CHAPTER 7

Managing WCS User Accounts

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

- Adding WCS User Accounts, page 7-1
- Viewing or Editing User Information, page 7-6
- Viewing or Editing Group Information, page 7-6
- Setting Lobby Ambassador Defaults, page 7-7
- Viewing the Audit Trail, page 7-9
- Enabling Audit Trails for Guest User Activities, page 7-11
- Creating Guest User Accounts, page 7-11
- Managing WCS Guest User Accounts, page 7-14
- Adding a New User, page 7-20

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.

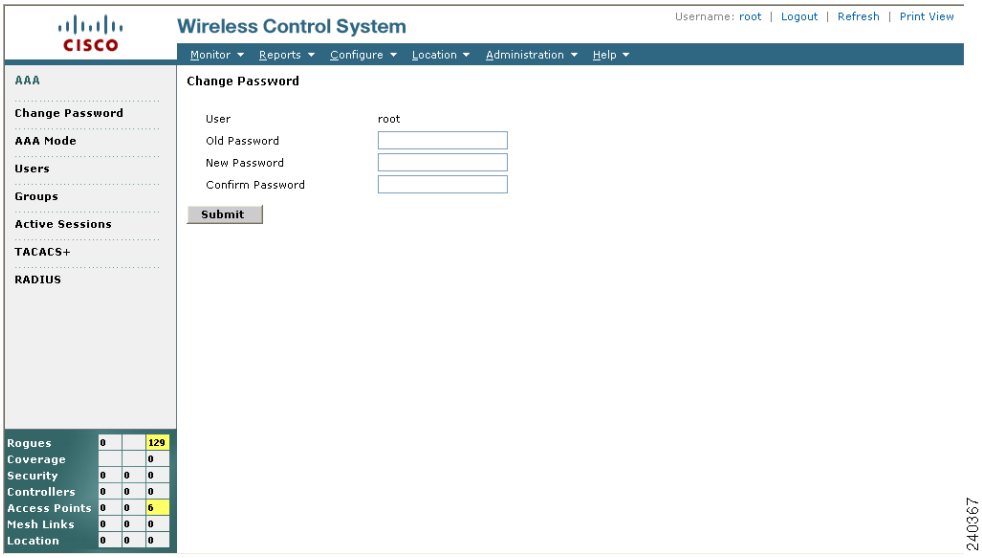
Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-12.

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 window appears (see Figure 7-1).

Figure 7-1 Change Password Window



Step 4 In the Old Password field, 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 Under Groups Assigned to this User, check the appropriate check box to assign the new user account to one of the user groups supported by WCS:

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.

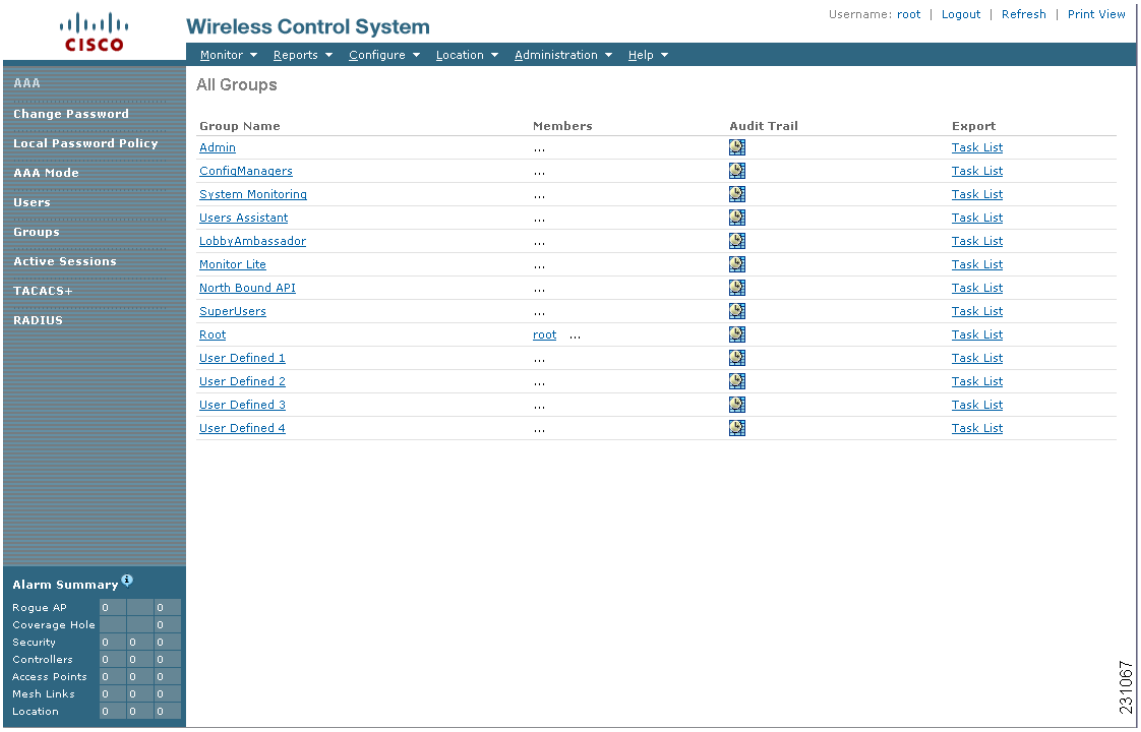
Note If you create a user assistant user, login as that user, and go to Monitor > Controller, you receive a permission denied message as expected behavior.

