

# Configureer externe webverificatie met WLC's

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Externe webverificatieprocedure](#)

[Netwerkinstelling](#)

[Configureren](#)

[Een dynamische interface voor de gastgebruikers maken](#)

[Een verificatie vooraf maken](#)

[Maak een lokale database op de WLC voor de Gastgebruikers](#)

[Configureer de WLC voor externe webverificatie](#)

[WLAN's voor gastgebruikers configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Clients die worden omgeleid naar externe webverificatieserver ontvangen een certificaatwaarschuwing](#)

[Fout: "Pagina kan niet worden weergegeven"](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

In dit document wordt uitgelegd hoe u een externe webserver kunt gebruiken om een draadloze LAN-controller (WLC) voor webverificatie in te stellen.

## [Voorwaarden](#)

### [Vereisten](#)

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Basiskennis van de configuratie van Lichtgewicht access points (LAP's) en Cisco WLC's
- Basiskennis van Lichtgewicht access point protocol (LWAP) en controle en provisioning van draadloze access points (CAPWAP)
- Kennis over het instellen en configureren van een externe webserver
- Kennis over het instellen en configureren van DHCP- en DNS-servers

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 WLC met firmwarerelease 7.0.116.0
- Cisco 1131AG Series netwerkmodule
- Cisco 802.11a/b/g draadloze clientadapter waarop firmware-release 3.6 wordt uitgevoerd
- Externe webserver waarop de inlogpagina voor webverificatie wordt gehost
- DNS- en DHCP-servers voor adresresolutie en IP-adrestoewijzing aan draadloze clients

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## Achtergrondinformatie

Web authenticatie is een Layer 3-beveiligingsfunctie die ervoor zorgt dat de controller geen IP-verkeer (behalve DHCP- en DNS-gerelateerde pakketten) van een bepaalde client toestaat totdat die client op de juiste manier een geldige gebruikersnaam en wachtwoord heeft ingevoerd. Web Verificatie is een eenvoudige verificatiemethode zonder dat er een applicatie of client hulpprogramma nodig is.

Web authenticatie kan worden uitgevoerd met:

- Standaard inlogvenster op de WLC
- Gewijzigde versie van het standaardinlogvenster op de WLC
- Een aangepast inlogvenster dat u configureert op een externe webserver (externe webverificatie)
- Een aangepast inlogvenster dat u naar de controller downloadt

Dit document biedt een configuratievoorbeeld om uit te leggen hoe de WLC moet worden geconfigureerd om een inlogscript te gebruiken van een externe webserver.

## Externe webverificatieprocedure

Met externe webverificatie wordt de inlogpagina die voor webverificatie wordt gebruikt, opgeslagen op een externe webserver. Dit is de volgorde van gebeurtenissen wanneer een draadloze client probeert toegang te krijgen tot een WLAN-netwerk waarvoor externe webverificatie is ingeschakeld:

1. De client (eindgebruiker) maakt verbinding met het WLAN en opent een webbrowsen en voert een URL in, zoals [www.cisco.com](http://www.cisco.com).
2. De client stuurt een DNS-verzoek naar een DNS-server om [www.cisco.com](http://www.cisco.com) naar IP-adres op te lossen.
3. De WLC stuurt het verzoek door naar de DNS server die op zijn beurt [www.cisco.com](http://www.cisco.com) naar

IP adres oplost en een DNS antwoord verstuurt. De controller stuurt het antwoord door naar de klant.

4. De client probeert een TCP-verbinding met het www.cisco.com IP-adres te initiëren door het TCP/SYN-pakket naar het www.cisco.com IP-adres te verzenden.
5. De WLC heeft regels geconfigureerd voor de client en kan daarom fungeren als een proxy voor www.cisco.com. Het stuurt een TCP SYN-ACK pakket terug naar de client met bron als IP-adres van www.cisco.com. De client stuurt een TCP-ACK-pakket terug om de drieweg-TCP-handdruk te voltooien en de TCP-verbinding is volledig tot stand gebracht.
6. De client verzendt een HTTP GET pakket naar www.google.com. De WLC onderschept dit pakket, verstuurt het voor omleidingsbehandeling. De HTTP applicatie gateway bereidt een HTML body voor en verstuurt het terug als het antwoord op de HTTP GET gevraagd door de client. Deze HTML maakt de client naar de standaard webpagina URL van de WLC, bijvoorbeeld `http://<Virtual-Server-IP>/login.html`.
7. De client start vervolgens de HTTPS-verbinding naar de doorgestuurde URL die het doorstuurt naar 1.1.1.1. Dit is het virtuele IP-adres van de controller. De client moet het servercertificaat valideren of negeren om de SSL-tunnel te kunnen openen.
8. Omdat externe webverificatie is ingeschakeld, wordt de client door de WLC omgeleid naar de externe webserver.
9. De externe web auth login URL wordt toegevoegd met parameters zoals de AP\_Mac\_Address, de client\_url (www.cisco.com) en de action\_URL die de client nodig heeft om contact op te nemen met de controller webserver. **Opmerking:** De action\_URL vertelt de webserver dat de gebruikersnaam en het wachtwoord zijn opgeslagen op de controller. De referenties moeten naar de controller worden teruggestuurd om te worden geverifieerd.
10. De externe webserver URL leidt de gebruiker naar een inlogpagina.
11. De login pagina neemt gebruikersreferenties input, en verzendt het verzoek terug naar action\_URL, voorbeeld `http://1.1.1.1/login.html`, van de WLC webserver.
12. De WLC webserver dient de gebruikersnaam en het wachtwoord in voor verificatie.
13. De WLC initieert het RADIUS-serververzoek of gebruikt de lokale database op de WLC en verifieert de gebruiker.
14. Als de authenticatie succesvol is, door:sturen de WLC webserver of de gebruiker aan de gevormde omleiden URL of aan URL de cliënt waarmee, zoals www.cisco.com is begonnen.
15. Als de authenticatie mislukt, dan zal de WLC-webserver de gebruiker terugleiden naar de inlogpagina van de klant.

**Opmerking:** geef deze opdracht op om externe webverificatie te configureren voor gebruik van andere poorten dan HTTP en HTTPS:

