CHAPTER 13

Configuring Cisco Broadband Access Center

This chapter describes the Cisco Broadband Access Center (Cisco BAC) configuration tasks that you perform by selecting the options in the Configuration menu:

Configuring Class of Service

Using the Cisco BAC administrator user interface, you can configure the Class of Service offered to your customers. For example, you can associate DOCSIS options with different DOCSIS Class of Service. You use the Cisco BAC administrator user interface to add, modify, view, or delete any selected Class of Service.

Table 13-1 identifies the fields and buttons that appear when you click **Configuration > Class of Service > Manage Class of Service**.

Table 13-1 Manage Class of Service Page

Field or Button	Description
Class of Service	
Class of Service	A drop-down list that identifies the technology Class of Service that you can search for. Available options are: • CableHome WAN-Data • CableHome WAN-MAN • Computer • DOCSIS Modem • PacketCable Multimedia Terminal Adapter (MTA) • STB **Note** For additional information on these areas of technology, see Configuring Defaults, page 13-6.
Class of Service	Displays the names of Class of Service objects.

Adding a Class of Service

To add a specific Class of Service:

Step 1 From the Manage Class of Service page, select the device type for which you want to add a Class of Service using the Class of Service drop-down list.

Step 2 Click **Add**.

The Add Class of Service page appears. This page identifies the various settings for the selected Class of Service.

Step 3 Enter the name for the new Class of Service, and choose the device type from the Class of Service Type drop-down list. For example, assume that you want to create a new Class of Service called Gold-Classic for DOCSIS modems. You might enter **Gold-Classic** as the Class of Service Name, and choose **DOCSISModem** from the service type drop-down list.

Step 4 Choose a property and enter its corresponding value in the Property Value field. For example, if you choose as the property name */cos/docsis/file,* enter **Gold-Classic.cm** in the Property Value field, and continue with the rest of this procedure.

Note When adding a DOCSISModem Class of Service, you must specify the */cos/docsis/file* property with the value being the name of a previously added file. This file is used when provisioning a DOCSIS device that has this Class of Service.

Cisco BAC provides automatic selection of a cable modem configuration file that enables the highest DOCSIS version compatible with the modem. To enable this feature, you must configure the Class of Service with multiple configuration files, one for each DOCSIS level. Use the following properties to allow the selection of a configuration file specific to a DOCSIS version:

- */cos/docsis/file/1.0*—Selects a configuration file specific to DOCSIS 1.0.
- */cos/docsis/file/1.1*—Selects a configuration file specific to DOCSIS 1.1.
- */cos/docsis/file/2.0*—Selects a configuration file specific to DOCSIS 2.0.
- */cos/docsis/file/3.0/ipv4*—Selects a configuration file specific to DOCSIS 3.0 in the IPv4 mode.
- */cos/docsis/file/3.0/ipv6*—Selects a configuration file specific to DOCSIS 3.0 in the IPv6 mode.

When adding a PacketCable Class of Service, you must specify the */cos/packetCableMTA/file* property with the value being the name of a previously added file. This file is used when provisioning a PacketCable device that has this Class of Service.

When adding a CableHome WAN-MAN Class of Service, you must specify the */cos/cableHomeWanMan/file* property with the value being the name of a previously added file. This file is used when provisioning a CableHome WAN-MAN device that has this Class of Service.

Step 5 Click **Add** to add the property to the Class of Service.

Step 6 Click **Submit** to finalize the process.

After submitting the Class of Service, the Manage Class of Service page appears to show the newly added Class of Service for the particular device type.

Modifying a Class of Service

You modify your Class of Service by selecting the various properties and assigning appropriate property values. When creating a Class of Service for the first time you must select all the required properties and assign values to them. If you make a mistake, or your business requirements for a certain Class of Service change, you can either change the property value before submitting your previous changes or delete the Property Name:Property Value pair altogether.

Note Changes to the Class of Service object trigger the Configuration Regeneration Service (CRS) to regenerate configurations for all affected devices and send configurations to the DPEs. The CRS performs this task as a background job.

You can view the status of the CRS from the View RDU Details page.

To add, delete, or modify Class of Service properties:

Step 1 From the Manage Class of Service page, select the Class of Service for the specific device type.

The Modify Class of Service page appears.

- To add a new property to the selected Class of Service:
  - Select the first property that you want assigned to the selected Class of Service from the Property Name drop-down list and, after choosing the appropriate value for that property, click **Add**.
  - Repeat for any other properties that you want to assign to the selected Class of Service.
- To delete a property for the selected Class of Service:
  - Locate the unwanted property in the list immediately above the Property Name drop-down list.
  - Click **Delete**.
- To modify the value currently assigned to a property:
  - Delete the appropriate property as described above.
  - Add the same property again with the new property value.

Note If you delete a property that is required for your business process, add the property again and select the appropriate value before you submit the change.

Step 2 Click **Submit**.

Each property added to a Class of Service appears when you click **Submit**. After doing so, a confirmation page appears to regenerate the configurations for the devices with the selected Class of Service.

Step 3 Click **OK.**

The modified Class of Service is available in the Manage Class of Service page.

Deleting a Class of Service

You can delete any existing Class of Service, but before you attempt to do so, ensure that no devices are associated with that Class of Service.

Tip When large numbers of devices associated with a Class of Service need to be deleted, use the Cisco BAC application programming interface (API) to write a program to iterate through these devices to reassign another Class of Service to the devices.

Note You cannot delete a Class of Service if it is designated as the default Class of Service or if devices are associated with it. Therefore, you cannot delete the **unprovisioned-docsis** Class of Service object. If you try to delete a Class of Service with devices associated with it, this error message appears:

```
The following error(s) occurred while processing your request.
Error: Class Of Service [sample-CoS] has devices associated with it, unable to delete

Please correct the error(s) and resubmit your request.
```

The specific Class of Service is specified within the error message. This example uses *sample-CoS*.

To delete a Class of Service:

Step 1 From the Manage Class of Service page, select the Class of Service for the specific device type that you want to delete.

Step 2 Click the **Delete** icon (🗑) for that Class of Service.

A confirmation dialog box appears.

Step 3 Click **OK**.

Configuring Custom Properties

Custom properties let you specify additional customizable device information to be stored in the RDU database. To configure custom properties, click **Configuration > Custom Property > Manage BAC Custom Properties**. You use this page to add or delete custom properties.

Caution Although you can delete custom properties if they are currently in use, doing so could cause extreme difficulty to other areas where the properties are in use.

After the custom property is defined, you can use it in the property hierarchy. See Property Hierarchy, page 4-7.

Adding a Custom Property

To add a custom property:

Step 1 From the Manage Cisco BAC Custom Properties page, click **Add**.

The Add Custom Property page appears.

Step 2 Enter the name of the new custom property.

Step 3 Choose a type for the custom property from the options available in the drop-down list.

Step 4 Click **Submit**.

After the property is added to the database, the Manage Cisco BAC Custom Properties page appears.

Deleting a Custom Property

To delete a custom property:

Step 1 From the Manage Cisco BAC Custom Properties page, identify the custom property to be deleted.

Step 2 Click the **Delete** icon corresponding to the custom property.

The confirmation dialog box appears.

Step 3 Click **OK**.

The Manage Cisco BAC Custom Properties page appears with the custom property deleted from the database.

Configuring Defaults

You can access the default settings for the overall system, including the Regional Distribution Unit (RDU), Network Registration extensions, and all supported technologies. To configure or view default settings, click **Configuration > Defaults.** The Configure Defaults page appears.

To access specific defaults page, click the specific link from the Default links on the left of the screen.

