CHAPTER 16

Using the Administrator User Interface

This chapter describes the administration tasks performed from the Cisco Broadband Access Center (BAC) administrator user interface. These tasks mainly involve monitoring the actions of various Cisco BAC components and include:

- User Management, page 16-1
- Device Management, page 16-4
- Group Management, page 16-18
- Viewing Servers, page 16-22

Note The procedures described in this chapter are presented in a tutorial manner. Wherever possible, examples are included to illustrate the possible results of each procedure.
For details on server configurations, see Configuring Broadband Access Center, page 17-1.

User Management

Managing users involves adding, modifying, and deleting users who administer Cisco BAC. Depending on your user type, you can use this menu to add, modify, and delete users. This menu displays all users configured to use Cisco BAC and identifies their user types.

There are three types of Cisco BAC users: an Administrator, a Read/Write user, and a Read-Only user. Each has different levels of access, with unique permissions to ensure access control and the integrity of provisioning data.

The assigned user type appears near the top right corner of every screen on the administrator user interface.

Administrator

Cisco BAC recognizes only one administrator and allows this user to view, add, modify, delete device data, and create other users. As an Administrator, you can also change other users' permissions from Read/Write to Read Only, and vice-versa. In addition, you have the ability to change the passwords of any other user type.

You cannot delete the "Administrator" user.

Read/Write User

As a Read/Write user, you can perform the same functions as the administrator except creating other users, changing the user types of others, or changing their passwords. Read/Write users can change their own password.

Read-Only User

As a Read-Only user, you have basic access including the ability to change your password and to view, but not change, device data. You cannot perform any action that is considered disruptive. You cannot, for example, perform reset or regenerate instructions.

This section contains instructions for managing Cisco BAC users including:

- Adding a New User
- Modifying Users
- Deleting Users

Note You can add and delete users only if you are logged in as the Administrator.

Adding a New User

Adding a new user is a simple process of entering the user's name and creating a password. However, while creating a new user you do have to determine which type of user it will be: a Read/Write user or a Read-Only user. Cisco BAC comes with one Administrator user already created; you cannot create an Administrator as a new user.

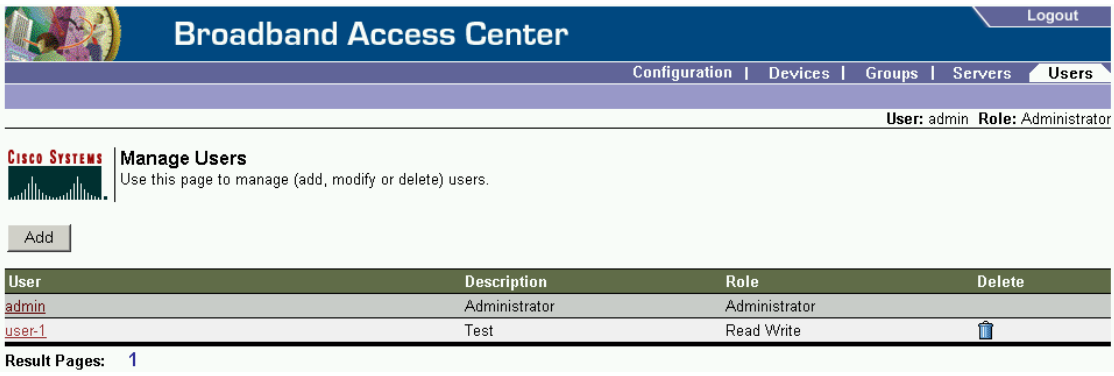
To add a new user:

Step 1 Click **Users**, from the Main Menu or the Primary Navigation bar.

The Manage Users page appears. (See Figure 16-1.)

Step 2 Click **Add** to display the Add User page.

Figure 16-1 Manage Users Page



Step 3 Enter the new user's username and a password.

Step 4 Confirm the new user's password, and select whether the new user's role is to be read only or read/write. See User Management, page 16-1, for complete descriptions of each user type.

Step 5 Enter a short description of the new user.

Tip Use the description field to identify the user's job or position, something that identifies the unique aspects of the new user.

Step 6 Click **Submit**.

The Manage Users page appears with the new user added.

Note The new user's password must be recorded and stored in a safe place. This helps prevent loss or theft of the password and possible unauthorized entry.

Modifying Users

Although any user type can modify their password and user description, only the administrator can modify any other user's information.

To modify user properties:

Step 1 From the Main Menu or the Primary Navigation bar, click **Users.**

The Manage User page appears.

Step 2 Click the correct user name to display the Modify User page for that user.

Step 3 Make the necessary changes to the password, user type (provided that you are logged in as the Administrator), and the user's description.

Step 4 Click **Submit**.

The Manage Users page appears with the modified user information.

Deleting Users

Only the administrator can delete any other user that appears in the Manage Users page. You cannot delete the default user, called **bacadmin**.

To delete a user:

Step 1 From the Main menu or the Primary Navigation bar, click **Users.**

The Manage User page appears.

Step 2 Click the **Delete** icon ( ) corresponding to the user you want to delete.

Step 3 The Delete User dialog box appears. Click **OK**.

The Manage Users page appears without the deleted user.

Device Management

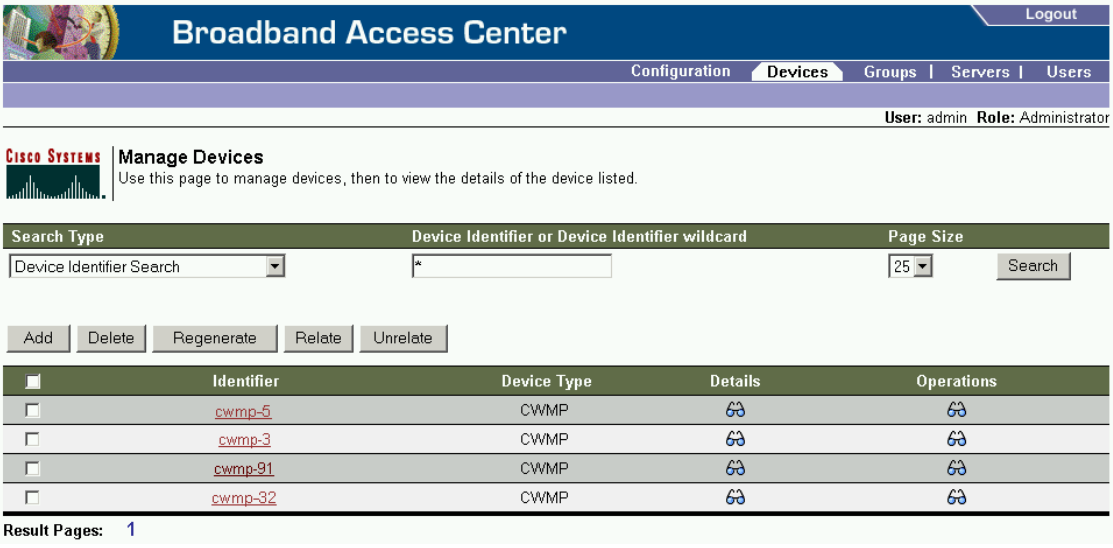
Use the Devices menu to provision and manage TR-069-enabled devices. You can:

