CHAPTER 7

Managing WCS User Accounts

This chapter describes how to configure global e-mail parameters and manage Cisco WCS user accounts. It contains these sections:

Adding WCS User Accounts

This section describes how to configure a WCS user. The accounting portion of the AAA framework is not implemented at this time. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. WCS supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

The username and password supplied by you at install time are always authenticated, but the steps you take here create additional superusers. If the password is lost or forgotten, the user must run a utility to reset the password to another user-defined password.

Follow these steps to add a new user account to WCS.

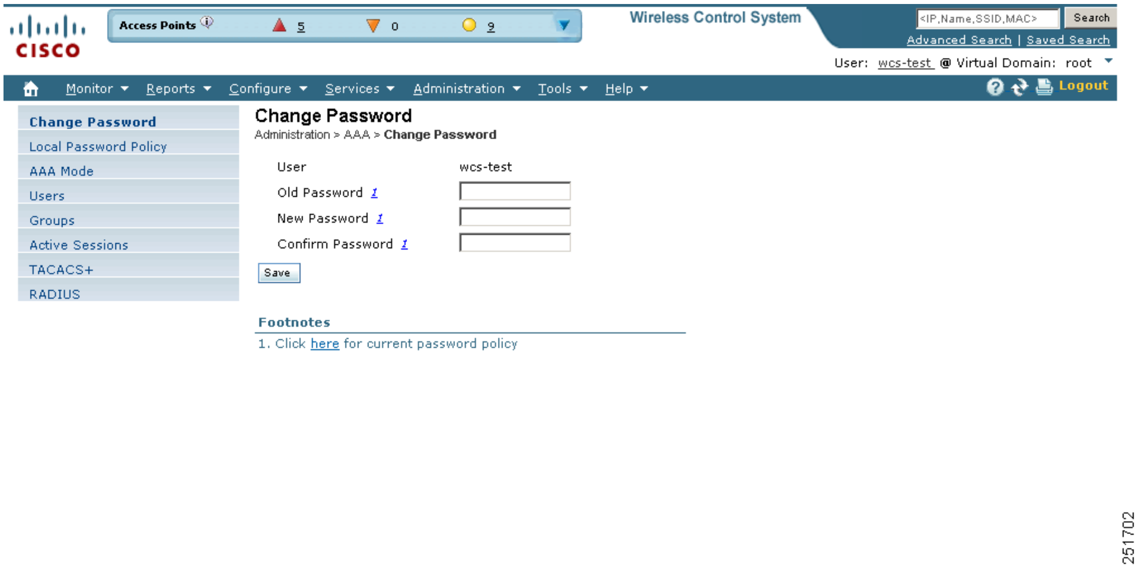
Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as *Super1*.

Note Cisco recommends that you create a new superuser assigned to the SuperUsers group and delete Super1 to prevent unauthorized access to the system.

Step 3 Click **Administration > AAA** and the Change Password page appears (see Figure 7-1).

Figure 7-1   Change Password Page



Change Password

Administration > AAA > **Change Password**

User	wcs-test
Old Password [1]	
New Password [1]	
Confirm Password [1]	

Footnotes

1. Click here for current password policy

Step 4 In the Old Password text box, enter the current password that you want to change.

Step 5 Enter the username and password for the new WCS user account. You must enter the password twice.

Note These entries are case sensitive.

Step 6 Click **Groups** from the left sidebar menu. The All Groups page displays the following group names (see Figure 7-2).

Note Some usergroups cannot be combined with other usergroups. For instance, you cannot choose both lobby ambassador and monitor lite.

- System Monitoring—Allows users to monitor WCS operations.
- ConfigManagers—Allows users to monitor and configure WCS operations.
- Admin—Allows users to monitor and configure WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.

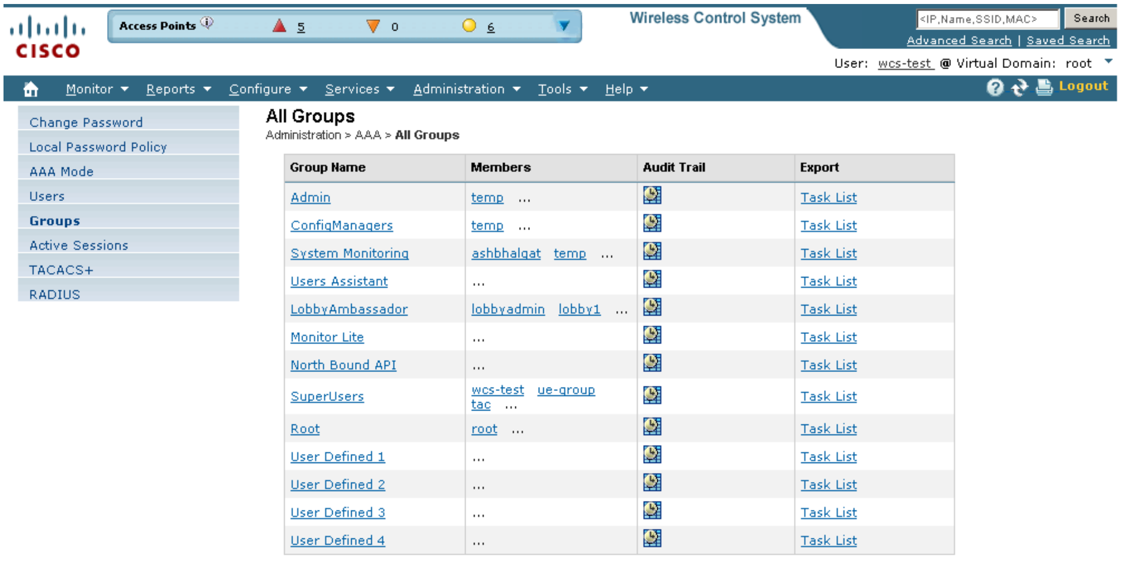
  Note If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.

- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superusers tasks can be changed.
- North bound API—A user group used only with WCS Navigator.
- Users Assistant—Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller path to configure these local net features.

Note If you create a user assistant user, login as that user, and choose Monitor > Controller, you receive a permission denied message as expected behavior.

- Lobby Ambassador—Allows guest access for only configuration and managing of user accounts.
- Monitor lite—Allows monitoring of assets location.
- Root—Allows users to monitor and configure WCS operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

Figure 7-2 All Groups Page



All Groups

Administration > AAA > All Groups

Group Name	Members	Audit Trail	Export
Admin	temp ...	▣	Task List
ConfigManagers	temp ...	▣	Task List
System Monitoring	ashbhalgat temp ...	▣	Task List
Users Assistant	...	▣	Task List
LobbyAmbassador	lobbyadmin lobby1 ...	▣	Task List
Monitor Lite	...	▣	Task List
North Bound API	...	▣	Task List
SuperUsers	wcs-test ue-group tac ...	▣	Task List
Root	root ...	▣	Task List
User Defined 1	...	▣	Task List
User Defined 2	...	▣	Task List
User Defined 3	...	▣	Task List
User Defined 4	...	▣	Task List

Step 7 Click the name of the user group to which you assigned the new user account. The Group Detail > *User Group* page shows a list of this group's permitted operations.

