Readme for Cisco Broadband Access Center 3.5.2

Revised: Aug 20, 2010, OL-22879-01

This readme provides information on the installation procedure, upgrading procedure, bug fixes, and documentation for Cisco Broadband Access Center (Cisco BAC), Release 3.5.2.

Contents

This document includes the following sections:

- Introduction, page 1
- System Requirements, page 2
- System Hardening, page 2
- Package Details, page 2
- Downloading the Package, page 3
- Installing Cisco BAC 3.5.2, page 3
- Upgrading from Cisco BAC 3.5 or 3.5.1 or 3.5.1.1 or 3.5.1.2, page 4
- Caveats, page 5
- Abbreviations and Definitions, page 6
- Related Documentation, page 7
- Obtaining Documentation and Submitting a Service Request, page 7

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.
- 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*.

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_3.5.2_SolarisK9) contains the files that are described in Table 1.

Table 1 Cisco BAC 3.5.2 Software Package Details

Files	Description
README.pdf	Readme for Cisco Broadband Access Center 3.5.2 (This document).
setup.bin	The Cisco BAC 3.5.2 installation program. See Installation Guide for Cisco Broadband Access Center, Release 3.5 for information about installing Cisco BAC 3.5.2.
upgrade/352Upgrade.tar	The product upgrade tar file.

Table 1 Cisco BAC 3.5.2 Software Package Details

Files	Description
version.txt	The product identification file.
Documentation/javadoc	Javadoc for the Cisco BAC Provisioning API.
kiwi/femtoConfig.kiwi	The configuration script file.
femto-cwmp-dictionary.xml	Sample dictionary.
sample-femto-cwmp-config.xml, sample-femto-cwmp-shutdown-config.xml, sample-femto-cwmp-firmware-rules.xml	Sample templates.

Downloading the Package

To download the Cisco BAC software (BAC_3.5.2_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.**

Step 4 The Select a Software Type page appears.

Step 5 Click the **Broadband Access Center for Telco Wireless Software** link.

Step 6 The Select a Release page appears.

Step 7 Choose **Latest Releases > 3.5.2**.

Step 8 The Release 3.5.2 Software page appears.

Step 9 Click the **Download Now** button next to BAC_3.5.2_Solaris.gtar.gz.

Step 10 The Download Cart page appears with the details of the software.

Step 11 Click the **Proceed With Download** button.

Step 12 Review Cisco's End User Software License Agreement and Software Download Rules, and click **Accept**.

Step 13 Choose one of the following download options:

- Download Manager Option
- Non Java Download Option

Step 14 Follow the prompts to download the package.

Installing Cisco BAC 3.5.2

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

Upgrading from Cisco BAC 3.5 or 3.5.1 or 3.5.1.1 or 3.5.1.2

You must apply the Cisco BAC 3.5.2 upgrade on your existing Cisco BAC 3.5 or 3.5.1 or 3.5.1.1 or 3.5.1.2 RDU and Cisco BAC 3.5 or 3.5.1 or 3.5.1.1 or 3.5.1.2 DPE. The Cisco BAC 3.5.2 installation instructions in this section are based on the assumption that you have Cisco BAC release 3.5 or 3.5.1 or 3.5.1.1 or 3.5.1.2 already installed.

Upgrading the RDU

To apply this patch on your Cisco BAC RDU server:

Step 1 Untar the file, 352Upgrade.tar.

Step 2 Go to the */upgrade*352 directory.

Step 3 Go to the */bin* directory.

Step 4 Run the *./352-upgrade-rdu.sh* script.

The Cisco BAC watchdog is stopped by the script.

The following message appears confirming the upgrade for Cisco BAC 3.5.2:

```
RDU Upgrade for BAC 3.5.2 Completed Successfully
```

Step 5 Start the Cisco BAC watchdog agent. To do this, run the following command:

/etc/init.d/bprAgent start

Step 6 Run AddProperties.kiwi, which is available in */upgrade352* directory, through Cisco BAC Tools.

Upgrading the DPE

To apply this patch on your Cisco BAC DPE server:

Step 1 Untar the file, 352Upgrade.tar.

Step 2 Go to the */upgrade*352 directory.

Step 3 Go to the */bin* directory.

Step 4 Run the *./352-upgrade-dpe.sh* script.

The Cisco BAC watchdog is stopped by the script.

The following message appears confirming the upgrade for Cisco BAC 3.5.2:

```
DPE Upgrade for BAC 3.5.2 Completed Successfully
```

Step 5 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 in Cisco BAC 3.5.2. Table 3 describes significant software issues that are known to exist in Cisco BAC 3.5.2.

For information on the complete list of Cisco BAC 3.5.2 bugs, see the *BAC352_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 lists the bugs resolved in this Cisco BAC 3.5.2 release.

Table 2 Resolved Problems

Bug ID	Summary
CSCtd25362	A forced configuration synchronization followed by a connection request for the device was showing an error in the DPE logs.
CSCtf99200	Database recovery performed after an upgrade from Cisco BAC 3.5.1 to 3.5.2 used to encounter a problem with the connectionUseSourceAddress flag.
CSCta65365	While changing the log level, the setloglevel tool was displaying incorrect message instead of successful log level change message.
CSCtf16198	The RDU was closing the connection for timeout if it took more than 2 minutes to send a message.
CSCtf59060	Provisional Group page was displaying incorrect fault information.
CSCta92181	While exporting the csv file using deviceExport.sh, the list values were not properly delimited.
CSCtg05626	getParamNames message was parsing the nextLevel incorrectly.
CSCtf79486	FAPs used to display the provisioning status wrongly. The following message used to get displayed: Service Enabled: Details: NWL outside of allowed tolerance.
CSCtf16196	Writing time-out feature of messaging system was not working.
CSCsz42402	replaceFile API command for generic files was executed non-concurrently.
CSCtf04976	Retrieving faults for a single device had issues.
CSCtg31800	DPE extension was displaying incorrect error message when no details was provided.
CSCtf76685	Messaging system was failing to send connection down event on write process timeout.
CSCth21396	DPE was not sending ACK for proxy ops.
CSCtf81330	BAC UI was not allowing entering a large string for the custom property.
CSCth84179	While deserializing an object, the device export tool was failing randomly.
CSCth86309	The verifyDb.sh tool was reporting that the Related PObject does not exist while verifying the relationship between the provisioning group and the IP device.
CSCth86455	The backupDb.sh tool was not copying all the bytes of a file.
CSCtf56369	deviceExport.sh tool had performance issue.

Known Problems

Table 3 identifies known bugs in this Cisco BAC 3.5.2 release, with possible workarounds.

Table 3 Known Software Problems

Bug ID	Summary	Explanation
CSCtd89992	Device operations such as get live data are getting timed out.	This occurs when a device takes more than 20 seconds to respond to the DPE. Workaround: Increase the connection read timeout value. To do this: 1. Add the property /server/http/services/1/read/timeout/msec, with appropriate time out value (in milliseconds) in the dpe.properties file. 2. Restart the DPE.

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.

Table 4 Abbreviations and Definitions

Term	Description
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.
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 3.5.2* (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.