- Search for a specific device or for a group of devices that share criteria that you specify. See Searching for Devices, page 16-5.
- Add, modify, or delete devices in the RDU database. See:
  - Adding Device Records, page 16-11
  - Deleting Device Records, page 16-11
- View device data, such as configuration, properties, discovered data, and faults. See Viewing Device Details, page 16-7.
- Regenerate device instructions. See Regenerating Device Instructions, page 16-12.
- Relate and unrelate any device to a specific group. See Relating and Unrelating Devices, page 16-13.
- Enable device troubleshooting. See Configuring Device Troubleshooting, page 8-10.
- Perform various operations, such as an IP Ping, and live data retrieval, on the device to gain more insight. See Performing Operations on Device, page 16-14.

Manage Devices Page

The Manage Devices page appears when you click **Devices** on the Main menu or the Primary Navigation bar. This page, shown in Figure 16-2, contains the fields and controls necessary to perform all device management functions.

Figure 16-2 Manage Devices Page



Searching for Devices

By using Cisco BAC, you can search for device information in a number of different ways.

To select the search type, from the Manage Devices page, click the Search Type drop-down list. Subsequent search pages contain screen components that may be unique to the search type selected.

The Manage Device page utilizes two separate but related areas to generate search results that let you perform many device management functions. These areas are the Search Type drop-down list, which defines which search to perform, and search value field, which qualifies the search type. You can perform these searches:

- Device Identifier Search—Searches by using the device ID. This search function supports wildcard searching at the end of the search string. You can also look up a single device by providing a complete device ID of a specific device.
- FQDN Search—Searches by using the fully qualified domain name (FQDN) associated with the device.
- Group Search—Searches devices which are part of a particular group.
- Owner ID search—Searches by using the owner ID associated with the device. The owner ID may identify the service subscriber's account number, for example. This search function does not support wildcard searching.
- Registered Class of Service Search—Searches by using the Class of Service that a device has been provisioned with.
- Related Class of Service Search—Searches by using both the registered and selected Class of Service.
- Selected Class of Service Search—Searches by using the Class of Service selected by the RDU for a device that, for one reason or another, cannot retain its registered Class of Service.

Some searches that you can perform allow the use of a wildcard character (*) to enhance the search function. Cisco BAC provides specific wildcards for each search, as described in Table 16-1.

Table 16-1 Searches Supported for Device Management

Menu Search	Search Type Options
Device Identifier Search	Full Device Identifier or partial Device Identifier followed by a wildcard asterisk (*) character at the end of the string. For example, to search for a device with the ID 0010BF-ZAA001A00001, you can try 0010BF-*, but searching by using *-ZAA001A00001 does not yield results.
FQDN Search	Full FQDN or partial FQDN string beginning with an wildcard asterisk (*) character. For example, to search for a device with the FQDN IGW-1234.ACME.COM, you can try: • *.acme.com • *.com • *

Table 16-1 Searches Supported for Device Management (continued)

Menu Search	Search Type Options
Group Search	Group Name (Group Type) • Drop-down list Full Device Identifier or partial Device Identifier followed by a wildcard asterisk (*) character at the end of the string.
Owner ID Search	Owner ID Wildcard searches are not supported. You must enter the complete owner ID.
Registered Class of Service Search	Class of Service (Type) • Drop-down box
Related Class of Service Search	Class of Service (Type) • Drop-down box
Selected Class of Service Search	Class of Service (Type) • Drop-down box

In addition, a Page Size drop-down lets you limit the number of search results displayed per page. You can select 25, 50, or 75 results for display. When the number of search results is greater than the selected page size, paging controls appear in the lower left corner of the page. These controls let you scroll forward or backward one page at a time, or to select a specific page.

Note A maximum of 1,000 results are returned for any query, with a maximum of 75 results displayed per page. You can change the default maximum by modifying the /adminui/maxReturned property, in the *BPR_HOME/rdu/conf/adminui.properties* file, and then running the **bprAgent restart tomcat** command (located in the */etc/init.d/* directory) to restart the Cisco BAC Tomcat component.

Device Management Controls

These buttons are located directly below the search function fields and are generally used in conjunction with the search function. For example, you might search for devices belonging to a specific group of devices in order to perform some sort of management function. The following buttons are available, although each management function may not be available depending on the search type used.

Add

The Add button lets you add a new device to the RDU database. See Adding Device Records, page 16-11, for the appropriate instructions.

Delete

The Delete button lets you delete any selected device(s) from the RDU database. See Deleting Device Records, page 16-11, for the appropriate instructions.

Regenerate

Use the Regenerate button to force immediate regeneration of instructions for selected device(s).

Relate

The Relate button lets you associate a device (by using its Device ID) with a specific group (referred to as Node in the API).

Unrelate

The Unrelate button cancels the relationship between a selected device and the group that the device is currently related to.

Searching for devices returns results under the following headings or links that appear on the page:

Identifier

Identifies all devices matching the search criteria. Each of the identifiers displayed has a link to another page from which you can modify the device.

Device Type

Displays the available device type; in this case, CWMP.

Details

Displays all available details for the selected device. See Viewing Device Details, page 16-7, for additional information.

Operations

Displays a drop-down list of available device operations. See Performing Operations on Device, page 16-14, for additional information.

