



Release Notes for Cisco Broadband Access Center 4.0

December 31, 2007

These release notes describe new software features and fixes to software issues in Cisco Broadband Access Center, Release 4.0.

Contents

- [Introduction, page 1](#)
- [System Components, page 2](#)
- [Supported Devices, page 2](#)
- [Supported Standards, page 3](#)
- [New and Changed Features, page 4](#)
- [Before Installing BAC 4.0, page 7](#)
- [Caveats, page 12](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)

Introduction

Cisco Broadband Access Center, referred to as BAC throughout this document, automates the tasks of provisioning and managing customer premises equipment (CPE) in a broadband service-provider network. The application provides a simple and easy way to deploy high-speed data, voice technology, and home networking devices.

BAC can be scaled to suit networks of virtually any size, even those deploying millions of devices. It also offers high availability, made possible by its distributed architecture with centralized management.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

BAC incorporates support for many technologies to provide provisioning services for your network. These technologies include:

- DOCSIS high-speed data
- PacketCable voice service, both Secure and Basic workflows
- Non-secure CableHome

This release provisions and manages CPE that is compliant with the DOCSIS 3.0 specification, the third generation of the data-over-cable systems specification. With IP version 6 (IPv6) being a large part of DOCSIS 3.0, this release supports DHCPv6 and DNSv6.

System Components

The BAC product comprises:

- The Regional Distribution Unit (RDU), which is the primary server in a BAC deployment. Through its extensible architecture, the RDU supports the addition of new technologies and services.
- The Device Provisioning Engine (DPE), which handles all device interactions with the RDU.
- Cisco Network Registrar extension points, which are the link between BAC and Network Registrar. Network Registrar provides BAC with the DHCP and Domain Name System functionality.
- The Key Distribution Center (KDC), which is a Kerberos server that authenticates PacketCable Multimedia Terminal Adapters (MTAs).
- An administrator user interface, which you can use to monitor and manage BAC.
- A Java provisioning application programming interface (API), which you use to integrate BAC into an existing operations support-system environment.

For information on installation, refer to [Before Installing BAC 4.0, page 7](#). Additionally, refer to the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*.

Supported Devices

BAC provides provisioning and managing of residential devices, namely DOCSIS cable modems and set-top boxes (STBs), PacketCable eMTAs, CableHome devices, and computers.

This release of BAC supports provisioning and managing of:

- IPv6 devices, which include:
 - Cable modems compliant with DOCSIS 3.0
 - Computers
 - STBs
- Video STBs, specifically the RNG-200 STB, which is based on the evolving OpenCable Application Platform.
- Variants of eSAFE (embedded Service/Application Functional Entities) devices, such as mixed-IP mode PacketCable Multimedia Terminal Adapters (MTAs). A mixed-IP mode MTA is an eSAFE device that consists of an IPv6 embedded cable modem and an IPv4 eMTA. This class of devices embeds additional functionality with cable modems, such as packet-telephony, home networking, and video.

As in previous releases, BAC continues to provision:

- Cable modems and STBs compliant with DOCSIS 1.0, 1.1, and 2.0
- Embedded Media Terminal Adapters (eMTAs) compliant with PacketCable versions 1.x
- Devices compliant with CableHome 1.0
- Computers

Supported Standards

BAC complies with these applicable Requests for Comments (RFCs), protocols, standards, and Internet Engineering Task Force (IETF) drafts:

- IPv6—Complies with RFC 2460 (IPv6 specification), 2461 (Neighbor Discovery protocol), 2462 (Stateless Address Autoconfiguration), 2463 (Internet Control Message Protocol–ICMP), 3513 (Addressing Architecture).
- DHCPv6—Complies with RFC 3315 (DHCPv6 specification), 3633 (IPv6 Prefix Options), 3736 (Stateless DHCP Service for IPv6), 4014 (Remote Authentication Dial-In User Service–RADIUS–Attributes Suboption for the Relay Agent Information Option), 4580 (Relay Agent Subscriber-ID Option), 4649 (Relay Agent Remote-ID Option), and 4704 (DHCPv6 Client Fully Qualified Domain Name (FQDN) Option).
- IPv4 and IPv6 interoperability—Complies with RFC 4038 (Application of IPv6 Transition) and 4472 (Operational Issues and Considerations with IPv6 DNS).
- TFTP and ToD servers—Complies with RFC 868 (Time Protocol) and 2349 (TFTP Blocksize Option).

