Introduction

The paradigm of public access has extended to the enterprise itself. Our highly mobile, information-on-demand culture requires on-demand network connectivity. For this reason, enterprise guest access services are becoming increasingly important and a necessity in the corporate environment.

While there is broad recognition that guest networking is becoming increasingly important, there is also well-founded apprehension over how to safeguard internal corporate information and infrastructure assets. When implemented correctly, an enterprise that implements a guest access solution will most likely improve their overall security posture as a result of the network audits associated with the implementation process.

In addition to overall improved security, implementing a guest access network offers these additional general benefits.

- Authentication and authorization control of guests based on variables including date, duration, and bandwidth.
- An audit mechanism to track who is currently using, or has used, the network.

Additional benefits of a wireless-based guest access include the following:

- It provides wider coverage by including areas such as lobbies and other common areas that otherwise might not have been wired for network connectivity.
- It removes the need for designated guest access areas or rooms.
Scope

Several architectures can be implemented to offer guest access in the enterprise. It is not the goal of this chapter to cover all possible solutions. Instead, this chapter focuses on the implementation of wireless guest networking using the Cisco Unified Wireless Network solution. For more information on deploying wired and wireless Guest Access services in other topology scenarios, see: Network Virtualization--Guest and Partner Access Deployment Guide

Wireless Guest Access Overview

Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using embedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Guest Access using the Cisco Unified Wireless Network Solution

The Cisco Unified WLAN solution offers a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the centralized architecture. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLC endpoints. The benefit of this approach is that there are no additional protocols or segmentation techniques that must be implemented to isolate guest traffic from the enterprise.

See Figure 10-1 for an example of guest access topology using a centralized WLAN architecture.
As illustrated in Figure 10-1 the anchor controller is located in the enterprise DMZ where it performs an "anchor" function. The anchor controller is responsible for terminating EoIP tunnels that originate from other campus controller throughout the network. These "foreign" controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs are transported via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are encapsulated using CAPWAP from the AP to the foreign controller and then encapsulated in EoIP from the foreign management system to a guest VLAN defined on the anchor WLC. In this way, guest user traffic is forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

**WLAN Controller Guest Access**

The Guest Access solution is self-contained and does not require any external platforms to perform access control, web portal, or AAA services. All these functions are configured and run within the anchor controller. However, the option exists to implement one or all of these functions externally and is discussed later in the chapter.

**Supported Platforms**

The anchor function, which includes tunnel termination, web authentication, and access control is supported on the following WLC platforms (using version 8.1 or later):

- WLC 2504
- WLC 5508
- WLC 5520
- WiSM-2
- WLC 8510
- WLC 8540

The following WLC platforms cannot be used for anchor functions, but can be used for standard controller deployments and guest mobility tunnel origination (foreign WLC) to a designated anchor controller(s):
- Cisco WLAN Controller Module for Integrated Service Routers (ISR-SM)
- WLC 7500
- Virtual WLC

Auto Anchor Mobility to Support Wireless Guest Access

Auto anchor mobility, or guest WLAN mobility, is a key feature of the Cisco Unified Wireless Network solution. It offers the ability to map a provisioned guest WLAN to one or more (anchor) WLCs by using an EoIP tunnel. Auto anchor mobility allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ (see Figure 10-2).

Figure 10-2  Auto Anchor EoIP Tunnels

Figure 10-3 shows a sniffer trace of an Ethernet in IP tunnel (highlighted) between a foreign controller with a guest WLAN provisioned and an anchor controller that is performing local web authentication. The first IP detail shown represents the Ethernet in IP tunnel between the foreign and anchor controllers. The second IP detail is that of guest traffic (in this case, a DNS query).
Anchor Controller Deployment Guidelines

This section provides guidelines for deploying an anchor controller to support wireless guest access.

Anchor Controller Positioning

Because the anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet, it is typically positioned in the enterprise Internet DMZ. In doing so, rules can be established within the firewall to precisely manage communications between authorized controllers throughout the enterprise and the anchor controller. Such rules might include filtering on source or destination controller addresses, UDP port 16666 for inter-WLC communication, and IP protocol ID 97 Ethernet in IP for client traffic. Other rules that might be needed include the following:

- UDP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80, 443 and 8443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for CLI access
- UDP 123 for NTP
- TCP 514 for Syslog
- UDP 1812 and 1813 RADIUS

Depending on the topology, the firewall can be used to protect the anchor controller from outside threats.
For the best possible performance and because of its suggested positioning in the network, it is strongly recommended that the guest anchor controller be dedicated to supporting guest access functions only. In other words, the anchor controller should not be used to support guest access in addition to controlling and managing other CAPWAP APs in the enterprise.

DHCP Services

As previously described, guest traffic is transported at Layer 2 via EoIP. Therefore, the first point at which DHCP services can be implemented is either locally on the anchor controller or the controller can relay client DHCP requests to an external server. See Guest Access Configuration, for configuration examples.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a dynamic interface/VLAN on the anchor. Depending on the topology, this interface might connect to an interface on a firewall, or directly to an Internet border router. Therefore, a client's default gateway IP is either that of the firewall or the address of a VLAN/interface on the first hop router. For ingress routing, it is assumed the guest VLAN is directly connected to a DMZ interface on a firewall or to an interface on a border router. In either case, the guest (VLAN) subnet is known as a directly connected network and advertised accordingly.

Anchor Controller Sizing and Scaling

The most cost-effective platform to support guest networking, in most enterprise deployments is the Cisco 2504 Series controller. Assuming the controller is being deployed to support guest access with EoIP tunnel termination only, the 2504 with support for 12 APs is sufficient because it is assumed the controller is not going to be used to manage APs in the network.

A single wireless LAN controller can support EoIP tunnels from up to 71 foreign controllers within the enterprise.

The selection of the guest anchor controller is a function of the amount of guest traffic, as defined by the number of active guest client sessions, or as defined by the uplink interface capacity on the controller, or both.

Total throughput and client limitations per guest anchor controller are as follows:

- 2504 WLC = 1 Gbps and 1000 guest clients
- 5508 WLC = 8 Gbps and 7,000 guest clients
- 5520 WLC = 20Gbps and 20,000 guest clients
- Catalyst 6K WiSM-2 = 20G bps and 15,000 guest clients
- WLC 7500 = 10 Gbps and 20,000 guest clients
- 8510 WLC = 10 Gbps and 20,000 guest clients
- 8540 WLC = 40 Gbps and 64,000 guest clients
Anchor Controller Redundancy N+1

Beginning with Release 4.1 of Cisco Unified Wireless Network solution software, a "guest N+1" redundancy capability was added to the auto anchor/mobility functionality. This feature introduced an automatic ping function that enables a foreign controller to proactively ping anchor controllers to verify control and data path connectivity. In the event of failure or an active anchor becomes unreachable, the foreign controller does the following:

- Automatically detects that the anchor has become unreachable.
- Automatically disassociates any wireless clients that were previously associated with the unreachable anchor.
- Automatically re-associates wireless client(s) to an alternate anchor WLC.

