Cisco Broadband Access Center 3.10 Release Notes

Published: May, 2015

These release notes contain details on the new software features, bug fixes, and documentation for Cisco Broadband Access Center (Cisco BAC), Release 3.10.

Contents

Introduction

Cisco Broadband Access Center (Cisco BAC) 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 enables you to provision and manage 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, TR-106, and TR-196 standards. These devices include Ethernet and ADSL gateway devices, wireless gateways, VoIP ATAs, DLC, and other devices that are compliant with CWMP. For details about the features supported in Cisco BAC 3.10, see New Features in Cisco BAC 3.10, page 4 section.

System Components

Cisco BAC comprises:

- A Regional Distribution Unit (RDU) that is a 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) that is a 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). You can use this 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, run CWMP operations on the device, and configure the entire Cisco BAC provisioning system.
- Cisco Network Registrar extensions (CNR extensions), are the links between Cisco BAC and Cisco Network Registrar. You should install this component on all Cisco Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a failover environment, ensure that you install the extensions on the failover servers, as well.
- The Cisco Prime Access Register (PAR) Extensions are the links between Cisco BAC and Cisco Prime Access Registrar. You should install this component on all Cisco Prime Access Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a fail-over environment, ensure that you also install the extensions on the fail-over servers.

Installation Components

Pre-Maintenance Script

This script is used to automate the pre-maintenance window activities such as backup, database recovery and also verification, migration of the data base before any major upgrade from BAC version 3.8.1, 3.8.1.x or 3.9 to 3.10. This script should be run on the server where the RDU is installed. You can either choose a single prompt to complete all the above activities or execute them one-by-one by providing the appropriate inputs.

The script location is: **<BAC_Linux_Install_directory>/BAC_3.10_LinuxK9/pre_maintenance.sh**

Upgrade Prompt Change

Upgrading BAC from 3.8.1, 3.8.1.x or 3.9 to 3.10 has been improved for ease of use. The <BAC_Linux_Install_directory>/BAC_3.10_LinuxK9/install_bac.sh script has been enhanced to include automation of the following processes: backup, recovery, verify, migration and restore database.

This script also has the prompt to skip the above processes and execute them instead using the Pre-maintenance script.

Inter Build Upgrade

From BAC 3.10 release onwards, user can upgrade between the different build numbers of 3.10 version. Inter-build upgrade also supports the various database operations being automated using <BAC_Linux_Install_directory>/BAC_3.10_LinuxK9/install_bac.sh script.

System Requirements

- You must have Linux 5.x or 6.4 operating system installed on your system to use the Cisco BAC software. For information on installation, see the *Cisco Broadband Access Center 3.10 Installation Guide*.
- BAC uses Cisco Prime Network Registrar 8.3
- BAC uses Cisco Prime Access Registrar 7.0
- BAC 3.10 does not include a STUN server.

Note **Please note that the Solaris operating system is NOT supported for this release.**

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
- Feature Pack Licensing

Note Feature Pack licensing is required only for Java based DPE Technology extensions. If you have not yet received your licenses, contact your Cisco representative.

New Features in Cisco BAC 3.10

The following new features have been added to this release:

- IP Based Location Verification, page 4
- BAC_PROV_FLOW OPTIMIZATION, page 4
- Security Hardening, page 6
- Integrating BAC with Prime Central in DR Mode, page 6

IP Based Location Verification

IP Address To Location (IPL) is a new Location Verification (LV) method added to the Generally Available [GA] Provisioning flow. The main objective of this LV method is to validate the location of an AP using the IP Address. This LV method will be executed after ISM and before DNB. Similarly to other LV methods the IPL can also be part of the DNB. The IPL LV execution can be carried out on particular Event Codes. These Event Codes can be configured in the RDU Device record.

The location versification method needs a generic file, which should be preloaded to RDU. The existing “file add” mechanism (through admin UI / using file add API calls) can used to load this file to RDU.The file contents format should be << IpAddress,LAT,LONG >>. The file should be added to RDU as file type “Generic”.

BAC_PROV_FLOW OPTIMIZATION

BAC can now avoid unwanted configuration syncs on each inform.

