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 allows you to configure different roles for your guests. Guest roles allow you to provide different levels of access to different guest accounts (for example, to map different guest roles to Clean Access Manager roles, to assign different RADIUS attributes, or to only allow access to guests from certain IP address ranges).

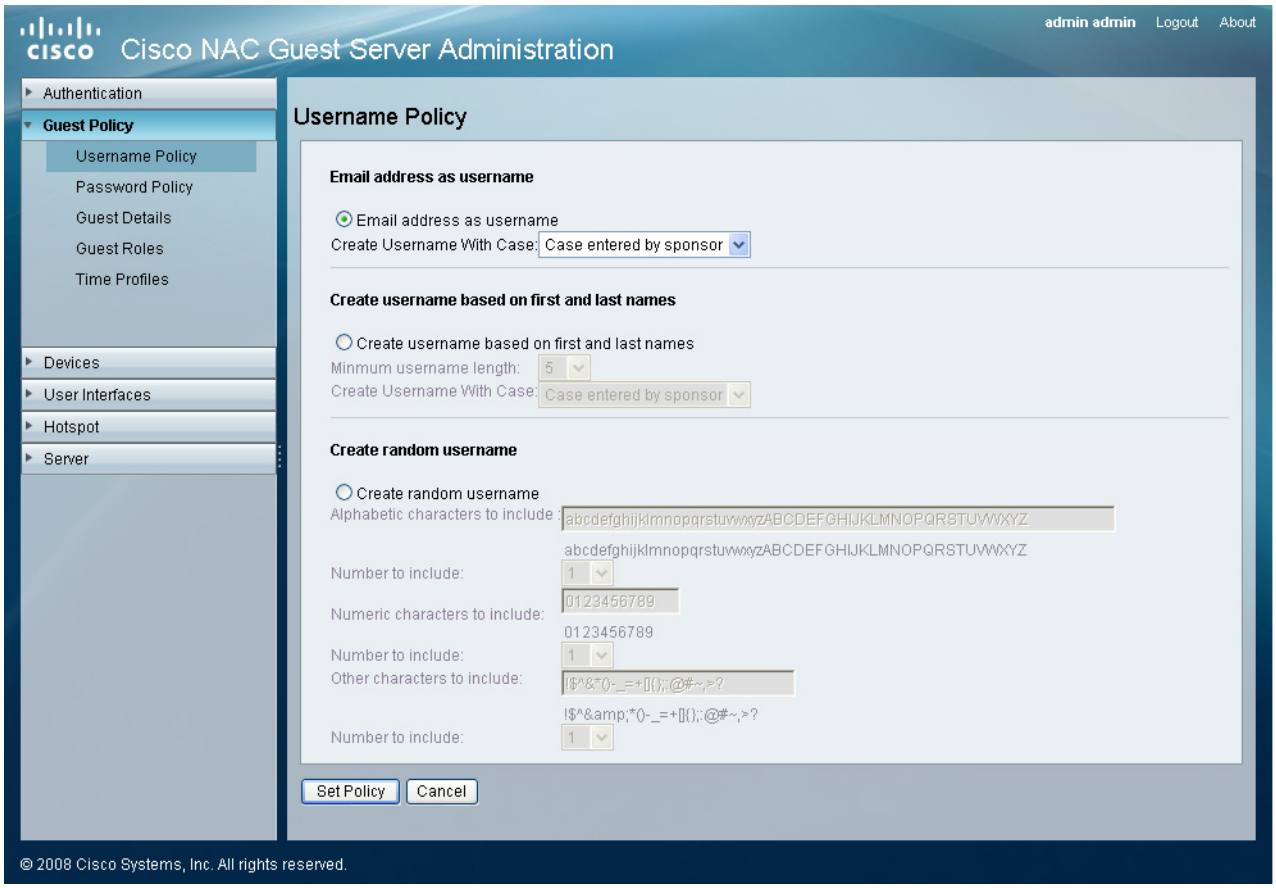
This chapter describes the following:

Setting 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** as shown in Figure 6-1.

Figure 6-1 Guest Username Policy



Step 2 Choose one of the username policy options for creating the user name for the guest account:

a. Username Policy 1 - Email address as username

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.

With the **Create Username With Case** option, you can determine the case of the guest username created by the sponsor:

- **Case entered by sponsor—**The username remains in the same case set by the sponsor.
- **UPPERCASE**—The username is forced into uppercase after being set by the sponsor.
- **lowercase**—The username is forced into lowercase after being set by the sponsor.

b. Username Policy 2 - Create username based on first and last names

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.