Additionally, BAC complies with these applicable CableLabs and Comcast standards:

- DOCSIS 3.0 Specifications:
 - CM-SP-SECv3.0-I04-070518
 - CM-SP-PHY3.0-I04-070518
 - CM-SP-MULPIv3.0-I04-070518
 - CM-SP-OSSIv3.0-I03-070518
- DOCSIS 2.0 Specification CM-SP-RFI2.0-I12-071206
- DOCSIS L2VPN Specification CM-SP-L2VPN-I06-071206
- PacketCable MTA Device Provisioning Specification PKT-SP-PROV1.5-I03-070412
- CableHome CH-SP-CH1.0-I05-030801
- COMCAST-SP-RNG-200-ProvOSS-I04-070102
- OpenCable specification OC-SP-HOST2.0-CFR-I13-070323

New and Changed Features

These sections briefly describe new or modified features in the 4.0 release:

- [DOCSIS 3.0 and IPv6 Support, page 4](#)
- [STB Support, page 5](#)
- [Enhanced Scalability and Performance, page 5](#)
- [Improved Management, page 5](#)
- [Increased Security, page 6](#)
- [Enhanced Troubleshooting and Diagnostics, page 6](#)
- [New Installation, page 7](#)
- [Automated Migration, page 7](#)
- [Licensing Using Cisco Standard, page 7](#)

DOCSIS 3.0 and IPv6 Support

This BAC release introduces support for DOCSIS 3.0, which defines the third generation of the high-speed data-over-cable systems specification. DOCSIS 3.0 provides for:

- Provisioning of IPv6 devices
- Expanded addressability of network elements
- Increased channel capacity via channel bonding
- Enhanced network security
- Enhanced multicast capabilities
- New service offerings

This release enhances these existing features in BAC to facilitate IPv6 transport:

- Lease Query—You can request current IP address information directly from the Network Registrar DHCP servers in a provisioning group. This feature, thus, provides:
 - IP address information for device resets and management
 - Reporting details of IPv4 and IPv6 devices

You can also configure the IP addresses of the DHCP servers in the provisioning group using an autoconfiguration mechanism, which makes for easier network administration.

- TFTP and ToD Services—The BAC DPE provides integrated TFTP and Time of Day (ToD) services.
TFTP service—The DPE's high-performance TFTP service allows on-delivery customization that DOCSIS uses to mix time-sensitive information into the file that is to be delivered. This BAC release enhances the TFTP service to:
 - Support IPv6 transport.
 - Support compression of dynamic TFTP files that a DPE caches, thus enhancing DPE performance.

- Provide an optional block-size option, which specifies the number of data octets and allows the client and server to negotiate a block size more applicable to the network medium. The block-size option in BAC complies with RFC 2348.
- Maintain statistics for the number of TFTP packets that are processed for TFTPv4 and TFTPv6.

ToD service—The DPE's ToD service provides high-performance UDP implementation of RFC 868. This service provides:

- Support for IPv6 transport.
 - Statistics for the number of ToD packets that are processed for ToDv4 and ToDv6.
- SNMP support—The BAC RDU supports SNMP management over IPv6 to provide device disruption for IPv6 cable modems and STBs.

STB Support

This BAC release introduces support for the video STB, specifically the RNG-200 STB, which is based on the evolving OpenCable Application Platform.

