External Web Authentication with Wireless LAN Controllers Configuration Example

Document ID: 71881

Introduction

This document explains how to use an external web server in order to set up a wireless LAN controller (WLC) for web authentication.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of the configuration of Lightweight Access Points (LAPs) and Cisco WLCs
- Basic knowledge of Lightweight Access Point Protocol (LWAPP)
- Knowledge on how to set up and configure an external web server
- Knowledge on how to set up and configure DHCP and DNS servers

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2006 WLC that runs firmware release 4.0
- Cisco 1000 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 2.6
- External web server that hosts the web authentication login page

- DNS and DHCP Servers for address resolution and IP address allocation to wireless clients

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP−related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN (WLAN), their users must enter the username and password when prompted by a login window.

Use these features to perform web authentication on the WLC:

- Default login window
- Modified version of the default login window
- A customized login window that you configure on an external web server (External web authentication)
- A customized login window that you download to the controller

This document provides a configuration example to explain how to configure the WLC to use a login script from an external web server.

External Web Authentication Process

This is the sequence of events when a wireless client tries to access a WLAN network which has external web authentication enabled:

1. The client (end user) opens a web browser with a URL, such as www.yahoo.com.
2. If the client is not authenticated, the WLC forwards the request to the web server of the WLC in order to collect client authentication credentials.
3. Because external web authentication is used, the WLC redirects the user to the external web server URL. The external web auth login URL is appended with parameters such as the AP_Mac_Address, the client_url (www.yahoo.com) and the action_URL that the customer needs to contact the switch web server.
4. The external web server URL leads the user to a login page. At this point, the user can use a preauthentication access control list (ACL) in order to access the Walled Garden Sites.
5. The login page takes user credentials input, and sends the request back to the action_URL example, http://1.1.1.1/login.html, of the WLC web server. This is provided as an input parameter to the customer redirect URL, where 1.1.1.1 is the Virtual Interface Address on the switch.
6. The WLC web server submits the username and password for authentication.
7. The WLC initiates the RADIUS server request or uses the local database on the WLC and authenticates the user.
8. If authentication is successful, the WLC web server either forwards the user to the configured redirect URL or to the URL the client started with, such as www.yahoo.com.
9. If authentication fails, then the WLC web server redirects user back to the customer login URL.

Note: In order to configure external webauthentication to use ports other than HTTP and HTTPS, issue this command:

