



Managing User Accounts

This chapter explains how to create and manage guest user accounts, describes the web authentication process, and provides instructions for customizing the web authentication login page. It contains these sections:

- [Creating Guest User Accounts, page 10-2](#)
- [Obtaining a Web Authentication Certificate, page 10-7](#)
- [Web Authentication Process, page 10-10](#)
- [Choosing the Web Authentication Login Page, page 10-13](#)
- [Configuring Wired Guest Access, page 10-28](#)

Creating Guest User Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator account, also known as a lobby ambassador account. Once this account has been created, a lobby ambassador can create and manage guest user accounts on the controller. The lobby ambassador has limited configuration privileges and access only to the web pages used to manage the guest accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

The local user database is limited to a maximum of 2048 entries, which is also the default value (on the Security > AAA > General page). This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

Creating a Lobby Ambassador Account

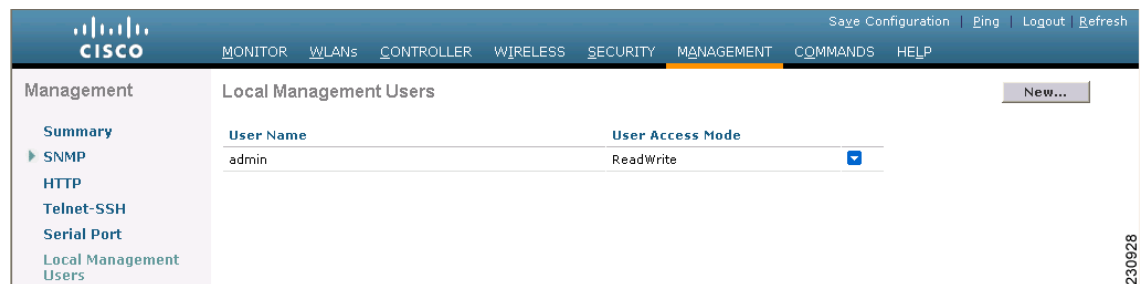
You can create a lobby ambassador account on the controller through either the GUI or the CLI.

Using the GUI to Create a Lobby Ambassador Account

Follow these steps to create a lobby ambassador account using the controller GUI.

- Step 1** Choose **Management > Local Management Users** to open the Local Management Users page (see [Figure 10-1](#)).

Figure 10-1 Local Management Users Page



This page lists the names and access privileges of the local management users.



Note

If you want to delete any of the user accounts from the controller, hover your cursor over the blue drop-down arrow and choose **Remove**. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

- Step 2** To create a lobby ambassador account, click **New**. The Local Management Users > New page appears (see [Figure 10-2](#)).

Figure 10-2 Local Management Users > New Page

- Step 3** In the User Name field, enter a username for the lobby ambassador account.



Note Management usernames must be unique because they are stored in a single database.

- Step 4** In the Password and Confirm Password fields, enter a password for the lobby ambassador account.



Note Passwords are case sensitive.

- Step 5** Choose **LobbyAdmin** from the User Access Mode drop-down box. This option enables the lobby ambassador to create guest user accounts.



Note The **ReadOnly** option creates an account with read-only privileges, and the **ReadWrite** option creates an administrative account with both read and write privileges.

- Step 6** Click **Apply** to commit your changes. The new lobby ambassador account appears in the list of local management users.

- Step 7** Click **Save Configuration** to save your changes.

Using the CLI to Create a Lobby Ambassador Account

Enter this command to create a lobby ambassador account using the controller CLI:

```
config mgmtuser add lobbyadmin_username lobbyadmin_pwd lobby-admin
```



Note Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

Creating Guest User Accounts as a Lobby Ambassador

A lobby ambassador would follow these steps to create guest user accounts.

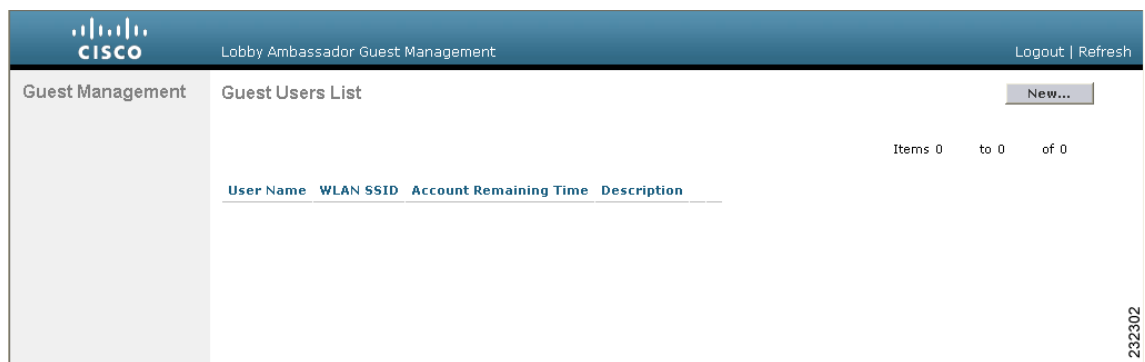


Note

A lobby ambassador cannot access the controller CLI interface and therefore can create guest user accounts only from the controller GUI.

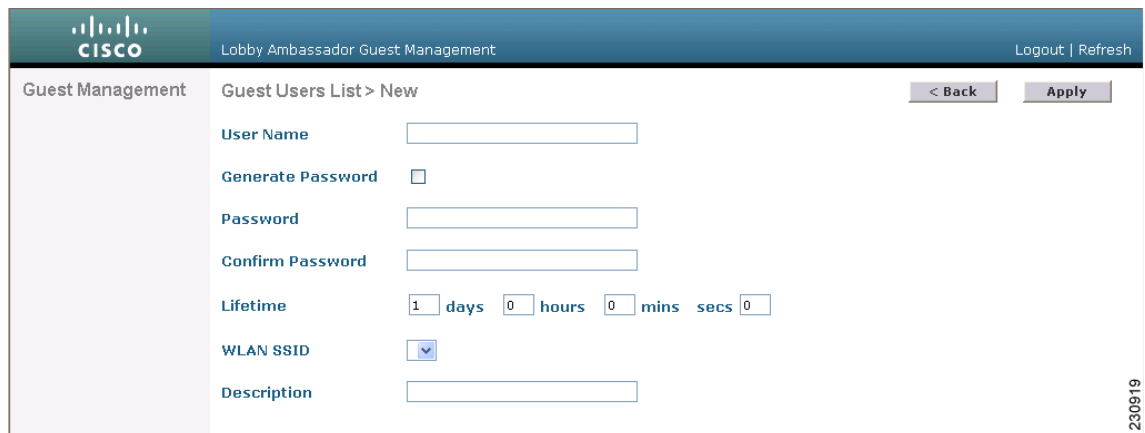
- Step 1** Log into the controller as the lobby ambassador, using the username and password specified in the “[Creating a Lobby Ambassador Account](#)” section above. The Lobby Ambassador Guest Management > Guest Users List page appears (see [Figure 10-3](#)).

Figure 10-3 Lobby Ambassador Guest Management > Guest Users List Page



- Step 2** Click **New** to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears (see [Figure 10-4](#)).

Figure 10-4 Lobby Ambassador Guest Management > Guest Users List > New Page



- Step 3** In the User Name field, enter a name for the guest user. You can enter up to 24 characters.

Step 4 Perform one of the following:

- If you want to generate an automatic password for this guest user, check the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password fields.
- If you want to create a password for this guest user, leave the **Generate Password** check box unchecked and enter a password in both the Password and Confirm Password fields.



Note Passwords can contain up to 24 characters and are case sensitive.

Step 5 From the Lifetime drop-down boxes, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four fields creates a permanent account.

Default: 1 day

Range: 5 minutes to 30 days



Note The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires reauthentication.



Note You can change a guest user account with a non-zero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent using the controller GUI, you must delete the account and create it again. If desired, you can use the **config netuser lifetime user_name 0** CLI command to make a guest user account permanent without deleting and recreating it.

Step 6 From the WLAN SSID drop-down box, choose the SSID that will be used by the guest user. The only WLANs that are listed are those for which Layer 3 web authentication has been configured.