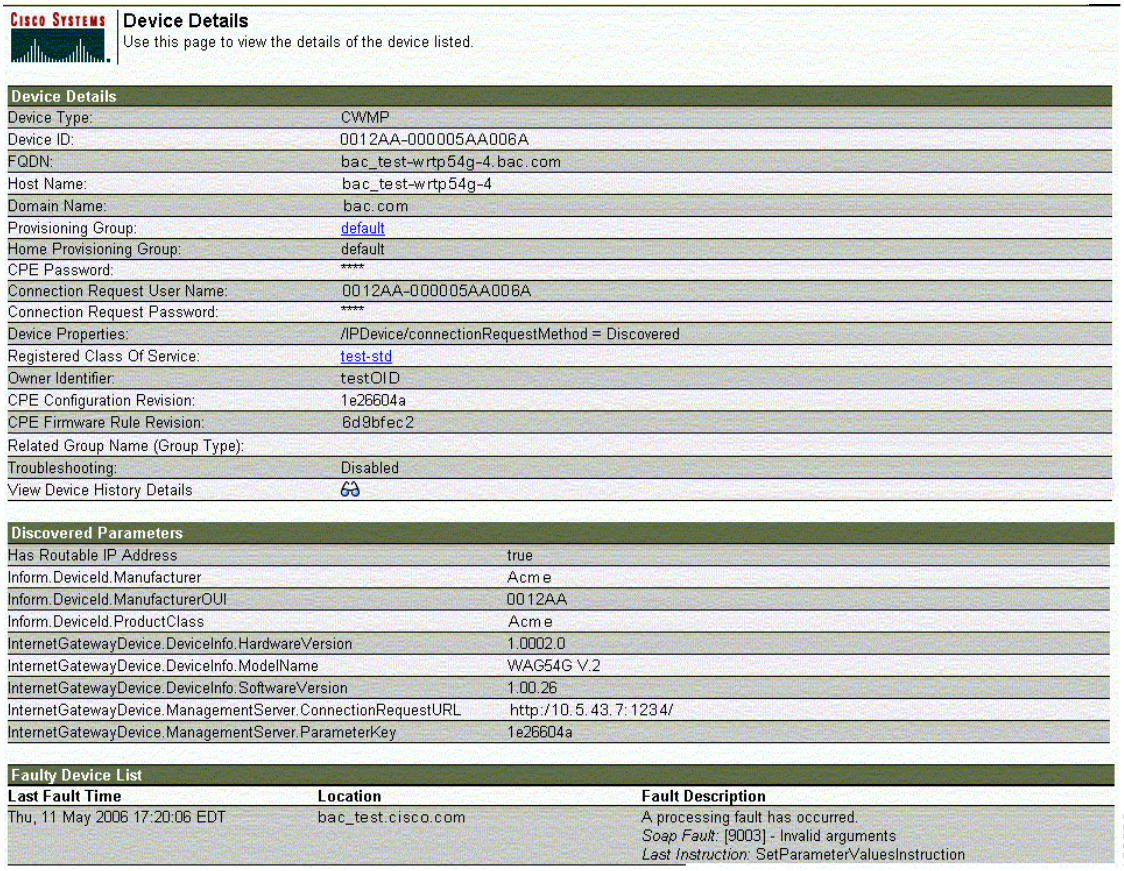
Viewing Device Details

You can view the details of any device identified in the search results.

To view any device details, click the **View Details** icon ( ) corresponding to the device you want to view, and the Device Details page appears.

Figure 16-3 provides a sample Device Details page.

Figure 16-3 Device Details Page



Cisco Systems

Device Details

Use this page to view the details of the device listed.

Device Details	
Device Type:	CWMP
Device ID:	0012AA-000005AA006A
FQDN:	bac_test-wrtp54g-4.bac.com
Host Name:	bac_test-wrtp54g-4
Domain Name:	bac.com
Provisioning Group:	default
Home Provisioning Group:	default
CPE Password:	****
Connection Request User Name:	0012AA-000005AA006A
Connection Request Password:	****
Device Properties:	/IPDevice/connectionRequestMethod = Discovered
Registered Class Of Service:	test-std
Owner Identifier:	testOID
CPE Configuration Revision:	1e26604a
CPE Firmware Rule Revision:	6d9bfec2
Related Group Name (Group Type):	
Troubleshooting:	Disabled
View Device History Details	

Discovered Parameters	
Has Routable IP Address	true
Inform.DeviceId.Manufacturer	Acme
Inform.DeviceId.ManufacturerOUI	0012AA
Inform.DeviceId.ProductClass	Acme
InternetGatewayDevice.DeviceInfo.HardwareVersion	1.0002.0
InternetGatewayDevice.DeviceInfo.ModelName	WAG54G V.2
InternetGatewayDevice.DeviceInfo.SoftwareVersion	1.00.26
InternetGatewayDevice.ManagementServer.ConnectionRequestURL	http://10.5.43.7:1234/
InternetGatewayDevice.ManagementServer.ParameterKey	1e26604a

Faulty Device List

Last Fault Time	Location	Fault Description
Thu, 11 May 2006 17:20:06 EDT	bac_test.cisco.com	A processing fault has occurred. *Soap Fault:* [9003] - Invalid arguments *Last Instruction:* SetParameterValuesInstruction

156329

Table 16-2 identifies the fields shown in Figure 16-3.

Table 16-2 Device Details Page

Field or Button	Description
Device Details	
Device Type	Identifies the device type.
DeviceID	Identifies the device identifier.
FQDN	Identifies the fully qualified domain name for the selected device. For example, IGW-1234.ACME.COM is a fully qualified domain name.
Host Name	Identifies the host. For example, in the FQDN description above, IGW-1234 is the hostname.
Domain Name	Identifies the domain within which the host resides. For example, in the FQDN description above, ACME.COM is the domain name.
Provisioning Group	Identifies the provisioning group to which the device has been pre-assigned or assigned automatically.

Table 16-2 Device Details Page (continued)

Field or Button	Description
Home Provisioning Group	Identifies the provisioning group to which the device should belong.
CPE Password	Identifies the password used to authenticate the device when establishing a connection to Cisco BAC. This password is used only for HTTP-based authentication of the customer premises equipment (CPE). For security purposes, it returns a string with asterisk (*) characters regardless of the actual value unless the password has not been set, in which case an empty value is displayed.
Connection Request User Name	Identifies the username used to authenticate a ConnectionRequest from Cisco BAC to the CPE.
Connection Request Password	Identifies the password used to authenticate a ConnectionRequest from Cisco BAC to the CPE. For security purposes, this parameter returns an empty string regardless of the actual value.
Device Properties	Identifies any properties, other than those that appear on this page, that can be set for this device. This field includes the display of custom properties.
Registered Class of Service	Identifies the Class of Service assigned to this device. If a different Class of Service has been selected for the device by extension, an additional field with Selected Class of Service appears.
Owner Identifier	Identifies the device. This may be a user ID, and account number, or may be blank.
CPE Configuration Revision	Identifies the configuration rules revision number, which is set for the device *ParameterKey* following a successful configuration synchronization.
CPE Firmware Rule Revision	Identifies the firmware rules revision for this CPE.
Related Group Name (Group Type)	Identifies the group(s) name and type to which this device is related. See Group Management, page 16-18, for additional information.
Troubleshooting	Identifies if CPE troubleshooting is enabled or disabled. **Note** If troubleshooting is enabled, a View Troubleshooting Log link appears on this page.
View Device History Details	Provides a link to the history of configuration changes on the CPE.
Discovered Parameters **Note** This section includes any parameters discovered from the device. This section does not appear unless discovered parameters are available for the device. For details on how to configure discovered parameters, see Discovering CPE Parameters, page 4-4.	
Has Routable IP Address	Identifies if a device is generally reachable; that is, if the source IP address of the last request was the same as the WAN IP address reported by the CPE in the Inform message.