This section describes:

- CableHome WAN Defaults, page 13-7
- Computer Defaults, page 13-7
- DOCSIS Defaults, page 13-8
- Network Registrar Defaults, page 13-9
- PacketCable Defaults, page 13-11
- RDU Defaults, page 13-12
- System Defaults, page 13-14
- STB Defaults, page 13-16

CableHome WAN Defaults

There are two distinct CableHome WAN default screens: one for WAN-Data devices and one for WAN-MAN devices. In either case, select the desired defaults from the list on the left pane.

- When you select the CH WAN-Data Defaults link, the CableHome WAN-Data Defaults page appears. Use this page to configure the WAN-Data device.
- When you select the CH WAN-MAN Defaults link, the CableHome WAN-MAN Defaults page appears. Use this page to configure the WAN-MAN device type.

Each WAN default page contains identical fields as described in Table 13-2.

Table 13-2 Configure Defaults–CH WAN-Data/CH WAN-MAN Defaults Page

Field or Button	Description
CableHome WAN-Data Defaults/CableHome WAN-MAN Defaults	
Extension Point	Identifies the extension point to execute when generating a configuration for a WAN device.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a WAN device.
Service-level Selection Extension Point	Identifies the extension used to determine the DHCP Criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default Class of Service for a WAN-Data. New, unrecognized WAN devices are assigned to this Class of Service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP Criteria for a specific device technology. New, unrecognized WAN devices are assigned this default DHCP Criteria. Use the drop-down list to select a new default value.
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automated FQDN generation is disabled. **Note** See Automatic FQDN Generation, page 13-32, for additional information.

Computer Defaults

When you select the Computer Defaults link, the list of default values currently applied to the computers supported by Cisco BAC appears. See Table 13-2 for the description of the fields that appear on this page.

Note Changes to the default Class of Service or default DHCP Criteria cause regeneration to occur. Other changes made to this page do not affect existing devices.

DOCSIS Defaults

When you select the DOCSIS Defaults link, the list of default values currently applied to the cable modems supported by Cisco BAC appears. See Table 13-3 for the description of all fields and buttons that appear on this page.

Table 13-3 Configure Defaults–DOCSIS Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a DOCSIS device.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a DOCSIS device.
Service-level Selection Extension Point	Identifies the extension used to determine the DHCP Criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default Class of Service for a device. New, unrecognized devices are assigned to this Class of Service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP Criteria for a specific device technology. New, unrecognized devices are assigned this default DHCP Criteria. Use the drop-down list to select a new default value.
TFTP Modem Address Option	Identifies whether the TFTP modem address option is enabled.
TFTP Time Stamp Option	Identifies whether the TFTP server will issue a timestamp.
Note If you enable either or both of the TFTP options on this page, that appropriate TFTP information is included in the TFTP file before it is sent to the DOCSIS cable modem.	
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automatic FQDN generation is disabled. **Note** See Automatic FQDN Generation, page 13-32, for additional information.
CMTS Shared Secret	Identifies the character string that Cisco BAC uses in the calculation of the CMTS MIC in the configuration file. The CMTS uses it to authenticate the configuration file that a cable modem submits to the CMTS for authorization.
CMTS Default DOCSIS Version	Specifies the default DOCSIS version used by all CMTSs. If you do not enter a DOCSIS version in this field, it will default to version 1.0.
Relay Agent IP Address to CMTS Version Mapping file	Identifies the mapping file used by the CMTS. This file specifies the DOCSIS version that the CMTS will use.
Extended CMTS MIC Option	Identifies whether the Extended CMTS MIC (EMIC) option is enabled. **Note** Only if this field is enabled do subsequent fields in this section appears.

Table 13-3 Configure Defaults–DOCSIS Defaults Page (continued)

Field or Button	Description (continued)
Extended CMTS MIC HMAC Type	Identifies the default Hash-based Message Authentication Code (HMAC) type for EMIC calculation. Choose one of the following HMAC type: • MD5 • MMH16 **Note** By default, MMH16 is used for EMIC calculation.
Extended CMTS MIC Digest Explicit Option	Identifies whether the Extended CMTS MIC Digest explicit digest option is enabled. By default, Extended CMTS MIC explicit digestion is used for EMIC calculation.
Extended CMTS MIC Shared Secret	Identifies the character string that Cisco BAC uses in the calculation of the Extended CMTS MIC in the configuration file. The CMTS uses it to authenticate the configuration file that a cable modem submits to the CMTS for authorization.
Extended CMTS MIC Fields	Identifies the TLVs that are to be included in Extended CMTS MIC calculation.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.

Note Changes to the default Class of Service or default DHCP Criteria cause regeneration to occur. Changes to any TFTP option come into effect starting from the next TFTP transfer.

Network Registrar Defaults

Cisco BAC provides Cisco Network Registrar (NR) extension points that allow Cisco BAC to pull information from incoming DHCP packets to detect a device's technology. The extension points also let Cisco BAC respond to device DHCP requests with options that correspond to the configuration stored at the DPE.

When you select the NR Defaults link, the list of default values currently applied to Network Registrar extensions appears. Table 13-4 identifies the fields that appear on this page.

Table 13-4 Configure Defaults–Network Registrar Defaults Page

Field or Button	Description
NR Extension Point Settings (Cisco BAC 2.6, 2.7)	
Attributes Required in Request Dictionary	Identifies a comma-separated list of attributes that the Network Registrar request dictionary must include when sending a request to the RDU for configuration generation.

Table 13-4 Configure Defaults–Network Registrar Defaults Page (continued)

Field or Button	Description
Attributes from Request Dictionary as Bytes	Identifies a comma-separated list of attributes pulled out of the Network Registrar request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Attributes from Request Directory as Strings	Identifies a comma-separated list of attributes pulled from the Network Registrar request dictionary as strings when sending a request to the RDU to generate a device configuration.
NR Extension Point Settings (Cisco BAC 4.0.1.x or higher)	
Attributes Required in DHCPv4 Request Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv4 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is the relay agent remote ID option. If you do not set the **relay-agent-remote-id** value in this field, Network Registrar extensions reject devices from triggering a request for configuration generation.
Attributes from DHCPv4 Request Dictionary as Bytes	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv4 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Attributes from DHCPv4 Request Dictionary as Strings	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv4 request dictionary as strings when sending a request to the RDU to generate a device configuration.
Attributes Required in DHCPv6 Request Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv6 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is **none**.
Options Required in DHCPv6 Request Dictionary	Specifies a comma-separated list of DHCP options that the Network Registrar DHCPv6 request dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Attributes from DHCPv6 Request Dictionary as Bytes	Identifies a comma-separated list of attributes pulled from the Network Registrar DHCPv6 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Options from DHCPv6 Request Dictionary as Bytes	Specifies a comma-separated list of DHCP options pulled from the Network Registrar DHCPv6 request dictionary as bytes when sending a request to the RDU to generate a device configuration.
Attributes Required in DHCPv6 Relay Dictionary	Identifies a comma-separated list of attributes that the Network Registrar DHCPv6 relay dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration. The default value for this field is **peer-address**.

Table 13-4 Configure Defaults–Network Registrar Defaults Page (continued)

Field or Button	Description
Options Required in DHCPv6 Relay Dictionary	Identifies a comma-separated list of DHCP options that the Network Registrar DHCPv6 relay dictionary must include for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Attributes from DHCPv6 Relay Dictionary as Bytes	Identifies a comma-separated list of attributes pulled out of the Network Registrar DHCPv6 relay dictionary as bytes for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
Options from DHCPv6 Relay Dictionary as Bytes	Identifies a comma-separated list of DHCP options pulled out of the Network Registrar DHCPv6 relay dictionary as bytes for Network Registrar extensions to submit a request to the RDU to generate a device configuration.
NR Extension Point Environment Settings	
Attributes from Environment Dictionary	Identifies a comma-separated list of attributes pulled out of the Network Registrar environment dictionary as strings when sending a request to the RDU to generate a device configuration.