Note Cisco recommends that the system administrator create a specific guest WLAN to prevent any potential conflicts. If a guest account expires and it has a name conflict with an account on the RADIUS server and both are on the same WLAN, the users associated with both accounts are disassociated before the guest account is deleted.

Step 7 In the Description field, enter a description of the guest user account. You can enter up to 32 characters.

Step 8 Click **Apply** to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page (see [Figure 10-5](#)).

Figure 10-5 Lobby Ambassador Guest Management > Guest Users List Page

User Name	WLAN SSID	Account Remaining Time	Description
guest1	test	23 h 59 m 59 s	Guest1 user account

From this page, you can see all of the guest user accounts, their WLAN SSID, and their lifetime. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Step 9 Repeat this procedure to create any additional guest user accounts.

Viewing Guest User Accounts

After a lobby ambassador has created guest user accounts, the system administrator can view them from the controller GUI or CLI.

Using the GUI to View Guest Accounts

To view guest user accounts using the controller GUI, choose **Security > AAA > Local Net Users**. The Local Net Users page appears (see Figure 10-6).

Figure 10-6 Local Net Users Page

User Name	WLAN Profile	Guest User	Role	Description
abc	guestLAN	No	N/A	guest
devesh1	guestLAN	No	N/A	wired
quest1	test	Yes		Guest1 user account

From this page, the system administrator can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Using the CLI to View Guest Accounts

To view all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

```
show netuser summary
```

Obtaining a Web Authentication Certificate

The controller's operating system automatically generates a fully functional web authentication certificate, so you do not need to do anything in order to use certificates with Layer 3 web authentication. However, if desired, you can prompt the operating system to generate a new web authentication certificate, or you can download an externally generated SSL certificate.

Support for Chained Certificate

In controller versions earlier than 5.1.151.0, web authentication certificates can be only device certificates and should not contain the CA roots chained to the device certificate (no chained certificates).

With controller version 5.1.151.0 and later, the controller allows for the device certificate to be downloaded as a chained certificate (up to a level of 2) for web authentication. For more information about chained certificates, see the *Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC* document at

<http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html>.

Using the GUI to Obtain a Web Authentication Certificate

Using the controller GUI, follow these steps to view the current web authentication certificate, generate a new certificate, or download an externally generated certificate.

-
- Step 1** Choose **Security > Web Auth > Certificate** to open the Web Authentication Certificate page (see [Figure 10-7](#)).

Figure 10-7 Web Authentication Certificate Page

The screenshot shows the Cisco configuration interface for the Web Authentication Certificate. The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth (with sub-items Web Login Page and Certificate), and Advanced. The main content area is titled 'Web Authentication Certificate' and includes 'Apply' and 'Regenerate Certificate' buttons. Under 'Current Certificate', the following details are listed:

- Name: bsnSslWebauthCert
- Type: 3rd Party
- Serial Number: 469652449
- Valid: From 2008 Nov 18th, 00:00:01 GMT Until 2018 Nov 18th, 00:00:01 GMT
- Subject Name: C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=1.1.1.1
- Issuer Name: C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=1.1.1.1
- MD5 Fingerprint: 45:f1:58:6c:53:19:28:49:3e:47:92:b8:0f:e4:fc:be
- SHA1 Fingerprint: 02:7b:01:0f:92:87:26:14:8d:0b:c1:64:83:6d:a6:a4:80:0b:90:8a

Below the details is a checked checkbox for 'Download SSL Certificate *'. A note states: '* Controller must be rebooted for the new certificate to take effect.' Underneath is a section titled 'Download SSL Certificate From Server' with the following input fields:

- Server IP Address: 209.165.200.225
- Maximum retries: 10
- Timeout (seconds): 6
- Certificate File Path: /
- Certificate File Name: (empty)
- Certificate Password: (empty)

This page shows the details of the current web authentication certificate.

- Step 2** If you want to use a new operating system-generated web authentication certificate, follow these steps:
- Click **Regenerate Certificate**. The operating system generates a new web authentication certificate, and a successfully generated web authentication certificate message appears.
 - Reboot the controller to register the new certificate.
- Step 3** If you prefer to use an externally generated web authentication certificate, follow these steps:
- Verify that the controller can ping the TFTP server.
 - Check the **Download SSL Certificate** check box.
 - In the Server IP Address field, enter the IP address of the TFTP server.
 - The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that each download can be attempted in the Maximum Retries field and the amount of time (in seconds) allowed for each download in the Timeout field.
 - In the Certificate File Path field, enter the directory path of the certificate.
 - In the Certificate File Name field, enter the name of the certificate (*certname.pem*).

- g. In the Certificate Password field, enter the password for the certificate.
- h. Click **Apply** to commit your changes. The operating system downloads the new certificate from the TFTP server.
- i. Reboot the controller to register the new certificate.

Using the CLI to Obtain a Web Authentication Certificate

Using the controller CLI, follow these steps to view the current web authentication certificate, generate a new certificate, or download an externally generated certificate.

Step 1 To see the current web authentication certificate, enter this command:

show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

Step 2 If you want the operating system to generate a new web authentication certificate, follow these steps:

- a. To generate the new certificate, enter this command:
config certificate generate webauth
- b. To reboot the controller to register the new certificate, enter this command:
reset system

Step 3 If you prefer to use an externally generated web authentication certificate, follow these steps:



Note Cisco recommends that the Common Name (CN) of the externally generated web authentication certificate be a virtual interface IP address in order for the client's browser to match the domains of the web authentication URL and the web authentication certificate.

- a. To specify the name, path, and type of certificate to be downloaded, enter these commands:
transfer download mode tftp
transfer download datatype webauthcert
transfer download serverip *server_ip_address*
transfer download path *server_path_to_file*
transfer download filename *certname.pem*
transfer download certpassword *password*
transfer download tftpMaxRetries *retries*
transfer download tftpPktTimeout *timeout*

**Note**

The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that each download can be attempted for the *retries* parameter and the amount of time (in seconds) allowed for each download for the *timeout* parameter.

- b. To start the download process, enter this command:

transfer download start

- c. To reboot the controller to register the new certificate, enter this command:

reset system

Web Authentication Process

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. Then when the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

**Note**

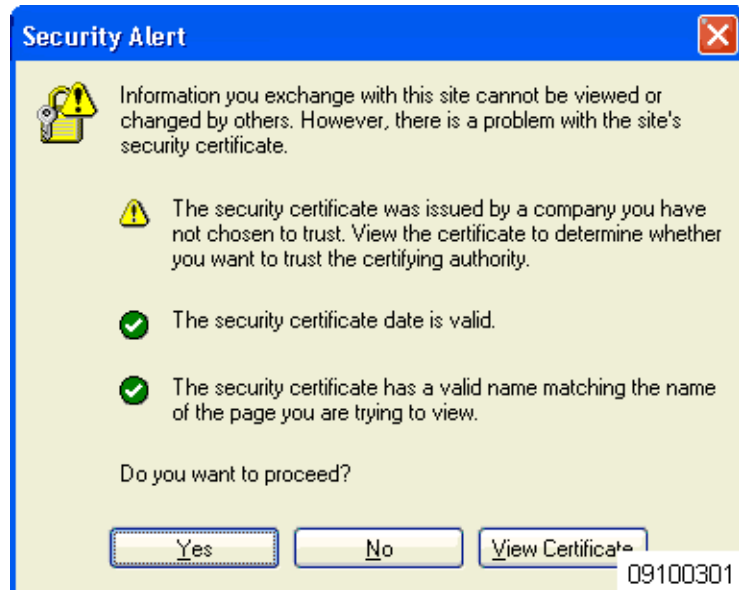
On pure web authentication without any L2 protection, it is possible to do MAC address spoofing and hijack connections. This is a security issue coming from the use of 802.11 open technologies, and not from web authentication itself.

This can be prevented by using 802.11i encryption or VPN IPsec/SSL technologies.

If you are using pure web authentication, you should take measures to ensure that guest access clients cannot access sensitive resources.

When web authentication is enabled (under Layer 3 Security), users might receive a web-browser security alert the first time that they attempt to access a URL. [Figure 10-8](#) shows a typical security alert.