With the **Create Username With Case** option, you can determine the case of the guest username created by the sponsor:

- **Case entered by sponsor—**The username remains in the same case set by the sponsor.
- **UPPERCASE**—The username is forced into uppercase after being set by the sponsor.
- **lowercase**—The username is forced into lowercase after being set by the sponsor.

c. Username Policy 3 - Create random username

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.

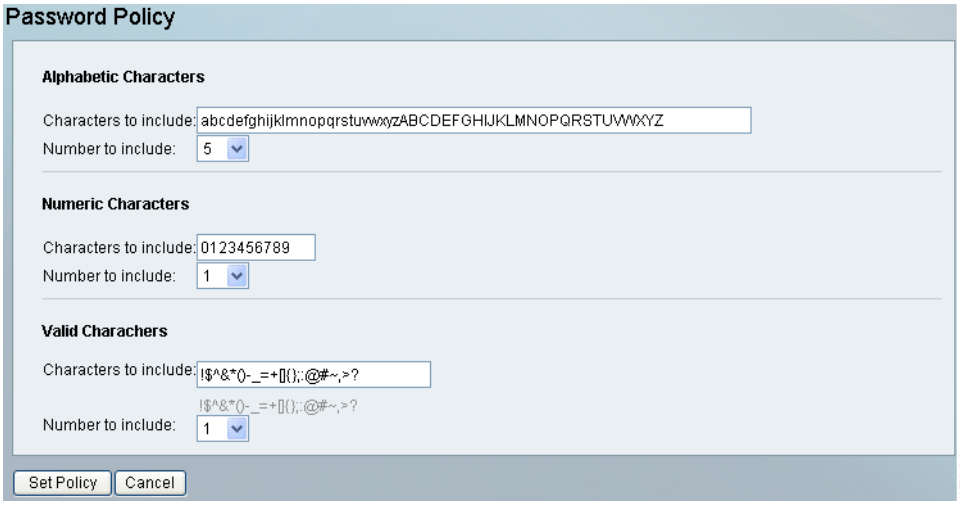
Step 3 When done, click **Save** to have the username policy take effect.

Setting 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** as shown in Figure 6-2.

Figure 6-2 Password Policy



Step 2 In the **Alphabetic Characters** section, enter the characters to be used in the password and the number to be included.

Step 3 In the **Numeric Characters** section, enter the numerals to be used in the password and the number to be included.

Step 4 In the **Other Characters** section, enter the special characters to be used in the password and the number to be included.

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 the **Save** button to save the settings.

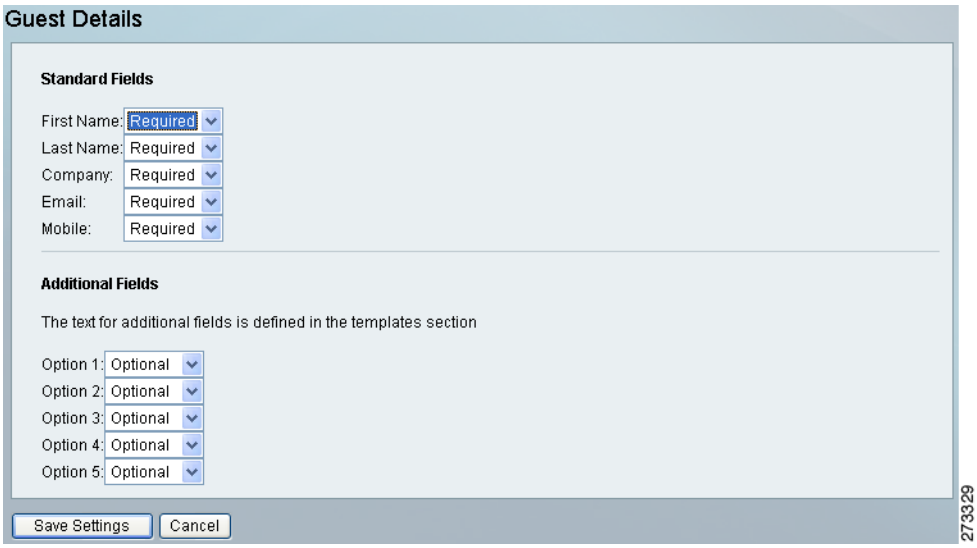
Note The total length of the password is determined by the total number of characters included. You can choose between 0 and 20 characters per type (alphabetic, numeric, or other).

Setting Guest Details Policy

The Guest Details policy determines the data the sponsor needs to enter to create a guest account.

Step 1 From the administration interface, select **Guest Policy > Guest Details** as shown in 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 Account 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 Account 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 Account page and no value is required.

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

Note There are five **Additional Fields** that you can use to add any additional information that you require sponsors to fill out when creating guest accounts. These are described on the Guest Details page 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 11-1.