Table 16-2 Device Details Page (continued)

Field or Button	Description
Inform.DeviceId.Manufacturer	Identifies the manufacturer of the CPE reported in the last Inform message.
Inform.DeviceId.ManufacturerOUI	Identifies the unique identifier of the manufacturer of the CPE reported in the last Inform message.
Inform.DeviceId.ProductClass	Identifier a manufacturer's product or class of product over which the *SerialNumber* parameter is unique. The device reports this parameter in the Inform message.
InternetGatewayDevice.DeviceInfo.HardwareVersion	Identifies the hardware version of the CPE.
InternetGatewayDevice.DeviceInfo.ModelName	Identifies the model name of the CPE.
InternetGatewayDevice.DeviceInfo.SoftwareVersion	Identifies the software version currently installed on the CPE. The software version is also known as firmware version.
InternetGatewayDevice.ManagementServer.ParameterKey	Specifies the value of the *ParameterKey* reported by the device in the last Inform message or last set by the DPE, whichever occurred last.
Faulty Device List	
Note This information is displayed only if faults occur at the devices. For more information, see Device Faults, page 8-6.	
Last Fault Time	Specifies the date and time that a recurring fault occurred for this device.
Location	Specifies the server on which this fault occurred.
Fault Description	Provides a description of the recurring fault.

Managing Devices

The Devices menu lets you add devices to the RDU databases and update preprovisioned data. Device management includes:

- Adding, deleting, and modifying RDU device records
- Regenerating instructions
- Relating selected devices to management objects, such as Provisioning Group, Class of Service, Group, and so on.
- Executing operations on devices. These operations are actually performed on the device and include:
  - Reboot
  - Request Connection
  - Factory Reset
  - Display Live Data
  - Ping Diagnostic
  - Force Firmware Upgrade
  - Force Configuration Synchronization

For detailed information on these operations, see Performing Operations on Device, page 16-14.

This section describes how to perform the various device management functions on new or existing devices.

Adding Device Records

To add a device record:

Step 1 From the Manage Devices page, click **Add.**

The Add Device page appears.

Step 2 Choose the device type and Class of Service, and complete the other fields on the page.

Step 3 In addition to the fields described earlier in this section, you can optionally add new values for existing property name/value pairs.

- Property Name—Identifies the name of the custom or built-in device property.
- Property Value—Identifies the value of the property.

To add the property, click **Add**.

Step 4 Click **Submit** to add the device, or **Reset** to clear all fields.

Modifying Device Records

To modify a device record:

Step 1 From the Manage Devices page, click the Identifier link corresponding to the correct device.

The Modify Device page appears.

Step 2 Enter the data in the correct field. You can modify any existing property name/value pairs by clicking **Add,** or delete any of them by clicking the **Delete** button.

Step 3 Click **Submit** to save the changes made to this device, or **Reset** to clear all fields.

Deleting Device Records

Deleting device records is a simple process, but one that you should use carefully. To undo the delete, you must restore a previously backed up database or re-add the device.

Note See Database Restore, page 10-6, for additional information if restoration of a backed-up database becomes necessary.

To delete a device record:

Step 1 From the Manage Devices page, locate the device that you want to delete. You can use one of the search types for this purpose.

Step 2 Click the check box to the left of the correct device.

Step 3 Click **Delete**.

The device record stored in the RDU database is removed.

Viewing Device History

To view the history of a device configuration:

Step 1 From the Manage Devices page, locate the device whose history you want to view. You can use one of the search types for this purpose.

Step 2 Click the **View Details** icon corresponding to the device.

The Device Details page appears.

Step 3 Against View Device History Details, click the **View Details** icon.

The Device History Details page appears.

Regenerating Device Instructions

The Regenerate button or API operation force immediate regeneration of instructions for the device. These instructions are sent to the DPEs in the device's provisioning group. Normally, the process of regenerating the instruction is automatically triggered following changes to device, Class of Service, or other such impacting changes. However, after a change to a Class of Service, the system takes time to regenerate instructions for all devices. This button can be used to expedite regeneration of instructions for a given device. This may be desirable during proactive troubleshooting.

Device instructions are automatically regenerated whenever:

- A file related to a Class of Service, that is, a template, is updated.
- The default Class of Service for a device type is changed.
- The provisioning group object is changed via the administrator user interface or the API.
- The Class of Service object properties are changed.
- The DPE sends a configuration regeneration request to the RDU.
- The device properties or relationship is updated.

Some instructions cannot be automatically regenerated because the Cisco BAC system cannot determine if the change impacts device instructions. In such cases, you must manually regenerate instructions by using the `generationConfiguration()` method or the administrator user interface. Instructions that must be manually regenerated are those that become necessary whenever:

- A technology default is changed.
- The system defaults are changed.

Note Regardless of how instructions are regenerated, they are not propagated to the devices until the device configuration is activated, that is, the device contacts the DPE either on schedule or as a result of a connection request initiated from the DPE.

Relating and Unrelating Devices

You can define any number of arbitrary groups. The Relate function lets you associate a device to a specific group, which is in turn associated with a specific group type.

Relating a Device to a Group

Note You can relate devices to group(s) only one by one via the administrator user interface.

To relate a device to a group:

Step 1 From the Manage Devices page, locate the device which you want to relate to a group. You can use one of the search types for this purpose.

Step 2 Check the check box corresponding to the device Identifier, and click the **Relate** button.

The Relate Device to Group(s) page appears.

Step 3 Select the Group Type from the drop-down list and the Group(s) from the list of defined groups.

Note To select multiple groups from the Group list, press **Control** or **Shift**.

Step 4 Click **Submit**.

The Manage Devices page appears.

Note To verify if the device has been added to the group, click the **View Details** icon corresponding to the device. On the Device Details page that appears, check the status against Related Group Name (Group Type).

Unrelating a Device from a Group

Note You can relate devices to group(s) only one by one via the administrator user interface.

To unrelate a device to a group:

Step 1 From the Manage Devices page, locate the device which you want to unrelate from a group.

Step 2 Check the check box corresponding to the device Identifier, and click the **Unrelate** button.

The Unrelate Device from Group page appears.

Step 3 From the list of defined Group(s), select the group(s) from which you want to unrelate the device.

Note To select multiple groups from the Group list, press **Control** or **Shift**.

Step 4 Click **Submit**.

The Manage Devices page appears.

Searching Device(s) in a Group

To search for device(s) belonging to a particular group:

Step 1 From the Manage Devices page, select the Group Search option from the drop-down list under Search Type.

The Group Name (Group Type) and the Device Identifier options appear.

Step 2 From the Group Name (Group Type) drop-down list, select the Group Name of the device(s) which you want to search.

Step 3 Enter a device ID in the Device Identifier field, or use a wildcard (*).

Step 4 Click **Search**.

The device(s) related to the group appears.

Performing Operations on Device

You can perform the following functions from the Device Operations page:

- Reboot—Enables you to reboot the device. This operation is primarily intended for diagnostic purposes.
- Request Connection—Instructs the device to establish a CWMP session with Cisco BAC.
- Factory Reset—Enables you to reset a preregistered device settings to its original factory settings.
- Display Live Data—Enables you to view live device parameter values.