- 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.

Step 7 Click **Submit**. The name of the new user account appears on the All Users page and can be used immediately.

Step 8 In the sidebar, click **Groups** to display the All Groups page (see Figure 7-2).

Figure 7-2 All Groups Window



Step 9 Click the name of the user group to which you assigned the new user account. The Group > User Group page shows a list of this group's permitted operations.

Step 10 Make any desired changes by checking or unchecking the appropriate check boxes.

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

Step 11 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 2-12.

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

Step 3 Click **Administration > Accounts** to display the All Users page.

Step 4 Check the check box to the left of the user account(s) to be deleted.

Step 5 From the Select a command drop-down menu, 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 2-12.

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

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

Step 4 Click the name of the user account for which you want to change the password. You can change the password here or through the User > Edit window.

Step 5 Enter your old password, unless you are the root user. (A root user can change any password without entering the old password.)

Step 6 On the User > *Username* page, enter the new password in both the New Password and Confirm New Password fields.

Step 7 Click **Submit** to save your changes. The password for this user account has been changed and can be used immediately.

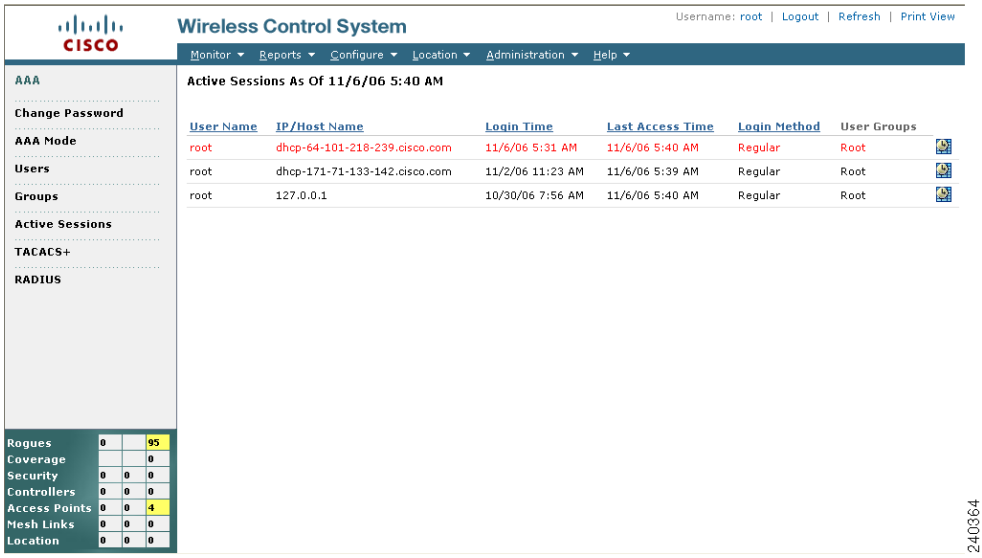
Monitoring Active Sessions

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 window appears (see Figure 7-3).

Figure 7-3 Active Sessions Window



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 window 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.