Configuring Guest Roles

Guest roles provide a way to give different levels of access to different guest accounts. For example, to map different guest roles to Clean Access Manager roles, to assign different RADIUS attributes, or to only allow access to guests from certain IP address ranges.

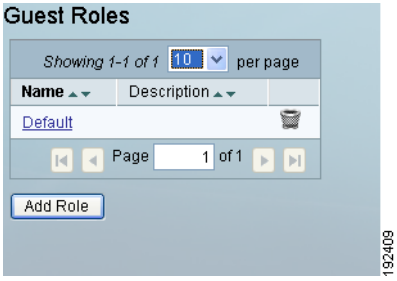
Once guest roles have been created, you must change the user group to allow sponsors in that group to be able to provision accounts in the appropriate role. See Assigning Guest Roles, page 5-13 for instructions on how to allow sponsors to assign different guest roles.

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** as shown in Figure 6-4.

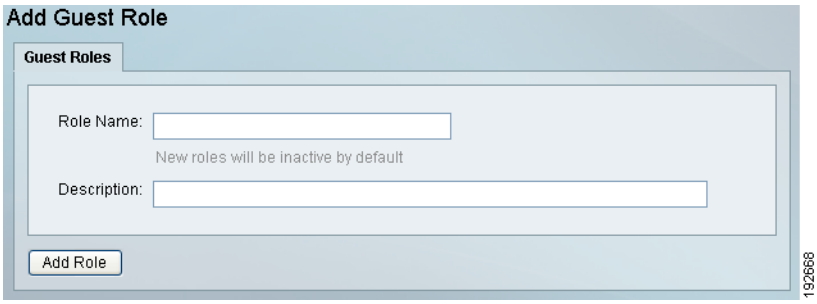
Figure 6-4 Guest Roles



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

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

Figure 6-5 Add New Guest Role



Step 4 Enter a Role Name and its Description in the fields provided.

Step 5 Click the **Add Role** button to add the guest role. You can now edit the settings for the new guest role as described in Editing Guest Roles, page 6-6.

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 underlined name of that role as shown in Figure 6-6 to bring up the NAC Roles edit. You can edit the following attributes:

- Edit NAC Roles
- Edit RADIUS Attributes
- Edit Locations
- Edit Authentication Settings

Edit NAC Roles

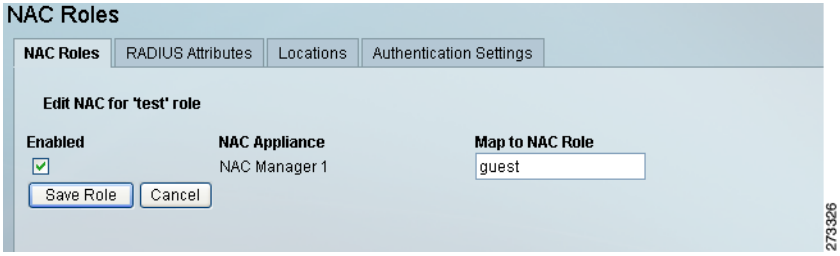
For each role, you can specify the Clean Access Managers for which the guest account will be provisioned onto and the role name on which the Clean Access Manager will be used.

By default, no Clean Access Managers are selected and the role that is shown is copied from the relevant Cisco NAC Appliance setting. Refer to Chapter 7, "Integrating with Cisco NAC Appliance" for additional details.

Step 1 From the administration interface, select **Guest Policy** > **Guest Roles** and click the underlined name of the role you want to edit.

Step 2 Select **NAC Roles** from the top of the page.

Figure 6-7 NAC Role



Step 3 For each Cisco NAC Appliance, check the **Enabled** box if you want accounts created with this guest role to be provisioned onto that Clean Access Manager.

Step 4 For each Cisco NAC Appliance, enter the role in the Map to NAC Role field that corresponds to the role on the Cisco NAC Appliance in which you want to create the guest account.

Step 5 Click the **Save Role** button.

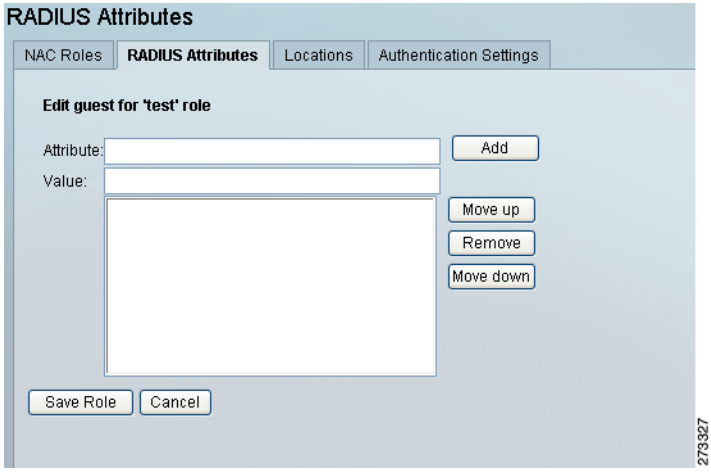
Edit RADIUS Attributes

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 are sent upon successful authentication.

