CHAPTER 17

Configuring Broadband Access Center

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

Configuring the Class of Service

By using the Cisco BAC administrator user interface, you can configure the Classes of Service offered to your customers. You can use the administrator user interface to add, modify, view, or delete any selected Class of Service. Start with the Manage Class of Service page, as shown in Figure 17-1.

Figure 17-1 Manage Class of Service Page

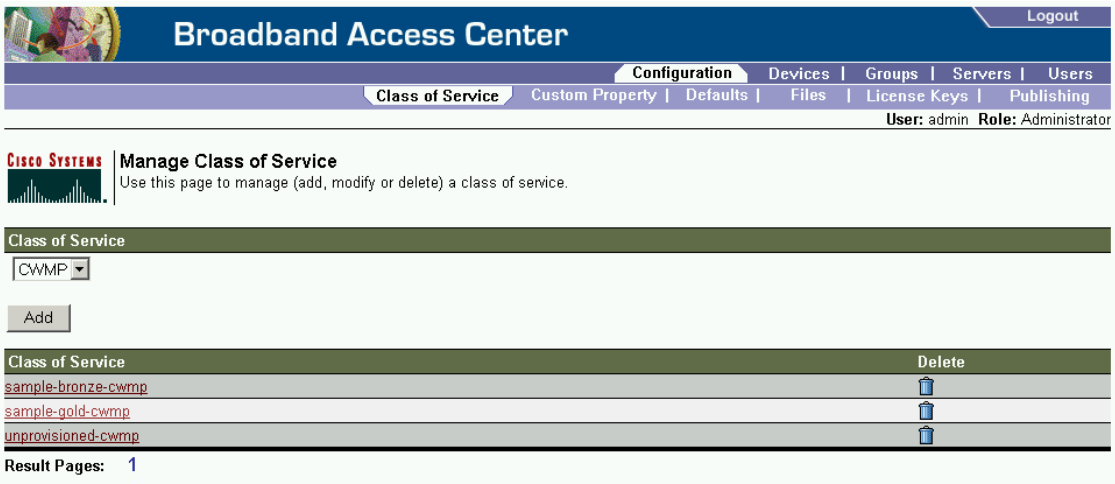


Table 17-1 identifies the fields and buttons shown in Figure 17-1.

Table 17-1 Manage Class of Service Page

Field or Button	Description
Class of Service	
Class of Service	A drop-down list that identifies the technology classes of service that you can search for. Available selections, as they appear on screen, include: • CWMP. **Note** For additional information on these areas of technology, see Configuring Defaults, page 17-6.
Add	Lets you add a new Class of Service.
Class of Service	
Class of Service list	Displays the names of Class of Service objects.
Delete	Lets you delete selected Classes of Service.

Table 17-2 identifies the fields and buttons shown in the Add Class of Service page.

Table 17-2 Add Class of Service Page

Field or Button	Description
Class of Service Name and Type	
Class of Service Name	Lets you enter the name of the new Class of Service.
Class of Service Type	A drop-down list that identifies the types of Classes of Service that you can select.
Configuration Template File	A drop-down list that identifies the configuration template file that you associate with a Class of Service.
Firmware Rule File	A drop-down list that identifies the firmware rules file that you associate with a Class of Service.
Property Name/Value	
Property Name	Specifies the appropriate property. You can select the correct property from the drop-down list.
Property Value	Specifies the value for the property name. You can select the correct value from the drop-down list.
Add	Adds the new Property Name:Property Value pair to create the new Class of Service.
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

Adding a Class of Service

To add a specific Class of Service:

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

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Click **Add**.

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

Step 4 Enter the name of your new class of service.

For example, assume that you want to create a new Class of Service called Gold-Classic for CWMP. You might enter **provisioned-cwmp** as the Class of Service Name, and choose CWMP from the service type drop-down list.

Step 5 Choose a Configuration Template File. For example, choose sample-cwmp-config.xml from the configuration file template drop-down list.

Step 6 Choose also a Firmware Rule File. For example, choose sample-cwmp-firmware-rules.xml from the firmware rule file drop-down list.

Step 7 Enter a Property Name and Property Value in the appropriate fields. This lets you configure standard or custom properties for this class of service object.

For example, choose as property name /IPDevice/connectionRequestMethod. Choose Discovered from the Property Value drop-down list and then continue with the rest of this procedure.

Note The API constant for /IPDevice/connectionRequestMethod is `IPDeviceKeys.CONNECTION_REQUEST_METHOD`.

Multiple Property Name:Property Value pairs could appear on this page. You use the **Delete** button to remove any unwanted pairs from the class of service.

Step 8 Click **Add** to add the property to the defining Class of Service.

Step 9 Click **Submit** to finalize the process or **Reset** to return all fields to their previous setting.

After submitting the Class of Service, the Manage Class of Service page appears to show the newly added Class of Service.

Modifying a Class of Service

You modify your Classes of Service by selecting the various properties and assigning appropriate property values. When creating a Class of Service for the first time you select all of the appropriate 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 Instruction Generation Service (IGS) to regenerate instructions for all affected devices and send instructions to the DPEs. IGS does this task as a background job. The status of the IGS can be observed using the View RDU Details page.

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

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

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Choose the Class of Service to be modified.

Step 4 Click the link corresponding to the correct Class of Service.

The Modify Class of Service page appears; note that the selected Class of Service name and type appear below the page description.

