Readme for Cisco Broadband Access Center 3.5.1

Revised: Feb 24, 2010, OL-20839-01

This readme provides information on new software features, installation procedure, bug fixes, and documentation for Cisco Broadband Access Center (Cisco BAC), Release 3.5.1

Contents

This document includes the following sections:

Introduction

Cisco Broadband Access Center, referred to as Cisco BAC through out this document, automates the tasks of provisioning and managing customer premises equipment (CPE) in a broadband service provider network. The product 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

With the high-performance capabilities of Cisco BAC, you can scale the product to suit networks of virtually any size, even those with millions of CPE. It also offers high availability, made possible by the product's distributed architecture and centralized management.

Cisco BAC supports provisioning and managing of CPE by using the Broadband Forum's CPE WAN Management Protocol (CWMP), a standard defined in the TR-069 specification. Cisco BAC integrates the capabilities defined in TR-069 to increase operator efficiency and reduce network-management problems.

Cisco BAC supports devices based on the TR-069, TR-098, TR-104, and TR-106 standards. These devices include Ethernet and ADSL gateway devices, wireless gateways, VoIP ATAs, and other devices compliant with CWMP.

This release provides:

- Bug fixes for various issues that had previously affected Cisco BAC 3.5 performance. See Resolved Problems, page 5, for the Cisco BAC 3.5 bugs that are resolved in this release.
- Other bug fixes related to DPE extensions.

For the Cisco BAC Architecture and system components, refer to *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.

New Features in Cisco BAC 3.5.1

This section describes the changes made in the Cisco BAC 3.5.1.

- Upgrading Capability

  This Cisco BAC 3.5.1 release supports upgrading from the Cisco BAC 3.5 version. For more information on upgrading Cisco BAC 3.5 to Cisco BAC 3.5.1, see Upgrading from Cisco BAC 3.5, page 4.
- DPE Extensions Backward Compatibility Support

  Cisco BAC 3.5.1 DPE extensions are compatible with device firmware (RMM 5.4 or later version) and legacy firmware (RMM 5.3 or earlier version).

System Requirements

For information on installation and operating system requirements, see the *Installation Guide for Cisco Broadband Access Center, Release 3.5*.

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 to define application stamina when exposed to Denial of Service attacks and protocol irregularities.

For information on the System Hardening, see *Cisco Broadband Access Center Hardening Guidelines, Release 3.5.*

Package Details

Cisco BAC software (BAC_3.5.1_SolarisK9) contains the files that are described in Table 1.

Table 1 Cisco BAC 3.5.1 Software Package Details

Files	Description
README.pdf	Readme for Cisco Broadband Access Center 3.5.1 (This document).
setup.bin	The Cisco BAC 3.5.1 installation program. See Installation Guide for Cisco Broadband Access Center, Release 3.5 for information about installing Cisco BAC 3.5.1.
BAC3_5_1_upgrade.tar	The product upgrade tar file.
version.txt	The product identification file.
Documentation/javadoc	Javadoc for the Cisco BAC Provisioning API.
femtoConfig.kiwi	The configuration script file.
femto-cwmp-dictionary.xml	Sample dictionary.

Downloading the Package

To download the Cisco BAC software (BAC_3.5.1_SolarisK9) package:

Step 1 Go to http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268439477.

Step 2 Log in with your Cisco.com username and password.

Note You must be a registered Cisco.com user to download from this package.

Step 3 Choose **Video, Cable and Content Delivery Management > Cisco Broadband Access Center > Cisco Broadband Access Center Telco Wireless 3.5.1.** The Select a Software Type page appears.

Step 4 Click the **Broadband Access Center for Telco Wireless Software** link. The Select a Release page appears.

Step 5 Choose **Latest Releases > 3.5.1**. The Release 3.5.1 Software page appears.

Step 6 Click the **Download Now** button next to BAC_3.5.1_Solaris.gtar.gz. The Download Cart page appears with the details of the software.

Step 7 Click the **Proceed With Download** button.

Step 8 Review Cisco's End User Software License Agreement and Software Download Rules, and click Accept.

Step 9 Choose one of the following download options:

- Download Manager Option
- Non Java Download Option

Step 10 Follow the prompts to download the package.