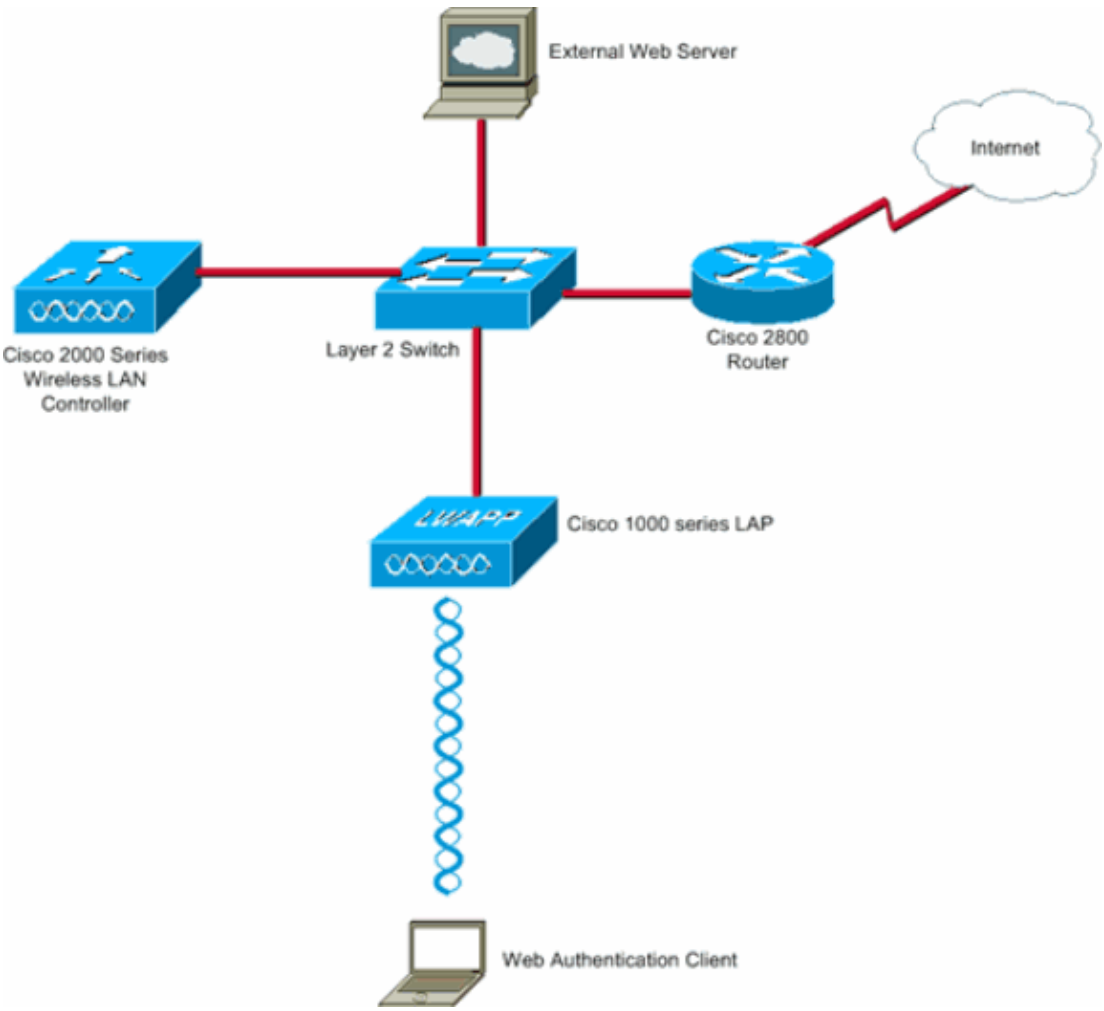
```
(Cisco Controller) >config network web-auth-port

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

Network Setup

The configuration example uses this setup. A LAP is registered to the WLC. You need to configure a WLAN guest for the guest users and have to enable web authentication for the users. You also need to ensure that the controller redirects the user to the external web server URL (external web authentication). The external web server hosts the web login page which is used for authentication.

Note: You can use a customized version of the login script, which will be used for web authentication. Here is a sample web_authentication.zip script that can be used for external web authentication. Right click and save this script to your external web server directory.

The user credentials must be validated against the local database maintained on the controller. After successful authentication, the users should be allowed access to the WLAN guest. You need to configure the controller and other devices for this setup.



Note: This document assumes that the DHCP, DNS and external web servers are configured. Refer to the appropriate third party documentation for information on how to configure the DHCP, DNS and external web server.

Configure

Before you configure the WLC for external web authentication, you must configure the WLC for basic operation and register the LAPs to the WLC. This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. Refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) if you are a new user trying to set up the WLC for basic operation with LAPs.