Step 1 From the administration interface, select **Guest Policy** > **Guest Roles** and click the underlined name of that role you want to edit.

Step 2 Select **RADIUS Attributes** from the top of the page as shown in Figure 6-8.

Figure 6-8 RADIUS Attributes



Step 3 Enter each **Attribute** and **Value** pair and click the **Add** button.

Step 4 If you need to re-order the attributes that are sent, use the **Move up** and **Move down** buttons.

Step 5 Click the **Save Role** button to save the RADIUS Attributes.

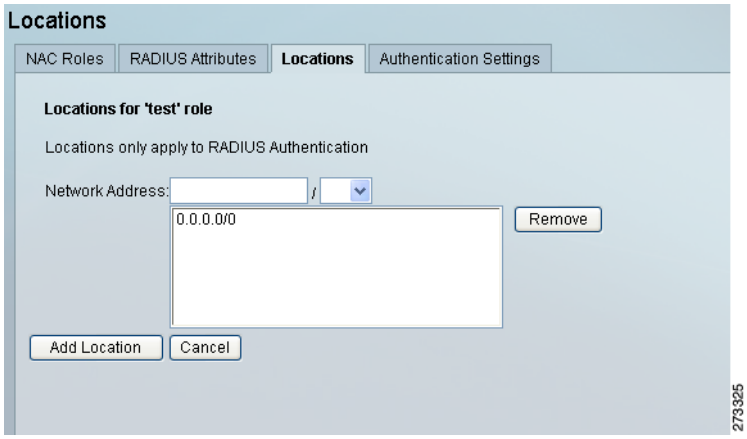
Edit Locations

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 From the administration interface, select **Guest Policy** > **Guest Roles** and click the underlined name of that role you want to edit.

Step 2 Click the **Locations tab** as shown in Figure 6-9.

Figure 6-9 Locations



Step 3 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 4 Click the **Add Location** button 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.

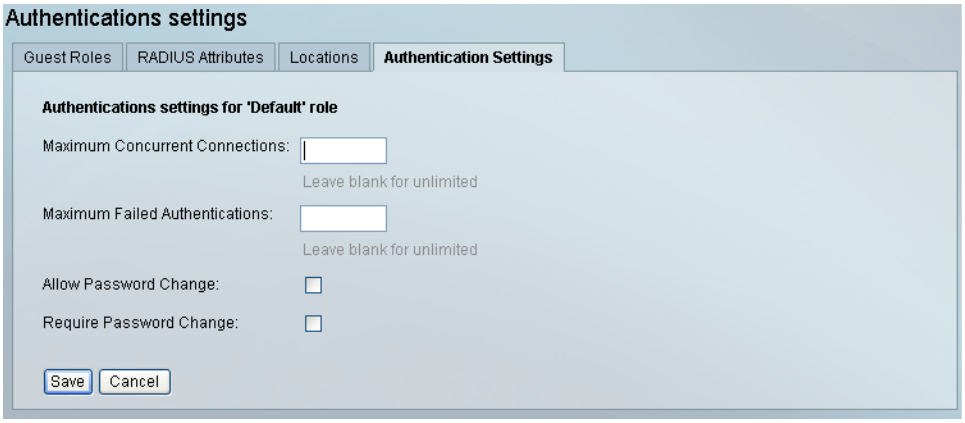
Note Locations only apply to users authenticating through RADIUS clients such as the Cisco Wireless LAN Controller.

Edit Authentication Settings

Step 1 From the administration interface, select **Guest Policy > Guest Roles** and click the underlined name of the role you want to edit.

Step 2 Click the **Authentication Settings** tab as shown in Figure 6-10.

Figure 6-10 Authentication Settings



Step 3 Enter a number for the **Maximum Concurrent Connections** for Guests in this Role. This sets the maximum number of concurrent connections to which a guest account is allowed to be associated. Leave the field blank for an unlimited number of connections and authentications.

Step 4 Enter a number for the **Maximum Failed Authentications** for Guests in this Role. This sets the maximum number of failed authentication attempts a guest is allowed to have before the account is suspended. Leave the field blank for an unlimited number of connections and authentications.

Step 5 Check the **Allow Password Change** checkbox to allow the Guest to change the password. Check this option to use the Password Change widget.