From this page you can also show an audit trail of login and logout patterns or export a task list.

Step 8 Make any desired changes by checking or unchecking the appropriate check boxes for task permissions and members.

Note Any changes you make will affect all members of this user group.

Note To view complete details on the Monitor > Client details screen and to perform operations such as Radio Measurement, users in User Defined groups need permission for Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location.

Step 9 Click **Submit** to save your changes or **Cancel** to leave the settings unchanged.

Deleting WCS User Accounts

Follow these steps to delete a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > AAA**.

Step 4 Click **Users** from the left sidebar menu to display the Users page.

Step 5 Select the check box to the left of the user account(s) to be deleted.

Step 6 From the Select a command drop-down list, choose **Delete User(s)**, and click **Go**.

When prompted, click **OK** to confirm your decision. The user account is deleted and can no longer be used.

Changing Passwords

Follow these steps to change the password for a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-16.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration > AAA** to display the Change Password page.

Step 4 Enter your old password, unless you are the root user. (A root user can change any password without entering the old password.)

Step 5 Enter the new password in both the New Password and Confirm New Password text boxes.

Step 6 Click **Save** to save your changes. The password for this user account has been changed and can be used immediately.

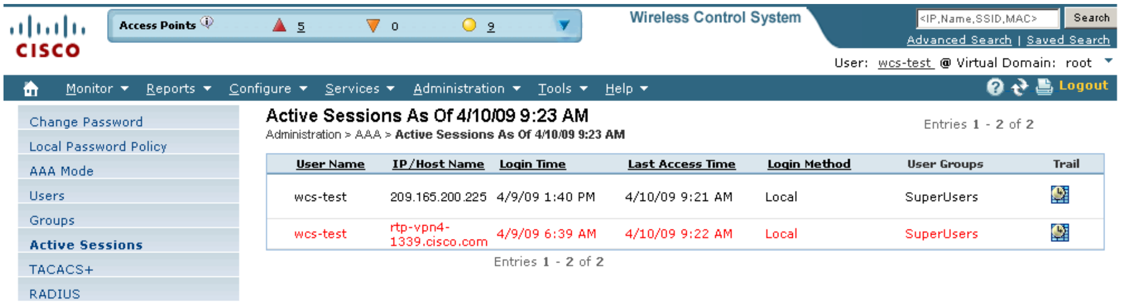
Monitoring Active Sessions

Follow the steps below to view a list of active users.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Active Sessions**. The Active Sessions page appears (see Figure 7-3).

Figure 7-3 Active Sessions Page



Active Sessions As Of 4/10/09 9:23 AM

Administration > AAA > Active Sessions As Of 4/10/09 9:23 AM

Entries 1 - 2 of 2

User Name	IP/Host Name	Login Time	Last Access Time	Login Method	User Groups	Trail
wcs-test	209.165.200.225	4/9/09 1:40 PM	4/10/09 9:21 AM	Local	SuperUsers	
wcs-test	rtp-vpn4-1339.cisco.com	4/9/09 6:39 AM	4/10/09 9:22 AM	Local	SuperUsers	

Entries 1 - 2 of 2

251704

The user highlighted in red represents your current login. If a column heading is a hyperlink, click the heading to sort the list of active sessions in descending or ascending order along that column. The sort direction is toggled each time the hyperlink is clicked.

The Active Sessions page has the following columns:

- IP/Host Name: The IP address or the hostname of the machine on which the browser is running. If the hostname of the user machine is not in DNS, the IP address is displayed.
- Login Time: The time at which the user logged in to WCS. All times are based on the WCS server machine time.
- Last Access Time: The time at which the user's browser accessed WCS. All times are based on the WCS server machine time.

Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status panel. However, if a user navigates to a non-WCS Navigator web page in the same browser, the disparity in time is greater upon returning to WCS Navigator. This disparity results because alarm counts are not updated while the browser is visiting non-WCS Navigator web pages.

- Login Method:
  - Web Service: Internal session needed by Navigator to manage WCS.
  - Regular: Sessions created for users who log into WCS directly through a browser.
  - Navigator Redirect: Sessions created for Navigator uses who are redirected to WCS from Navigator.
- User Groups: The list of groups to which the user belongs. (North bound API is a user group used only with WCS Navigator.)
- Audit trail icon: Link to page that displays the audit trail (previous login times) for that user.

Viewing or Editing User Information

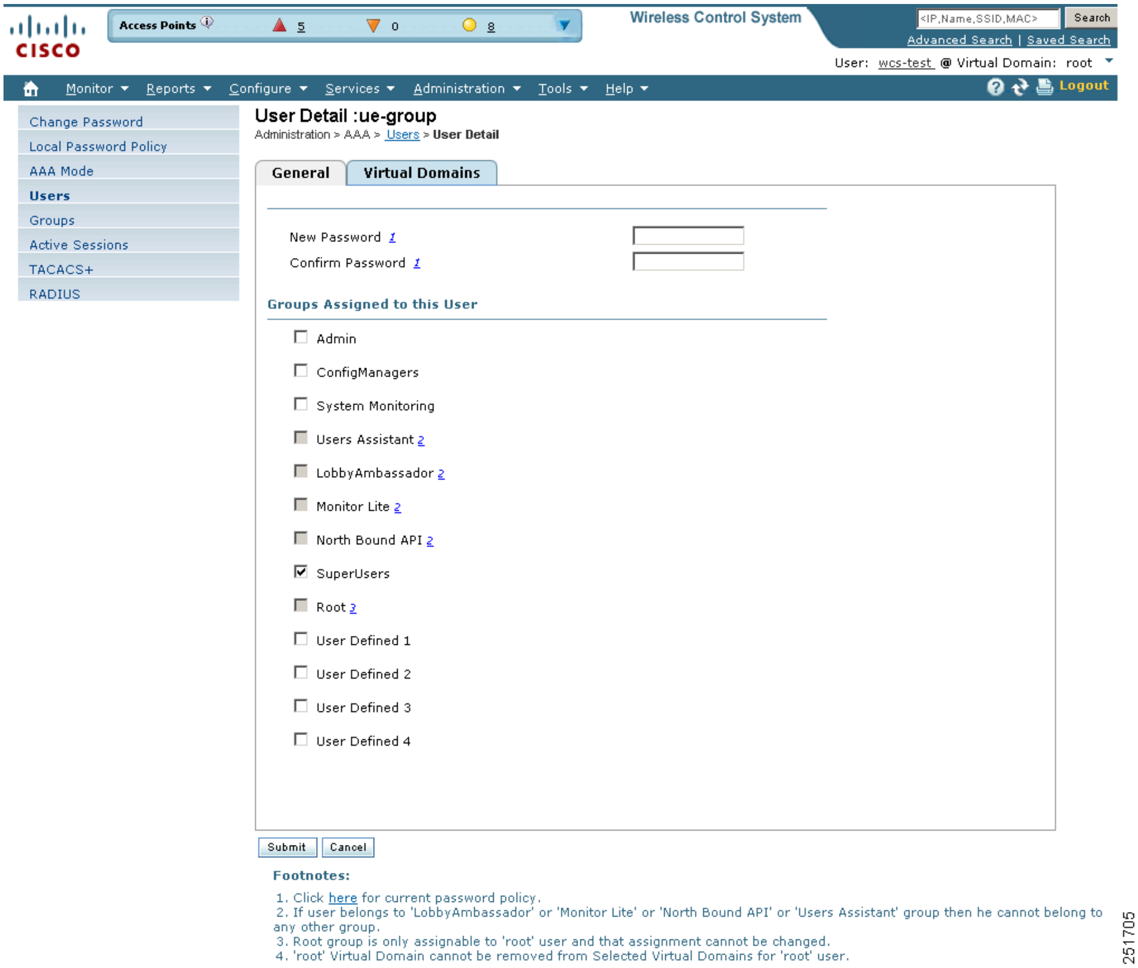
Follow these steps to see the group the user is assigned to or to adjust a password or group assignment for that user.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click in the User Name column. The User Detail : *User Group* page appears (see Figure 7-4).