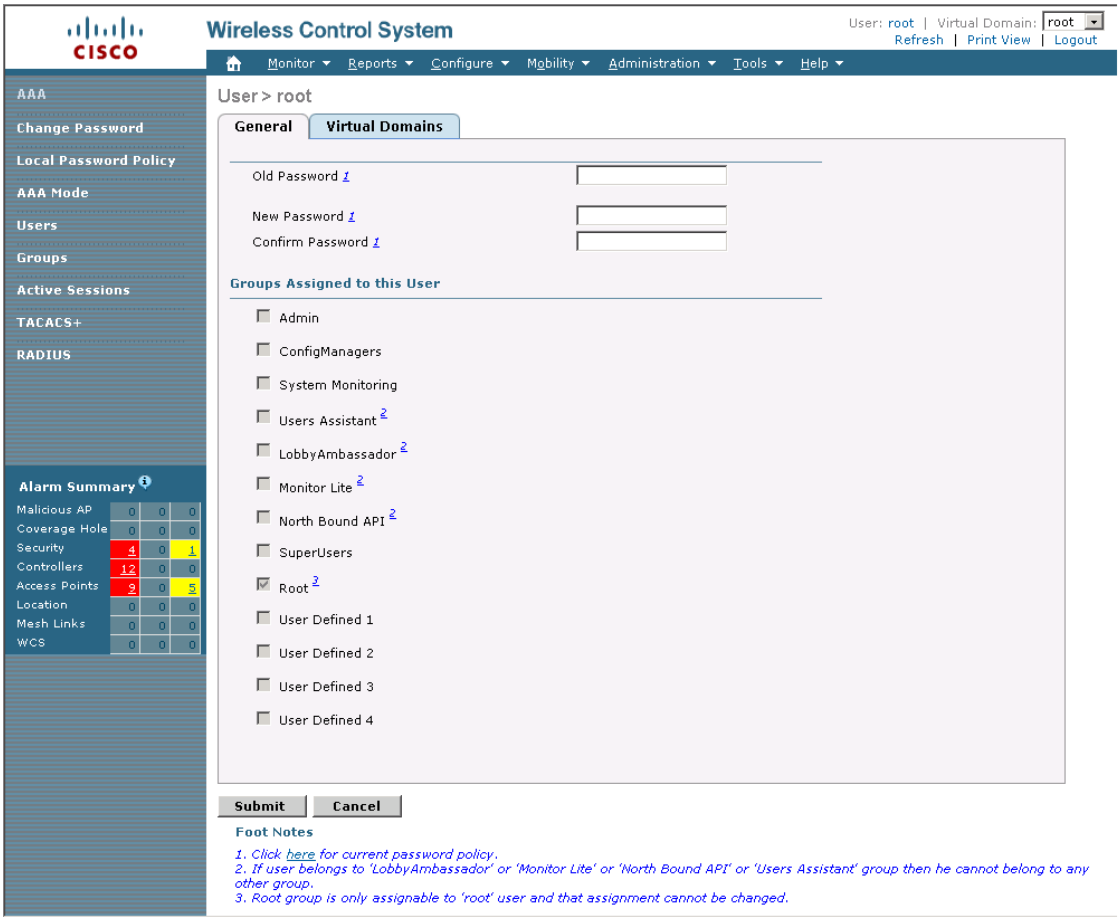
Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status panel. However, if a user navigates to a non-WCS Navigator web page in the same browser, the disparity in time is greater upon 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 window that displays the audit trail (previous login times) for that user.

Viewing or Editing User Information

Click in the User Name column of the Users window to see the group the user is assigned to or to adjust a password or group assignment. The detailed users window appears (see Figure 7-4).