Step 6 Check the **Require Password Change** checkbox to force the Guest to change the password during first login. This option applies to all widgets that allow guest login (Login, Self Service, Billing), and forces the guest to change the password before logging in to the Guest Server. To include the Password Change in a page, add the following script:

```
<html>
<head>
```

```
</head>
<body>
<script type="text/javascript"
src="/sites/js/ngs_password.js"></script>
</body>
</html>"
```

Step 7 Click the **Save** button to save your changes. Refer Creating a Password Change Page (WLC and Switch), page 12-26 for further information.

Configuring Time Profiles

Time Profiles provide a way to give different levels of time access to different guest accounts. For example, you can assign a time profile that allows a guest access during a working week day and not on a weekend.

Once time profiles are created, you must change the sponsor user group to allow sponsors in that group to be able to provision accounts to the appropriate time profiles created. See Assigning Time Profiles, page 5-14 for instructions on how to allow sponsors to assign different time profiles.

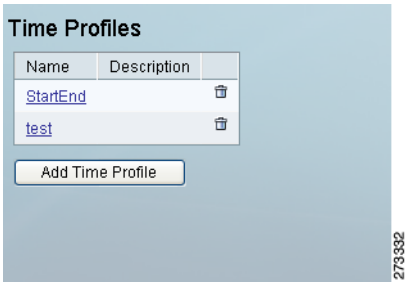
Note Cisco NAC Guest Server Version 2.0 supports only start/end and from creation profiles when used with Cisco NAC Appliances.

Adding Time Profiles

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

Step 1 From the administration interface, select **Guest Policy** > **Time Profiles** as shown in Figure 6-11.

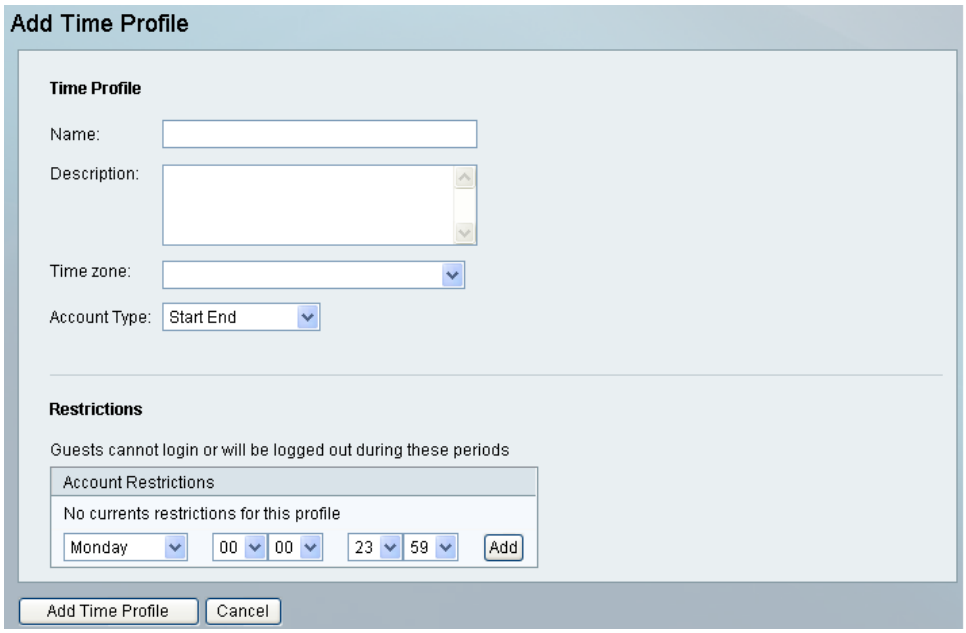
Figure 6-11 Time Profiles



Step 2 Click the **Add Time Profile** button to add a new Time Profile.

Step 3 From the Add Time Profile page as shown in Figure 6-12, type the **Name** and **Description** of the new time profile.

Figure 6-12 Add Time Profile Page



Step 4 From the **Timezone** dropdown menu, specify the timezone for which any Account Restrictions will apply.

Note The **Timezone** function is only available starting from version 2.0.1 and later. In version 2.0.0, the account restrictions are determined by the timezone set on the Date/Time settings in the Server configurations.

Step 5 From the **Account Type** dropdown menu, you can choose one of the predefined options:

- **Start End**—Allows sponsors to define start and end times for account durations.
- **From First Login—**Allows sponsors to define a length of time for guest access from their first login.
- **From Creation** - Allows sponsors to define a length of time for guest access from the moment of account creation.

Note The **From Creation** option is only available starting from version 2.0.1 and later.

- **Time Used**—Allows sponsors to create a time period during which the guest can login. For example, account can be valid for 2 hours and usable for any time within 24 hours from first login.