Figure 10-8 Typical Web-Browser Security Alert



After the user clicks **Yes** to proceed (or if the client's browser does not display a security alert), the web authentication system redirects the client to a login page (see [Figure 10-9](#)).

To prevent the security alert from appearing, the user can perform these steps:

-
- Step 1** Click **View Certificate** on the Security Alert page.
 - Step 2** Click **Install Certificate**.
 - Step 3** When the Certificate Import Wizard appears, click **Next**.
 - Step 4** Choose **Place all certificates in the following store** and click **Browse**.
 - Step 5** At the bottom of the Select Certificate Store page, check the **Show Physical Stores** check box.
 - Step 6** Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.
 - Step 7** Click **OK**.
 - Step 8** Click **Next > Finish**.
 - Step 9** When the "The import was successful" message appears, click **OK**.
 - Step 10** Because the issuer field is blank on the controller self-signed certificate, open Internet Explorer, choose **Tools > Internet Options > Advanced**, uncheck the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.
 - Step 11** Reboot the PC. On the next web authentication attempt, the login page appears (see [Figure 10-9](#)).

Figure 10-9 Default Web Authentication Login Page

155945

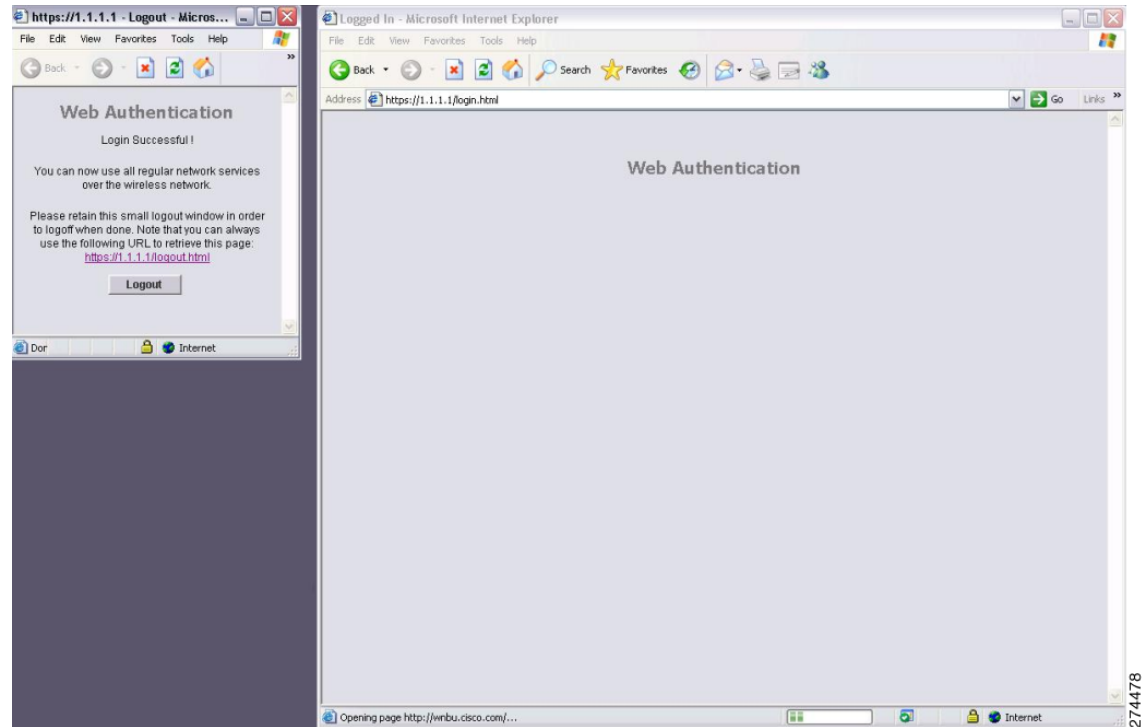
The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- The default login page
- A modified version of the default login page
- A customized login page that you configure on an external web server
- A customized login page that you download to the controller

The [“Choosing the Web Authentication Login Page”](#) section on page 10-13 provides instructions for choosing how the web authentication login page appears.

When the user enters a valid username and password on the web authentication login page and clicks **Submit**, the web authentication system displays a successful login page and redirects the authenticated client to the requested URL. [Figure 10-10](#) shows a typical successful login page.

Figure 10-10 Successful Login Page



The default successful login page contains a pointer to a virtual gateway address URL: `https://1.1.1.1/logout.html`. The IP address that you set for the controller virtual interface serves as the redirect address for the login page (see the for more information on the virtual interface).

Choosing the Web Authentication Login Page

This section provides instructions for specifying the content and appearance of the web authentication login page. Follow the instructions in one of these sections to choose the web authentication login page using the controller GUI or CLI:

- [Choosing the Default Web Authentication Login Page, page 10-14](#)
- [Creating a Customized Web Authentication Login Page, page 10-18](#)
- [Using a Customized Web Authentication Login Page from an External Web Server, page 10-20](#)
- [Downloading a Customized Web Authentication Login Page, page 10-22](#)
- [Assigning Login, Login Failure, and Logout Pages per WLAN, page 10-26](#)



Note

If you do not want users to connect to a web page using a browser that is configured with SSLv2 only, you can disable SSLv2 for web authentication by entering this command: **`config network secureweb cipher-option sslv2 disable`**. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is enabled.

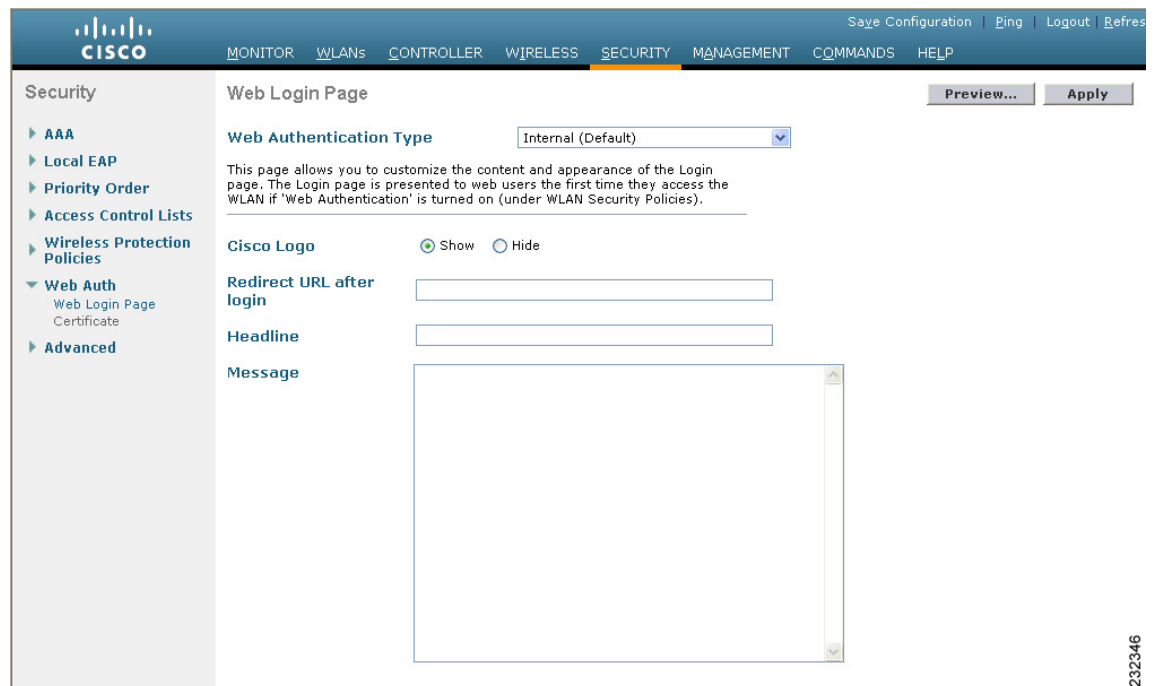
Choosing the Default Web Authentication Login Page

If you want to use the default web authentication login page as is (see [Figure 10-9](#)) or with a few modifications, follow the instructions in the GUI or CLI procedure below.

Using the GUI to Choose the Default Web Authentication Login Page

- Step 1** Choose **Security > Web Auth > Web Login Page** to open the Web Login page (see [Figure 10-11](#)).