Note Changes made to this page do not take effect until the Network Registrar extensions are reloaded.

PacketCable Defaults

The PacketCable Defaults page identifies those defaults necessary to support the PacketCable voice technology. When you select the PacketCable Defaults link, the list of default values currently applied to PacketCable devices appears. Table 13-5 identifies the fields that are unique to this defaults page.

Table 13-5 Configure Defaults–PacketCable Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for a device of this technology.
Disruption Extension Point	Identifies the extension point to be executed to disrupt a device of this technology.
Service-level Selection Extension Point	Identifies the extension used to determine the DHCP Criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default Class of Service for a device. New, unrecognized devices are assigned to this Class of Service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP Criteria for a specific device technology. New, unrecognized devices are assigned this default DHCP Criteria. Use the drop-down list to select a new default value.
SNMP Set Timeout	Identifies the SNMP set timeout in seconds.

Table 13-5 Configure Defaults–PacketCable Defaults Page (continued)

Field or Button	Description
MTA Provisioning Notification	Notification that an MTA event has taken place. An event occurs when the MTA sends its provisioning complete inform based on the selected choice. Options available include: • On Failure • On Success • During Provisioning • Always • Never
Automatic FQDN Generation	Identifies whether a fully qualified domain name (FQDN) will be generated.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.

RDU Defaults

When you select the RDU Defaults link, the defaults settings that you have configured for the RDU appear. Use this page to configure the RDU to communicate with Network Registrar. For additional information, see the *User Guide for Cisco Network Registrar 7.2*.

Table 13-6 describes the fields that appear on the RDU Defaults page.

Table 13-6 Configure Defaults–RDU Defaults Page

Field or Button	Description
Configuration Extension Point	Identifies the common extension points executed before any other technology extension point is executed.
Device Detection Extension Point	Identifies the extension point used to determine a device type (for example, DOCSIS or computer) based on information pulled from the device DHCP Discover requests.
Publishing Extension Point	Identifies the extension point to be used for an RDU publishing plug-in. This information is useful when you need to publish RDU data into another database.
Extension Point JAR File Search Order	Specifies the sequence in which the classes are searched in the JAR files that are listed in the preceding four fields.
CCM Server IP Address	Identifies the IP address of the CCM server.
CCM Server Port	Identifies the CCM server port on which Cisco BAC communicates.
CCM Server User	Identifies the CCM server username and is used in conjunction with the password fields.
CCM Server Password	Identifies the password used to authenticate the CCM Server User.
CCM Server Confirm Password	Authenticates the CCM Server Password.

Table 13-6 Configure Defaults–RDU Defaults Page (continued)

Field or Button	Description
CCM Server	Specifies whether the Cisco BAC interface to the CCM Server is enabled or disabled.
CCM Server Timeout	Specifies the length of time, in seconds, that Cisco BAC attempts to connect with the CCM Server until Cisco BAC declares the connection down.
CRS	Identifies whether the Configuration Regeneration Service (CRS) is enabled. There are two options: • Enable—Enables the CRS within Cisco BAC. • Disable—Disables the CRS within Cisco BAC.
Authentication Mode	Identifies the authentication mode to be used. The options are: • Local—Authenticates the user in the local RDU database. • RADIUS—Authenticates the user, using the RADIUS server.
Number of Sessions per User	Specifies the maximum number of allowed sessions for a user. You could specify any value between 1 to 100. The default value for this property is 100. If this property value is not assigned to a user, the value available in the RDU defaults is considered.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.

Configuration Details for RADIUS Authentication

This table lists the fields required for configuring RADIUS authentication.

Table 13-7 Configure Defaults–RDU Defaults Page–Server Authentication Mode Property Details–RADIUS mode

Field or Button	Description
RADIUS Class	Identifies the class containing the RADIUS authentication extensions. The default value is "**com.cisco.provisioning.cpe.extensions.builtin.authentication.RadiusAuthentication**".
RADIUS Primary Host	Identifies the primary IP address of the RADIUS server.
RADIUS Primary SharedSecret	Identifies the primary shared secret used to authenticate the RADIUS server user.
RADIUS Primary Port	Identifies the primary authentication port number of the RADIUS server. The default port number is 1812.
RADIUS Secondary Host	Identifies the secondary IP address of the RADIUS server, which is optional.
RADIUS Secondary SharedSecret	Identifies the secondary shared secret used to authenticate the RADIUS server user, which is optional.
RADIUS Secondary Port	Identifies the secondary authentication port number of the RADIUS server, which is optional.

Table 13-7 Configure Defaults–RDU Defaults Page–Server Authentication Mode Property Details–RADIUS mode

Field or Button	Description
RADIUS Timeout	Specifies the maximum length of time for which RDU waits for a response when trying to connect to the RADIUS server. The value will be specified in milliseconds and the default value is 1000 milliseconds. The value can be between 1000-5000 milliseconds.
RADIUS Retries	Specifies the maximum number of times RDU attempts to connect with the RADIUS server. The default value is 1 and the value can be between 1-5.

Note If the RADIUS time out exceeds 10000 milliseconds then BAC authentication will fail. RADIUS time out and retries must be configured so that it does not exceed greater than 10000 milliseconds.

Note See Managing RDU Extensions, page 13-27, for information on RDU extension points.

System Defaults

When you select the Systems Defaults link, the System Defaults page appears. Table 13-8 describes the fields that appear on this page.

Note You can configure the default values using the Cisco BAC API.

Table 13-8 Configure System Defaults Page

Field or Button	Description
System Defaults	
SNMP Write Community String	Identifies the default write community string for any device that may require SNMP information. The default write community string is **private**.
SNMP Read Community String	Identifies the default read community string for any device that can read or access the SNMP MIB. The default read community string is **public**.

Table 13-8 Configure System Defaults Page (continued)

Field or Button	Description
System Defaults	
Default Device Type for Device Detection	Identifies the default device type for a device not previously registered in the RDU. The options include: • DOCSIS • COMPUTER • PacketCableMTA • STB • CableHomeWanMan • CableHomeWanData • None **Note** If the device detection extension is unable to identify the device type, the “default type” (for example, COMPUTER) specifies the device type. If you set the Default Device Type to None, the device record is not added to the RDU.
Maximum Diagnostics Device Count	Identifies the maximum number of MAC addresses (devices) that you can troubleshoot at any one time.
MIB List	Identifies a list of MIBs used by the RDU that do not require restarting the RDU.
Supplemental MIB List	Identifies an extended list of MIBs used by the RDU.
Excluded MIB Tokens	Defines those keywords, or tokens, that cannot be redefined by a MIB.
Excluded Supplemental MIB Tokens	Defines those additional keywords, or tokens, that cannot be redefined by a MIB and do not appear in the Excluded MIB Tokens list.
Promiscuous Policy Settings	
CableHome WanData Promiscuous Mode	Enables or disables CableHome WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous Mode	Enables or disables CableHome WAN-MAN devices in the promiscuous mode.
Computer Promiscuous Mode	Enables or disables computers in the promiscuous mode.
PacketCable Promiscuous Mode	Enables or disables PacketCable devices in the promiscuous mode.
STB Promiscuous Mode	Enables or disables STBs in the promiscuous mode.
CableHome WanData Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision WAN-MAN devices in the promiscuous mode.
Computer Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision computers in the promiscuous mode.