Installing Cisco BAC 3.5.1

For installation steps, see the *Installation Guide for Cisco Broadband Access Center 3.5*.

Upgrading from Cisco BAC 3.5

You must apply the Cisco BAC 3.5.1 patch on your existing Cisco BAC 3.5 RDU and Cisco BAC 3.5 DPE. The Cisco BAC 3.5.1 installation instructions in this section are based on the assumption that you have Cisco BAC release 3.5 already installed.

Upgrading the RDU

To apply this patch on your Cisco BAC 3.5 RDU server:

Step 1 Untar the file, BAC3_5_1_upgrade.tar.

Step 2 Go to the */upgrade351* directory.

Step 3 Run the *./createpackage.sh* script.

Step 4 Go to the */bin* directory.

Step 5 Run the *./351-upgrade-rdu.sh* script.

The Cisco BAC watchdog is stopped by the script.

The following message appears confirming the upgrade for Cisco BAC 3.5.1:

```
RDU Upgrade for BAC 3.5.1 Completed Successfully
```

Step 6 Start the Cisco BAC watchdog agent. To do this, run the following command:

/etc/init.d/bprAgent start

Step 7 Run AddProperties.kiwi through Cisco BAC Tools.

Upgrading the DPE

To apply this patch on your Cisco BAC DPE server:

Step 1 Untar the file, BAC3_5_1_upgrade.tar.

Step 2 Go to the */upgrade351* directory.

Step 3 Run the *./createpackage.sh* script.

Step 4 Go to the */bin* directory.

Step 5 Run the *./351-upgrade-dpe.sh* script.

The Cisco BAC watchdog is stopped by the script.

The following message appears confirming the upgrade for Cisco BAC 3.5.1:

```
DPE Upgrade for BAC 3.5.1 Completed Successfully
```

Step 6 Start the Cisco BAC watchdog agent. To do this, run the following command:

/etc/init.d/bprAgent start

Caveats

Table 2 describes software issues that are resolved and Table 3 describes significant software issues that are known to exist in this release of Cisco BAC.

For information on the complete list of Cisco BAC bugs, see the *BAC351_BugList.html* file in the *documentation/* subdirectory of the Cisco BAC CD-ROM or electronic distribution.

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 2 Resolved Problems

Bug ID	Summary
CSCsx50443	You could not get to the next page on clicking the arrow button, or navigate to the required page number, when you queried multi-page groups.
CSCta57648	Whenever two users made some property changes or change in the class of service for a particular device in the device modify page, the Admin UI did not update the device with the changes made by the second user.
CSCsx70264	Cisco BAC 3.5 installer did not uninstall the product completely. The installer does not remove /opt/CSCObac from the system.
CSCsy40930	Changing the priority group warned the user about the device regeneration but it did not regenerate the device and failed to change the device configuration in the DPE.

Table 2 Resolved Problems

Bug ID	Summary
CSCta53709	The RDU used to run out of memory during file synchronization if it contained a large number of files (more than 50) that were large in size (bigger than 1MB).
CSCsx64645	When a connection request to the DPE was generated using a simulator, the connection request was successful, but the status code did not get updated in the perfstat.log file.
CSCsz46175	The DPE (Device Provisioning Engine) registered the CPE (IOS router) with a wrong name when unique client certificates were configured on the DPE and CPE.
CSCte70678	Connection request was reported as successful.

Known Problems

Table 3 identifies known bugs in this Cisco BAC 3.5.1 release, with possible workarounds.

