Release Notes for Cisco Broadband Access Center 4.1.0.1

Revised: December 20, 2010, OL-24085-01

These release notes describe new software features and fixes to software issues in Cisco Broadband Access Center, Release 4.1.0.1.

Contents

Introduction

Cisco Broadband Access Center, referred to as Cisco 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.

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

Cisco 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.

Cisco 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
- OpenCable Set-top box

System Components

The Cisco BAC product comprises:

- The Regional Distribution Unit (RDU), which is the primary server in a Cisco 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 Cisco BAC and Network Registrar. Cisco Network Registrar provides Cisco 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 Cisco BAC.
- A Java provisioning application programming interface (API), which you use to integrate Cisco BAC into an existing operations support-system environment.

For information on system requirements, licensing, and upgrading, see Before Installing Cisco BAC 4.1.0.1, page 6. See also the *Installation and Setup Guide for Cisco Broadband Access Center 4.1.0.1*.

Supported Devices

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

This release of Cisco BAC supports provisioning and managing:

- DOCSIS 2.0 IPv4 and IPv6 devices (booted using the IPv4 or IPv6 provisioning flow or dual stack).
- IPv6 devices, including cable modems compliant with DOCSIS 3.0, computers, and set-top boxes (STBs).
- Variants of eSAFE (embedded Service/Application Functional Entities) devices, such as mixed-IP mode PacketCable 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, Cisco BAC continues to provision:

- Cable modems and STBs compliant with DOCSIS 1.0, 1.1, and 2.0.
- eMTAs compliant with PacketCable version 1.5
- Devices compliant with CableHome 1.0.
- Computers.

Supported Standards

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

- eDOCSIS
  - CM-SP-eDOCSIS-I20-1000611
- DOCSIS 2.0
  - CM-SP-RFIv2.0-C01-081104
  - CM-SP-DOCSIS2.0-IPv6-I01-090518 DOCSIS 3.0
  - CM-SP-MULPIv3.0-I08-080522
  - CM-SP-SECv3.0-I08-080522
- DOCSIS Business Services
  - CM-SP-L2VPN-I08-080522
  - ECN L2VPN-N-10.0918-2
- DOCSIS Set-top Gateway (DSG)
  - CM-SP-DSG-I15-100611
- PacketCable MTA Device Provisioning Specification
  - PKT-SP-PROV1.5-I03-070412
  - PKT-SP-SEC1.5-I03-090624
- PacketCable 2.0 e-DVA
  - CM-SP-eDOCSIS-I20-1000611

- OpenCable specification
  - OC-SP-HOST2.1-CFR-I11-100507
- CableHome
  - CH-SP-CH1.0-C01-060728
  - CH-SP-CH1.1-C01-060728
- Cross Project
  - CL-SP-CANN-I02-080306
  - CM-SP-CL-SP-CANN-DHCP-Reg-I02-080306

New and Changed Features

The following sections briefly describe enhancements and new or modified features in this release:

RADIUS Authentication Support

Remote Authentication Dial-In User Service (RADIUS) is a UDP based protocol used for enabling centralized authentication, authorization, and accounting for network access. RADIUS authentication involves authenticating the users accessing the network services via the RADIUS server using the RADIUS standard protocol defined in RFC 2865. RADIUS Authentication support is provided at RDU and DPE CLI. Accounting and Authorization features are not supported.

To enable RADIUS Authentication in RDU, configuration properties must be configured in RDU Defaults page by selecting the authentication mode as RADIUS. See the *Administrator Guide for Cisco Broadband Access Center 4.1* for more details.

New commands have been added to support RADIUS authentication in DPE CLI. See the *Cisco Broadband Access Center DPE CLI Reference 4.1* for more details.

In addition, this release supports RADIUS authentication through RSA Secure ID Tokens in both RDU and DPE CLI. You must install RSA Authentication Manager and have RSA SecureID Token with a pin assigned to it.