With guest N+1 redundancy, two or more anchor WLCs can be defined for a given guest WLAN. Figure 10-4 shows a generic guest access topology with anchor controller redundancy.

---

**Figure 10-4**  
Guest Access Topology with Guest Anchor N+1 Redundancy

---

Keep in mind the following in regards to guest N+1 redundancy:

- A given foreign controller load balances wireless client connections across the list of anchor controllers configured for the guest WLAN. There is currently no method to designate one anchor as primary with one or more secondary anchors.

- Wireless clients that are associated with an anchor WLC that becomes unreachable are re-associated with another anchor defined for the WLAN. When this happens, assuming web authentication is being used, the client is redirected to the web portal authentication page and required to re-submit their credentials.

---

**Note**  
Multicast traffic is not supported over guest tunnels, even if multicast is enabled on the Cisco Unified Wireless Network.
Anchor Controller Redundancy Priority

The guest anchor priority feature provides a mechanism that gives "active/standby" load distribution amongst the anchor WLCs. This is achieved by assigning a fixed priority to each anchor WLC, by distributing the load to highest priority WLC and in round-robin fashion if they have the same priority value.

<table>
<thead>
<tr>
<th>Releases Prior to 8.1</th>
<th>With Release 8.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>All guest clients are load balanced in round robin fashion amongst anchor WLCs.</td>
<td>All guest clients are sent to anchor controller with highest priority in relation to local internal WLC.</td>
</tr>
<tr>
<td>If an anchor fails, guest clients will be load balanced amongst remaining anchor WLCs.</td>
<td>If an anchor fails, guest clients will be sent to the next highest priority or round robin if remaining anchors have same priority value.</td>
</tr>
</tbody>
</table>

You can configure a priority to the guest anchor when you configure a WLAN. Priority values range from 1 (high) to 3 (low) or primary, secondary or tertiary and defined priority is displayed with guest anchor. Only one priority value is allowed per anchor WLC. Selection of guest anchor is round-robin based on a single priority value. If a guest anchor is down, the fallback would be on guest anchors with equal priority. If all guest anchors with same priority value are down, the selection would be on a round-robin basis on next highest priority and so on. Default priority value is 3. If WLC is upgraded to Release 8.1, it will be marked with priority 3. Priority configurations are retained across reboots. The priority configuration would be synchronized on HA pair for seamless switchover. Same set of rules apply in determining the anchor WLC regardless of IPv4 and/or IPv6 addressing. That is, highest priority value is determinant and not addressing including dual stack case.

Restrictions

- No hard limit on the number of times a priority value is used.
- Feature applies only to wireless and "old" mobility model.
- Maximum supported anchor per WLAN is 24 (same as maximum anchor per WLAN in releases prior to 8.1).
- Downgrading from Release 8.1 would void this feature since it is not supported on earlier images.
- If a guest anchor with higher priority comes up, the existing connections will not shift to the new high priority anchor and only the new connections will go to it.
- This feature is applicable when all internal and anchor WLCs are using Release 8.1.
- There should not be a local address with priority of zero at the Internal/Foreign controller. Priority 0 in the output indicates a local IP address. For example at the anchor WLC on DMZ with tunnel termination.

Deployment Considerations

- Priority configuration should only be done on foreign controller WLAN. On the mobility list if you are seeing value zero and non-zero that means the same controller is acting as Anchor for few WLANs and foreign controller for few WLAN, if you have WLC in DMZ and there is no APs connected to it, then we should not see any non-zero priority for any of its WLANs, as this should be the terminating point for all the clients on the network.
Ideally we should not see priority zero on foreign WLC and non-zero on anchor WLC. Example: 10.10.10.10(Site A) and 20.20.20.20(Site B) should not have any priority with zero and DMZ controller 172.10.10.10(Site A) and 172.20.20.20(Site B) should not have any priority with non-zero values.

Here priority values zero is not configurable when we select the controller own IP Address as anchor. It will automatically set the priority zero if controller own IP address is selected as anchor.

**Examples**

- Local anchor WLCs may be grouped together with higher priority value than group of remote anchor WLCs.
- Guest client traffic goes to Anchor WLC(s) that is/are local to internal WLC rather than remote one(s) due to having higher priority value.
- Guest client traffic will be load balanced in round-robin across local anchor WLCs since local anchors have same priority value.
- If all local anchor WLCs fail then traffic will be load balanced in round-robin across remote anchor WLC with next priority level.

**Web Portal Authentication**

The Cisco Centralized Guest Access solution offers a built-in web portal that is used to solicit guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer or acceptable use policy information (see Figure 10-5).
The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customized page is required, administrators have the option of importing and locally storing a customized page. Additionally, if an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. See Guest Access Configuration, for web page configuration guidelines.

**User Redirection**

As is typical for most web-based authentication systems, in order for guest clients to be redirected to the WLC web authentication page, they must launch a web browser session and attempt to open a destination URL. For redirection to work correctly, the following conditions must be met:

- **DNS resolution**—The guest access topology must ensure that valid DNS servers are assigned via DHCP and those DNS servers are reachable to users prior to authentication. When a client associates to a web policy WLAN for authentication, all traffic is blocked except DHCP and DNS. Therefore, the DNS servers must be reachable from the anchor controller. Depending on the topology, this might require opening up conduits through a firewall to permit DNS or modifying ACLs on an Internet border router.

- **Resolvable Home Page URL**—The home page URL of a guest user must be globally resolvable by DNS. If a user home page is, for example, an internal company home page that cannot be resolved outside of their company intranet, that user is not redirected. In this case, the user must open a URL to a public site such as www.yahoo.com or www.google.com.

---

**Welcome to the Cisco wireless network**

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
</table>

The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customized page is required, administrators have the option of importing and locally storing a customized page. Additionally, if an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. See Guest Access Configuration, for web page configuration guidelines.
HTTP Port 80—If the home page of a user is resolvable, but connects to a web server on a port other than port 80, they are not redirected. Again, the user is required to open a URL that uses port 80 to be redirected to the WLC web authentication page.

Note

In addition to port 80, there is an option to configure one additional port number that the controller can monitor for redirection. The setting is available only through the CLI of the controller:

```shell
<controller_name> config> networkweb-auth-port <port>
```

### Guest Credentials Management

Guest credentials can be created and managed centrally using the management system beginning with release 4.0 and later. A network administrator can create a limited privilege account within the management system that permits lobby ambassador access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted to do is create and assign guest credentials to controllers that have web-policy configured WLANs.