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

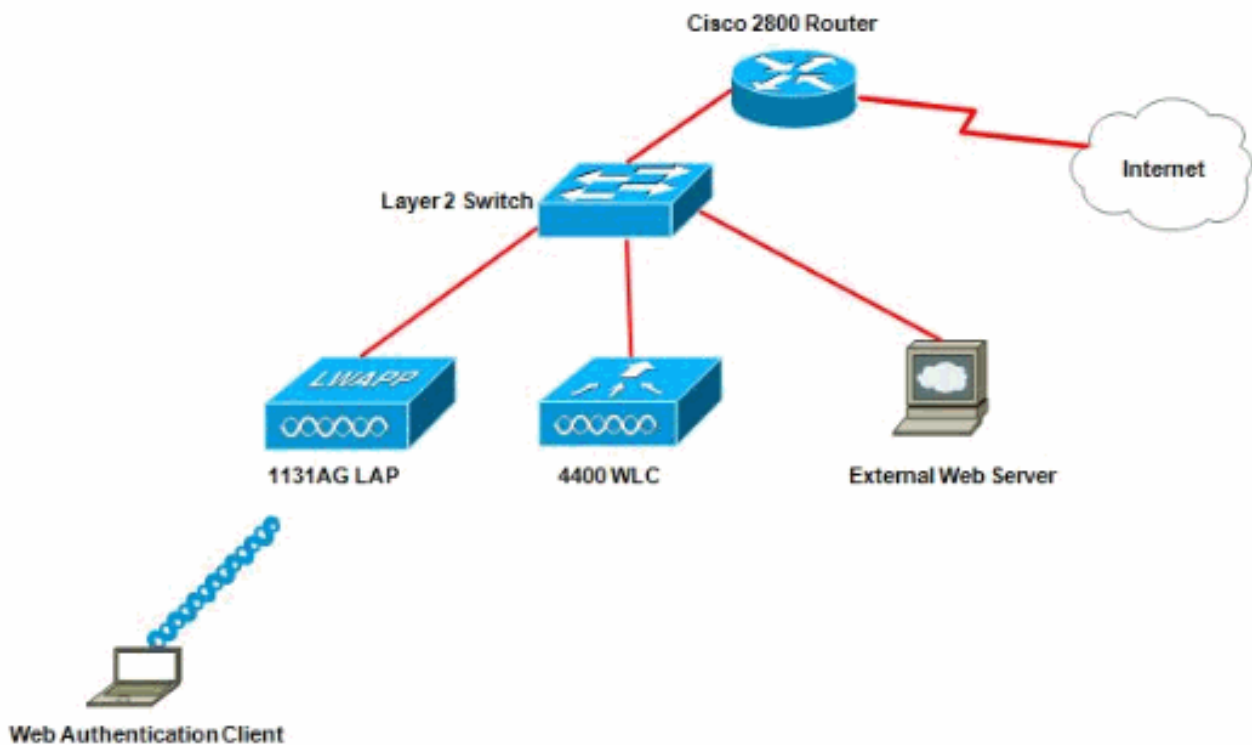
```
<port>           Configures an additional port to be redirected for web authentication.
```

## [Netwerkinstelling](#)

Het configuratievoorbeeld gebruikt deze instelling. Een LAP is geregistreerd bij de WLC. U moet een WLAN-**gast** configureren voor de gastgebruikers en webverificatie voor de gebruikers inschakelen. U moet er ook voor zorgen dat de controller de gebruiker omleidt naar de externe webserver URL (voor externe webverificatie). De externe webserver host de web login pagina die wordt gebruikt voor authenticatie.

De gebruikersreferenties moeten worden gevalideerd tegen de lokale database op de controller. Na succesvolle verificatie moeten de gebruikers toegang tot de WLAN-gast krijgen. De controller en andere apparaten moeten voor deze installatie worden geconfigureerd.

**Opmerking:** U kunt een aangepaste versie van het inlogscript gebruiken, die voor webverificatie wordt gebruikt. U kunt een voorbeeldscript voor webverificatie downloaden vanaf de pagina [Cisco-softwaredownloads](#). Voor de 4400 controllers bijvoorbeeld, navigeer naar **Producten > Draadloos > Draadloze LAN-controller > Standalone controllers > Cisco 4400 Series draadloze LAN-controllers > Cisco 4404 draadloze LAN-controller > Software op chassis > Wireless LAN Controller Web Authenticatiebundel-1.0.1** en download het bestand `webauth_bundle.zip`.



**Opmerking:** de aangepaste webauth bundel heeft een limiet van maximaal 30 tekens voor bestandsnamen. Zorg ervoor dat geen bestandsnamen binnen de bundel groter zijn dan 30 tekens.

**Opmerking:** in dit document wordt ervan uitgegaan dat de DHCP-, DNS- en externe webserver zijn geconfigureerd. Raadpleeg de relevante documentatie van derden voor informatie over het configureren van de DHCP-, DNS- en externe webserver.

## [Configureren](#)

Alvorens u WLC voor externe webverificatie vormt, moet u WLC voor basisverrichting vormen en de LAPs registreren aan WLC. Dit document veronderstelt dat WLC voor basisverrichting wordt gevormd en dat de LAPs aan WLC worden geregistreerd. Raadpleeg [Lichtgewicht AP \(LAP\)-registratie voor een draadloze LAN-controller \(WLC\)](#) als u een nieuwe gebruiker bent die de WLC probeert in te stellen voor basisgebruik met LAP's.

Voltooi deze stappen om de LAP's en WLC voor deze installatie te configureren:

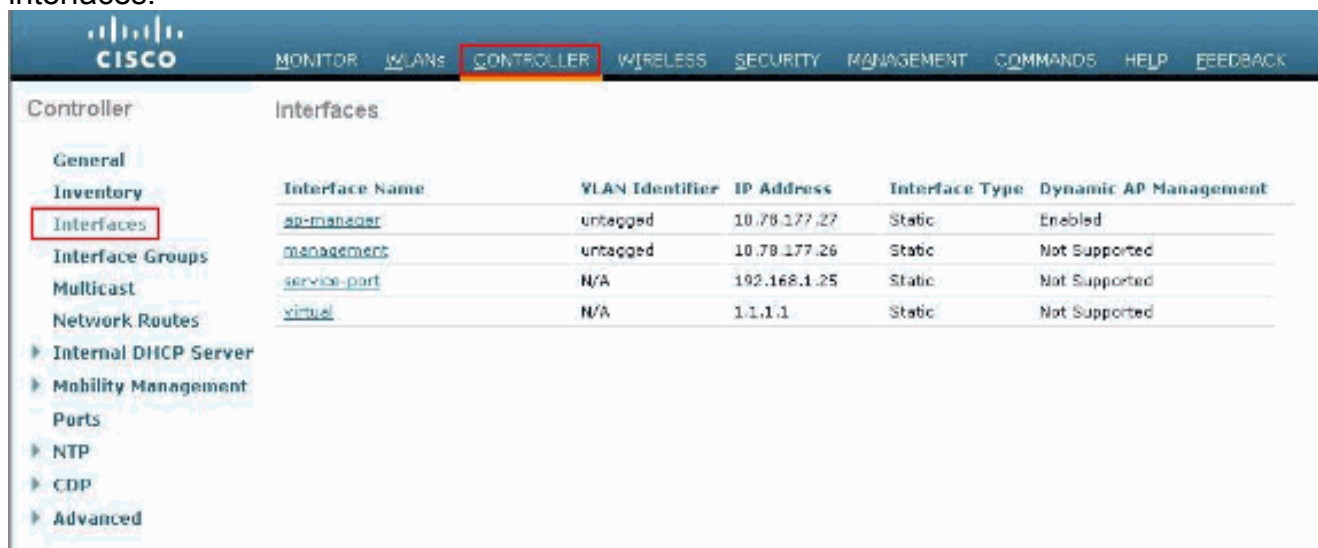
1. [Een dynamische interface voor de gastgebruikers maken](#)

2. [Een verificatie vooraf maken](#)
3. [Maak een lokale database op de WLC voor de Gastgebruikers](#)
4. [Configureer de WLC voor externe webverificatie](#)
5. [WLAN's voor gastgebruikers configureren](#)

## Een dynamische interface voor de gastgebruikers maken

Voltooi deze stappen om een dynamische interface voor de gastgebruikers te creëren:

1. Kies in de WLC GUI de optie **Controllers > Interfaces**. Het venster Interfaces verschijnt. Dit venster toont de interfaces die op de controller zijn geconfigureerd. Hieronder vallen de standaardinterfaces, te weten de beheerinterface, de ap-manager interface, de virtuele interface en de service-poortinterface en de door de gebruiker gedefinieerde dynamische interfaces.