Enhanced Scalability and Performance

This BAC release provides:

- Massive scalability of the RDU and the DPEs in your network. The RDU can support up to 60 million devices, and a provisioning group can support 2 million devices, of which 500,000 can be Secure PacketCable devices.
- Enhanced DPE synchronization with the RDU, rendering the process in the background so that the RDU is not overloaded with synchronization requests. The process is also updated to support requests for the DPE based on the DHCP Unique Identifier (DUID) of an IPv6 device.
- Enhanced performance of the template parser (which DOCSIS, PacketCable, and CableHome extensions use to provide dynamic configurations) to optimize generation of device configurations based on templates. Additionally, you can compress all configurations that are generated, thus decreasing overhead at the DPE to enhance server performance.
- Enhanced multivendor support by enabling scoping of Option 43 and its suboptions. It also gives you the option of using a single template to specify various TLV 43s from many vendors.

Improved Management

This BAC release enables you to manage your network better by introducing support for:

- Provisioning group properties on the property hierarchy—Enhances the flexibility that the BAC property hierarchy provides by including the properties of a device's provisioning group.
- Provisioning group capabilities—Allows you to control the device type support that must be enabled for the provisioning groups in your deployment. In earlier BAC releases, each DPE in a provisioning group registered what it was capable of supporting with the RDU at startup. This information was combined with that of other DPEs in the provisioning group to determine the device types that the group could support. Thus, the capabilities of a provisioning group were automatically enabled.

In this release, however, you must manually enable the capabilities of a provisioning group from the administrator user interface or the API. You can thus choose to enable only specific capabilities and ignore others in keeping with your requirements.

- “Services” interface on the DPE command line—Provides flexibility in configuring the DPE to suit your requirements. Using the “services” interface, you can choose to enable only certain services; for example, you can enable the TFTP service for IPv4 transport, but not for IPv6 transport. All services on the DPE are by default disabled.

Increased Security

This BAC release provides increased security via:

- User-configurable IP addresses and ports to support:
 - Multipathing—Earlier BAC versions enable you to configure a DPE interface for provisioning using the Solaris interface names. This BAC release enables you to configure the provisioning interfaces using the IP addresses of the DPE interface, thus allowing one interface to back up for another by switching its IP address in case of failure.
 - Multi-interface binding—When communicating with Network Registrar extension points, previous BAC DPEs rely on the operating system to determine the interface for use, because the extensions require the reply to come from the interface that the request was sent to. In this BAC release, you can configure this interface, which by default is all IPv4 interfaces.
 - Firewall compatibility—Earlier BAC releases rely on the operating system to determine the source interface and the source port in communications between the DPE and the RDU. In this BAC release, you can configure the source interface and the port, and thus segment management traffic and create firewall rules.
- CMTS MIC for DOCSIS 3.0—Supports DOCSIS 3.0 for the Extended CMTS MIC Configuration Setting that configures how the CMTS checks the integrity of a message. By providing 3.0 support for this setting, BAC uses advanced hashing techniques to detect unauthorized modification or corruption of the cable modem configuration file.
- Password policy—Enforces a password policy to access the RDU from the administrator user interface. The password that you use to log in to the administrator user interface must have at least 8 characters.
- HTTP over SSL (HTTPS)—Provides access to the administrator user interface using a secure SSL connection.

Enhanced Troubleshooting and Diagnostics

This BAC release provides options for:

- Device troubleshooting using the device ID—Enhances device troubleshooting to provide detailed records of device interactions with BAC servers using the IDs of the devices designated for troubleshooting. Using this feature, you can focus on a single device, identified by its MAC address or its DUID, and use that diagnostic information for further analysis.
- Server troubleshooting using diagnostics tool—Provides diagnostics scripts to collect performance statistics—down to a specific type of statistic—for BAC servers.

Using individual scripts, you can:

- Gather diagnostics concurrently
- Determine the status of diagnostics collection
- Stop diagnostics prematurely

This release also provides many scripts to collect server and system configuration data that may be required for support escalations. You can use additional scripts to bundle the diagnostics data for support.

New Installation

This BAC release provides an improved and flexible installer that uses the Solaris package system, rather than the InstallShield installer. The package installer gives you the option of installing from the command-line interface in interactive or noninteractive modes.