Previously, the GA provisioning flow script triggered change-properties each time, even if there was no chassis found. This increased unwanted configuration sync on each inform. With this release, changes are done on triggering to avoid the unwanted configuration sync.

The following events sent via NBI can be enabled or disabled using flags.

- Connect Event
- Firmware Event
- Tampered Event

- Service Event
- Location Event
- Assign Data Notification Event (needs new flag)
- Group Updated Event (needs new flag)
- IPL Update Event

The ACKED flag needs to be implemented for the following two events: Assign Data Notification Event, Group Updated Event. The flag details are listed in the table below.

S. No.	Property Name	Data Type	Default Value
1	FC-ACKED-ASSIGN-DATA-EVENT	Boolean	False
2	FC-ACKED-GROUP-UPDATE-EVENT	Boolean	False

These flags can be enabled at PG Level, CoS Level and Device Level.

BAC will send all required attributes in events to avoid subsequent **get** done by PMG

For the events Service, Tampered, Connected and Firmware Verified the additional attributes added are cell id (UMTS/LTE) & FC-OTA-CELL-ID (UMTS).

For the event Location the additional attributes added are cell id (UMTS/LTE), FC-OTA-CELL-ID (UMTS) and FC-DNM-LIST.

ISM LV Optimization

Parsing and Caching Network IDs

- Only one data structure/file will have all the Subnet IDs and these are common for all devices, so should not parse/process the file each time.
- ISM File needs to be reloaded into the ISM Files Cache after its content has been updated.

Types of Informs which Trigger ISM LV

- ISM check only needs to be on specific informs as the device IP address only changes on specific conditions (such as device reboot, device location change, service provider GW IP change, etc.)
- The ISM LV processes the following default informs:
  - BOOTSTRAP
  - BOOT
  - VALUE CHANGE

Caching EID to IP, Subnet mapping

- Since the ISM file content is static, the ISM LV status for a device will not change frequently, you need to cache (in-memory) the EID to Device source IP, subnet ID mapping and reuse it from cache without doing subnet processing again. (This cache is called AP Specific Cache)
- If the ISM file is reimported, then the cache entry for the ISM file will be cleared. In addition, the entire cache will be cleared when the DPE is restarted.

Security Hardening

The encrypted user password is now stored in the kiwi files. Both encrypted password and clear text passwords can be used. The property UserDetailsKeys.IS_ENCRYPTED_PASSWORD in the same batch determines whether or not the password in the kiwi is encrypted.

BAC will lock the user session for an administrator-configured interval of time when the threshold for incorrect login attempts is reached.

If the user session is locked due to incorrect login, it will be automatically unlocked after the configured interval time. If the user needs to unlock within the configured interval time, BAC will allow administrator to override the configured time and unlock the user account.

Upon successful login access, the BAC will display the date and time of the user's last successful access and last failed access to the RMS.

Integrating BAC with Prime Central in DR Mode

This release supports integrating BAC with Prime central in Disaster Recovery (DR) mode. The existing primeIntegration.sh script has been enhanced to extend its support to Active and DR modes.

To successfully integrate BAC with Prime central in DR mode, you need to specify a valid Domain Manager (DM) ID. Before integrating BAC with Prime central in DR mode, the user must ensure dmid.xml file does not exist. The dmid.xml file resides in the directory <BAC_HOME>/prime_integrator.

Broadband Access Center 3.10 Bugs

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Procedure

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter **Broadband Access Center 3.10**, and press **Enter** (Leave the other fields empty).

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Tip To export the results to a spreadsheet, click **Export Results to Excel**.

Related Documentation

For details, see the Cisco Broadband Access Center 3.10 Administration Guide and the Cisco Broadband Access Center 3.10 Installation Guide.

The following document gives you the list of user documents for Cisco Prime Network Registrar 8.3:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_registrar/8-3/doc_overview/guide/CPNR_8_3_Doc_Guide.html

The following document gives you the list of user documents for Cisco Prime Access Registrar 7.0:

http://www.cisco.com/en/US/docs/net_mgmt/prime/access_registrar/7.0/roadmap/guide/PrintPDF/ardocgd.html

Accessibility Features in Broadband Access Center 3.10

For a list of accessibility features in Broadband Access Center, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

Note All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.