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. Klik op **Nieuw** om een nieuwe dynamische interface te maken.
3. Voer in het venster **Interfaces > Nieuw** de interfacenaam en VLAN-id in. Klik vervolgens op **Toepassen**. In dit voorbeeld wordt de dynamische interface **guest** genoemd en wordt de VLAN-id toegewezen aan **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. In het venster **Interfaces > Edit**, voor de dynamische interface, ga het IP adres, het subnetmasker, en de standaardgateway in. Wijs het toe aan een fysieke poort op de WLC en voer het IP-adres van de DHCP-server in. Klik vervolgens op **Toepassen**.

The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. The left sidebar lists various configuration options, with 'Interfaces' highlighted. The main content area is titled 'Interfaces > Edit' and displays the configuration 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: ; 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

## Een verificatie vooraf maken

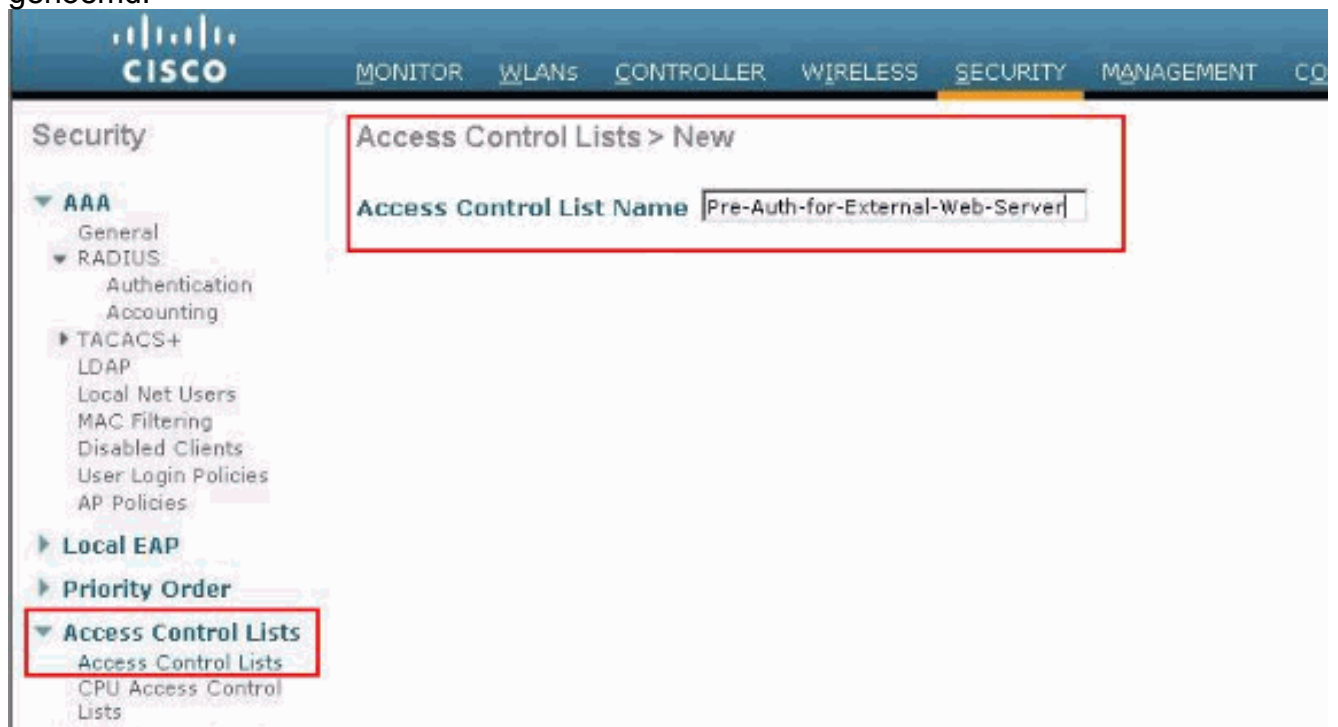
Wanneer u een externe webserver voor webverificatie gebruikt, hebben sommige WLC-platforms een pre-authenticatie ACL nodig voor de externe webserver (de Cisco 5500 Series controller, een Cisco 2100 Series controller, Cisco 2000 Series en de controller-netwerkmodule). Voor de andere WLC-platforms is pre-authenticatie ACL niet verplicht.

Het is echter een goede praktijk om een pre-authenticatie ACL voor de externe webserver te configureren wanneer externe webverificatie wordt gebruikt.

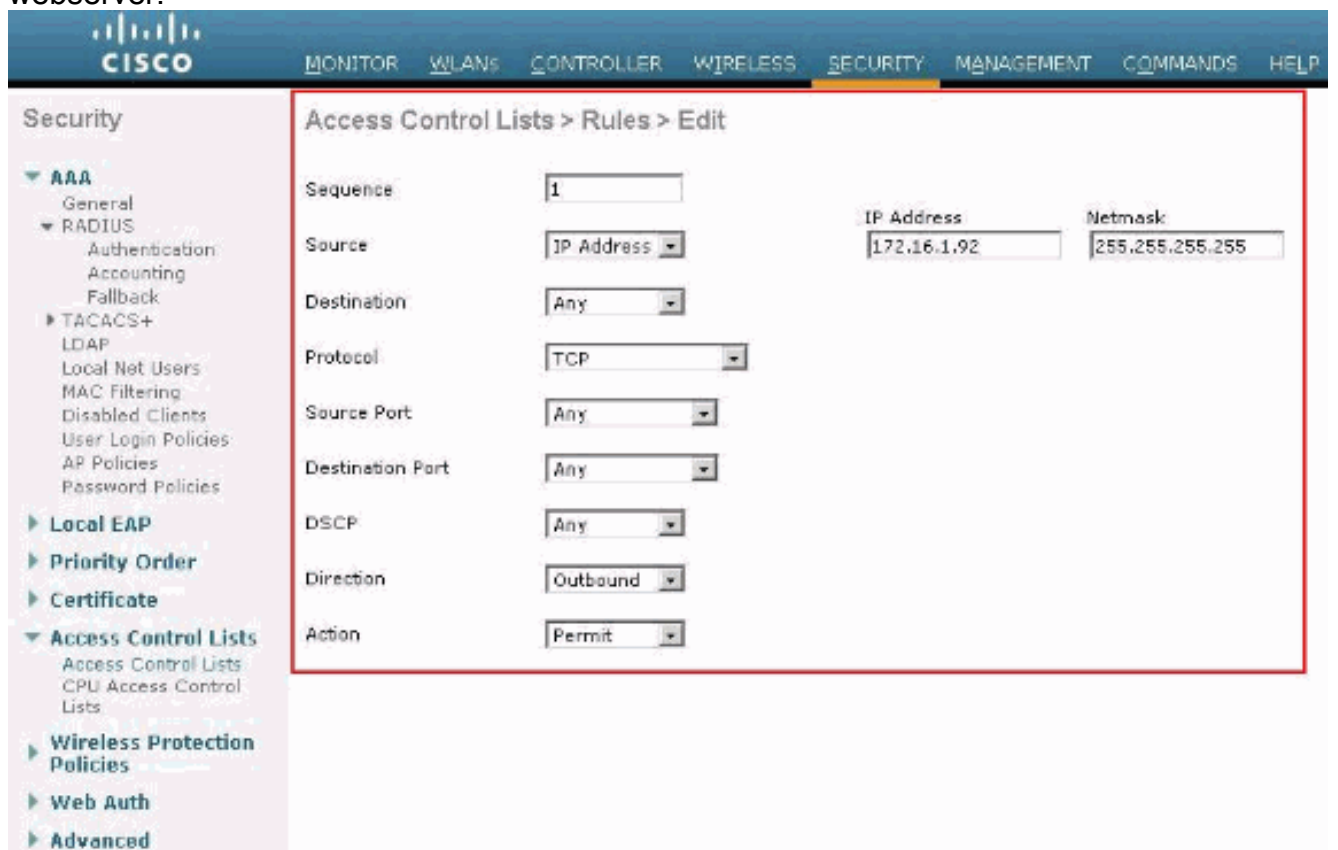
Voltooi de volgende stappen om de ACL voor voorverificatie van het WLAN te configureren:

1. Kies in de WLC GUI **Security > Access Control Lists**. In dit venster kunt u huidige ACL's bekijken die vergelijkbaar zijn met standaardfirewall-ACL's.
2. Klik op **Nieuw** om een nieuwe ACL te maken.
3. Voer de naam van de ACL in en klik op **Toepassen**. In dit voorbeeld wordt de ACL **Pre-Auth-for-External-Web-Server**

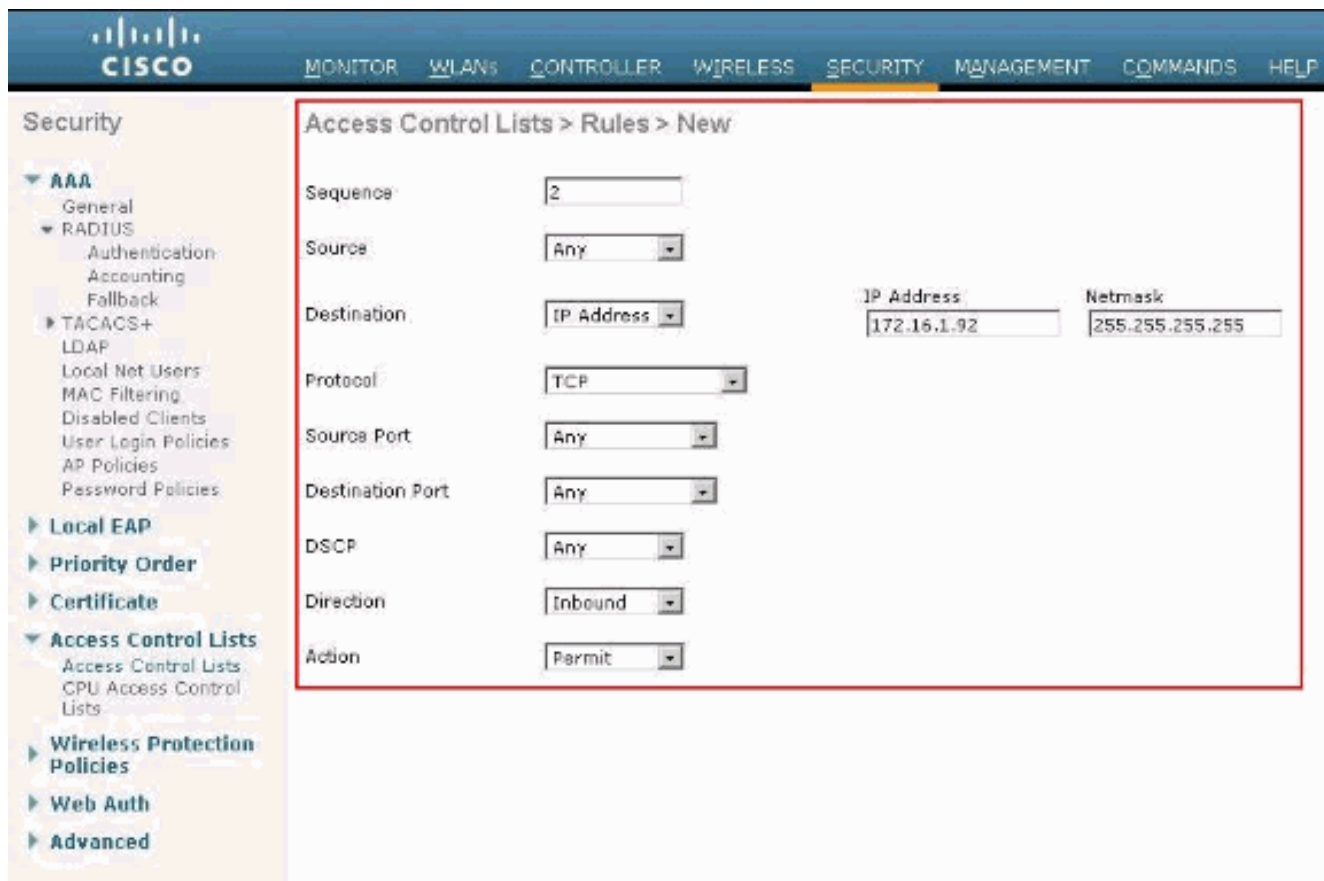
genoemd.



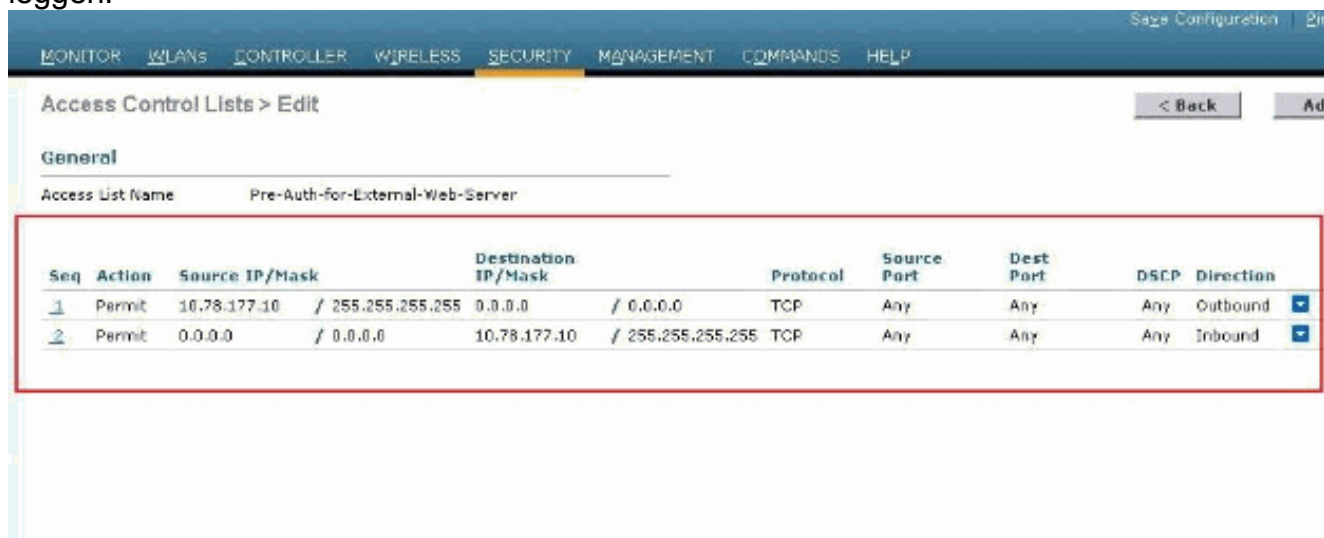
4. Klik voor de nieuwe ACL die is gemaakt op **Bewerken**. Het venster ACL > Bewerken verschijnt. Dit venster laat de gebruiker nieuwe regels bepalen of regels van ACL wijzigen die bestaan.
5. Klik op **Nieuwe regel toevoegen**.
6. Definieer een ACL-regel die toegang geeft voor de clients tot de externe webserver. In dit voorbeeld is 172.16.1.92 het IP-adres van de externe webserver.