Automated Migration

This BAC release supports:

- Automatic migration of the RDU database from the 2.6.2.7 version to 4.0
- Automatic migration of the DPE cache
- Compatibility of the 4.0 RDU and DPE with earlier versions of Solaris DPEs and Network Registrar servers, respectively, for gradual online migration

Licensing Using Cisco Standard

This BAC release enhances licensing to provide flexible options, greater reliability and security, and ease of use. While earlier BAC versions used a proprietary model of licensing, this release incorporates support for FlexLM, a Cisco license management system.

In previous BAC releases, you were licensed for the technologies that provisioned the devices in your network. In this release, you are licensed to provision a specific number of services for any device type. Each service translates to three IP addresses that are provisioned in the system.

For more information, see [Licensing Requirements, page 8](#).

Before Installing BAC 4.0

Review the following information before you begin to install BAC 4.0.

- [System Requirements, page 8](#)
- [Licensing Requirements, page 8](#)
- [Installation Notes, page 12](#)

System Requirements

To successfully install BAC software on your system, you must meet these requirements:

- Operating system—You must install BAC on a Sun SPARC platform running the Solaris 9 or 10 operating system with at least 4 GB of memory. Cisco recommends that you use a Sun SPARC multiprocessor platform.



Note When enabling IPv6 support, you must use the Solaris 10 operating system.

- Network Registrar—You must have Cisco Network Registrar version 7.0 installed on the servers on which you are installing BAC extensions.
- Administrator user interface—At a minimum, you must have Microsoft Internet Explorer 6.0 (Service Pack 2) or Firefox 1.5.
- API client
 - Ensure that you install Java 1.6.0_02 to support the API client in release 4.0. API clients in versions earlier than 4.0, however, support JRE versions earlier than 1.6_0_02.
 - Ensure that the files *bpr.jar* and *bacbase.jar* are available in the classpath.

For detailed information on system requirements, refer to the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*.

Licensing Requirements

This BAC release moves away from the proprietary licensing model used previously and incorporates support for the FlexLM licensing system, a Cisco license management system. The new system provides enhanced reliability and security, ease of use, and flexible licensing options.

This section describes:

- [What Has Changed, page 9](#)
- [How to Obtain and Install Your Licenses, page 9](#)
 - [Obtaining a Permanent License, page 10](#)
 - [Obtaining an Evaluation License, page 10](#)
 - [Installing Your License, page 11](#)

What Has Changed

To successfully provision devices using BAC 4.0, note the licensing changes that [Table 1](#) describes.

Table 1 *Licensing Changes in BAC 4.0*

Previous BAC Releases	In BAC 4.0...
You received a license key for each technology that provisioned the devices in your network.	You receive a service license to provision a specific number of services using BAC. Each service translates to three IP addresses that are provisioned in the system; for example, a 10,000 service license equates to 30,000 IP addresses. You can provision any device type using the service license. You still require separate licenses—permanent or evaluation—for the following BAC components: • The DPE • The KDC, if you configure your network to support voice technology Note While you must install the DPE license from the administrator user interface, the KDC license continues to be proprietary as in previous BAC releases, and is licensed during BAC installation.
You received license strings.	You receive a single license file. The license file contains one or more license keys that you have purchased for your deployment.
You received your license keys via e-mail as a single file.	You receive the appropriate license file via e-mail only after you request evaluation and permanent licenses by registering your purchase online. See Obtaining a Permanent License, page 10 .
Your evaluation licenses expired a specific number of days after installation.	Your evaluation licenses become invalid on a predetermined date. You receive an evaluation license only after contacting your Cisco representative. See Obtaining an Evaluation License, page 10 .

How to Obtain and Install Your Licenses

Each license in this release is available as a permanent license or an evaluation license.

- **Permanent**—You purchase a permanent license for use in your network environment and to activate the specific features for which it is intended.
- **Evaluation**—You purchase an evaluation license to enable functionality for a specific length of time. You can upgrade an evaluation license to a permanent license.



