CHAPTER 7

Integrating with Cisco NAC Appliance

This chapter describes the following:

- Adding Clean Access Manager Entries
- Editing Clean Access Manager Entries
- Deleting Clean Access Manager Entries
- Configuring the CAM for Reporting

Guest users commonly authenticate to networks via a captive portal through which they provide their authentication details using a web browser. Cisco NAC Appliance provides a secure guest user access portal which administrators can customize.

The Cisco NAC Guest Server integrates with the Clean Access Manager through the use of the Cisco NAC Appliance API. This is an HTTPS-based API that requires the Guest Server to communicate with the Clean Access Manager, also known as the Clean Access Manager (CAM).

Note Refer to the "API Support" section of the applicable *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* for details on the Cisco NAC Appliance API.

The Cisco NAC Guest Server creates the guest user accounts on the CAM as Local User accounts assigned to a specific role that you define for guest users. The Guest Server creates new accounts that are valid every minute. Every minute it also removes accounts that have expired. When accounts are suspended, the Guest Server removes both the accounts from the CAM and the guest users from the network if they are logged in.

The Clean Access Manager can also send accounting information to the Cisco NAC Guest Server via RADIUS accounting. This information is used for reporting and tracking of guests by access time and IP address.

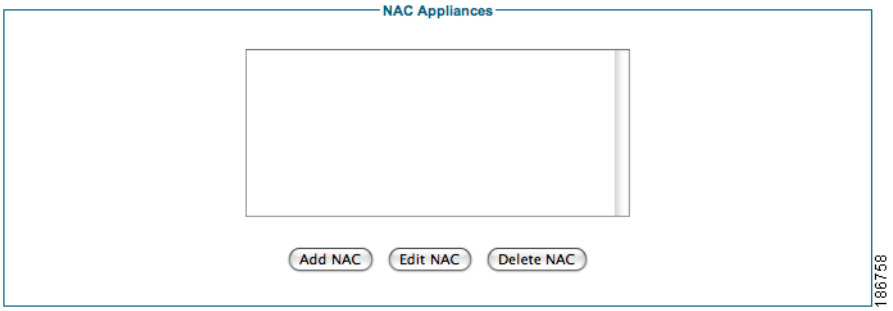
You may add multiple Clean Access Managers to the Cisco NAC Guest Server. When accounts are provisioned they are created on all active Clean Access Managers that are defined.

Adding Clean Access Manager Entries

The following steps describe how to configure the Cisco NAC Guest Server and Cisco NAC Appliance Manager so that they can communicate with one another. You must add API information to the Cisco NAC Guest Server for each Clean Access Manager on which you want the Guest Server to create accounts.

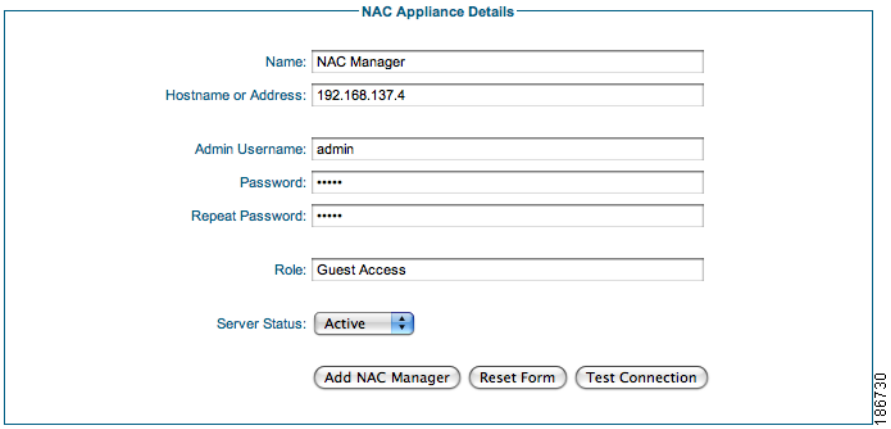
Step 1 From the Guest Server administration interface, select **Devices > NAC Appliance** from the left hand menu (Figure 7-1).

Figure 7-1 Cisco NAC Appliances



Step 2 Click the **Add NAC** button (Figure 7-2).