DCFG Support for Groovy Scripting

The Dynamic Configuration File Generation with Groovy scripting offers increased functionality over template-based file generation. Templates are still supported for backward compatibility.

To support dynamic configuration, the device discovered data are used at runtime by Groovy script through exposed API's.

Groovy scripts are supported for all CableLabs standard devices and IP-modes supported by previous versions of Cisco BAC (DOCSIS IPv4/IPv6, PacketCable and OpenCable IPv4/IPv6).

The command line configuration file utility is updated to execute Groovy script. The command line configuration file utility also supports the conversion from binary file to Groovy script and vice versa.

DPE Device Configuration Compression Support

In the previous release (Cisco BAC 4.0), the DPE supported compressed TFTP configurations, but the configurations were compressed individually. In the Cisco BAC 4.1.0.1 release, the DHCP, TFTP and SNMP configuration information are compressed using the delta compression technique as defined in RFC 3284. This feature will enable the DPE to store more than two million device configurations.

GSLB Support

GSLB directs DNS requests to the best-performing GSLB website in a distributed internet environment. In Cisco BAC 4.1.0.1, GSLB is used to implement the failover, the continuation of RDU service after the failure of primary RDU. When the primary RDU fails, all the client requests will be routed to the secondary RDU. In the previous releases (Cisco BAC 2.7 and 4.0), when the IP address of RDU FQDN is changed, the clients (DPE, CNR_EP, API) should be restarted to reconnect with the secondary RDU or RDU with the new IP address. In Cisco BAC 4.1.0.1, if the IP address of FQDN is changed and also the primary RDU is down, FQDN will be resolved to the new IP address and all the client will be routed to the secondary RDU.

Linux Support for DPE and CNR_EP

Cisco BAC 4.1.0.1 release includes support for the DPE and CNR extensions running on Red Hat Enterprise Linux platform using x86 based hardware. This includes RPM based installations and mixed platform provisioning group deployments. For example, CNR extensions can run on a Linux platform and DPEs can either run on a Linux or Solaris platform. However, mixing the platform for a server type is not recommended.

Non-root Solaris 10 Support

This feature allows non-root users to run Cisco BAC on a Solaris environment. The non-root user should be assigned Solaris privileges before installing the product. The Cisco BAC 4.1.0.1 installer prompts for user name and group name that are associated with the non-root user. The processes gets initiated with the user name and the group name that where provided during the installation. Any other non-root user who is in the same group provided during the installation will be able to run the product.

ZFS Support

Cisco BAC 4.1.0.1 supports the block size between 8K to 64K for the database files and database log files under ZFS.

DOCSIS 3.0 EMIC Support

The EMIC feature is enhanced to support the implementation as specified in the CableLabs specification: CM-SP-MULPIv3.0-I13-100611.

The Extended CMTS MIC Configuration Setting parameter is a multi-part encoding that configures how the CMTS performs message integrity checking. This is used to detect unauthorized modification or corruption of the CM configuration file, using more advanced hashing techniques, or requiring different TLVs to be included in the HMAC calculation. In addition, Admin UI and DPE CLI support is provided for EMIC framework. The EMIC support has been tested with CMTS version IOS12.2(11)CX.

Combining License Support

The Cisco BAC 4.1.0.1 Licensing feature supports combining the evaluation license with the permanent license and vice versa for both DPE and service license.

Berkeley DB 5.1.19 Support

The Berkeley DB used in the Cisco BAC 4.1.0.1 is upgraded to 5.1.19 from 4.1.25 which was used in Cisco BAC 4.0.1. This upgrade helps in bug fixes and out of disk space handling, and provides better performance, improved feature support, improved caching efficiency and faster database recovery.

Before Installing Cisco BAC 4.1.0.1

Review the following information before you begin to install Cisco BAC 4.1.0.1.