- 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 and then, after choosing the appropriate value for that property, click **Add**.
  - Repeat for any other properties 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.
  - Click the **Delete** button.
- To modify the value currently assigned to a property:
  - Delete the appropriate property as described above.
  - Add the same property back to the Class of Service while entering the new Property Value.

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

Step 5 Click **Submit** to make the modifications to the class of service.

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

Step 6 Click **OK**.

The modified Class of Service will be 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, you must ensure that there are no devices associated with that Class of Service.

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

To delete a Class of Service:

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

Step 2 Choose **Class of Service** from the Secondary Navigation bar.

Step 3 Click the **Delete** icon ( ) for the correct Class of Service, and a confirmation dialog box appears.

Note A Class of Service cannot be deleted if devices are associated with it or, if it is designated as the default Class of Service. Therefore, you cannot delete the **unprovisioned-cwmp** Class of Service object.

Step 4 Click **OK** to delete the file, or **Cancel** to return to the Manage Class of Service page. (See Figure 17-1.)

If you try to delete a Class of Service with devices associated with it, this error message is displayed:

```
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. In this example this is represented by *sample-COS*.

Configuring Custom Properties

Custom properties let you specify additional customizable device information to be stored in the RDU database. The Custom Property configuration page is found under the Configuration menu, and 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 this property hierarchy. See Authoring Configuration Templates, page 5-12, for how to use the property hierarchy. Properties can be configured on the following objects for use in the property hierarchy:

- Device
- Group
- Provisioning Group
- Class of Service

- Device Type
- System defaults

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

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

Step 2 Choose **Custom Property** on the Secondary Navigation bar,

The Manage Cisco BAC Custom Properties page appears.

- To add a custom property:

a. Click **Add** on the Manage Cisco BAC Custom Properties page,

The Add Custom Property page appears.

b. Enter the name of the new custom property.

c. Choose a custom property value type from the drop-down list.

d. Click **Submit** when complete.

After the property has been added to the administrative database, the Manage Cisco BAC Custom Properties page appears.

- To delete a custom property:

a. Identify the custom property to be deleted from the Manage Cisco BAC Custom Properties page.

b. Click the **Delete** icon corresponding to the correct custom property,

The custom properties deletion dialog box appears.

c. Click **OK** to delete the custom property.

Configuring Defaults

The Defaults page, found under the Configuration option, lets you access the default settings for the overall system, including the Regional Distribution Unit (RDU), and the CWMP technology.

Selecting Configuration Options

The procedure for configuring specific default types is identical. Complete this procedure to access the desired defaults page and then refer to the appropriate section within this chapter for a description of the various page components.

Step 1 Choose **Configuration** on either the Primary Navigation bar or Main Menu page.

Step 2 Choose **Defaults** from the Secondary Navigation bar.

The Configure Defaults page appears.

Step 3 Choose the correct default type from the list to the left of the screen.

The appropriate defaults page appears.

CWMP Defaults

The CWMP Defaults page (Figure 17-2) displays a list of CWMP technology configuration settings.

Figure 17-2 Configure CWMP Defaults Page

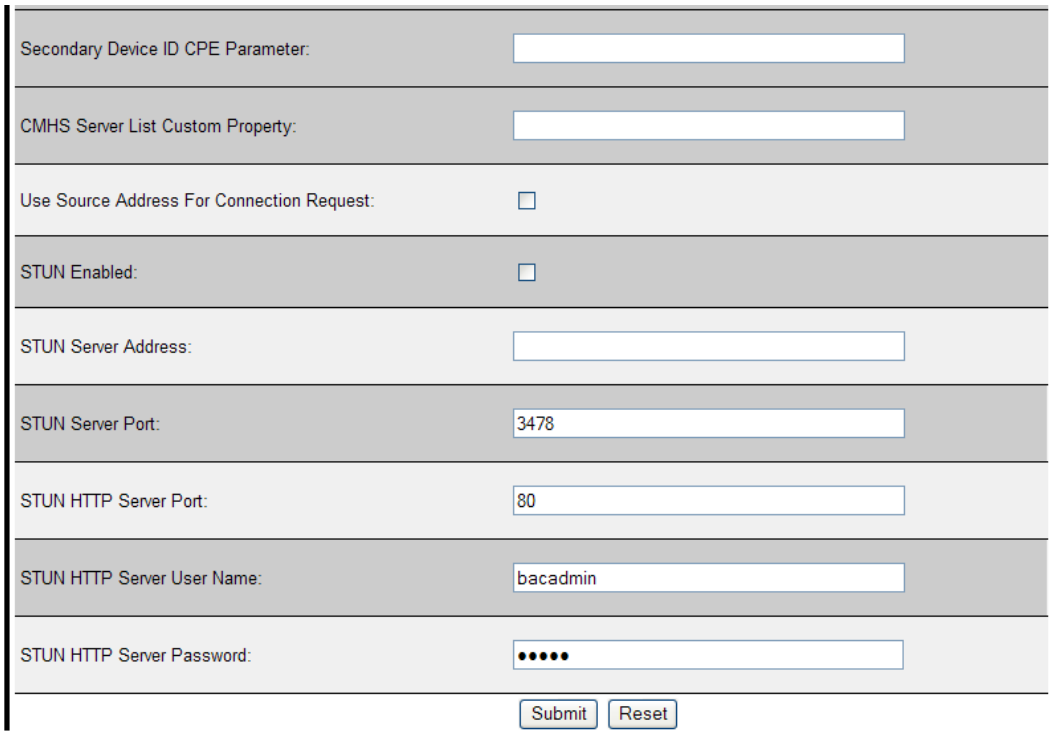


Table 17-4 describes all fields and buttons appearing in Figure 17-2.