Figure 10-11 Web Login Page



- Step 2** From the Web Authentication Type drop-down box, choose **Internal (Default)**.
- Step 3** If you want to use the default web authentication login page as is, go to [Step 8](#). If you want to modify the default login page, go to [Step 4](#).
- Step 4** If you want to hide the Cisco logo that appears in the top right corner of the default page, choose the Cisco Logo **Hide** option. Otherwise, click the **Show** option.
- Step 5** If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter the desired URL (such as `www.AcompanyBC.com`) in the Redirect URL After Login field. You can enter up to 254 characters.




Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

- Step 6** If you want to create your own headline on the login page, enter the desired text in the Headline field. You can enter up to 127 characters. The default headline is “Welcome to the Cisco wireless network.”

- Step 7** If you want to create your own message on the login page, enter the desired text in the Message field. You can enter up to 2047 characters. The default message is “Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.”
- Step 8** Click **Apply** to commit your changes.
- Step 9** Click **Preview** to view the web authentication login page.
- Step 10** If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes. Otherwise, repeat any of the previous steps as necessary to achieve your desired results.
-

Using the CLI to Choose the Default Web Authentication Login Page

- Step 1** To specify the default web authentication type, enter this command:
- ```
config custom-web webauth_type internal
```
- Step 2** If you want to use the default web authentication login page as is, go to [Step 7](#). If you want to modify the default login page, go to [Step 3](#).
- Step 3** To show or hide the Cisco logo that appears in the top right corner of the default login page, enter this command:
- ```
config custom-web weblogo {enable | disable}
```
- Step 4** If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter this command:
- ```
config custom-web redirecturl url
```
- You can enter up to 130 characters for the URL. To change the redirect back to the default setting, enter **clear redirecturl**.
-  **Note** The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.
- 
- Step 5** If you want to create your own headline on the login page, enter this command:
- ```
config custom-web webtitle title
```
- You can enter up to 130 characters. The default headline is “Welcome to the Cisco wireless network.” To reset the headline to the default setting, enter **clear webtitle**.
- Step 6** If you want to create your own message on the login page, enter this command:
- ```
config custom-web webmessage message
```
- You can enter up to 130 characters. The default message is “Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.” To reset the message to the default setting, enter **clear webmessage**.
- Step 7** Enter **save config** to save your settings.

- Step 8** If you want to import your own logo into the web authentication login page, follow these steps:
- a. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Keep these guidelines in mind when setting up a TFTP server:
    - If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
    - If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
    - A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.
  - b. Enter **ping ip-address** to ensure that the controller can contact the TFTP server.
  - c. Copy the logo file (in .jpg, .gif, or .png format) to the default directory on your TFTP server. The maximum file size is 30 kilobits. For an optimal fit, the logo should be approximately 180 pixels wide and 360 pixels high.
  - d. To specify the download mode, enter **transfer download mode tftp**.
  - e. To specify the type of file to be downloaded, enter **transfer download datatype image**.
  - f. To specify the IP address of the TFTP server, enter **transfer download serverip tftp-server-ip-address**.




---

**Note** Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

---

- g. To specify the download path, enter **transfer download path absolute-tftp-server-path-to-file**.
- h. To specify the file to be downloaded, enter **transfer download filename {filename.jpg | filename.gif | filename.png}**.
- i. Enter **transfer download start** to view your updated settings and answer **y** to the prompt to confirm the current download settings and start the download. Information similar to the following appears:
 

```
Mode..... TFTP
Data Type..... Login Image
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... <filename.jpg|.gif|.png>
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```
- j. Enter **save config** to save your settings.




---

**Note** If you ever want to remove this logo from the web authentication login page, enter **clear webimage**.

---

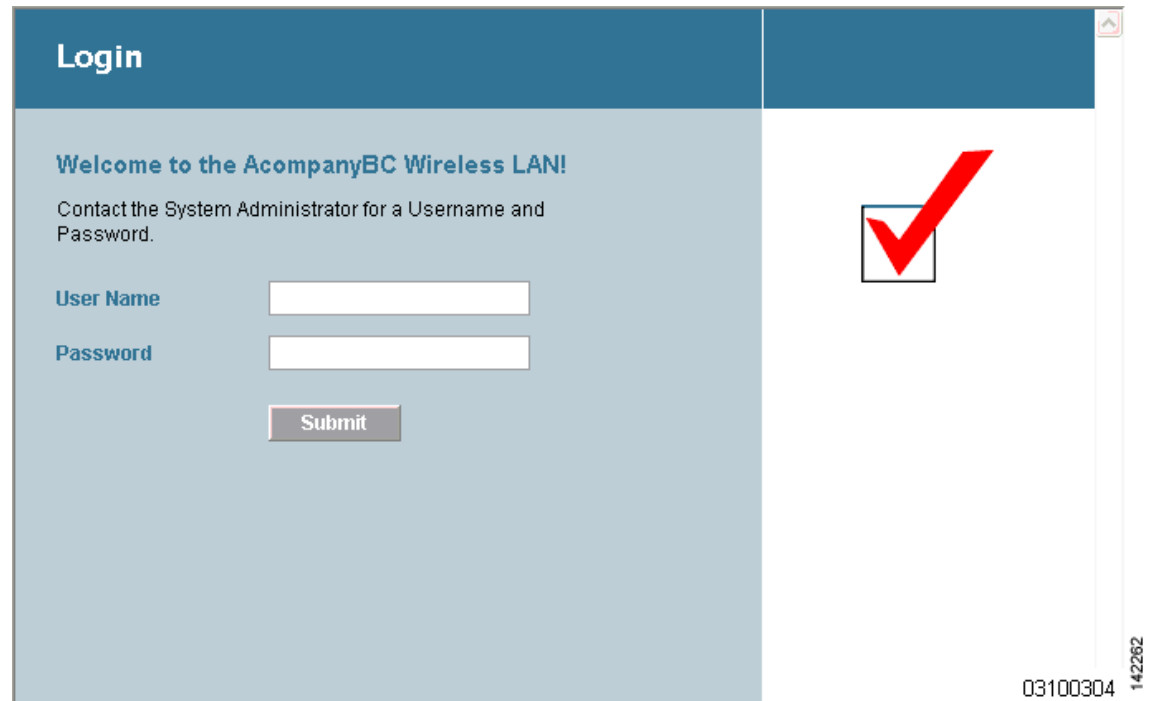
- Step 9** Follow the instructions in the [“Using the CLI to Verify the Web Authentication Login Page Settings” section on page 10-25](#) to verify your settings.
-



## Modified Default Web Authentication Login Page Example

Figure 10-12 shows an example of a modified default web authentication login page.

**Figure 10-12** Modified Default Web Authentication Login Page Example



These are the CLI commands used to create this login page:

```
config custom-web weblogo disable
```

```
config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!
```

```
config custom-web webmessage Contact the System Administrator for a Username and Password.
```

```
transfer download start
```

```
Mode..... TFTP
Data Type..... Login Image
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... /
TFTP Filename..... Logo.gif
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

```
config custom-web redirecturl http://www.AcompanyBC.com
```

```
show custom-web
```

```
Cisco Logo..... Disabled
CustomLogo..... 00_logo.gif
Custom Title..... Welcome to the AcompanyBC Wireless LAN!
Custom Message Contact the System Administrator for a Username and Password.
Custom Redirect URL..... http://www.AcompanyBC.com
Web Authentication Mode..... Disabled
Web Authentication URL..... Disabled
```