Figure 7-2 Add Clean Access Manager



Step 3 Enter the following settings in the Cisco NAC Appliance Details page (Figure 7-2):

- Name—Type a descriptive name for the Clean Access Manager.
- Hostname of Address—Type the DNS name or IP address for the CAM.
- Admin Username—Enter an admin username which has API permission to the CAM.
- Password—Type the password for the account.
- Repeat Password—Retype the password to ensure it matches correctly.
- Role—Type the name of the User Role on the CAM to which you will assign guest users. This should match exactly with the User Role name configured on the CAM, including correct case.
- Server Status—Set the status to be Active for the CAM to have accounts provisioned on it by the Cisco NAC Guest Server.

Step 4 Click the **Add NAC Manager** button.

Step 5 Optionally click the **Test Connection** button to ensure that the settings are working correctly.

Step 6 In the Clean Access Manager admin console, navigate to **Monitoring > Event Logs** and verify that the account nacguest_test was successfully created and then deleted.

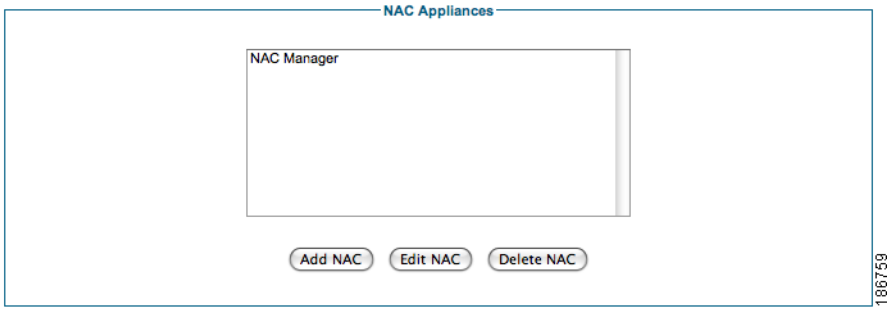
Note Clean Access Managers are automatically added to the **Default** guest role, and set to provision using the role name specified here. If you do not want the Clean Access Manager to be added to the role, you must manually remove the entry.

Editing Clean Access Manager Entries

The following steps describe how to edit an existing entry for a Clean Access Manager.

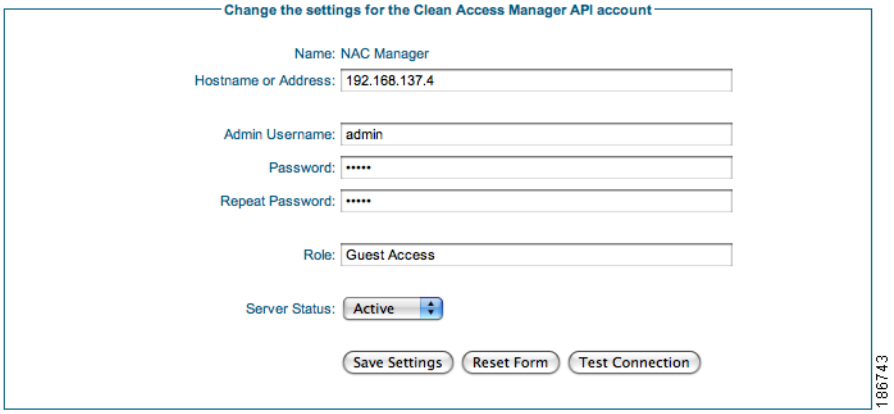
Step 1 From the Guest Server administration interface, select **Devices > NAC Appliance** from the left hand menu (Figure 7-3).

Figure 7-3 List of Cisco NAC Appliances



Step 2 Select the Cisco NAC Appliance that you want to edit from the list and click the **Edit NAC** button (Figure 7-4).

Figure 7-4 Edit a Clean Access Manager



Step 3 In the Cisco NAC Appliance Settings page (Figure 7-4), enter the following settings:

- Hostname of Address—Type the DNS name or IP address for the CAM.
- Admin Username—Enter an admin username which has API permission to the CAM.
- Password—Type the password for the account.
- Repeat Password—Retype the password to ensure it matches correctly.
- Role—Type the name of the User Role on the CAM to which you will assign guest users. This should match exactly with the User Role name configured on the CAM, including correct case.
- Server Status—Set the status to be Active for the CAM to have accounts provisioned on it by the Cisco NAC Guest Server.

Step 4 Click the **Save Settings** button.

Step 5 Optionally click the **Test Connection** button to ensure that the settings are working correctly.

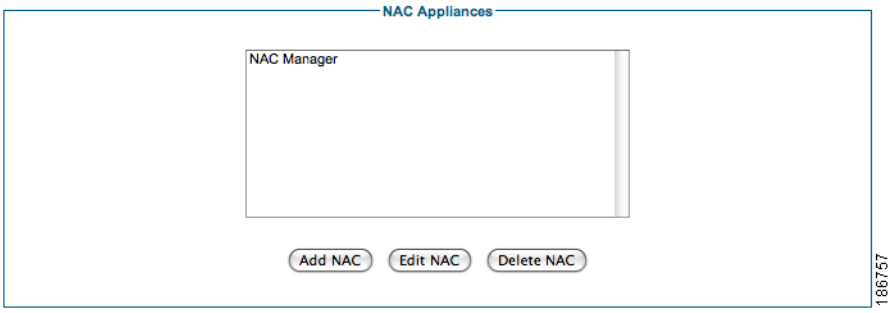
Step 6 In the Clean Access Manager admin console, navigate to **Monitoring > Event Logs** and verify that the account nacguest_test was successfully created and then deleted.

Deleting Clean Access Manager Entries

The following steps describe how to delete Cisco NAC Appliance entries.

Step 1 From the Guest Server administration interface, select **Devices > NAC Appliance** from the left hand menu (Figure 7-5).

Figure 7-5 List of Cisco NAC Appliances



Step 2 Select the Cisco NAC Appliance that you want to delete from the list and click the **Delete NAC** button. You will receive a warning message which you must agree to for the appliance entry to be deleted.

Configuring the CAM for Reporting

In order for the Cisco NAC Guest Server to correctly display details for guest users when reporting is run, you need to configure the CAM to send RADIUS accounting information to the Guest Server. Additionally, the CAM needs to format the information correctly.

Note For detailed instructions on how to access and configure settings on the CAM, refer to the applicable *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide.*

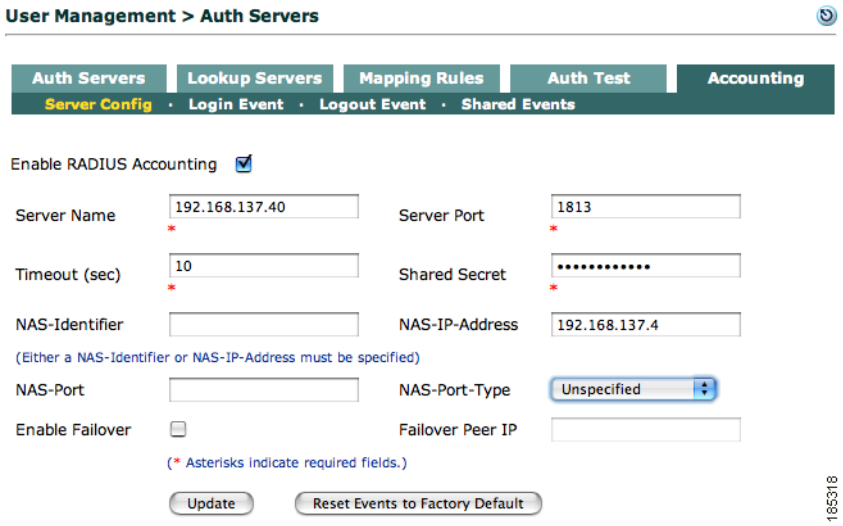
Adding a RADIUS Accounting Server

Step 1 Log into the CAM web console as an admin user with an appropriate password (default username/password is **admin/cisco123**).

Note Any CAM admin user with Edit privileges can perform this configuration.