  You can choose the parameters that you want to view for this device operation by selecting from the options under the Parameter List File drop-down box. Each parameter list is an XML file that details the parameters each file will return; click the **View Details** icon to view the parameters.

  You can also define the parameters that you want to be retrieved in parameter lists. Cisco BAC provides a sample list of live data templates which specify various parameters to be read during a view live data query.
- Ping Diagnostic—Enables you to perform an IP ping diagnostics test from the device to any host.

Note For all of the above operations, if the device is not reachable, an error message appears.

- Force Firmware Upgrade—Enables you to force a device to update its firmware on next contact regardless of the MaintenanceWindow restrictions set in the firmware rules.
- Force Configuration Synchronization—Enables you to force an individual device to synchronize its configuration regardless of the current configuration version on the device.

Note The operations forcing a firmware upgrade or a configuration synchronization take effect on the next device contact with the autoconfiguration server (ACS).

Performing a Reboot

To reboot the device:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon ( ) corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select Reboot.

Step 4 Click **Submit**.

Performing a Request Connection

To force the device to initiate a connection request:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select Request Connection.

Step 4 Click **Submit**.

Performing a Factory Reset

To reset device settings to its original factory settings:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select Factory Reset.

Step 4 Click **Submit**.

Displaying Live Data

To display parameters from a device:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select Display Live Data.

Step 4 Enter a duration in seconds for the operation to time out. The default timeout is 90 seconds.

Step 5 From the Parameter List File drop-down list, select the file, each of which is an XML file that details the parameters that are returned. Click on the **View Details** icon to view the parameters.

Note You can also view these sample templates under the **Configuration > Files** tabs. From the View Files page, select the Parameter List option under the File Type drop-down list. Click **Search**. A list of sample parameter list files appears.

Step 6 Click **Submit**.

Note If the device is not reachable, an error message appears.

Performing a Ping Diagnostic

To perform a ping operation to a device by using its IP address:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select Ping Diagnostic.

Step 4 Enter values in the following fields:

- Device operation timeout (in seconds)—Specifies the duration after which the Ping operation times out.
- Name of the hostname to be pinged—Identifies the hostname of the CPE to be pinged.
- Interface—Identifies the WAN interface from which the Ping should originate on the CPE.
- Number of repetitions—Specifies the number of times the Ping operation should run.
- Time out—Specifies the timeout for the Ping packet.
- Data block size—Specifies the size of each Ping packet.
- DSCP—Specifies the DSCP value in each Ping packet.

Step 5 Click **Submit**.

Forcing a Firmware Upgrade

To force a firmware upgrade on a device on next contact and bypassing the MaintenanceWindow restrictions set in the firmware rules:

Step 1 From the **Devices > Manage Devices** page, locate the device whose configuration you want to synchronize.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Perform Device Operation, select Force Firmware Upgrade.

Step 4 Click **Submit**.

Forcing a Configuration Synchronization

To force a device to synchronize its configuration on next contact with the DPE regardless of the current configuration version on the device:

Step 1 From the **Devices > Manage Devices** page, locate the device whose configuration you want to synchronize.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Perform Device Operation, select Force Configuration Synchronization.

Step 4 Click **Submit**.

The device configuration is synchronized with the DPE.

Setting Device Operations Timeout

You can set the duration within which an operation is to be executed on device. After that period, the operation times out.

Note In addition to the procedure described in this section, you can set the default timeout duration in the Device Operation Timeout field via **Configuration > Defaults > CWMP Defaults**.

To set the timeout value for a device operation:

Step 1 From the **Devices > Manage Devices** page, locate the correct device.

Step 2 Click the **Operations** icon corresponding to the device.

The Device Operations page appears.

Step 3 From the drop-down list under Device Operation, select the operation you want to perform.

Step 4 Enter a value (in seconds) in the Device Operation Timeout field. The default value for a device operation to time out is 90 seconds.

Step 5 Click **Submit**.

Group Management

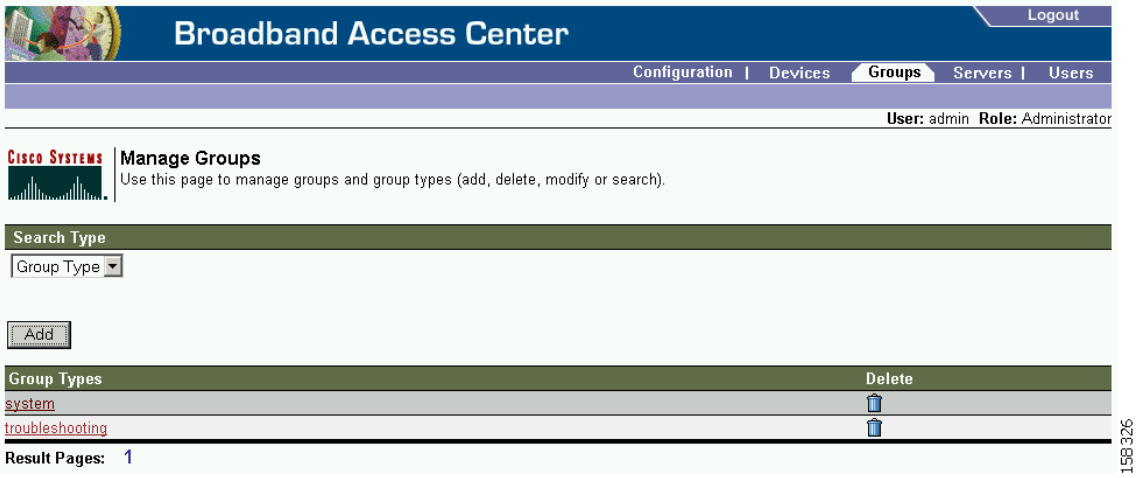
Group management allows the creation, modification, and deletion of groups and group types.

Note Group priorities in the property hierarchy (see Property Hierarchy, page 4-4) are handled through group types.

Managing Group Types

Access the Manage Groups page (shown in Figure 16-4) by selecting Groups from either the main menu or the primary menu bar. Group Type is the default setting when this page appears.

Figure 16-4 Manage Groups Page



Adding a Group Type

To add a new group type:

Step 1 Click the **Groups** tab to open the Manage Groups page.

Step 2 Change the **Search Type** to Group Type.

Step 3 Click **Add** to open the Add Group Type page. (See Figure 16-5.)

Figure 16-5 Add Group Type Page

Step 4 Enter a name for the group type.

Step 5 Enter the priority value for the group type.

The value can range from 1 through 100, with 1 as the highest priority. For example, if the priority values of two member groups are 5 and 20, respectively, then the group with priority value 5 has more priority than the group with priority value 20.

The Group Type Priority is, by default, set to 50.