Figure 7-4 Detailed Users Page



User Detail :ue-group

Administration > AAA > Users > **User Detail**

New Password 1

Confirm Password 1

Groups Assigned to this User

☐ Admin

☐ ConfigManagers

☐ System Monitoring

☐ Users Assistant 2

☐ LobbyAmbassador 2

☐ Monitor Lite 2

☐ North Bound API 2

☑ SuperUsers

☐ Root 3

☐ User Defined 1

☐ User Defined 2

☐ User Defined 3

☐ User Defined 4

Footnotes:

1. Click here for current password policy.
2. If user belongs to 'LobbyAmbassador' or 'Monitor Lite' or 'North Bound API' or 'Users Assistant' group then he cannot belong to any other group.
3. Root group is only assignable to 'root' user and that assignment cannot be changed.
4. 'root' Virtual Domain cannot be removed from Selected Virtual Domains for 'root' user.

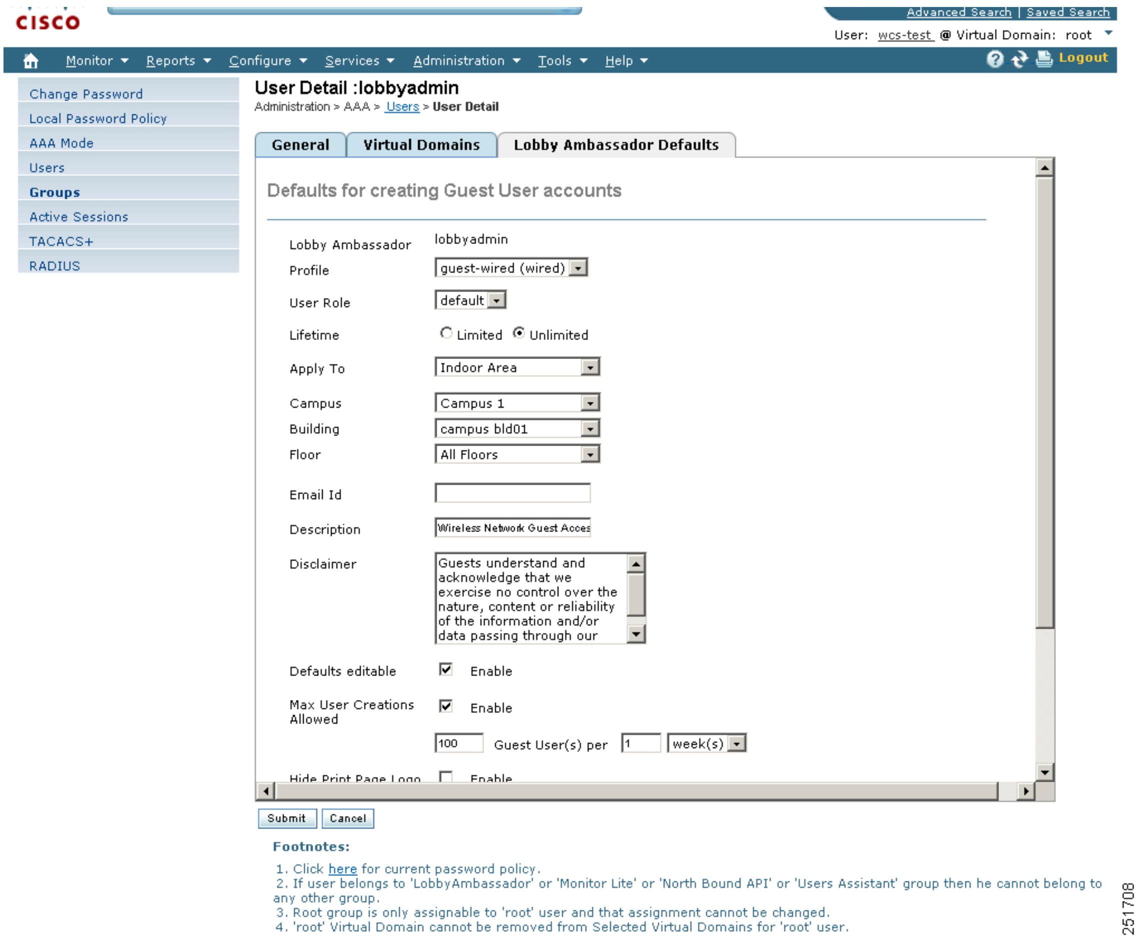
You can see which group is assigned to this user or change a password or group assignment.

Setting the Lobby Ambassador Defaults

If you choose a Lobby Ambassador from the User Name column, a Lobby Ambassador Defaults tab appears (see Figure 7-5). All of the guest user accounts created by the lobby ambassador have these credentials by default. If the default values are not specified, the lobby ambassador must provide the required guest user credential fields.

Note If no default profile is chosen on this tab, the defaults do not get applied to this lobby ambassador. The lobby ambassador account does get created, and you can create users with any credentials you choose.