Complete these steps in order to configure the LAPs and WLC for this setup:

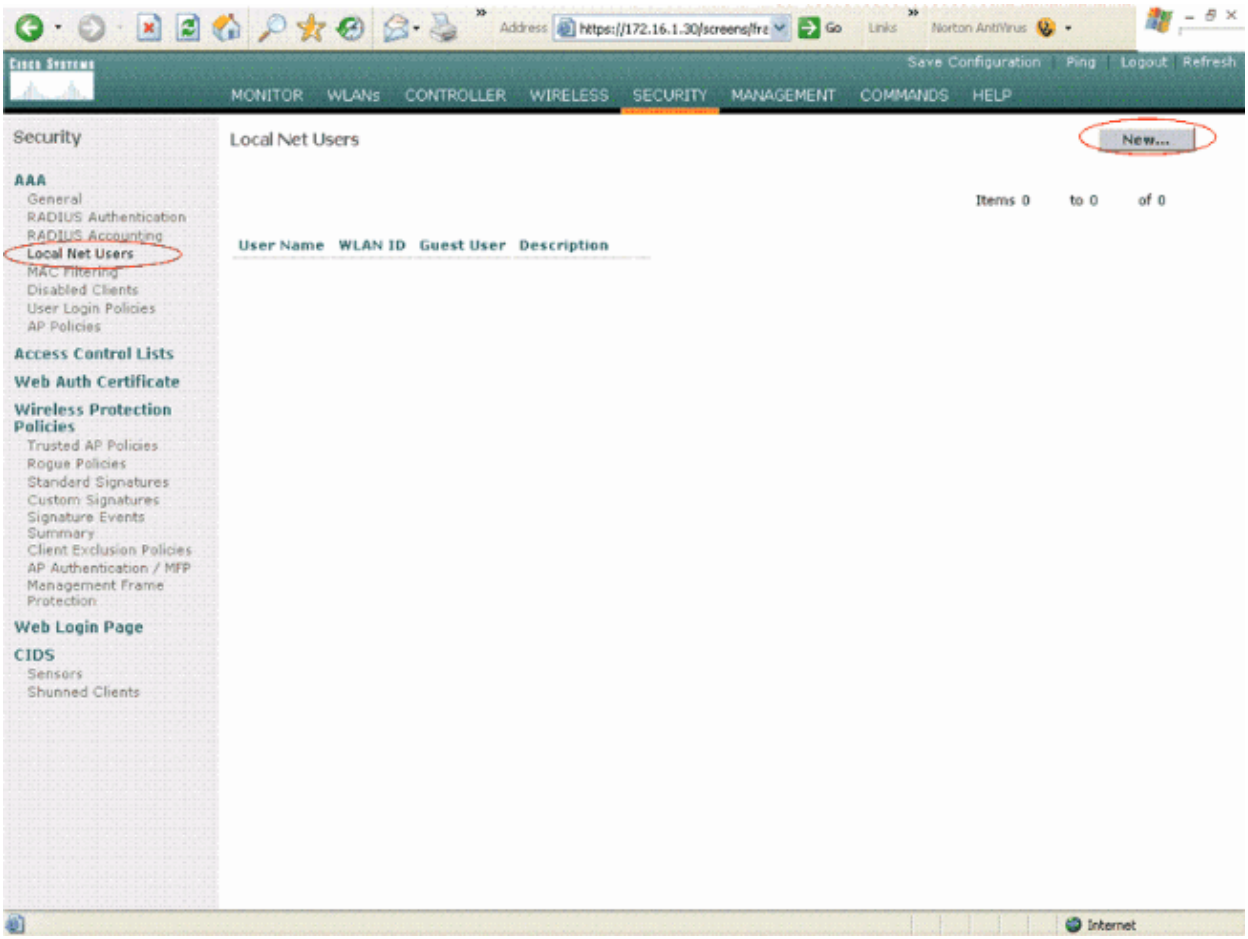
1. Create a Local Database on the WLC for the Guest Users
2. Create a Preauthentication ACL (Only for 2000 Series WLCs)
3. Create a Dynamic Interface for the Guest Users
4. Configure the WLAN for Guest Users
5. Configure the WLC for External Web Authentication

Create a Local Database on the WLC for the Guest Users

Local authentication allows the local authentication of the user to the WLC. You must create a Local Net User and define a password for web authentication client login. Complete these steps in order to create the user database on the WLC:

1. From the WLC GUI, choose **Security**.
2. Click **Local Net Users** from the AAA menu on the left.
3. Click **New** in order to create a new user.

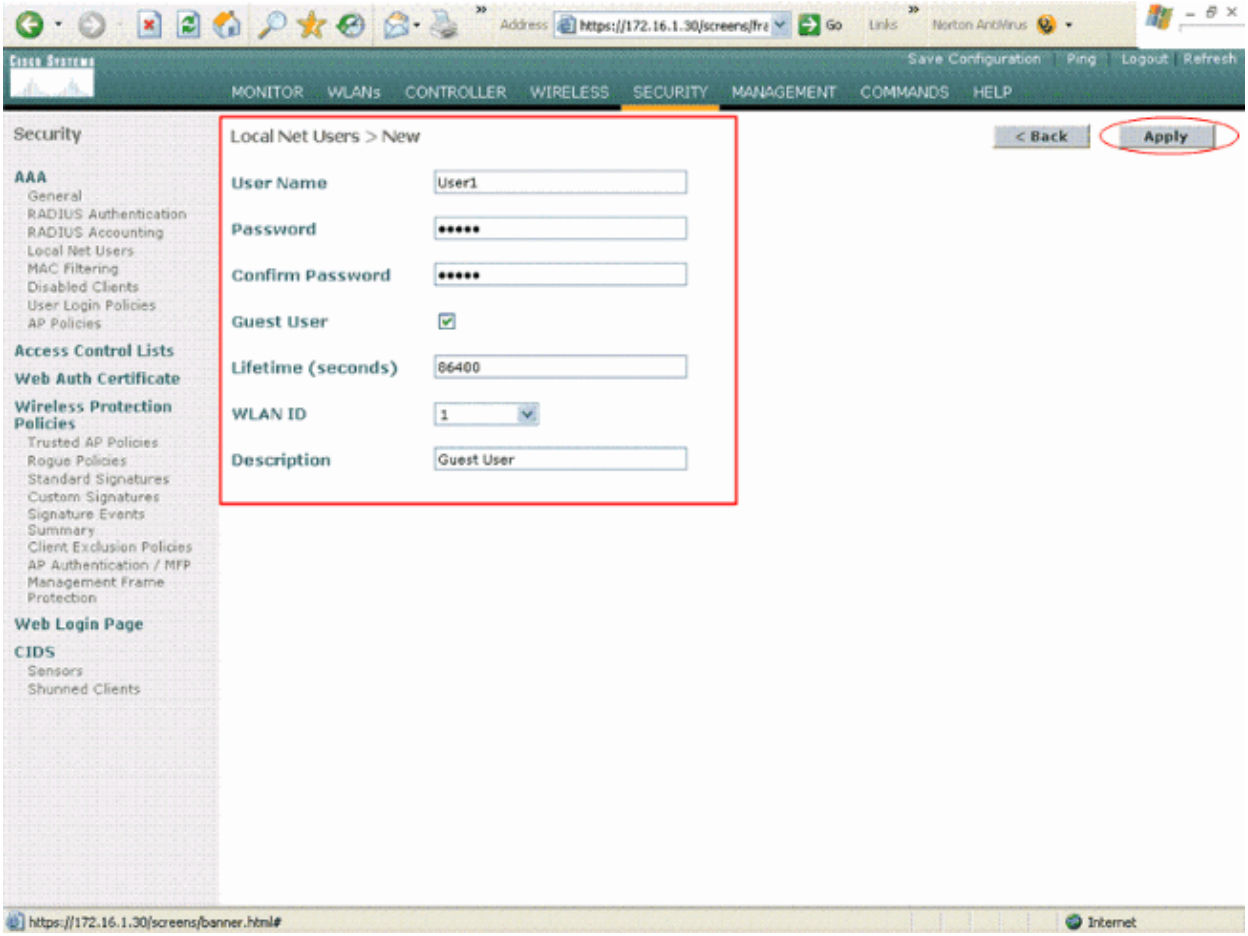
   A new window displays that asks for username and password information.



4. Enter a User Name and Password in order to create a new user, then confirm the password that you want to use.

   This example creates the user named **User1**.
5. Add a description, if you choose.

   This example uses **Guest User**.
6. Click **Apply** in order to save the new user configuration.



7. Repeat steps 3−6 to add more users to the database.

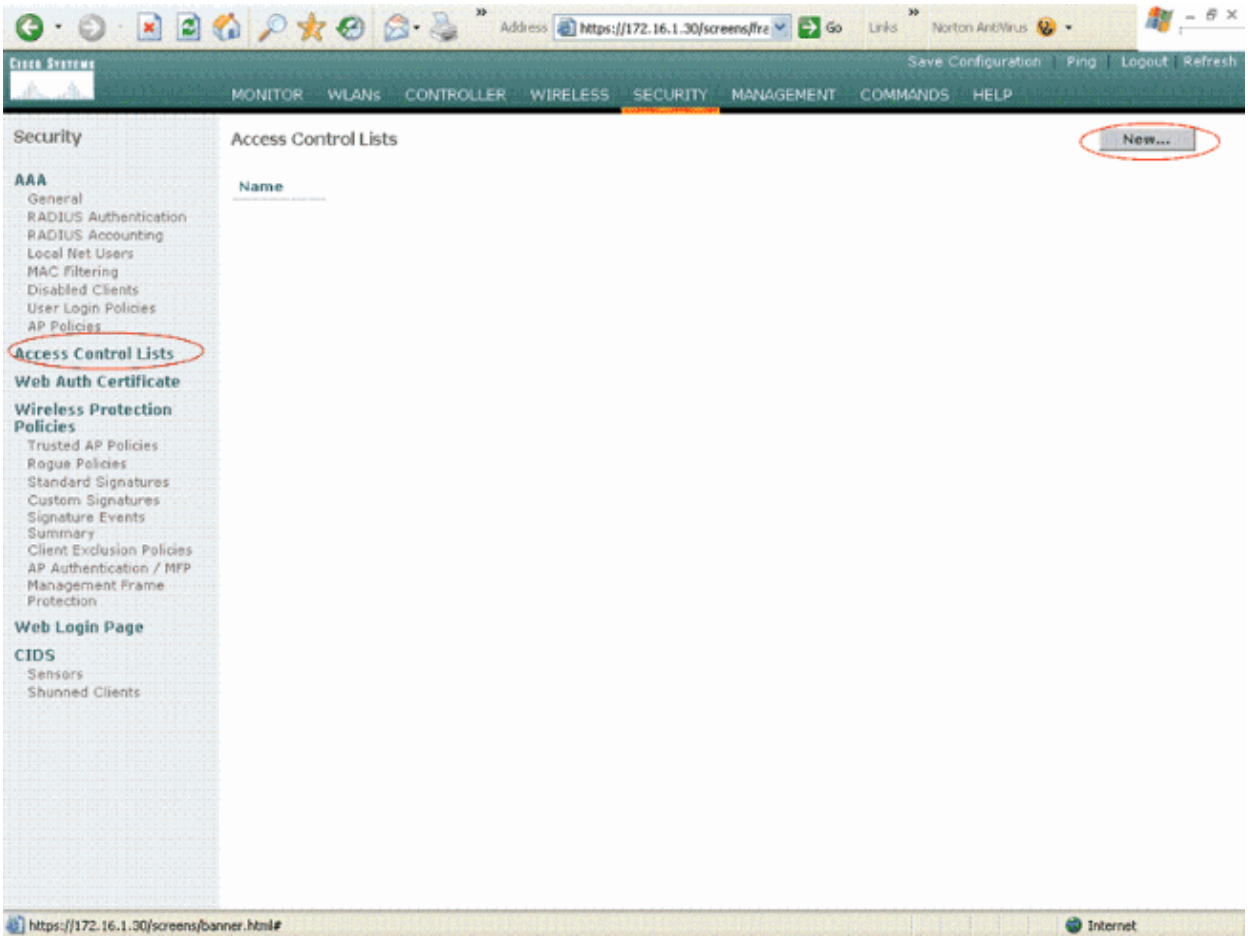