Table 13-8 Configure System Defaults Page (continued)

Field or Button	Description
System Defaults	
Packetcable Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision PacketCable devices in the promiscuous mode.
STB Promiscuous DHCP Criteria	Identifies the DHCP Criteria used to provision STBs in the promiscuous mode.
CableHome WanData Promiscuous Class of Service	Identifies the Class of Service used to provision WAN-Data devices in the promiscuous mode.
CableHome WanMan Promiscuous Class of Service	Identifies the Class of Service used to provision WAN-MAN devices in the promiscuous mode.
Computer Promiscuous Class of Service	Identifies the Class of Service used to provision computers in the promiscuous mode.
Packetcable Promiscuous Class of Service	Identifies the Class of Service used to provision PacketCable devices in the promiscuous mode.
STB Promiscuous Class of Service	Identifies the Class of Service used to provision STBs in the promiscuous mode.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.

STB Defaults

The STB Defaults page identifies those defaults necessary to support any STB compliant with CableLabs OpenCable Application Platform. Table 13-9 describes the fields that appear on this page.

Table 13-9 Configure Defaults–STB Defaults Page

Field or Button	Description
Extension Point	Identifies the extension point to execute when generating a configuration for an STB.
Disruption Extension Point	Identifies the extension point to be executed to disrupt an STB.
Service-level Selection Extension Point	Identifies the extension used to determine the DHCP Criteria and Class of Service required for a device.
Default Class of Service	Identifies the current default Class of Service for an STB. New, unrecognized STB devices are assigned to this Class of Service. Use the drop-down list to select a new default value.
Default DHCP Criteria	Identifies the current default DHCP Criteria for a specific device technology. New, unrecognized STBs are assigned this default DHCP Criteria. Use the drop-down list to select a new default value.

Table 13-9 Configure Defaults–STB Defaults Page (continued)

Field or Button	Description
Automatic FQDN Generation	Automatically generates a host and domain name for the device. Two selectable options are available: • Enabled—Automatic generation of the FQDN is enabled. • Disabled—Automatic FQDN generation is disabled. **Note** See Automatic FQDN Generation, page 13-32, for additional information.
CableLabs Configuration Filename Script	Identifies the Groovy script to be used to generate the dynamic TFTP filename.

Note Subsequent device configurations will include the changes you implement here. However, all existing configurations are not changed. To make the changes in any existing configuration, you must regenerate the configuration using the API.

Configuring DHCP Criteria

In Cisco BAC, DHCP Criteria describe the specific criteria for a device when selecting a scope in Network Registrar. For example, a DHCP Criteria called **provisioned-docsis** has an inclusion selection tag called **tagProvisioned**. The DHCP Criteria is associated with a DOCSIS modem. When this modem requests an IP address from the Network Registrar, Network Registrar looks for scopes associated with the scope-selection tag **tagProvisioned**.

To access the DHCP Criteria page, choose **Configuration > DHCP Criteria.** The Manage DHCP Criteria page appears, listing the DHCP Criteria that identify the technology DHCP Criteria that you have added.

Adding DHCP Criteria

To add a DHCP Criteria:

Step 1 From the Manage DHCP Criteria page, click **Add**.

The Add DHCP Criteria page appears.

Step 2 Enter the name of the DHCP Criteria you want to create.

Step 3 Enter the DHCP Criteria client-class name.

Step 4 Enter the inclusion and exclusion selection tags.

Note When creating new DHCP Criteria, the client-class and inclusion and exclusion selection tag names you enter must be the exact names from within Network Registrar. For additional information on client class and selection tags, see the *User Guide for Cisco Network Registrar 7.2,* and *CLIFrame.html* in the */docs* directory. You should specify either the client class, or inclusion and exclusion selection tag names, when creating a new DHCP Criteria.

Step 5 You can add properties that are added on the DHCP Criteria. Select a Property Name, and enter the appropriate Property Value.

Step 6 Click **Add**.

Step 7 Click **Submit**.

After the DHCP Criteria is successfully added in the RDU database, it will be visible in the Manage DHCP Criteria Page.

Modifying DHCP Criteria

Note Once you change the DHCP Criteria, subsequent device configurations will include the changes you implement. All existing configurations are regenerated, although the devices on the network will not get the new configuration until they are rebooted.

To modify existing DHCP Criteria:

Step 1 On the Manage DHCP Criteria page, click the DHCP Criteria link that you want to modify.

The Modify DHCP Criteria page appears.

Step 2 Make the desired changes to the client class, inclusion and exclusion selection tags, and the property value settings.

Step 3 Click **Submit**.

After successful modification of the DHCP Criteria in the RDU database, the Manage DHCP Criteria page appears.

Deleting DHCP Criteria

Deleting DHCP Criteria using the administrator application does not delete the actual DHCP server configurations from the DHCP server. You must delete the DHCP server configurations manually.

To delete an existing criteria:

Note You can delete a DHCP Criteria only if there are no devices associated with that criteria, and it is not designated as the default DHCP Criteria. If a DHCP Criteria has devices associated with it, you must associate a different DHCP Criteria before deleting the criteria.

Step 1 On the Manage DHCP Criteria page, click the **Delete** icon corresponding to the DHCP Criteria you want to delete.

A confirmation dialog box appears.

Step 2 Click **OK**.

The Manage DHCP Criteria page appears.

Managing Files

Using the Cisco BAC administrator user interface, you can manage the TFTP server files or template files for dynamic generation for DOCSIS, PacketCable MTAs, and WAN-MAN files, or software images for devices. Use this page to add, delete, replace, or export any file type, including:

- Template files—These are text files that contain DOCSIS, PacketCable, or CableHome options and values that, when used with a particular Class of Service, provide dynamic file generation.

  Note Template files can be created in any text editor, but must have a *.tmpl* file type. For additional template information, see Template Files–An Overview, page 5-14.

- Static configuration files—These files are used as a configuration file for a device. For example, a static configuration file, called *gold.cm*, would identify the gold DOCSIS Class of Service. Cisco BAC treats this file type like any other binary file.
- Firmware images—These are images of device firmware, which can be downloaded to devices to upgrade their functionality. Cisco BAC treats this file type like any other binary file. These firmware images can also include IOS images for Cisco devices.

Table 13-10 describes the fields that appear on the View Files page.

Table 13-10 View Files Page

Field or Button	Description
Search Type	Identifies the types of searches that you can perform for files using the Cisco BAC administrator user interface. The options include: • Search by File Name—Searches for files using the filename pattern that you specify. • Search by File Type—Searches for files using the file type that you specify. The options include: – Firmware File—Specifies a firmware image file. – CableLabs Configuration File—Specifies a static configuration file for CableLabs. – CableLabs Configuration Script—Specifies a configuration script file for CableLabs. – CableLabs Configuration Template—Specifies a configuration template file for CableLabs. – CableLabs Configuration Filename Script—Specifies a configuration filename with a script for CableLabs. – Generic File—Specifies a generic file. – JAR File—Specifies a JAR file. – MIB File—Specifies a MIB file. – Script File—Specifies a script file.
Search Criteria	Identifies the filename or file type. You can use an asterisk (*) as a wildcard character to search for partial filenames. For example, you can enter ***.cm** to list all files ending with the *.cm* extension. An example of an invalid wildcard is bronze*.
Page Size	Identifies the number of results that must appear on a single page.
Files	Displays a list of files that match the search criteria. **Note** The check boxes immediately to the left of any selected item in this list must be checked before the item can be deleted.
View	Displays the details of the selected binary file.
File Type	Identifies the type of file.
Export	Exports any selected file to the client's computer.

Adding Files

To add an existing file:

Step 1 From the View Files page, click **Add**.