Table 17-3 Configure CWMP Defaults Page

Field or Button	Description
Configuration Generation Extension Point	Identifies the common extension points executed before any other technology extension point is executed.
Activation Extension Point	Identifies the extension point that activates a device.
Service Level Extension Point	Identifies the extension point that determines what Class of Service to use for configuration generation and returns that information to the RDU.

Table 17-3 Configure CWMP Defaults Page (continued)

Field or Button	Description
Default Class of Service	Changes to the default Class of Service cause regeneration of instructions for all devices associated with the default Class of Service. The Instruction Generation Service (IGS) performs automatic regeneration of instructions and distributes them to appropriate DPEs. Any other changes made to this page do not affect the current devices.
Connection Request Method	Identifies the method in which Cisco BAC attempts to perform a connection request. You can choose to disable this feature by selecting the Disabled option, or choose from: • Discovered • Use FQDN • Use IP • LeaseQuery • Annex G • Use CMHS The selected method dictates how Cisco BAC determines the connection request URL to be used to contact the device.
Connection Request Path	Specifies the URL path based on the device IP address, using which the DPE constructs the Connection Request URL.
Connection Request Port	Specifies the device port number, using which the DPE constructs the Connection Request URL.
Device Operation Timeout	Specifies, in seconds, the time after which an operation on a device times out
Custom Discover Parameters	Specifies the custom parameter(s) in comma-separated format that are to be discovered from the device.
Custom Firmware Changed Parameters	Specifies custom parameters that are to be checked if the device reported a new firmware version.
Connection Request Master Secret	Specifies the value that is used along with the device identifier to generate a connection request password for a device, if autogeneration of connection request password is enabled.
Signature Key Name	Specifies the name of the key that is used by the gateway to look up the shared secret key. You must change the signature key name when the signature secret is changed.
Signature Validity	Specifies the number of seconds for which the signature is considered valid, following the signature timestamp. The default value is 3600.
Signature Secret	Specifies the secret that is used to compute the signature.
Secondary Device ID CPE Parameter	Specifies the IMEI number of the device which is used as the secondary device ID. It is stored in the device record in the RDU.
CMHS Server List Custom Property	Specifies the CMHS custom property name.It is not a predefined and must be specified.
Use Source Address For Connection Request	Check this box if you want to configure Cisco BAC to use the same source IP reported by the device.

Table 17-3 Configure CWMP Defaults Page (continued)

Field or Button	Description
STUN Enabled	Check this box if you want the STUN server to be enabled for the device.
STUN Server Address	Specifies the STUN server address.
STUN Server Port	Specifies the STUN server port.
STUN HTTP Server Port	Specifies the STUN server HTTP port.
STUN HTTP Server User Name	Specifies the STUN server HTTP user name.
STUN HTTP Server Password	Specifies the STUN server HTTP password
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

RDU Defaults

When you click the RDU defaults link, the RDU Defaults page (see Figure 17-3) appears. Use this page to configure settings affecting RDU operations.

Figure 17-3 Configure RDU Defaults Page

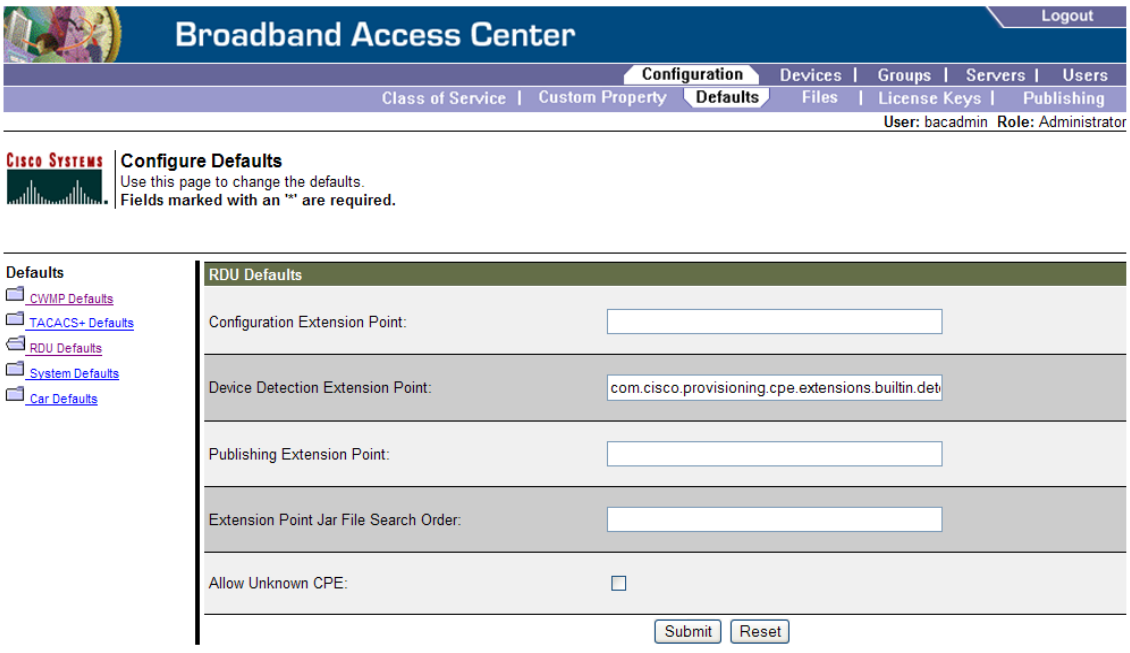


Table 17-4 describes all fields and buttons appearing in Figure 17-3.

Table 17-4 Configure RDU Defaults Page

Field or Button	Description
Configuration Extension Point	Identifies the configuration extension executed before any other technology extension is executed.
Device Detection Extension Point	Identifies the extension used to determine a device's type.
Publishing Extension Point	Identifies the extension to be used for an RDU publishing plug-in.This is useful when you need to publish RDU data to 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.