   Note: You can also use a RADIUS server, such as Cisco Secure ACS or any other RADIUS server, to create a user database. Refer to the RADIUS server documentation for instructions on how to create the user database.

Create a Preauthentication ACL (Only for 2000 Series WLCs)

For 2000 Series WLCs, you need to configure a preauthentication ACL on the WLAN to allow wireless clients to be redirected to the external web server login URL. This ACL should be set as the WLAN preauthentication ACL under Web Policy. Complete these steps in order to configure the preauthentication ACL for the WLAN:

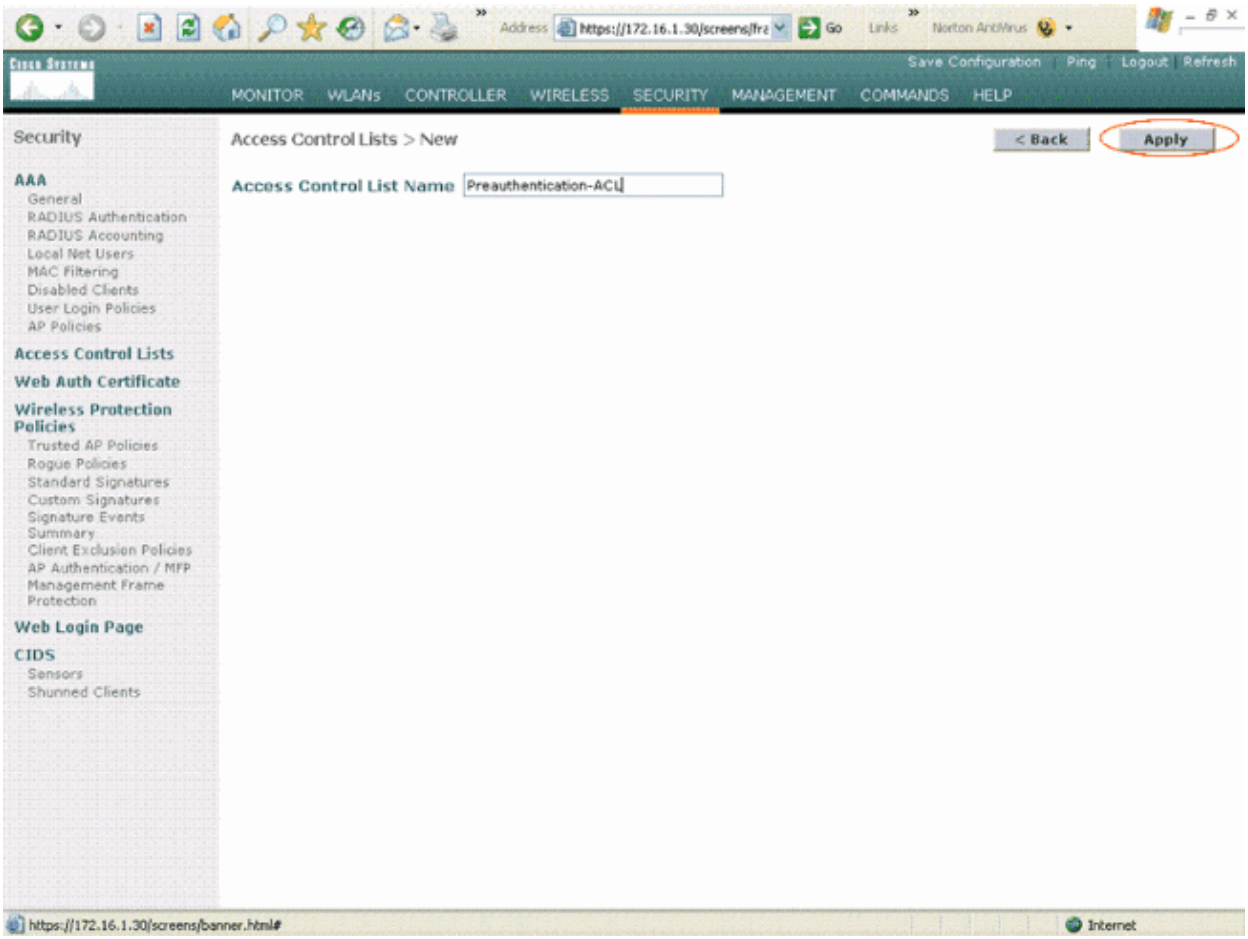
1. From the WLC GUI, choose **Security > Access Control Lists**.

   This window allows you to view current ACLs that are similar to standard firewall ACLs.
2. Click **New** in order to create a new ACL.

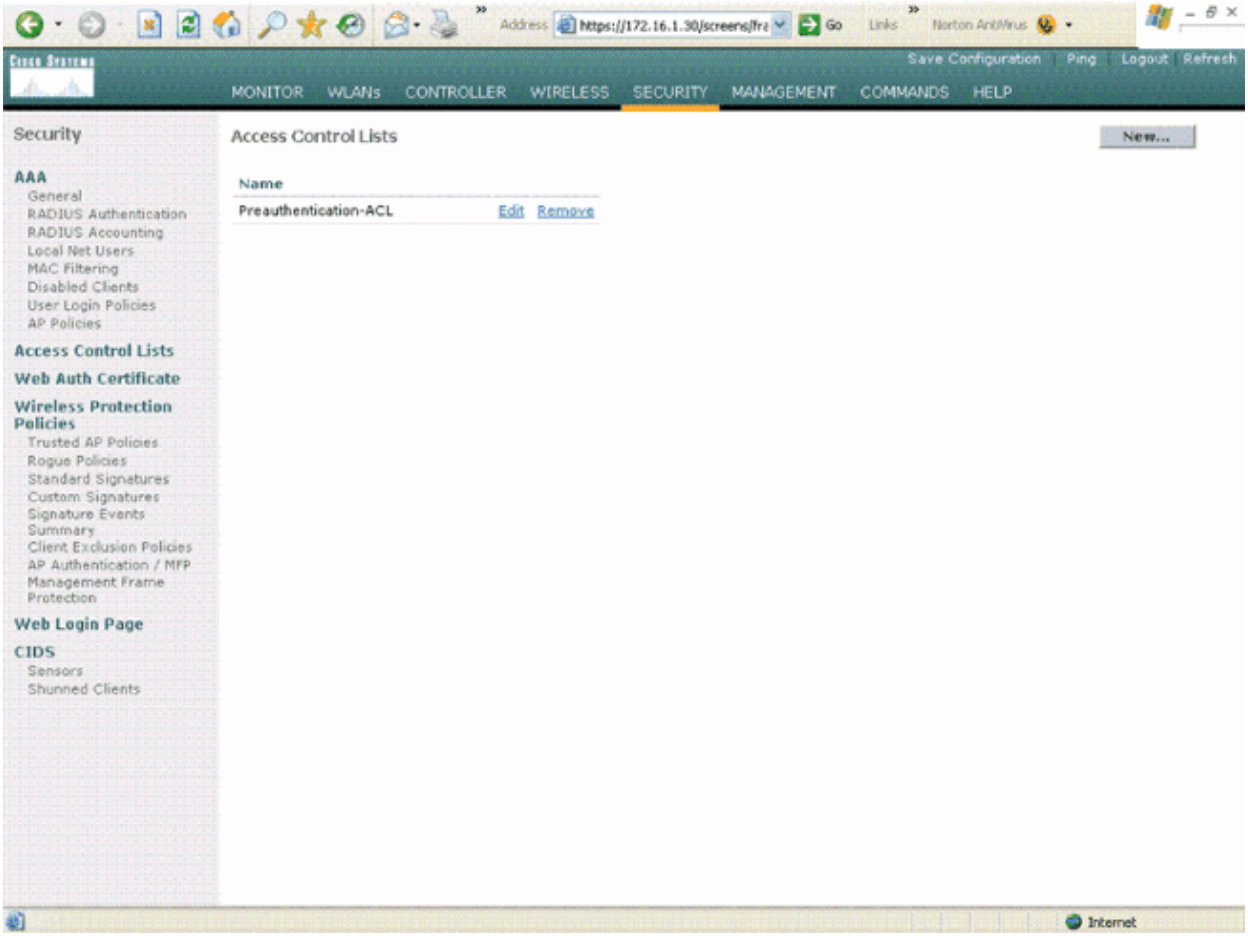


3. Enter the name of the ACL and click **Apply**.

   In this example, the ACL is named **Preauthentication−ACL**.

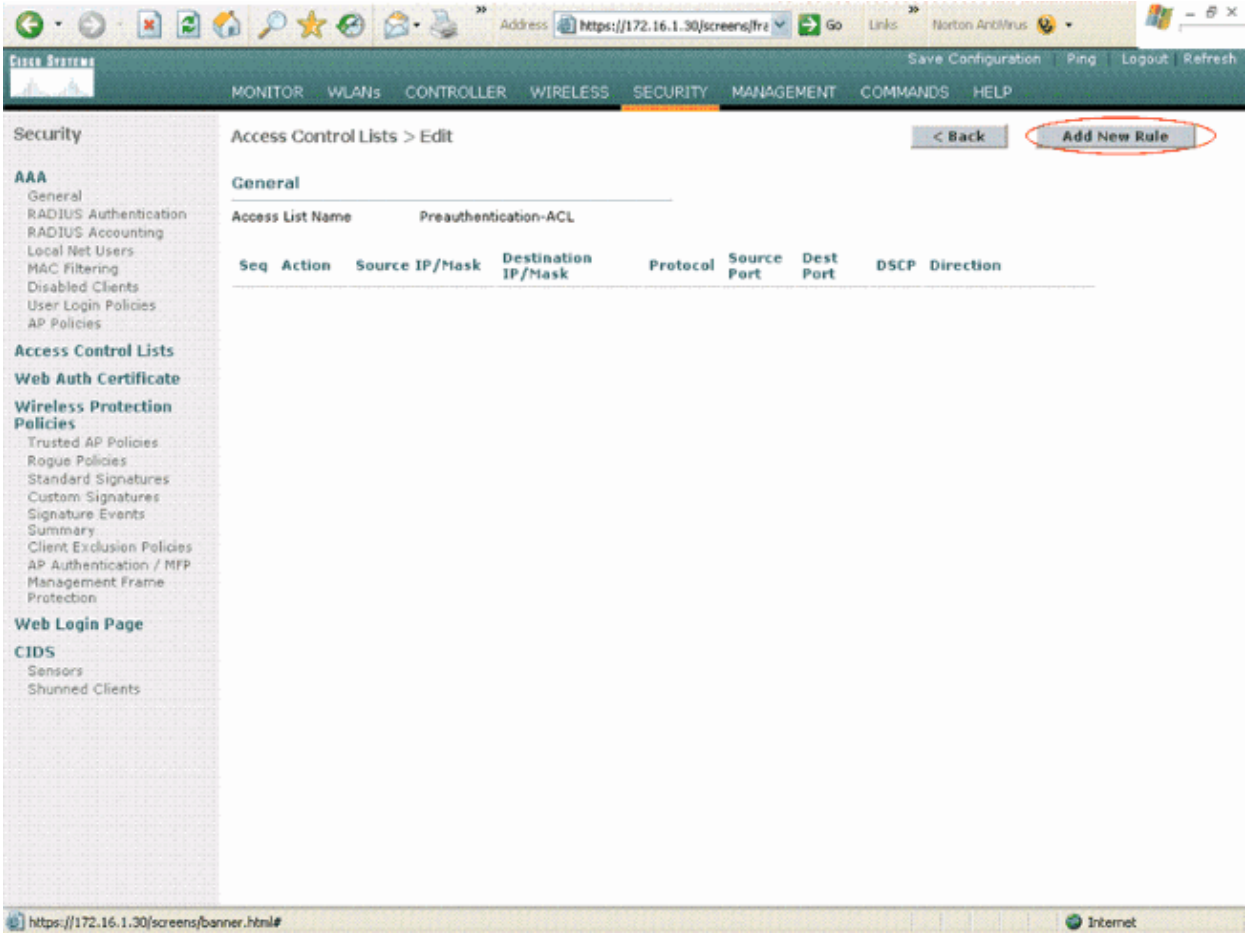


4. For the new ACL created, click **Edit**.



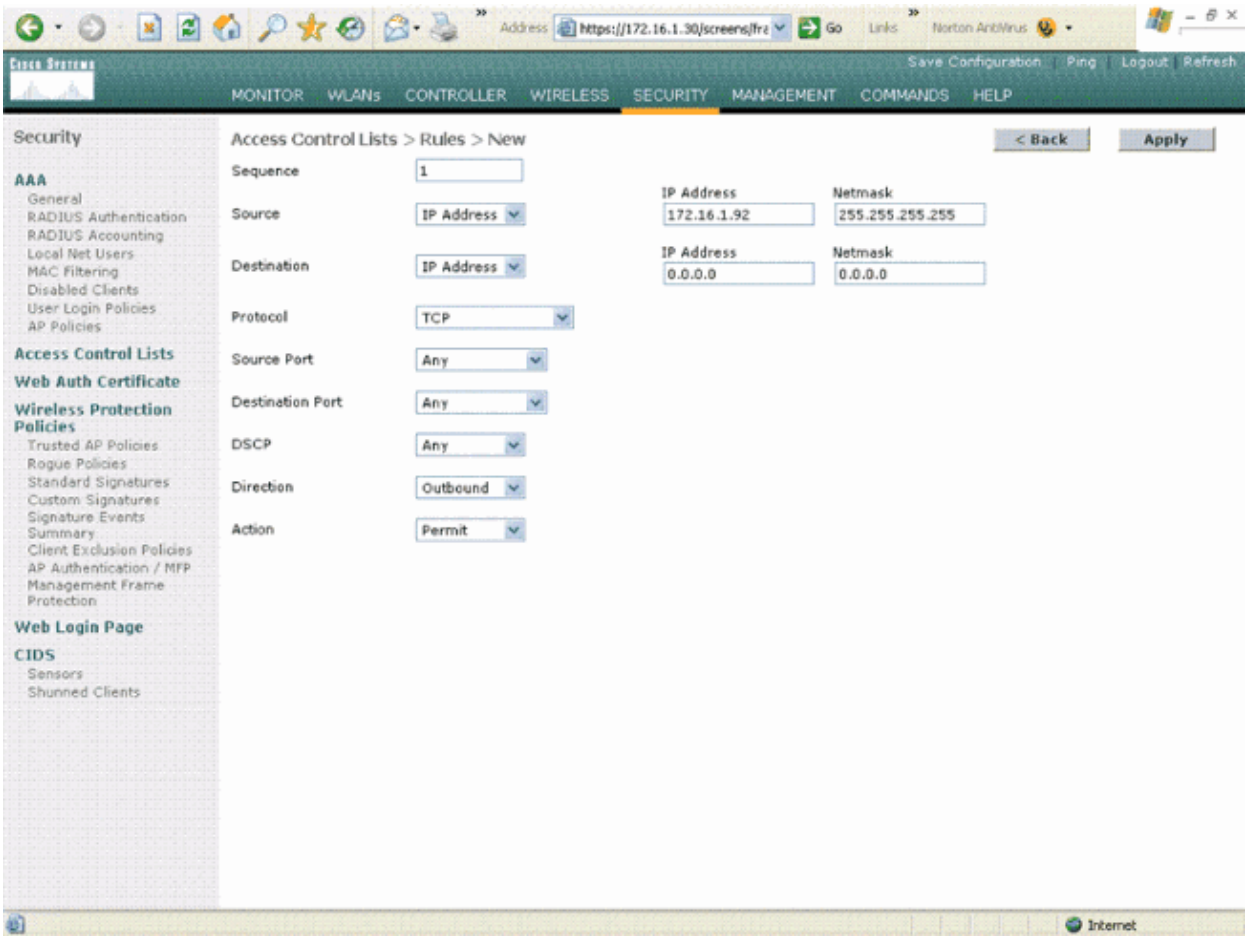
The ACL > Edit window appears. This window lets the user define new rules or modify rules of the ACL that exist.

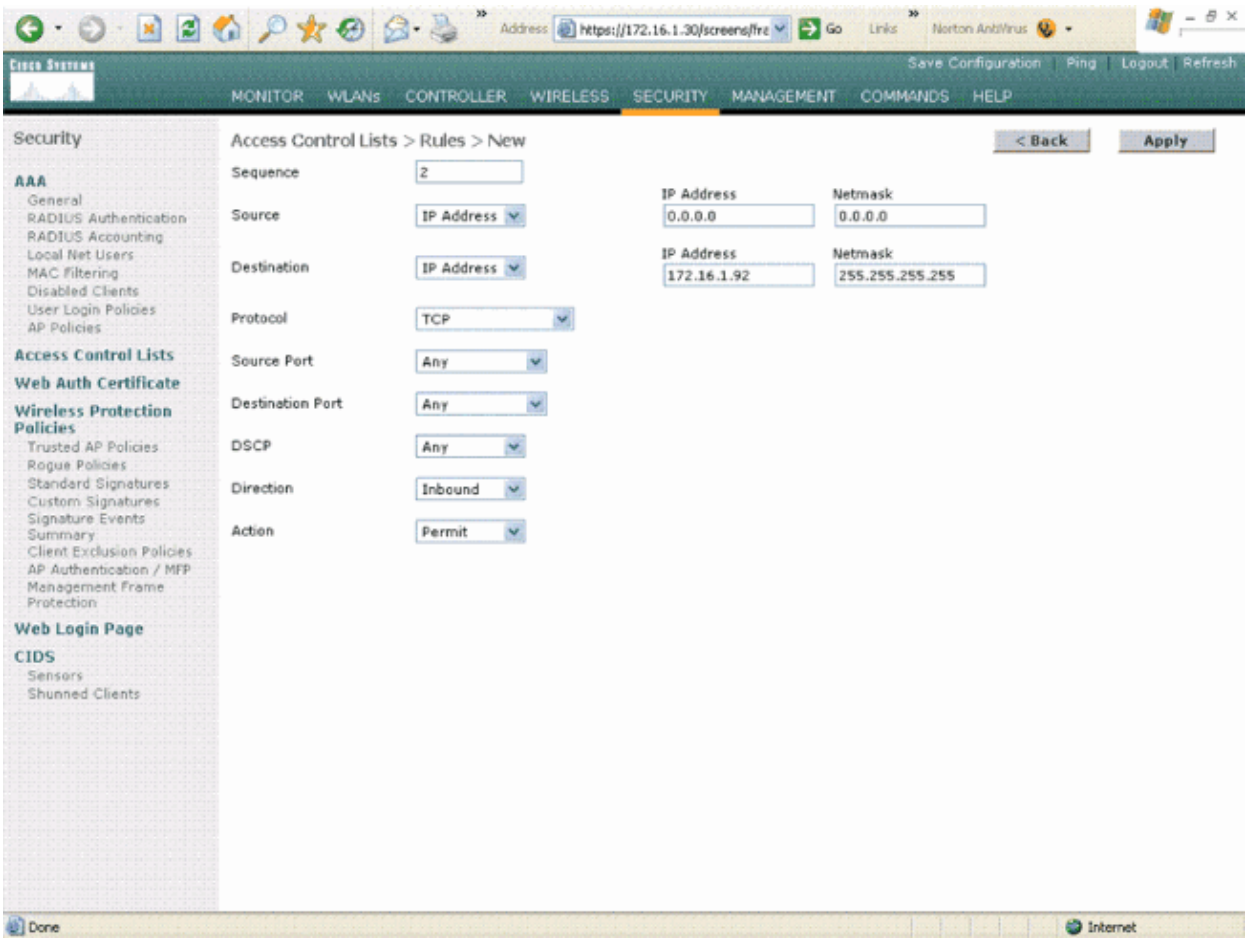
5. Click **Add New Rule**.



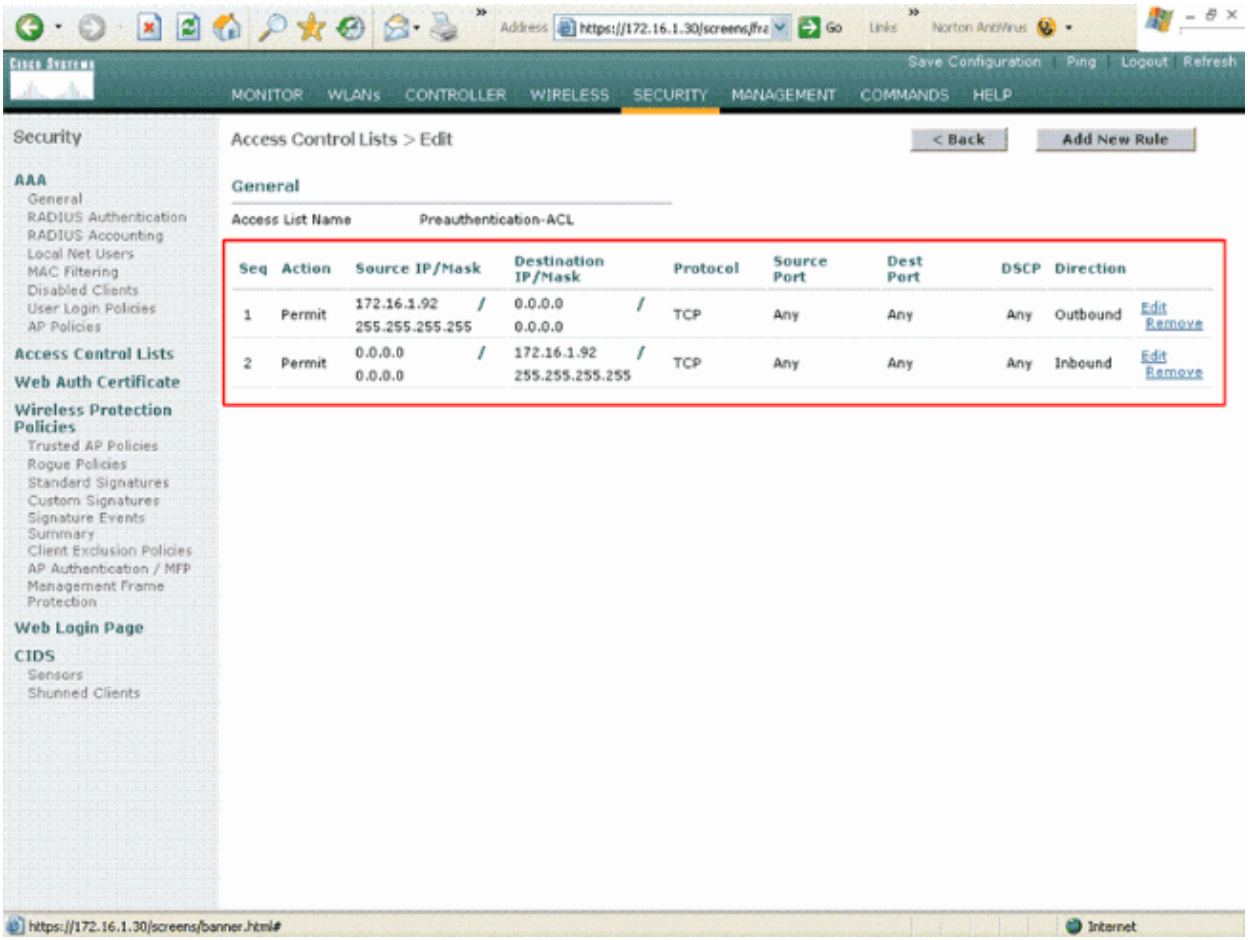
6. Define an ACL rule which allows access for the clients to the external web server.

   In this example, 172.16.1.92 is the external web server IP address.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence
1
Source
IP Address
IP Address
172.16.1.92
Netmask
255.255.255.255
Destination
IP Address
IP Address
0.0.0.0
Netmask
0.0.0.0
Protocol
TCP
Source Port
Any
Destination Port
Any
DSCP
Any
Direction
Outbound
Action
Permit
Internet


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence
2
Source
IP Address
IP Address
0.0.0.0
Netmask
0.0.0.0
Destination
IP Address
IP Address
172.16.1.92
Netmask
255.255.255.255
Protocol
TCP
Source Port
Any
Destination Port
Any
DSCP
Any
Direction
Inbound
Action
Permit
Done
Internet

7. Click **Apply** in order to commit the changes.



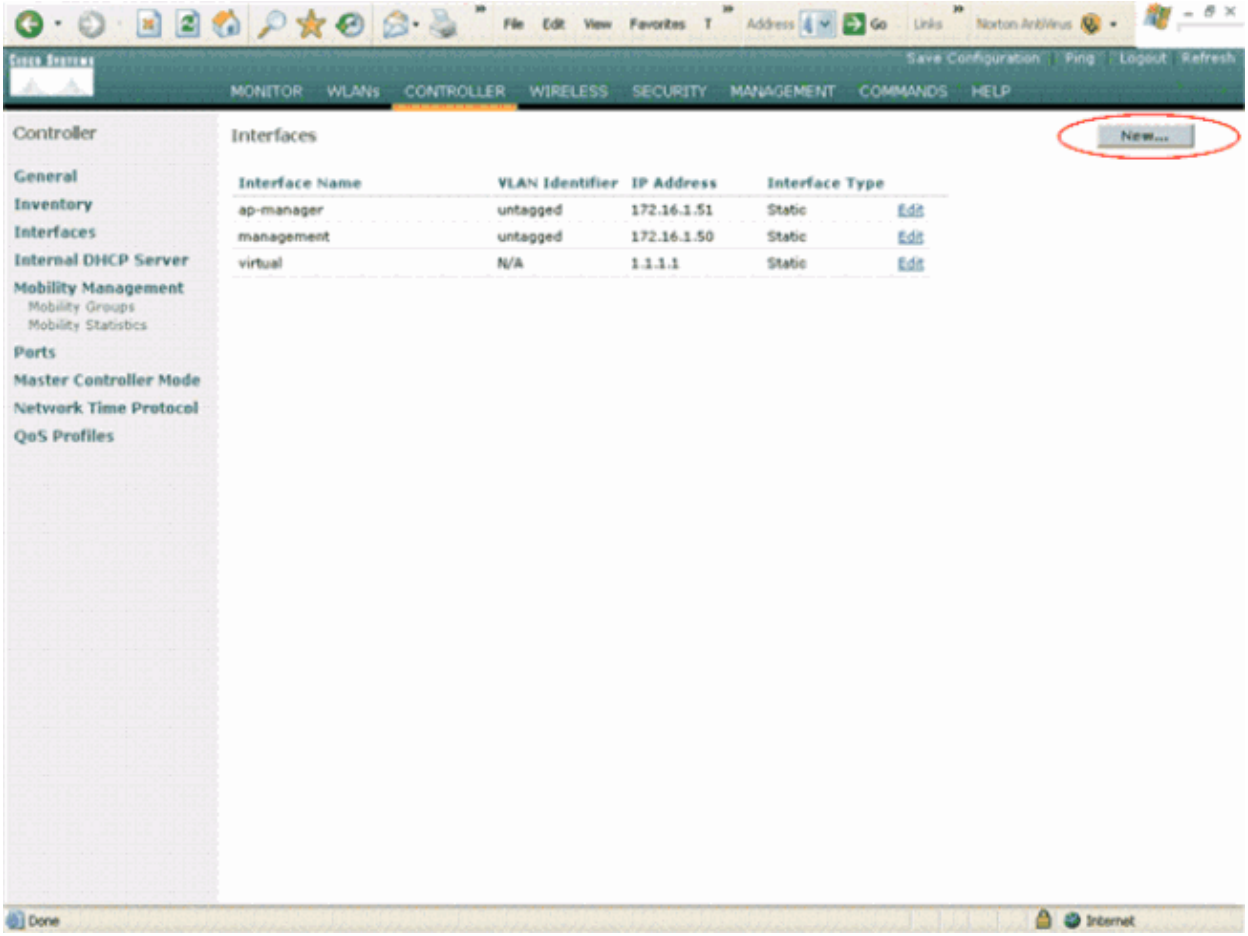
Note: You do not need to configure any preauthentication ACL for Cisco 4100 Series WLCs or Cisco 4400 Series WLCs.

Create a Dynamic Interface for the Guest Users

Complete these steps in order to create a dynamic interface for the guest users:

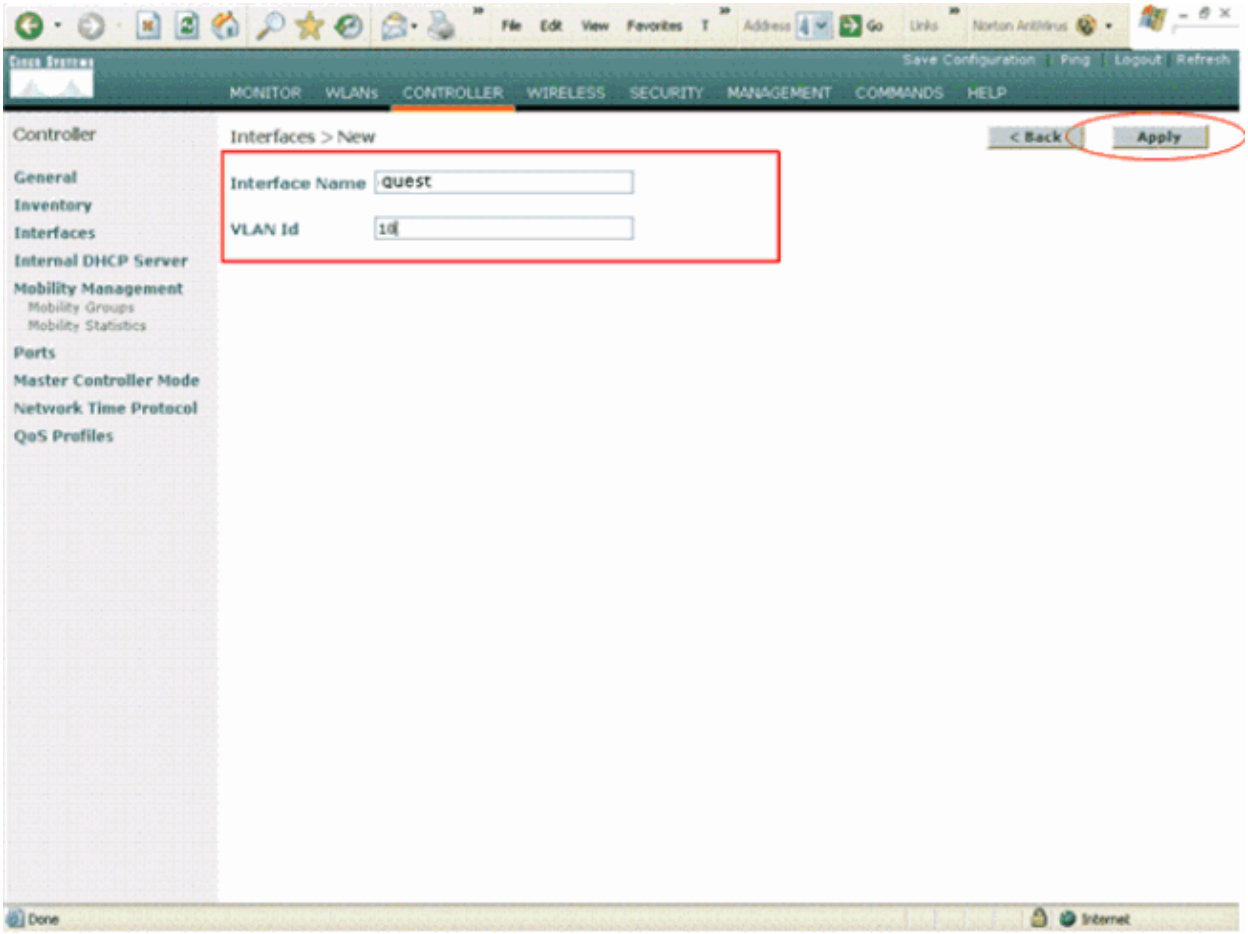
1. From the WLC GUI, choose **Controllers > Interfaces**.

   The Interfaces window appears. This window lists the interfaces that are configured on the controller. This includes the default interfaces, which are the management interface, ap−manager interface, the virtual interface and the service port interface, and the user defined dynamic interfaces.

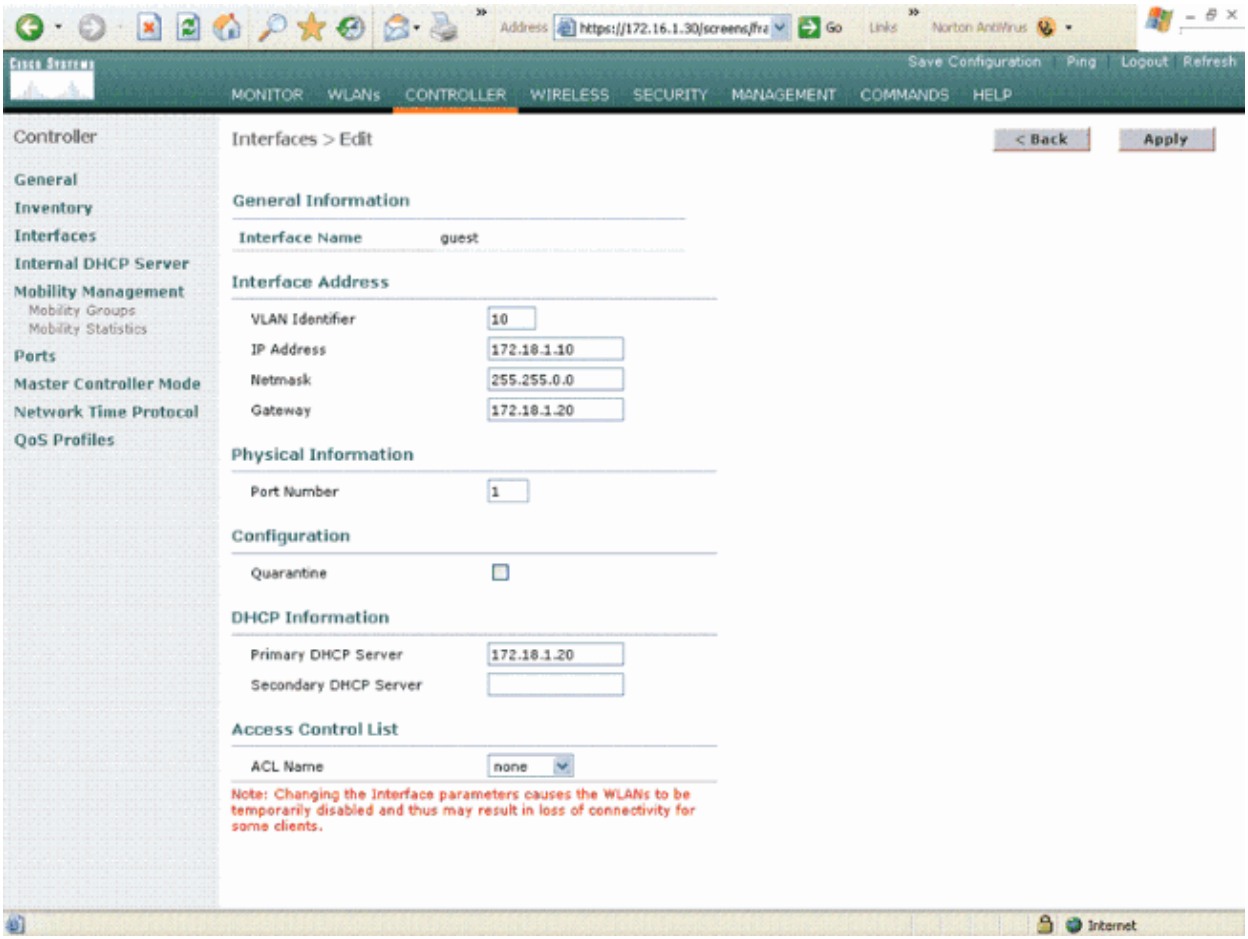


2. Click **New** in order to create a new dynamic interface.
3. In the Interfaces > New window, enter the Interface Name and the VLAN Id. Then, click **Apply**.