7. Klik op **Toepassen** om de wijzigingen vast te leggen.



## [Maak een lokale database op de WLC voor de Gastgebruikers](#)

De gebruikersdatabase voor de gastgebruikers kan worden opgeslagen op de lokale database van de draadloze LAN-controller of kan buiten de controller worden opgeslagen.

In dit document wordt de lokale database op de controller gebruikt om gebruikers te verifiëren. U moet een lokale Net-gebruiker aanmaken en een wachtwoord definiëren voor de aanmelding van de webverificatieclient. Voltooi deze stappen om het gebruikersgegevensbestand op WLC te creëren:

1. Kies **Beveiliging** in de WLC GUI.
2. Klik links op **Local Net Gebruikers** in het menu

AAA.

The screenshot shows the Cisco configuration interface. At the top, there is a navigation bar with the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. On the left, a 'Security' sidebar contains a tree view with 'AAA' expanded to show 'Local Net Users' highlighted with a red box. The main content area is titled 'Local Net Users' and features a table with the following headers: 'User Name', 'WLAN Profile', 'Guest User', 'Role', and 'Description'. The table body is currently empty.

3. Klik op **Nieuw** om een nieuwe gebruiker te maken. Een nieuw venster toont dat vraagt om gebruikersnaam en wachtwoordinformatie.
4. Voer een gebruikersnaam en wachtwoord in om een nieuwe gebruiker te maken en bevestig vervolgens het wachtwoord dat u wilt gebruiken. In dit voorbeeld wordt de gebruiker **Gebruiker1** genoemd.
5. Voeg desgewenst een beschrijving toe. In dit voorbeeld wordt **gastgebruiker1** gebruikt.
6. Klik op **Toepassen** om de nieuwe gebruikersconfiguratie op te slaan.

The first screenshot shows the 'Local Net Users > New' configuration page. The fields are filled with the following values:

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

The second screenshot shows the 'Local Net Users' list table:

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

7. Herhaal stap 3-6 om meer gebruikers aan de database toe te voegen.

## Configureer de WLC voor externe webverificatie

De volgende stap is om WLC voor de externe webverificatie te configureren. Voer de volgende stappen uit:

1. Kies **Security > Web Auth > Web Login Page** in de GUI van de controller om toegang te krijgen tot de Web Login Pagina.
2. Kies **Extern** in de vervolgkeuzelijst Web Verification Type (**omleiden naar externe server**).
3. In de **Externe** sectie van de **Webserver**, voeg de nieuwe externe webserver toe.
4. Voer in het veld **URL na aanmelding** de URL in van de pagina waarnaar de eindgebruiker bij succesvolle verificatie zal worden doorgestuurd. Voer in het veld **Externe URL voor webautorisatie** de URL in waar de inlogpagina is opgeslagen op de externe webserver.

**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).

Cisco Logo:  Show  Hide

Headline:

Message:

**External Web Servers**

Web Server IP Address:

**Add Web Server**

**Web Login Page**

Web Authentication Type:

Redirect URL after login:

External Webauth URL:

**External Web Servers**

Web Server IP Address:

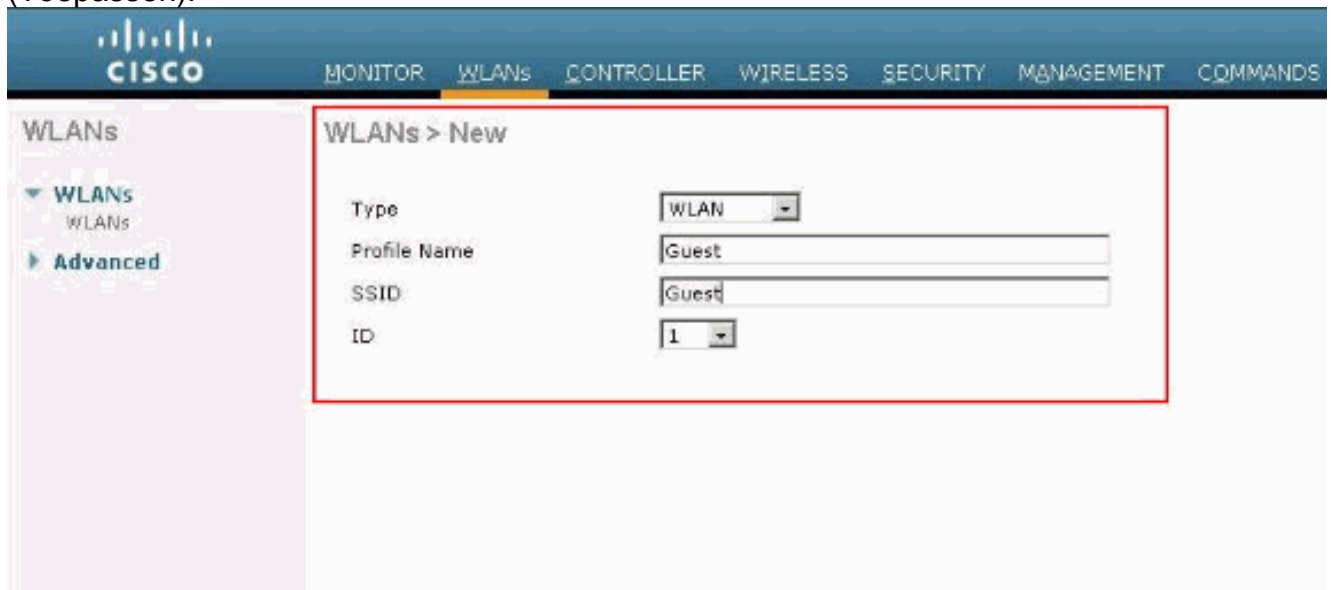
**Add Web Server**

**Opmerking:** In WLC versies 5.0 en hoger kan de logout pagina voor web-authenticatie ook worden aangepast. Raadpleeg de sectie [Toewijzen aan aanmelding, inlogfout en uitlogpagina's per WLAN](#)-sectie van de *configuratiehandleiding voor draadloze LAN-controllers, 5.2* voor meer informatie over het configureren ervan.