Allow Unknown CPE	Check this option if you wish to enable devices, that need to be provisioned but are not yet added to the RDU.
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

Note See Managing RDU Extensions, page 17-22, for related information on RDU extension points.

System Defaults

When you click the Systems Defaults link, the System Defaults page (see Figure 17-4) appears.

Figure 17-4 System Defaults Page

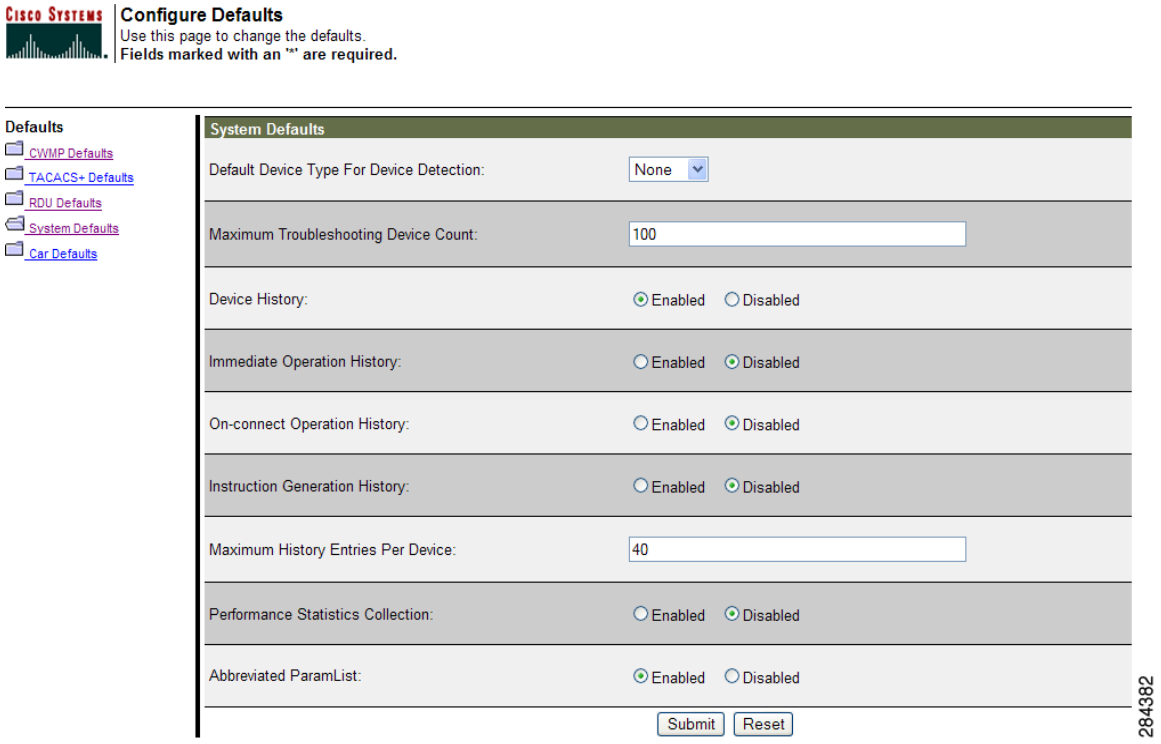


Table 17-5 describes all fields and buttons appearing in Figure 17-4.

Table 17-5 Configure System Defaults Page

Field or Button	Description
Default Device Type for Device Detection	Identifies the default device type for a device not previously registered in the RDU. The options include: • CWMP • None If the device detection extension is unable to identify the device type, the "default type" (CWMP or None) specifies the device type. If you set the Default Device Type as None, the device record is not added to the RDU. Unregistered devices can request the RDU for configurations only if you have enabled the **service cwmp** *num* **allow-unknown-cpe** option from the DPE command line interface. Otherwise, a request from an unknown device is not forwarded to the RDU.
Maximum Troubleshooting Device Count	Identifies the maximum number of devices that you can troubleshoot at any one time. The default number is 100.
Device History	Identifies if logging device record and device configurations is enabled or disabled.
Immediate Operation History	Identifies if logging of history of device operation initiated from the API using immediate mode is enabled or disabled.

Table 17-5 Configure System Defaults Page (continued)

Field or Button	Description
On-Connect Operation History	Identifies if logging of history of device operation initiated from the API using on-connect mode is enabled or disabled.
Instruction Generation History	Identifies if logging the history of device instruction generation is enabled or disabled.
Maximum History Entries Per Device	Defines the maximum number of entries of device history that will be stored for each device. The default number of entries is 40.
Performance Statistics Collection	Determines if statistics collection is enabled. See Monitoring Performance Statistics, page 11-14, on performance statistics.
Abbreviated ParamList	Enable this if you want to abbreviate the parameter names available in the configuration template. If enabled, parameter names are replaced with a dot (.).
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

TACACS+ Defaults

When you click the TACACS+ Defaults link, the TACACS+ Defaults page appears.

Figure 17-5 TACACS+ Defaults Page

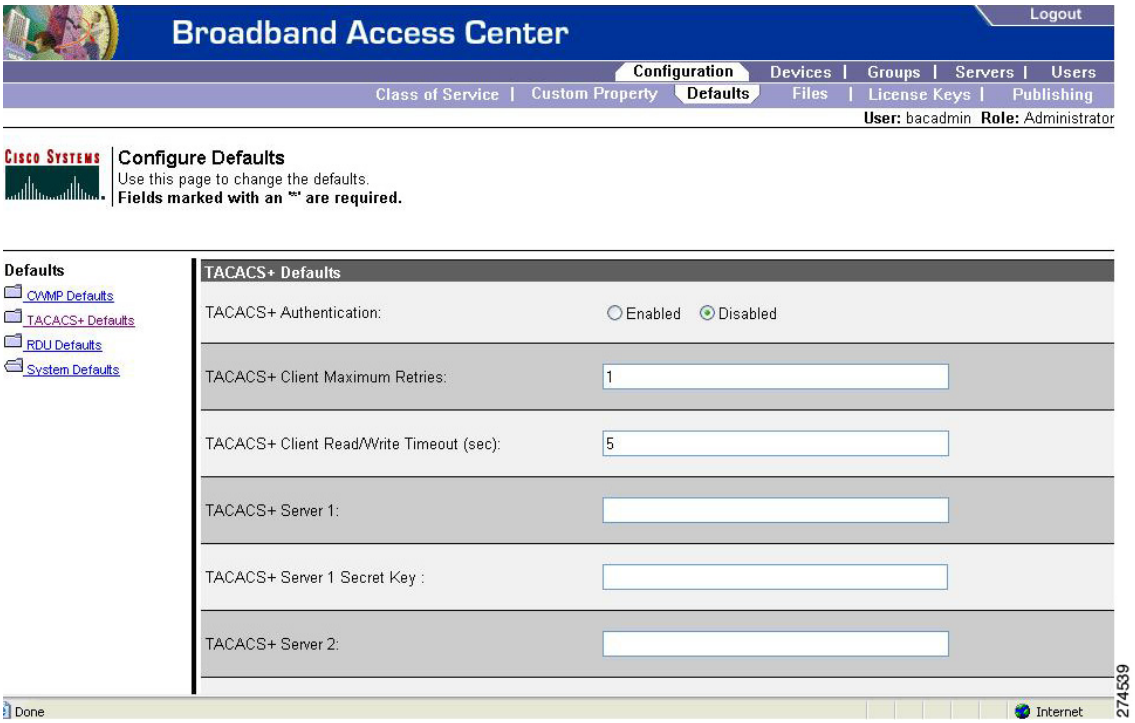


Table 17-6 describes all fields and buttons appearing in Figure 17-5.

Table 17-6 Configure TACACS+ Defaults Page

Field or Button	Description
TACACS+ Authentication	Allows you to enable or disable TACACS+ Authentication. TACACS+ Authentication is disabled by default.
TACACS+ Client Read/Write timeout	Specifies the duration that the TACACS+ client waits for a TACACS+ server to reply to TACACS+ protocol requests. The range is from 1 to 300 seconds. The default is 5 seconds and applies to all TACACS+ servers
TACACS+ Client Maximum retries	Specifies the number of times the TACACS+ client attempts a valid TACACS+ protocol exchange with a TACACS+ server if it fails to respond to the initial request. The range is from 0 to 10. The default is 1 and applies to all TACACS+ server defined

Field or Button	Description
TACACS Server 1	Specifies the IP address or the hostname of the TACACS+ server that has the highest priority and serves as the first choice for the TACACS+ clients. When TACACS+ authentication is enabled, the client attempts user login authentication to each server sequentially in the list until a successful authentication exchange is achieved, or the list is exhausted. If the list is exhausted, the client automatically falls back to the local authentication mode.
TACACS Server 1 Secret Key	Specifies the secret key used for encryption between the RDU and the TACACS+ server 1. The secret key is stored in the RDU database.
