l'avviso di certificato dal controller e dal server Web esterno, a meno che entrambi non dispongano di un certificato valido.

Per eliminare tutti gli avvisi del certificato, è necessario che sia stato emesso e scaricato nel controller un certificato di livello radice. Il certificato viene rilasciato per un nome host che viene inserito nella casella Nome host DNS nell'interfaccia virtuale del controller. Inoltre, è necessario aggiungere il nome host al server DNS locale e puntarlo all'indirizzo IP virtuale (1.1.1.1) del WLC.

Per ulteriori informazioni, fare riferimento a [Generazione della richiesta di firma del certificato \(CSR\) per un certificato di terze parti su un controller WLAN \(WLC\)](#).

[Errore: impossibile visualizzare la pagina](#)

Problema: dopo l'aggiornamento del controller alla versione 4.2.61.0, quando si utilizza una pagina Web scaricata per l'autenticazione Web viene visualizzato il messaggio di errore "pagina non visualizzabile". Questa procedura ha funzionato bene prima dell'aggiornamento. La pagina Web interna predefinita viene caricata senza alcun problema.

Soluzione: dalla versione 4.2 del WLC e successive è stata introdotta una nuova funzionalità che consente di avere più pagine di login personalizzate per l'autenticazione Web.

Per caricare correttamente la pagina Web, non è sufficiente impostare il tipo di autenticazione Web come **personalizzato** globalmente nella **pagina Sicurezza > Web Auth > Accesso Web**. Deve essere inoltre configurato su una particolare WLAN. A tale scopo, effettuare le seguenti operazioni:

1. Accedere alla GUI del WLC.
2. Fare clic sulla scheda **WLAN** e accedere al profilo della WLAN configurata per l'autenticazione Web.
3. Nella pagina WLAN > Modifica, fare clic sulla scheda **Sicurezza**. Quindi, scegliete **Layer 3**.
4. In questa pagina scegliere **Nessuno** come protezione di livello 3.
5. Selezionare la casella **Criteri Web** e scegliere l'opzione **Autenticazione**.
6. Selezionare la casella Override Global Config **Enable** (Ignora configurazione globale), scegliere **Customized (Scaricato)** come Tipo di autenticazione Web, quindi selezionare la pagina di login desiderata dal menu a discesa **Login Page** (Pagina di login). Fare clic su **Apply** (Applica).

[Informazioni correlate](#)

- [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#)
- [Video: autenticazione Web sui Cisco Wireless LAN Controller \(WLC\)](#)
- [Esempio di configurazione delle VLAN nei Wireless LAN Controller](#)
- [Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

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