Step 6 Depending on the Account Type selected, enter the duration in the following fields:

- **Start End**—Allows sponsors to define start and end times for account durations; therefore, no duration is necessary.
- **From First Login—**Allows sponsors to define a length of time for guest access from their first login. Duration in days is required.
- **From Creation** - Allows sponsors to define a length of time for guest access from the moment of account creation.

Note The **From Creation** option is only available starting from version 2.0.1 and later.

- **Time Used**—Allows sponsors to create a time period during which the guest can login. For example account can be valid for 2 hours and usable for any time within 24 hours from first login. You need to specify how long the sponsor can allocate a guest account for, and the time frame in which it must end.
- Click the **Save** button to save.

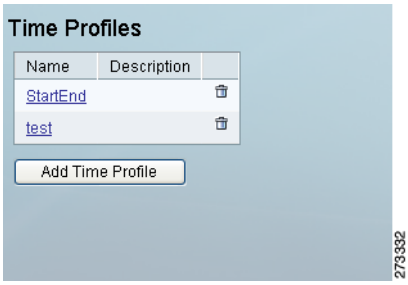
Step 7 Once a Time Profile is created, you can implement Account Restrictions in the **Restrictions** section. Use the dropdown menus to select the days and time you wish to restrict guest access to and from. Once a time criteria is complete, click **Add**, then create the next restriction.

Editing Time Profiles

The following steps describe how to edit Time Profiles.

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

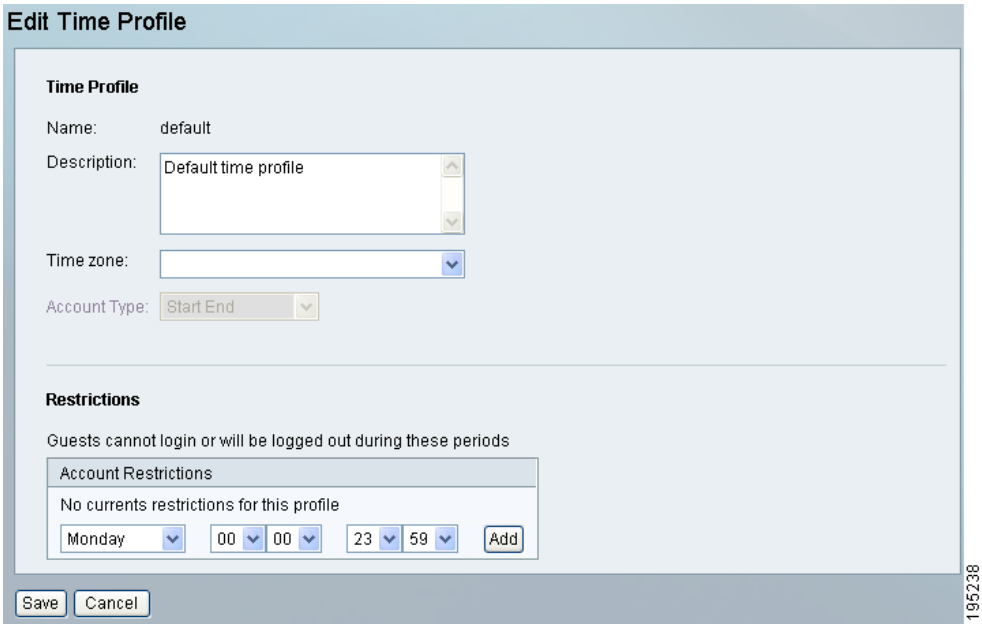
Figure 6-13 Editing a Time Profile



Step 2 Select the time profile you wish to edit and click the underlined name of that role as shown in Figure 6-13.

Step 3 From the Edit Time Profile page as shown in Figure 6-14, you can edit the **Name** and **Description** of that profile.

Figure 6-14 Edit Time Profile



Step 4 From the **Timezone** dropdown menu, specify the timezone for which any Account Restrictions will apply.

Note The **Timezone** function is only available starting from version 2.0.1 and later. In version 2.0.0, the account restrictions are determined by the timezone set on the Date/Time settings in the Server configurations.

Step 5 From the **Account Type** dropdown menu, you can choose one of three predefined options:

- **Start End**—Allows sponsors to define start and end times for account durations.
- **From First Login—**Allows sponsors to define a length of time for guest access from their first login.
- **From Creation** - Allows sponsors to define a length of time for guest access from the moment of account creation.

Note The **From Creation** option is only available starting from version 2.0.1 and later.

- **Time Used**—Allows sponsors to create a time period during which the guest can login. For example account can be valid for 2 hours and usable for any time within 24 hours from first login.

Step 6 Depending on the Account Type selected, enter the duration in the following fields:

- **Start End**—Allows sponsors to define start and end times for account durations; therefore, no duration is necessary.
- **From First Login—**Allows sponsors to define a length of time for guest access from their first login. Duration in days is required.
- **From Creation** - Allows sponsors to define a length of time for guest access from the moment of account creation.