As with many configuration tasks within the management system, guest credentials are created using templates. Some of the newer guest user template options and capabilities are:

- There are two types of guest templates: one for scheduling immediate guest access with limited or unlimited lifetime, and the other permits administrators to schedule "future" guest access and offers time of day as well as day of week access restrictions.
- The solution offers administrators the ability to e-mail credentials to guest users. Additionally, when the "schedule" guest template is used, the system automatically e-mails credentials for each new day (interval) that access is offered.
- Guest credentials can be applied to the WLC(s) based on a (guest) WLAN SSID and the management system mapping information: campus/building/floor location or based on a WLAN SSID and a specific controller or list of controllers. The latter method is used when deploying guest access using the guest mobility anchor method as discussed in this chapter.

After a lobby ambassador has created a guest template, it is applied to one or more controllers depending on the guest access topology. Only controllers with a "web" policy-configured WLAN are listed as a candidate controller to which the template can be applied. This is also true when applying guest templates to controllers based on the management system map location criteria.

Guest credentials, once applied, are stored locally on the (anchor) WLC (under Security > Local Net Users) and remain there until expiration of the "Lifetime" variable as defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLC stops forwarding traffic and returns to the WEBAUTH_REQD policy state for that user. Unless the guest credentials are re-applied (to the controller), the user is no longer able to access the network.

Note

The Lifetime variable associated with guest credentials is independent of the WLAN session timeout variable. If a user remains connected beyond the WLAN session timeout interval, they are de-authenticated. The user is then redirected to the web portal and, assuming their credentials have not expired, must log back in to regain access. To avoid annoying redirects for authentication, the guest WLAN session timeout variable should be set appropriately.
Local Controller Lobby Admin Access

In the event that a centralized management system is not deployed or unavailable, a network administrator can establish a local admin account on the anchor controller, which has only lobby admin privileges. A person who logs in to the controller using the lobby admin account has access to guest user management functions. Configuration options available for local guest management are limited in contrast to the capabilities available through the management system, and include:

- User name
- Generate password
- Administrator assigned password
- Confirm the password
- Lifetime-days:hours:minutes:seconds
- SSID
- Guest Role Profile
- Only WLANs configured for Layer 3 web policy authentication are displayed
- Description

Any credentials that may have been applied to the controller by the management system are shown when an admin logs into the controller. A local lobby admin account has privileges to modify or delete any guest credentials that were previously created by the management system. Guest credentials that are created locally on the WLC do not automatically appear in the management system unless the controller's configuration is updated/refreshed in the management system. Locally created guest credentials that are imported into the management system as a result of a WLC configuration refresh appear as a new guest template that can be edited and re-applied to the WLC.

Guest User Authentication

As previously discussed in Guest Credentials Management, when an administrator uses the management system or a local account on a controller to create guest user credentials, those credentials are stored locally on the controller, which in the case of a centralized guest access topology, would be the anchor controller.

When a wireless guest logs in through the web portal, the controller handles the authentication in the following order:

1. The controller checks its local database for username and password and, if present, grants access. If no user credentials are found, then:

2. The controller checks to see if an external RADIUS server has been configured for the guest WLAN (under WLAN configuration settings). If so, then the controller creates a RADIUS access-request packet with the user name and password and forwards it to the selected RADIUS server for authentication.

If no specific RADIUS servers have been configured for the guest WLAN:

3. The controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate "network" users are queried with the guest user credentials. Otherwise, if no RADIUS servers have "network user" checked, and the user has not authenticated as a result of 1 or 2 above, authentication fails.
Note

A RADIUS server can still be used to support network user authentication even if the Network User check box is cleared under the WLC Security > AAA > RADIUS settings. However, to do so, a server must then be explicitly selected under the Security > AAA Servers settings of a given WLAN.

External Authentication

WLC and the guest account management (lobby ambassador) capabilities can be used only to create and apply guest user credentials for local authentication on the WLC. However, there may be cases where an enterprise already has an existing guest management/authentication solution deployed as part of a wired guest access or NAC solution. If this is the case, the anchor controller/guest WLAN can be configured to forward web portal authentication to an external RADIUS server, as described in Guest User Authentication.

The default protocol used by the controller to authenticate web users is Password Authentication Protocol (PAP). In the event you are authenticating web users to an external AAA server, be sure to verify the protocols supported by that server. The anchor controller can also be configured to use CHAP or MD5-CHAP for web authentication. The web auth protocol type is configured under the Controller configuration settings of the WLC.

External Authentication using ISE or Cisco Secure ACS and Microsoft User Databases

If a guest access deployment is planning to use ISE or a Microsoft user database in conjunction with Cisco ACS to authenticate guest users, see the following additional Cisco ACS configuration caveats:

Cisco Secure Access Control System

See specifically the following:

Installation and Upgrade Guide for Cisco Secure Access Control System

Active directory integration with ISE:
Active Directory Integration with Cisco ISE

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an enterprise may still need to present an acceptable use policy or disclaimer page to users before granting access. If this is the case, then a guest WLAN can be configured for web policy pass through. In this scenario, a guest user is redirected to a portal page containing disclaimer information.

Pass through mode also has an option for a user to enter an e-mail address before connecting (see Figure 10-6 and Figure 10-7 for sample pages). See Guest Access Configuration, for configuration examples.
Guest Access Configuration

This section describes how to enable a wireless guest access service within the Cisco Unified Wireless Network solution. The configuration tasks require the use of a web browser. A web session is established with the controller by opening an HTTPS session to the controller management IP address: https://management_IP or optionally to a controller service port IP address.
The following procedures assume there is already a deployed infrastructure of controllers and LAPs with the possible exception of the anchor WLC(s). For more information, see Anchor Controller Deployment Guidelines.

Note
Cisco recommends that the configuration steps outlined in this section be followed in the order in which they are presented.

The following references are used throughout the configuration sections:
- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility EoIP tunnel.
- Anchor WLC—Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility EoIP tunnel termination, web redirection, and user authentication.

Note
Only the relevant portion of a given configuration screen capture is shown in this section.