TACACS Server 2	Specifies the IP address or the hostname of the TACACS+ server that is queried by the TACACS+ client when the TACACS+ server 1 is unreachable.
TACACS Server 2 Secret Key	Specifies the secret key used for encryption between the RDU and the TACACS+ server 2.
TACACS Server 3	Specifies the IP address or the hostname of the TACACS+ server that is queried by the TACACS+ client when the TACACS+ server 1 and TACACS+ server 2 are unreachable.
TACACS Server 3 Secret Key	Specifies the secret key used for encryption between the RDU and the TACACS+ server 3.
TACACS Server 4	Specifies the IP address or the hostname of the TACACS+ server that is queried by the TACACS+ client when the TACACS+ server 1, TACACS+ server 2 and TACACS+ server 3 are unreachable.
TACACS Server 4 Secret Key	Specifies the secret key used for encryption between the RDU and the TACACS+ server 4.
TACACS Server 5	Specifies the IP address or the hostname of the TACACS+ server that is queried by the TACACS+ client when the TACACS+ server 1, TACACS+ server 2, TACACS+ server 3 and TACACS+ server 4 are unreachable.
TACACS Server 5 Secret Key	Specifies the secret key used for encryption between the RDU and the TACACS+ server 5.
Submit	Activates or implements the changes you have made.
Reset	Returns all settings to their previous settings.

If you remove one TACACS+ server and replace it with another server, the newly added server will have the same priority as the removed server.

To change the order of the TACACS+ servers in the priority list, remove all server addresses and re-enter them in the desired order.

Managing Files

By using the Cisco BAC administrator user interface, you can manage the template files and the parameter dictionaries for dynamic generation for CWMP files, or software images for devices (see Figure 17-6). You can add, delete, replace, or export any file type, including:

- Configuration Template—These are XML files that contain CWMP configuration policy, including parameter value settings, Notification attributes and Access Control attributes. See Authoring Configuration Templates, page 5-12, for additional information.
- Firmware File—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. See Firmware Management, page 6-1, for additional information.
- Firmware Rules Template—These are XML files written according to a published schema document. Each firmware rules template contains one or more rules that trigger firmware updates based on specific conditions. Firmware Management, page 6-1, for additional information.
- JAR File—This file type is used to load Cisco BAC extensions.
- Parameter Dictionary—These are XML files that list valid objects and parameters used by Cisco BAC to configure a device. The dictionaries validate the objects and parameters used in the configuration and firmware rule templates. See Parameter Dictionaries, page 7-1, for additional information.
- Parameter List—These XML files list a predefined set of parameters from the device that are retrieved every time the device contacts Cisco BAC.

Note Figure 17-6 is displayed after clicking the Search button on the Manage Files page.

Figure 17-6 Manage Files Page

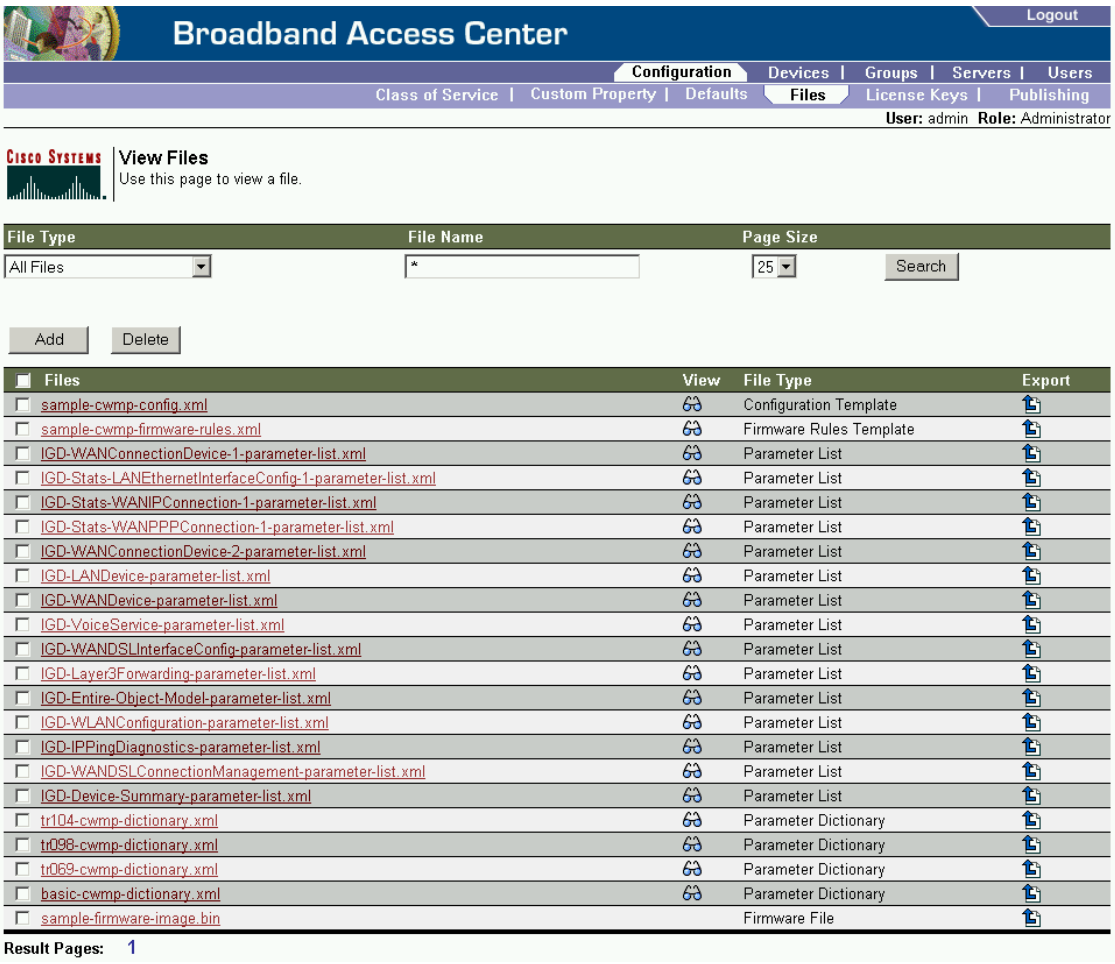


Table 17-7 identifies the fields and buttons shown in Figure 17-6.

Table 17-7 Manage Files Page

Field or Button	Description
File Type	
File Type	Identifies the file type.
File Name	Identifies the file name. This value can be a complete file name or can contain a wildcard character at the start of the string to match all files with a given suffix.
Page Size	Identifies the length of page to be displayed.
Search	Initiates the search for files with a name that matches the selected File Type and File Name search parameters.
Add	Adds a new file.
Delete	Removes any selected files from the database.
Files	

Table 17-7 Manage Files Page (continued)

Field or Button	Description
File Type	
Files list	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 it can be deleted.
View	Displays the details of the selected file.
File Type	Identifies the type of file; for example, Configuration Template, Firmware Rules Template, Parameter List.
Export	Exports any selected file to the client's computer.

Adding Files

To add an existing file to the RDU database:

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

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

The View Files page appears.

Step 3 Click **Add.**

Step 4 Choose the File Type.

Note For Firmware file type, two additional fields are provided: Firmware Version and Description, both of which are purely informational. You can enter any string in these fields.

Step 5 Enter the Source File Name and the File Name.

If you do not know the exact name of the source file, use the **Browse** function to locate the desired directory and select the file. By default, file sizes up to 10 MB are supported.

Step 6 Click **Submit.**

The View Files page appears to indicate that the file has been added.

Cisco BAC now extends the http file service so that it can read the firmware file from the DPE file system or DPE cache

When the firmware image size is very large (say 100 MB), adding the file through RDU may not be efficient. These files can be manually transferred to all the DPEs using tools such as scp, ftp and later when device requests for these files, they can be transferred to the device from the DPE.

Viewing Files

To view the contents of a file:

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

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

The View Files page appears.

Step 3 Search for the required file by using File Type.

Step 4 Click the **View Details** icon () corresponding to the File Type you had specified for a search.

The View File page appears.

Replacing Files

To replace an existing file:

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

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

Step 3 Select the link that corresponds to the file you want to replace from the search output list.

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

Step 4 Enter the path and filename of the source file to be used as a replacement for the displayed filename.

Note If you do not know the exact name or location of the source file, use the **Browse** function to locate the desired directory and select the file.

Step 5 Click **Submit**.

If you are updating a configuration or firmware template which is associated with a Class of Service, after submitting the replacement file, a confirmation page appears to indicate that Cisco BAC will regenerate instructions for the affected devices.

The Instruction Generation Service automatically regenerates instructions for all devices associated with this template using the Class of Service association and sends new instructions to the appropriate DPEs.

Step 6 Click **OK**

The View Files page appears.

Exporting Files

You can copy files to your local hard drive by 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 Choose **Configuration** on the Primary Navigation bar.

Step 2 Choose **Files** from the Secondary Navigation bar.

Step 3 Identify the file that you want to export.

Step 4 To export

- Binary files, click the **Export** icon () and you are prompted to either open the file or save it.
- XML files, such as templates, clicking the **Export** icon displays the file content. Therefore, you must right-click the **Export** icon and select **Save Target As**.

Step 5 Return to the Cisco BAC administrator user interface.

Deleting Files

Complete this procedure to delete an existing file:

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

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

Step 3 In the Files area, enter the filename of the file that you want to modify.

Step 4 Click **Search**.

The appropriate file appears in the Files list.

Step 5 Choose the appropriate file or files.

Step 6 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, causes the instruction regeneration service to fail.

Note You cannot delete a file associated with a Class of Service. You must remove the Class of Service association before proceeding. See Configuring the Class of Service, page 17-1, for additional information.

Managing License Keys

Software licenses are used to activate specific features or to increase the functionality of your installation. Each license is available as either a permanent license 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 amount of time after installation. You can upgrade an evaluation license to a permanent license by entering a new permanent license number.

