Release Notes for Cisco Broadband Access Center 3.5

Revised: June 15, 2009, OL-18608-01

These release notes describe new software features, bug fixes, and documentation for Cisco Broadband Access Center (Cisco BAC), Release 3.5.

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.

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.

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

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 supports mass scale provisioning and managing of Femtocell Access Point (FAP) devices that function as a mini 3G cell tower in customer premises and backhaul via customer's internet connection. For details about the features supported in Cisco BAC 3.5, *see* New Features in Cisco BAC 3.5 section.

System Components

Cisco BAC comprises:

- A Regional Distribution Unit (RDU), which is software that you install on your server. The RDU 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 is software that you install on your server. The DPE server handles all device interactions for the RDU.
- An administrator user interface through which you can 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. You can use the provisioning API to register devices in Cisco BAC, assign device configuration policies, execute CWMP operations on the device, and configure the entire Cisco BAC provisioning system.

System Requirements

You must have the Solaris 10 operating system installed on your system to use the Cisco BAC software. For information on installation, refer to *Installation Guide for Cisco Broadband Access Center*, Release 3.5, which is available at: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_installation_guides_list.html.

Licensing Requirements

You require a valid license key to successfully provision devices that use Cisco BAC. These licenses are specific to the:

- CWMP technology
- DPE component

Note If you have not yet received your licenses, contact your Cisco representative.

New Features in Cisco BAC 3.5

This release supports mass scale provisioning and managing of Femtocell Access Point (FAP) devices that function as mini 3G cell tower in customer premises and backhaul via the customer's internet connection. The following features are supported in Cisco BAC 3.5:

CPE Redirection

Cisco BAC redirects a device to its home provisioning group by having the provisioning groups communicate among themselves to find the correct home provisioning group of the device.

When a device attempts to establish a CWMP session with a DPE, the DPE searches its cache for an entry related to that device. If it cannot find an entry for that device, it queries the other provisioning groups to determine the home provisioning group of the device. If the device's home provisioning group is found, it is redirected via HTTP to its home provisioning group.

To select the best available DPE in each provisioning group, the DPE maintains the status data of all other DPEs in the deployment. The DPE sends a status request at configured time intervals to update its knowledge of the state of other provisioning groups.

Centralized Connection Request Password Management

The connection request passwords can be autogenerated or specified by the Operational Support System (OSS). Cisco BAC can generate a unique connection request password for each CWMP device. The password is generated using the connection request master secret and is sent to all the DPEs. You specify the connection request master secret in the CWMP Defaults page in the administrator's user interface.

If the DPE fails to authenticate using the current password, Cisco BAC attempts to authenticate by using the old password derived from the earlier master secret. Cisco BAC stores the last 15 passwords, by default, and attempts authentication by using each of those passwords in reverse order, until authentication succeeds.

Signed Configuration

Cisco BAC uses the Signed Configuration feature to sign a portion of the CPE configuration that is targeted to be passed to the Femtocell Gateway by the CPE. For example, a CPE with Femtocell functionality passes the access control entries to the Femtocell Gateway.

The configuration is signed using a secret key that is shared between Cisco BAC and the Femtocell Gateway. The signed configuration eliminates the need to separately configure the Femtocell Gateway for each individual CPE. The signature provides proof to the gateway that the configuration:

- Was generated by Cisco BAC.
- Was not falsified during transmit.
- Is targeted for a specific CPE.
- Is targeted for a specific Gateway.
- Is current.

To prevent replay attacks, the time of the signature generation and its validity period are also incorporated in the signature.

Chatty Client Filter

Cisco BAC uses the Chatty client filter feature to detect and block devices that make an excessive number of TR-069 and HTTP file server calls. You can use this feature to reduce the adverse impact of chatty devices on services that are provided to other devices.

Using this feature, you can detect the chatty devices and throttle their access to the DPE. You can disable this feature from the DPE CLI, using the **chatty-client filter enabled** {*true* | *false*} command.

Cisco BAC uses the chatty client filter feature to monitor the CPE events based on the device identifier. If the number of events received from the device during the sample time interval is greater than the value configured for the sample-hits-to-throttle property, the DPE throttles the device. When a device is in the throttled state, all events that the device generates are discarded.

Cisco BAC continues to monitor the activity on the throttled device to determine whether the device can be restored to the normal state. If the device generates fewer events than the value configured for the quiet-hits property, the DPE moves the device back to the normal state.

Traffic Profiling

This release of BAC gives details about the traffic between the CPE and the DPE to provide visibility into flows that may be causing issues. This traffic profiling provides statistics on the following:

- Number of CWMP sessions handled
- Number of devices rejected
- Number of HTTP file requests handled
- Home provisioning Group redirection status
- Traffic caused by chatty clients

The periodic statistics provides details, including the name of each Remote Procedure Call (RPC) and the specific types of Inform messages.

To enable or disable traffic statistics on the RDU, from the user interface, choose **Configuration > Defaults > System Defaults.**

- To enable this feature, against Performance Statistics Collection, click the **Enabled** radio button.
- To disable this feature, against Performance Statistics Collection, click the **Disabled** radio button.