The implementation of the Cisco Unified Wireless Network Guest Access solution can be broken into the following configuration categories:
- Anchor WLC Installation and Interface configuration—This section briefly discusses installation requirements, steps and caveats associated with implementing one or more anchor WLCs. When implementing guest access for the first time in an existing Cisco Unified Wireless Network deployment, the anchor WLC is usually a new platform that is installed at the Internet edge of an Enterprise network.
- Mobility Group Configuration—This section outlines the parameters that must be configured in order for the foreign WLCs to be able to initiate EoIP tunnels to one or more guest anchor WLCs. The mobility group configuration does not itself create the EoIP tunnels, but rather establishes peer relationships between the foreign and anchor WLCs in order to support a guest access WLAN service.
- Guest WLAN Configuration—Highlights WLAN specific configuration parameters that are required to map the guest WLAN (originating from a foreign WLC) to the anchor WLC. It is during this portion of the guest access solution configuration that EoIP tunnels are created between the foreign and anchor WLCs. This section also covers the settings required to invoke Layer 3 redirection for web-based authentication.
- Guest Account Management—This section outlines how to configure and apply guest user credentials locally on the anchor WLC using controllers the anchor WLC's lobby admin interface.
- Other Features and Solution Options—Discusses other features that may be configured including, but not limited to:
  - Web-portal page configuration and management
  - Support for external web redirection
  - Pre-authentication ACLs
  - Anchor WLC DHCP configuration
  - External radius authentication
  - External access control
Anchor WLC Installation and Interface Configuration

As described in Anchor Controller Positioning, Cisco recommends that the anchor WLC be dedicated solely to guest access functions and not be used to control and manage LAPs in the enterprise.

This section does not address all aspects of interface configuration on the anchor WLC. It is assumed the reader is familiar with the WLC initialization and configuration process required upon initial bootup using the serial console interface.

This section offers specific information and caveats as they pertain to configuring interfaces on a WLC being deployed as an anchor in a guest access topology.

As part of the initial configuration (using the serial console interface), you are required to define the following three static interfaces:

- **Controller management**—This interface/IP is used for communications with other controllers in the network. It is also the interface used to terminate EoIP tunnels that originate from the foreign controllers.

- **AP manager interface**—Even though the controller is not used to manage APs, you are still required to configure this interface. Cisco recommends the AP manager interface be configured on the same VLAN and subnet as the management interface.

- **Virtual interface**—The controller quickstart installation documentation recommends defining the virtual IP with an address, such as 192.0.2.1. This address needs to be the same for all controllers that are members of the same mobility group name. The virtual interface is also used as the source IP address when the controller redirects clients for web authentication.

Guest VLAN Interface Configuration

The interfaces previously described are for operations and administrative functions associated with the controller. To implement a guest access service, another interface must be defined. This is the interface through which guest traffic is forwarded for routing to the Internet. As previously described in Anchor Controller Positioning, the guest interface will likely connect to a port on a firewall or be switched to an interface on an Internet border router.

**Defining a New Interface**

Perform the following to define and configure an interface to support guest traffic:

1. **Step 1** Click the **Controller** tab.
2. **Step 2** In the left pane, click **Interfaces** (See Figure 10-8).
Step 3  Click New.

Step 4  Enter an interface name and VLAN ID. (See Figure 10-9).

Step 5  Define the following properties:

- Interface IP
- Mask
- Gateway (for the firewall or next hop router connected to the anchor controller)
- DHCP Server IP (If using an external DHCP server, use the IP address of that server in the Primary DHCP Server field.). See Figure 10-10.
Note

Internal DHCP server is not recommended but if DHCP services are to be implemented locally on the anchor controller, populate the primary DHCP server field with the management IP address of the controller. Review if internal DHCP server support is present on the controller platform. If guest N+1 redundancy is being implemented in the DMZ, repeat the above interface configuration for each additional anchor WLC being deployed.
Mobility Group Configuration

The following default mobility group parameters should already be defined on the foreign WLC(s) as part of a standard centralized WLAN deployment. To support auto-anchor mobility for guest access, the anchor WLC(s) must also be configured with a mobility group domain name.

Defining the Default Mobility Domain Name for the Anchor WLC

Configure a default mobility domain name for the anchor WLC. The anchor's mobility domain name should be different than what is configured for the foreign WLCs. In the examples below, the WLCs (foreign controllers) associated with the enterprise wireless deployment are all members of mobility group 'SRND'. The guest anchor WLC on the other hand, is configured with a different mobility group name: "ANC". This is done to keep the anchor WLC logically separate from the primary mobility domain associated with the enterprise wireless deployment.

Step 1: Click the Controller tab.
Step 2: Enter a name in the Default Mobility Domain Name field.
Step 3: Click Apply. (See Figure 10-11.)

Figure 10-11  Defining a Default Mobility Domain Name on the Anchor WLC

Defining Mobility Group Members of the Anchor WLC

Every foreign WLC within the enterprise deployment that is going to support the guest WLAN must be defined as a mobility group member in the guest anchor WLC(s).

Step 1: Click the Controller tab.
Step 2: In the left pane, click Mobility Management and then Mobility Groups. (See Figure 10-12.)
Step 3  Click New to define a MAC and IP address for each foreign controller that will support the guest access WLAN. (See Figure 10-13.)

The "Group Name" in Figure 10-13 above is the name configured under the foreign WLC's 'Default Mobility Domain Name', which should be different than the name used by the anchor WLC. The member IP and MAC address are those addresses associated with the management interface of the foreign WLCs. Repeat the above steps for each additional foreign WLC that will support the guest WLAN. If more than one anchor is being deployed (guest anchor redundancy), then repeat the steps in Defining the Default Mobility Domain Name for the Anchor WLC and Defining Mobility Group Members of the Anchor WLC.

Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC

As described in Auto Anchor Mobility to Support Wireless Guest Access, each foreign WLC maps the guest WLAN into an EoIP tunnel that terminates on the anchor WLC. Therefore, the anchor WLC(s) must be defined as a mobility group member in each foreign controller. In the example below, note that the group name entry for the anchor WLC is 'ANC' (see Defining Mobility Group Members of the Anchor WLC) whereas the other WLCs that comprise the enterprise wireless deployment are members of the mobility group: 'SRND'.
**Step 1**
Click **New** to add the anchor WLC's IP, MAC address, and Group Name to the mobility members table.

**Step 2**
Repeat these steps for each additional foreign controller. (See **Figure 10-14**.)

**Figure 10-14  Adding Anchor Controller(s) to Foreign WLC**

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address(1pv4/1pv6)</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Status</th>
<th>Hash Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>88:1d:fc:99:fa:1b</td>
<td>172.20.227.112</td>
<td>SRND</td>
<td>0.0.0.0</td>
<td>Up</td>
<td>none</td>
</tr>
<tr>
<td>4c:00:82:71:5a:40</td>
<td>172.20.227.103</td>
<td>SRND</td>
<td>0.0.0.0</td>
<td>Up</td>
<td>none</td>
</tr>
<tr>
<td>f4:46:05:21:85:67</td>
<td>172.20.227.5</td>
<td>ANC</td>
<td>0.0.0.0</td>
<td>Up</td>
<td>none</td>
</tr>
</tbody>
</table>

**Note**
If guest anchor redundancy capability is being deployed, two or more anchor WLC entries are added to each foreign WLC's Mobility Group Members list.