Figure 7-5 Lobby Ambassador Default Tab



User Detail :lobbyadmin

Administration > AAA > Users > **User Detail**

Defaults for creating Guest User accounts

Lobby Ambassador	lobbyadmin
Profile	guest-wired (wired)
User Role	default
Lifetime	○ Limited ● Unlimited
Apply To	Indoor Area
Campus	Campus 1
Building	campus bld01
Floor	All Floors
Email Id	
Description	Wireless Network Guest Acces
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our
Defaults editable	☑ Enable
Max User Creations Allowed	☑ Enable
	100 Guest User(s) per 1 week(s)
Hide Print Page Logo	☐ Enable

Footnotes:

1. Click here for current password policy.
2. If user belongs to 'LobbyAmbassador' or 'Monitor Lite' or 'North Bound API' or 'Users Assistant' group then he cannot belong to any other group.
3. Root group is only assignable to 'root' user and that assignment cannot be changed.
4. 'root' Virtual Domain cannot be removed from Selected Virtual Domains for 'root' user.

Step 4 Use the Profile drop-down list to choose the guest user to connect to.

Wired-guest is an example of a profile that might be defined to indicate traffic that is originating from wired LAN ports. See the "Configuring Wired Guest Access" section on page 10-50.

Step 5 Choose a user role to manage the amount of bandwidth allocated to specific users within the network. They are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).

Step 6 Choose **Limited** or **Unlimited** at the Lifetime parameter.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When *unlimited* is chosen, no expiration date for the guest account exists.

Step 7 Use the Apply to drop-down list to choose from the following options. What you choose determines what additional parameters appear.

- Indoor area—A campus, building, or floor.
- Outdoor area—A campus or outdoor area.
- Controller list—A list of controller(s) with the selected profile created.
- Config Group—Those config group names configured on WCS.

Step 8 Enter the e-mail ID of the host to whom the guest account credentials are sent.

Step 9 Provide a brief description of the account.

Step 10 If you want to supply disclaimer text, enter it.

a. Select the **Defaults Editable** check box if you want to allow the lobby ambassador to override these configured defaults. This allows the Lobby Ambassadors to modify Guest User default settings while creating guest account from the Lobby Ambassador portal.

Note If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created, and the Lobby Ambassador can create users with credentials as desired.

Step 11 Select the **Max User Creations Allowed** check box to set limits on the number of guest users that can be created by the lobby ambassador in a given time period. The time period is defined in hours, days, or weeks.

Step 12 Click the **Preview Current Logo** link to see what is currently being used as a logo, and then you can click to enable it or browse to another location to update the logo.

Step 13 If you want additional page header text, you can enter it at the Print Page Header Text parameter.

Step 14 Click **Submit**.

Viewing or Editing Group Information

Follow these steps to see specific tasks the user is permitted to do within the defined group or make changes to the tasks.

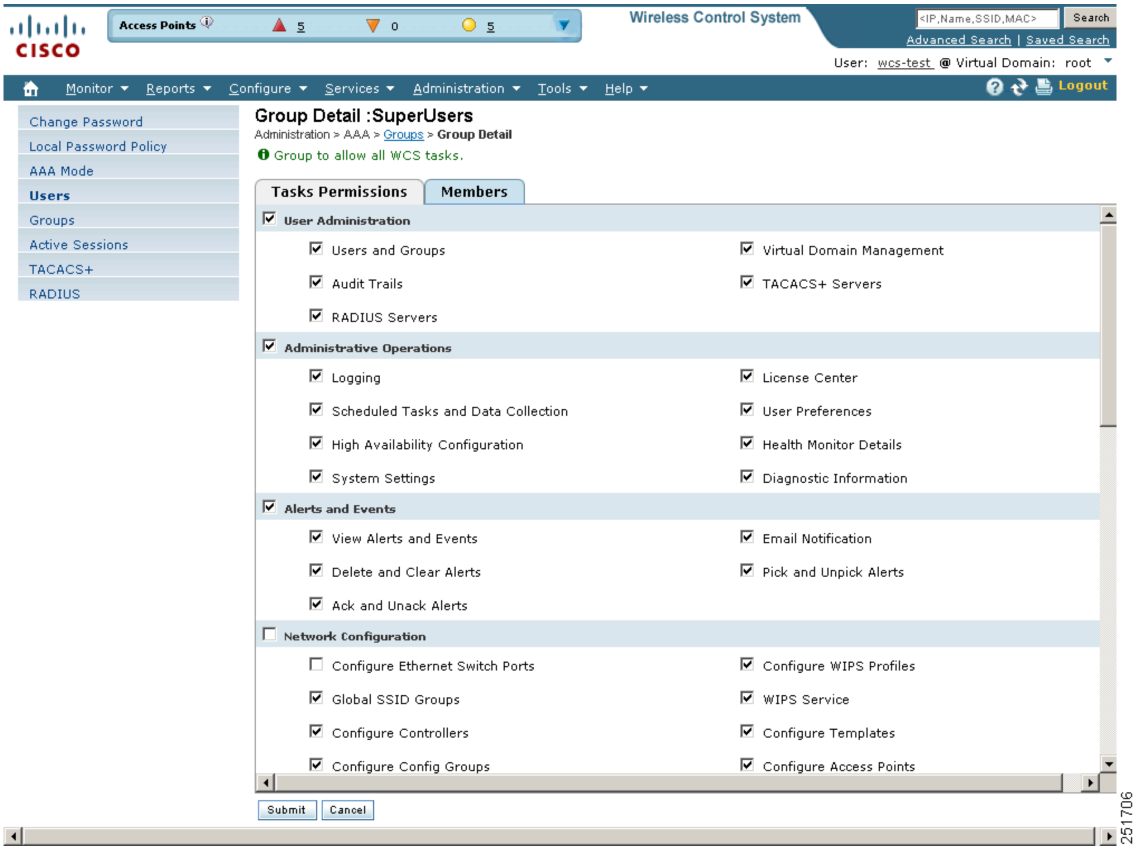
Step 1 Choose **Administration > AAA**.

Step 2 Choose **Users** from the left sidebar menu.

Step 3 Click in the **Member Of** column. The Group Detail: *User Group* page appears (see Figure 7-6).

Note The detailed page varies based on what group you choose. Figure 7-6 shows the detailed page of the superuser.

Figure 7-6 Detailed Group Page



Group Detail :SuperUsers

Administration > AAA > Groups > Group Detail

Group to allow all WCS tasks.