Note The **From Creation** option is only available starting from version 2.0.1 and later.

- **Time Used**—Allows sponsors to create a time period during which the guest can login. For example, account can be valid for 2 hours and usable for any time within 24 hours from first login. You need to specify how long the sponsor can allocate a guest account for, and the time frame in which it must end.
- Click the **Save** button to save.

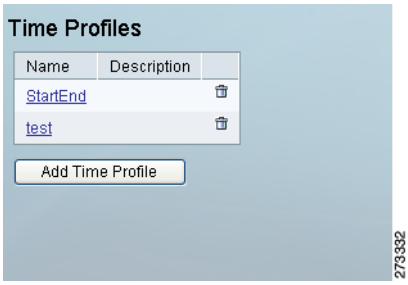
Step 7 Once a Time Profile is created, you can implement Account Restrictions in the **Restrictions** section. Use the dropdown menus to select the days and times you wish to restrict guest access to and from. Once a time criteria is complete, click **Add**, then create the next restriction.

Deleting Time Profiles

The following steps describe how to delete Time Profiles.

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

Figure 6-15 Deleting a Time Profile



Step 2 From the **Time Profiles** page as shown in Figure 6-15, choose the profile you wish to delete and click the bin icon.

Step 3 Confirm the deletion when prompted.

Note Only time profiles that have never been used to create guest accounts can be deleted. The used time profiles cannot be deleted as they are required for audit purposes.

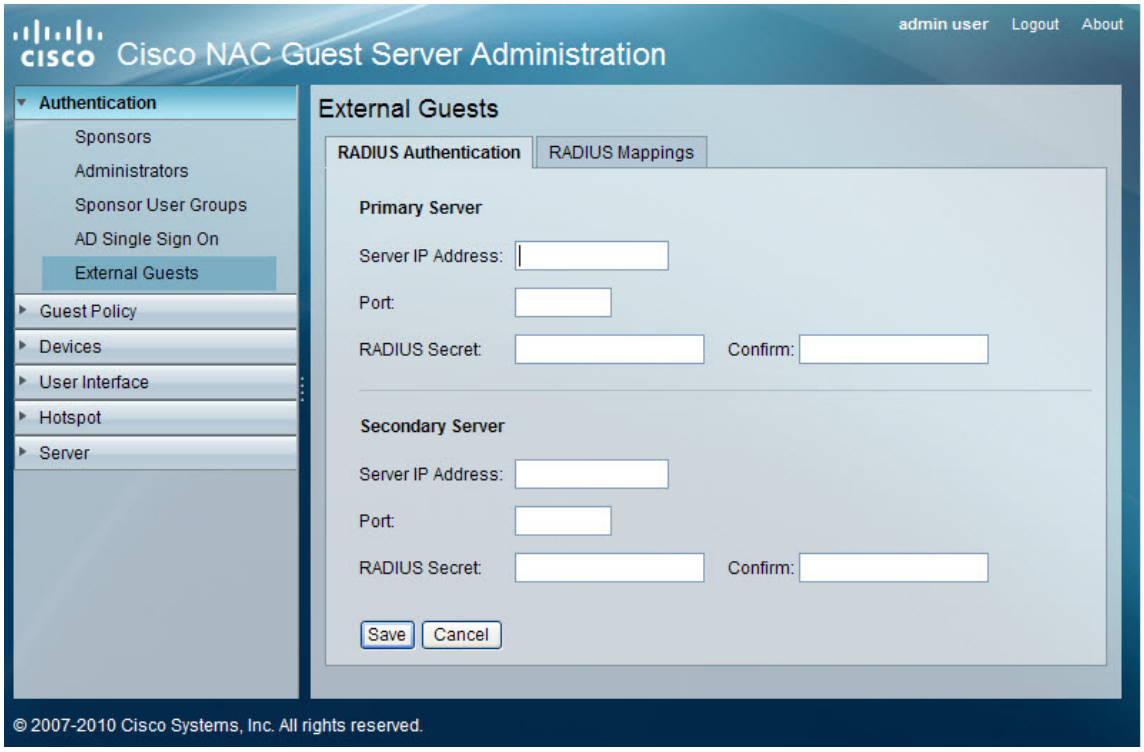
External Guest Authentication

RADIUS authentication authenticates guest users to the Cisco NAC Guest Server using their existing RADIUS user accounts. The guests do not need to have another set of user names and passwords to authenticate to the Guest Server. RADIUS authentication also enables guests to quickly roll out and create their own Guest Access because there is no need to involve a sponsor to create the local guest accounts.

Step 1 From the administration interface, select **Authentication > External Guests**.