**Guest WLAN Configuration**

The following section describes how to configure a single guest WLAN. The guest WLAN is configured on every foreign WLC that manages APs where guest access is required. Even though the anchor WLC(s) is not specifically used to manage LAPs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor WLC is a logical extension of the WLAN where user traffic is ultimately bridged (using CAPWAP between the AP and the foreign controller, and EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor WLC.

**Note**
It is extremely important to note that all parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign WLC(s). **Figure 10-15** shows a high level diagram illustrating the WLAN configuration discussed below.
**Note**  The parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign controller(s).

### Foreign WLC-Guest WLAN Configuration

**Step 1**  Click the **WLANs** tab and then click **New**. (See **Figure 10-16**.)
Step 2 Define an SSID that is intuitive or easily recognized by potential guest users. The controller automatically assigns a VLAN ID. Administrators have the option of selecting 1 - 16, as long as the ID is not already in use by another SSID/ WLAN.

Step 3 Define a Profile Name.

Step 4 Click Apply. (See Figure 10-17.)

After creation of the new WLAN, the configuration page appears, as shown in Figure 10-18.
Guest Access Configuration

Chapter 10  Cisco Unified Wireless Network Guest Access Services

Guest Access Configuration

Figure 10-18  WLAN Configuration Page

<table>
<thead>
<tr>
<th>General</th>
<th>Security</th>
<th>QoS</th>
<th>Policy-Mapping</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Guest Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>WLAN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td>Guest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policies</td>
<td>[WPA2][Auth(802.1X)]</td>
<td></td>
<td>(Modifications done under security tab will appear after applying the changes.)</td>
<td></td>
</tr>
<tr>
<td>Radio Policy</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface/Interface Group(G)</td>
<td>management</td>
<td>▼</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast VLAN Feature</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS-ID</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note

The default interface used by the foreign WLC for the guest WLAN is the management interface. If the EoIP tunnel cannot be established with the anchor, the foreign controller will disassociate any wireless clients that were previously associated with the unreachable anchor and then assign new clients and reassociate clients to the interface configured under the guest WLAN of the foreign itself. Therefore, it is recommended to link the guest WLAN on the foreign to a non-routable network, or alternatively configure the DHCP server of the management interface with an unreachable IP address. If the anchor becomes unreachable, this prevents the guest clients to gain access to the management network.

Defining Guest WLAN Parameters and Policies

Under the General Configuration tab, perform the following steps:

Step 1  Enable the WLAN by clicking the box next to WLAN Status.

Step 2  Optionally, set the radio policy if you wish to restrict which bands support the guest access.

- Broadcast SSID is enabled by default; leave enabled.
- By default, the WLAN is assigned to the "management" interface of the WLC. Do not change this.

Step 3  Click the Security tab. (See Figure 10-19.)
Step 4  Set the Layer 2 Security to none from its default setting (802.1x WPA/WPA2). (See Figure 10-20.)

Step 5  Click the Layer 3 tab. (See Figure 10-22.)
Step 6  Click the Web Policy check box (a list of additional options will be presented).

A dialog warning box appears, indicating that the WLC will pass DNS traffic to and from clients prior to authentication.

Step 7  Select Authentication or Pass-through for the web policy. (See Guest User Authentication).
A pre-authentication ACL can be used to apply an ACL that allows un-authenticated clients to connect to specific hosts or URL destinations before authentication. The ACL is configured under Security > Access Control Lists. If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client will be unable to resolve and connect to a destination host/URL that would otherwise be allowed by the ACL.

**Step 8** Select the **QoS** tab, as shown in **Figure 10-23**.

**Figure 10-23  Guest WLAN QoS Configuration**

**Step 9** Optionally, set the upstream QoS profile for the guest WLAN. The default is 'Silver (Best Effort)'. In this example, the guest WLAN has been re-assigned to the lowest QoS class.

**Step 10** Click the **Advanced** tab. (See **Figure 10-24**.)

**Figure 10-24  Guest WLAN Advanced Configuration**

**Step 11** Set Session Timeout (this is optional).
Note
Any session timeout greater than 0 (default) forces de-authentication after expiration, and requires the user to re-authenticate through the web portal.

Step 12
Set DHCP Addr. Assignment to "Required".

Note
Setting DHCP Addr. Assignment to "Required" is recommended to prevent guest users from attempting to use the guest network using a static IP configurations.

Step 13
Click Apply when finished.

Establishing the Guest WLAN Mobility Anchor(s)

Step 1
From the WLAN menu on the foreign WLC find the newly created guest WLAN.

Step 2
Highlight and click Mobility Anchors from the right-hand pull-down selection list. (See Figure 10-25.)

Figure 10-25 WLAN Mobility Anchor

Step 3
In the Switch IP Address (Anchor) pull-down selection list, select the IP address corresponding to the management interface of the anchor WLC deployed in the network DMZ. This is the same IP address configured in Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC.

Step 4
In the Priority field, select a priority number for the anchor WLC (applicable if there are more than one anchor WLCs configured).

Step 5
Click Mobility Anchor Create. (See Figure 10-27.)
Once configured, the screen shown in Figure 10-28 shows the mobility anchor (selected from above), assigned to the Guest WLAN.
For ease of verification, the page displays whether or not the mobility tunnel data path and CAPWAP control path have been established with the anchor. The pull-down selection list to the right offers the option to send a ping to the destination anchor WLC.

**Step 6**
When finished, click **Back**.

**Step 7**
Repeat the steps above for each additional anchor WLC being deployed (guest anchor redundancy).

This completes the guest WLAN configuration. Repeat all steps from Foreign WLC-Guest WLAN Configuration through Establishing the Guest WLAN Mobility Anchor(s) for each additional foreign WLC that will support the guest WLAN.

### Guest WLAN Configuration on the Anchor WLC

Guest WLAN configuration on the anchor controller(s) is identical to that of the foreign controller except for minor differences in the WLAN interface and mobility anchor configuration, which are detailed below.

**Note**
The SSID defined for the guest WLAN must be exactly the same as what is defined on the foreign WLCs.
Anchor WLC-Guest WLAN Interface

As indicated above, the parameters configured for the guest WLAN on the anchor WLC are the same except the interface to which the WLAN is mapped. In this case, the guest WLAN is assigned to an interface/VLAN on the anchor WLC, which connects to an interface on a firewall or Internet border router.

**Step 1** Click the WLANs tab.

**Step 2** Create, configure, and enable the guest WLAN the same way it was configured on the foreign WLC(s) except for the following:

In the WLANs general configuration, under Interface, choose the interface name created in Guest VLAN Interface Configuration. (See Figure 10-29.)

**Step 3** Click Apply.

![Anchor WLC Guest WLAN Interface Configuration](image)

Anchor WLC-Defining the Guest WLAN Mobility Anchor

The second parameter that differs in configuration from the foreign WLC is the WLAN mobility anchor configuration. The guest WLAN mobility anchor is the anchor WLC itself.

**Step 1** Click the WLANs tab.

**Step 2** Find the Guest WLAN and click Mobility Anchors.

**Step 3** From the pull-down selection list, choose the IP address representing the anchor controller. The IP address has (Local) next to it.

**Step 4** Click Mobility Anchor Create. (See Figure 10-30.)
Guest Access Configuration

Chapter 10  Cisco Unified Wireless Network Guest Access Services

Figure 10-30  Defining the Guest WLAN Mobility Anchor

<table>
<thead>
<tr>
<th>WLAN SSID</th>
<th>Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP Address (Anchor)</td>
<td>local</td>
</tr>
<tr>
<td>Data Path</td>
<td>up</td>
</tr>
<tr>
<td>Control Path</td>
<td>up</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
</tr>
</tbody>
</table>

Mobility Anchors

Note

The guest WLAN mobility anchor is local. (See Figure 10-31.)

Figure 10-31  Verifying Guest Mobility Anchor

Because the mobility anchor for the guest WLAN is the anchor WLC itself, the Data and Control Path status will always show “up”. If not, check to ensure that you have selected the local WLC as the anchor from the 'Switch IP Address (Anchor) drop down menu. Anchor controller will always have priority 0 for the ssid.
Step 5  If guest anchor redundancy is being implemented; repeat the WLAN configuration for each additional anchor WLC being deployed. Otherwise, this completes the configuration steps required to create the guest WLAN on the anchor WLC.

Guest Account Management

If guest credentials are going to be managed locally on the anchor controller, there are two methods by which they can be created and applied:

- Through a lobby ambassador admin or super user/root admin account.
- Directly on the controller via a local lobby admin account or other management account with read/write access.

Guest Management Using the Management System

The following configuration examples assume the management system version 2.2 or later has been installed and configured, and a lobby ambassador account has been created.

Note: Ensure that the individual WLC configurations are synchronized with the management system before creating guest templates.

Log in to the management system using the Lobby Ambassador credentials assigned by the system administrator. (See Figure 10-32.)

Figure 10-32 Lobby Ambassador

After logging in, the screen shown in Figure 10-33 appears.
Cisco Prime Infrastructure was formally known as WCS and NCS.

There are two types of guest templates:

- The **Add Guest User** template allows administrators to create and immediately apply guest credentials to one or more anchor WLCs.

- The **Schedule Guest User** template allows administrators to create guest credentials that are applied to one or more anchor WLCs at some future month, day, and time. (See Figure 10-34.)
Using the Add Guest User Template

**Step 1**  
From the pull-down selection list, select **Add Guest User** and click **Go**.

**Step 2**  
The template shown in Figure 10-35 appears.

*Figure 10-35  Add Guest User Template*

![Cisco Prime Infrastructure](File:91a.png)  
Guest Users > Create a Guest User Account

**Create a Guest User Account**

<table>
<thead>
<tr>
<th>General</th>
<th>Advanced</th>
</tr>
</thead>
</table>

> Please use "Import from file" option in the Advanced tab for bulk creation.

**Guest Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td><em>guest</em></td>
</tr>
<tr>
<td>Generate Password</td>
<td>[ ]</td>
</tr>
<tr>
<td>Password</td>
<td>*****</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>*****</td>
</tr>
<tr>
<td>Description</td>
<td>Wireless Network Guest Access</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network. [ ] Make this Disclaimer default</td>
</tr>
</tbody>
</table>

![Save Button](File:91c.png)  
![Cancel Button](File:91d.png)

*Figure 10-36 shows an example of guest user account creation.*
Step 3 Under **Guest Information**, enter a User Name and Password.

Passwords are case sensitive. User names are restricted to 24 characters or less. Administrators also have an option to allow the system to automatically generate a password by clicking on the **Generate Password** check box.

Step 4 Under **Account Configuration**, select the following:

- **Profile**—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
- **User Role**—They are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).
- **Life Time**—Select "limited" or "unlimited".
- **End Time**—If the guest account is "limited", select the month, day, and time the credentials are to expire.
- **Apply To**—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.
Note

As seen in Figure 10-36, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the management system mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

- **Description**—Enter a description. The description is displayed on the WLC to which the credentials are applied under Security > Local Net Users. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.
- **Disclaimer**—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network.

**Step 5**

Click **Save** when finished. The summary screen shown in Figure 10-37 appears, acknowledging that credentials have been applied to the anchor controller(s). The admin is also presented with an option to print or e-mail the credentials to the guest user.
Step 6  Click **Print/Email Guest User Credentials**. The screen shown in Figure 10-38 appears.
Guest Account Details

**Credentials for Guest User:guest**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest User Name</td>
<td>guest</td>
</tr>
<tr>
<td>Password</td>
<td>guest</td>
</tr>
<tr>
<td>Profile</td>
<td>ANY PROFILE</td>
</tr>
<tr>
<td>Start Time</td>
<td>Tue Sep 22 14:05:00 PDT 2015</td>
</tr>
<tr>
<td>End Time</td>
<td>Wed Sep 23 13:59:00 PDT 2015</td>
</tr>
</tbody>
</table>

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

Regards,

Admin Team.

---

**Note**

For details on setting up an SMTP mail server to support e-mailing guest account information to users, see the Prime Infrastructure Configuration Guide.

After printing and or e-mailing the account details, the screen shown in Figure 10-39 appears. By clicking the User Name, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting Delete Guest User from the pull-down selection list.
Figure 10-39  Cisco Prime Infrastructure Guest Users Summary

Note
If a user template is deleted from Cisco Prime Infrastructure while a user is active, they are de-authenticated.

Using the Schedule Guest User Template

For details about configuring guest accounts, see Prime Infrastructure Configuration Guide. Figure 10-40 shows the guest user template option.

Step 1
From the pull-down selection list, select Schedule Guest User and click Go.

The template shown in Figure 10-41 appears.
Figure 10-40 Guest User Template Option

Figure 10-41 Schedule Guest User Template
Figure 10-42 shows an example of a schedule guest user account creation.

**Figure 10-42  Schedule Guest User Account Creation**

![Schedule Guest User Account Creation](image)

**Step 2** Under Guest Information, enter a User Name. User names can be up to 24 characters long. When using the schedule-based template, administrators have the option to allow the system to automatically generate the user name for each new day that access is being offered. Also, when using this template, the system automatically generates the user password. There is no option to manually assign a password.

**Step 3** Under Account Configuration, select the following:

- **Profile**—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
- **User Role**—They are predefined by the administrator and are associated with the guests’ access (such as contractor, customer, partner, vendor, visitor, and so on).
- **Life Time**—Select "limited" or "unlimited".
- **Start Time**—Select the time, month, and day when the account is to become active.

**Note** The start time cannot begin within the current day that the account is being created. The start day must be one or more days beyond the day the account is being created.

- **End Time**—If the account is "limited", select the stop time, month, and day.

**Note** The stop day can be a period no longer than 30 days from the start day.

- **Days of Week**—Depending on the lifetime of the account, administrators have the ability to control for which days of the week access is available. Click the check boxes next to those days of the week access is permitted.
Chapter 10      Cisco Unified Wireless Network Guest Access Services

Guest Account Management

Note

If "Days of the Week" is selected, the start and stop times represent the period within each day that access is available. Upon expiry within a given day, Cisco Prime Infrastructure removes the credentials from the applicable controllers. For each new day/interval that access is permitted, Cisco Prime Infrastructure automatically generates a new password (and optionally a username), e-mails it to the guest user, and re-applies the new credentials to the applicable WLCs. If "Days of the Week" is not defined, access begins based on the start day and time and is continuously active until the end day and time.

- **Apply To**—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.

Note

As seen in Figure 10-42, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the management system mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

- **E-mail Credentials to**—Enter the e-mail address for whom an account is being established. This is a mandatory field.

Note

An SMTP mail server must be configured in Cisco Prime Infrastructure so that it can use to send guest account information. For details, see **Cisco Wireless System Configuration Guide**.

- **Description**—Enter a description. The description is displayed on the WLC to which the credentials are applied under **Security > Local Net Users**. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.

- **Disclaimer**—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network.

**Step 4**

Click **Save** when finished. The screen shown in Figure 10-43 appears, acknowledging that the scheduled account has been created. The admin is also presented with an option to print or e-mail the credentials to the guest user.
Step 5 Optionally, click **Print/Email Guest User Credentials**. The screen shown in Figure 10-44 appears.

**Figure 10-44 Print/E-mail Guest User Details**

**Guest Account Details**

**Credentials for Guest User: test2**

- **Guest User Name**: test2
- **Password**: PhWTjPtH
- **Profile**: ANY PROFILE
- **Start Time**: Thu Jul 23 08:00:00 PDT 2015
- **End Time**: Thu Jul 23 17:00:00 PDT 2015

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

Regards,
Admin Team.

After printing and/or e-mailing the account details, the summary screen shown in Figure 10-45 appears. By clicking the **User Name**, an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.
If a user template is deleted from Cisco Prime Infrastructure while a user is active, they are de-authenticated.

This completes the steps required to create a guest account using the lobby ambassador interface in Cisco Prime Infrastructure.

Managing Guest Credentials Directly on the Anchor Controller

The following procedure assumes that a network administrator has established a local management account with lobby admin privileges on one or more anchor controllers.

**Step 1**
Login to the anchor controller using the lobby admin credentials assigned by the system administrator. Remember that conduits might need to be opened through a firewall to permit HTTP/HTTPS for web administration of the controller. See Anchor Controller Positioning.

After login, the screen shown in Figure 10-46 appears.

**Step 2**
Click New.

The screen shown in Figure 10-47 appears.
To create user credentials, perform the following steps:

1. Enter a username and password (manual or auto).
2. Select the WLAN/SSID to which the guest account applies (only WLANs configured with an L3 web policy are displayed).
3. Enter a lifetime for the credentials.
4. Enter User Role if needed.
5. Enter a description for the user.

Click **Apply**.

The screen shown in Figure 10-48 appears and shows the newly-added guest user.
Guest Account Management

Figure 10-48  Anchor WLC Guest Users List

From this screen you have the option to do the following:

- Edit the existing user (link at far right; not visible).
- Delete the existing user (link at far right; not visible).
- Add a new user.

Configuring the Maximum Number of User Accounts

The default number of guest user accounts that can be defined on the controller is 2048. This value can be changed by completing the following steps.

Step 1  Click the Security tab. (See Figure 10-49.)

Figure 10-49  Configuring the Maximum Number of User Accounts

<table>
<thead>
<tr>
<th>User Name</th>
<th>WLAN SSID</th>
<th>Account Remaining Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1</td>
<td>Guest</td>
<td>1 d</td>
<td>Guest Access WLAN</td>
</tr>
</tbody>
</table>

Step 2  In the left pane, click General under AAA properties.
Step 3  Configure the maximum number of user database entries (maximum 2048).
Step 4  Click Apply.
Maximum Concurrent User Logins

The maximum number of concurrent logins for a local user account on the WLC can be configured. Values include 0 for unlimited concurrent logins or can be limited from 1 to 8. The maximum user logins is configured by completing the following steps:

Step 1  Click the Security tab. (See Figure 10-50.)

Figure 10-50  User Login Policies

Step 2  In the left pane, click User Login Policies under AAA.

Step 3  Configure the maximum number of concurrent user logins (between 0-8).

Step 4  Click Apply.

Guest User Management Caveats

Note the following caveats:

- Guest accounts can be added using either method above or both methods together.
- When using Cisco Prime Infrastructure, the lobby admin may not have visibility of user accounts that might have been created locally on the anchor controller if the controller configuration has not been recently synchronized with Cisco Prime Infrastructure. If this is the case and a Cisco Prime Infrastructure lobby admin attempts to add an account with a user name that is already configured on the WLC, the Cisco Prime Infrastructure configuration overrides the local configuration.
- When adding user accounts locally on the controller, the local admin will have visibility of all accounts that have been created, including those that were created via Cisco Prime Infrastructure.
- If a guest user is currently authenticated to a WLAN and their credentials are deleted from Cisco Prime Infrastructure or locally on the controller, the user traffic stops flowing, and the user is de-authenticated.
Other Features and Solution Options

Web Portal Page Configuration and Management

The internal web server and associated functionality is hosted locally on the anchor controller. When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default. No further configuration is required. The internal portal includes a few optional configuration parameters.

Internal Web Page Management

Step 1  Click the Security tab.
Step 2  In the left pane, click Web Auth and then Web Login Page.

The configuration screen shown Figure 10-51 is displayed. You can change the heading and message information that appears on the portal page. You can also choose a post-authentication redirect URL.

Figure 10-51  Web Login Page Configuration Screen

Step 3  Click Apply.
Step 4  Optionally, click Preview to view what the user sees when redirected.
Importing a Web Page

You can download a customized web page and store it locally on the anchor controller. To import a customized web page, perform the following steps.