If two member groups have the same priority value, the group type names are sorted in alphabetical order to decide the priority. If this results in two member groups with the same priority, they are sorted based on the group names.

Step 6 Click **Submit**.

The new group type is recorded in the RDU, and the new group type appears on the Manage Group Types page.

)

Modifying Group Types

To modify group type priority:

Step 1 Click the **Groups** tab to open the Manage Groups page.

Step 2 Change the **Search Type** to Group Type.

Step 3 Click the name of the group type to open the Modify Group Type page.

Step 4 Make the necessary changes to the Group Type Priority.

Step 5 Click **Submit**.

The Manage Groups page appears with the modified description.

Deleting Group Types

To delete group types:

Step 1 Click the **Groups** tab to open the Manage Groups page

Step 2 Locate the correct group type and click the **Delete** icon ( ) corresponding to it.

Step 3 In the Delete Group Type dialog box, click **OK** to delete the selected group type, or **Cancel** to return to the previous page.

The Manage Groups page appears without the deleted Group Type.

Managing Groups

You can create and modify groups, and delete unwanted groups.

Adding a New Group

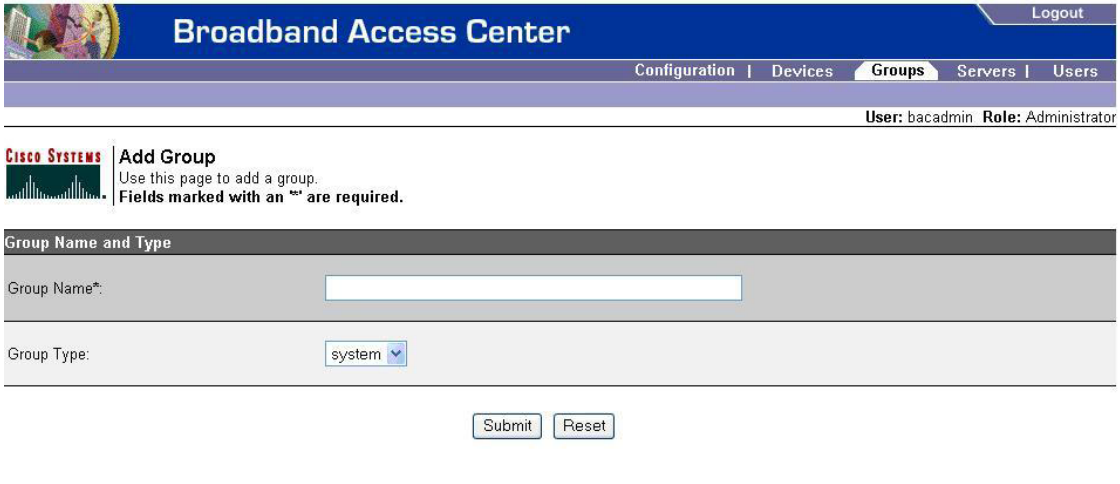
To add a new group:

Step 1 Select **Group** from the drop-down list on the Manage Groups page.

Step 2 Click **Add.**

The Add Group page appears (shown in Figure 16-6).

Figure 16-6 Add Group Page



Step 3 Enter the name for the new group.

Step 4 Select the appropriate Group Type from the drop-down list.

Step 5 Click **Submit**.

The new group is recorded in the RDU, and the new group appears on the Manage Groups page.

Modifying a Group

To modify group properties:

Step 1 Select **Group** from the drop-down list on the Manage Groups page.

Step 2 Select the group that needs to be modified from the group list.

The Modify Group page appears.

Step 3 Make the necessary changes and Click **Submit.**

The Manage Group page appears with the appropriately modified description.

Deleting Groups

You can delete any group that appears in the Manage Groups page by checking the box corresponding to the correct group and clicking the **Delete** button.

Relating/Unrelating Groups to Groups

The relate and unrelate functions are used to establish a relationship between group objects. To either relate or unrelate this relationship:

Step 1 Click **Relate** or **Unrelate**, as desired, for the selected group. The Relate Group or the Unrelate Group page appears.

Step 2 Select the appropriate Group Type from the drop-down list and select the group to which the node will be related/unrelated.

Step 3 Click **Submit.**

The Manage Groups page appears.

Viewing Group Details

To view details of a group:

Step 1 From the Manage Groups page, select the Group option from the Search Type drop-down list.

Step 2 Select the correct Group Type and enter the Group or Group wildcard in the appropriate field.

Step 3 Click **Search**.

Step 4 Click the link corresponding to the Group whose details you want to view.

The Modify Group page appears, with details of the Group Name and Group Type.

Viewing Servers

This section describes the Cisco BAC server pages:

- Viewing Device Provisioning Engines, page 16-22
- Viewing Provisioning Groups, page 16-24
- Viewing Regional Distribution Unit Details, page 16-26

Viewing Device Provisioning Engines

The Manage Device Provisioning Engines page lets you monitor the list of all DPEs currently registered with the Cisco BAC database. Each DPE name displayed on this page is a link to another page that shows the details for that DPE. Click this link to display the details page, which is similar to Figure 16-7.

Note The RDU determines the names of the DPEs by performing a reverse DNS lookup on the DPE interfaces through which the DPE contacts the RDU.

