Wireless LAN Controller Web Authentication Configuration Example

Document ID: 69340

Introduction

This document shows you how to configure a Cisco 4400 Series Wireless LAN (WLAN) Controller (WLC) to support a web authentication client.

Prerequisites

Requirements

This document assumes that you already have an initial configuration on the 4400 WLC.

Components Used

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

- A 4400 series WLC that runs version 5.0.148.0

- Cisco Secure Access Control Server (ACS) version 4.2 installed on a Microsoft Windows 2003 Server
- Cisco Aironet 1230 Series Light Weight Access Point
- Cisco Aironet 802.11 a/b/g CardBus Wireless Adapter that runs version 3.6

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.

Web Authentication

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. Web Authentication is the only security policy that allows the client to get an IP address before Authentication. It is a simple Authentication method without the need for a supplicant or client utility.Web authentication can be done either locally on a WLC or over a RADIUS server. Web authentication is typically used by customers who want to deploy a guest−access network. Typical deployments can include "hot spot" locations such as T−Mobile or Starbucks.

Web authentication provides simple authentication without a supplicant or client utility. Keep in mind that web authentication does not provide data encryption. Web authentication is typically used as simple guest access for either a "hot spot" or campus atmosphere where the only concern is the connectivity.

In this document a new VLAN interface is created along with a WLAN for web authentication. This VLAN interface is assigned to the WLAN so that the users associating to this WLAN are on a separate subnet. In situations where you do not want a separate subnet, you can associate the Management interface to the WLAN. The Configure the Controller for Web Authentication section of this document provides the procedure to create a new VLAN interface.

Configure the Controller for Web Authentication

In this document, a WLAN is configued for web authentication and mapped it to a dedicated VLAN. These are the steps involved to configure a WLAN for web authentication:

- Create a VLAN Interface
- Add a WLAN Instance
- Set Up DHCP and DNS Servers on the WLC
- Reboot the WLC
- Configure Authentication Type (Two Ways to Authenticate Users in Web Authentication)

In this section, you are presented with the information to configure the controller for web authentication.

These are the IP addresses used in this document:

- The IP address of the Wireless LAN Controller (WLC) is 10.77.244.204.
- The IP address of the the ACS server is 10.77.244.196.

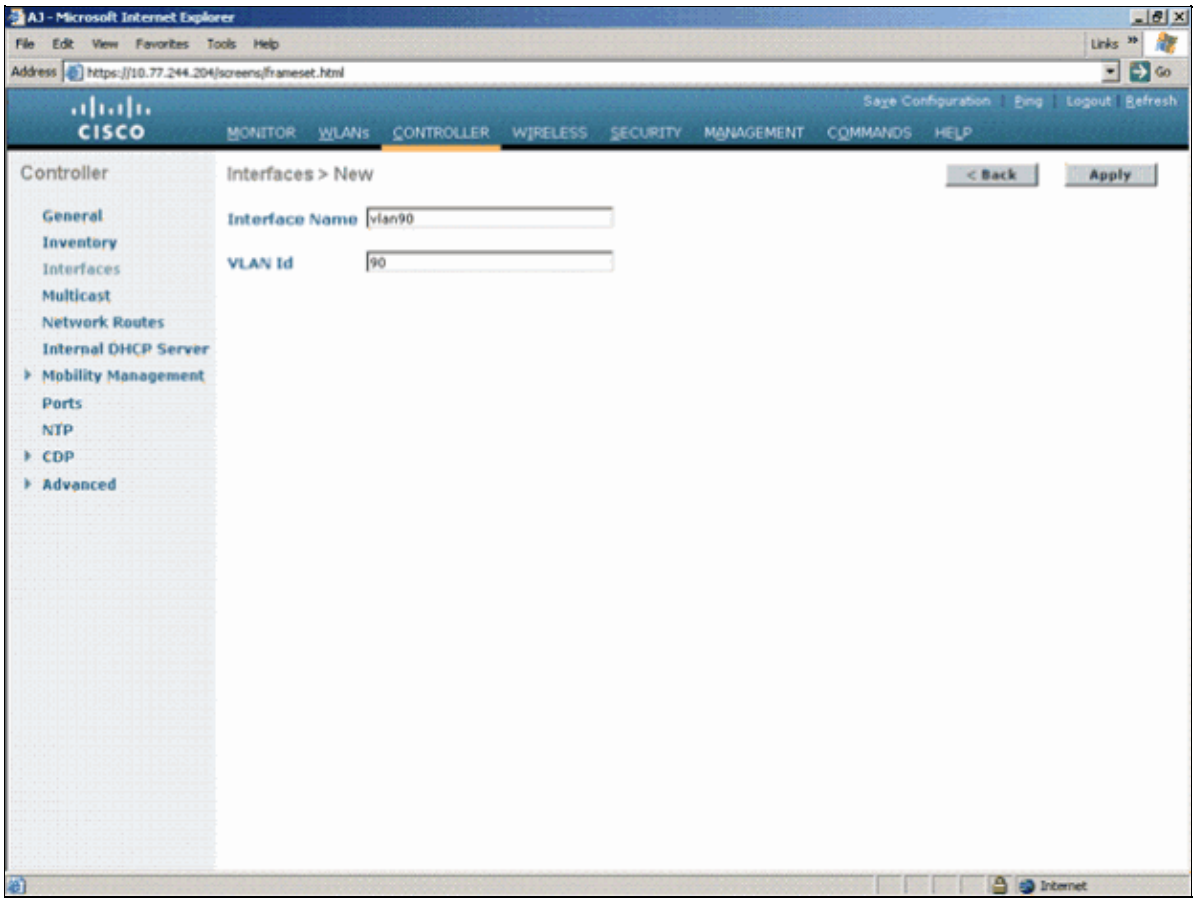
Create a VLAN Interface

Complete these steps:

1. In the main Controller window, choose **Controller** from the menu at the top, choose **Interfaces** from the menu on the left, and click **New** on the upper right side of the window.

   The window in Figure 1 appears. This example uses Interface Name *vlan90* with a VLAN ID of *90*:

   Figure 1



2. Click **Apply** in order to create the VLAN interface.

   A new window appears that asks you to fill in some information.
3. This document uses these parameters:

   - IP Address¡0.10.10.2
   - Netmask¢55.255.255.0 (24 bits)
   - Gateway¡0.10.10.1
   - Port Number¢
   - Primary DHCP Server¡0.77.244.204

     Note: This parameter should be the IP address of your RADIUS or DHCP server. In this example, the management address of the WLC is used as the DHCP server because the Internal DHCP scope is configured on the WLC.
   - Secondary DHCP Server .0.0.0

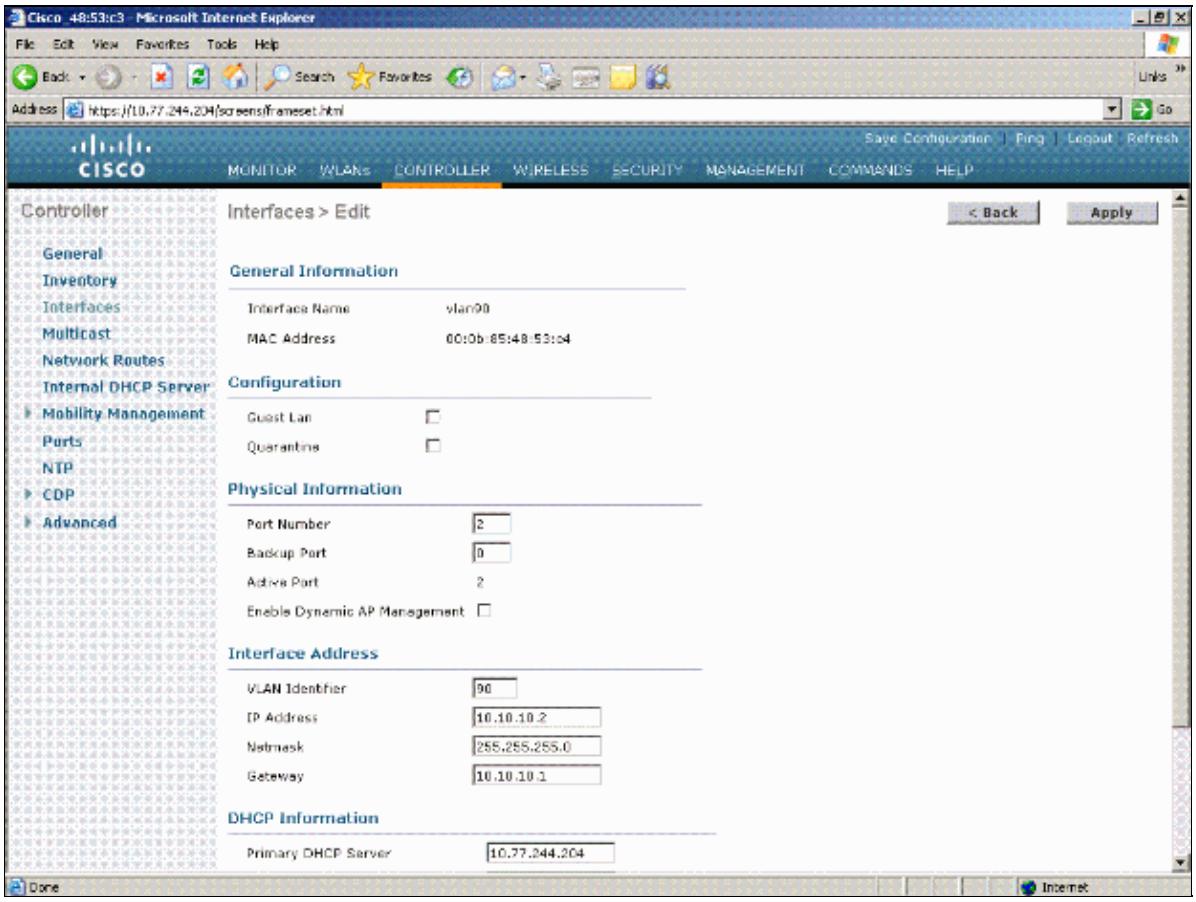
     Note: The example does not have a secondary DHCP server, so uses 0.0.0.0. If your

configuration has a secondary DHCP server, add the server IP address in this field.

- ACL Name None

Figure 2 shows a screenshot with these parameters configured:

Figure 2



4. Click **Apply** in order to save the changes.

Add a WLAN Instance

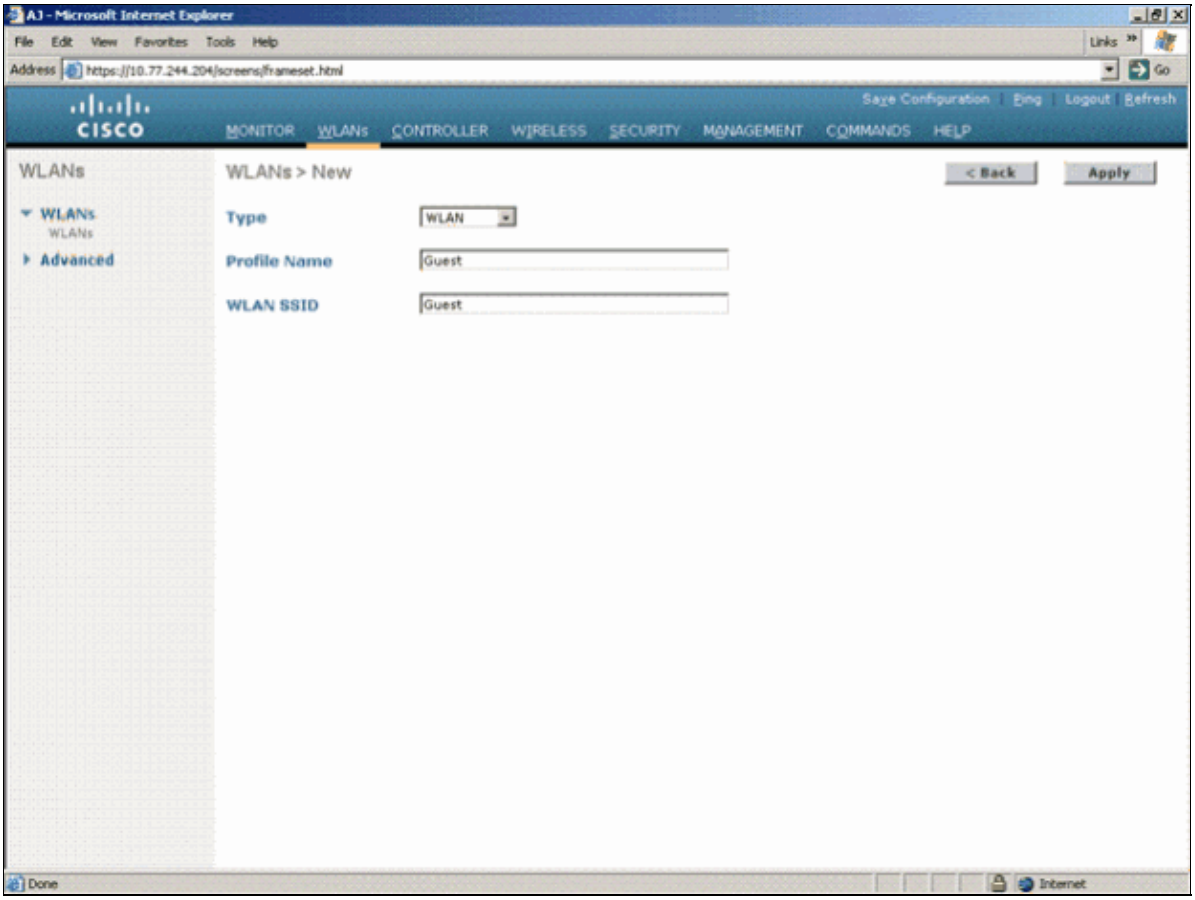
Now that there is a VLAN interface dedicated for web authentication, you must provide a new WLAN/SSID in order to support the web authentication users.

Complete these steps in order to create a new WLAN/SSID:

1. Open the WLC browser, click **WLAN** in the menu at the top, and click **New** on the upper right side. A screen as shown in the Figure 3 appears.

   Choose **WLAN** as the Type. Choose a profile name and WLAN SSID for Web authentication. This example uses **Guest** for both the Profile Name and WLAN SSID.

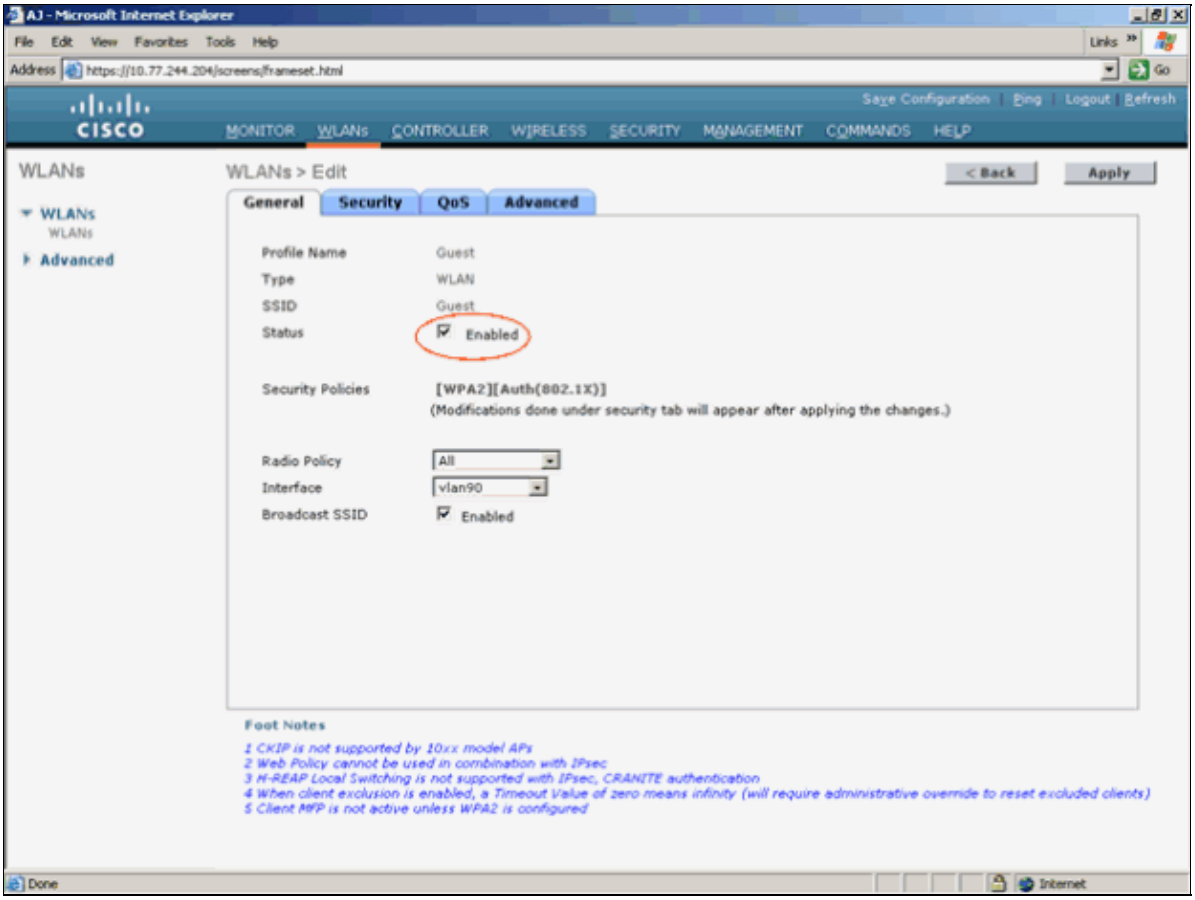
   Figure 3



2. Click **Apply**.

   A new WLANs > Edit window appears, as shown in Figure 4.

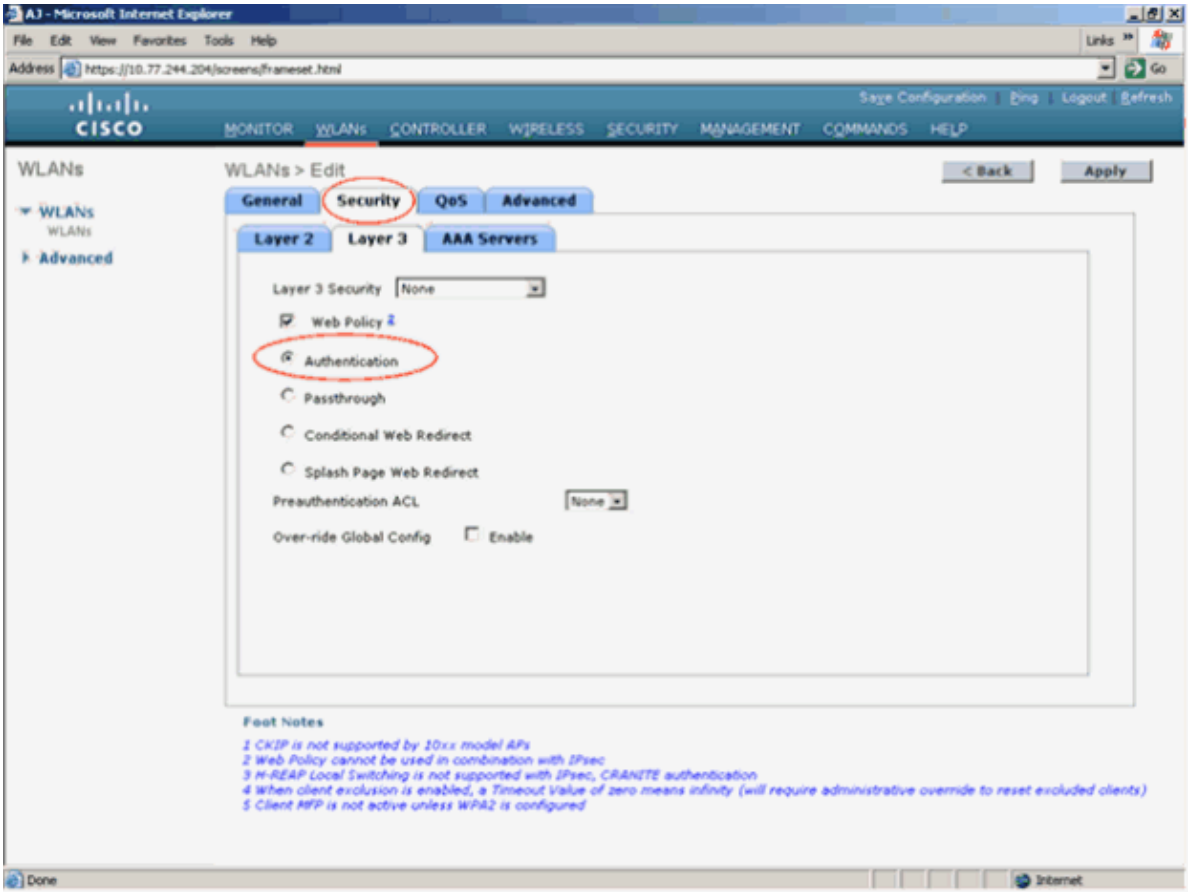
   Figure 4



3. Check the status box of the WLAN in order to enable the WLAN. From the Interface menu, select the name of the VLAN interface that you created previously. In this example, the Interface Name is *vlan90*.

   Note: Leave the default value for other parameters on this screen.
4. Click the Security tab. The window shown in Figure 5 appears.

   Figure 5



Complete these steps in order to configure web authentication:

a. Click the Layer 2 tab and set the security to ***None*** .

Note: You cannot configure web passthrough as Layer 3 security with 802.1x or WPA/WPA2 as Layer 2 Security for a WLAN. Refer to Wireless LAN Controller Layer 2 Layer 3 Security Compatibility Matrix for more information on the Wireless LAN Controller Layer 2 and Layer 3 security compatibility.

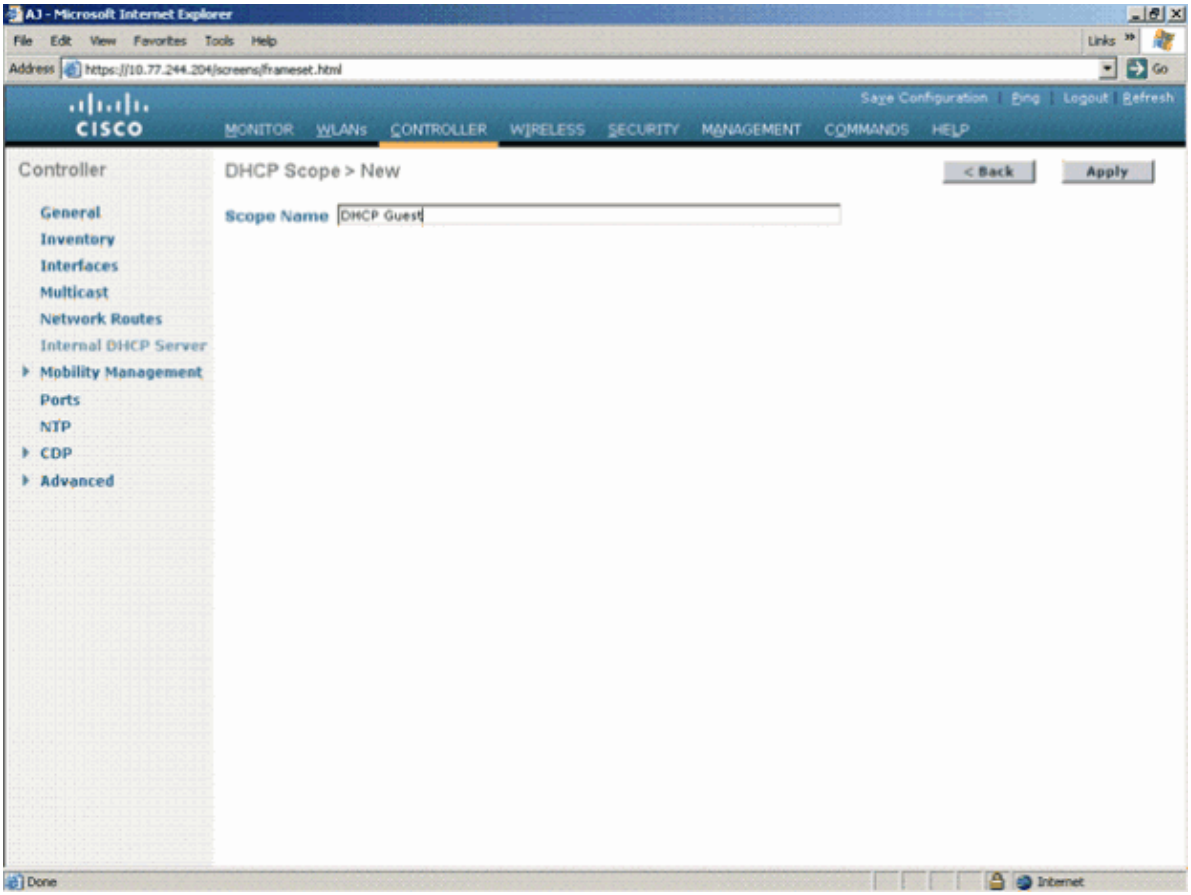
b. Click the Layer 3 tab. Check the Web Policy box and choose the ***Authentication*** option, as shown in **Figure 5** .
c. Click Apply in order to save the WLAN.
d. You are returned to the WLAN summary window. Make sure that the Web−Auth is enabled under the Security Policies column of the WLAN table for the SSID Guest.

Set Up DHCP and DNS Servers on the WLC

Complete these steps:

1. Click **Controller** in the menu at the top.
2. Click **Internal DHCP Server** in the menu on the left.
3. Click **New** in order to create a DHCP pool.
4. Enter the DHCP pool that you wish to use for your clients as shown in the Figure 6.

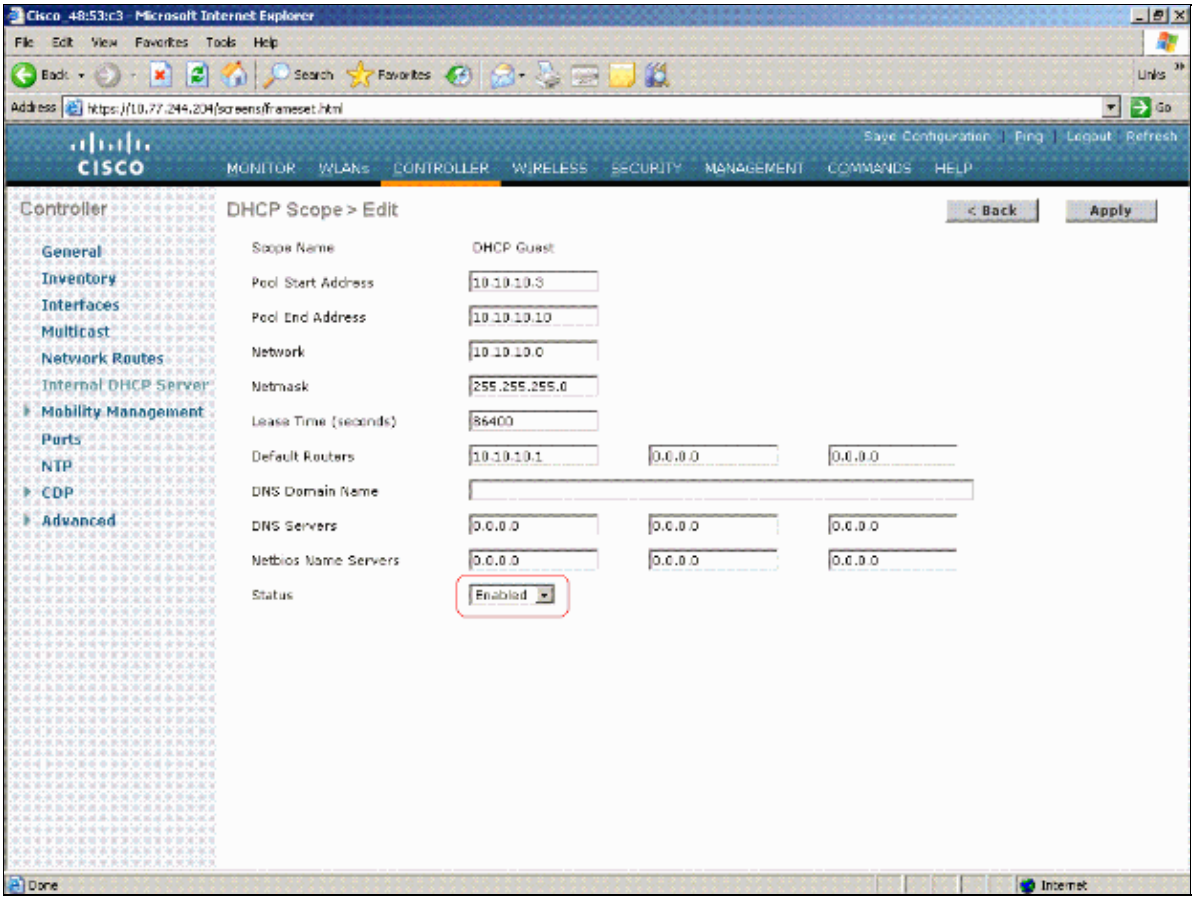
Figure 6



5. Click Apply.
6. The DHCP Scope > Edit window appears .
7. Enter the Pool start and end addresses. In this example, the DHCP pool is the set of addresses from 10.10.10.3 to 10.10.10.10.
8. Enter the IP address of the Default Router, which is 10.10.10.1.
9. Enter the DNS domain name and IP address of the DNS server. Make sure that the **Status** is enabled.

Figure 7 provides an example:

Figure 7



10. Click Apply.

Reboot the WLC

You must reboot the WLC because one or more of the WLAN changes cannot be made while the system is active. The changes must be made before or during the boot. Complete these steps in order to reboot the WLC:

1. In the main Controller window, choose **Commands** in the menu at the top.
2. In the new window, choose **Reboot** in the menu on the left.

   You are prompted to save and reboot if there are unsaved changes in your configuration.
3. Click **Save and Reboot** in order to save the configuration and reboot the switch.
4. Monitor your system reboot from the console connection.

   When the WLC is up, you can create your web authentication subscriber.

Two Ways to Authenticate Users in Web Authentication

There are two ways to authenticate users when you use web authentication. Local authentication allows you to authenticate the user in the Cisco WLC. You can also use an external RADIUS server in order to authenticate the users. In order to configure local authentication within the WLC, complete these steps:

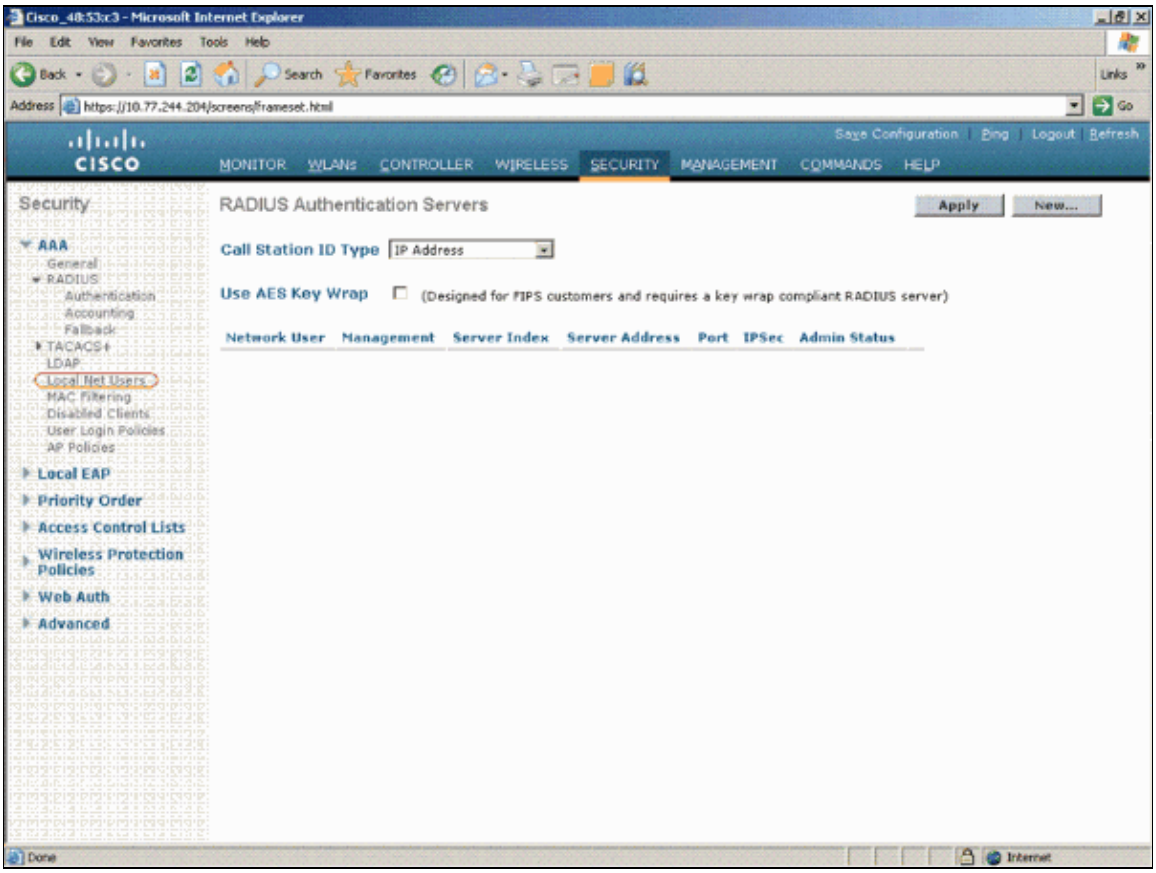
Local Authentication

User names and passwords are stored in the local database of the controller. Users are authenticated by WLC against this database. These steps show how to create a new username and password on the WLC.

1. Choose **Security** in the menu at the top in order to go to the Security window on your WLC.
2. Choose **Local Net Users** from the AAA menu on the left.

   Figure 8 provides an example:

   Figure 8



3. Click **New** on the upper right side in order to create a new user.

   A new window displays that asks for user name and password information.
4. Provide the User Name and Password, and confirm the password that you want to use.

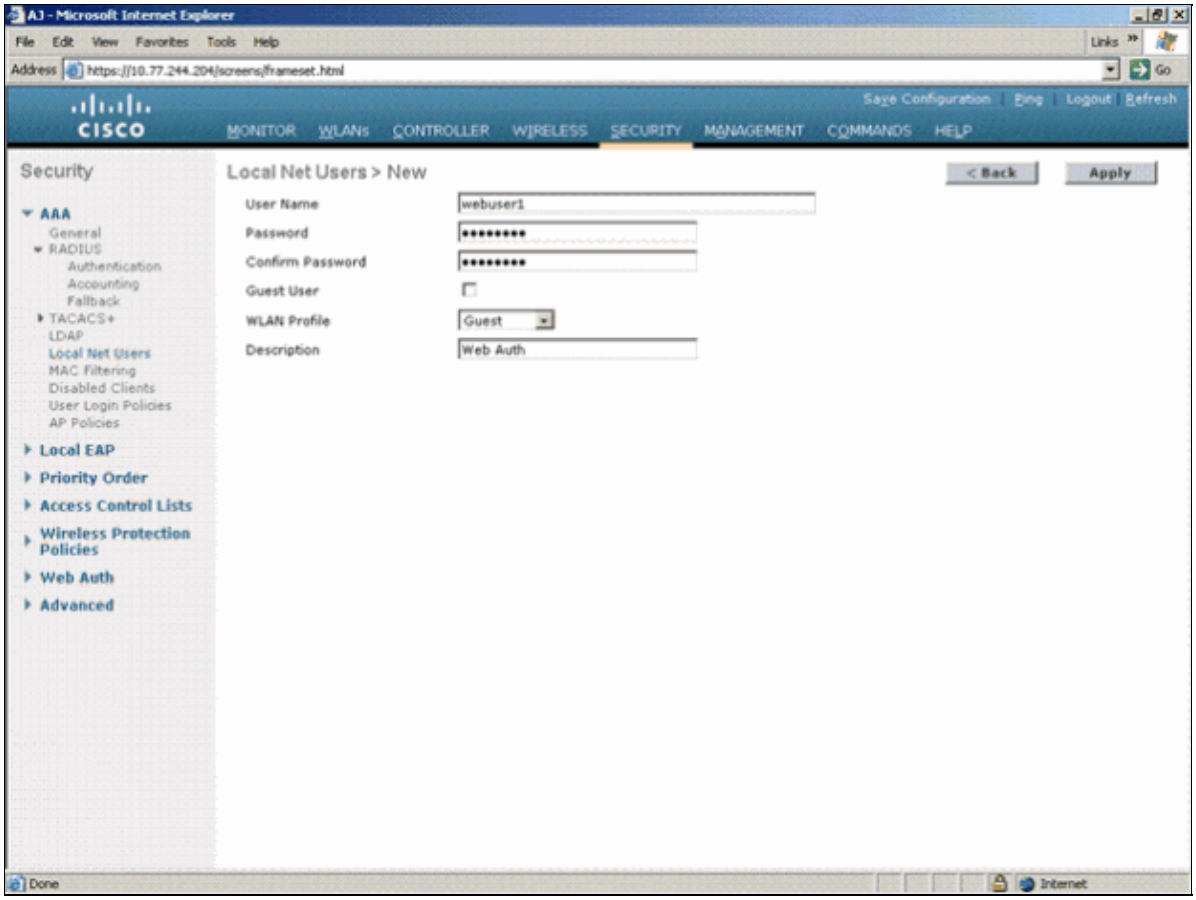
   This example creates the user *webuser1*.
5. Verify that you have assigned the correct WLAN Profile. This makes sure that users are authenticated only to specific WLANs.

   In this example, the WLAN Profile is *Guest*, which is used for web authentication.
6. Add a description, if you choose.

   This example uses *Web Auth*.
7. Click **Apply** in order to save the new user configuration.

   Figure 9 provides the example parameters:

   Figure 9



RADIUS Server for Web Authentication

This document uses a wireless ACS on Windows 2003 Server as the RADIUS server. You can use any available RADIUS server that you currently deploy in your network.

Note: ACS can be set up on either Windows NT or Windows 2000 Server. In order to download ACS from Cisco.com, refer to Software Center (Downloads) − Cisco Secure Software (registered customers only) . You need a Cisco web account in order to download the software.

When web authentication is done through a RADIUS server, the first query for authentication is attempted locally at the WLC. If there is no response at the WLC, the second query goes out to a RADIUS server. The Set Up ACS section shows you how to configure ACS for RADIUS. You must have a fully functional network with a Domain Name System (DNS) and a RADIUS server.

Set Up ACS

In this section, you are presented with the information to set up ACS for RADIUS.

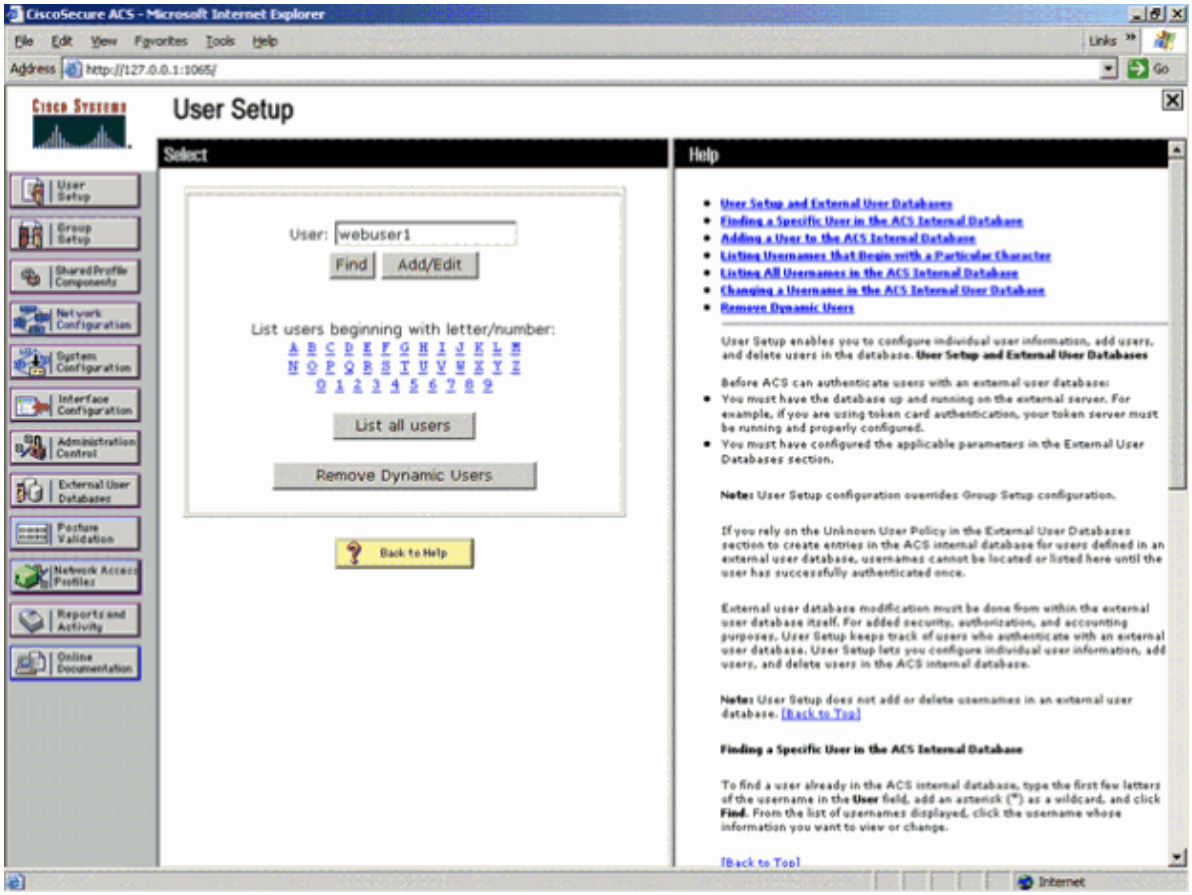
Set up ACS on your server and then complete the following steps in order to create a user for authentication:

1. When ACS asks if you want to open ACS in a browser window to configure, click **yes**.

   Note: After you set up ACS, you also have an icon on your desktop.
2. In the menu on the left, click **User Setup**.

   This action takes you to User Setup screen as shown in the Figure 10.

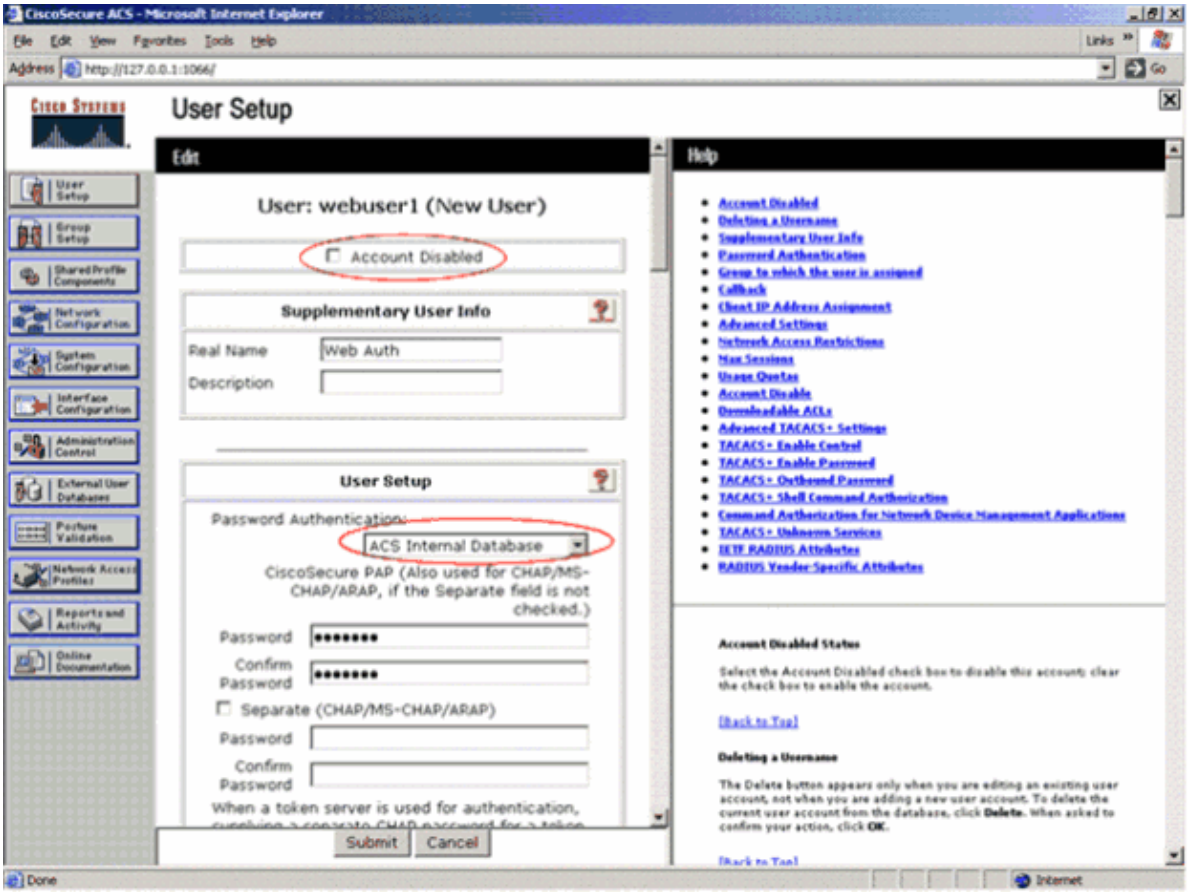
   Figure 10



3. Enter the user that you want to use for web authentication, and click **Add/Edit**.

   After the user is created, a second window opens as shown in the Figure 11.

   Figure 11



4. Ensure that the **Account Disabled** Box at the Top is not checked as shown in the Figure 11.
5. Choose the ACS Internal Database for Password Authentication option.
6. Provide the password twice.
7. Click Submit.

Enter Your RADIUS Server Information into the Cisco WLC

Complete these steps:

1. Click **Security** in the menu at the top.
2. Click **Radius Authentication** in the menu on the left.
3. Click **New**, and enter the IP address of your ACS/RADIUS server. In this example, the IP address of the ACS server is **10.77.244.196**
4. Enter the shared secret for the Radius server. Make sure that this secret key is the same as the one you entered in the Radius server for WLC.
5. Leave the Port number at the default, 1812.
6. Ensure that the **Server Status** option is Enabled.
7. Check the **Network User Enable** Box so that this Radius Server is used for authenticating users of your wireless network.
8. Click **Apply**.

Figure 12 provides an example:

Figure 12

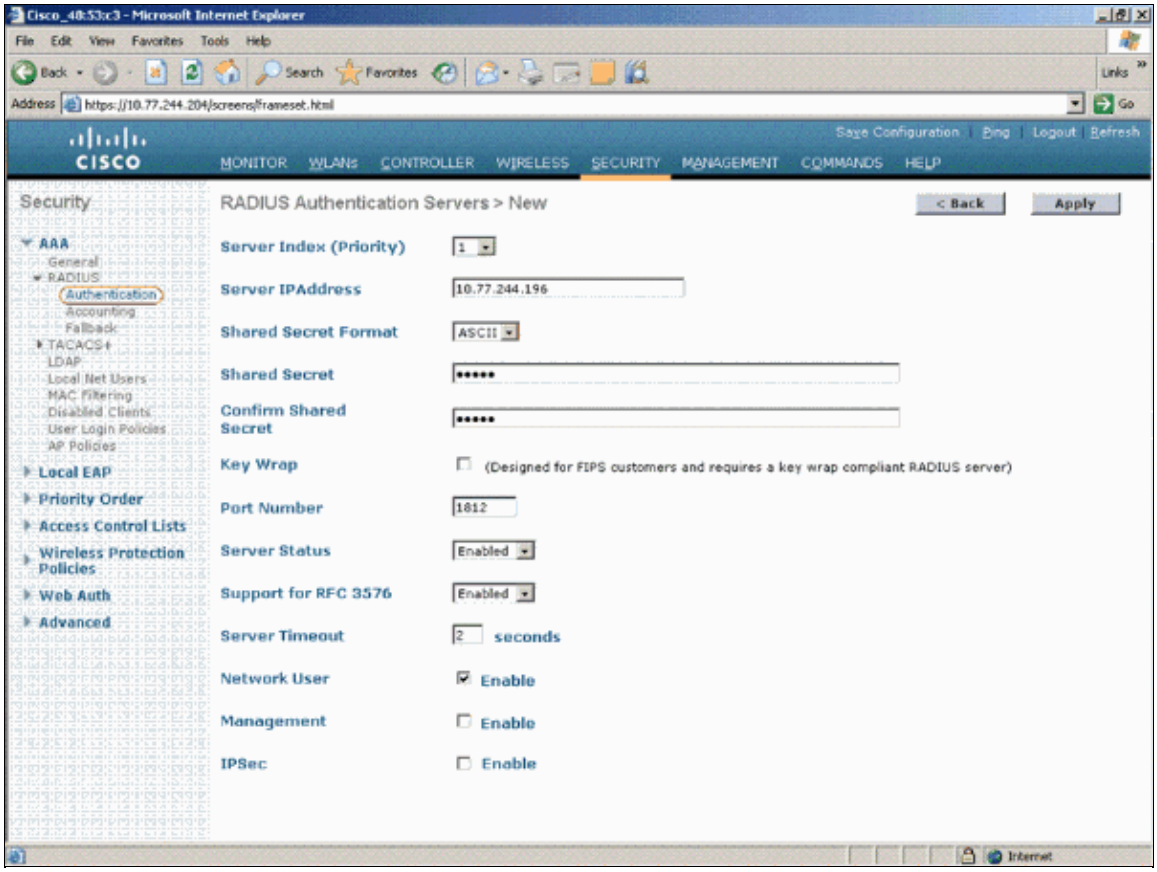
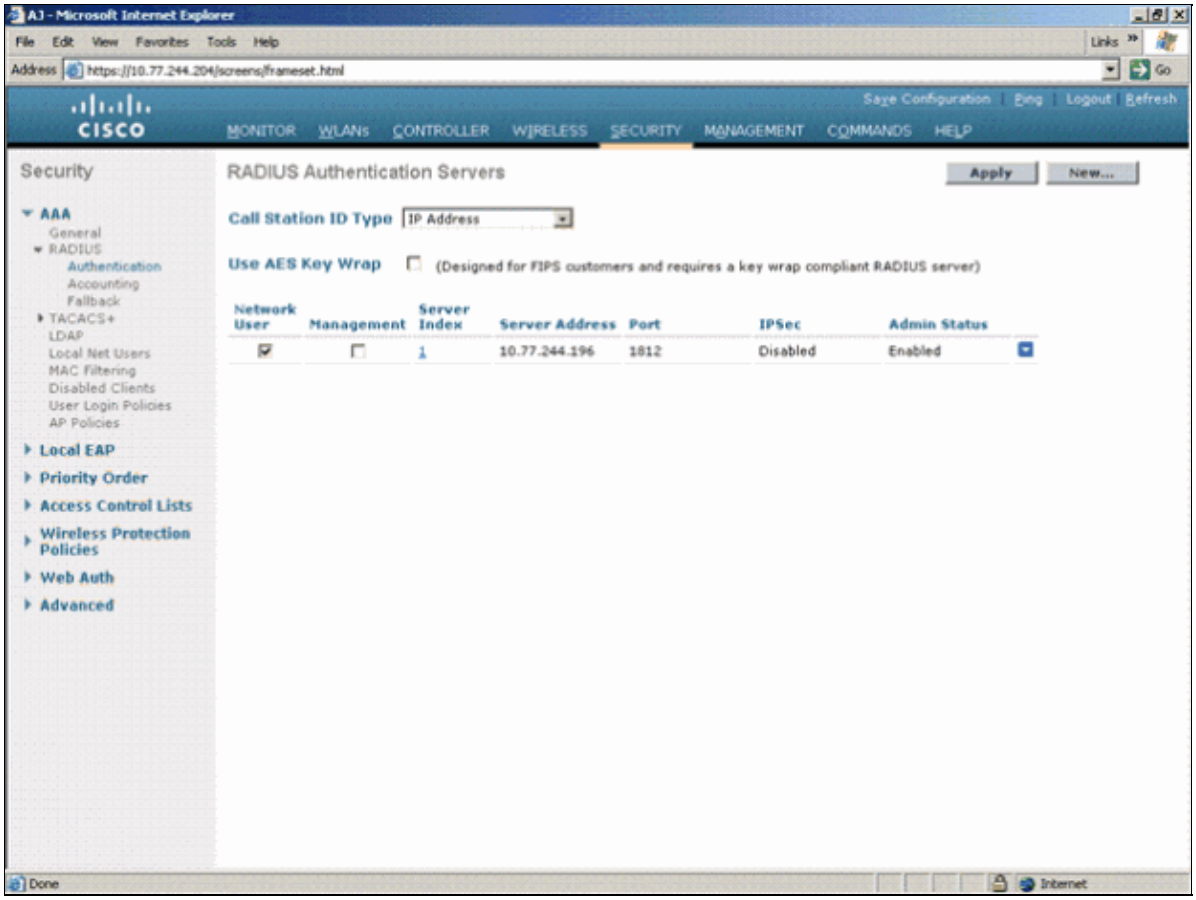


Figure 13 shows a configured RADIUS server. Make sure that the *Network User* Box is checked and *Admin Status* is Enabled.

Figure 13

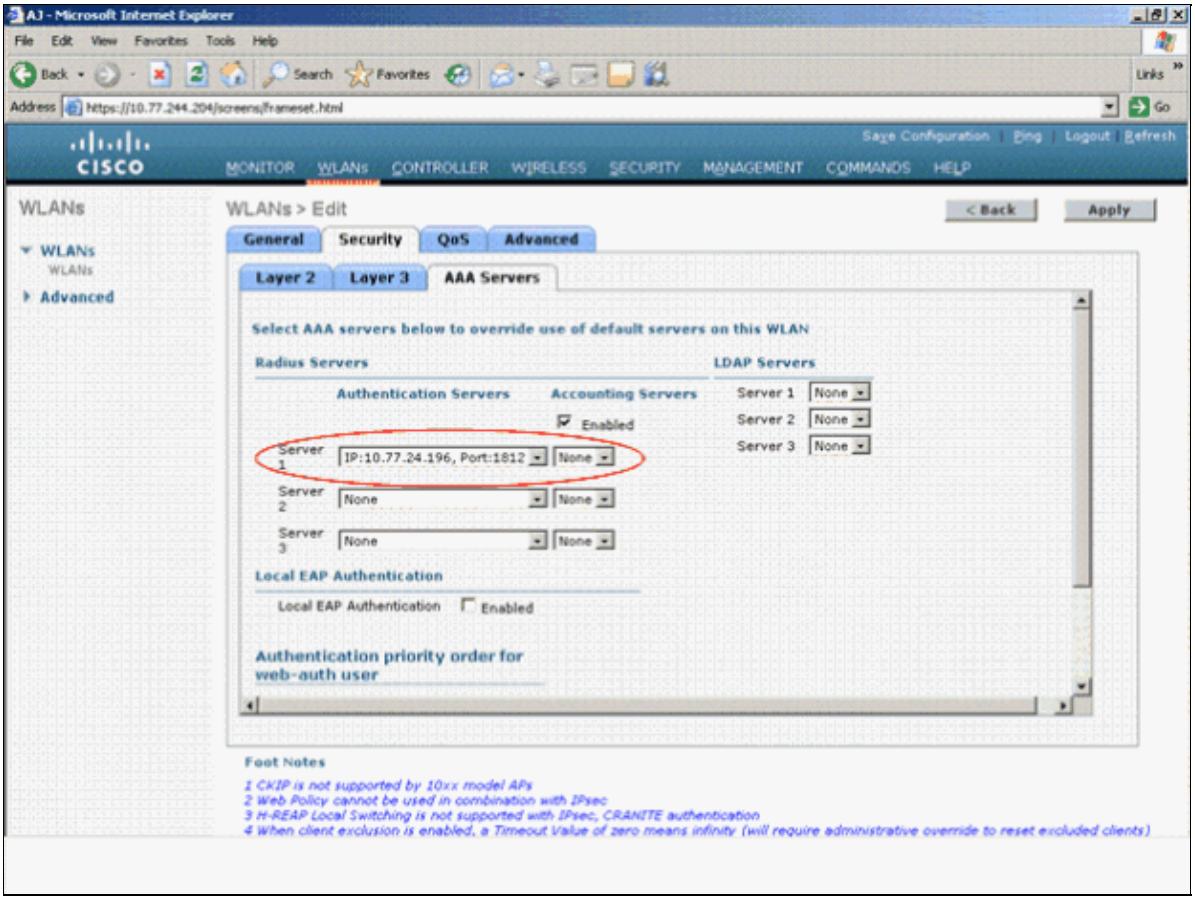


Configuring WLAN with RADIUS Server

Now that the RADIUS server is configured on the WLC, you need to configure the WLAN to use this RADIUS server for web authentication. Complete these steps in order to configure WLAN with the RADIUS server.

1. Open your WLC browser and click **WLANs**. It displays the list of WLANs configured on the WLC. Click on the WLAN **Guest** which was created for Web Authentication.
2. On the **WLANs>Edit** Page click on the **Security** Menu. Click on **AAA Servers** Tab under Security. Then choose the Radius Server which is 10.77.244.196 in our Example as shown in the Figure 14.

   Figure 14



3. Click Apply.

Configure Your Windows Machine to Use Web Authentication

Once the WLC is configured, the client must be configured appropriately for Web authentication. In this section, you are presented with the information to configure your Windows system for web authentication.

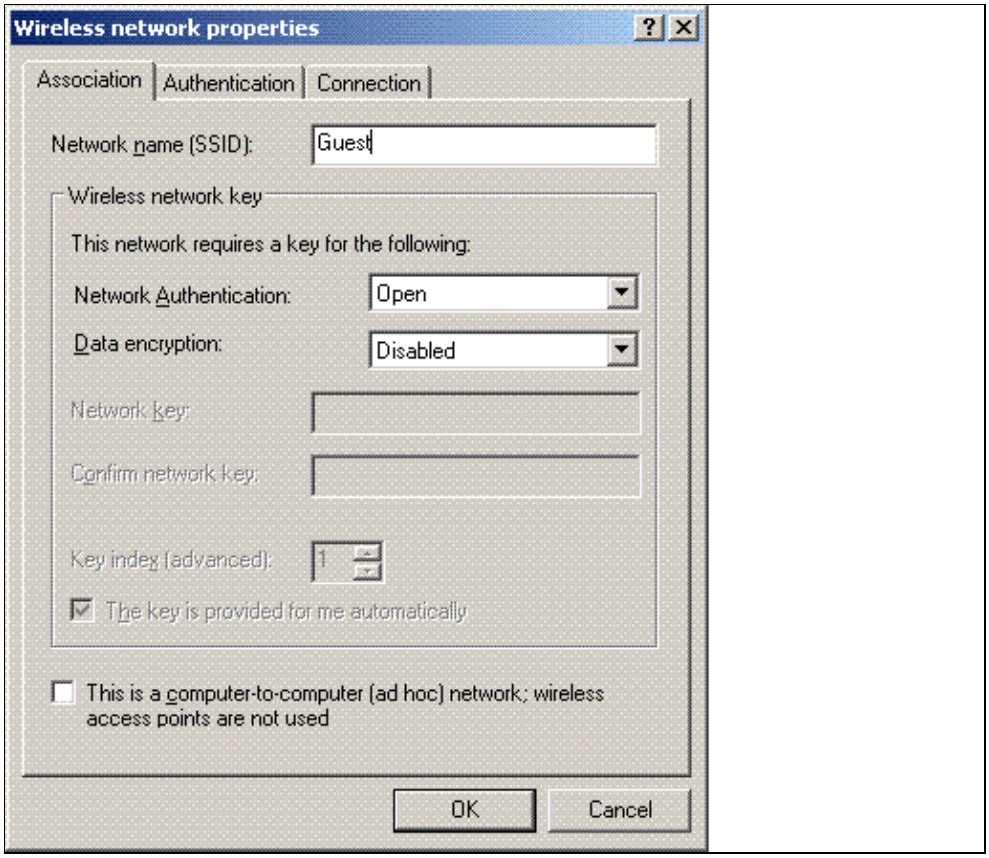
Client Configuration

The Microsoft wireless client configuration remains mostly unchanged for this subscriber. You only need to add the appropriate WLAN/SSID configuration information. Complete these steps:

1. From the Windows **Start** menu, choose **Settings > Control Panel > Network and Internet Connections**.
2. Click the **Network Connections** icon.
3. Right−click the **LAN Connection** icon and choose **Disable**.
4. Right−click the **Wireless Connection** icon and choose **Enable**.
5. Right−click the **Wireless Connection** icon again and choose **Properties**.
6. From the Wireless Network Connection Properties window, click the **Wireless Networks** tab.
7. Under the preferred networks, area click **Add** in order to configure the Web authentication SSID.
8. Under the Association tab, enter the Network Name (WLAN/SSID) value that you want to use for web authentication.

   Figure 15 provides an example:

   Figure 15



Note: The Data Encryption is Wired Equivalent Privacy (WEP) by default. Disable Data Encryption in order for web authentication to work.

9. Click **OK** at the bottom of the window in order to save the configuration.

   When you communicate with the WLAN, you see a beacon icon in the Preferred Network box.

Figure 16 shows a successful wireless connection to web auth. The WLC has provided your wireless Windows client with an IP address.

Figure 16

Note: If your wireless client is also a VPN end point and you have Web Authentication configured as a security feature for WLAN, then the VPN tunnel is not established until you go through the Web Authentication process explained here. In order to establish a VPN tunnel, the client must first go through the process of Web Authentication with success. Only then does VPN tunneling become successful.

Note: After a successful login, if the wireless clients are idle and do not communicate with any of the other devices, the client is disassociated after the session timeout period is configured on the WLAN. When that occurs, the client is stuck in a **Webauth_Reqd** state that cannot be restored unless you close and re−open the browser to establish a new connection. This is the expected behavior, if the session timeout period expires.

Client Login

Complete these steps:

1. Open a browser window and select the virtual IP address that you set for the local authentication.

   Use the secure https://1.1.1.1/login.html.

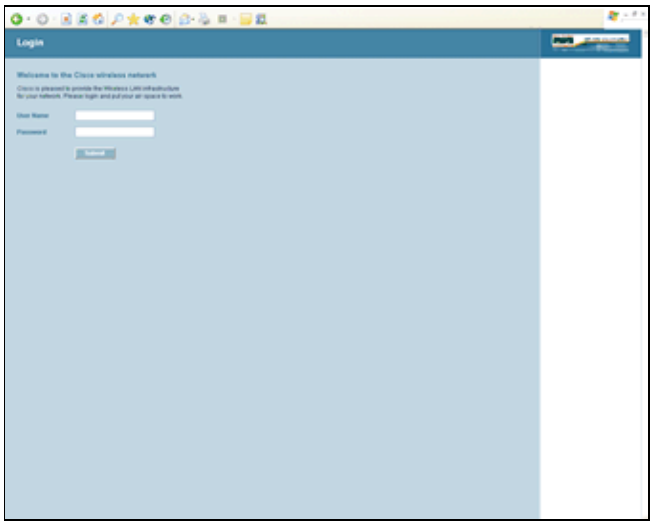
   This step is important in code that is earlier than 3.0, but the step is not necessary in later code. In later code, any URL brings you to the web authentication page. Also, in all recent controller versions, web authentication via http login is also supported. This is tied to the management login on the controller . In order to verify this, disable https login and enable only http for management. Now if you try the web authentication, it goes to the http login.

   A security alert window displays.
2. Click **Yes** in order to proceed.
3. When the Login window appears, enter the user name and password of the Local Net User that you created.

   If your login is successful, you see two browser windows. Larger Window indicates successful login and you can this window to browse the internet. Use the smaller window in order to log out when your use of the guest network is complete.

   Figure 17 shows a successful redirect for web authentication.

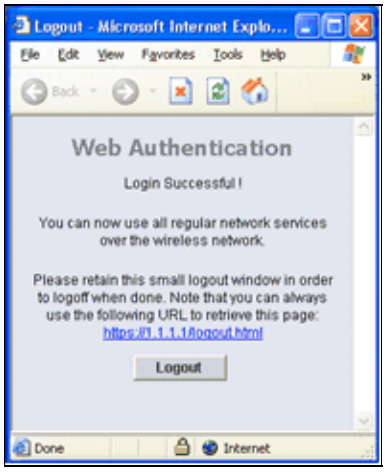
   Figure 17



   Note: This is the default Web authentication page provided by Cisco. This page can also be customized. To know how to customize refer to the Customize the Web Passthrough or Web Authentication Login Page section of this document.

   Figure 18 shows the Login Successful window, which displays when authentication has occurred within the ACS.

Figure 18



Use Certificates for Web−Authentication

You can also perform Web−Authentication with certificates. Refer to Generate CSR for Third−Party Certificates and Download Unchained Certificates to the WLC for more information on how to create and download certificates to the WLC.

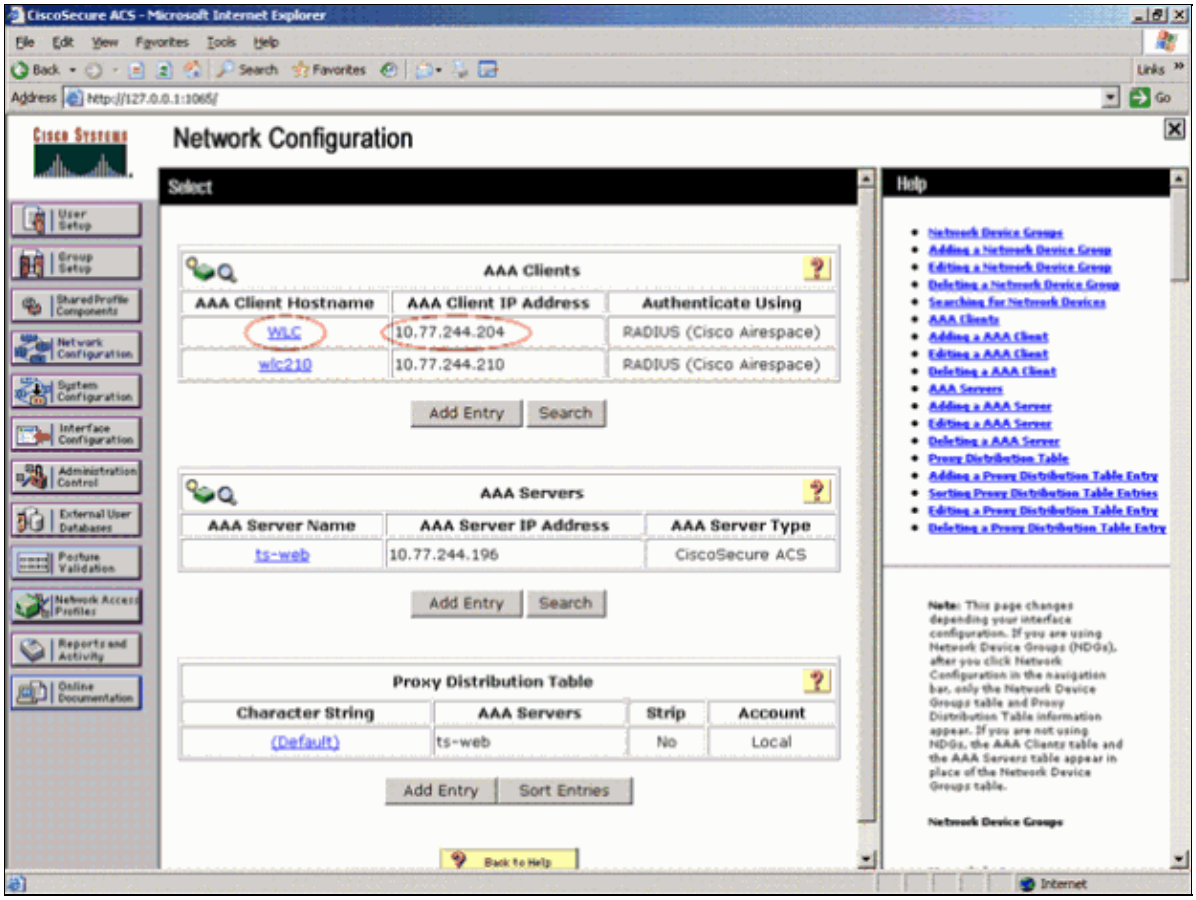
On the client side, you need to ensure that the Root Certificate of the CA that issued the certificate to the WLC is uploaded. Refer to the CLIENT Configuration for EAP−TLS using Windows Zero Touch section of EAP−TLS under Unified Wireless Network with ACS 4.0 and Windows 2003 for more information on how to configure the client to accept certificates.

Verify

Verify ACS

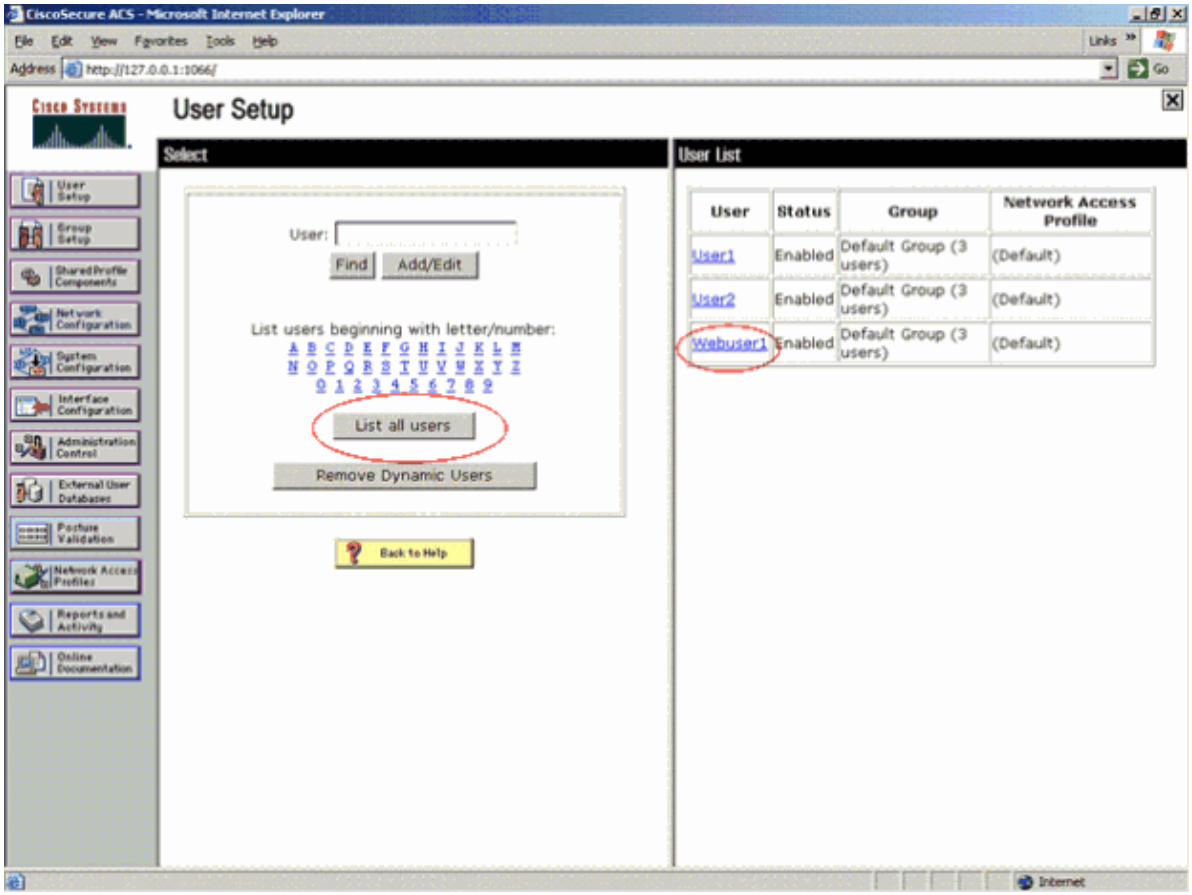
When you set up ACS, remember to download all the current patches and latest code. This should solve impending issues. In case you are using Radius Authentication be sure that your WLC is listed as one of the AAA Client as shown in the Figure 19. Click on the **Network Configuration** menu on the left hand side to check this. Click on the AAA client and verify the password and the authentication type configured. Refer to the Configuring AAA Clients section of User Guide for Cisco Secure Access Control Server 4.2 for more information on how to configure an AAA client.

Figure 19



And, when you choose User Setup, verify again that your users actually exist. Click on **List All Users**. A window as shown in Figure 20 appears. Make sure the user that has been created exists in the list.

Figure 20



Verify Internal Web Authentication

Use this section to confirm that your internal web authentication configuration works properly.

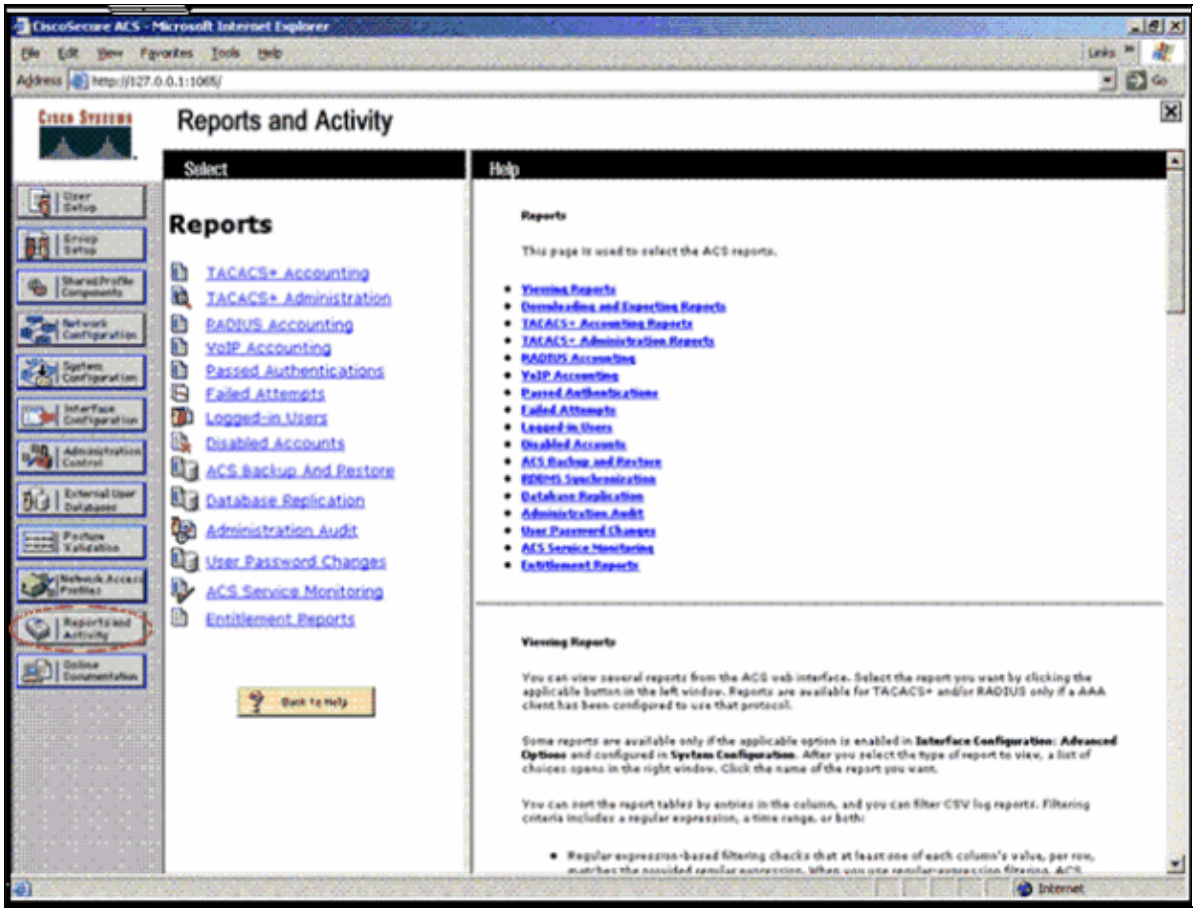
The setup for web authentication is relatively straightforward. Remember to check simple attributes in your Windows client in your wireless network connection. Under the Wireless Networks tab, look for the **Use Windows to Configure My Wireless Network** setting. Be sure that this option is checked if you use the Windows Zero configuration. If you use a different client, be sure to refer to the documentation that came with that client in order to set up web authentication. Ensure the virtual interface is configured properly on the **Controller > Interfaces** page. Also, verify that you have specified this WLAN/SSID on the WLC, that you have enabled the WLAN/SSID, and that it is correctly set up for web authentication.

Troubleshoot Web authentication

Troubleshoot ACS

If you have issues with password authentication, click **Reports and Activity** on the lower left side of the ACS in order to open all available reports. After you open the reports window, you have the option to open RADIUS Accounting, Failed Attempts for login, Passed Authentications, Logged−in Users, and other reports. These reports are .csv files, and you can open the files locally on your machine. See Figure 21. The reports help uncover issues with authentication, such as incorrect user name and/or password. ACS also comes with online documentation. If you are not connected to a live network and have not defined the service port, ACS uses the IP address of your Ethernet port for your service port. If your network is not connected, you most likely end up with the Windows 169.254.x.x default IP address.

Figure 21



Note: If you type in any external URL, the WLC automatically connects you to the internal web authentication page. If the automatic connection does not work, you can enter the management IP address of the WLC in the URL bar in order to troubleshoot. Look at the top of the browser for the message that says to redirect for web authentication.

Refer to Troubleshooting Web Authentication Redirection on the WLC for more information on Troubleshooting Web Authentication.

Guidelines for Customized Web Authentication

Use these guidelines when you create a customized login window for web authentication.

- Name the login page **login.html**. The controller prepares the web authentication URL based on this name. If the controller does not find this file after the webauth bundle is untarred, the bundle is discarded, and an error message appears.
- Include input fields for both a username and password.
- Retain the redirect URL as a hidden input item after extracting from the original URL.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- Make sure that all paths used in the main page (to refer to images, for example) are relative.
- Before you upload the customized page to the WLC , compress the customized page and the image files into .tar format. When this .tar file is downloaded from a local TFTP server, WLC extracts these files in an untarred format into its filesystem. If you load a webauth bundle with a .tar compression application that is not GNU compliant, the controller cannot extract the files in the bundle and these error messages appear: `Extracting error` and `TFTP transfer failed`. Therefore, Cisco recommends that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file.

Customize the Web Passthrough or Web Authentication Login Page

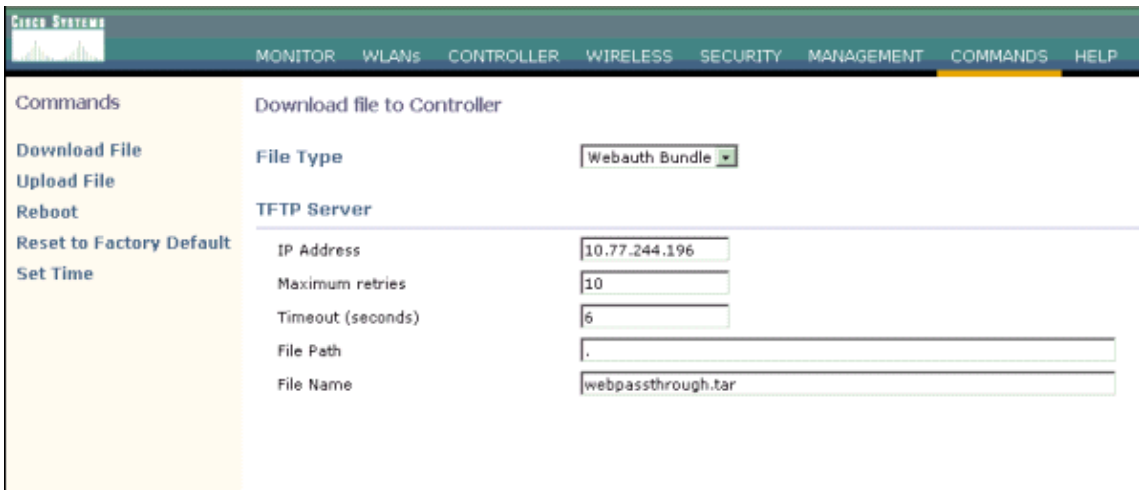
Customize the Web Passthrough or Web Authentication Login Page from the WLC

Complete these steps from the WLC GUI in order to customize the Web Passthrough or the Web Authentication Login page:

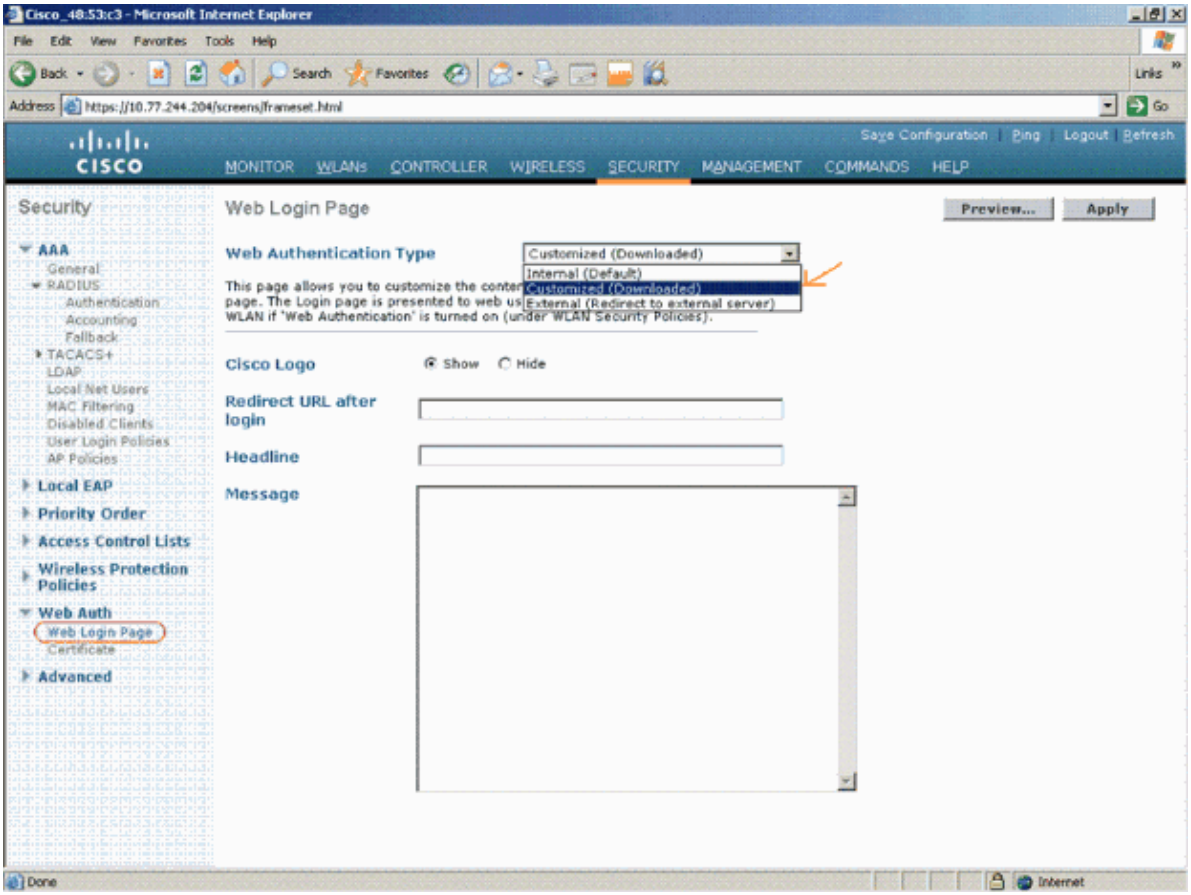
1. From the WLC GUI, choose **Commands > Download File**.

   The Download File to Controller page appears.
2. From the File Type pull−down menu select **Webauth Bundle**.
3. Enter the IP address of the TFTP server, file path (root directory of the TFTP server) and file name of the customized login script (name of the .tar file to be downloaded). Click **Download**.

   The new customized login page is downloaded to the controller. Here is an example.



4. Choose **Security > Web Login Page** in order to access the Web Login page.
5. From the Web Authentication Type drop−down box, choose **Customized (Downloaded)**.
6. Click **Apply** in order to commit your changes. This picture shows how to do this.



7. Save the controller configuration.

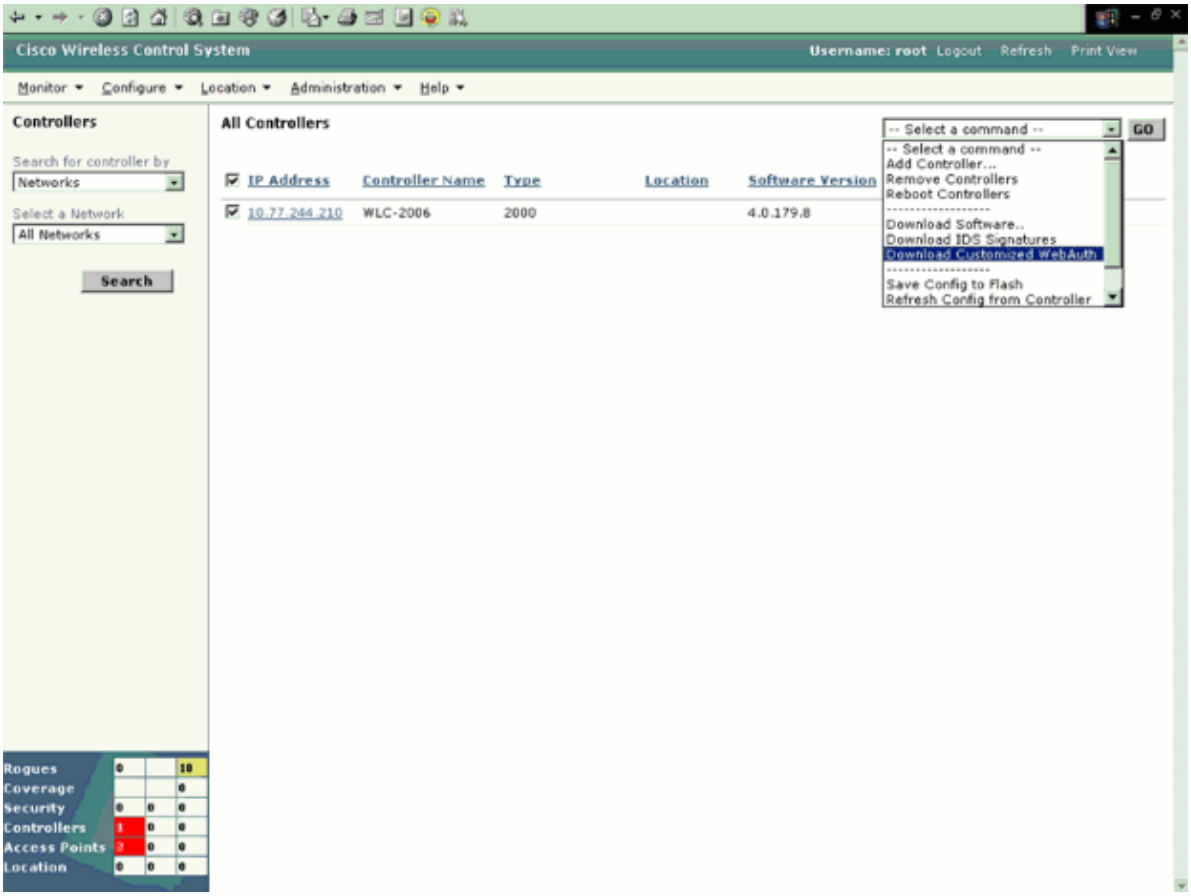
   Note: In WLC versions earlier than 4.1 you can have only one web authentication page per WLC. In WLC version 4.2 and later, you can have customized web authentication pages for each WLAN in the WLC. Refer to the Using the GUI to Assign Login, Login Failure, and Logout Pages per WLAN section of Cisco Wireless LAN Controller Configuration Guide, Release 5.0 for more information.

Customize the Web Passthrough or Web Authentication Login Page using the WCS

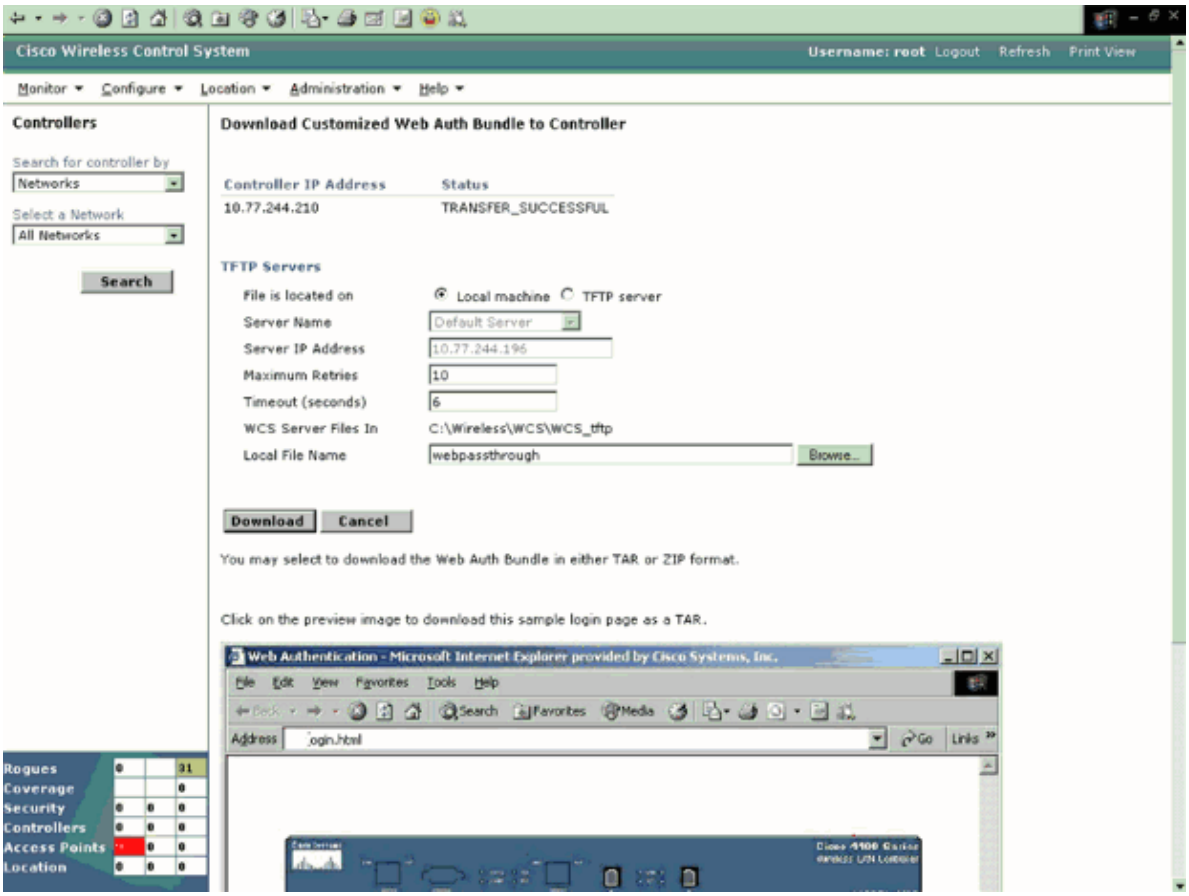
Complete these steps from the WCS GUI in order to customize the Web Passthrough or the Web Authentication Login page using the WCS.

1. From the Wireless Control System GUI, choose **Configure > Controllers**.

   The All Controllers page appears.
2. Select the controllers for which the Web Authentication or Web Passthrough Login page needs to be customized.
3. From the Select the Command pull−down menu, select **Download Customized WebAuth** and click on **Go**.



4. In the Download Customized Web Auth Bundle to Controller page, enter the file name (name of the customized login .tar file) and click **Download**.
5. The customized Web Auth/Web Passthrough page is pushed to the controller.



6. Complete steps 4 through 7 from the Customize Web Passthrough and Web Authentication Login Page using the WLC section of this document (on the WLC GUI) in order to use this customized page for web login.

Assigning Login, Login Failure, and Logout Pages per WLAN

You can display different web authentication login, login failure, and logout pages to users per WLAN. This feature enables user−specific web authentication pages to be displayed for a variety of network users, such as guest users or employees within different departments of an organization.

Different login pages are available for all web authentication types (internal, external, and customized). However, different login failure and logout pages can be specified only when you choose customized as the web authentication type.

Use the GUI to Assign Login, Login Failure, and Logout Pages per WLAN

You can use the controller GUI in order to assign web login, login failure, and logout pages to a WLAN. Complete these steps:

1. Click WLANs to open the WLANs page.
2. Click the profile name of the WLAN to which you want to assign a web login, login failure, or logout page.
3. Choose **Security > Layer 3**.
4. Make sure that **Web Policy** and **Authentication** are selected.
5. In order to override the global authentication configuration web authentication pages, check the **Override Global Config** check box.
6. When the Web Auth Type drop−down box appears, choose one of these options in order to define the web authentication pages for wireless guest users:

    - **Internal** Displays the default web login page for the controller. This is the default value.
    - **Customized** Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop−down boxes appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop−down box if you do not want to display a customized page for that option.

      Note: These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. Refer to Downloading a Customized Web Authentication Login Page for information on downloading custom pages.
    - **External** Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL field.

      You can select specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.
7. If you chose External as the web authentication type in Step 6, click AAA Servers and choose up to three RADIUS and LDAP servers from the drop−down boxes.

   Note: The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.
8. In order to establish the priority in which the servers are contacted to perform web authentication, complete these steps. The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.
b. Click the **Up** and **Down** buttons until the desired server type is at the top of the box.
c. Click the **<** arrow in order to move the server type to the priority box on the left.
d. Repeat these steps in order to assign priority to the other servers.

9. Click **Apply** in order to commit your changes.
10. Click **Save Configuration** in order to save your changes.

Conditional Web Redirect with 802.1x Authentication

A new feature in controller software release 4.0.206.0 enables a user to be conditionally redirected to a particular web page after 802.1x authentication has completed successfully. Such conditions might include when the user's password reaches expiration, when the user needs to pay their bill for continued usage, and so on. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. If the RADIUS server returns the Cisco AV−pair "url−redirect," then the user is redirected to the specified URL when they open a browser. If the server also returns the Cisco AV−pair "url−redirect−acl," the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point but is only allowed to pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, change a password or pay a bill), it must reauthenticate. When the RADIUS server does not return a "url−redirect," the client is considered fully authorized and allowed to pass traffic. The conditional web redirect feature is available only for WLANs that are configured for 802.1x or WPA1+WPA2 Layer 2 Security. You can configure this feature through the controller GUI or CLI.

For more information on this feature and how to configure this feature read the release note for 4.0.206.0 available at Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.0.206.0.

Related Information

- **External Web Authentication with Wireless LAN Controllers Configuration Example**
- **Troubleshooting Web Authentication Redirection on the WLC**
- **Cisco Wireless LAN**
- **Wired Guest Access using Cisco WLAN Controllers Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 5.0 − Managing User Accounts**
- **Authentication of Wireless LAN Controller's Lobby Administrator via RADIUS Server**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 13, 2008 Document ID: 69340