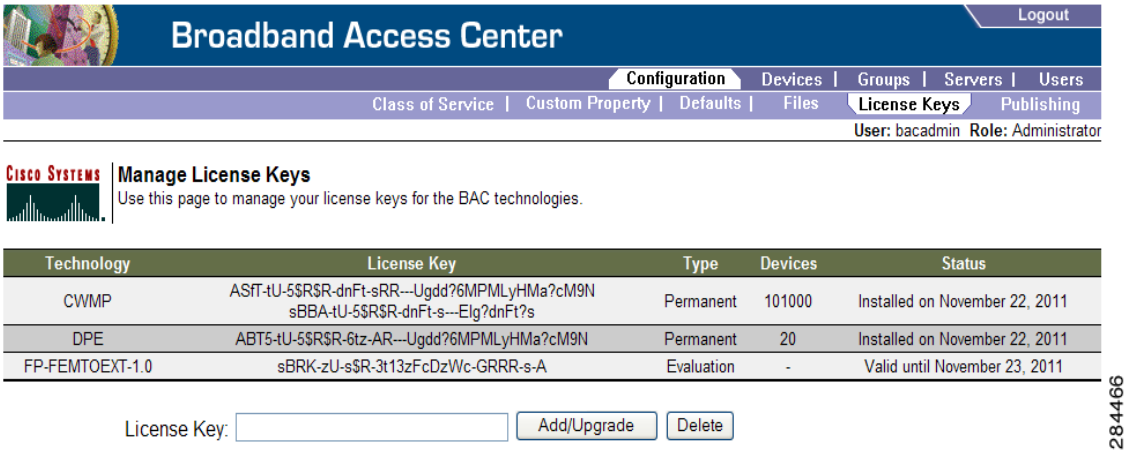
Caution Do not attempt to deploy into a fully operational network with an evaluation license key installed. Any provisioning done by using an evaluation license is disabled when that evaluation license expires.

When you upgrade from an evaluation license to a permanent license, you do not have to re-install the software or reconfigure Cisco BAC. You simply have to provide the permanent license using the Cisco BAC administrator user interface.

The Manage License Keys page (Figure 17-7) displays a list of licenses that have been entered for your implementation. This Cisco BAC release supports both evaluation and permanent licenses for the CWMP-compliant devices, and DPEs. The status of each available license appears as active, expired, or identifies the expiration date.

Note You can upgrade a permanent license to increase the number of authorized devices by adding an additional license. When you reach the limit of your number of licensed devices you cannot provision new devices, but existing devices that are already provisioned continue to receive service.

Figure 17-7 Manage License Keys Page



Adding and Modifying a License

To add, modify, or upgrade a license:

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

Step 2 Choose **License Keys** on the Secondary Navigation bar.

Step 3 Obtain your new license key from either your Cisco Systems representative or the Cisco Technical Assistance Center (TAC) website. See the Preface in this guide for TAC contact information.

Step 4 Enter the new license key in the License Key field.

Step 5 Click **Add/Upgrade** to install the new license key.

- If you enter a permanent license key, it overwrites the corresponding evaluation key (if that key was installed).
- If you enter a license key (permanent or evaluation) for a new technology, it will appear in the technology list.

Managing DPE Feature Pack Extensions

Cisco BAC provides a mechanism to license DPE feature packs extension. The feature pack licenses indicate the count of the devices that can be processed by the feature pack extension. The feature pack licenses can be added to the RDU through BAC Admin UI (**Configuration -> License Key**) or API independently with or without CWMP or DPE licenses.

You must buy enough CWMP licenses to cover the number of devices that would use the feature pack extensions. For instance, if you buy a Femto feature pack license for X number of devices and DLC feature pack license for Y number of devices, then you must buy CWMP License for at least X+Y number of devices.

The feature pack licensing leverages BAC's existing licensing mechanism. Adding feature pack licenses to the RDU is similar to adding other licenses such as DPE and CWMP.

The DPE feature pack license is similar to RDU, DPE and CWMP license. However, in the case of DPE feature pack license, the MANIFEST of the DPE feature pack extension JAR should have the attribute **Extension-Name** defined and its value should be in the format *FP- Technology Name - versionnumber*.

Where:

FP—Denotes it is a feature pack license.

ExtensionName— DPE extension technology name. For example, Femto, DLC, CPEaaS.

VersionNumber— DPE extension technology version. This version number must be the same or lower than the version of the feature pack license added in DPE. If not, the DPE registration fails.

A few examples for *FP- Technology Name - versionnumber* would be FP-CPEaas-1.0, FP-CPEaas2.0, FP-Femto-10, FP-DLC-1.0 and so on.

Writing a New Class for DPE Feature Pack Extensions

The instructions for writing a new class for DPE feature pack extension are similar to writing a new class for RDU. See Writing a New Class for RDU, page 17-23 for details how to write a new class. This section also provides details about how to add a new class and integrate it with the DPE.

An example of the manifest:

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.6.2
Created-By: 17.0-b16 (Sun Microsystems Inc.)
Implementation-Title: Cisco Broadband Access Center Femtocell Extension
Implementation-Version: FEMTOEXT 3.7 (test-build)
Implementation-Vendor: Cisco Systems, Inc.
Extension-Name: FP-femtoext-3.7
```