Figure 7-4 Detailed Users Window

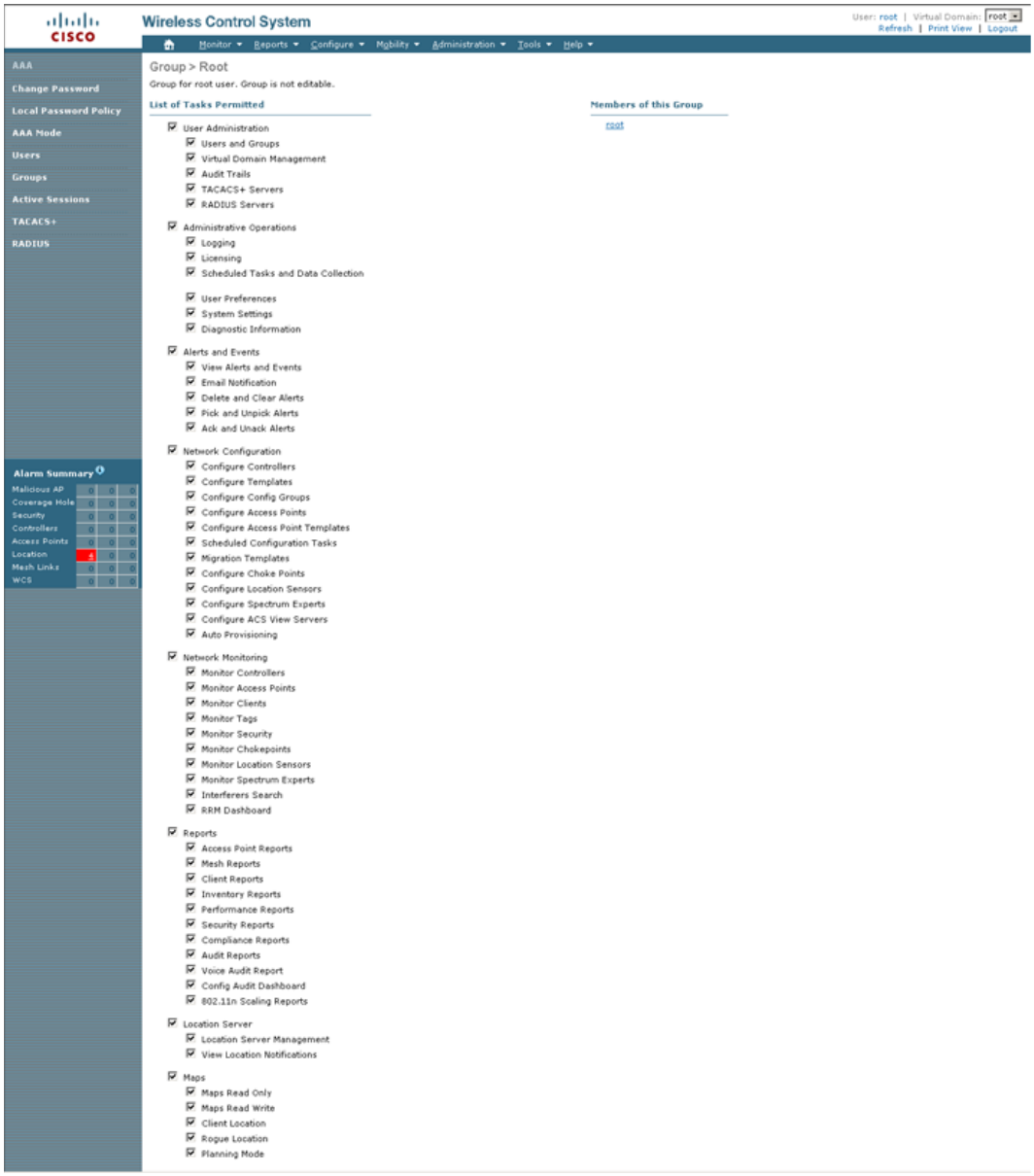


Viewing or Editing Group Information

Click in the Member Of column of the User window to see specific tasks the user is permitted to do within the defined group or to make changes and submit them. The detailed group window appears (see Figure 7-5).

Note The detailed window varies based on what group you choose. Figure 7-5 shows the detailed window of the root group.

Figure 7-5 Detailed Group Window

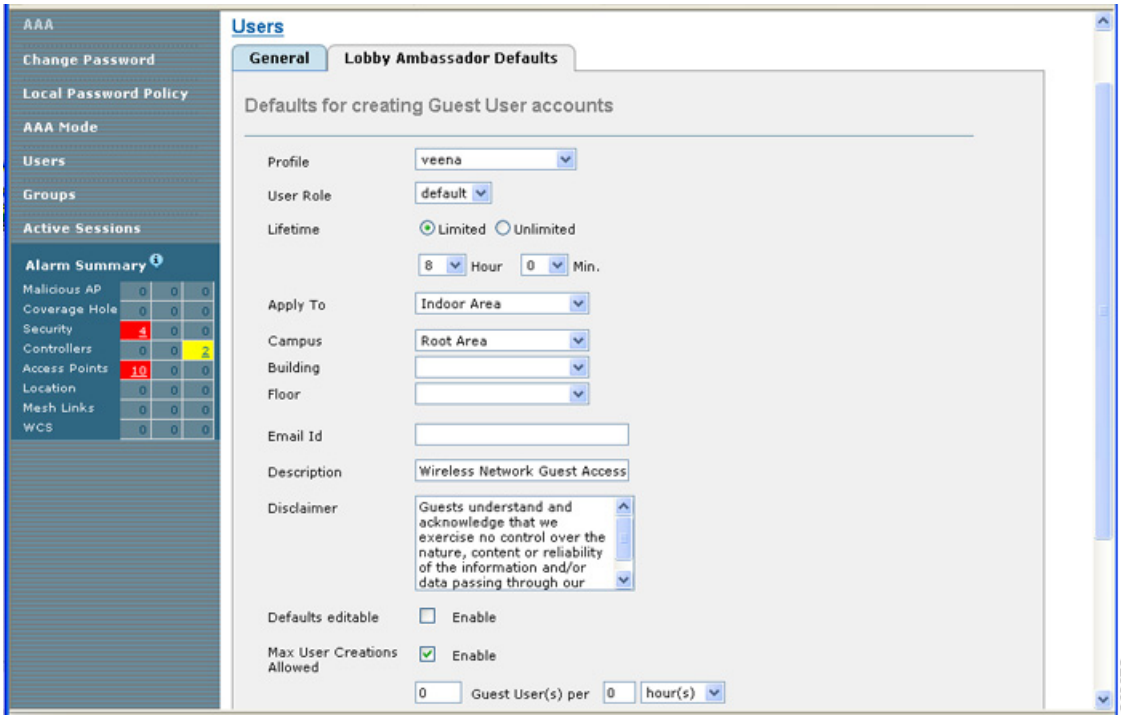


Setting Lobby Ambassador Defaults

If you click the Lobby Ambassador check box when creating a user group, a Lobby Ambassador Defaults tab appears (see Figure 7-6). 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 7-6 Lobby Ambassador Defaults



Step 1 Use the Profile drop-down menu to choose the guest user to connect to.

Step 2 Choose **Limited** or **Unlimited** at the Lifetime parameter. If you choose limited, you can specify the number of hours and minutes. By default the lifetime is limited to 8 hours.

Step 3 Use the Apply to drop-down menu 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 4 Enter the e-mail ID of the host to whom the guest account credentials are sent.

Step 5 Provide a brief description of the account.

Step 6 If you want to supply disclaimer text, enter it.

Step 7 Check the **Defaults Editable Enable** check box if you want to allow the lobby ambassador to override these configured defaults.

Step 8 Check the **Max User Creations Allowed Enable** check box to allow the lobby ambassador to set limits on the number of guest users that can be on the network in a given time period. The time period is defined in hours, days, or weeks.