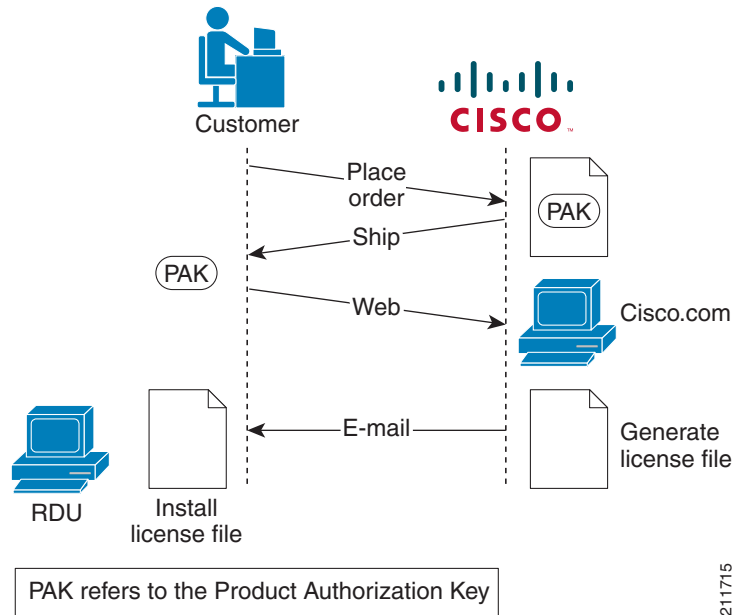
Caution

Do not attempt to deploy into a fully operational network with an evaluation license. When the evaluation license expires, you will not be able to use BAC to provision the devices in your network.

Obtaining a Permanent License

To request a permanent license, follow the procedure that [Figure 1](#) depicts.

Figure 1 **License Claim Process**



Note

With FlexLM licensing, you receive a Product Authorization Key (PAK) for each software CD package that you purchase. The PAK is affixed as a sticky label on the Software License Claim Certificate card that is included in your CD-ROM package.

To obtain a permanent license:

1. Keep your PAK handy and access <http://www.cisco.com/go/license>. You must have a valid Cisco.com account to log in to this site.

The Product License Registration website appears.

2. Complete the steps detailed at the Product License Registration page.



Note

During license registration, submit each PAK that you have received. For each PAK that you submit, a license file is generated and sent to you via e-mail.

3. Once you receive your license file, install it using the procedure described in [Installing Your License, page 11](#).

Obtaining an Evaluation License

For an evaluation license, contact your Cisco representative, who will generate the necessary key from the Cisco licensing website and e-mail it to you. Once you receive your license file, install it using the procedure described in [Installing Your License, page 11](#).

Installing Your License

Before installing your license file, ensure that you back up your licenses in case you have to reinstall the BAC software.

To install your permanent or evaluation license:

Step 1 Once you receive your license file, save each file to the system on which you plan to launch the BAC administrator user interface.

Step 2 Launch your web browser on that system.

Step 3 Enter the administrator's location using this syntax:

`http://machine_name:port_number/`



Note To access the administrator user interface via HTTPS, enter:

`https://machine_name:port_number/`

- *machine_name*—Identifies the computer on which the RDU is running.
- *port_number*—Identifies the computer port on which the server side of the administrator application runs. The default port number is:
 - 8100 for HTTP over TCP
 - 8443 for HTTP over SSL

The main login page appears.

Step 4 Enter the default username (**admin**) and the default password (**changeme**).

- a. If you are logging in for the first time, the Change Password screen appears.
- b. Enter a new password and confirm it. Ensure that the password that you enter has at least 8 characters.

Step 5 Click **Login**.

The Main Menu page appears.

Step 6 Click the license link at the top of the Main Menu page, or choose **Configuration > License Keys**.

The Manage License Keys page appears.

Step 7 In the License File field, enter the complete path to the location of the license file on your local system. Remember to include the name of the license file while specifying the pathname.