System Requirements

To install Cisco BAC 4.1.0.1 on your system successfully, you must meet these requirements:

- **Operating system:**
  - **Solaris:** You must install Cisco BAC on a Sun SPARC platform running the Solaris 10 operating system with at least 4 GB of memory. We recommend that you use a Sun SPARC multiprocessor platform.
  - **Linux:** You must install Cisco BAC on Red Hat Enterprise Linux 5.3 (2.6.18 or later) using x86 and 64 bit hardware system. The SELinux should be disabled.
- **Network Registrar**—You must have Cisco Network Registrar version 7.1.2.1 installed on the servers on which you are installing Cisco BAC extensions.
- **Administrator user interface**—At a minimum, you must have Microsoft Internet Explorer 6.0 (Service Pack 2) or Firefox 1.5 and later.
- **API client**—Ensure that:
  - You install Java 1.6.0_23 to support the API client in release 4.1.0.1. API clients in versions earlier than 4.1.0.1, however, support JRE versions earlier than 1.6.0_23.
  - The files *bpr.jar* and *bacbase.jar* are available in the classpath.

Licensing

This Cisco 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.

Obtaining Licenses

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

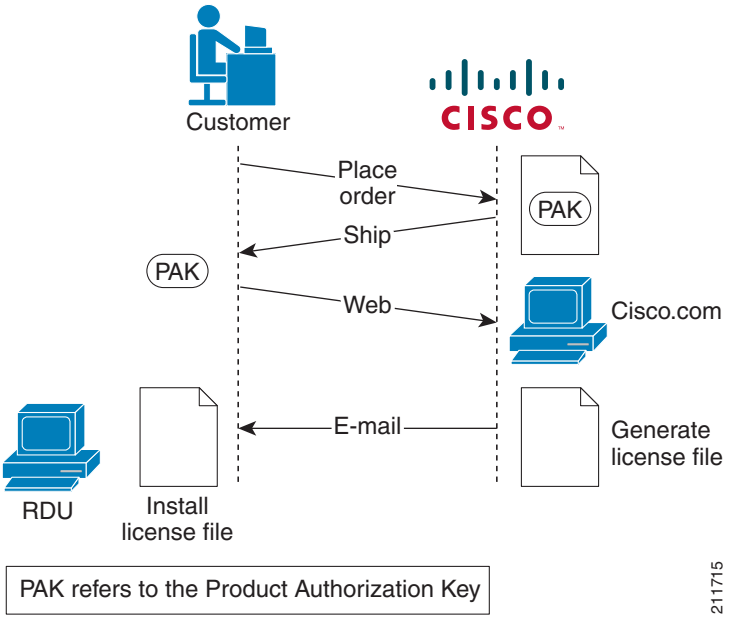
- **Permanent**—You purchase a permanent license for use in your network environment and to activate the specific features for which it is intended.
- **Evaluation**—You purchase an evaluation license to enable functionality for a specific length of time.

Caution Do not attempt to deploy Cisco BAC into a fully operational network with an evaluation license. When the evaluation license expires, you will not be able to use Cisco 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 the License, page 9.

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 the License, page 9.

Installing the License

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

To install a 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 Cisco 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*—The machine on which the RDU is running.
- *port_number*—Port on which the server side of the administrator application runs. The default port 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**.

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 Cisco BAC 4.1.0.1.

- Ensure that your system meets the requirements described in System Requirements, page 7.
- Ensure that you download and install the recommended patches from the Sun Microsystems support site.
- Obtain the Cisco BAC license file, as described in Obtaining Licenses, page 7. Then install the license, as described in Installing the License, page 9.
- Verify the file-system block size of the directory in which you intend to install the Cisco BAC database and database transaction log files. For optimum performance and reliability of the Cisco 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, see the *Installation and Setup Guide for Cisco Broadband Access Center 4.1.0.1*.

Upgrading to Cisco BAC 4.1.0.1

Cisco BAC 4.1.0.1 provides upgrades from:

- Cisco BAC 2.7.1.*x*.
- Cisco BAC 4.0.1.*x*.