Table 3 Known Software Problems

Bug ID	Summary	Explanation
CSCsy74948	DPE CLI allows to provision the ethernet interface (for example: ce1, ce2) even if the interface is UP and not in the RUNNING state.	If DPE is running, then the interfaces should be UP and RUNNING state before the interface is configured to be provisioning enabled. If that is not the case, the interface will not be handling the CWMP requests even if the DPE CLI allows to provision the interface. Workaround: None.
CSCta46063	The RDU fails to authenticate any users.	The RDU fails to authenticate users, or is unable to process batches, especially, reliable batches. Workaround: You must restart the RDU process.
CSCtc80013	IE crashes if diagnostic log has MBs of data.	The Cisco BAC Admin UI does not limit number of lines when viewing diagnostic log. This can cause IE to crash if there are many MBs of data. The number of lines MUST be limited in the Admin UI. Workaround: None.
CSCtc97591	RPC instruction is not validating the response message type.	RPC instruction is not validating the response message type. Instead it accepts any response. Workaround: None.
CSCtd28368	An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.	This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml. Workaround: None.
CSCtd25362	CPE synchronization problem during the forced config synchronization.	When the configuration template is not empty, issuing the force configuration synchronization followed by connection request throws an exception with SetParameterValuesRecord:empty parameterValues in the DPE logs. This happens only when the configuration template is not empty and there are no changes in the configuration. Workaround: None

Table 3 Known Software Problems (continued)

Bug ID	Summary	Explanation
CSCte90206	In firmware file, if a match string specified for operator value contains a comma(,), Cisco BAC automatically splits the value into comma-separated list.	Workaround: Instead of using comma for values, provide individual value for parameter and specify matchAll/noMatch attribute for operator field.
CSCte84617	DPE outage occurs intermittently.	DPE becomes unresponsive and needs to be restarted. Workaround: None

Abbreviations and Definitions

Table 4 Abbreviations and Definitions

Term	Description
AC	Access Controller, also known as FGW
ACE	Application Control Engine — A Cisco load-balancing and SSL acceleration device, which is available as a blade for Cisco routers as well as stand-alone appliance.
BAC	Broadband Access Center — A mass-scale CPE provisioning and management product, which also implements TR-069 (auto configuration server - ACS - functions).
CLI	Command Line Interface such as the one exposed by the Cisco BAC DPE.
CPE	Customer Premises Equipment — A device such as an FAP, which is deployed at customer's premises.
DPE	Device Provisioning Engine — Distributed server in Cisco BAC architecture, which interfaces with CPE.
FAP	Femtocell Access Point — A device that functions as a mini 3G cell tower in customer home and backhauls cellular calls via customer's internet connection through the FGW.
FCAPS	Fault, Configuration, Accounting, Performance, and Security.
FGW	Femtocell Gateway, also known as AC. Each Femtocell Gateway (FGW) supports a large set of Femtocell Access Points (FAP). Each FAP is configured to associate with a specific FGW, and each FGW must be specifically provisioned to authorize and service each FAP.
FPG	Femto Provisioning Gateway — An application developed by SA, which provides Femto provisioning workflow glue between AT&T systems and Cisco BAC NB API.
GPS	Global Positioning Satellite — It is used to verify the location of the FAP.
IMSI	International Mobile Subscriber Identifier. This is the SIM card ID.
Network Listen	A radio network test performed by the FAP. A measure of received code power from the neighborhood cells, used to pick the code with the least interference as well as to assist in the location verification.
Polygon	A Polygon is a geo-political county which is significant for provisioning differentiation. A device is determined to be in a given Polygon based on its location.
RDU	Regional Distribution Unit. Central server in Cisco BAC architecture, which exposes NB API.
SA	Scientific Atlanta is a division of Cisco. SA is the systems integrator for AT&T Femtocell solution.

Table 4 Abbreviations and Definitions

Term	Description
SSL	Secure Socket Layer. Authentication and encryption protocol originally defined by Netscape. This specification has been superseded by IETF standard for TLS protocol, which is based on SSL 3.0 and is compatible with SSL 3.0.The term SSL is used to refer to both SSL 3.0 and TLS 1.0 since they are compatible and both are typically implemented.
White list	Access control list that specifies which cell phones can register with FAP.

Related Documentation

This release of the Cisco BAC product is supported by the following documents:

- *Installation Guide for Cisco Broadband Access Center, Release 3.5.*
- *Cisco Broadband Access Center Administrator's Guide, Release 3.5.*
- *Integration Developer's Guide for Cisco Broadband Access Center, Release 3.5.*
- *Cisco Broadband Access Center DPE CLI Reference, Release 3.5.*
- *Cisco Broadband Access Center 3.5 Third Party and Open Source Copyrights.*
- *Readme for Cisco Broadband Access Center, Release 3.5.1* (This guide).

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 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.