☑ User Administration

- ☑ Users and Groups
- ☑ Virtual Domain Management
- ☑ Audit Trails
- ☑ TACACS+ Servers
- ☑ RADIUS Servers

☑ Administrative Operations

- ☑ Logging
- ☑ License Center
- ☑ Scheduled Tasks and Data Collection
- ☑ User Preferences
- ☑ High Availability Configuration
- ☑ Health Monitor Details
- ☑ System Settings
- ☑ Diagnostic Information

☑ Alerts and Events

- ☑ View Alerts and Events
- ☑ Email Notification
- ☑ Delete and Clear Alerts
- ☑ Pick and Unpick Alerts
- ☑ Ack and Unack Alerts

□ Network Configuration

- □ Configure Ethernet Switch Ports
- ☑ Configure WIPS Profiles
- ☑ Global SSID Groups
- ☑ WIPS Service
- ☑ Configure Controllers
- ☑ Configure Templates
- ☑ Configure Config Groups
- ☑ Configure Access Points

You can see the specific tasks the user is permitted to do within the defined group or make changes to the tasks.

Editing the Guest User Credentials

Click the WCS user name of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

Note While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Viewing the Audit Trail

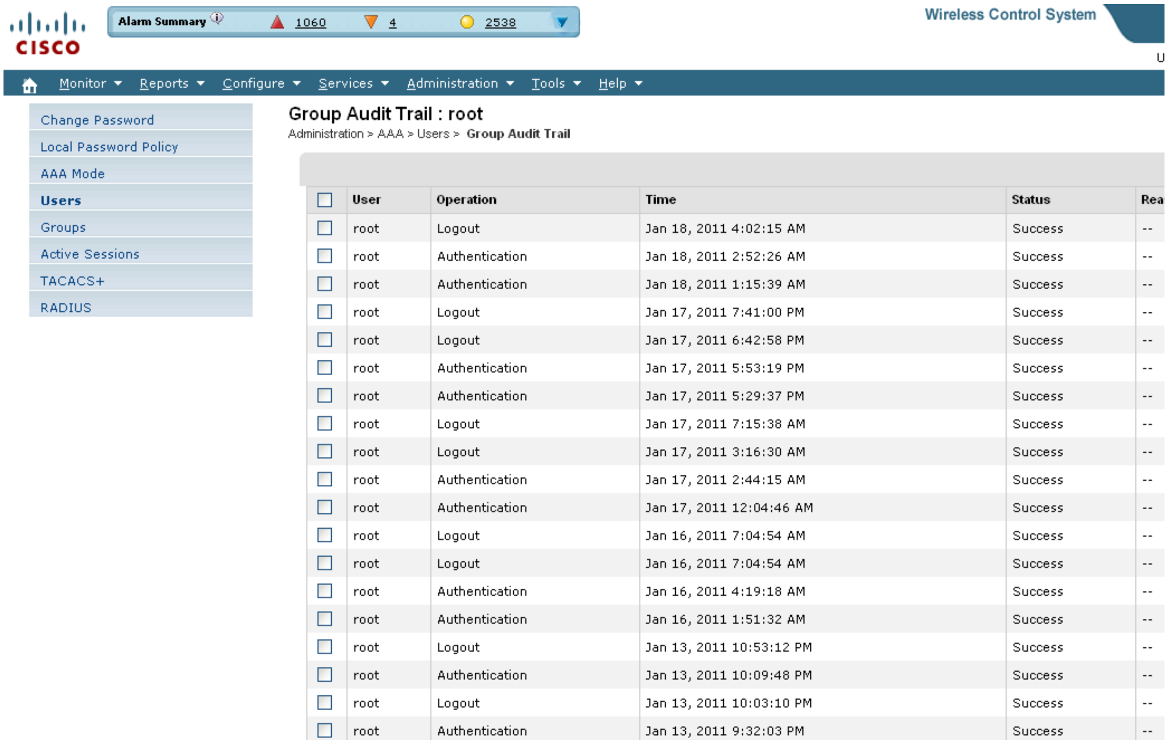
Click the **Audit Trail** icon in the Users page to view a log of authentication attempts. The Audit Trail page appears (see Figure 7-7).

This page enables you to view the following data:

- User: User login name

- Operation: Type of operation audited
- Time: Time operation was audited
- Status: Success or failure

Figure 7-7 Audit Trail



Group Audit Trail : root

Administration > AAA > Users > Group Audit Trail

□	User	Operation	Time	Status	Rea
□	root	Logout	Jan 18, 2011 4:02:15 AM	Success	--
□	root	Authentication	Jan 18, 2011 2:52:26 AM	Success	--
□	root	Authentication	Jan 18, 2011 1:15:39 AM	Success	--
□	root	Logout	Jan 17, 2011 7:41:00 PM	Success	--
□	root	Logout	Jan 17, 2011 6:42:58 PM	Success	--
□	root	Authentication	Jan 17, 2011 5:53:19 PM	Success	--
□	root	Authentication	Jan 17, 2011 5:29:37 PM	Success	--
□	root	Logout	Jan 17, 2011 7:15:38 AM	Success	--
□	root	Logout	Jan 17, 2011 3:16:30 AM	Success	--
□	root	Authentication	Jan 17, 2011 2:44:15 AM	Success	--
□	root	Authentication	Jan 17, 2011 12:04:46 AM	Success	--
□	root	Logout	Jan 16, 2011 7:04:54 AM	Success	--
□	root	Logout	Jan 16, 2011 7:04:54 AM	Success	--
□	root	Authentication	Jan 16, 2011 4:19:18 AM	Success	--
□	root	Authentication	Jan 16, 2011 1:51:32 AM	Success	--
□	root	Logout	Jan 13, 2011 10:53:12 PM	Success	--
□	root	Authentication	Jan 13, 2011 10:09:48 PM	Success	--
□	root	Logout	Jan 13, 2011 10:03:10 PM	Success	--
□	root	Authentication	Jan 13, 2011 9:32:03 PM	Success	--

Creating Guest User Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in WCS. A guest network provided by an enterprise allows access to the internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. 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 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.

The network administrator must first set up a lobby ambassador account. Guest user accounts are for visitors, temporary workers, and so on. who need network access. A lobby ambassador account has limited configuration privileges and only allows access to the screens used to configure and manage guest user accounts.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

This section describes how to perform the following procedures:

- Logging in to the WCS User Interface as a Lobby Ambassador, page 7-11
- Managing WCS Guest User Accounts, page 7-12

Follow these steps to create guest user accounts in WCS.

Note You should have SuperUser privilege (by default) to create a lobby ambassador account and not administration privileges. Multiple lobby ambassador accounts can be created by the administrator with varying profiles and permissions.

Note A root group, which is created during installation, has only one assigned user, and no additional users can be assigned after installation. This root user cannot be changed. Also, unlike a super user, no task changes are allowed.

Step 1 Log into the WCS user interface as an administrator.

Step 2 Click **Administration > AAA**.

Step 3 From the left sidebar menu, choose **Users**.

Step 4 From the Select a Command drop-down list, choose **Add User**, and click **Go**. The Users page appears.

Step 5 Enter the username.

Step 6 Enter the password. The minimum is six characters. Reenter and confirm the password.

Note The password must include at least three of the following four types of elements: lowercase letters, uppercase letters, numbers, and special characters.