Figure 16-7 View Device Provisioning Engine Details Page

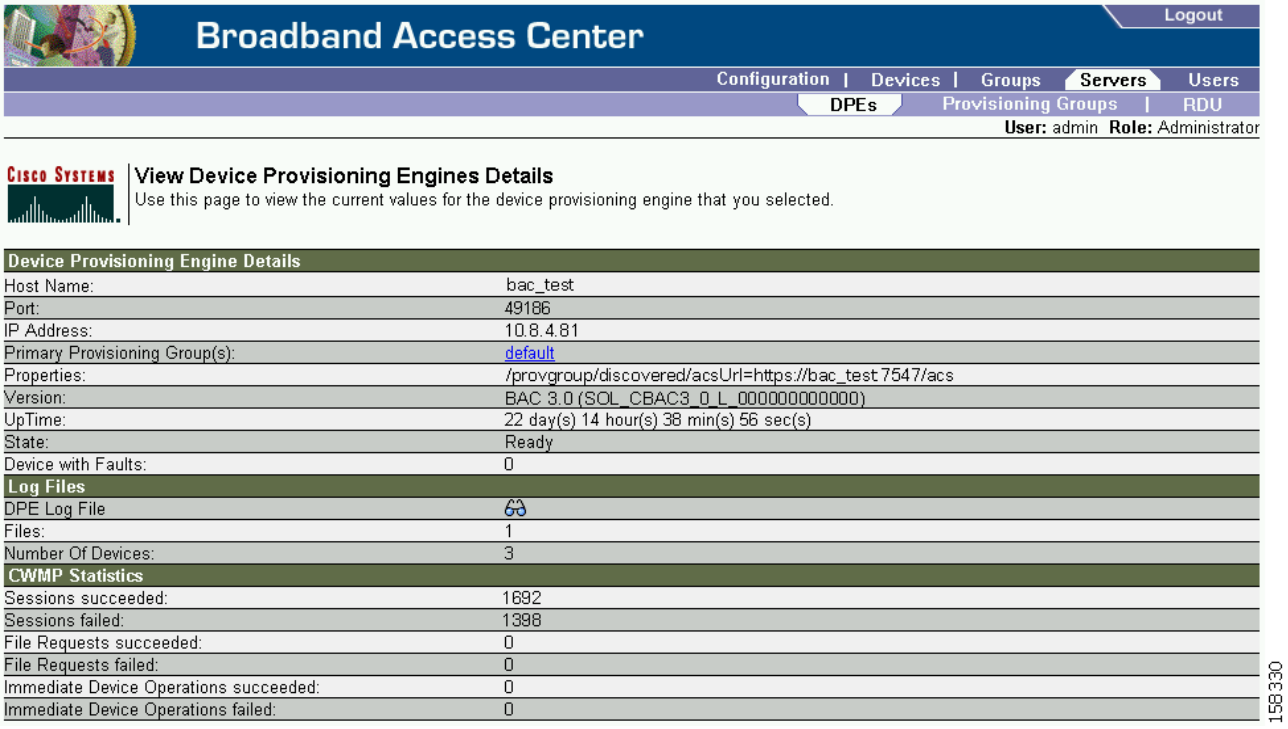


Table 16-3 identifies the fields and buttons shown in Figure 16-7.

Table 16-3 View Device Provisioning Engine Details Page

Field or Button	Description
Device Provisioning Engine Details	
Host Name	Identifies the DPE hostname.
Port	Identifies the DPE port number from which DPE established connection to the RDU.
IP Address	Identifies the IP address of the DPE.
Primary Provisioning Group(s)	Identifies the primary provisioning group that the selected DPE belongs to. This is an active link that, if clicked, displays the Provisioning Group Details page for that provisioning group.
Properties	Identifies which properties have been configured for this DPE.
Version	Identifies the version of DPE software currently in use.
UpTime	Specifies the total time that the DPE has been operational since its last start-up.
State	Identifies whether the DPE is ready for operations. These states include: • Registering • Initializing • Synchronizing • Populating • Ready • Offline If this field reads Offline, the options from the Uptime field onwards do not appear. The DPE is prepared to service client requests in any state except Offline.
Device with Faults	Displays number of devices with faults at this DPE. If number is greater than zero, features the View Details icon which if clicked, displays details of devices with faults.
Log Files	
DPE Log File	Features the View Details icon that if clicked displays the View Log File Contents page, which provides details of *dpe.log*.
Files	Identifies the number of files, such as firmware images, that are cached at the DPE.
Number of Devices	Identifies the number of CWMP devices for which the DPE maintains instructions. In a fully synchronized DPE, this number should equal the number of CWMP devices in the DPE's provisioning group.
CWMP Statistics **Note** This section displays statistics from the last time the DPE was started.	
Sessions succeeded	Identifies the number of successful CWMP sessions.
Sessions failed	Identifies the number of failed CWMP sessions.
File Requests Succeeded	Identifies the number of successful firmware file download requests.
File Requests Failed	Identifies the number of failed firmware file download requests.

Table 16-3 View Device Provisioning Engine Details Page (continued)

Field or Button	Description
Immediate Device Operations Succeeded	Identifies the number of immediate device operations that succeeded.
Immediate Device Operations failed	Identifies the number of immediate device operations that failed.
Home PG Redirection Statistics	
Succeeded	Identifies the number of successful home provisioning group redirections.
Failed	Identifies the number of failed home provisioning group redirections.

Viewing Provisioning Groups

The Manage Provisioning Groups page lets you monitor all current provisioning groups. Each provisioning group appearing in this list is a link to its own details page. Click this link to display the details page, which is similar to Figure 16-8.

Figure 16-8 View Provisioning Group Details Page

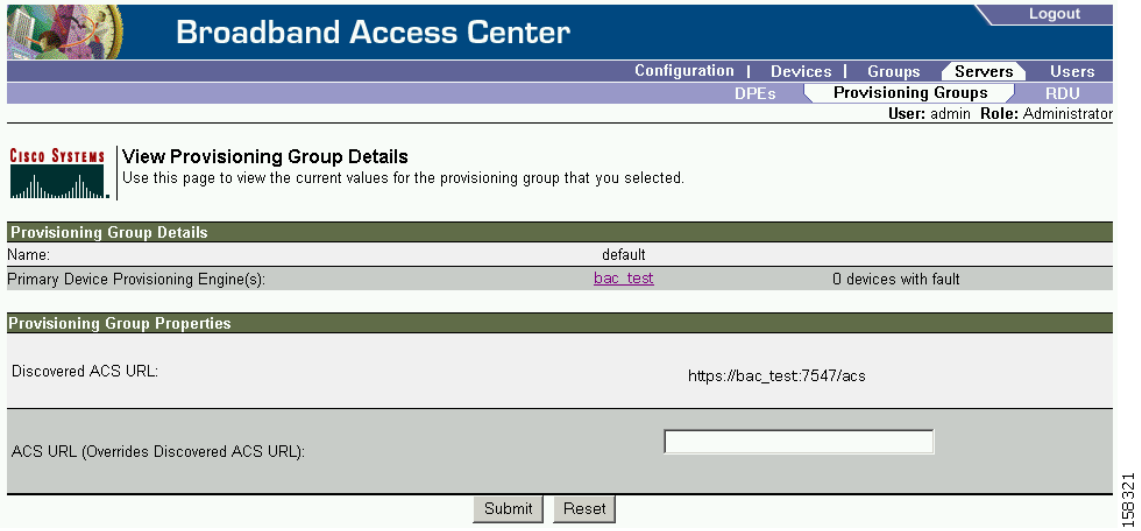


Table 16-4 identifies the fields and buttons shown in Figure 16-8. The fields described in Table 16-4 may include active links that, if clicked, display the appropriate details page.

Table 16-4 View Provisioning Groups Details Page

Field or Button	Description
Provisioning Group Details	
Name	Identifies the provisioning group name selected from the List Provisioning Groups page.
Primary Device Provisioning Engine(s)	Identifies the hostnames of the DPEs that are primary for this provisioning group.
Provisioning Group Properties	

Table 16-4 View Provisioning Groups Details Page (continued)

Field or Button	Description
Discovered ACS URL	Identifies the DPE URL through which the provisioning group connects to the DPE. Discovered URL is based on DPE interface configured for provisioning operations via the DPE CLI. The parameters is based on registration information from the DPE which registered last with the RDU. This URL is used for operations such as redirection of CPE to a different provisioning group.
ACS URL (Overrides Discovered ACS URL)	Identifies the configured URL of the Cisco BAC server associated with each provisioning group. This URL is used by devices to contact the DPEs in a given provisioning group, and is used for operations such as redirection of CPE to a a different provisioning group.
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

Viewing Regional Distribution Unit Details

The RDU option, from the Servers menu, displays details of the RDU. Figure 16-9 illustrates a sample RDU details page.