**Step 1**  Click the **Commands** tab. (See Figure 10-52.)

**Figure 10-52  Importing a Web Page**

![Figure 10-52 Importing a Web Page](image)

**Step 2**  Under File Type, select **Web Auth Bundle**.

**Step 3**  Define the IP address and file path on the TFTP server where the files reside.

**Step 4**  Click **Download** to begin.

Be aware of these caveats when downloading a web auth bundle:

- Select **Web Auth Bundle** from the pull-down selection list to ensure that the files are stored in the correct directory on the controller.
- The **Web Auth Bundle** must be a .tar file of the HTML and image files associated with the custom web login page. When downloaded, the WLC un-tars the files and places them in the appropriate directory.
- The **Web Auth Bundle** (.tar file) cannot be larger than 1 MB.
- The file name for the HTML login page must be **login.html**.

For more information about downloading and using customized web pages, see **Cisco Wireless Controller Configuration Guide**.

Selecting an Imported Web Auth Page

To use a customized web auth page that has been downloaded to the controller, perform the following steps:
Step 1  Click the Security tab.
Step 2  In the left pane, click Web Auth and then Web Login Page.
Step 3  From the Web Authentication Type pull-down selection list, select Customized (Downloaded).
Step 4  Click Preview to view the downloaded page.
Step 5  Click Apply when finished. (See Figure 10-53.)

**Figure 10-53  Selecting an Imported Web Auth Page**

---

Internal Web Certificate Management

The web auth login page uses SSL for safeguarding user credentials. For simplicity, the controller uses a self-signed certificate. Because the certificate is self-signed, guest users can expect to see a pop-up alert similar to the following when they are redirected to the authentication page shown in Figure 10-54.
At this point, you can proceed by either clicking Yes or you can select View Certificate and manually install it as a trusted site. The web server uses the virtual interface IP address configured in Anchor WLC Installation and Interface Configuration, as its source address. If a hostname is defined along with the IP address, that host name must be resolvable by DNS so that:

- The client is redirected to the web auth page.
- The user does not encounter a web certificate error because of conflicts between hostname and host IP address.

**Importing an External Web Certificate**

For cases where a legitimate web certificate issued by a trusted root CA is required, one can be downloaded to the controller by performing the following steps:

**Step 1**

Click the Security tab.

In the left pane, click Web Auth and then Certificate. (See Figure 10-55.)
**Figure 10-55  Importing an External Web Certificate**

**Step 2**  Place a check mark in the **Download SSL Certificate** check box.

**Step 3**  Complete the required fields for downloading the certificate.

**Step 4**  Click **Apply**.

**Step 5**  After the certificate has been downloaded, reboot the server.

---

**Support for External Web Redirection**

In some cases, an enterprise might already have deployed a web-portal system to support wired guest access or NAC functionality. If this is the case, the anchor controller can be configured to redirect wireless guest users to an external web portal using the following steps:

**Step 1**  Click the **Security** tab.

**Step 2**  In the left pane, click **Web Auth** and then **Web Login Page**. (See Figure 10-56.)
Step 3 Fill in the redirect URL after login and external webauth URL fields.

Step 4 Click Apply.

Anchor WLC-Pre-Authentication ACL

A pre-authentication ACL (pre-auth ACL) can be applied to the guest WLAN, which allows unauthenticated clients to connect to specific hosts or URL destinations prior to authenticating. The pre-auth ACL is applied under the guest WLAN Layer 3 Security settings and, if enabled, is performed only on the anchor WLC(s). (See Figure 10-57.)
The specific ACL is configured under Security > Access Control Lists (See Figure 10-58 and Figure 10-59.)

Note

If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client is unable to resolve and connect to a destination host/URL that is otherwise allowed by the ACL.
External Radius Authentication

As described in Guest User Authentication, an external RADIUS server can be used to authenticate guest users in place of creating and storing guest credentials locally on the anchor controller. If this method is used, the lobby admin features described in Guest Account Management cannot be used. It is assumed that some other guest management system will be used in conjunction with the external RADIUS server.

To configure a guest WLAN to use an external RADIUS server, perform the following configuration steps on the anchor controller.

Adding a RADIUS Server

Step 1  Click the Security tab.

A summary screen is displayed. (See Figure 10-60.)
Figure 10-60  Summary Screen

![Figure 10-60  Summary Screen](image)

**RADIUS Authentication Servers**

Auth Called Station ID Type: AP MAC Address: SSID

Use AES Key Wrap: □

MAC Delimiter: Hyphen

Framed MTU: 1300

<table>
<thead>
<tr>
<th>Network User</th>
<th>Management</th>
<th>Tunnel Proxy</th>
<th>Server Index</th>
<th>Server Address(IPv4/IPv6)</th>
<th>Port</th>
<th>IPSec</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>172.20.227.110</td>
<td>1812</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>172.20.227.113</td>
<td>1812</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Step 2**

Click **New**.

The screen shown in Figure 10-61 appears.

![Figure 10-61  Defining RADIUS Server Settings](image)

**RADIUS Authentication Servers -> New**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.20.30.17</td>
<td>ASCII</td>
<td>************</td>
<td></td>
</tr>
</tbody>
</table>

Key Wrap: □

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User Management: Enable

Management: Enable

Management Retransmit Timeout: 2 seconds

Tunnel Proxy IPSec: Enable

IPSec: Enable

**Step 3**

To define RADIUS server settings, configure the IP address, shared secret, and authentication port number as defined on the RADIUS server.
If the Network User check box is cleared, the RADIUS server is used only for user authentication when it is specifically selected under the RADIUS setting of a given WLAN. Otherwise, if the Network User check box is checked, the server is used globally for all user authentications based on its server priority.

**Step 4**  
Click **Apply**.

The summary screen shown in **Figure 10-62** shows the newly-added server.

**Figure 10-62  Summary Screen**

![Summary Screen](image1)

**Step 5**  
To select a RADIUS server, click the **WLANs** tab.

The screen shown in **Figure 10-63** appears.

**Figure 10-63  WLANs Tab**

![WLANs Tab](image2)

**Step 6**  
Find the guest WLAN and click on its **Profile Name**.

The guest WLAN configuration screen is displayed, as shown in **Figure 10-64**.
Step 7  Select AAA Servers under the WLAN Security tab.

Step 8  Select the RADIUS server to be used for web authentication from the pull-down selection list under Authentication Servers.

Verifying Guest Access Functionality

The guest access service is working correctly if a user:

- Can associate to the guest WLAN.
- Receives an IP address via DHCP.
- Opens their browser and is redirected to the web authentication page.
- Enters their credentials and connects to the Internet (or other authorized upstream services).