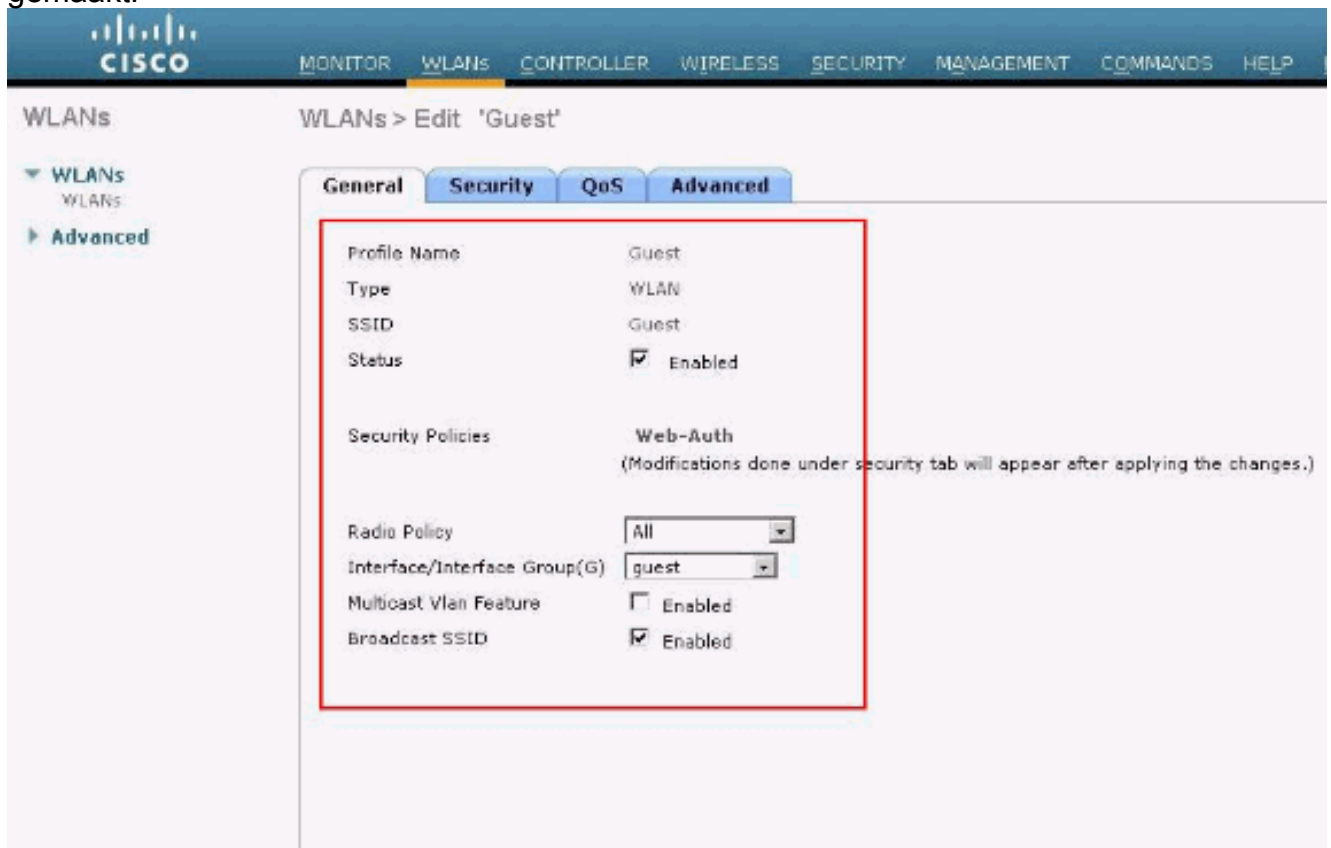
## [WLAN's voor gastgebruikers configureren](#)

De laatste stap is het maken van WLAN's voor de gastgebruikers. Voer de volgende stappen uit:

1. Klik op **WLAN's** vanuit de controller-GUI om een WLAN te maken. Het WLAN-venster verschijnt. Dit venster toont de WLAN's die op de controller zijn geconfigureerd.
2. Klik op **Nieuw** om een nieuw WLAN te configureren. In dit voorbeeld wordt het WLAN **Guest** genoemd en is de WLAN-id **1**.
3. Klik op **Apply** (Toepassen).