Step 2 Click the **RADIUS Authentication** tab as shown in Figure 6-16.

Figure 6-16 RADIUS Authentication



Step 3 Type the **Server IP Address** for the Primary RADIUS Server.

Step 4 Type the **Port** that RADIUS authentication is running on for that server (default is 1645 or 1812).

Step 5 Type the shared secret to be used between the RADIUS Server and the NAC Guest Server, in the **RADIUS Secret** field.

Step 6 Confirm the secret to make sure that it is set correctly.

Step 7 Enter details for a Secondary RADIUS Server. These details are used when the NAC Guest Server does not receive response from the Primary RADIUS Server. These fields are optional.

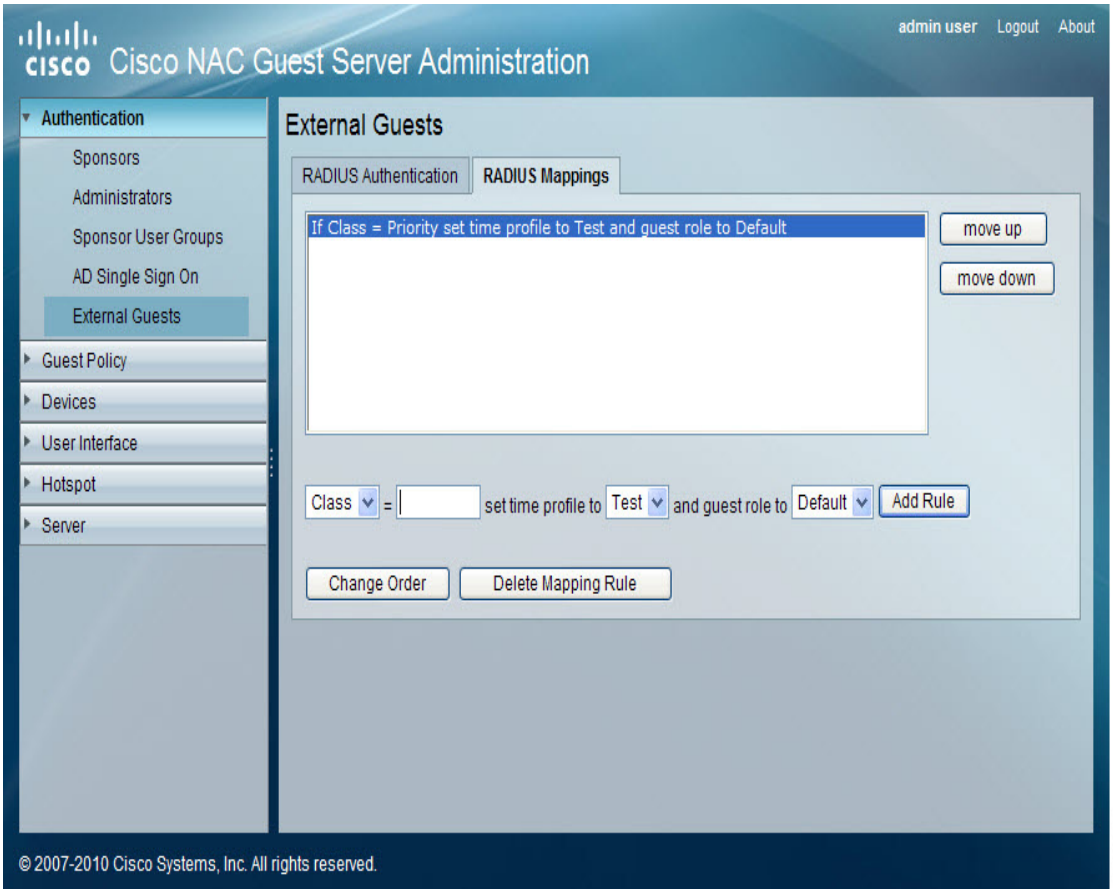
Step 8 Click **Save** to save the Administrator RADIUS settings.

You can now enter RADIUS mappings required.

Step 1 From the administration interface, select **Authentication > External Guests**.

Step 2 Click the **RADIUS Mappings** tab as shown in Figure 6-17.

Figure 6-17 RADIUS Mapping



Step 3 You can enter RADIUS mapping in the blank field and by using the drop down menus that have pre-defined text in them. The text within the drop down menu relates to time profiles and guest roles that have been previously created by the Administrator on the NAC Guest Server.

Note External Guest Authentication supports only the **From First Login** time profile.

Step 4 Once a rule has been created, click the **Add Rule** button to apply.

Step 5 You can change the order of the rules by selecting and highlighting rules and then clicking the **move up** and **move down** buttons. Click **Change Order** button to apply the changes.