To enable or disable traffic statistics on the DPE, from the DPE CLI in the enabled mode, enter **debug dpe statistics**. To disable traffic profiling from the CLI, use the **no debug dpe statistics** command.

After you enable the traffic statistics feature, you can view the traffic statistics from the *perfstat.log* file or analyze the data by using the **runStatAnalyzer.sh** tool.

You can view the traffic statistics by using the administrator user interface. Choose **Servers > DPEs > Manage Device Provisioning Page > View Device Provisioning Engines Details**.

TACACS+ Support at RDU

From this release, Cisco BAC supports local authentication as well as TACACS+ authentication at the RDU. TACACS is a protocol that provides access control for routers, network access servers, and other network computing devices, using one or more centralized servers.

TACACS+ can be configured via administration user interface and Cisco BAC APIs. This enables the centralized remote authentication of the RDU and DPE users as well as API client via the TACACS+ server. When TACSCS+ authentication is enabled, the client attempts user login authentication to each server sequentially until a successful authentication exchange is executed, or the list is exhausted. After TACACS+ authentication is done, user authorization is retrieved from the RDU database.

Groups in Property Hierarchy

When Cisco BAC processes the configuration templates for substitutable parameters, it searches objects for this property using a certain order called property hierarchy. Cisco BAC properties allow you to access and store data in Cisco BAC using the API. Preprovisioned, discovered, and status data can be retrieved through the properties of corresponding objects, using the API. Properties also enable you to configure BAC at the appropriate level of granularity (from system level to device groups and to individual devices).

The Cisco BAC property hierarchy gives you the flexibility to define system-wide or service class defaults that can be overridden by individual devices.

Cisco BAC allows you to store any number of properties on objects in its data model. You can reference these properties in configuration templates or firmware rules. You can use properties in the following hierarchy:

- Device
- Group
- Provisioning Group
- Class of Service
- Device Type
- System Defaults

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 was tested for application stamina when exposed to Denial of Service attacks and protocol irregularities.

For information on the System Hardening, see http://cisco.com/en/US/docs/net_mgmt/broadband_access_center/3.5/release/notes/BAC35-HardeningGuidelines.pdf

Caveats

For information on the complete list of Cisco BAC bugs, see the *BAC35_BugList.html* file in the *docs/* subdirectory of the Cisco BAC CD-ROM or electronic distribution.

Table 1 describes significant software issues that are known to exist in this release of Cisco BAC.

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).

Known Software Problem

Table 1 identifies known bugs in this Cisco BAC release, with possible workarounds.

Table 1 Known Software Problems

Number	Description	Resolution
CSCsv39907	The Cisco BAC Administration UI does not display certain types of nodes in templates, if a template contains the *RandomDateTimeInRange* node. For example, when you view the details of the configuration template that has the *PeriodicInformTime* parameter, the Administration UI does not display the node value.	Currently, there is no workaround for this issue.
CSCsy69024	The Device Details page shows troubleshooting mode as disabled. This occurs when a device is related to the troubleshooting group and any other group, the Details page in the Administration UI for the device shows that *troubleshooting is disabled* for the device.	Currently, there is no workaround for this issue.

Table 1 Known Software Problems (continued)

Number	Description	Resolution
CSCsy40930	When you change the group type priority, automatic re-generation of device instructions does not occur. This error occurs because the DPE fails to re-generate the device configuration when you change group type priority. Therefore, the device can communicate with the DPE with the old configuration details.	Manually invoke the instruction generation service by searching for the devices related to the affected groups and then pressing *Regenerate All*.
CSCsx09726	The *Device History* log displays incorrect user information. This problem occurs when you log into the Administration UI, concurrently, with different IDs, and make changes to device properties. If you log into the Administration UI with two different sessions and user IDs that is, User1 and User2, and as User1 change some device properties, the device history log correctly shows that User1 has changed the device properties. Subsequently if you make changes to device properties as User2, the device history log correctly shows that User2 has changed the device properties. After this, if you modify device properties as User1, the device history log incorrectly shows that User2 has modified the device properties.	Use only one user ID with the Administration UI.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on http://www.cisco.com for any updates.

Table 2 describes the product documentation that is available.

Table 2 Product Documentation

Document Title	Available Formats
Release Notes for Cisco Broadband Access Center, Release 3.5. (This guide).	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_release_notes_list.html • On Software download page.
Installation Guide for Cisco Broadband Access Center, Release 3.5	• PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_installation_guides_list.html • On Software download page.

Table 2 Product Documentation (continued)

Document Title	Available Formats
Cisco Broadband Access Center Administrator's Guide, Release 3.5	• PDF on the product CD-ROM • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_maintenance_guides_list.html • On Software download page.
Integration Developer's Guide for Cisco Broadband Access Center, Release 3.5	• PDF on the product CD-ROM • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html • On Software download page.
Cisco Broadband Access Center DPE CLI Reference, Release 3.5.	• PDF on the product CD-ROM • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html • On Software download page.
Cisco Broadband Access Center 3.5 Third Party and Open Source Copyrights	On Cisco.com at this URL: http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_release_notes_list.html

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.