See Table 1 for upgrade task details.

Upgrade the Cisco BAC components in this order:

1. Upgrade the RDU and client APIs simultaneously.
2. In each provisioning group, upgrade the DPEs first, followed by the KDC, then the Network Registrar extensions.

Note Cisco BAC 4.1.0.1 features are available only after the administrator explicitly enables them. You cannot upgrade DPE appliances; only Solaris DPEs are supported.

Upgrade Tasks

The upgrade tasks are described in Table 1:

Table 1 Upgrading to Cisco BAC 4.1.0.1

Version	RDU	DPE	KDC	Network Registrar Extension Points
Cisco BAC 2.7.1.*x* **Note** Migration of RDU database is required.	Run **pkgadd**. At the end, the installer prompts you to run the migration tool. (See Migration Tool, page 12.)	Run **pkgadd** to upgrade the DPE.	Run **pkgadd** to upgrade the KDC.	Run **pkgadd** to upgrade the Cisco Network Registrar extensions.
Cisco BAC 4.0.1.*x* **Note** Migration of RDU database is not required.	Run **pkgadd**. At the end, the installer prompts you to run the migration tool. (See Migration Tool, page 12.)	Run **pkgadd** to upgrade the DPE.	Run **pkgadd** to upgrade the KDC.	Run **pkgadd** to upgrade the Cisco Network Registrar extensions.

When upgrading to Cisco BAC 4.1.0.1, you must enter a new target location for these directories:

- Home (*BPR_HOME*)—This prompt is the only one in a Cisco BAC 4.0.0.1-to-Cisco BAC 4.1.0.1 migration.
- Data (*BPR_DATA*)
- Database logs (*BPR_DBLOG*)

Database Migration

When Cisco BAC is installed over the earlier versions, the installer detects if RDU DB migration is necessary. At the end of installation, the user is prompted to start the migration process. The user has to run the migrateDb.sh shell script which is present in the BPR_HOME/migration directory.

The RDU database migration script allows you to migrate your RDU database from:

- Cisco BAC 2.7.1.x to Cisco BAC 4.1.0.1
- Cisco BAC 4.0.1.x to Cisco BAC 4.1.0.1

Migration Procedure

1. Backup the Cisco BAC 4.0.1.x/2.7.1.x DB using backupDb.sh tool
2. Execute recoverDb.sh tool over backed up database
3. Upgrade the RDU from Cisco BAC 4.0.1.x/2.7.1.x to Cisco BAC 4.1.0.1 using the Cisco BAC 4.1.0.1 upgrade script
4. Execute migrateDb.sh tool to perform database migration
5. Restore the database to Cisco BAC 4.1.0.1 active RDU DB directories
6. Start the RDU

Note Migration is not supported for the DPE cache. During DPE upgrade, all the old DPE cache will be deleted and it will be rebuilt by synchronizing with the RDU. If DPE is not upgraded, it will continue to run with the old cache and synchronization will happen. In this case, the new Cisco BAC 4.1.0.1 RDU will be compatible with the old release DPEs.

Migration Tool

The **–cmtsv** flag is used only in migrating from Cisco BAC 2.6.*x* and later releases to Cisco BAC 4.0 and 4.1.0.1. The flag is not used in migrating from Cisco BAC 2.7.1.*x* or later, which uses an internal property setting.

Cisco BAC 4.1.0.1 also includes changes to the default values to certain promiscuous device settings for the **migrateDb.sh** tool (see Table 2).

Table 2 Promiscuous Device Settings for migrateDb.sh Tool

Argument	Description	Required	Optional	Default
-pdcpc *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous computers.		✓	unprovisioned-computer
-pdcmta *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous MTAs.		✓	packet-cable-mta
-pdcchwd *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous CableHome WAN-Data devices.		✓	unprovisioned-cablehome wan-data
-pdcchwm *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous CableHome WAN-MAN devices.		✓	unprovisioned-cablehome wan-man
-pdccpe *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous custom CPE.		✓	unprovisioned-customcpe

System Hardening

This Cisco BAC release has undergone comprehensive security testing. The objective of this security testing was to identify and eliminate any security vulnerabilities pertaining to Cisco BAC and its supporting software and hardware. This release was also tested for protocol robustness, which tests for application stamina when exposed to Denial of Service attacks and protocol irregularities.