Step 2 Navigate to **User Management > Auth Servers > Accounting > Server Config**

Figure 7-6 Configure RADIUS Accounting Server



Step 3 Click the checkbox for **Enable RADIUS Accounting** and configure the following fields:

- Server Name— Type the IP address of the Cisco NAC Guest Server
- Server Port —Type 1813 as the port
- Timeout (sec)—Type a timeout value; 10 seconds is typically sufficient.
- Shared Secret—Type the shared secret used with the Cisco NAC Guest Server. This must match the shared secret configured on the Guest Server when adding the CAM as a RADIUS client to the Guest Server, as described in Adding RADIUS Clients, page 8-2. Make sure both shared secrets are the same.
- NAS-IP-Address—Type the address of the CAM itself as the NAS-IP-Address.

Step 4 Click the **Update** button.

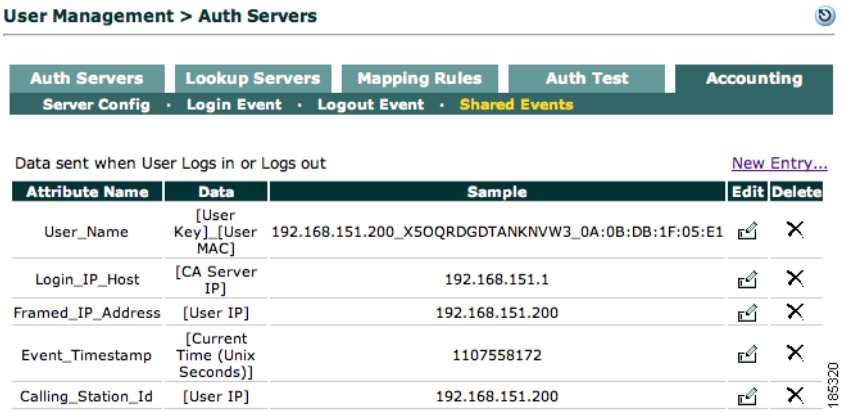
Configure the CAM to Format RADIUS Accounting Data

The CAM can be configured to place many different attributes into the RADIUS accounting packets and the attributes themselves can be formatted in many different ways. You need to configure the CAM to send attribute information in a specific format so that the Cisco NAC Guest Server can understand it.

Note Refer to the "RADIUS Accounting" section of the applicable *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* for additional details.

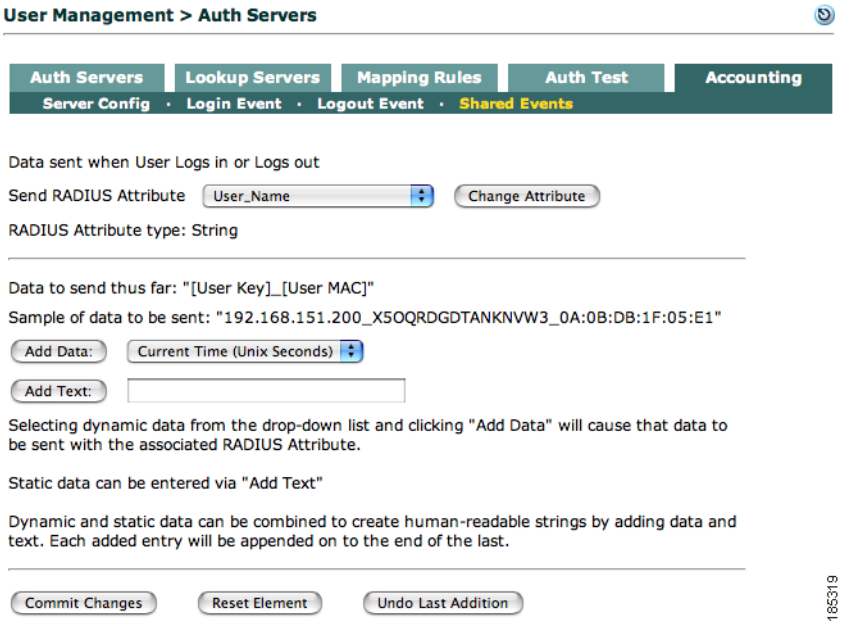
Step 1 Log into the CAM admin console, and navigate to **User Management > Auth Servers > Accounting > Shared Events** (Figure 7-7).