   In this example, the dynamic interface is named **guest** and the VLAN Id is assigned **10**.



4. In the Interfaces > Edit window, for the dynamic interface, enter the IP address, the subnet mask, and the default gateway. Assign it to a physical port on the WLC, and enter the IP address of the DHCP server. Then, click **Apply**.



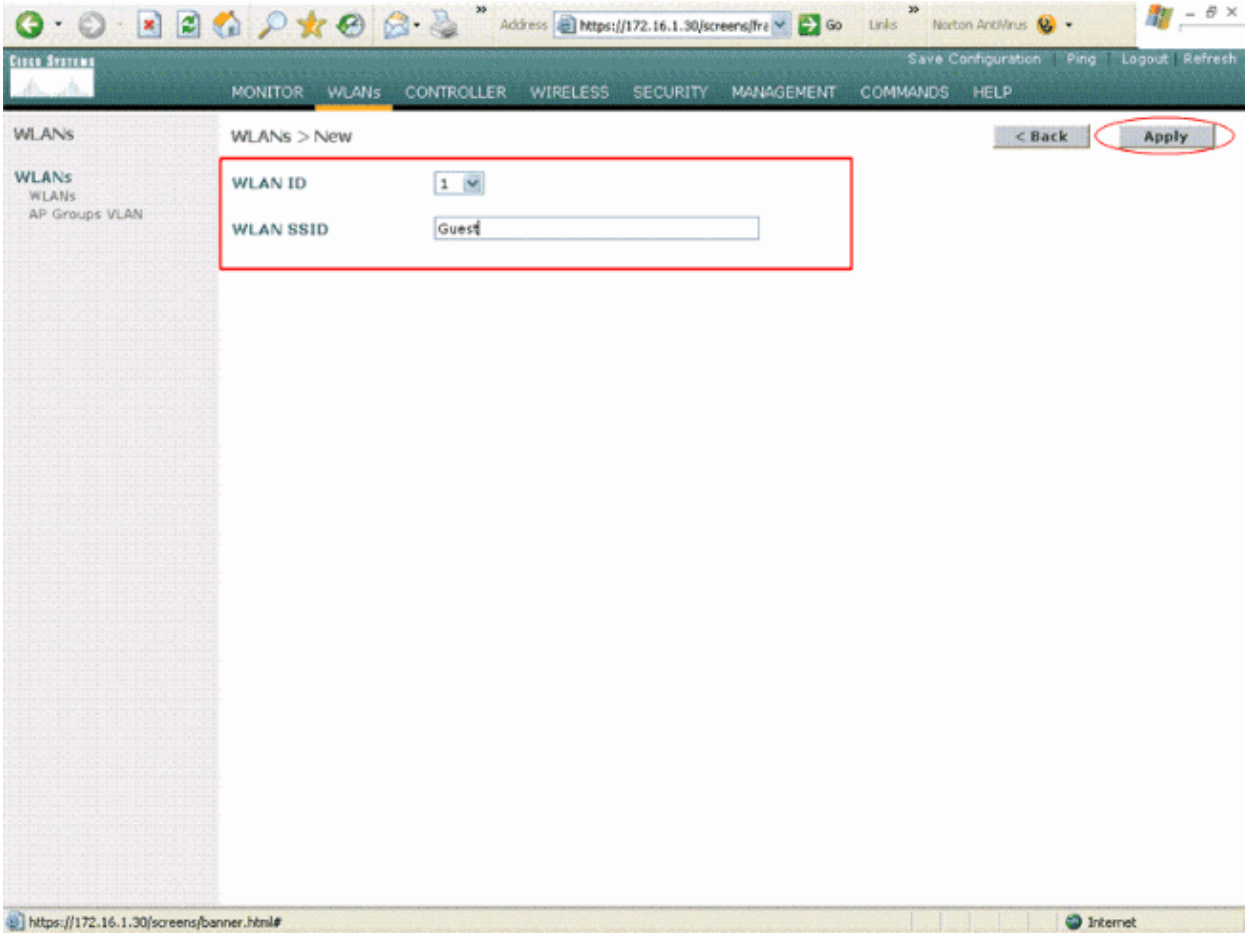
Configure the WLAN for Guest Users

The next step is to create WLANs for the guest users. Also, the security methods that are used to authenticate the guest and wireless users must be defined. Complete these steps:

1. Click **WLANs** from the controller GUI in order to create a WLAN.

   The WLANs window appears. This window lists the WLANs configured on the controller.
2. Click **New** in order to configure a new WLAN.

   In this example, the WLAN is named **Guest** and the WLAN ID is **1**.
3. Click **Apply**.



4. In the WLAN > Edit window, define the parameters specific to the WLAN.

   a. For the guest WLAN, choose the appropriate interface from the Interface Name field.

      This example maps the dynamic interface **guest** that was previously created to the WLAN guest.

   b. In the Layer 3 Security field, check the **Web Policy** check box and choose the **Authentication** option.

      This option is chosen because web authentication is used to authenticate the wireless guest clients.

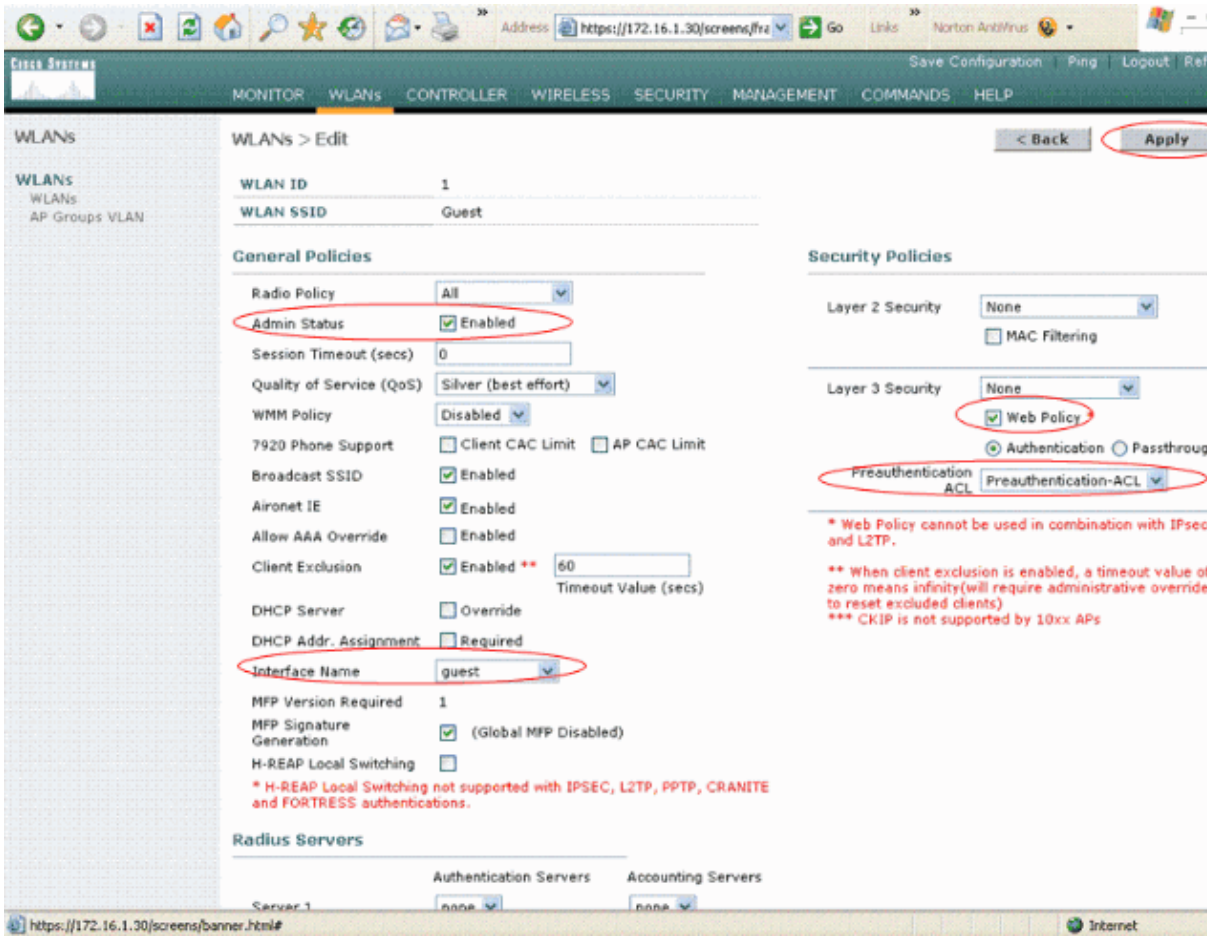
      Note: Web authentication is not supported with 802.1x authentication. This means you cannot choose 802.1x or a WPA/WPA2 with 802.1x as the Layer 2 security when you use web authentication.

      Note: Web authentication is supported with all other Layer 2 security parameters.

   c. Choose the appropriate Preauthentication ACL from the drop−down menu.

      In this example, the preauthentication ACL that was created previously is used.

   d. Click **Apply**.

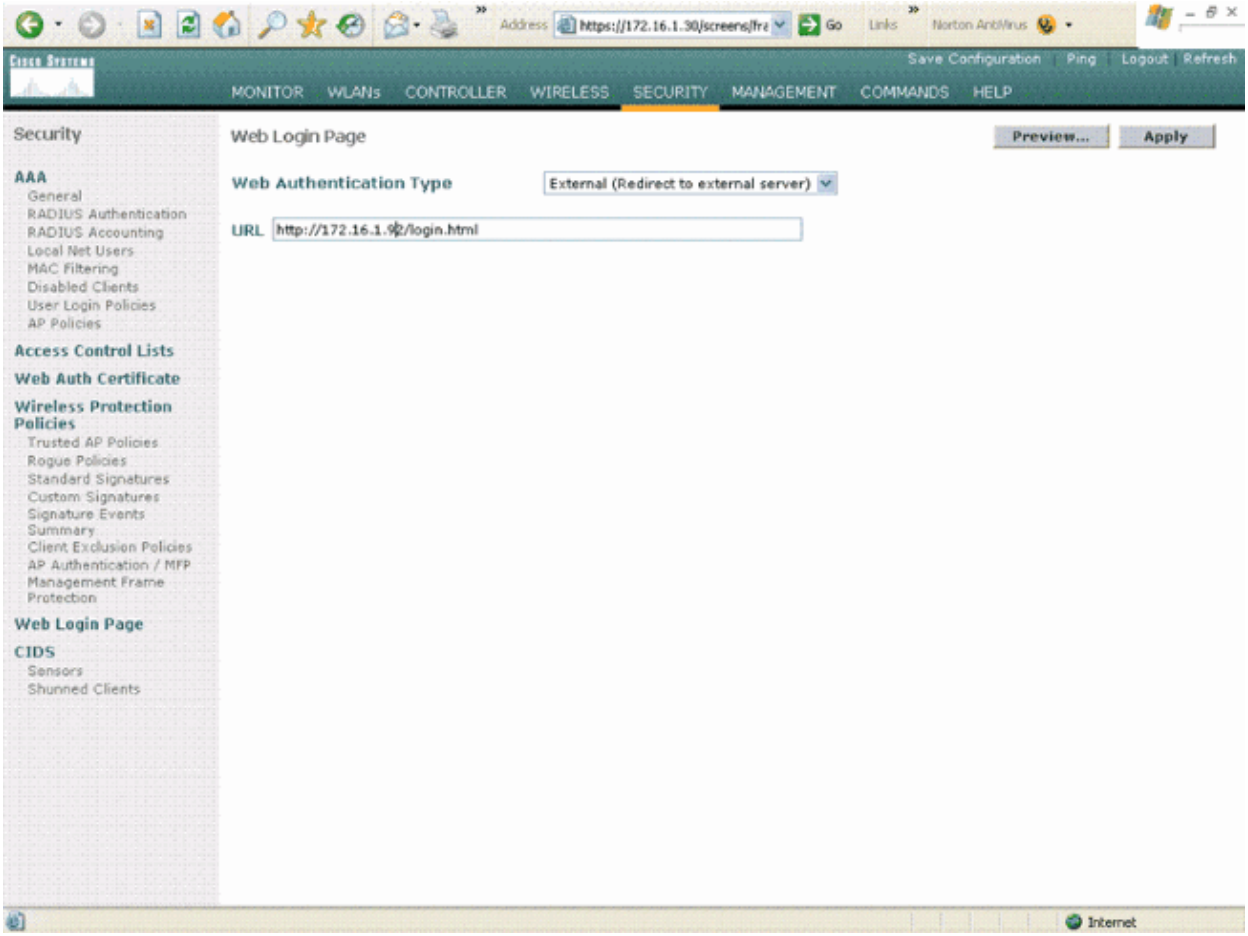


Note: In this example, Layer 2 Security methods to authenticate guest users are not used. Therefore, choose **None** in the Layer 2 Security field. By default, the Layer 2 Security option is 802.1x.

Configure the WLC for External Web Authentication

The final step is to configure the WLC for the external web authentication. Complete these steps:

1. From the controller GUI, choose **Security > Web Login Page** in order to access the Web Login Page.
2. From the Web Authentication Type drop−down box, choose **External (Redirect to external server)**.
3. In the URL field, enter the URL of the customized web authentication login window on your web server. You can enter up to 252 characters.



Now all the devices are set up. You can try to connect a wireless client and check if the configuration works as expected.

Note: The URL present in the **Redirect URL after login** field that appears in the GUI when internal web authentication is selected will also be used for external web authentication. In order to change the Redirect URL after login for external web authentication, use this CLI command:

```
config custom-web redirectUrl <URL>
```

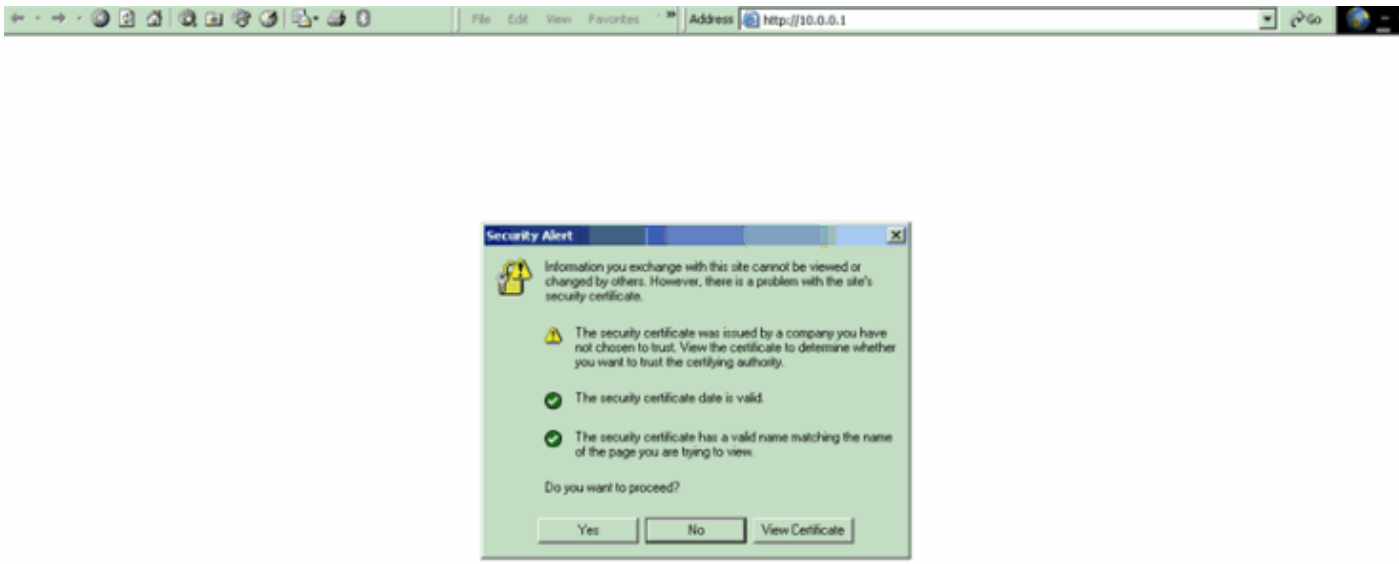
Note: In WLC version 5.0 and later, the logout page for web−authentication can also be customized. Refer to the Assign Login , Login failure and Logout pages per WLAN section of Wireless LAN Controller Configuration Guide,5.2 for more information on how to configure it.

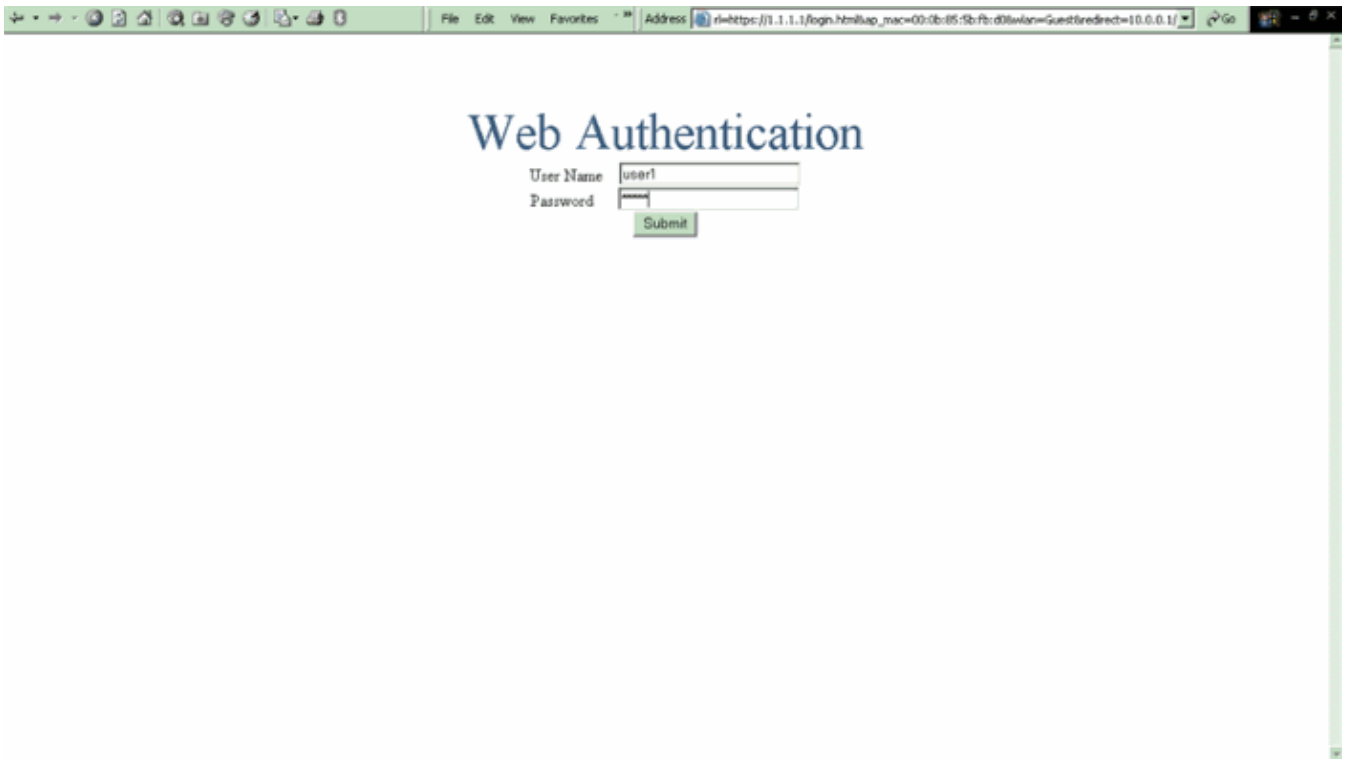
Verify

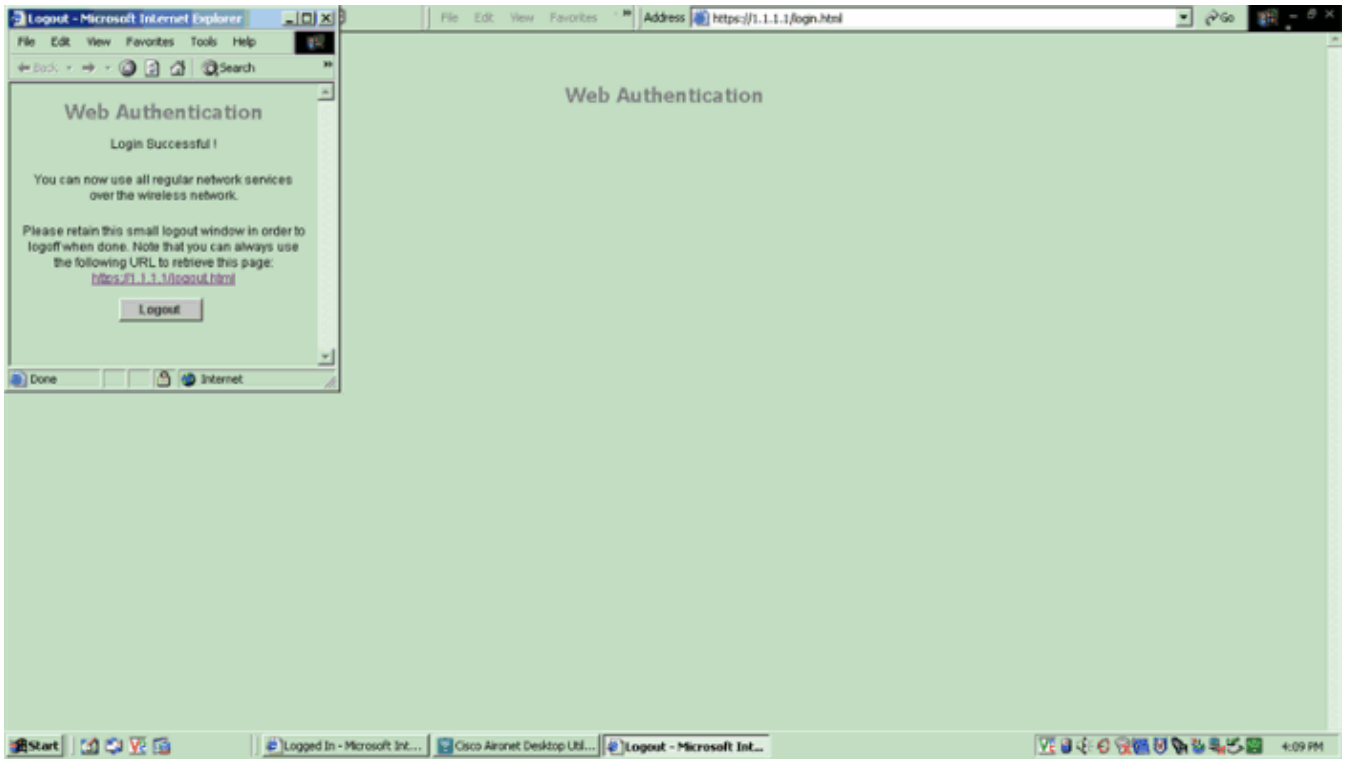
The wireless client comes up and the user enters the URL, such as www.yahoo.com, in the web browser. Because the user has not been authenticated, the WLC redirects the user to the external web login URL.

The user is prompted for the user credentials. Once the user submits the username and password, the login page takes user credentials input and on submit sends the request back to the action_URL example, http://1.1.1.1/login.html, of the WLC web server. This is provided as an input parameter to the customer redirect URL, where 1.1.1.1 is the Virtual Interface Address on the switch.

The WLC authenticates the user against the local database configured on the WLC. After successful authentication, the WLC web server either forwards the user to the configured redirect URL or to the URL the client started with, such as www.yahoo.com.


File Edit View Favorites
Address http://10.0.0.1
Go
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?
Yes
No
View Certificate


File Edit View Favorites
Address rl=https://1.1.1.1/login.html&ap_mac=00:0b:85:5b:fb:d0&wlan=Guest&redirect=10.0.0.1/
Go
Web Authentication
User Name
user1
Password
Submit



Troubleshoot

Use these debug commands in order to troubleshoot your configuration.

- 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 this section to troubleshoot your configuration.

Customized Logo for Web Authentication/Passthrough Does Not Load Upon Preview

This is because of Cisco bug ID CSCsg45847 (registered customers only) . When you use the Internal (Default) login page on theWLC for web authentication/passthrough, the preview page (available at the Security > Web login page on the WLC) loads without a problem. However, when a customer customizes the logo on the web authentication page (available internally on the controller), the preview function does not work.

The web authentication/passthrough page loads the customized web logo correctly when the wireless clients try to authenticate to the wireless network. Only the preview function does not work. This bug has been resolved in code 4.0.206.0.

Clients Redirected to External Web Authentication Server Receive a Certificate Warning

Problem: When clients are redirected to Cisco's external web authentication server, they receive a certificate warning. There is a valid certificate on the server, and if you connect to the external web authentication server directly the certificate warning is not received. Is this because the virtual IP address (1.1.1.1) of the WLC is presented to the client instead of the actual IP address of the external web authentication server that is associated with the certificate?

Solution: Yes. Whether or not you perform local or external web authentication, you still hit the internal web server on the controller. When you redirect to an external web server, you still receive the certificate warning from the controller unless you have a valid certificate on the controller itself. If the redirect is sent to https, you receive the certificate warning from the controller and from the external web server, unless both have a valid certificate.

In order to get rid of the certificate warnings all together, you need to have a root level certificate issued and downloaded onto your controller. The certificate is issued for a host name and you put that host name in the DNS host name box under the virtual interface on the controller. You also need to add the host name to your local DNS server and point it to the virtual IP address (1.1.1.1) of the WLC.

Refer to Certificate Signing Request (CSR) Generation for a Third−Party Certificate on a WLAN Controller (WLC) for more information.

Error: "page cannot be displayed"

Problem: After the controller is upgraded to 4.2.61.0, the "page cannot be displayed " error message appears when you use a downloaded web page for web authentication. This worked well prior to the upgrade. The default internal web page loads without any problem .

Solution: From the WLC version 4.2 and later a new feature is introduced wherein you can have multiple cutomized login pages for Web authentication.

In order to have the web page load properly, it is not sufficient to set the web−authentication type as **customized** globally in the **Security > Web Auth > Web login page**. It must also be configured on a particular WLAN . In order to do this, complete these steps:

1. Log into the GUI of the WLC.
2. Click on the **WLANs** tab, and access the profile of the WLAN configured for Web−authentication.
3. On the WLAN > Edit page, click the **Security** tab. Then, choose **Layer 3.**
4. On this page, choose **None** as the Layer 3 Security.
5. Check the **Web Policy** box, and choose the **Authentication** option.
6. Check the Over−ride Global Config **Enable** box, choose **Customized (Downloaded)** as the Web Auth Type, and select the desired login page from the **Login Page**pull down menu. Click **Apply**.

Related Information

- **Wireless LAN Controller Web Authentication Configuration Example**
- **VLANs on Wireless LAN Controllers Configuration Example**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Technical Support & Documentation − Cisco Systems**