CHAPTER 6

Configuring Guest Policies

Organizations commonly have policies in place for creating accounts for their internal users and systems, such as the format or length of the username and/or complexity of password. The Cisco NAC Guest Server allows you to configure guest username and password creation policies to match your organization's policy or to create a policy specific to guest accounts.

You can also use the guest details policy to define specific guest user information on the Cisco NAC Guest Server.

The Cisco NAC Guest Server also allows you to configure different roles for your guests. Guest roles provide a way to give different levels of access to different guest accounts (e.g. assigning different roles on the Clean Access Manager, assigning different RADIUS attributes, or only allowing access to guests from certain IP address ranges).

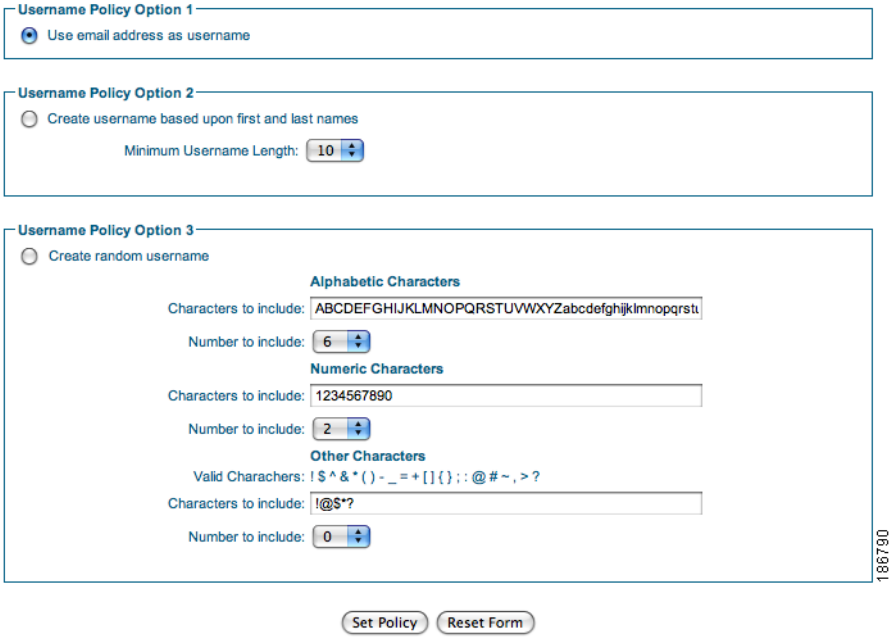
This chapter describes the following:

Setting the Username Policy

The Username Policy determines how to create user names for all guest accounts.

Step 1 From the administration interface, select **Guest Policy > Username Policy** from the left hand menu (Figure 6-1).

Figure 6-1 Guest Username Policy



Step 2 Choose one of three options for creating the user name for the guest account.

- **Username Policy 1 (email)**

  Use the guest's email address as the username. If an overlapping account with the same email address exists, a random number is added to the end of the email address to make the username unique. Overlapping accounts are accounts that have the same email address and are valid for an overlapping period of time.

- **Username Policy 2 (FirstLast)**

  Create a username based on combining the first name and last name of the guest. You can set a Minimum Username Length for this username from 1 to 20 characters (default is 10). User names shorter than the minimum length are padded up to the minimum specified length with a random number.

- **Username Policy 3 (Random)**

  Create a username based upon a random mixture of Alphabetic, Numeric or Other characters. Type the characters to include to generate the random characters and the number to use from each set of characters.

Note The total length of the username is determined by the total number of characters included.