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 17-8 lists the RDU extension points that Cisco BAC requires to execute extensions.

Table 17-8 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

Table 17-8 Required RDU Extension Points (continued)

Extension Point	Description	Use	Specific to Technology?
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 through 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 for RDU, page 17-23
- Installing RDU Custom Extensions, page 17-24
- Viewing RDU Extensions, page 17-25

Note You can specify multiple extension points by making them run one after another. You do this by specifying the extensions points in a comma-separated list.

Writing a New Class for RDU

This procedure illustrates 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.

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: "TOD synchronization"
Specification-Version: "1.0"
Specification-Vendor: "General TW, Inc."
Implementation-Title: "Remove the time-servers DHCP option"
Implementation-Version: "1.0"
Implementation-Vendor: "Cisco Systems, Inc."
```

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 using 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 Extensions

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 17-17.

Use the Browse function to locate the Jar file created in the procedure, Writing a New Class for RDU, page 17-23, and select this file as the Source File; leaving the File Name blank assigns the same filename for both source and external. The filename is what you will see through the administrator user interface.

Step 2 Click **Submit**.

Step 3 Return to the RDU Defaults page and note that 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.

The RDU returns an error if the class name does not exist within the jar file or if Cisco BAC detects any other errors. 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.

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 care must be exercised because 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 17-17). 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. C

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 from enabled to disabled.

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,

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 17-9 identifies the fields shown in the Modify Publishing Plug-Ins page.

Table 17-9 Modify Publishing Plug-ins Page

Field or Button	Description
Plug-In	Identifies publishing plug-in name.
Server	Identifies the server name on which the data store resides.
Port	Identifies the port number on which the data store resides.
IP Address	Identifies the IP address of the server on which the data store resides. This 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	This is used to confirm 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, or click **Reset** to clear all fields on this page.

Configuring Lease Query

Cisco BAC, by default, binds to the IP addresses and ports that are described in the below table.

Table 17-10 Modify Publishing Plug-ins Page

Protocol	IP Address	Port
IPv4	WildCard	Any available port

The wildcard is a special local IP address. It usually means "any" and can only be used for bind operations.

You can also configure the IP address and port of your choice for lease query communication using the same properties. For example:

/cnrQuery/clientSocketAddress=10.1.2.3:166

Using this property, the DPE binds to the IP address and the port that you specify.