Or, click **Browse** and navigate to the license file.

Step 8 Click **Add/Upgrade**.

The details regarding the number of services and the DPEs that you are licensed to use appear.

Installation Notes

Review the following notes before installing BAC 4.0.

- Ensure that your system meets the requirements described in [System Requirements, page 8](#).
- Ensure that you download and install the recommended patches from the Sun Microsystems support site.
- Obtain the BAC license file.
- Verify the file-system block size of the directory in which you intend to install the BAC database and database transaction log files. For optimum performance and reliability of the BAC database, configure the file system or systems that contain the database files and database log files with an 8-KB or greater block size.
- Ensure that the file system in which you place database files is configured to support files larger than 2 GB.

For complete information on installation procedures, refer to the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*.

Caveats

For information on the complete list of BAC bugs, see the *BAC40_BugList.html* file in the *docs/* subdirectory of the BAC CD-ROM or at the BAC software download site on <http://www.cisco.com>.

- [Table 2](#)—Describes the major bugs fixed in this release.
- [Table 3](#)—Describes the open bugs in this release.

Fixed Bugs in BAC 4.0

[Table 2](#) lists major software issues fixed in this release of BAC.

Table 2 **Bugs Fixed in BAC 4.0**

CDETS Number	Description	Workaround/Resolution
CSCef90805	You cannot delete a property using the <i>change property</i> API call, and then add the property back in the same call.	Delete and add the property using separate API calls.
CSCsj12710	Errant eMTA generates invalid MAC address, resulting in an invalid USM Name being generated by the DPE PacketCable service. This condition may occur because of poor network conditions, coupled with corrupt eMTA firmware images.	Isolate the eMTA generating the invalid MAC address.

Open Bugs in BAC 4.0

Table 3 lists major software issues open in this release of BAC.

Table 3 **Bugs Open in BAC 4.0**

CDETS Number	Description	Workaround/Resolution
CSCeg87139	When the TFTP server receives a bad Ack for a previous data block but not for the one that was sent out last, it automatically resends the data block instead of waiting for the real Ack.	Currently, there is no workaround for this issue.
CSCeh03452	The syntax that the runCfgUtil.sh tool uses does not allow generation of options in cases of nested suboptions. For example, when using DOCSIS 2.0 Option 41: <pre>41. 41.1 41.1.1 30 41.1.1.2 10000000 41.1.2 10000000 41.1 41.1.1 30 41.1.2 20000000 41. 41.2 41.2.1 30 41.2.2 30000000</pre>	Break multiple suboptions into multiple groups. According to the DOCSIS 2.0 RF spec, this definition achieves the same result: <pre>41. 41.1 41.1.1 30 41.1.2 10000000 41. 41.1 41.1.1 30 41.1.2 20000000 41. 41.2 41.2.1 30 41.2.2 30000000</pre>
CSCeh49666	The <code>/snmp/mibs/mibList</code> property expands the list of MIBs that are to be loaded at the RDU. This property, which is set in the <code>BPR_HOME/rdu/conf/rdu.properties</code> file, overrides the internal default MIB list in the RDU, causing configuration generation to fail.	Populate the value of the property to include the default MIB list and the custom lists.
CSCse98518	When the DPE sends a <code>KRB_AP_ERR_SKEW</code> error to the MTA, to address the clock skew at the MTA, the MTA rejects the error message because it detects an incorrect checksum.	Currently, there is no workaround for this issue.