Figure 16-9 View Regional Distribution Unit Details Page

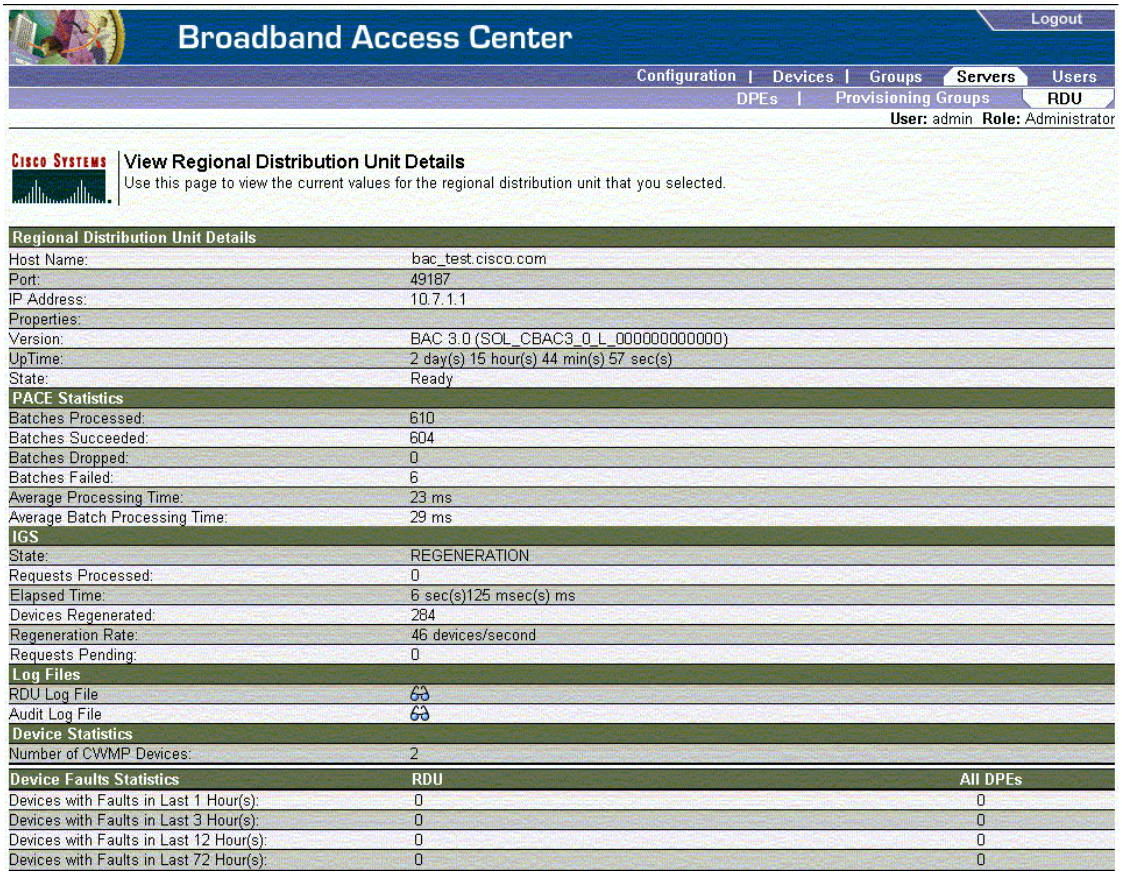


Table 16-5 identifies the fields and buttons shown in Figure 16-9.

Table 16-5 View RDU Details Page

Field or Button	Description
Regional Distribution Unit Details	
Host Name	Identifies the host name of the system that is running the regional distribution unit.
Port	Identifies the RDU listening port number for connections from the DPEs. The default port number is 49187, but a different port can be selected during installation of the RDU.
IP Address	Identifies the IP address assigned to the RDU.
Properties	Identifies properties configured for the RDU.
Version	Specifies the version of RDU software currently in use.

Table 16-5 View RDU Details Page (continued)

Field or Button	Description
UpTime	Specifies the total time that the RDU has been operational since its last period of downtime.
State	Identifies whether the RDU is ready to respond to requests. The only state that is featured via the administrator user interface is Ready.
PACE Statistics	
Batches Processed	Identifies how many individual batches have been processed since the last RDU start-up.
Batches Succeeded	Identifies how many individual batches have been successfully processed since the last RDU start-up.
Batches Dropped	Identifies how many batches have been dropped since the last RDU start-up.
Batches Failed	Identifies how many batches have failed processing since the last RDU start-up.
Average Processing Time	Identifies the average time, in milliseconds, that it takes to process the batch excluding the time it spends in the queue if RDU is too busy.
Average Batch Processing Time	Identifies the average time, in milliseconds, that it takes to process the batch including the time it spends in the queue if RDU is too busy.
IGS This is the Instruction Generation Service.	
State	Identifies the operational state of the instruction generation service. This could be: • Idle—Specifies that the IGS is not processing regeneration requests. • Regeneration—Specifies that the IGS is processing regeneration requests. • Waiting Regeneration—Specifies that the IGS is unable to regenerate instructions for a device. When the IGS is stuck in this state, consult the *rdu.log* for details.
Requests Processed	Identifies the number of instruction generation requests processed since last RDU start-up.
Elapsed Time	Identifies, in seconds, the time elapsed since the start of regeneration.
Devices Regenerated	Identifies the number of device instructions regenerated since the regeneration process started.
Regeneration rate	Identifies the cumulative rate of device instructions regenerated since the regeneration process started.
Requests pending	Identifies the number of regeneration requests in queue.
Log Files	
RDU Log File	Features the View Details icon, that, if clicked, displays the View Log File Contents page, which provides details of the *rdu.log* file.
Audit Log File	Features the View Details icon, that, if clicked, displays the View Log File Contents page, which provides details of the *audit.log* file.

Table 16-5 View RDU Details Page (continued)

Field or Button	Description
Device Statistics	
Number of CWMP Devices	Identifies the number of devices in the RDU database.
Device Faults Statistics	
Devices with Faults in Last 1 Hour(s)	Identifies the number of devices with faults over the last one hour, at both the RDU and the DPEs.
Devices with Faults in Last 3 Hour(s)	Identifies the number of devices with faults over the last three hours, at both the RDU and the DPEs.
Devices with Faults in Last 12 Hour(s)	Identifies the number of devices with faults over the last 12 hours, at both the RDU and the DPEs.
Devices with Faults in Last 72 Hour(s)	Identifies the number of devices with faults over the last 72 hours, at both the RDU and the DPEs.