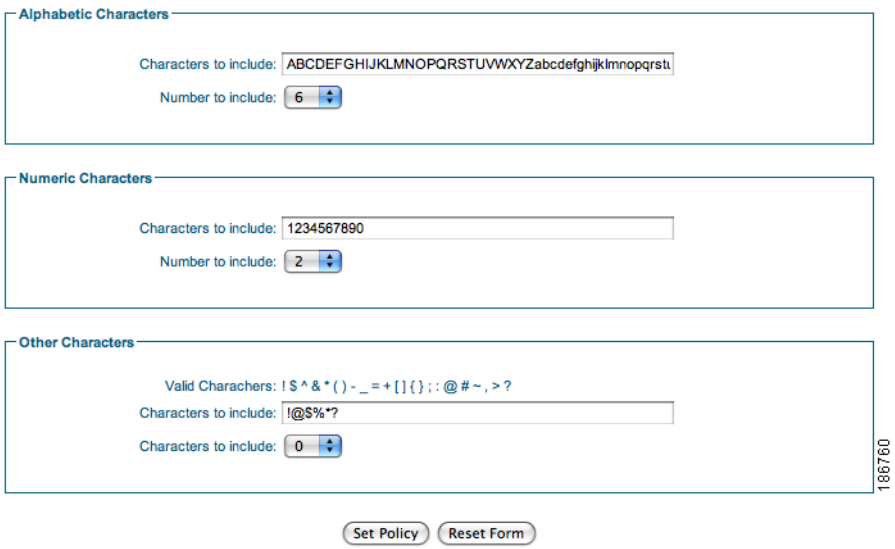
Step 3 When done, click **Set Policy** to have the username policy take effect.

Setting the Password Policy

The password policy determines how to create the password for all guest accounts.

Step 1 From the administration interface, select **Guest Policy > Password Policy** from the left hand menu (Figure 6-2).

Figure 6-2 Password Policy



Step 2 In the **Alphabetic Characters** section, enter the characters to use in the password and the amount to include.

Step 3 In the **Numeric Characters** section, enter the numerals to use in the password and the amount to include.

Step 4 In the **Other Characters** section, enter the special characters to use in the password and the amount to include.

Caution For passwords, use only the following characters for the "Other Characters" field: **! $ ^ & * ( ) - _ = + [ ] { } ; : @ # ~ , > ?**.
Do **not** use the following characters in the "Other Characters" field, as they are **not** supported by the Clean Access Manager API: £ % < ¬ ` ' \ |.

Step 5 Click **Set Policy** to save the settings.

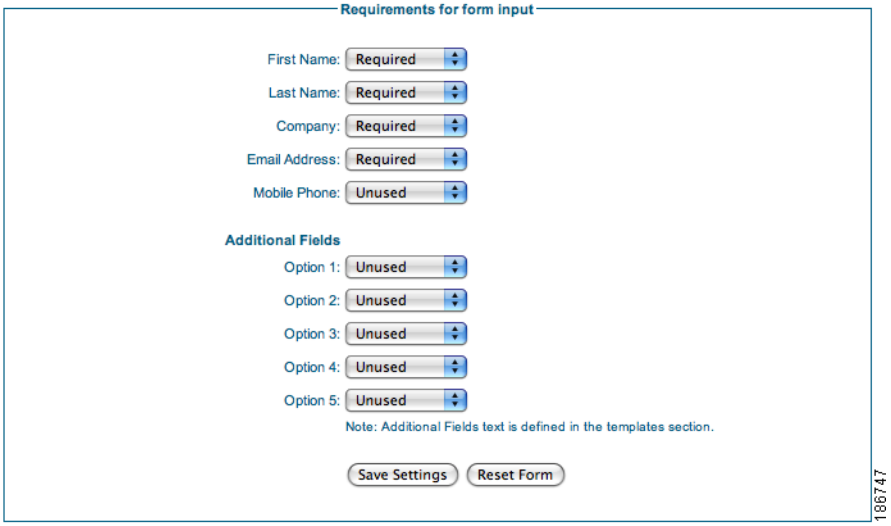
Note The total length of the password is determined by the total number of characters included. You can choose between 0 and 20 characters per type (alphabetic, numeric, or other).

Setting the Guest Details Policy

The guest details policy determines what data the sponsor needs to enter to create a guest account.