Figure 7-7 Shared Events



Step 2 On the Shared Events page, click the **Edit** button to the right of the User_Name attributes entry

Figure 7-8 Edit User Name Attribute



Step 3 In the Edit User_Name attribute page (Figure 7-8), click the **Reset Element** button to remove the existing sample data format.

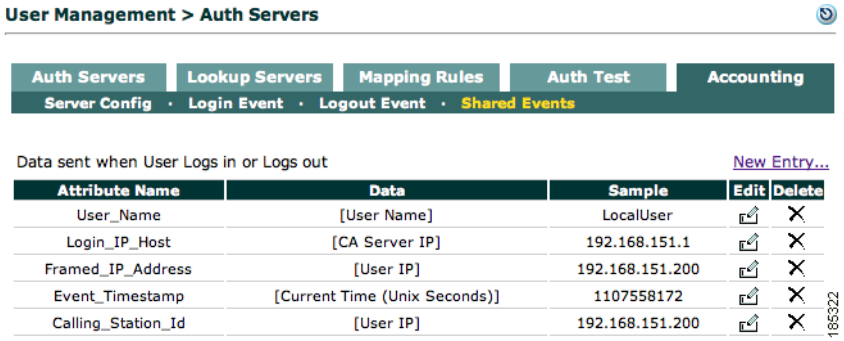
Step 4 Select **User Name** from the Add Data dropdown menu.

Step 5 Click the **Add Data** button.

Step 6 Click the **Commit Changes** button.

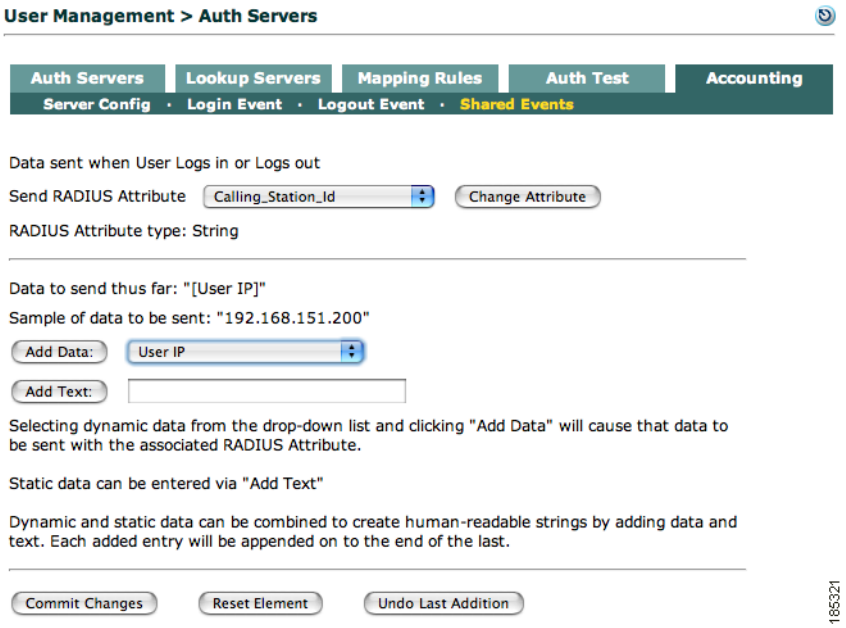
Step 7 The main Shared Events lists page reappears (Figure 7-9). Verify that the Data column lists "[User_Name]".

Figure 7-9 Shared Events with Username Changed



Step 8 Click the **New Entry...** link to the right of the page (Figure 7-9) to add additional attributes.

Figure 7-10 Add Calling Station Id Attribute



Step 9 In the New Shared Events attribute form (Figure 7-10), select **Calling_Station_Id** from the Send RADIUS Attributes dropdown menu.

Step 10 Click the **Change Attribute** button.

Step 11 Select **User IP** from the Add Data dropdown menu.

Step 12 Click the **Add Data** button.

Step 13 Click **Commit Changes**.

Note Remember to add the CAM as a RADIUS client using the instructions in Chapter 8, "Configuring RADIUS Clients."