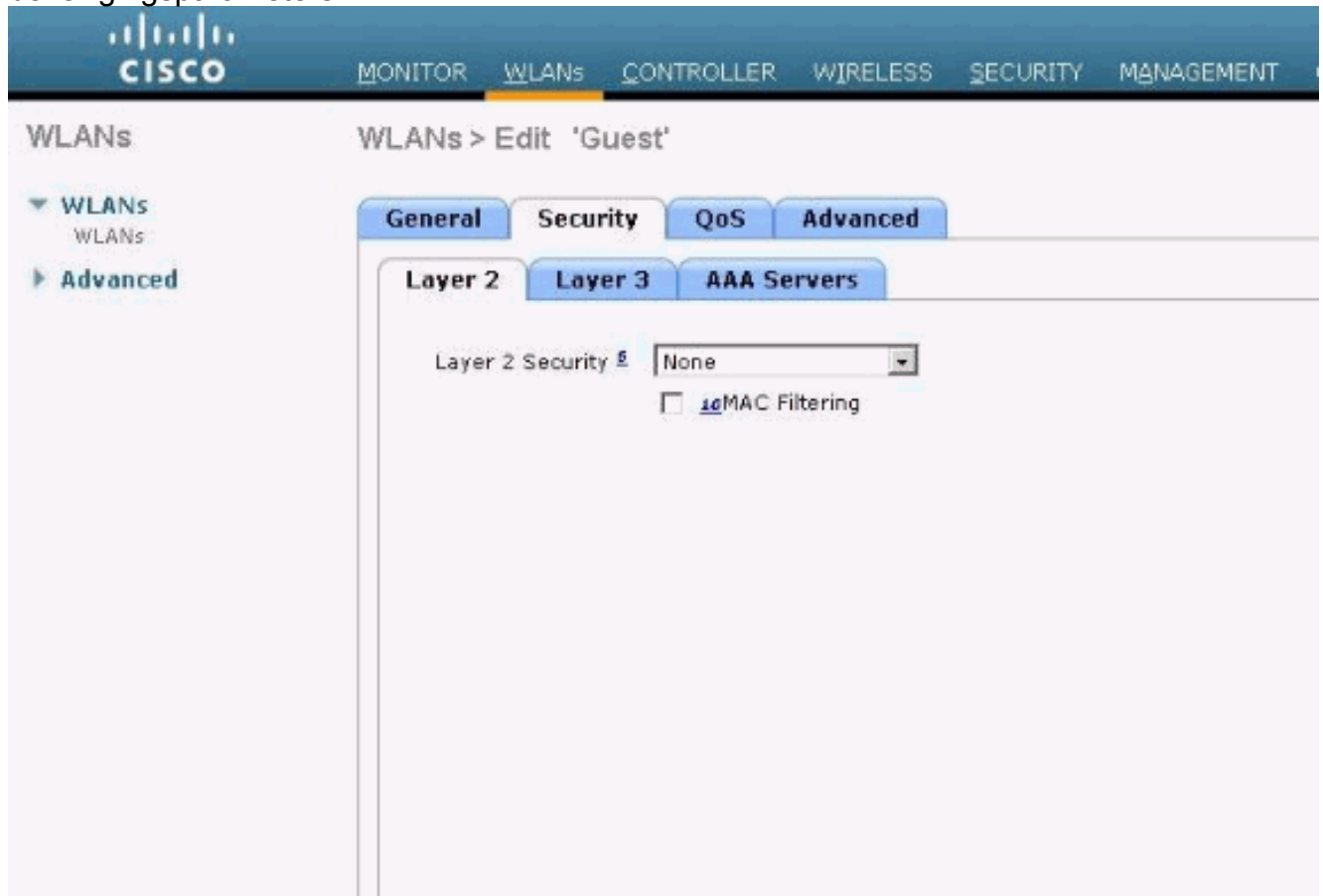


4. Definieer in het venster WLAN > Bewerken de parameters die specifiek zijn voor het WLAN. Voor de gast WLAN, op het tabblad Algemeen, kiest u de juiste interface uit het veld Interfacenaam. Dit voorbeeld brengt de dynamische **interfaceguest** in kaart die eerder aan de WLAN-gast is gemaakt.

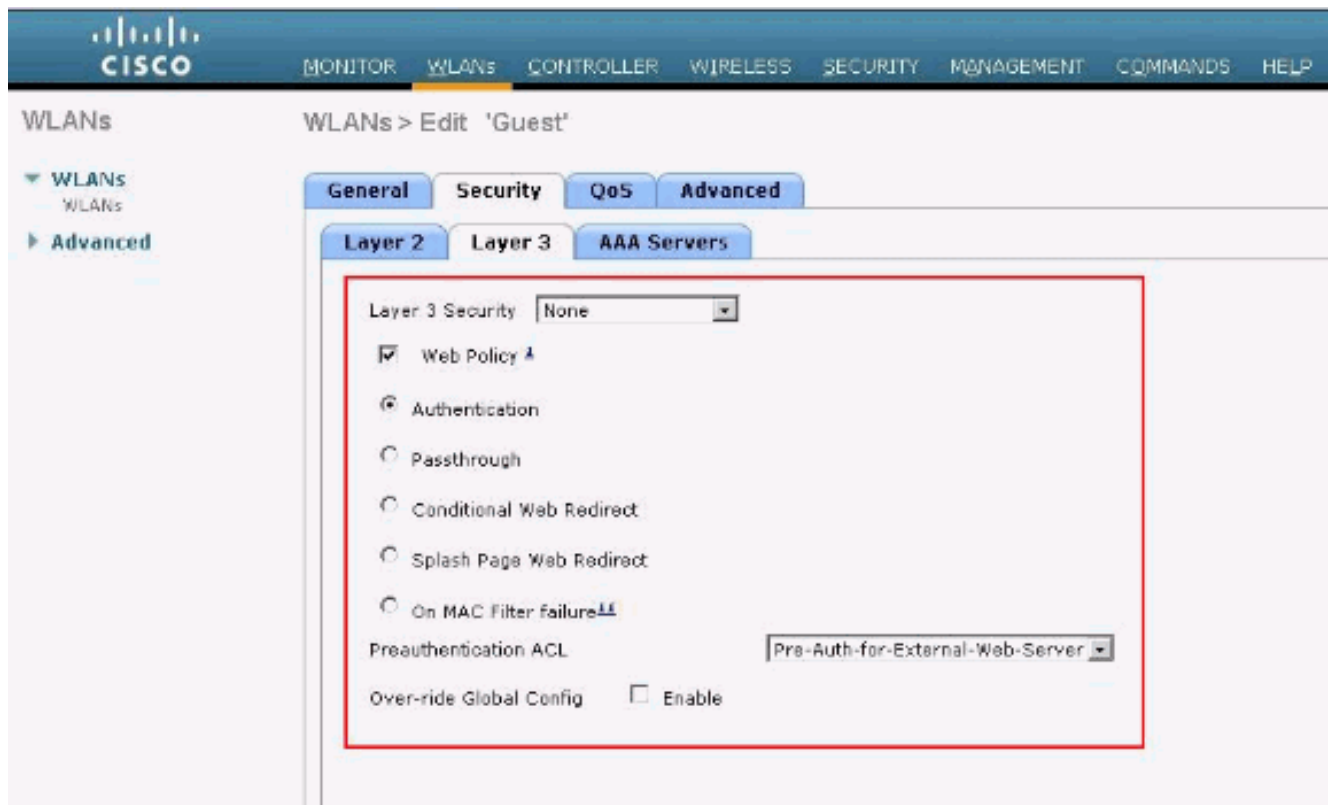


Ga naar het tabblad Beveiliging. Onder Layer 2 Security is **Geen** geselecteerd in dit voorbeeld. **Opmerking:** webverificatie wordt niet ondersteund met 802.1x-verificatie. Dit betekent dat u geen 802.1x of een WPA/WPA2 met 802.1x kunt kiezen als Layer 2-

beveiliging wanneer u webverificatie. Web-verificatie gebruikt wordt ondersteund door alle andere Layer 2-beveiligingsparameters.



Selecteer in het veld Layer 3 Security het aankruisvakje **Web Policy** en kies de optie **Verificatie**. Deze optie is gekozen omdat web authenticatie wordt gebruikt om de draadloze gast clients te authenticeren. Kies de juiste ACL-verificatie voor aanmelding in het vervolkeuzemenu. In dit voorbeeld wordt de voorverificatie ACL die eerder is gemaakt, gebruikt. Klik op **Apply** (Toepassen).



## Verifiëren

De draadloze client komt omhoog en de gebruiker voert de URL, zoals [www.cisco.com](http://www.cisco.com), in de webbrowser in. Omdat de gebruiker niet is geverifieerd, wordt de gebruiker door de WLC omgeleid naar de externe web login URL.

De gebruiker wordt gevraagd om de gebruikersreferenties. Nadat de gebruiker de gebruikersnaam en het wachtwoord heeft ingevoerd, neemt de inlogpagina de inloggegevens van de gebruiker in en stuurt de aanvraag bij het indienen terug naar het `action_URL`-voorbeeld `http://1.1.1.1/login.html` van de WLC-webserver. Dit wordt geleverd als een invoerparameter voor de klant om URL om te leiden, waarbij 1.1.1.1 het Virtual Interface Address op de switch is.

De WLC authenticceert de gebruiker tegen de lokale database die op de WLC is geconfigureerd. Na succesvolle verificatie stuurt de WLC-webserver de gebruiker door naar de geconfigureerde doorverwijzing-URL of naar de URL waarmee de client is gestart, zoals [www.cisco.com](http://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.