Table 3 **Bugs Open in BAC 4.0 (continued)**

CDETS Number	Description	Workaround/Resolution
CSCsh83907	During installation, when you enter invalid names that use more than the maximum of 64 characters for these directories: • Home (<i>BPR_HOME</i>) • Data (<i>BPR_DATA</i>) • Database logs (<i>BPR_DBLOG</i>) the installation program does not display the appropriate error message and continues with the installation without prompting you to install these directories.	Ensure that you select valid directories for <i>BPR_HOME</i> , <i>BPR_DATA</i> , and <i>BPR_DBLOG</i> .
CSCsj03649	Device configuration is not automatically updated following certain system-wide configuration changes. When you change technology defaults or system properties, the Configuration Regeneration Service (CRS) does not regenerate configurations for all the devices that may be impacted. For example, changing the default DHCP Criteria for a CPE in system properties does not regenerate devices associated with the previous DHCP Criteria. Similarly, changing extension classes does not trigger the CRS to automatically regenerate a configuration for the device. Note This condition does not occur when you change the default Class of Service and the default DHCP Criteria.	Use any one of the following workarounds: 1. Trigger the CRS by submitting any change to the relevant Class of Service or DHCP Criteria objects. 2. Avoid using policies on technology defaults and at the system level when you can set the same policy on Class of Service or DHCP Criteria objects. 3. Submit batches via the API to regenerate specific sets of devices.
CSCsj04077	When you try to log in to the RDU via the administrator user interface, the login fails. The error message that appears indicates that the login could not be completed because the RDU is down or because invalid login credentials were entered. This message appears either because the RDU is not operational or because the password that you entered is incorrect.	Verify if the RDU is operational and if you used the appropriate credentials to log in. You can also check the RDU log for authentication error messages.
CSCsj31360	The DPE command line does not automatically complete the IPv4 and IPv6 keys in related commands. Instead, the following error appears: Invalid input detected at '^' marker.	Currently, there is no workaround for this issue.

Table 3 **Bugs Open in BAC 4.0 (continued)**

CDETS Number	Description	Workaround/Resolution
CSCsj44708	The <i>Configuration.getLicenseKeyData</i> API call does not return the name of the organization for which a specific license was issued.	Parse out the organization name from the Issuer field, which is returned in the API call results.
CSCsj66565	While trying to add JAR files from the administrator user interface at the Configuration > Files > View Files > Add Files page, you can add any file type, instead of only JAR files.	Delete the file that you added. Then, add the file again by selecting the appropriate file type from the File Type drop-down list.
CSCsj89853	You can set properties anywhere on the property hierarchy, including the provisioning group, but the Provisioning Group Details page on the administrator user interface (Servers > Provisioning Groups > Manage Provisioning Groups) does not display the properties.	Use the API to add custom properties to the provisioning group.
CSCsk09593	When you search for devices from the administrator user interface (via Devices > Manage Devices) using the IP address search option, the IP Address field is prepopulated with the 10.10.10.10 IP address.	Delete the 10.10.10.10 address, and enter the IP address that you want to look up.
CSCsk09598	The TFTP and ToD services that you configured on the DPE do not take effect. This error occurs if you have not enabled IPv4 or IPv6 interfaces for provisioning.	Before configuring TFTP or ToD services, enable provisioning on IPv4 and/or IPv6 interfaces.
CSCsk78321	The setLogLevel.sh tool reports that the RDU is configured for a specific severity level, but the <i>rdu.log</i> file does not log messages related to the configured severity level or logs messages of another severity level. This error occurs when you configure logging at the RDU using the <i>rdu.properties</i> file instead of the setLogLevel.sh tool. See also CSCs130492 .	Remove logging property settings from the <i>rdu.properties</i> file, and configure the RDU for the appropriate severity level using the setLogLevel.sh tool.
CSCsk85277	The DPE fails to obtain its license even though the: • RDU database contains a DPE license. • DPE is connected to the RDU. This error occurs if you reinstalled the RDU with a clean database.	Restart the DPE from the command line, using the dpe reload command.