For this release, the security testing was performed using *5.10 Generic_127127-11 sun4v sparc SUNW, Solaris 10 5/08 s10s_u5wos_10*, hardened with Solaris Security Toolkit 4.2.

To mitigate security threats when deploying a Cisco BAC release, we recommend that you harden the systems.

Note Complying to these recommended hardening guidelines does not guarantee the elimination of all security threats. However, implementing these recommended guidelines will achieve a higher level of security and help manage unforeseen risks.

We recommend that you complete the following activities to harden your systems:

- Ensure that all Sun Microsystems-recommended OS and Security patches have been applied. Contact Sun Microsystems Support to download the recommended patches and check for any applicable updates.
- Disable all unused network services. At a minimum, run the following Solaris command:

  ```
  # netservices limited
  ```

- Use the latest version of the Solaris Security Toolkit to assist with system hardening.
- Disable unused daemons and services, especially services that use network resources; for example:

  ```
  # svcadm disable svc:/network/smtp:sendmail
  # svcadm disable svc:/network/finger:default
  ```

- Uninstall all unused applications.
- Apply the highest level of password protection to all network applications and services. Ensure that you change the default passwords.
- Use HTTPS to access the Cisco BAC administrator user interface and disable the HTTP access. HTTP access to the administrator user interface (using port 8100) is enabled by default on the RDU. Currently, there is no way to disable the HTTP service using standard Cisco BAC administrative methods. You can, however, disable HTTP access using the Tomcat server.xml file, which is located at *BPR_HOME*/rdu/tomcat/conf.

  To do this:

  a. Comment out the HTTP/8100 connector directive in the Tomcat server.xml file. For example:

  ```
  <!-- <Connector port="8100" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
  enableLookups="false" redirectPort="9453" acceptCount="100"
  connectionTimeout="20000" disableUploadTimeout="true" /> -->
  ```

  b. Reload the Tomcat process to make your changes take effect. For example:

  ```
  # /etc/init.d/bprAgent restart tomcat
  Process [tomcat] has been restarted.
  ```

- If SNMP is not being used to manage the Cisco BAC components, then shut down the SNMP service. The SNMP service is enabled by default on the RDU and DPEs. This SNMP service uses UDP port 8001. You can disable this service for the RDU or a DPE using the **snmpAgentCfgUtil.sh stop** command from *BPR_HOME*/snmp/bin. For example:

  ```
  # ./snmpAgentCfgUtil.sh stop
  Process [snmpAgent] has stopped.
  ```

Caveats

For information on the complete list of Cisco BAC bugs, see the BAC4101_BugList.html file in the /docs subdirectory of the Cisco BAC CD-ROM, or at the Cisco BAC software download site on http://www.cisco.com.

Note To obtain more information about known problems, access the Cisco Software Bug Toolkit at http://www.cisco.com/pcgi-bin/Support/Bugtool/home.pl. (You will be prompted to log into cisco.com).

Resolved Problems

Table 3 lists the bugs resolved in this Cisco BAC 4.1.0.1 release.