Step 1 From the administration interface, select **Guest Policy > Guest Details** from the left hand menu (Figure 6-3).

Figure 6-3 Guest Details Policy



Step 2 You can specify one of three settings for each requirement:

- Required—If a field is set to required it is displayed on the create guest page and it is mandatory for the sponsor to complete.
- Optional—If a field is set to optional it is displayed on the create guest page however the sponsor can choose not to complete the field.
- Unused—If a field is set to unused then it is not displayed on the create guest page and no value is required.

Step 3 Click the **Save Settings** button to save the guest details policy.

Note There are five additional fields that can have any information that you require entered into them. These are described on the screen as Option 1 through Option 5. If you want to use these fields, Cisco recommends customizing the text that is shown to the sponsor by editing the templates as described in User Interface Templates, page 10-1.

Configuring Guest Roles

Guest roles provide a way to give different levels of access to different guest accounts (e.g. assigning different roles on the Clean Access Manager, assigning different RADIUS attributes, or only allowing access to guests from certain IP address ranges).

Once guest roles have been created, you must change the user group to allow sponsors in that group to be able to provision accounts in the appropriate role. See Assigning Guest Roles, page 5-10 for instructions on how to allow sponsors to assign different guest roles.

Adding Guest Roles

You can add a new guest role using the following steps.

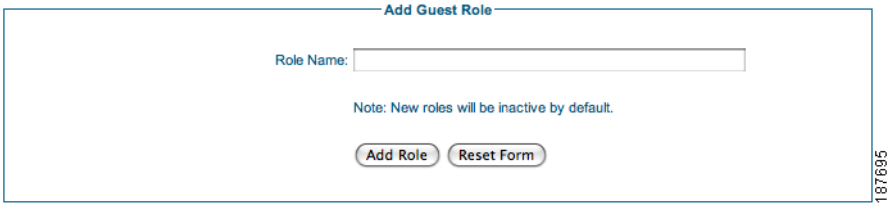
Step 1 From the administration interface select **Guest Policy > Guest Roles** from the left hand menu (Figure 6-4).

Figure 6-4 Guest Roles

Step 2 Click the **Add Role** button to add a new guest role.

Step 3 From the Add Guest Role page (Figure 6-5), enter the name for a new guest role.

Figure 6-5 Add New Guest Role



Step 4 Click the **Add Role** button to add a guest role. You can now edit the settings for the new guest role as described in Editing Guest Roles.

Editing Guest Roles

The following steps describe how to edit guest roles.

Step 1 From the administration interface select **Guest Policy** > **Guest Roles** from the left hand menu.

Figure 6-6 Edit Guest Roles

Step 2 Select the role you wish to edit and click the **Edit Role** button (Figure 6-6).

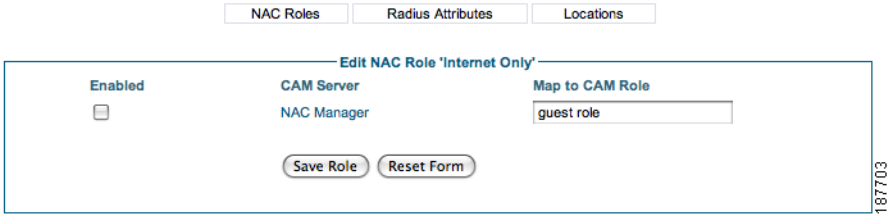
Edit NAC Roles

For each role you can specify which Clean Access Managers the guest account will be provisioned onto and which role name on the Clean Access Manager will be used.

By default, no Clean Access Managers are selected and the role that is shown is copied from the relevant Cisco NAC Appliance setting.

Step 1 Select **NAC Roles** from the top of the page.

Figure 6-7 NAC Role



Step 2 For each Cisco NAC Appliance check the **Enabled** box if you would like accounts created with this guest role to be provisioned on that Clean Access Manager.

Step 3 For each Cisco NAC Appliance enter the role that corresponds to the role on the Cisco NAC Appliance that you would like to create the guest account in.

