Managing User Accounts

This chapter contains these sections:

Information About Creating Guest Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator user, 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.

Restrictions on Managing User Accounts

- The local user database is limited to a maximum of 2048 entries, which is also the default value. 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.
- For net user accounts or guest user accounts, the following special characters are allowed along with alphanumeric characters: ~, @, #, $, %, ^, &, (,), !, _, -, `, ., [,], =, +, *, :, ;, {, }, ,, /, and \.

Creating a Lobby Ambassador Account

Creating a Lobby Ambassador Account (GUI)

Step 1 Choose **Management > Local Management Users** to open the 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 Click **New** to create a lobby ambassador account. The Local Management Users > New page appears.

Step 3 In the User Name text box, 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** text boxes, enter a password for the lobby ambassador account.

Note Passwords are case sensitive. The settings for the management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 5 Choose **LobbyAdmin** from the User Access Mode drop-down list. 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.

Creating a Lobby Ambassador Account (CLI)

To create a lobby ambassador account use the following command:

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 (GUI)

Step 1 Log into the controller as the lobby ambassador, using the username and password. The Lobby Ambassador Guest Management > Guest Users List page appears.

Step 2 Click **New** to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears.

Step 3 In the User Name text box, 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, select the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password text boxes.
- If you want to create a password for this guest user, leave the **Generate Password** check box unselected and enter a password in both the **Password** and **Confirm Password** text boxes.

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

Step 5 From the Lifetime drop-down lists, 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 text boxes 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 nonzero 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* command to make a guest user account permanent without deleting and recreating it.

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

Note We recommend that you 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 text box, 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.
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

Viewing the Guest Accounts (GUI)

To view guest user accounts using the controller GUI, choose **Security** > **AAA** > **Local Net Users**. The Local Net Users page appears.

From this page, you 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.

Viewing the Guest Accounts (CLI)

To see 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

Information About Web Authentication Certificates

The operating system of the controller 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.

Starting with 7.0.250.0 and 7.3.101.0 releases (but not in 7.2.x release), SHA2 certificates are supported.

Note The WEB UI home page may not load when **ip http access class** command is enabled. When you encounter this issue, we recommend that you do the following:

1 Run the **show iosd liin** command.

2 Get the internet-address and configure the same ip as *permit* in the access-list.

Note For WEB UI access using TACACS+ server, custom method-list for authentication and authorization pointing to the TACACS+ server group does not work. You should use the default authorization method-list pointing to the same TACACS+ server group for the WEB UI to work.

Obtaining Web Authentication Certificates

Obtaining a Web Authentication Certificate (GUI)

Step 1 Choose **Security** > **Web Auth** > **Certificate** to open the Web Authentication Certificate page.
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:

a) Click **Regenerate Certificate**. The operating system generates a new web authentication certificate, and a successfully generated web authentication certificate message appears.
b) Reboot the controller to register the new certificate.

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

a) Verify that the controller can ping the TFTP server.
b) Select the **Download SSL Certificate** check box.
c) In the Server IP Address text box, enter the IP address of the TFTP server.
The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.
d) Enter the maximum number of times that each download can be attempted in the Maximum Retries text box and the amount of time (in seconds) allowed for each download in the Timeout text box.
e) In the Certificate File Path text box, enter the directory path of the certificate.
f) In the Certificate File Name text box, enter the name of the certificate (**certname**.pem).
g) In the Certificate Password text box, 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.

Obtaining a Web Authentication Certificate (CLI)

Step 1 See the current web authentication certificate by entering 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 We recommend that the Common Name (CN) of the externally generated web authentication certificate be 1.1.1.1 (or the equivalent 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.

1 Specify the name, path, and type of certificate to be downloaded by entering 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.

2 Start the download process by entering this command:

transfer download start

3 Reboot the controller to register the new certificate by entering 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. When the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

Note If a client uses more than 20 DNS resolved addresses, the controller overwrites the 21st address in the first address space in the Mobile Station Control Block (MSCB) table, but the first address is still retained in the client. If the client again tries to use the first address, it will not be reachable because the controller does not have this address in the list of allowed addresses for the client's MSCB table.