Table 3 **Bugs Open in BAC 4.0 (continued)**

CDETS Number	Description	Workaround/Resolution
CSCs103366	The administrator user interface displays the number of devices in the database incorrectly in the Device Statistics section of the View Regional Distribution Unit Details (Servers > RDU) page. Note The Device Statistics section appears only when the appropriate devices are present in the RDU database. This error occurs if an operational RDU shuts down unexpectedly; for example, if the RDU server crashes because of power failure or if the RDU process is killed.	Currently, there is no workaround for this issue.
CSCs106558	When you configure the timeout for the PacketCable SNMP service to less than the default value of 10 seconds, using the service packetcable 1..1 snmp timeout command, the following error appears: Invalid execution parameters.	Use a timeout value greater than 9 seconds.
CSCs117155	When you connect a BACC 2.6.2.7 Solaris DPE to the BAC 4.0 RDU, you cannot view the DPE log on the View Device Provisioning Engine Details page (Servers > DPEs > Manage Device Provisioning Engines).	Currently, there is no workaround for this issue.
CSCs119090	The Provisioning API Command Engine (PACE), at times, reports a duplicate batch error. This error occurs when System defaults are changed in two batches with the same batch name that are executed one after another.	Assign unique names to batches.
CSCs120473	When you are logged in as admin, you are unable to delete other users, with the following error message appearing: Nonadmin user cannot add or delete user. Error: Nonadmin user cannot add or delete user.	Before deleting the user from your admin login, ensure that the user has logged out.

Table 3 **Bugs Open in BAC 4.0 (continued)**

CDETS Number	Description	Workaround/Resolution
CSCsl21402	When you manually configure IP addresses for lease queries using the administrator user interface on the Provisioning Group Details page (Servers > Provisioning Groups > Manage Provisioning Groups), the Add to IP Address List in the Configured IP Address List (IPv4) and the Configured IP Address List (IPv6) sections displays duplicates of IPv4 and IPv6 addresses, respectively.	Select only one IP address from the duplicate entries if that IP address is to be used for lease query operations.
CSCsl30492	The setLogLevel.sh tool does not dynamically update a change in severity level. This error occurs when you configure logging at the RDU using the <i>rdu.properties</i> file instead of the setLogLevel.sh tool. See also CSCsk78321 .	Remove logging property settings from the <i>rdu.properties</i> file, and configure the RDU for the appropriate severity level using the setLogLevel.sh tool.
CSCsl41609	When you modify the DHCP Criteria using the administrator user interface, the Configuration Regeneration Service (CRS) regenerates many configurations for the devices associated with the DHCP Criteria. This condition occurs regardless of the number of attributes you have changed on the Modify DHCP Criteria page (Configuration > DHCP Criteria > Manage DHCP Criteria).	Use the API to modify only the relevant changes for that DHCP Criteria. Note If you change more than one attribute, it still results in duplicate CRS events.
CSCsl71128	When upgrading a Solaris DPE from BACC 2.6.x to BAC 4.0, the <i>dpe.properties</i> file does not upgrade correctly. This error occurs if you have configured the DPE with logical interfaces (for example, bge0:1) and have enabled provisioning on these interfaces.	Reconfigure the DPE from the command line using these commands: • interface ip pg-communication • interface ip provisioning • interface ip provisioning fqdn
CSCsl85905	The Network Registrar extensions in BAC 4.0 successfully register with the RDU and join a provisioning group containing 2.6.2.x Solaris DPEs. This error occurs when the capabilities of the Network Registrar extensions match those of the provisioning group that the extensions intend to join, even though BAC 4.0 does not support a provisioning group comprising 2.6.2.x DPEs and 4.0 Network Registrar extensions.	Before upgrading the Network Registrar extensions, upgrade the 2.6.2.x DPEs in the provisioning group to BAC 4.0.

Related Documentation

These related guides support this BAC release:

- *Installation and Setup Guide for Cisco Broadband Access Center 4.0*
- *Cisco Broadband Access Center DPE CLI Reference 4.0*
- *Administrator Guide for Cisco Broadband Access Center 4.0*

Additionally, you can refer to:

- *Release Notes for Cisco Network Registrar 7.0*
- *Installation and Setup Guide for Cisco Network Registrar 7.0*
- *User Guide for Cisco Network Registrar 7.0*
- *Quick Start Guide for Cisco Network Registrar 7.0*
- *CLIFrame.html* in the /docs directory

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, Phone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2007 Cisco Systems, Inc. All rights reserved.