The Add Files page appears.

Step 2 Select the File Type from the drop-down list.

Step 3 Enter the path to the source file.

If you do not know the exact name of the source file, use **Browse** to navigate to the desired directory and select the file.

Step 4 Enter the name of the file.

If you are adding a CableLabs Configuration Template or a Firmware File, you must also complete these steps, otherwise go to Step 6.

a. When adding a CableLabs Configuration Template or a Firmware File, you can deliver the files that you add to the RDU to the DPE. To do so, click the **Enabled** radio button corresponding to the Is Deliverable field.

   While Cisco BAC sets a deliverable status for each file type, you can change the default setting only for a CableLabs Config Template or a Firmware File. The following list describes the default deliverable status for each file type:

   - Firmware File—Enabled
   - CableLabs Configuration File—Enabled
   - CableLabs Configuration Template—Disabled
   - Generic File—Disabled
   - JAR File—Disabled
   - MIB File—Disabled
   - CableLabs Configuration Script—Disabled

b. In the case of a Firmware File, additionally enter the file version and a suitable description for that version.

Step 5 Click **Submit.**

Note File sizes up to 4 MB are supported. If the size of the file that you are adding is over 4 MB, an error appears.

The View Files page appears, indicating that the file has been added.

Viewing Files

To view the contents of a DOCSIS or PacketCable voice technology file:

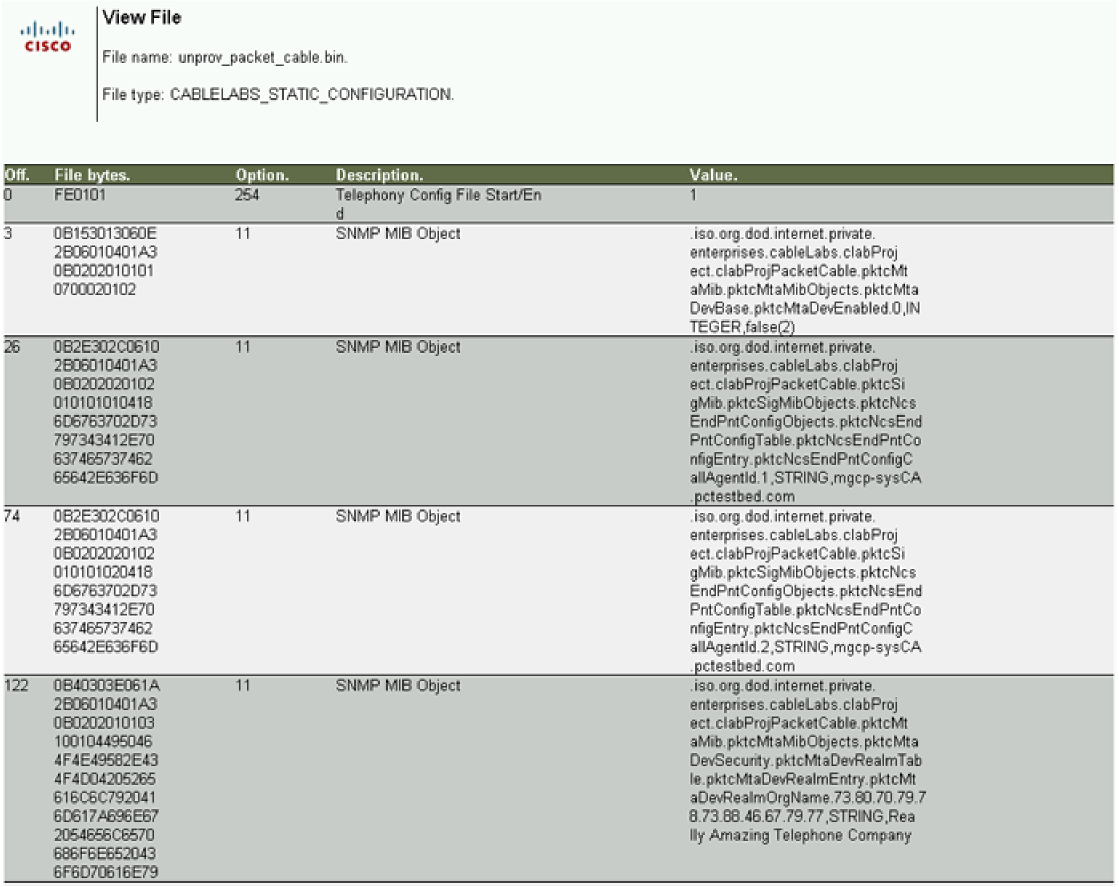
Step 1 From the View Files page, search for the required file using the file type or file name search options.

Step 2 Click the **View Details** icon (🔍) corresponding to the file.

The View File page appears with details of the file contents.

Figure 13-1 identifies sample binary file content.

Figure 13-1 Sample Binary File Content



View File

File name: unprov_packet_cable.bin.

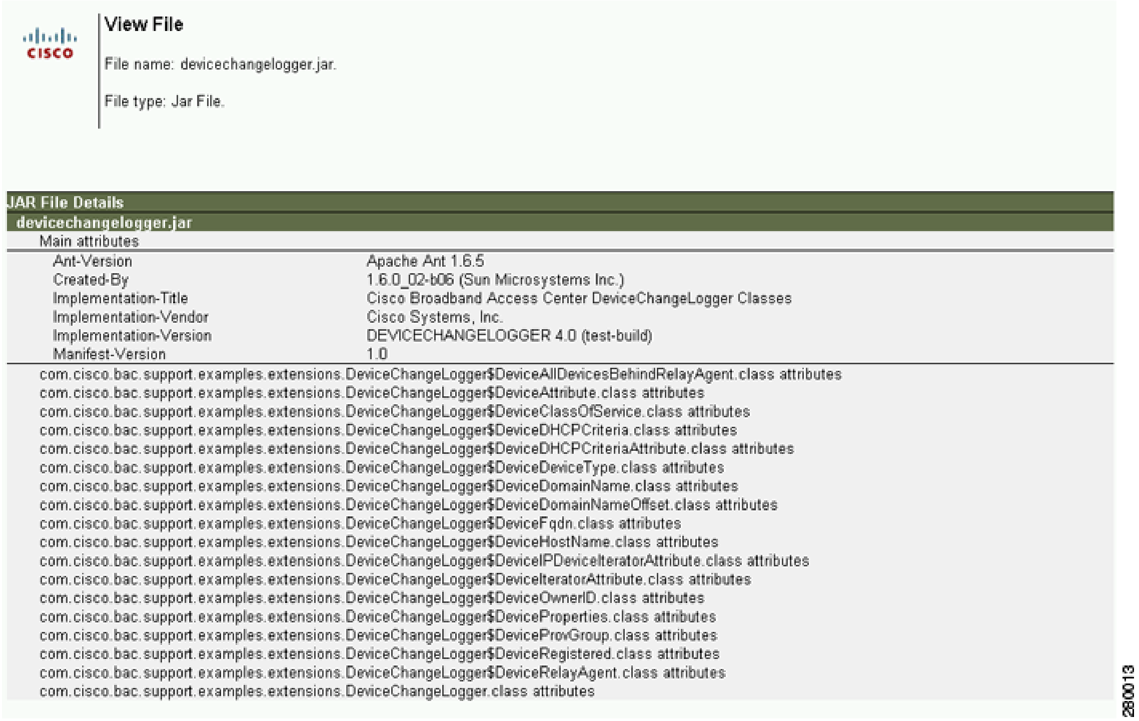
File type: CABLELABS_STATIC_CONFIGURATION.