Editing the Default Lobby Ambassador Credentials

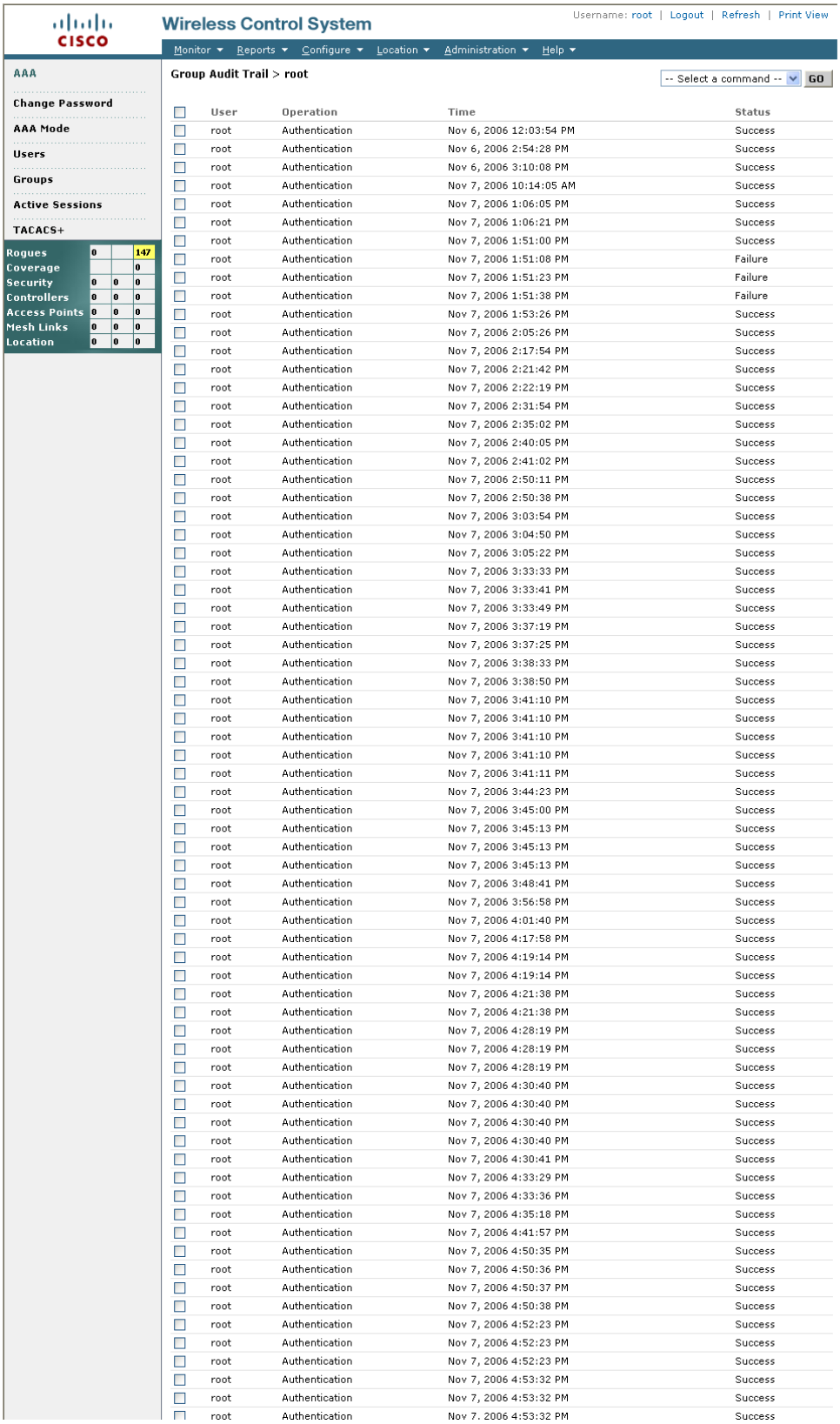
Click the WCS username in the Users window to edit the lobby ambassador default credentials. The Lobby Ambassador Default tab appears, and you can modify the credentials.

Note If you remove the profile selection, the defaults for this lobby ambassador are removed.

Viewing the Audit Trail

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

Figure 7-7 Audit Trail



Enabling Audit Trails for Guest User Activities

Follow these steps to enable audit trails for guest user activities.

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

Step 2 Click **Administration > AAA**, then click **Users** in the left sidebar menu to display the Users window.

Step 3 At the Users window, click the **Audit Trail** icon for the lobby ambassador account that you want to view. The Audit Trail window for the lobby ambassador appears.

The window enables you to view a list of lobby ambassador activities over time. Each entry displays the following information:

- User: User login name (for example, *lobby*)
- Operation: Type of operation audited (such as, creation and deletion of guest users reported by name)
- Time: Time operation was audited
- Status: Success or failure of activity

Note WCS keeps all Audit Trail records for up to 7 days. The nightly data cleanup task cleans all records which are older than 7 days.

Step 4 To clear a specific entry from the audit trail listing, check the check box next to that entry and choose **Clear Audit Trail** from the Select a command drop-down menu and click **GO**.

You can select multiple entries for deletion at one time.

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 administrator account. Guest user accounts are for visitors, temporary workers, etc. 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 administrator has no access to online help.