Table 3 Resolved Problems

Bug ID	Summary
CSCsq63171	BACC upgrade was not modifying the /var/sadm/install/contents.
CSCsu07859	Upgrading Cisco BAC in the same location was throwing message rm -rf /opt/CSCObac.
CSCsu44746	The installer was repeatedly displaying the message to remove the BPR_DATA folder.
CSCsy74552	RDU DB was reporting Physical layer error while using verifyDB.
CSCsz56765	Cisco BAC CNR extensions was posting more than one generate batch for same packet.
CSCsu25124	DPE CLI command *show tftp files* was displaying incorrect count of cached files.
CSCsu40836	While running the *nmap* command the RDU was getting restarted.
CSCsu54215	Cisco BAC 4.1.0.1 installer was not throwing proper error message when */tmp* is 100%.
CSCsx17670	Changing more than one technology default was causing erroneous log entry.
CSCsx20670	Adding/changing device via API was not checking the Class of Service type.
CSCsx41938	RDU and DPE were not generating Traps.
CSCsx68723	Cisco BAC Admin UI License Key page was failing when using the evaluation license in non-US Locale.
CSCsx81952	Adding a zero size file to RDU was causing the DPE to crash.
CSCsx81962	Using Property */pktcbl/prov/locale=IETF* was resulting in NullPointerException.
CSCsy30360	DPE upgrade to Cisco BAC 4.0.1 was not updating the hard links in rc0.d, rc1.d, rc2.d.
CSCta04977	PACEConnection was not able to released.
CSCta21090	DPE was doing reverse lookups and was slow because of DNS.
CSCtb16654	DPE docsis shared-secret string was allowing a maximum of 80 characters only.
CSCtc76102	Problems were there in stopping bprAgent on multiprocessor machine.
CSCtd05810	Cisco BAC CNR extensions was reporting: failed to find thread index.
CSCte96398	RDU was running out of memory while processing API command IPDevice.searchDevice.
CSCtf36808	RDU was crashing due to NullPointerException for device without MAC address.
CSCtf69693	PACEConnectionException was not thrown if host does not exist.
CSCtk11640	BAC 4.1 upgrade was removing the customer MIB files before copying the new Cisco-supplied MIBs.

Table 3 Resolved Problems

Bug ID	Summary
CSCtj90972	After upgrading to BAC 4.1, the device configuration was failing with: `java.lang.IllegalArgumentException: Error occurred during parsing of MIB files. Cannot find MIB file [DOCS-CABLE-DEVICE-MIB-OBSOLETE].`
CSCtk52701	The RDU "Device Details" page was not showing the lease information for DOCSIS 3.0 Cable Modem.

Known Problems

Table 4 lists major software issues open in the Cisco BAC 4.1.0.1.

Table 4 Known Problems

Bug ID	Description	Workaround/Resolution
CSCth16781	runCfgUtil.sh fails to generate PacketCable 2.0 dial plan TLV.	The length of the TLV values should not be more than 1024 characters.
CSCtg71861	Groovy scripts do not have variable bindings for devices.	If device object bindings are used inside Groovy scripts, the scripts cannot be encoded or decoded using runCfgUtil. But it can be used in RDU to generate the configuration files.
CSCti93245	Upgrading from Cisco BAC 4.0.1 to Cisco BAC 4.1.0.1 displays the following message without any steps as it suggests: After migration, you should run the following steps to completely remove the previous version of BPR from your system.	Follow the instructions provided in the Cisco BAC 4.1.0.1 Installation guide.
CSCtj25387	EMIC configuration throws illegal argument exception in DPE logs.	• Use encrypted secret while configuring EMIC shared secret in DPE CLI using option 7. • Use plain text while configuring EMIC shared secret in DPE CLI using option 0.
CSCtj30159	When you provide the relative path instead of absolute path while restoring the database, the following error message is displayed in the console: `Database recovery failed.`	Provide the absolute path instead of the relative path.
CSCti98378	runCfgUtil decoder truncates the output TLV numbers. This makes it difficult to read the decoder output. However, this occurs only when the output is displayed in the user console.	Convert the output to a file and read the options and values from the file.