Off.	File bytes.	Option.	Description.	Value.
0	FE0101	254	Telephony Config File Start/End	1
3	0B153013060E2B06010401A30B02020101010700020102	11	SNMP MIB Object	.iso.org.dod.internet.private.enterprises.cableLabs.clabProject.clabProjPacketCable.pktcMtaMib.pktcMtaMibObjects.pktcMtaDevBase.pktcMtaDevEnabled.0,INTEGER,false(2)
26	0B2E302C06102B06010401A30B02020201020101010104186D6763702D73797343412E7063746573746265642E636F6D	11	SNMP MIB Object	.iso.org.dod.internet.private.enterprises.cableLabs.clabProject.clabProjPacketCable.pktcSigMib.pktcSigMibObjects.pktcNcsEndPntConfigObjects.pktcNcsEndPntConfigTable.pktcNcsEndPntConfigEntry.pktcNcsEndPntConfigCallAgentId.1,STRING,mgcp-sysCA.pctestbed.com
74	0B2E302C06102B06010401A30B02020201020101010204186D6763702D73797343412E7063746573746265642E636F6D	11	SNMP MIB Object	.iso.org.dod.internet.private.enterprises.cableLabs.clabProject.clabProjPacketCable.pktcSigMib.pktcSigMibObjects.pktcNcsEndPntConfigObjects.pktcNcsEndPntConfigTable.pktcNcsEndPntConfigEntry.pktcNcsEndPntConfigCallAgentId.2,STRING,mgcp-sysCA.pctestbed.com
122	0B40303E061A2B06010401A30B020201010310010449504F4E49582E434F4D04205265616C6C792041 6D617A696E672054656C6570686F6E6520436F6D70616E79	11	SNMP MIB Object	.iso.org.dod.internet.private.enterprises.cableLabs.clabProject.clabProjPacketCable.pktcMtaMib.pktcMtaMibObjects.pktcMtaDevSecurity.pktcMtaDevRealmTable.pktcMtaDevRealmEntry.pktcMtaDevRealmOrgName.73.80.70.79.78.73.88.46.67.79.77,STRING,Really Amazing Telephone Company

Note The output featured in this graphic has been trimmed.

Figure 13-2 identifies sample JAR file content.

Figure 13-2 Sample JAR File Content



View File

File name: devicechangelogger.jar.

File type: Jar File.

JAR File Details

devicechangelogger.jar

Main attributes

Ant-Version	Apache Ant 1.6.5
Created-By	1.6.0_02-b06 (Sun Microsystems Inc.)
Implementation-Title	Cisco Broadband Access Center DeviceChangeLogger Classes
Implementation-Vendor	Cisco Systems, Inc.
Implementation-Version	DEVICECHANGELOGGER 4.0 (test-build)
Manifest-Version	1.0

```
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceAllDevicesBehindRelayAgent.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceAttribute.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceClassOfService.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceDHCPCriteria.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceDHCPCriteriaAttribute.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceDeviceType.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceDomainName.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceDomainNameOffset.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceFqdn.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceHostName.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceIPDeviceIteratorAttribute.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceIteratorAttribute.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceOwnerID.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceProperties.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceProvGroup.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceRegistered.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger$DeviceRelayAgent.class attributes
com.cisco.bac.support.examples.extensions.DeviceChangeLogger.class attributes
```

Replacing Files

To replace an existing file:

Step 1 From the View Files page, click the Files link that corresponds to the file you want to replace.

The Replace File page appears. Note that the selected filename already appears on this page.

Step 2 Enter the path and filename of the source file that is to replace the file present in the RDU database. If you do not know the exact name or location of the source file, use **Browse** to navigate to the desired directory and select the file.

Step 3 Click **Submit**.

After submitting the replacement file, a confirmation page appears to indicate that, after replacement, Cisco BAC will regenerate configurations for the affected devices.

Step 4 Click **OK**.

The View Files page appears.

The configuration for all devices using this file through a Class of Service is regenerated after the replacement is finished.

Exporting Files

You can copy files to your local hard drive using the export function.

Note The procedure described below assumes that you are using Internet Explorer. This procedure is different if you are using Netscape Navigator.

To export a file:

Step 1 From the View Files page, click the Files link that corresponds to the file you want to export.

Step 2 Identify the file that you want to export.

Step 3 Click the **Export** icon (📤).

You are prompted to either open the file or save it.

Step 4 Return to the Cisco BAC user interface.

Deleting Files

To delete an existing file:

Step 1 From the View Files page, locate the file you want to delete using the search option.

The appropriate files appear in the Files list.

Step 2 Choose the appropriate file or files.

Step 3 Click **Delete.**

Caution Deleting a template file that is not directly linked to a Class of Service, but is referenced by another template file that is linked to a Class of Service, will cause the configuration regeneration service to fail.

Note You cannot delete a file that has a Class of Service associated with it. You must remove the Class of Service association before proceeding. See Configuring Class of Service, page 13-1, for additional information.

Managing Licenses

Software licenses are used to activate specific features or to increase the functionality of your installation. This section describes Cisco BAC handling of different licenses. For details on the licensing changes in this release and how to obtain your license file, see the *Release Notes for Cisco Broadband Access Center 4.2*.

Cisco BAC licenses are available either as a permanent or an evaluation license.

- Permanent—A permanent license is purchased for use in your network environment and activates the specific features for which it is intended.
- Evaluation—An evaluation license enables functionality for a specific length of time.

Cisco BAC evaluation licenses become invalid on a predetermined date. As such, evaluation licenses must be created when needed. To create your evaluation license, contact your Cisco representative, who will generate the necessary license file online and forward it to you via e-mail.

Cisco BAC enables licensing using a service file. These licenses allow you to provision a set number of services using Cisco BAC. Each service translates to three IP addresses provisioned in the system; thus, a 10,000 service license equates to 30,000 IP addresses. The license file that you receive will contain the number of services that are licensed.

Caution Do not edit your license file. Changing the data in any way invalidates the license file.

Using the service license, you can provision any device type in any combination up to the maximum number that is stated in the license file. The device types that Cisco BAC supports in this release are:

- DOCSIS cable modems
- PacketCable MTAs
- CableHome WAN-MAN and WAN-Data devices
- Computers
- Custom CPE

Note You still require separate licenses for the following Cisco BAC components:

- The DPE
- The KDC, if you configure your network to support voice technology

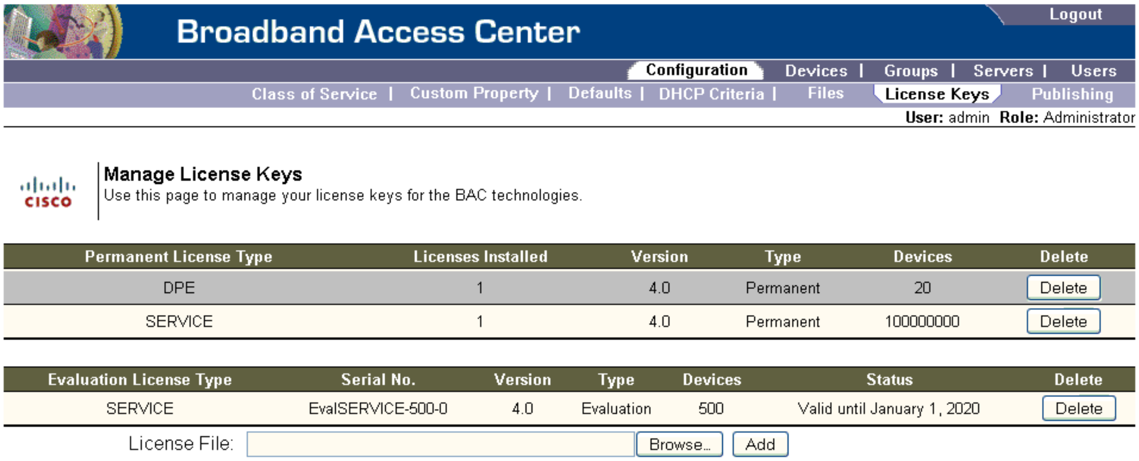
While you must install the DPE license from the administrator user interface, the KDC license continues to be proprietary as in previous Cisco BAC releases, and is licensed during Cisco BAC installation.