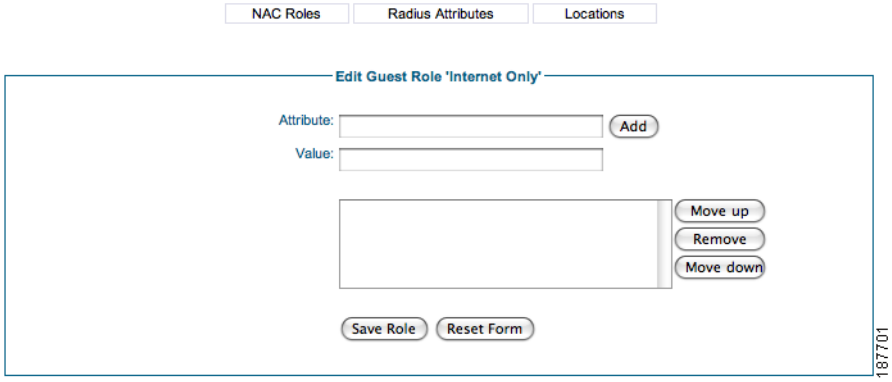
Step 4 Click **Save Role**.

Edit Radius Attributes

If a guest authenticates with a RADIUS client device such as a Cisco Wireless LAN controller then for each role you can specify additional RADIUS attributes that will be sent upon successful authentication.

Step 1 Select **RADIUS Attributes** from the top of the page (Figure 6-8).

Figure 6-8 RADIUS Attributes



Step 2 Enter each **Attribute** and **Value** pair and click the **Add** button.

Step 3 If you need to re-order the attributes that are sent use the **Move up** and **Move down** buttons.

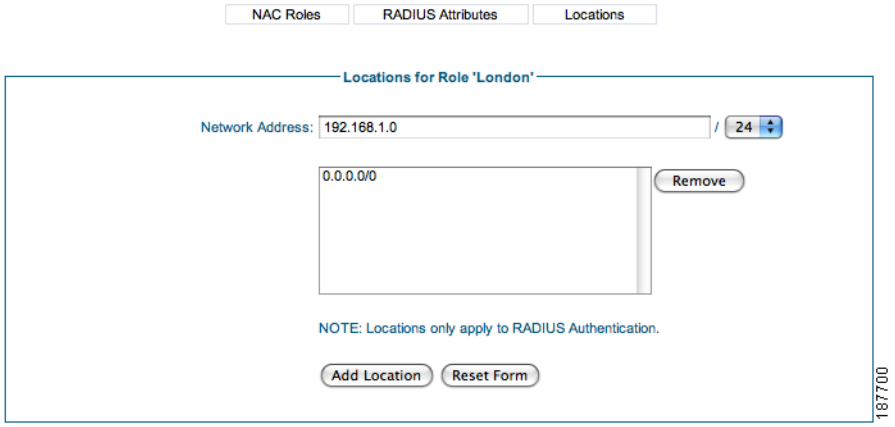
Step 4 Click **Save Role** when you want to save the Radius Attributes.

Edit Locations

If a guest authenticates with a RADIUS client device such as a Cisco Wireless LAN controller, you can specify from which IP address ranges the guest is allowed to authenticate for each role. This enables you to specify roles based upon location so that guests assigned to a specific role can only login from locations that you specify.

Step 1 Select **Locations** from the top of the page.

Figure 6-9 Locations



Step 2 Enter each **Network Address** and select the appropriate prefix length from the dropdown menu. Only valid Network Addresses will be accepted—host addresses must be specified using a /32 prefix length.

Step 3 Click **Add Location** to add the Network Address.

Note When you add a role the location 0.0.0.0/0 is automatically added. This means that the role is valid from any IP address. If you want to restrict to other IP address ranges you must remove this address.

Note Locations only apply to users authenticating through RADIUS clients such as the Wireless LAN Controller.