Step 7 In the *Groups Assigned to this User* section, select the **LobbyAmbassador** check box to access the **Lobby Ambassador Defaults** tab.

Step 8 Follow the steps in the "Setting the Lobby Ambassador Defaults" section on page 7-7.

Logging in to the WCS User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in WCS. You can then configure guest user accounts (through templates).

Follow these steps to log into the WCS user interface through a web browser.

Step 1 Launch Internet Explorer 7.0 or later on your computer.

Note Some WCS features may not function properly if you use a web browser other than Internet Explorer 7.0 or later on a Windows workstation.

Step 2 In the browser's address line, enter **https://*wcs-ip-address*** *(such as* https://1.1.1.1/login.html), where *wcs-ip-address* is the IP address of the computer on which WCS is installed. Your administrator can provide this IP address.

Step 3 When the WCS user interface displays the Login page, enter your username and password.

Note All entries are case sensitive.

Note The lobby ambassador can only define guest users templates.

Step 4 Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The Guest Users page is displayed. This page provides a summary of all created Guest Users.

To exit the WCS user interface, close the browser page or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

Note When a system administrator stops the WCS server during a WCS session, the session ends, and the web browser displays this message: "The page cannot be displayed." Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

Managing WCS Guest User Accounts

WCS guest user accounts are managed with the use of templates. This section describes how to manage WCS guest user accounts. It includes the following:

- Adding WCS Guest User Accounts, page 7-12
- Scheduling WCS Guest User Accounts, page 7-14
- Printing or E-mailing WCS Guest User Details, page 7-15
- Saving Guest Accounts on a Device, page 7-16

Adding WCS Guest User Accounts

Templates are used to create guest user accounts in WCS. For information about how to configure guest user templates, see "Configuring Guest User Templates" section on page 12-54. After the template is created, it is applied to all controllers that the guest users can access. Follow these steps to add a new guest user account to WCS:

Step 1 Log into the WCS user interface as lobby ambassador to open the Guest user window.

Step 2 From the Select a command drop-down menu, choose **Add Guest User**.

Step 3 Click **GO. Th**e ***Guest User* > New User** window has two tabs: General and Advanced. The lobby ambassador can either manually enter the username and password for an individual or can import a file with user names and passwords defined for multiple users by selecting the Generate Password option.

- If the username and password are entered manually, the password is entered twice for confirmation.
- If the Generate Password option is chosen, the Import From File option should be selected on the Advanced tab. The following fields can be imported for a guest user: username, password, lifetime setting, description, and disclaimer. Format for the fields in the CSV file is noted at the bottom of the Advanced panel.
- If the Import From File check box is checked, no username and password fields appear on the General tab.

Note Passwords are case sensitive and must be a minimum of 8 characters. The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, and special characters. Reenter and confirm the password.

Step 4 At the Advanced tab, check the **Import From File** option to upload the following information for multiple guest users: username, password, lifetime setting, description, and disclaimer.

Format for the fields in the CSV file is noted at the bottom of the Advanced panel.

Step 5 If Import From file is selected, browse to or enter the file name from which to upload the file.

Step 6 Choose a Profile from the drop-down menu.

The selectable profiles are predefined by a system administrator and define the length of time, user role (allocated bandwidth), and areas of the network (indoor, outdoor, controllers, and config groups) to which a guest user has access. Your administrator can advise which profile to use.

Step 7 Choose a user role from the drop-down menu. (This option is not seen if the Import From File check box is selected.)

Step 8 Choose the lifetime of the guest user account. The options are limited or unlimited. (This option is not seen if the Import From File check box is selected.)

- Limited—From the drop-down menus, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
- Unlimited—This user account never expires.

Step 9 Click **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can also restrict the guest user (wired or wireless) to a specific listed controller or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the Apply To drop-down menu, choose one of the following:

- Controller List: Check the check box for the controller(s) to which the guest user account applies. Only those controllers configured for guest access (wired or wireless) display.
- Indoor Area: Choose the applicable campus, building, and floor.
- Outdoor Area: Choose the applicable campus and outdoor area.
- Config Group: Choose the config group to which the guest user account applies.

Step 10 Review and modify, if necessary, the description field. (This option is not seen if the Import From File check box was selected.)

Step 11 Review and modify, if necessary, the disclaimer information. Use the scroll bar to move up and down. (This option is not seen if the Import From File check box was selected.)

Step 12 Click the **Make this Disclaimer Default** to use the disclaimer text as the default for all guest user accounts. Click the check box if you want to set new default disclaimer text for all future guest user accounts. (This option is not seen if the Import From File check box was selected.)

Step 13 Click **Save** to save your changes or **Cancel** to leave the settings unchanged.

Scheduling WCS Guest User Accounts

A lobby ambassador is able to schedule automatic creation of a guest user account. The validity and recurrence of the account can be defined. The generation of a new password on every schedule is optional and is enabled using a check box. For scheduled users, the password is automatically generated and is automatically sent by e-mail to the host of the guest. The e-mail address for the host is configured on the New User page. After clicking Save, the Guest User Details page displays the password. From this page, you can e-mail or printer the account credentials.

Follow these steps to schedule a recurring guest user account in WCS.

Step 1 Log in to the WCS user interface as lobby ambassador.

Step 2 Choose **Schedule Guest User** from the Guest User page.

Note You can also schedule guest users from the Configure > Controller Template Launch Pad > Security > Guest User option.

Step 3 On the Guest Users > Scheduling page, enter the guest user name. The maximum is 24 characters.

Step 4 Select the check box to generate a username and password on every schedule. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional.

Step 5 Select a Profile ID from the drop-down list. This is the SSID to which this guest user applies and must be a WLAN that has Layer 3 authentication policy configured. Your administrator can advise which Profile ID to use.

Step 6 Enter a description of the guest user account.

Step 7 Choose **limited** or **unlimited**.

- Limited: From the drop-down list, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 35 weeks.
  - Start time: Date and time when the guest user account begins.
  - End time: Date and time when the guest user account expires.
- Unlimited: This user account never expires.
- Days of the week: Select the check box for the days of the week that apply to this guest user account.

Step 8 Choose **Apply To** to restrict a guest user to a confined area by selecting a campus, building, or floor so that when applied, only those controllers and associated access points are available. You can use AP grouping to enforce access point level restrictions that determine which SSIDs to broadcast. Those access points are then assigned to the respective floors. You can also restrict the guest user to specific listed controllers or a configuration group, which is a group of controllers that has been preconfigured by the administrator.

From the drop-down lists, choose one of the following:

- Controller List: select the check box for the controller(s) to which the guest user account is associated.
- Indoor Area: choose the applicable campus, building, and floor.
- Outdoor Area: choose the applicable campus and outdoor area.
- Config group: choose the configuration group to which the guest user account belongs.