This Cisco BAC release enables you to install permanent and evaluation licenses at the same time. In addition, it also allows you to install more than one evaluation licenses. This enables you to increase your device limit when you are in short of licenses till you purchase a permanent license.

While you can install more than one evaluation license, expired license can be deleted and a new evaluation license (with a later expiry date), or a permanent license can be added. While deleting the expired license, ensure that the device limit of the new license at least equals the number of devices that is currently stored in the database.

Figure 13-3 identifies a sample Manage License Keys page, which displays a list of service licenses that have been entered for your implementation.

Figure 13-3 Manage License Keys Page


Broadband Access Center
Logout
Configuration
Devices | Groups | Servers | Users
Class of Service | Custom Property | Defaults | DHCP Criteria | Files | License Keys | Publishing
User: admin Role: Administrator
License File:
Browse...
Add
280015

Manage License Keys

Use this page to manage your license keys for the BAC technologies.

Permanent License Type	Licenses Installed	Version	Type	Devices	Delete
DPE	1	4.0	Permanent	20	Delete
SERVICE	1	4.0	Permanent	100000000	Delete

Evaluation License Type	Serial No.	Version	Type	Devices	Status	Delete
SERVICE	EvalSERVICE-500-0	4.0	Evaluation	500	Valid until January 1, 2020	Delete

Adding a License

Obtain your new license file via the claim process described in the *Release Notes for Cisco Broadband Access Center 4.2*. After you receive your license file, save each file to the system on which you plan to launch the Cisco BAC administrator user interface.

To add a permanent or evaluation license:

Step 1 Choose **Configuration > License Keys**.

Note If you are uploading a license for the first time, you can use the license link that appears on the Main Menu.

The Manage License Keys page appears.

Step 2 In the License File field, enter the complete path to the location of the permanent or evaluation license file on your local system.

Or, click **Browse** and navigate to the license file. Remember to include the name of the license file while specifying the pathname.

Step 3 Click **Add**.

The Manage License Keys page appears with the details of the services or the DPEs that are licensed to be used.

Deleting a License

You can choose to delete any license—evaluation or permanent—that appears on the Manage License Keys page.

Note You cannot delete a license if doing so brings the licensed capacity of the system below the number of devices provisioned in the system.

To delete a license:

Step 1 Choose **Configuration > License Keys**.

The Manage License Keys page appears.

Step 2 Click the **Delete** button corresponding to the permanent or evaluation license that you want to delete.

A confirmation dialog box appears.

Step 3 To confirm deleting the license, click **Yes**.

If you delete a license that contains multiple keys, the list of permanent licenses appears. Click the **Delete** button corresponding to the license that you want to delete.

The license key disappears from the Manage License Keys page.

Note To confirm if the license has been deleted, verify if the action has been recorded in *audit.log*.

Managing RDU Extensions

Creating a custom extension point is a programming activity that can, when used with the Cisco BAC administrator user interface, allow you to augment Cisco BAC behavior or add support for new device technologies.

Before familiarizing yourself with managing extensions, you should know the RDU extension points that Cisco BAC requires. At least one disruption extension must be attached to the associated technology’s disruption extension point when disrupting devices on behalf of a batch.

Table 13-11 lists the RDU extension points that Cisco BAC requires to execute extensions.

Table 13-11 Required RDU Extension Points

Extension Point	Description	Use	Specific to Technology?
Common Configuration Generation	Executed to generate a configuration for a device. Extensions attached to this extension point are executed after the technology-specific service-level selection extension and before the technology-specific configuration generation extensions. The default extensions built into this release do not use this extension point.	Optional	No
Configuration Generation	Executed to generate a configuration for a device.	Required	Yes
Device Detection	Executed to determine a device technology based on information in the DHCP Discover request packet of the device.	Required	No
Disruption	Executed to disrupt a device.	Optional	Yes
Publishing	Executed to publish provisioning data to an external datastore. The default extensions built into Cisco BAC do not include any publishing plug-ins.	Optional	No
Service-Level Selection	Executed to select the service level to grant to a device. Extensions attached to this extension point are executed before any common configuration generation extensions and the technology-specific configuration generation extensions.	Optional	Yes
Authentication	Executed to authenticate the user via remote authentication servers. Extensions will be attached to the extension points based on the authentication mode listed in RDU Defaults Page. RADIUS extensions are default built in authentication extensions in BAC.	Required	Yes

Managing extensions includes:

- Writing a New Class, page 13-29
- Installing RDU Custom Extension Points, page 13-30
- Viewing RDU Extensions, page 13-30

Note You can specify multiple extension points by specifying the extension points in a comma-separated list.

Writing a New Class

This procedure is included to better illustrate the entire custom extension creation process. You can create many different types of extensions; for the purposes of this procedure, a new Publishing Extension Point is used.

To write the new class:

Step 1 Create a Java source file for the custom publishing extension, and compile it.

Step 2 Create a manifest file for the JAR file that will contain the extension class.

Note For detailed information on creating a manifest file and using the command-line JAR tool, see Java documentation.

For example:

```
Name: com/cisco/support/extensions/configgeneration
Specification-Title: "DOCSIS TOD synchronization"
Specification-Version: "1.0"
Specification-Vendor: "General Cable, Inc."
Implementation-Title: "Remove the time-servers DHCP option"
Implementation-Version: "1.0"
Implementation-Vendor: "Cisco Systems, Inc."
```

Note Java JAR file manifests contain attributes that are formatted as name-value pairs and support a group of attributes that provide package versioning information. While Cisco BAC accepts extension JAR files that do not contain this information, we recommend that you include a manifest with versioning information in the files to track custom RDU extensions.

You can view manifest information from the administrator user interface via the **Servers > RDU > View Regional Distribution Unit Details** page. Detailed information on the installed extension JAR files and the loaded extension class files appears after the Device Statistics section. You can view manifest information from the RDU logs also.

Step 3 Create the JAR file for the custom extension point.

For example:

```
C:\>jar cm0vf manifest.txt removetimeservers.jar com
added manifest
adding: com/(in = 0) (out= 0)(stored 0%)
adding: com/cisco/(in = 0) (out= 0)(stored 0%)
adding: com/cisco/support/(in = 0) (out= 0)(stored 0%)
adding: com/cisco/support/extensions/(in = 0) (out= 0)(stored 0%)
adding: com/cisco/support/extensions/configgeneration/(in = 0) (out= 0)(stored 0%)
adding: com/cisco/support/extensions/configgeneration/
RemoveTimeServersExtension.class(in = 4038) (out= 4038)(stored 0%)
C:\>
```

Note You can give the JAR file any name. The name can be descriptive, but do not duplicate another existing JAR filename.

Installing RDU Custom Extension Points

After a JAR file is created, use the administrator user interface to install it:

Step 1 To add the new JAR file, see Adding Files, page 13-20.

Note Select the JAR file type. Use the Browse function to locate the JAR file created in the procedure described in Writing a New Class, page 13-29, and select this file as the Source File. Leaving the File Name blank assigns the same filename for both the source and the file. The filename is what you will see on the administrator user interface.