## Creating a Customized Web Authentication Login Page

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
 var link = document.location.href;
 var searchString = "redirect=";
 var equalIndex = link.indexOf(searchString);
 var redirectUrl = "";

 if (document.forms[0].action == "") {
 var url = window.location.href;
 var args = new Object();
 var query = location.search.substring(1);
 var pairs = query.split("&");
 for(var i=0;i<pairs.length;i++){
 var pos = pairs[i].indexOf('=');
 if(pos == -1) continue;
 var argname = pairs[i].substring(0,pos);
 var value = pairs[i].substring(pos+1);
 args[argname] = unescape(value);
 }
 document.forms[0].action = args.switch_url;
 }

 if(equalIndex >= 0) {
 equalIndex += searchString.length;
 redirectUrl = "";
 redirectUrl += link.substring(equalIndex);
 }
 if(redirectUrl.length > 255)
 redirectUrl = redirectUrl.substring(0,255);
 document.forms[0].redirect_url.value = redirectUrl;
 document.forms[0].buttonClicked.value = 4;
 document.forms[0].submit();
}

function loadAction(){
 var url = window.location.href;
 var args = new Object();
 var query = location.search.substring(1);
 var pairs = query.split("&");
 for(var i=0;i<pairs.length;i++){
 var pos = pairs[i].indexOf('=');
 if(pos == -1) continue;
 var argname = pairs[i].substring(0,pos);
 var value = pairs[i].substring(pos+1);
 args[argname] = unescape(value);
 }
}
//alert("AP MAC Address is " + args.ap_mac);
//alert("The Switch URL to post user credentials is " + args.switch_url);
//document.forms[0].action = args.switch_url;
```



These parameters are added to the URL when the user's Internet browser is redirected to the customized login page:

- **ap\_mac**—The MAC address of the access point to which the wireless user is associated.
- **switch\_url**—The URL of the controller to which the user credentials should be posted.
- **redirect**—The URL to which the user is redirected after authentication is successful.
- **statusCode**—The status code returned from the controller's web authentication server.
- **wlan**—The WLAN SSID to which the wireless user is associated.

These are the available status codes:

- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username is already logged into the system?"
- Status Code 4: "You have been excluded."
- Status Code 5: "The User Name and Password combination you have entered is invalid. Please try again."



**Note**

For additional information, refer to the *External Web Authentication with Wireless LAN Controllers Configuration Example* at this URL:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html>

## Using a Customized Web Authentication Login Page from an External Web Server

If you want to use a customized web authentication login page that you configured on an external web server, follow the instructions in the GUI or CLI procedure below. When you enable this feature, the user is directed to your customized login page on the external web server.



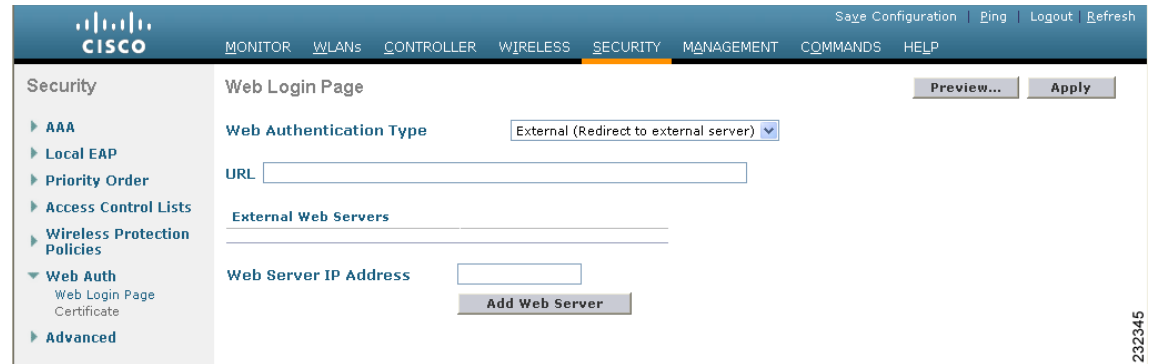
**Note**

For 5500 series controllers, 2100 series controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page. See the *Configuring Security Solutions* chapter for more information on ACLs.

## Using the GUI to Choose a Customized Web Authentication Login Page from an External Web Server

- Step 1** Choose **Security > Web Auth > Web Login Page** to open the Web Login page (see [Figure 10-13](#)).

Figure 10-13 Web Login Page



- Step 2** From the Web Authentication Type drop-down box, choose **External (Redirect to external server)**.
- Step 3** In the URL field, enter the URL of the customized web authentication login page on your web server. You can enter up to 252 characters.
- Step 4** In the Web Server IP Address field, enter the IP address of your web server. Your web server should be on a different network from the controller service port network.
- Step 5** Click **Add Web Server**. This server now appears in the list of external web servers.
- Step 6** Click **Apply** to commit your changes.
- Step 7** If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes.

## Using the CLI to Choose a Customized Web Authentication Login Page from an External Web Server

- Step 1** To specify the web authentication type, enter this command:  
**config custom-web webauth\_type external**
- Step 2** To specify the URL of the customized web authentication login page on your web server, enter this command:  
**config custom-web ext-webauth-url url**  
You can enter up to 252 characters for the URL.
- Step 3** To specify the IP address of your web server, enter this command:  
**config custom-web ext-webserver {add | delete} server\_IP\_address**
- Step 4** Enter **save config** to save your settings.
- Step 5** Follow the instructions in the [“Using the CLI to Verify the Web Authentication Login Page Settings” section on page 10-25](#) to verify your settings.

## Downloading a Customized Web Authentication Login Page

You can compress the page and image files used for displaying a web authentication login page into a .tar file for download to a controller. These files are known as the *webauth bundle*. The maximum allowed size of the files in their uncompressed state is 1 MB. When the .tar file is downloaded from a local TFTP server, it enters the controller's file system as an untarred file.



### Note

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 the following 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 for the webauth bundle.



### Note

Configuration backups do not include extra files or components, such as the webauth bundle or external licenses, that you download and store on your controller, so you should manually save external backup copies of those files or components.

Follow these guidelines when preparing the customized login page:

- Name the login page "login.html." The controller prepares the web authentication URL based on this name. If the server does not find this file after the webauth bundle has been 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 of relative type.
- Ensure that no filenames within the bundle are greater than 30 characters.

You can download a login page example from Cisco WCS and use it as a starting point for your customized login page. Refer to the "Downloading a Customized Web Auth Page" section in the Using Templates chapter of the *Cisco Wireless Control System Configuration Guide, Release 6.0* for instructions.

If you want to download a customized web authentication login page to the controller, follow the instructions in the GUI or CLI procedure below.

## Using the GUI to Download a Customized Web Authentication Login Page

- Step 1** Make sure that you have a TFTP server available for the file download. See the guidelines for setting up a TFTP server in [Step 8](#) of the "Using the CLI to Choose the Default Web Authentication Login Page" section on page 10-15.
- Step 2** Copy the .tar file containing your login page to the default directory on your TFTP server.
- Step 3** Choose **Commands > Download File** to open the Download File to Controller page (see [Figure 10-14](#)).

Figure 10-14 Download File to Controller Page

The screenshot shows the Cisco configuration interface for downloading a file to the controller. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The 'COMMANDS' tab is active. On the left, there is a sidebar with options: Download File, Upload File, Reboot, Reset to Factory Default, and Set Time. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type: Webauth Bundle (dropdown menu)
- Transfer Mode: TFTP (dropdown menu)
- Server Details section:
  - IP Address: 209.165.200.225
  - Maximum retries: 10
  - Timeout (seconds): 6
  - File Path: (empty text box)
  - File Name: AS\_4200\_5\_1\_84\_0.aes

At the top right of the form area, there are 'Clear' and 'Download' buttons. A vertical ID number '2801646' is visible on the right edge of the screenshot.

- Step 4** From the File Type drop-down box, choose **Webauth Bundle**.
- Step 5** From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.
- Step 6** In the IP Address field, enter the IP address of the TFTP server.
- Step 7** If you are using a TFTP server, enter the maximum number of times the controller should attempt to download the .tar file in the Maximum Retries field.  
**Range:** 1 to 254  
**Default:** 10
- Step 8** If you are using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the \*.tar file in the Timeout field.  
**Range:** 1 to 254 seconds  
**Default:** 6 seconds
- Step 9** In the File Path field, enter the path of the .tar file to be downloaded. The default value is “/.”
- Step 10** In the File Name field, enter the name of the .tar file to be downloaded.
- Step 11** If you are using an FTP server, follow these steps:
- In the Server Login Username field, enter the username to log into the FTP server.
  - In the Server Login Password field, enter the password to log into the FTP server.
  - In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.
- Step 12** Click **Download** to download the .tar file to the controller.
- Step 13** Choose **Security > Web Auth > Web Login Page** to open the Web Login page.
- Step 14** From the Web Authentication Type drop-down box, choose **Customized (Downloaded)**.
- Step 15** Click **Apply** to commit your changes.
- Step 16** Click **Preview** to view your customized web authentication login page.
- Step 17** If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes.

## Using the CLI to Download a Customized Web Authentication Login Page

- 
- Step 1** Make sure that you have a TFTP server available for the file download. See the guidelines for setting up a TFTP server in [Step 8](#) of the “Using the CLI to Choose the Default Web Authentication Login Page” section on page 10-15.
- Step 2** Copy the .tar file containing your login page to the default directory on your TFTP server.
- Step 3** To specify the download mode, enter **transfer download mode tftp**.
- Step 4** To specify the type of file to be downloaded, enter **transfer download datatype webauthbundle**.
- Step 5** To specify the IP address of the TFTP server, enter **transfer download serverip *tftp-server-ip-address***.



---

**Note** Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

---

- Step 6** To specify the download path, enter **transfer download path *absolute-tftp-server-path-to-file***.
- Step 7** To specify the file to be downloaded, enter **transfer download filename *filename.tar***.
- Step 8** Enter **transfer download start** to view your updated settings and answer **y** to the prompt to confirm the current download settings and start the download.
- Step 9** To specify the web authentication type, enter **config custom-web webauth\_type customized**.



- Step 10** Enter **save config** to save your settings.
- Step 11** Follow the instructions in the “Using the CLI to Verify the Web Authentication Login Page Settings” section on page 10-25 to verify your settings.

## Customized Web Authentication Login Page Example

Figure 10-15 shows an example of a customized web authentication login page.

**Figure 10-15** Customized Web Authentication Login Page Example

## Using the CLI to Verify the Web Authentication Login Page Settings

Enter **show custom-web** to verify your changes to the web authentication login page. This example shows the information that appears when the configuration settings are set to default values:

```
Cisco Logo..... Enabled
CustomLogo..... Disabled
Custom Title..... Disabled
Custom Message..... Disabled
Custom Redirect URL..... Disabled
Web Authentication Mode..... Disabled
Web Authentication URL..... Disabled
```

This example shows the information that appears when the configuration settings have been modified:

```
Cisco Logo..... Disabled
CustomLogo..... 00_logo.gif
Custom Title..... Welcome to the AcompanyBC Wireless LAN!
Custom Message..... Contact the System Administrator for a
 Username and Password.
Custom Redirect URL..... http://www.AcompanyBC.com
Web Authentication Mode..... Internal
Web Authentication URL..... Disabled
```

## 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.

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

Using the controller GUI, follow these steps to assign web login, login failure, and logout pages to a WLAN.

- 
- Step 1** Choose **WLANs** to open the WLANs page.
- Step 2** Click the ID number of the WLAN to which you want to assign a web login, login failure, or logout page.
- Step 3** Choose **Security > Layer 3**.
- Step 4** Make sure that **Web Policy** and **Authentication** are selected.
- Step 5** To override the global authentication configuration web authentication pages, check the **Override Global Config** check box.
- Step 6** When the Web Auth Type drop-down box appears, choose one of the following options 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. For details on downloading custom pages, refer to the [“Downloading a Customized Web Authentication Login Page”](#) section on page 10-22.

---

- **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.

- Step 7** If you chose External as the web authentication type in [Step 6](#), choose **AAA Servers** and choose up to three RADIUS and LDAP servers using 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.



---

- Step 8** To establish the priority in which the servers are contacted to perform web authentication, follow these steps. The default order is local, RADIUS, LDAP.
- 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.
  - Click the **Up** and **Down** buttons until the desired server type is at the top of the box.
  - Click the < arrow to move the server type to the priority box on the left.
  - Repeat these steps to assign priority to the other servers.
- Step 9** Click **Apply** to commit your changes.
- Step 10** Click **Save Configuration** to save your changes.
- 

## Using the CLI to Assign Login, Login Failure, and Logout Pages per WLAN

Using the controller CLI, follow these steps to assign web login, login failure, and logout pages to a WLAN.

---

- Step 1** To determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page, enter this command:
- show wlan summary**
- Step 2** If you want wireless guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the WLAN for which it should display:
- config wlan custom-web login-page** *page\_name wlan\_id*—Defines a customized login page for a given WLAN.
  - config wlan custom-web loginfailure-page** *page\_name wlan\_id*—Defines a customized login failure page for a given WLAN.
-  **Note** To use the controller's default login failure page, enter this command: **config wlan custom-web loginfailure-page none** *wlan\_id*.
- 
- config wlan custom-web logout-page** *page\_name wlan\_id*—Defines a customized logout page for a given WLAN.
-  **Note** To use the controller's default logout page, enter this command: **config wlan custom-web logout-page none** *wlan\_id*.
- 
- Step 3** If you want wireless guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:
- config wlan custom-web ext-webauth-url** *ext\_web\_url wlan\_id*

**Step 4** If you want to define the order in which web authentication servers are contacted, enter this command:

```
config wlan security web-auth server-precedence wlan_id {local | ldap | radius} {local | ldap | radius} {local | ldap | radius}
```

The default order of server web authentication is local, RADIUS, LDAP.




---

**Note** All external servers must be pre-configured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

---

**Step 5** To define which web authentication page displays for a wireless guest user, enter this command:

```
config wlan custom-web webauth-type {internal | customized | external} wlan_id
```

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web login page that was configured in [Step 2](#).




---

**Note** You do not need to define the web authentication type in [Step 5](#) for the login failure and logout pages as they are always customized.

---

- **external** redirects users to the URL that was configured in [Step 3](#).

**Step 6** To use a WLAN-specific custom web configuration rather than a global custom web configuration, enter this command:

```
config wlan custom-web global disable wlan_id
```




---

**Note** If you enter the **config wlan custom-web global enable** *wlan\_id* command, the custom web authentication configuration at the global level is used.

---

**Step 7** To save your changes, enter this command:

```
save config
```

---

## Configuring Wired Guest Access

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

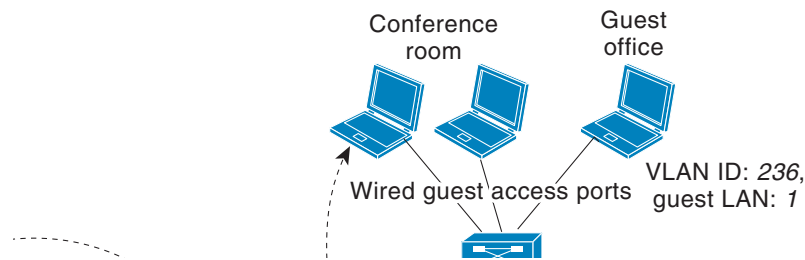
Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch. See [Figure 10-16](#).

**Note**

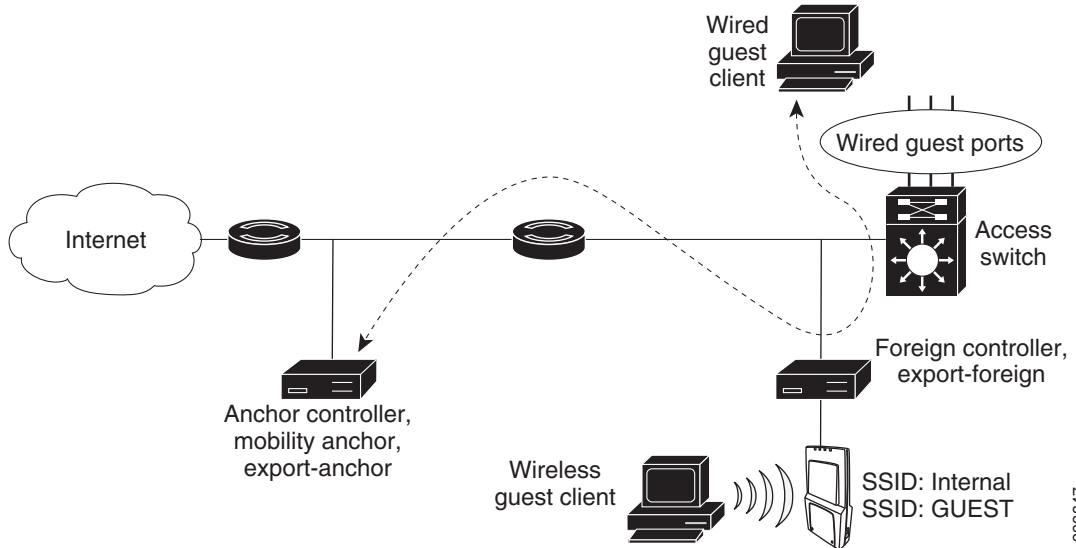
The DMZ controller set to *local* for mobility anchor should not have an ingress interface set. You cannot enable the WLAN if the ingress interface is not set to *none* and is changed to an ingress interface (defined under the Controller > Interface tab). You should recreate the mobility anchor and WLAN if the ingress interface is changed.

**Figure 10-16** Wired Guest Access Example with One Controller



If two controllers are being used, the foreign controller, which receives the wired guest traffic from the access switch, forwards it to the anchor controller. A bidirectional EoIP tunnel is established between the foreign and anchor controllers to handle this traffic. See [Figure 10-17](#).

Figure 10-17 Wired Guest Access Example with Two Controllers

**Note**

Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

**Note**

You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract. For details on configuring these features, refer to the [“Configuring Quality of Service Roles”](#) section on page 4-70.

## Configuration Overview

To configure wired guest access on a wireless network, you will perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

## Configuration Guidelines

Follow these guidelines before using wired guest access on your network:

- Wired guest access is supported only on the following controllers: 5500 and 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch.
- Wired guest access interfaces must be tagged.

- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not attempt to trunk a guest VLAN on the Catalyst 3750G Integrated Wireless LAN Controller Switch to multiple controllers. Redundancy cannot be achieved by doing so.

## Using the GUI to Configure Wired Guest Access

Using the controller GUI, follow these steps to configure wired guest user access on your network.

- Step 1** To create a dynamic interface for wired guest user access, choose **Controller > Interfaces**. The Interfaces page appears.
- Step 2** Click **New** to open the Interfaces > New page.
- Step 3** Enter a name and VLAN ID for the new interface.
- Step 4** Click **Apply** to commit your changes.
- Step 5** In the Port Number text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).
- Step 6** Check the **Guest LAN** check box.
- Step 7** Enter an IP address for the primary DHCP server.
- Step 8** Click **Apply** to commit your changes.
- Step 9** To create a wired LAN for guest user access, choose **WLANS**.
- Step 10** On the WLANS page, choose **Create New** from the drop-down box and click **Go**. The WLANS > New page appears (see [Figure 10-18](#)).

**Figure 10-18** WLANS > New Page

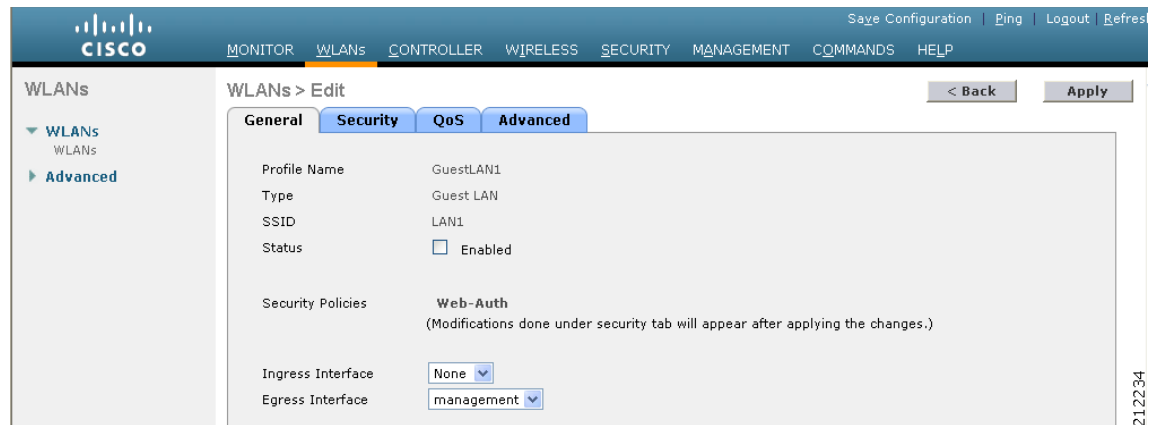
- Step 11** From the Type drop-down box, choose **Guest LAN**.
- Step 12** In the Profile Name field, enter a name that identifies the guest LAN. Do not use any spaces.
- Step 13** In the WLAN SSID field, enter an SSID that identifies the guest LAN. Do not use any spaces.
- Step 14** From the WLAN ID drop-down box, choose the ID number for this guest LAN.



**Note** You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).

- Step 15** Click **Apply** to commit your changes. The WLANS > Edit page appears (see [Figure 10-19](#)).

Figure 10-19 WLANs > Edit Page



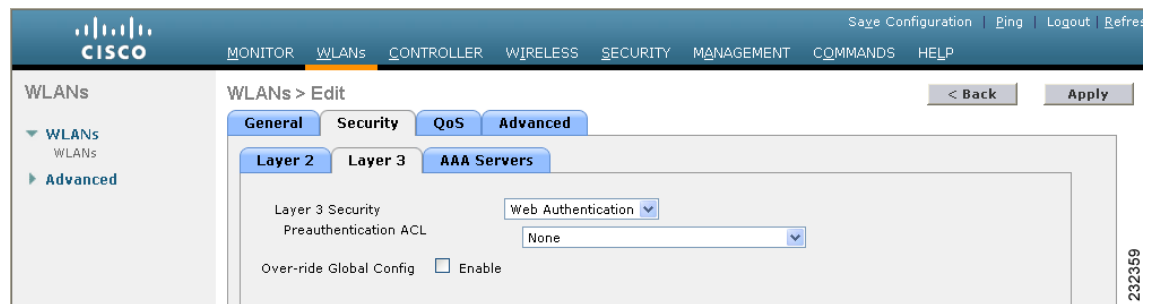
- Step 16** Check the **Enabled** check box for the Status parameter.
- Step 17** Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing [Step 18](#) and [Step 19](#).
- Step 18** From the Ingress Interface drop-down box, choose the VLAN that you created in [Step 3](#). This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.
- Step 19** From the Egress Interface drop-down box, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.



**Note** If you have only one controller in the configuration, choose **management** from the Egress Interface drop-down box.

- Step 20** If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security > Layer 3**. The WLANs > Edit (Security > Layer 3) page appears (see [Figure 10-20](#)).

Figure 10-20 WLANs > Edit (Security > Layer 3) Page



- Step 21** From the Layer 3 Security drop-down box, choose one of the following:
  - **None**—Layer 3 security is disabled.
  - **Web Authentication**—Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
  - **Web Passthrough**—Allows users to access the network without entering a username and password.



- Step 22** If you choose the Web Passthrough option, an **Email Input** check box appears. Check this check box if you want users to be prompted for their email address when attempting to connect to the network.
- Step 23** To override the global authentication configuration set on the Web Login page, check the **Override Global Config** check box.
- Step 24** When the Web Auth Type drop-down box appears, choose one of the following options to define the web authentication pages for wired 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.

---

- **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.

- Step 25** If you chose External as the web authentication type in [Step 24](#), choose **AAA Servers** and choose up to three RADIUS and LDAP servers using 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.

---

- Step 26** To establish the priority in which the servers are contacted to perform web authentication, follow these steps. The default order is local, RADIUS, LDAP.
- 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.
  - Click the **Up** and **Down** buttons until the desired server type is at the top of the box.
  - Click the < arrow to move the server type to the priority box on the left.
  - Repeat these steps to assign priority to the other servers.
- Step 27** Click **Apply** to commit your changes.
- Step 28** Click **Save Configuration** to save your changes.
- Step 29** Repeat this process if a second (anchor) controller is being used in the network.
- 

## Using the CLI to Configure Wired Guest Access

Using the controller CLI, follow these steps to configure wired guest user access on your network.

- 
- Step 1** To create a dynamic interface (VLAN) for wired guest user access, enter this command:  
**config interface create** *interface\_name* *vlan\_id*
- Step 2** If a link aggregation trunk is not configured, enter this command to map a physical port to the interface:  
**config interface port** *interface\_name* *primary\_port* {*secondary\_port*}
- Step 3** To enable or disable the guest LAN VLAN, enter this command:  
**config interface guest-lan** *interface\_name* {**enable** | **disable**}
- This VLAN is later associated with the ingress interface created in [Step 5](#).
- Step 4** To create a wired LAN for wired client traffic and associate it to an interface, enter this command:  
**config guest-lan create** *guest\_lan\_id* *interface\_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).




---

**Note** To delete a wired guest LAN, enter this command: **config guest-lan delete** *guest\_lan\_id*

---

- Step 5** To configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch, enter this command:  
**config guest-lan ingress-interface** *guest\_lan\_id* *interface\_name*
- Step 6** To configure an egress interface to transmit wired guest traffic out of the controller, enter this command:  
**config guest-lan interface** *guest\_lan\_id* *interface\_name*




---

**Note** If the wired guest traffic is terminating on another controller, repeat [Step 4](#) and [Step 6](#) for the terminating (anchor) controller and [Step 1](#) through [Step 5](#) for the originating (foreign) controller. Additionally, configure the following command for both controllers:  
**config mobility group anchor add** {**guest-lan** *guest\_lan\_id* | **wlan** *wlan\_id*} *IP\_address*

---

- Step 7** To configure the security policy for the wired guest LAN, enter this command:  
**config guest-lan security** {**web-auth enable** *guest\_lan\_id* | **web-passthrough enable** *guest\_lan\_id*}




---

**Note** Web authentication is the default setting.

---

- Step 8** To enable or disable a wired guest LAN, enter this command:  
**config guest-lan** {**enable** | **disable**} *guest\_lan\_id*
- Step 9** If you want wired guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the guest LAN for which it should display:
- **config guest-lan custom-web login-page** *page\_name* *guest\_lan\_id*—Defines a web login page.
  - **config guest-lan custom-web loginfailure-page** *page\_name* *guest\_lan\_id*—Defines a web login failure page.




---

**Note** To use the controller's default login failure page, enter this command: **config guest-lan custom-web loginfailure-page none** *guest\_lan\_id*.

---

- **config guest-lan custom-web logout-page** *page\_name guest\_lan\_id*—Defines a web logout page.



**Note** To use the controller's default logout page, enter this command: **config guest-lan custom-web logout-page none** *guest\_lan\_id*.

- Step 10** If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