Table 4 Known Problems

Bug ID	Description	Workaround/Resolution
CSCti83531	Session gets timed out and expires when the evaluation license expires.	Log in again and add the new license. You cannot log in by adding a new license. What I understand from the RNE is that you have to log in and add a new license. Also please note 'log in' becomes two words as it is a verb here.
CSCtj09014	UnexpectedInternalException is found in DPE logs when interface IP was enabled for both IPv4 and IPv6, and pg communication not enabled.	Always enable pg-communication when you enable interface IP for both IPv4 and IPv6.
CSCsm43002	The captureConfiguration.sh script copies the agent log files, but not the agent/conf/* files (agent.conf). This happen everytime captureConfiguration.sh is run.	Copy the files manually from agent/conf/.
CSCso85401	CM rejects the config file due to incorrect docsis shared-secret. Docsis shared-secret is not removed from the local.properties file unless the DPE rebooted.	Reload the DPE if the DPE shared-secret CLI command is used.
CSCsr70925	BAC upgrade aborts with the following error message: `Error: 8100 is in use. Please disable the process which is bound to this port.`	Ensure all the BAC processes are stopped before you perform an upgrade. To stop the bprAgent process, use the command: /etc/init.d/bprAgent stop.
CSCti60751	The RDU takes a long time to process the batch while generating the device configurations for the modem when too many PCs are connected to the modem. The device configurations are not sent to the DPE as they are generated. The DPE drops its connection to the RDU.	Ensure that only minimum number of PCs are connected to the DOCSIS modem.

Table 4 Known Problems

Bug ID	Description	Workaround/Resolution
CSCti56191	DPE crashes under load after the Solaris patch installation. Oracle has successfully diagnosed the problem and has opened this new defect against the offending Solaris driver, 6994017–ioctl sometimes returns errno EBADF on a valid open file descriptor for /dev/poll. After upgrading from Solaris 10 5/09 (5/14/2010, no patches) to patch cluster dated 6/18/2010 (142909-17), Java application utilizing nio fails with java.io.IOException: Bad file number with call to java.nio.channels.Selector.select. Truss reveals ioctl to fd open for /dev/poll and request DP_POLL is returning errno EBADF which is triggering the above exception. This behavior appears to be centered around thread interaction between one which is adding a descriptor to be monitored to the /dev/poll set which subsequently is closed and another thread which is issuing the ioctl DP_POLL call.	Remove the problematic Solaris kernel patch. This problem does not occur with patches like Generic_137111-06, 142900-03. This problem is seen in all patches released after 142900-04 (starting from 142900-05 to the recent patch Generic_142909-17).
CSCth16251	CNR extensions expect the relay agent information in DHCPINFORM messages.	Check whether if some additional configuration option has to be set on the CMTS that would cause it to add the relay-agent option to DHCPINFORM messages.
CSCte10940	The DPE crashes with the below log message, when a configured IP interface is down: `com.cisco.csrc.exceptions.InitializeFailException: Cannot start server services.`	1. Remove the interface from the DPE using CLI command. 2. Add a valid or active IP interface and bring up the DPE.

Related Documentation

See the following documents for more information about installing, configuring, and managing Cisco BAC 4.1.0.1:

Table 5 Related Documentation

Document Title	Available Formats
Installation and Setup Guide for Cisco Broadband Access Center 4.1.0.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_installation_guides_list.html
Cisco Broadband Access Center DPE CLI Reference 4.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html
Administrator Guide for Cisco Broadband Access Center 4.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_maintenance_guides_list.html
Release Notes for Cisco Broadband Access Center 4.1.0.1 (This document)	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_release_notes_list.html

See the following documents for information about CNR:

Document Title	Available Location
Quick Start Guide for Cisco Network Registrar 7.1	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/user/guide/cnr71_qs_book.html
User Guide for Cisco Network Registrar 7.1	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/user/guide/cnr71book.html
Installation Guide for Cisco Network Registrar 7.1	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/installation/guide/CNR71Install.html

Document Title	Available Location
CLI Reference Guide for Cisco Network Registrar 7.1	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/command/reference/CLIReferenceGuide.pdf
Release Notes for Cisco Network Registrar 7.1.2.1	• On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_release_notes_list.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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.