Note One-Time Passwords (OTP) are not supported on web authentication.

When a client is associated with 802.1X + WebAuth Security and when the client roams, the 802.1X username is updated in the client information.

Note Web Authentication does not work with IPv6 URL when WLAN is LS however IPv4 with LS and IPv6 with CS works.. The re-directed web-auth page is not displayed when IPv6 URL is typed in the browser and WLAN is in Local Switching.

Guidelines and Limitations

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 1: Typical Web-Browser Security Alert

Note When clients connect to a WebAuth SSID with preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

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.

To prevent the security alert from appearing, follow these steps:

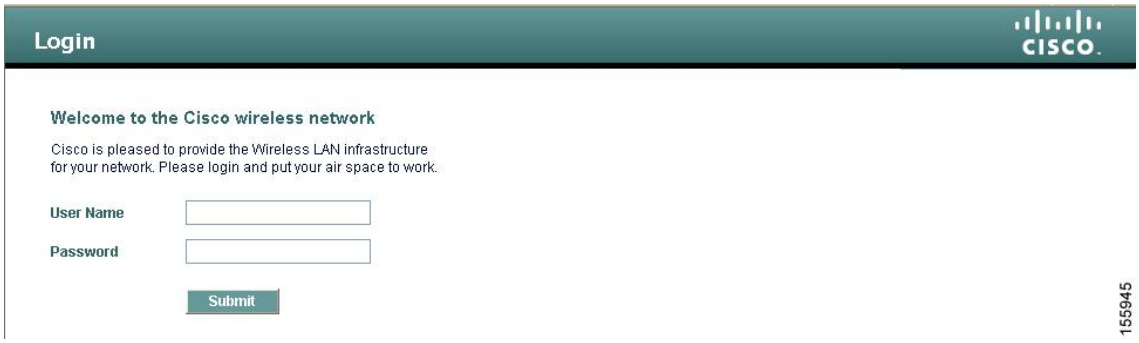
1. Click **View Certificate** on the Security Alert page.
2. Click **Install Certificate**.
3. When the Certificate Import Wizard appears, click **Next**.
4. Choose **Place all certificates in the following store** and click **Browse**.
5. At the bottom of the Select Certificate Store page, select the **Show Physical Stores** check box.
6. Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.
7. Click **OK**.
8. Click **Next** > **Finish**.
9. When the "The import was successful" message appears, click **OK**.

a Because the issuer text box is blank on the controller self-signed certificate, open Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**, unselect the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.

10 Reboot the PC. On the next web authentication attempt, the login page appears.

The following figure shows the default web authentication login page.

Figure 2: Default Web Authentication Login Page



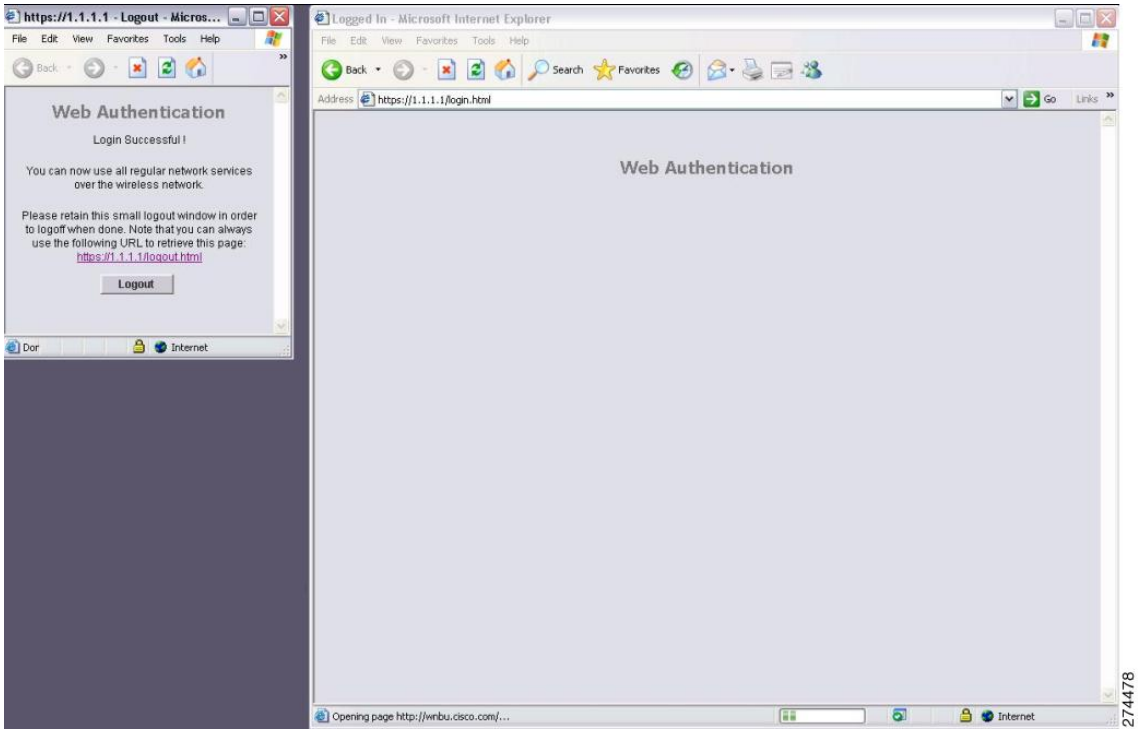
The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- 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 Default Web Authentication Login Page section 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 3: 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

Choosing the Default Web Authentication Login Page

Information About Default Web Authentication Login Page

If you are using a custom web-auth bundle that is served by the internal controller web server, the page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time (For example Firefox 4) if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.

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 the **config network secureweb cipher-option sslv2 disable command**. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is disabled.

Note Cisco TAC is not responsible for creating a custom webauth bundle.

If you have a complex custom web authentication module, it is recommended that you use an external web-auth config on the controller, where the full login page is hosted at an external web server.

Guidelines and Limitations

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 the **config network secureweb cipher-option sslv2 disable command**. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is disabled.

Choosing the Default Web Authentication Login Page (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, 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 in the Redirect URL After Login text box. You can enter up to 254 characters.

Step 6 If you want to create your own headline on the login page, enter the desired text in the Headline text box. 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 text box. 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.

Choosing the Default Web Authentication Login Page (CLI)

Step 1 Specify the default web authentication type by entering 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 the **clear redirecturl** command.

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 the **clear webtitle** command.

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 the **clear webmessage** command.

Step 7 To enable or disable the web authentication logout popup window, enter this command:
config custom-web logout-popup {**enable** | **disable**}

Step 8 Enter the **save config** command to save your settings.

Step 9 Import your own logo into the web authentication login page as follows:

1. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Follow these guidelines 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 Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.
2. Ensure that the controller can contact the TFTP server by entering this command:
   ping ip-address
3. 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.
4. Specify the download mode by entering this command:
   transfer download mode tftp
5. Specify the type of file to be downloaded by entering this command:
   transfer download datatype image

6 Specify the IP address of the TFTP server by entering this command:

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.

7 Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

8 Specify the file to be downloaded by entering this command:

transfer download filename {*filename.jpg* | *filename.gif* | *filename.png*}

9 View your updated settings and answer *y* to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

10 Save your settings by entering this command:

save config

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

Step 10 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 24 section to verify your settings.

Example: 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;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
      }
      else if(args.statusCode == 2){
       alert("You are not configured to authenticate against web portal. No further action
 is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username is
 already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>
```

```
<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password" name="password"
 SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

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.

The available status codes are as follows:

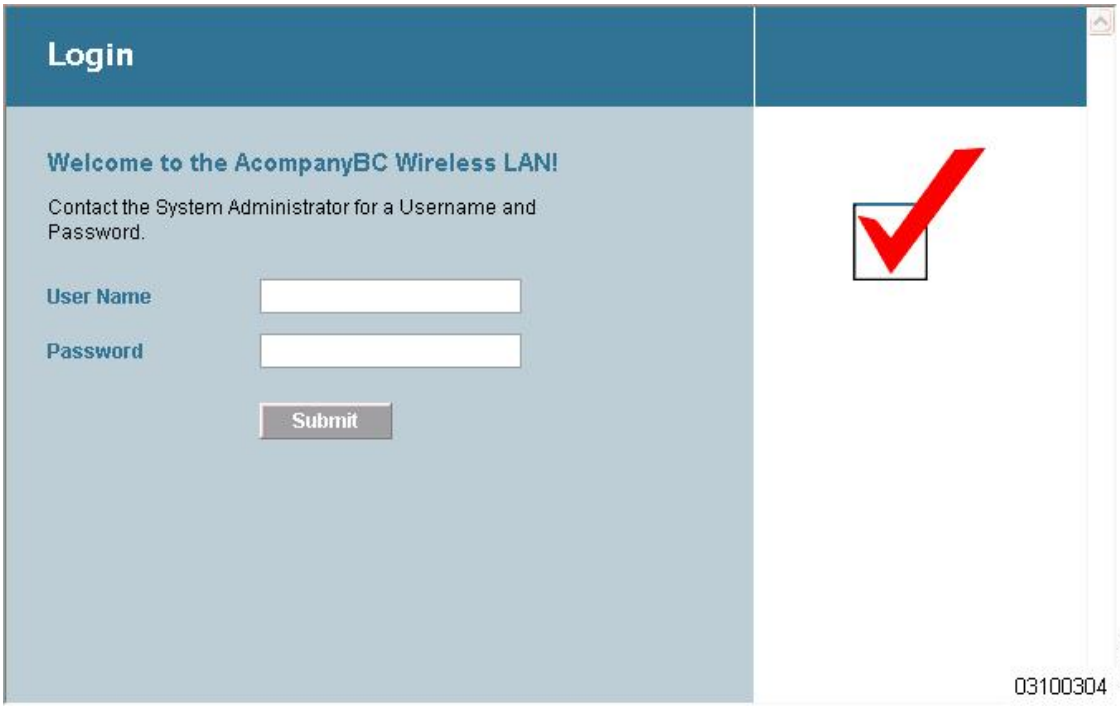
- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username 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, see the *External Web Authentication with Wireless LAN Controllers Configuration Example* at http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html

Example: Modified Default Web Authentication Login Page Example

This figure shows an example of a modified default web authentication login page.

Figure 4: Modified Default Web Authentication Login Page Example



These CLI commands were 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*
- **config custom-web redirecturl** *url*

Generating a Certificate Signing Request

Step 1 Install and open the OpenSSL application.

Step 2 Enter the command:

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

Controllers support a maximum key size of 2048 bits.

Note You must provide the correct Common Name. Ensure that the host name that is used to create the certificate (Common Name) matches the Domain Name System (DNS) host name entry for the virtual interface IP on the controller. This name should exist in the DNS as well. Also, after you make the change to the VIP interface, you must reboot the system in order for this change to take effect.

After you issue the command, you are prompted to enter information such as country name, state, city, and so on.

Information similar to the following appears:

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.....................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:
OpenSSL>
```

After you provide all the required details two files are generated:

- A new private key that includes the name *mykey.pem*
- A CSR that includes the name *myreq.pem*

Step 3 Copy and paste the Certificate Signing Request (CSR) information into any CA enrollment tool. After you submit the CSR to a third party CA, the third party CA digitally signs the certificate and sends back the signed certificate chain through e-mail. In case of chained certificates, you receive the entire chain of certificates from the CA. If you only have one intermediate certificate similar to the example above, you will receive the following three certificates from the CA:

- Root certificate.pem
- Intermediate certificate.pem
- Device certificate.pem

Note Ensure that the certificate is Apache-compatible with SHA1 encryption.

Step 4 Once you have all the three certificates, copy and paste into another file the contents of each .pem file in this order:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
```

```
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

Step 5 Save the file as *All-certs.pem*.

Step 6 Combine the All-certs.pem certificate with the private key that you generated along with the CSR (the private key of the device certificate, which is mykey.pem in this example), and save the file as final.pem.

Step 7 Create the All-certs.pem and final.pem files by entering these commands:

```
openssl> pkcs12 -export -in All-certs.pem -inkey mykey.pem
       -out All-certs.p12 -clcerts -passin pass:check123
       -passout pass:check123

openssl> pkcs12 -in All-certs.p12 -out final.pem
       -passin pass:check123 -passout pass:check123
```

final.pem is the file that we need to download to the controller.

Note You must enter a password for the parameters **-passin** and **-passout**. The password that is configured for the **-passout** parameter must match the certpassword parameter that is configured on the controller. In the above example, the password that is configured for both the **-passin** and **-passout** parameters is check123.

What to Do Next

Download the final.pem file to the controller either using CLI or GUI.

Downloading Third-Party Certificate (GUI)

Step 1 Copy the device certificate final.pem to the default directory on your TFTP server.

Step 2 Choose **Security > Web Auth > Certificate** to open the Web Authentication Certificate page.

Step 3 Check the **Download SSL Certificate** check box to view the Download SSL Certificate From Server parameters.

Step 4 In the **Server IP Address** text box, enter the IP address of the TFTP server.

Step 5 In the **File Path** text box, enter the directory path of the certificate.

Step 6 In the **File Name** text box, enter the name of the certificate.

Step 7 In the **Certificate Password** text box, enter the password to protect the certificate.

Step 8 Click **Apply**.

Step 9 After the download is complete, choose **Commands > Reboot** and click **Save and Reboot**.

Step 10 Click **OK** in order to confirm your decision to reboot the controller.

Downloading Third-Party Certificate (CLI)

Step 1 Move the *final.pem* file to the default directory on your TFTP server. Change the download settings by entering the following commands:

```
(Cisco Controller) > transfer download mode tftp
(Cisco Controller) > transfer download datatype webauthcert
(Cisco Controller) > transfer download serverip <TFTP server IP address>
(Cisco Controller) > transfer download path <absolute TFTP server path to the update file>
(Cisco Controller) > transfer download filename final.pem
```

Step 2 Enter the password for the .pem file so that the operating system can decrypt the SSL key and certificate.

```
(Cisco Controller) > transfer download certpassword password
```

Note Ensure that the value for *certpassword* is the same as the **-passout** parameter when you generate a CSR.

Step 3 Start the certificate and key download by entering the this command:
transfer download start

Example:

```
(Cisco Controller) > transfer download start

Mode............................................ TFTP
Data Type....................................... Site Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path......................................./
TFTP Filename................................... final.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

Step 4 Reboot the controller.

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

Information About Customized Web Authentication Login Page

You can customize the web authentication login page to redirect to an external web server. When you enable this feature, the user is directed to your customized login page on the external web server.

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.

Guidelines and Limitations

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.

Choosing a Customized Web Authentication Login Page from an External Web Server

Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **External (Redirect to external server)**.

Step 3 In the Redirect URL after login text box, enter the URL that you want the user to be redirected after a login. For example, you may enter your company's URL here and the users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page was served. of the customized web authentication login page on your web server. You can enter up to 252 characters.

Step 4 In the External Webauth URL text box, enter the URL that is to be used for external web authentication.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)

Step 1 Specify the web authentication type by entering this command:
config custom-web webauth_type external

Step 2 Specify the URL of the customized web authentication login page on your web server by entering this command:
config custom-web ext-webauth-url *url*

You can enter up to 252 characters for the URL.

Step 3 Specify the IP address of your web server by entering this command:
config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

Step 4 Enter the **save config** command to save your settings.

Step 5 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 24 section to verify your settings.

Additional References

See Configuring Security Solutions for more information on ACLs.

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.

You can download a login page example from Cisco Prime Infrastructure and use it as a starting point for your customized login page. For more information, see the Cisco Prime Infrastructure documentation.

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, we recommend 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.

Note If the customized webauth bundle has more than 3 separated elements, we advise you to use an external server to prevent page load issues that may be caused because of TCP rate-limiting policy on the controller.

Prerequisites for Downloading a Customized Web Authentication 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 text boxes 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).
- Ensure that no filenames within the bundle are greater than 30 characters.

Additional References

You can download a login page example from Cisco Prime Infrastructure and use it as a starting point for your customized login page. For more information, see the Cisco Prime Infrastructure documentation.

Downloading a Customized Web Authentication Login Page (GUI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the **File Type** drop-down list, choose **Webauth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**

Step 5 In the **IP Address** text box, enter the IP address of the server.

Step 6 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 text box.
The range is 1 to 254.

The default is 10.

Step 7 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 text box.
The range is 1 to 254 seconds.

The default is 6 seconds.

Step 8 In the **File Path** text box, enter the path of the .tar file to be downloaded. The default value is "/."

Step 9 In the **File Name** text box, enter the name of the .tar file to be downloaded.

Step 10 If you are using an FTP server, follow these steps:

1. In the **Server Login Username** text box, enter the username to log into the FTP server.
2. In the **Server Login Password** text box, enter the password to log into the FTP server.
3. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the .tar file to the controller.

Step 12 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 13 From the Web Authentication Type drop-down list, choose **Customized (Downloaded)**.

Step 14 Click **Apply**.

Step 15 Click **Preview** to view your customized web authentication login page.

Step 16 If you are satisfied with the content and appearance of the login page, click **Save Configuration**.

Downloading a Customized Web Authentication Login Page (CLI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Specify the download mode by entering this command:
transfer download mode {**tftp** | **ftp**}

Step 3 Specify the type of file to be downloaded by entering this command:
transfer download datatype webauthbundle

Step 4 Specify the IP address of the TFTP server by entering this command:
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 5 Specify the download path by entering this command:
transfer download path *absolute-tftp-server-path-to-file*

Step 6 Specify the file to be downloaded by entering this command:
transfer download filename *filename.tar*

Step 7 View your updated settings and answer **y** to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

Step 8 Specify the web authentication type by entering this command:
config custom-web webauth_type *customized*

Step 9 Enter the **save config** command to save your settings.

Additional References

See Web Authentication Process.

Example: Customized Web Authentication Login Page

This figure shows an example of a customized web authentication login page.

Figure 5: Customized Web Authentication Login Page Example

Verifying the Web Authentication Login Page Settings (CLI)

Verify your changes to the web authentication login page by entering this command:

show custom-web

Assigning Login, Login Failure, and Logout Pages per WLAN

Information About 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.

Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)

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, select the **Override Global Config** check box.

Step 6 When the Web Auth Type drop-down list 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 lists 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 list 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 text box.

  You can choose 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 lists.

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 Establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

1. 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.
2. Click **Up** and **Down** until the desired server type is at the top of the box.
3. Click the **<** arrow to move the server type to the priority box on the left.
4. 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.

Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)

Step 1 Determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page by entering 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 the **config wlan custom-web loginfailure-page none** *wlan_id* command.
- **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 the **config wlan custom-web logout-page none** *wlan_id* command.

Step 3 Redirect wireless guess users to an external server before accessing the web login page by entering this command to specify the URL of the external server:
config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

Step 4 Define the order in which web authentication servers are contacted by entering 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 and LDAP.

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

Step 5 Define which web authentication page displays for a wireless guest user by entering 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 Use a WLAN-specific custom web configuration rather than a global custom web configuration by entering 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 Save your changes by entering this command:
save config

Configuring Wired Guest Access

Information About 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.

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.

You can create a basic peer to peer WLAN ACL and apply it to the wired guest WLAN. This will not block peer to peer traffic and the guest users can still communicate with each other.

Prerequisites for Configuring Wired Guest Access

To configure wired guest access on a wireless network, you must 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

Restrictions for Configuring Wired Guest Access

- 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. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.
- The controller does not use the callStationIDType parameter configured for the Radius server while authenticating wired clients, instead the controller uses the system MAC address configured for the callStationIDType parameter.

Configuring Wired Guest Access

Configuring Wired Guest Access (GUI)

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 Select the **Guest LAN** check box.

Step 7 Click **Apply** to commit your changes.

Step 8 To create a wired LAN for guest user access, choose **WLANs**.

Step 9 On the WLANs page, choose **Create New** from the drop-down list and click **Go**. The **WLANs** > **New page** appears.

Step 10 From the Type drop-down list, choose **Guest LAN**.

Step 11 In the **Profile Name** text box, enter a name that identifies the guest LAN. Do not use any spaces.

Step 12 From the WLAN ID drop-down list, 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 13 Click **Apply** to commit your changes.

Step 14 Select the **Enabled** check box for the Status parameter.

Step 15 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 16* and *Step 17*.

Step 16 From the Ingress Interface drop-down list, 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 17 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18 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.

Step 19 From the Layer 3 Security drop-down list, 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.

  Note There should not be a Layer 3 gateway on the guest wired VLAN, as this would bypass the web authentication done through the controller.

Step 20 If you choose the Web Passthrough option, an **Email Input** check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21 To override the global authentication configuration set on the Web Login page, select the **Override Global Config** check box.

Step 22 When the Web Auth Type drop-down list 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 lists 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 list 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 text box.

  You can choose 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 23 If you chose External as the web authentication type in *Step 22*, choose **Security > AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note You can configure the Authentication and LDAP Server using both IPv4 and IPv6 addresses.

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 24 To establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

1. 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.
2. Click **Up** and **Down** until the desired server type is at the top of the box.
3. Click the **<** arrow to move the server type to the priority box on the left.
4. Repeat these steps to assign priority to the other servers.

Step 25 Click **Apply**.

Step 26 Click **Save Configuration**.

Step 27 Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Step 1 Create a dynamic interface (VLAN) for wired guest user access by entering this command:
config interface create *interface_name vlan_id*

Step 2 If 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 Enable or disable the guest LAN VLAN by entering 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 Create a wired LAN for wired client traffic and associate it to an interface by entering 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 the **config guest-lan delete** *guest_lan_id command.*

Step 5 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 by entering this command:
config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 Configure an egress interface to transmit wired guest traffic out of the controller by entering 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 **config mobility group anchor add** {**guest-lan** *guest_lan_id* | **wlan** *wlan_id} IP_address* command for both controllers.

Step 7 Configure the security policy for the wired guest LAN by entering 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 Enable or disable a wired guest LAN by entering 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 the **config guest-lan custom-web loginfailure-page none** *guest_lan_id* command.

- **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 the **config guest-lan custom-web logout-page none** *guest_lan_id* command.

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 preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 Define the web login page for wired guest users by entering 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 Use a guest-LAN specific custom web configuration rather than a global custom web configuration by entering 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 Save your changes by entering 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 Display the customized web authentication settings for a specific guest LAN by entering 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).

Step 16 Display a summary of the local interfaces by entering this command:
show interface summary

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

Display detailed interface information by entering this command:

show interface detailed *interface_name*

Step 17 Display the configuration of a specific wired guest LAN by entering this command:
show guest-lan *guest_lan_id*

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

Step 18 Display the active wired guest LAN clients by entering this command:
show client summary guest-lan

Step 19 Display detailed information for a specific client by entering this command:
show client detail *client_mac*

Supporting IPv6 Client Guest Access

The client is in WebAuth Required state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once authenticated, the user's MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

In order to support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com which returns a DNSv6 (AAAA) record.