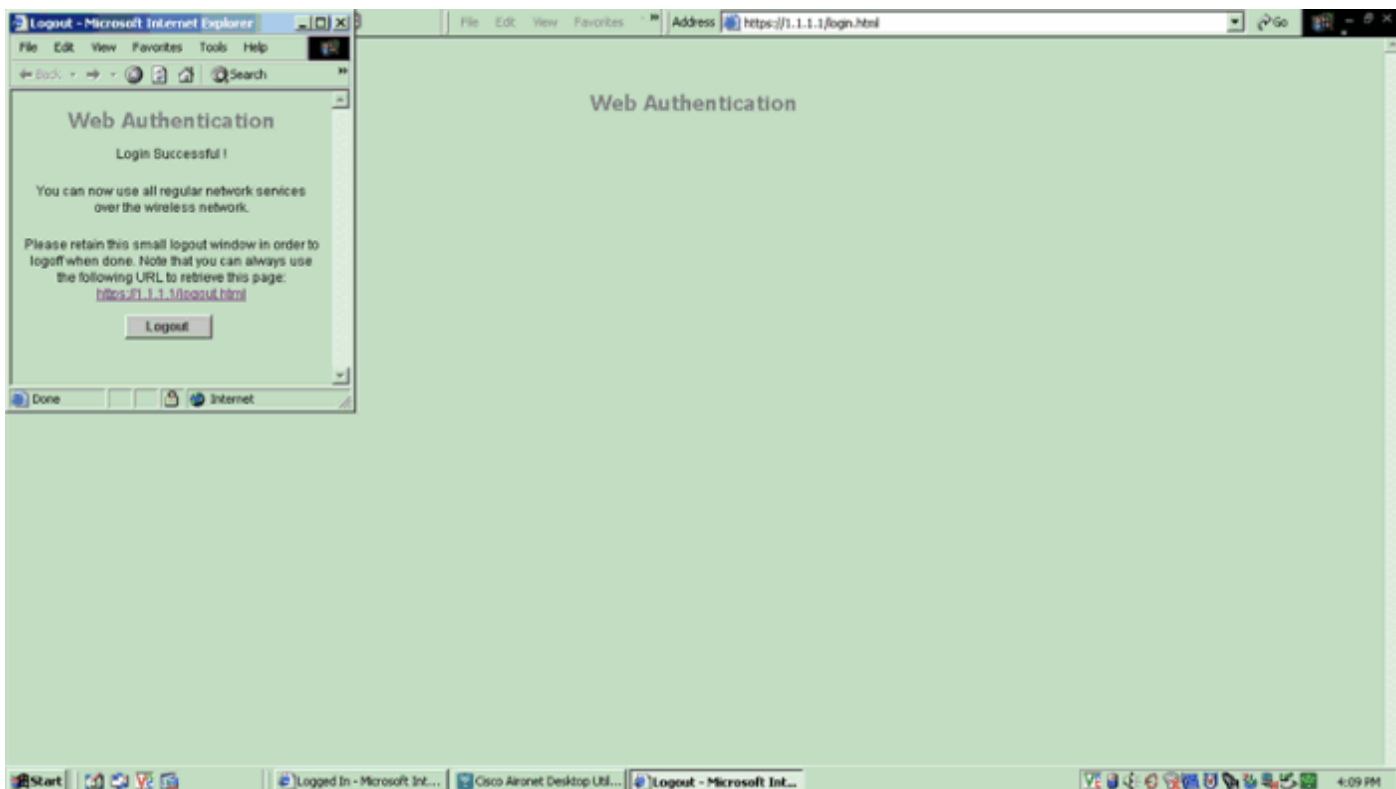
Do you want to proceed?

# Web Authentication

User Name

Password





## Problemen oplossen

Gebruik deze debug commando's om problemen op te lossen uw configuratie.

- debug mac addr <client-MAC-adres xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem gebeurtenissen activeren
- debug DHCP bericht activeren
- debug DHCP-pakket inschakelen
- debug pm sh-appgw inschakelen
- debug pm sh-tcp inschakelen

Deze sectie bevat informatie om uw configuratie te troubleshooten.

## Clients die worden omgeleid naar externe webverificatieserver ontvangen een certificaatwaarschuwing

**Probleem:** wanneer clients worden omgeleid naar de externe webverificatieserver van Cisco, ontvangen deze een certificaatwaarschuwing. Er is een geldig certificaat op de server, en als u rechtstreeks verbinding maakt met de externe webverificatieserver, wordt de certificaatwaarschuwing niet ontvangen. Is dit omdat het virtuele IP-adres (1.1.1.1) van de WLC aan de client wordt getoond in plaats van het feitelijke IP-adres van de externe webverificatieserver die aan het certificaat is gekoppeld?

**Oplossing:** Ja. Of u nu wel of niet lokale of externe webverificatie uitvoert, u raakt nog steeds de interne webserver op de controller. Wanneer u doorverwijst naar een externe webserver, ontvangt u nog steeds de certificaatwaarschuwing van de controller tenzij u een geldig certificaat op de controller zelf hebt. Als de redirect wordt verzonden naar https, ontvangt u de certificaatwaarschuwing van de controller en van de externe webserver, tenzij beiden een geldig

certificaat hebben.

Om zich te ontdoen van de certificaatwaarschuwingen allemaal samen, moet u een basisniveau certificaat afgegeven en gedownload hebben op uw controller. Het certificaat wordt afgegeven voor een hostnaam en u zet die hostnaam in het veld DNS-hostnaam onder de virtuele interface op de controller. U moet ook de hostnaam toevoegen aan uw lokale DNS-server en deze naar het virtuele IP-adres (1.1.1.1) van de WLC richten.

Raadpleeg de [Generatie van het verzoek om certificaatondertekening \(CSR\) voor een certificaat van derden inzake een WLAN-controller \(WLC\)](#) voor meer informatie.

## Fout: "Pagina kan niet worden weergegeven"

**Probleem:** Nadat de controller is geüpgraded naar 4.2.61.0, wordt de foutmelding "pagina kan niet worden weergegeven" weergegeven wanneer u een gedownloade webpagina voor webverificatie gebruikt. Dit werkte goed voor de upgrade. De standaard interne webpagina laadt zonder enig probleem.

**Oplossing:** Vanaf WLC versie 4.2 en later wordt een nieuwe functie geïntroduceerd waar u meerdere aangepaste login pagina's kunt hebben voor Web authenticatie.

Om de webpagina goed te laten laden, is het niet voldoende om het web-authenticatie type zoals globaal **aangepast** in de **Security > Web Auth > Web login pagina** instellen. Het moet ook worden geconfigureerd op een bepaalde WLAN. Voltooi de volgende stappen om dit te doen:

1. Log in op de GUI van de WLC.
2. Klik op het tabblad **WLAN's** en toegang tot het profiel van het WLAN dat is geconfigureerd voor webverificatie.
3. Klik op de pagina WLAN > Bewerken op het tabblad **Beveiliging**. Kies vervolgens **Layer 3**.
4. Kies op deze pagina **Geen** als Layer 3 Security.
5. Controleer het vakje **Web Policy** en kies de optie **Verificatie**.
6. Controleer het vakje Over-ride Global Config **Enable**, kies **Aangepast (gedownload)** als het Web Auth Type en selecteer de gewenste inlogpagina in het keuzemenu **Login Page**. Klik op **Apply** (Toepassen).

## Gerelateerde informatie

- [Configuratie van draadloze LAN-controller en webverificatie - voorbeeld](#)
- [Video: webverificatie op Cisco draadloze LAN-controllers \(WLC's\)](#)
- [Configuratievoorbeeld van VLAN's op wireless LAN-controllers](#)
- [Basisconfiguratievoorbeeld van draadloze LAN-controller en lichtgewicht access point](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.