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:

- Creating a Lobby Ambassador Account, page 7-12
- Managing WCS Guest User Accounts, page 7-14
- Logging the Lobby Ambassador Activities, page 7-19

Creating a Lobby Ambassador Account

Follow these steps to create a lobby ambassador account 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 menu, choose **Add User** and click **GO**. The Users window 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, check the **LobbyAmbassador** check box to access the **Lobby Ambassador Defaults** tab.

Step 8 At the Lobby Ambassador Default tab, follow these steps to set the defaults for a guest user account:

a. Choose a Profile for the guest user from the drop-down menu.

Wired-guest is an example of a profile that might be defined to indicate traffic that is originating from wired LAN ports. Refer to the "Configuring Wired Guest Access" section on page 10-23.

b. Choose a user role for the guest user from the drop-down menu. User roles are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).

User Role is used to manage the amount of bandwidth allocated to specific users within the network. User roles are defined in Cisco WCS on the Local Net User Role Template Window. Refer to the "Configuring Guest User Templates" section on page 11-35.

c. Define how long the guest user account will be active by choosing either the Limited or Unlimited Lifetime option.
   - For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down menus. The default value for Limited is one day (8 hours).
   - When *unlimited* is chosen, no expiration date for the guest account exists.

d. Choose the area (indoor or outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down menu.
   - If you choose the controller list option, a list of controller IP addresses appears. Check the check box next to all controller networks on which guest traffic is allowed.

e. (Optionally) Enter the e-mail ID of the host to whom the guest account credentials are sent.

f. (Optionally) Modify the default guest user description if necessary.

g. (Optionally) Modify the Disclaimer text, if necessary.

h. Check the Defaults Editable check box. This allows the Lobby Ambassadors to modify Guest User default settings on the Lobby Ambassador Default setting window.

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 9 Click **Submit**.

When the lobby ambassador is added, it is part of the lobby ambassador group. The name of the new lobby ambassador account is listed and can be used immediately.

Editing a Lobby Ambassador Account

The Lobby Ambassador default credentials can be edited from the username link on the WCS user list page.

To edit the Lobby Ambassador default credentials, follow these steps:

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

Step 2 Choose **Administration > AAA**.

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

Step 4 Click the applicable Lobby Ambassador account from the **User Name** column.

Step 5 From the **Lobby Ambassador Defaults** page, edit the credentials as necessary.

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

Step 6 Click **Submit**.

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 6.0 or later on your computer.

Note Some WCS features may not function properly if you use a web browser other than Internet Explorer 6.0 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 window, enter your username and password.

Note All entries are case sensitive.

Note The lobby administrator 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 window is displayed. This window provides a summary of all created Guest Users.

To exit the WCS user interface, close the browser window or click **Logout** in the upper right corner of the window. 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 user accounts. It includes the following:

- Adding Guest User Accounts, page 7-15
- Deleting Guest User Templates, page 7-17
- Scheduling WCS Guest User Accounts, page 7-18

- Printing or E-mailing WCS Guest User Details, page 7-19

Adding Guest User Accounts

Templates are used to create guest user accounts in WCS. 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. The *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. The Guest User Credentials window appears. See the "Guest User Credentials" section on page 7-16.

Guest User Credentials

The Guest User Credentials window displays the following information:

- IP Address: IP address of controller to which the guest user account applies.
- Controller Name: Name of controller.
- Operation Status: Indicates successful or unsuccessful creation of guest user account.
- Reason: Indicates why the creation of the guest user account was unsuccessful.
- Guest User Credentials:
  - Guest User Name: Guest user account login name.
  - Password: Guest user account password.
  - Start time: Date and time that the guest user account begins.
  - End time: Date and time that the guest user account expires.
  - Disclaimer: Disclaimer information for the guest user.
- Print/E-mail Guest User Credentials: Link to print or e-mail guest user information. See the "Printing or E-mailing WCS Guest User Details" section on page 7-19.

Viewing and Editing Guest Users

Follow these steps to view the current WCS guest users.

Step 1 Log into the WCS user interface as described in the "Logging into the WCS User Interface" section on page 2-13.

Step 2 On the Guest User window, click which item number under the User Name column you want to view or edit.

Step 3 On the **Guest Users > Users** window, you can edit the following items:

- Profile ID: The selectable profiles are predefined by the system administrator and define the length of time, user role (allocated bandwidth), and areas of the network (indoor, outdoor, controllers, config groups) to which a guest user has access. Your administrator can advise which profile to use.
- Description: Enter a description of the guest user account.
- Limited or Unlimited:
  - 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.
- 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 also restrict the guest user (wired or wireless) to a specific listed controller or a config group, which is a group of controllers that has been preconfigured by the administrator.

  From the Apply To drop-down menus, choose one of the following:
  - Controller List: Check the check box for the controller(s) to which the guest user account applies.
  - 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 4 Click **Save** to save your changes or **Cancel** to leave the settings unchanged. When you click **Save**, the screen refreshes.

Note The account expiry displays the controller(s) to which the guest user account was applied and the seconds remaining before the guest user account expires.

Deleting Guest User Templates

During deletion of the guest account, all client stations logged in and using the guest WLAN username are deleted. Follow these steps to delete a WCS guest user template.