Step 9 Enter the e-mail address to send the guest user account credentials. Each time the scheduled time comes up, the guest user account credentials are e-mailed to the specified e-mail address.

Step 10 Review the disclaimer information. Use the scroll bar to move up and down.

Step 11 Click **Save** to save your changes or **Cancel** to leave the settings unchanged.

Printing or E-mailing WCS Guest User Details

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests.

The e-mail and print copy shows the following details:

- Username: Guest user account name.
- Password: Password for the guest user account.
- Start time: Data and time when the guest user account begins.
- End time: Date and time when the guest user account expires.
- Profile ID: Profile assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer: Disclaimer information for the guest user.

When creating the guest user account and applying the account to a list of controllers, area, or configuration group, a link is provided to e-mail or print the guest user account details. You can also print guest user account details from the Guest Users List page.

Follow these steps to print guest user details from the Guest Users List page.

Step 1 Log into the WCS user interface as lobby ambassador.

Step 2 On the Guest User page, select the check box next to User Name and choose **Print/E-mail User Details** from the Select a command drop-down list, and click **Go**.

- If printing, click **Print** and from the print page, select a printer, and click **Print** or **Cancel**.
- If e-mailing, click **E-mai**l and from the e-mail page, enter the subject text and the recipient's e-mail address. Click **Send** or **Cancel**.

Note You can also print or email user details from the Configure > Controller Template Launch Pad > Security > Guest User option.

Saving Guest Accounts on a Device

Click the **Save Guest Accounts on Device** check box to save guest accounts to a WLC flash so that they are maintained across WLC reboots.

Note In the Configure > Controller Template Launch Pad > Security > Guest page, you choose **Save Guest Accounts on device** from the Select a command drop-down page.

Editing the Guest User Credentials

Click the WCS user name of the guest user whose credentials you want to edit. The Lobby Ambassador Default tab appears, and you can modify the credentials.

While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are removed for this Lobby Ambassador. The user must reconfigure the defaults to reinforce them.

Adding a New User

The Add User page allows the administrator to set up a new user login including user name, password, groups assigned to the user, and virtual domains for the user.

Note You can only assign virtual domains to a newly created user which you own. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note You must have SuperUser status to access this page.

This section includes the following topics:

- Adding User Names, Passwords, and Groups
- Assigning a Virtual Domain

Adding User Names, Passwords, and Groups

To add a new user, follow these steps:

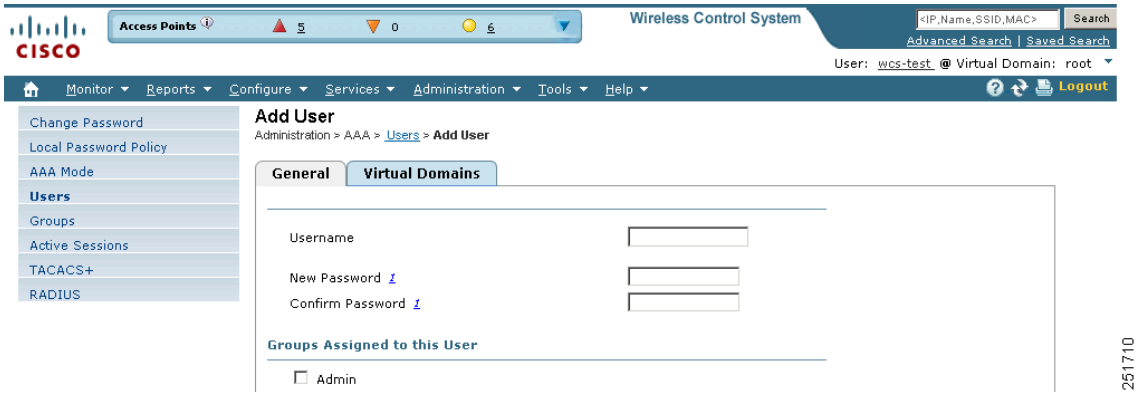
Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, select **Users**.

Step 3 From the **Select a command** drop-down list, choose **Add User**.

Step 4 Click **Go**. The Users page appears (see Figure 7-8).

Figure 7-8 Users Page



Add User

Administration > AAA > Users > Add User

General | Virtual Domains

Username

New Password

Confirm Password

Groups Assigned to this User

□ Admin

Step 5 Enter a new **Username**.

Step 6 Enter and confirm a password for this account.

Step 7 Select the check box(es) of the groups to which this user will be assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, Northbound API, or Users Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.
- ConfigManagers—Allows users to monitor and configure WCS operations.
- System Monitoring—Allows users to monitor WCS operations.
- Users Assistant—Allows local net user administration only.
- Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—A user group used only with WCS Navigator and WCS Web Service consumers.

  Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

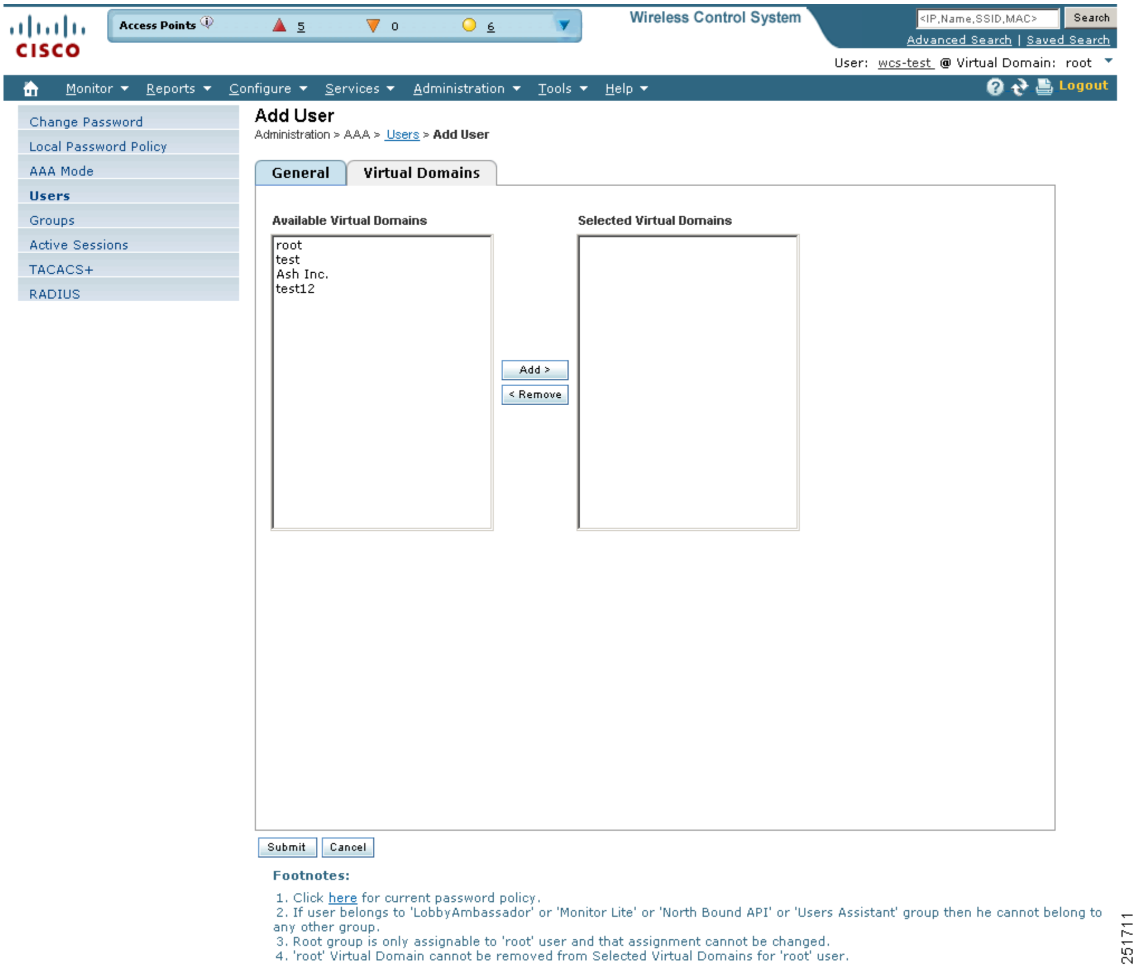
- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.
- User Defined