Step 2 Click **Submit**.

Step 3 Return to the RDU Defaults page and note if the newly added JAR file appears in the Extension Point JAR File Search Order field.

Step 4 Enter the extension class name in the Publishing Extension Point field.

Note The RDU returns an error if the class name does not exist within the JAR file. This error occurs mostly when replacing a JAR file, if, for example, the class you set up is not found in the replacement JAR file.

Step 5 Click **Submit** to commit the changes to the RDU database.

Step 6 View the RDU extensions to ensure that the correct extensions are loaded.

Viewing RDU Extensions

You can view the attributes of all RDU extensions directly from the View Regional Distribution Unit Details page. This page displays details on the installed extension JAR files and the loaded extension class files. See Viewing Regional Distribution Unit Details, page 12-32.

Publishing Provisioning Data

Cisco BAC has the capability to publish the provisioning data it tracks to an external datastore in real time. To do this, a publishing plug-in must be developed to write the data to the desired datastore. The Manage Publishing page identifies information such as the plug-in name, its current status (whether it is enabled or disabled), and switch to enable or disable it.

You can enable as many plug-ins as required by your implementation, but remember that the use of publishing plug-ins can decrease system performance.

Note Cisco BAC does not ship with any publishing plug-ins. You must create your own plug-ins and load them into Cisco BAC in the same way as JAR files are (see Adding Files, page 13-20). Then, manage the plug-ins from the Manage Publishing page.

Publishing Datastore Changes

To enable or disable a publishing plug-in:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Publishing** on the Secondary Navigation bar.

The Manage Publishing page appears. This page displays a list of all available database plug-ins and identifies the current status of each.

Step 3 Click on the appropriate status indicator to enable or disable the required plug-in. Note that as you click the status, it toggles between the two states.

Modifying Publishing Plug-In Settings

These settings are a convenient way for plug-in writers to store plug-in settings in the RDU for their respective datastore. To modify the publishing plug-in settings:

Step 1 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Publishing** on the Secondary Navigation bar, and the Manage Publishing page appears.

Step 3 Click the link corresponding to the plug-in you want to modify. The Modify Publishing Plug-Ins page appears.

Table 13-12 identifies the fields shown in the Modify Publishing Plug-Ins page.

Table 13-12 Modify Publishing Plug-Ins Page

Field	Description
Plug-In	Identifies the publishing plug-in name.
Server	Identifies the server name on which the datastore resides.
Port	Identifies the port number on which the datastore resides.
IP Address	Identifies the IP address of the server on which the datastore resides. This address is usually specified when the server name is not used.
User	Identifies the user to allow access to the data stored.
Password	Identifies the user’s password, which allows access to the data stored.
Confirm Password	Confirms the password entered above.

Step 4 Enter the required values in the Server, Port, IP Address, User, Password, and Confirm Password fields. These are all required fields and you must supply this information before proceeding.

Step 5 Click **Submit** to make the changes to the selected plug-in.

Automatic FQDN Generation

When configuring the PacketCable voice technology, a fully qualified domain name (FQDN) must reside in the Cisco BAC database for each voice device, because the KDC queries the registration server for that FQDN. The Cisco BAC automatic FQDN generation feature is not limited to any single voice technology; it can be used by any Cisco BAC technology.

Automatically Generated FQDN Format

Cisco BAC automatically generates FQDNs using the MAC address of a device or using the DHCP Unique Identifier (DUID) of an IPv6 device.

An automatically generated FQDN using a MAC address follows this format:

`prefix{htype-hlen-aa-bb-cc-dd-ee-ff | 00:00:00:00:00:00:00:00}suffix.domain`

- *prefix*, *suffix*, and *domain*—Identify the information that you set from the Cisco BAC administrator user interface or the provisioning API.
- *htype*, *hlen*, and aa-bb-cc-dd-ee-ff—Identify the device MAC address. For example, 1,6,aa-bb-cc-dd-ee-ff.
- 00:00:00:00:00:00:00:00—Identifies the DUID of an IPv6 device.

The entry of a prefix and suffix property is optional. If you do not specify these properties, and a hostname is not specified during PacketCable MTA provisioning and, if neither the prefix nor suffix property is defined in the Cisco BAC property hierarchy, the device MAC address or the device DUID followed by the domain name is used as the generated FQDN.

The FQDN format changes if you specify only the:

- Prefix and the device ID:
  `prefix{htype-hlen-aa-bb-cc-dd-ee-ff | 00:00:00:00:00:00:00:00}.domain`
- Suffix and the device ID:
  `{htype-hlen-aa-bb-cc-dd-ee-ff | 00:00:00:00:00:00:00:00}suffix.domain`

For example:

- A device with prefix **aaa**, suffix **bbb**, and MAC address **1,6,aa:bb:cc:dd:ee:ff** will have this FQDN generated:

  ```
  aaa1-6-aa-bb-cc-dd-ee-ffbbb.domain
  ```

- A device with only MAC address **(1,6,aa:bb:cc:dd:ee:ff)** will have this FQDN generated:

  ```
  1-6-aa-bb-cc-dd-ee-ff.domain
  ```

- A device with prefix **aaa**, suffix **bbb**, and DUID **00:00:00:00:00:00:00:00** will have this FQDN generated:

  ```
  aaa00-00-00-00-00-00-00-00bbb.domain
  ```

- A device with only DUID **00:00:00:00:00:00:00:00** will have this FQDN generated:

  ```
  00-00-00-00-00-00-00-00-00-aa.domain
  ```

- A device with prefix **aaa** and MAC address **1,6,aa:bb:cc:dd:ee:ff** will have this FQDN generated:

  ```
  aaa1-6-aa-bb-cc-dd-ee-ff.domain
  ```

- A device with suffix **bbb** and MAC address **1,6,aa:bb:cc:dd:ee:ff** will have this FQDN generated:

```
1-6-aa-bb-cc-dd-ee-ffbbb.domain
```

When configuring for PacketCable and other technologies, the domain name property must also be configured. If you do not specify a domain name while provisioning a PacketCable MTA, the Cisco BAC property hierarchy is searched and, if it is not found, the MTA is not provisioned.

If you do specify the domain name during MTA provisioning, that domain name is used regardless of the domain name property that is specified in the Cisco BAC property hierarchy.

Properties for Automatically Generated FQDNs

Properties can be defined at any acceptable point in the Cisco BAC property hierarchy. You can use the System Defaults, Technology Defaults, DHCP Criteria, or Class of Service to accomplish this, and you can also do this at the device level.

FQDN Validation

There are a few things to consider when entering the information that is used to generate an FQDN. These include:

- Use only valid alphanumeric characters in the generated FQDN.
- Keep the length of each label (characters between the dots in the generated FQDN) to fewer than 63 characters.
- Do not allow the overall length of the generated FQDN to exceed 254 characters.

Note The FQDN supports host and domain names as per RFC1035.

Sample Automatic FQDN Generation

This section provides an example of creating an automatically generated FQDN.

Step 1 Choose the appropriate Class of Service, and set the */fqdn/domain* property value to the DNS domain for all devices using this Class of Service.For the purposes of this example, assume that the domain in use is example.com, and that you want to provision a set of PacketCable devices into that domain.

Note If you do not specify a domain, devices in the Class of Service will not receive a DHCP configuration from Cisco BAC.

Step 2 Click **Submit**.

In this example, a device with MAC address 1,6,aa:bb:cc:dd:ee:ff will yield an automatically generated FQDN of 1-6-aa-bb-cc-dd-ee-ff.example.com.

Additionally, enable the Automatic FQDN Generation radio button in the device’s default configuration. See Configuring Defaults, page 13-6.