Step 1 Log into the WCS user interface as described in the "Logging into the WCS User Interface" section on page 2-13.

Step 2 On the Guest Users window, check the check box to the left of the guest user account(s) to be deleted.

Step 3 From the Select a Command drop-down menu, choose **Delete Guest User** and click **GO**.

Step 4 When prompted, click **OK** to confirm your decision.

Note The IP address and controller name to which the guest user account was applied appears, and you are prompted to confirm the removal of the template from the controller.

The controller sends a notification of a guest account expiry and deletion by invoking a trap. WCS processes the trap and deletes the user account expired from the configuration of that controller. If that guest account is not applied to other controllers, it can be deleted from the templates as well. A notice appears in the event logs also.

Step 5 Click **OK** to delete the guest user template from the controller or **Cancel** to leave the settings unchanged. When you delete the guest user template from the controller, you delete the specified guest user account.

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 username 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 window. After clicking Save, the Guest User Details window displays the password. From this window, 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 On the Guest User window, choose **Schedule Guest User** and click **GO** from the Select a command drop-down menu.

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

Step 4 Check 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 (unchecked), one password is supplied for a span of days. The generation of a new username and password on every schedule is optional.

Step 5 Select a Profile ID from the drop-down menu. 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 menu, 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: Check 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 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 menus, choose one of the following:

- Controller List: check 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 window.

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

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

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

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

Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- Lobby ambassador login: WCS logs the authentication operation results for all users.
- Guest user creation: When a lobby ambassador creates a guest user account, WCS logs the guest user name.

- Guest user deletion: When a lobby ambassador deletes the guest user account, WCS logs the deleted guest user name.
- Account updates: WCS logs the details of any updates made to the guest user account. For example, increasing the life time.

Follow these steps to view the lobby ambassador activities.

Note You must have superuser status to open this window.

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

Step 2 Click **Administration > AAA**, then click **Groups** in the left sidebar menu to display the All Groups window.

Step 3 On the All Groups windows, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail window for the lobby ambassador appears.

This window enables you to view a list of lobby ambassador activities over time.

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

Step 4 To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down menu and click **GO**.

Adding a New User

The Add User window 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.

- Add User Name, Password, and Groups
- Assign a Virtual Domain

Add User Name, Password, and Groups

To add a new user, follow these steps:

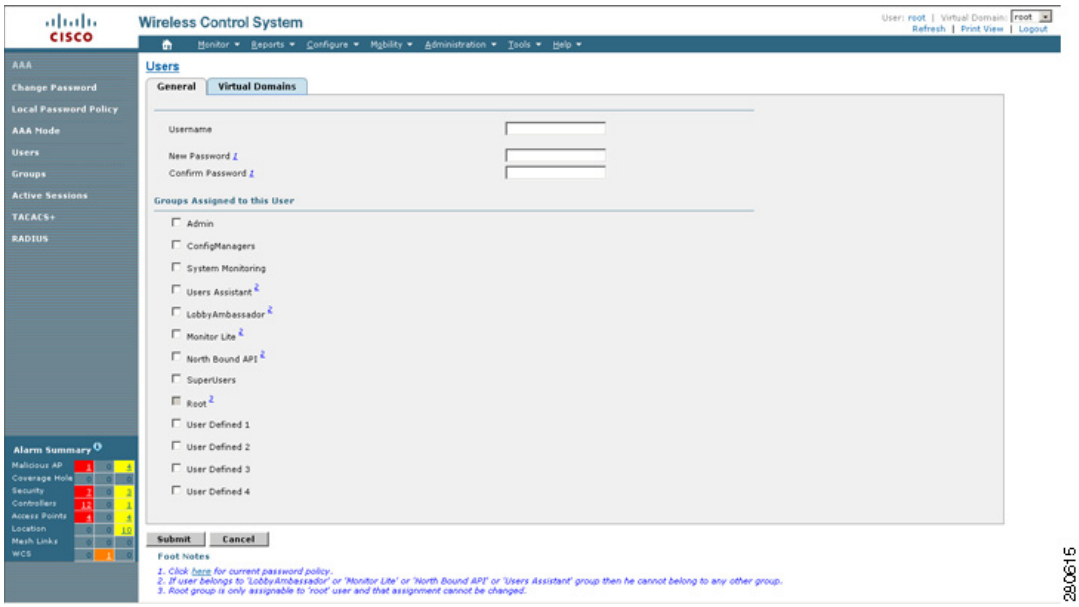
Step 1 Choose **Administration > AAA**.

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

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

Step 4 Click **GO**. The Users window appears (see Figure 7-8).

Figure 7-8 Users Window



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 adminstration 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. See "Creating a Lobby Ambassador Account" procedure on page 7-12" for more information on setting up a Lobby Ambassador account.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—Group used only with WCS Navigator.

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.