Assigning a Virtual Domain

Follow these steps to assign a virtual domain to this user:

Step 1 Click the **Virtual Domains** tab. This page displays all virtual domains available and assigned to this user (see Figure 7-9).

Figure 7-9 Users Virtual Domains Tab



Add User

Administration > AAA > Users > Add User

Available Virtual Domains

root
test
Ash Inc.
test12

Selected Virtual Domains

Footnotes:

1. Click here for current password policy.
2. If user belongs to 'LobbyAmbassador' or 'Monitor Lite' or 'North Bound API' or 'Users Assistant' group then he cannot belong to any other group.
3. Root group is only assignable to 'root' user and that assignment cannot be changed.
4. 'root' Virtual Domain cannot be removed from Selected Virtual Domains for 'root' user.

Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by holding down the Shift or Control key.

Step 3 Click **Add >**. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list, and click < **Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Choose **Submit** to or **Cancel** to close the page without adding or editing the current user.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy sidebar pre-formats the virtual domain's RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains into the ACS server screen and ensures that the users only have access to these virtual domains.

To apply the pre-formatted RADIUS and TACACS+ attributes to the ACS server, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, select to highlight the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 3 Click **Export**.

Step 4 Highlight the text inside of the RADIUS or TACACS+ Custom Attributes (depending on which one you are currently configuring), go to your browser's menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to User or Group Setup.

Note If you want to specify virtual domains on a per user basis, then you need to make sure you add ALL the custom attributes (for example, tasks, roles, virtual domains) information into the User custom attribute screen.

Step 7 For the applicable user or group, click **Edit Settings**.

Step 8 Use your browser's Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable text box.

Step 9 Click the check boxes to enable these attributes.

Step 10 Click **Submit**.

Step 11 Click **Restart**.

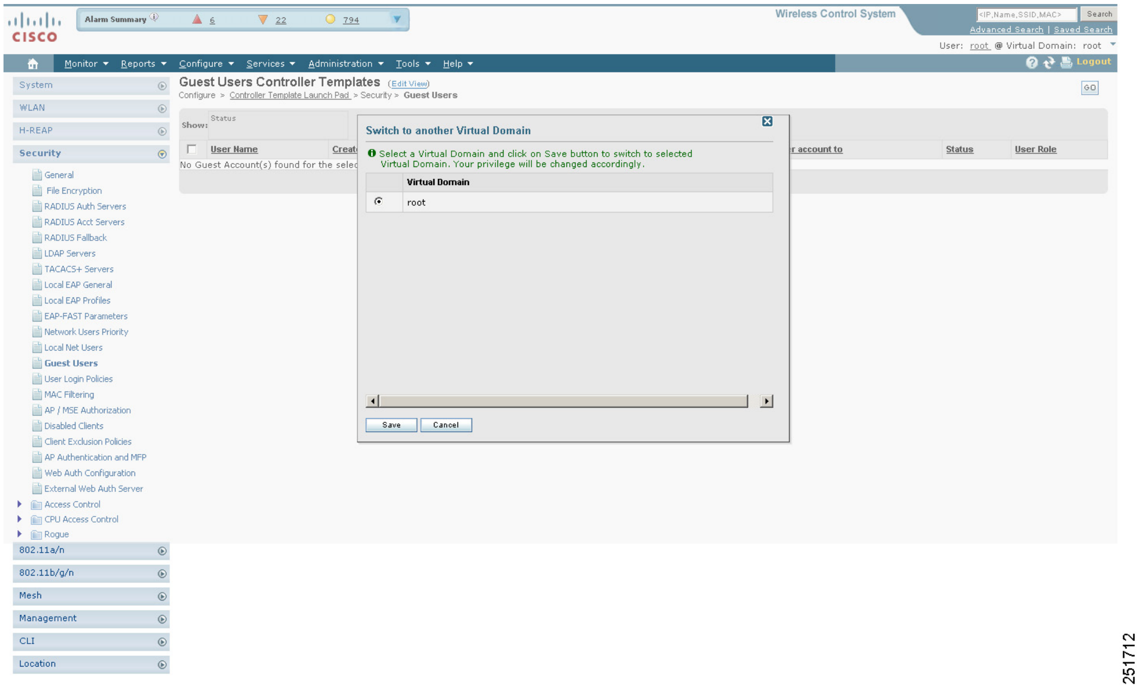
Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding WCS UserGroups into ACS for TACACS+" section on page 18-10 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 18-14.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the administrator assigned to you.

Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down list in the top of the WCS main page (see Figure 7-10). Only virtual domains that have been assigned to you are available in the drop-down list.

Figure 7-10 Virtual Domains Summary Tab



Switch to another Virtual Domain

Select a Virtual Domain and click on Save button to switch to selected Virtual Domain. Your privilege will be changed accordingly.

	Virtual Domain
●	root

No Guest Account(s) found for the selec

User: root @ Virtual Domain: root

Select a virtual domain and click Save to switch to the selected virtual domain. The privilege is changed accordingly.

Limited Menu Access

Non-root virtual domain users do not have access to the following WCS menus:

- Monitor > RRM
- Configure > Auto Provisioning
- Configure > ACS View Servers
- Mobility > Mobility Services

- Mobility > Synchronize Servers
- Administration > Background Tasks
- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit