



## CHAPTER 9

# Managing Cisco Broadband Access Center

---

This chapter describes the various subcomponents within Cisco Broadband Access Center (BAC) that you can use to manage the system.

This chapter includes the following sections:

- [Cisco BAC Process Watchdog, page 9-1](#)
- [Administrator User Interface, page 9-4](#)
- [Command Line Interface, page 9-5](#)
- [SNMP Agent, page 9-6](#)
- [Cisco BAC Tools, page 9-7](#)

## Cisco BAC Process Watchdog

The Cisco BAC process watchdog is an administrative process that monitors the runtime health of all Cisco BAC processes. This watchdog process ensures that, if a process stops unexpectedly, it is automatically restarted. One instance of the Cisco BAC process watchdog runs on every system which runs Cisco BAC components.

You can use the Cisco BAC watchdog as a command-line tool to start, stop, restart, and determine the status of any monitored processes.

You can enable the SNMP trap facility for Cisco BAC process watchdog. The SNMP traps are sent only when:

- there is a change in component's state.
- the component is gracefully shut down.

If a monitored application fails to start or stops unexpectedly, the Cisco BAC process watchdog reports the critical condition associated with the monitored application to the trap receiver through SNMP trap. The Cisco BAC process watchdog will wait for a prescribed amount of time before attempting to restart the monitored application. When the monitored application restarts, the Cisco BAC process watchdog sends another SNMP trap to the SNMP trap receiver informing the change in application's state.

At the beginning, restart attempt is made at an interval of 1 second, and is increased exponentially with every subsequent attempt until the interval becomes 5 minutes. After that, the process restart is attempted at 5-minute intervals until successful. Five minutes after a successful restart, the period is automatically reset to 1 second again.

For example:

- Process A fails.
- The Cisco BAC process watchdog server sends an SNMP trap informing the critical condition associated with the process A.
- The Cisco BAC process watchdog server attempts to restart it and the first restart fails.
- The Cisco BAC process watchdog server waits for 2 seconds, and attempts to restart it and the second restart fails.
- The Cisco BAC process watchdog server waits for 4 seconds, and attempts to restart it and the third restart succeeds.
- The Cisco BAC process watchdog server sends the SNMP trap to the trap receiver informing the change in state of process A.

## Using Cisco BAC Process Watchdog from the Command Line

The Cisco BAC watchdog agent automatically starts whenever the system boots up. Consequently, this watchdog also starts those Cisco BAC system components installed on the same system. You can also control the Cisco BAC watchdog through a simple command-line utility by running the `/etc/init.d/bprAgent` command.

Table 9-1 describes the command line interface commands available for use with the Cisco BAC watchdog process.

**Table 9-1 Cisco BAC Watchdog Agent CLI Commands**

Command	Description
<code>bprAgent start</code>	Starts the Cisco BAC watchdog agent, including all monitored processes.
<code>bprAgent stop</code>	Stops the Cisco BAC watchdog agent, including all monitored processes.
<code>bprAgent restart</code>	Restarts the Cisco BAC watchdog agent, including all monitored processes.
<code>bprAgent status</code>	Gets the status of the Cisco BAC watchdog agent, including all monitored processes.
<code>bprAgent start <i>process-name</i></code>	Starts one particular monitored process. The value <i>process-name</i> identifies that process.
<code>bprAgent stop <i>process-name</i></code>	Stops one particular monitored process. The value <i>process-name</i> identifies that process.
<code>bprAgent restart <i>process-name</i></code>	Restarts one particular monitored process. The value <i>process-name</i> identifies that process.

**Table 9-1 Cisco BAC Watchdog Agent CLI Commands (continued)**

Command	Description
bprAgent status <i>process-name</i>	Gets the status of one particular monitored process. The value <i>process-name</i> identifies that process.

The *process-name* mentioned in Table 9-1 can be:

- rdu—Specifies the RDU server.
- dpe—Specifies the DPE server.
- stun—Specifies the STUN server.
- snmpAgent—Specifies the SNMP agent.
- tomcat—Specifies the administrator user interface.
- cli—Specifies the DPE command line interface.

When the operating system (Solaris and Linux) is rebooted, the Cisco BAC process watchdog is first stopped, allowing Cisco BAC servers to shut down properly. To shut down or reboot the operating system gracefully, use the **init 6** command.

The **reboot** command does not execute application shut down hooks and kills Cisco BAC processes rather than shutting them down. While this action is not harmful to Cisco BAC, it may delay server start-up and skew certain statistics and performance counters.

The events that trigger an action in the Cisco BAC watchdog daemon, including process crashes and restarts, are logged in a log file, *<BPR\_HOME>/agent/logs/agent.log*. The watchdog daemon also logs important events to syslog under standard `local6` facility.

## Enabling SNMP Trap for Cisco BAC Process Watchdog

The Cisco BAC process watchdog can be configured to send SNMP traps to the trap receiver for all the critical conditions of Cisco BAC components. The critical conditions include:

- BAC process fails to start, restart, or stop
- BAC process stops unexpectedly
- Cisco BAC process watchdog fails to start or stop

The Cisco BAC process watchdog runs on the following BAC components:

- RDU
- DPE
- CLI
- Tomcat
- SNMPAgent
- STUNServer

To enable SNMP trap for Cisco BAC process watchdog:

- 
- Step 1** Log into Cisco BAC host as root.
- Step 2** Set the following parameters in *CbsServerTable.xml* file located at `<BPR_HOME>/snmp/xmlFiles/CISCO-BACC-SERVER-MIB`:
- `cbsServerType` - `<component>`
  - `cbsNotifEnableFlags` - 1
- Step 3** Configure the trap receiver to receive the SNMP traps from the BAC components. The trap receiver is added as SNMP host with the required community and listening port. For information on how to add SNMP host and community, see [Using the snmpAgentCfgUtil.sh Tool, page 11-6](#).
- Step 4** Start, stop, or restart the BAC components or watchdog, and verify if the trap receiver receives the SNMP traps.
- 

## Administrator User Interface

The Cisco BAC administrator user interface is a web-based application for central management of the Cisco BAC system. You can use this interface to:

- Configure global defaults
- Define custom properties
- Set up Classes of Service
- Manage firmware rules and configuration templates
- Add and edit device information
- Group devices
- Execute device operations
- View server status and statistics
- View device history
- View server logs
- Manage users

Refer to these chapters for specific instructions on how to use this interface:

- [Understanding the Administrator User Interface, page 15-1](#), describes how to access and configure the Cisco BAC administrator user interface.
- [Using the Administrator User Interface, page 16-1](#), provides instructions for performing administrative activities involving the monitoring of various Cisco BAC components.
- [Configuring Broadband Access Center, page 17-1](#), describes tasks that you perform to configure Cisco BAC.

# Command Line Interface

The Cisco BAC CLI is an IOS-like command line interface which you use to configure as well as view the status of the DPE by using Telnet. The CLI supports built-in command help and command autocompletion.

You can enable authentication of the CLI through a locally configured login and enable passwords, or through a remote username and password for a TACACS+ service.

To access the DPE CLI, open a Telnet session to port 2323 from a local or remote host.

## Accessing the DPE CLI from a Local Host

To access the CLI from a local host, you can use:

```
# telnet localhost 2323
```

or

```
# telnet 0 2323
```

## Accessing the DPE CLI from a Remote Host

To access the CLI from a remote host, enter:

```
# telnet remote-hostname 2323
```

**Note**

If you cannot establish a Telnet connection to the CLI, the CLI server might not be running. You may need to start the server; enter:

```
# /etc/init.d/bprAgent start cli
```

After you access the CLI, you must enter the DPE password to continue. The default login and enable passwords are **changeme**.

See the [Cisco Broadband Access Center 3.8 DPE CLI Reference](#), for specific information on the CLI commands that a DPE supports.

## SNMP Agent

Cisco BAC provides basic SNMP v2-based monitoring of the DPE and RDU servers. The Cisco BAC SNMP agents support SNMP informs and traps. You can configure the SNMP agent on the DPE by using the `snmp-server` CLI commands, and on the RDU by using SNMP configuration CLI commands.

The SNMP agent also provides support for monitoring essential Cisco BAC details, such as server state, server-specific statistics, communication between servers, and license information.

For additional information on the SNMP configuration command line tool, see [Monitoring Cisco Broadband Access Center, page 11-1](#). For additional information on the DPE CLI, refer to the [Cisco Broadband Access Center 3.8 DPE CLI Reference](#).

# Cisco BAC Tools

Cisco BAC provides automated tools that you use to perform certain functions more efficiently.

[Table 9-2](#) lists the various tools that this Cisco BAC release supports:

**Table 9-2** *List of Cisco BAC Tools*

Tool	Description	Refer ...
Configuration Tool	Used to test, validate, and view Cisco BAC template and configuration files.	<a href="#">Using the Configuration Utility, page 5-22</a>
Cisco BAC Process Watchdog	Interacts with the Cisco BAC watchdog daemon to observe the status of the Cisco BAC system components, and stop or start servers.	<a href="#">Using Cisco BAC Process Watchdog from the Command Line, page 9-2</a>
SNMP Agent Configuration Tool	Sets the log level of the RDU, and enables or disables debugging log output.	<a href="#">Using the snmpAgentCfgUtil.sh Tool, page 11-6</a>
RDU Log Level Tool	Retrieves device information from the Cisco BAC backup database and exports the information to a flat file.	<a href="#">The RDU Log Level Tool, page 21-5</a>
Device Export Tool	Sets threshold values for one or more file systems. When these thresholds are surpassed, an alert is generated until additional disk space is available.	<a href="#">Using the deviceExport.sh Tool, page 20-1</a>
Disk Space Monitoring Tool	Manages certificates in a certificate store in support of HTTP over SSL services on the DPE.	<a href="#">Using the disk_monitor.sh Tool, page 20-4</a>
Keytool Utility	Enables you to temporarily reset bacadmin authentication to local RDU, when TACACS+ authentication is enabled.	<a href="#">Configuring DPE Keystore by Using the Keytool, page 13-3</a>
Password Reset Tool	Sets the log level of the RDU, and enables or disables debugging log output.	<a href="#">Using the resetAdminPassword.sh Tool, page 20-5</a>
Event Monitor Tool	Used to view the events that are being fired in Cisco BAC.	<a href="#">Using the runEventMonitor.sh Tool, page 20-5</a>