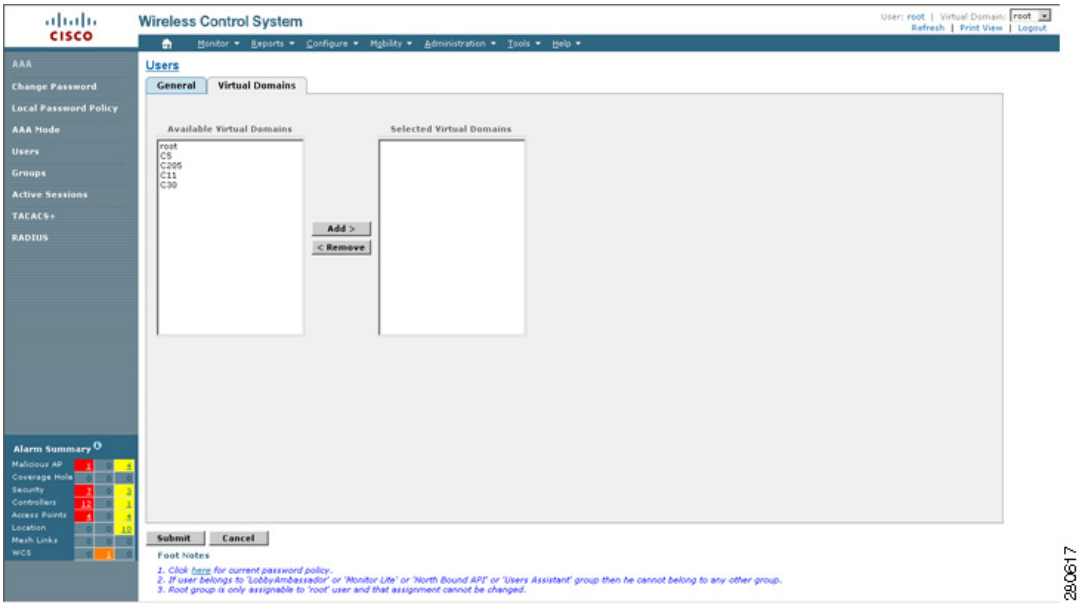
- SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.
- User Defined

Assign a Virtual Domain

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

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

Figure 7-9 Users Virtual Domains Tab



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 hightlight 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 hightlight 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 window without adding or editing the current user.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes window 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 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 2 Click **Export**.

Step 3 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 4 Log in to ACS.

Step 5 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 (i.e., tasks, roles, virutal domains) information into the User custom attribute screen.

Step 6 For the applicable user or group, click **Edit Settings**.

Step 7 Use your browser's **Edit > Paste** feature to place the RADIUS or TACACS+ custom attributes into the applicable field.

Step 8 Click the check boxes to enable these attributes.

Step 9 Click **Submit + Restart**.

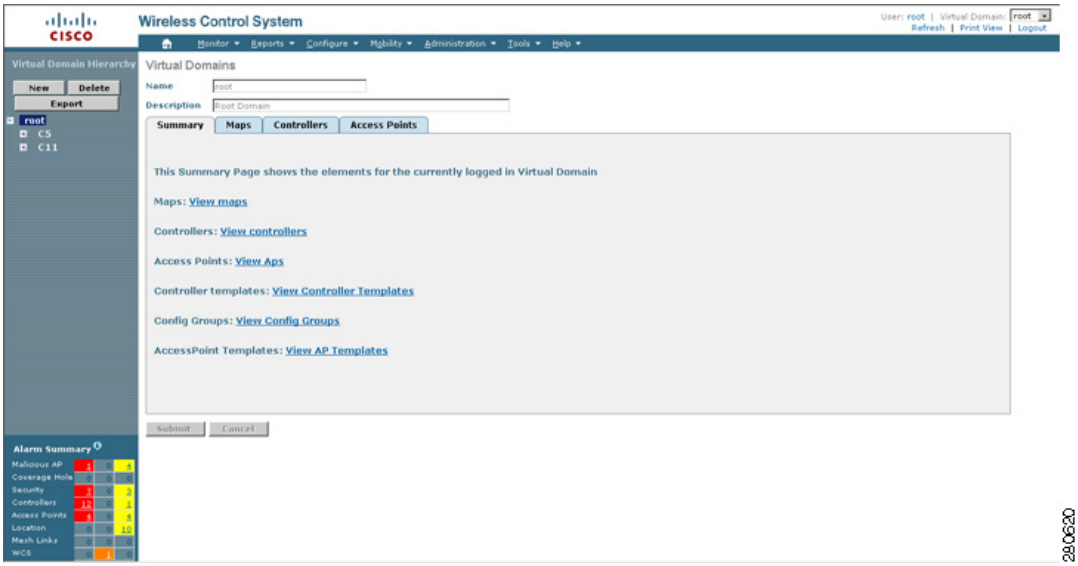
Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding WCS UserGroups into ACS for TACACS+" section on page 16-7 or the "Adding WCS UserGroups into ACS for RADIUS" section on page 16-11.

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 menu at the top of the screen (see Figure 7-10). Only virtual domains that have been assigned to you are available in the drop-down menu.

Figure 7-10 Virtual Domains Summary Tab



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 Service Engines
- Mobility > Synchronize Servers
- Administration > Background Tasks
- Administration > Settings
- Administration > User Preferences

- Tools > Voice Audit
- Tools > Config Audit