```
config guest-lan custom-web ext-webauth-url ext_web_url guest_lan_id
```

- Step 11** If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:

```
config wlan security web-auth server-precedence wlan_id {local | ldap | radius} {local | ldap | radius} {local | ldap | radius}
```

The default order of server web authentication is local, RADIUS, LDAP.



**Note** All external servers must be pre-configured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

- Step 12** To define the web login page for wired guest users, enter this command:

```
config guest-lan custom-web webauth-type {internal | customized | external} guest_lan_id
```

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web pages (login, login failure, or logout) that were configured in [Step 9](#).
- **external** redirects users to the URL that was configured in [Step 10](#).

- Step 13** To use a guest-LAN specific custom web configuration rather than a global custom web configuration, enter this command:

```
config guest-lan custom-web global disable guest_lan_id
```



**Note** If you enter the **config guest-lan custom-web global enable** *guest\_lan\_id* command, the custom web authentication configuration at the global level is used.

- Step 14** To save your changes, enter this command:

```
save config
```



**Note** Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

- Step 15** To display the customized web authentication settings for a specific guest LAN, enter this command:

```
show custom-web {all | guest-lan guest_lan_id}
```



**Note** If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Information similar to the following appears for the **show custom-web all** command:

```
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... None
Web Authentication Type..... External
External Web Authentication URL..... http:\\9.43.0.100\\login.html
```

External Web Server list

Index IP Address

```

1 9.43.0.100
2 0.0.0.0
3 0.0.0.0
4 0.0.0.0
5 0.0.0.0
...
20 0.0.0.0
```

Configuration Per Profile:

WLAN ID: 1

```
WLAN Status..... Enabled
Web Security Policy..... Web Based Authentication
Global Status..... Disabled
WebAuth Type..... Customized
Login Page..... login1.html
Loginfailure page name..... loginfailure1.html
Logout page name..... logout1.html
```

```

WLAN ID: 2
WLAN Status..... Enabled
 Web Security Policy..... Web Based Authentication
 Global Status..... Disabled
 WebAuth Type..... Internal
 Loginfailure page name..... None
 Logout page name..... None

```

```

WLAN ID: 3
WLAN Status..... Enabled
 Web Security Policy..... Web Based Authentication
 Global Status..... Disabled
 WebAuth Type..... Customized
 Login Page..... login.html
 Loginfailure page name..... LF2.html
 Logout page name..... LG2.html

```

Information similar to the following appears for the **show custom-web guest-lan *guest\_lan\_id*** command:

```

Guest LAN ID: 1
Guest LAN Status..... Disabled
Web Security Policy..... Web Based Authentication
Global Status..... Enabled
WebAuth Type..... Internal
Loginfailure page name..... None
Logout page name..... None

```

**Step 16** To display a summary of the local interfaces, enter this command:

**show interface summary**

Information similar to the following appears:

| Interface Name | Port | Vlan Id  | IP Address      | Type    | Ap Mgr | Guest |
|----------------|------|----------|-----------------|---------|--------|-------|
| ap-manager     | 1    | untagged | 1.100.163.25    | Static  | Yes    | No    |
| management     | 1    | untagged | 1.100.163.24    | Static  | No     | No    |
| service-port   | N/A  | N/A      | 172.19.35.31    | Static  | No     | No    |
| virtual        | N/A  | N/A      | 209.165.200.225 | Static  | No     | No    |
| wired          | 1    | 20       | 10.20.20.8      | Dynamic | No     | No    |
| wired-guest    | 1    | 236      | 10.20.236.50    | Dynamic | No     | Yes   |



**Note** The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

**Step 17** To display detailed interface information, enter this command:

```
show interface detailed interface_name
```

Information similar to the following appears:

```
Interface Name..... wired-guest
MAC Address..... 00:1a:6d:dd:1e:40
IP Address..... 0.0.0.0
DHCP Option 82..... Disabled
Virtual DNS Host Name..... Disabled
AP Manager..... No
Guest Interface..... No
```

**Step 18** To display the configuration of a specific wired guest LAN, enter this command:

```
show guest-lan guest_lan_id
```

Information similar to the following appears:

```
Guest LAN Identifier..... 1
Profile Name..... guestlan
Network Name (SSID)..... guestlan
Status..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wired
Ingress Interface..... wired-guest
WLAN ACL..... unconfigured
DHCP Server..... 10.20.236.90
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
Security
 Web Based Authentication..... Enabled
 ACL..... Unconfigured
 Web-Passthrough..... Disabled
 Conditional Web Redirect..... Disabled
 Auto Anchor..... Disabled
Mobility Anchor List
GLAN ID IP Address Status

```



**Note** Enter **show guest-lan summary** to view all wired guest LANs configured on the controller.

**Step 19** To display the active wired guest LAN clients, enter this command:

**show client summary guest-lan**

Information similar to the following appears:

```
Number of Clients..... 1
MAC Address AP Name Status WLAN Auth Protocol Port Wired

00:16:36:40:ac:58 N/A Associated 1 No 802.3 1 Yes
```

**Step 20** To display detailed information for a specific client, enter this command:

**show client detail *client\_mac***

Information similar to the following appears:

```
Client MAC Address..... 00:40:96:b2:a3:44
Client Username N/A
AP MAC Address..... 00:18:74:c7:c0:90
Client State..... Associated
Wireless LAN Id..... 1
BSSID..... 00:18:74:c7:c0:9f
Channel..... 56
IP Address..... 192.168.10.28
Association Id..... 1
Authentication Algorithm..... Open System
Reason Code..... 0
Status Code..... 0
Session Timeout..... 0
Client CCX version..... 5
Client E2E version..... No E2E support
Diagnostics Capability..... Supported
S69 Capability..... Supported
Mirroring..... Disabled
QoS Level..... Silver
...
```

