



CHAPTER 9

Managing Cisco Broadband Access Center

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

- [Cisco BAC Process Watchdog, page 9-1](#)
- [Administrator User Interface, page 9-3](#)
- [Command-Line Interface, page 9-3](#)
- [SNMP Agent, page 9-4](#)
- [Cisco BAC Tools, page 9-4](#)

Cisco BAC Process Watchdog

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

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

If a monitored application fails, it is restarted automatically. If, for any reason, the restart process also fails, the Cisco BAC process watchdog server waits a prescribed length of time before trying to restart.



Note

You do not have to use the Cisco BAC process watchdog and the SNMP agent to monitor the extensions that are installed on Cisco Network Registrar.

The period between restart attempts starts at 1 second and increases exponentially with every subsequent attempt until it reaches a length of 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:

1. Process A fails.
2. The Cisco BAC process watchdog server attempts to restart it and the first restart fails.
3. The Cisco BAC process watchdog server waits 2 seconds and attempts to restart the process and the second restart fails.

4. The Cisco BAC process watchdog server waits 4 seconds and attempts to restart the process and the third restart fails.
5. The Cisco BAC process watchdog server waits 16 seconds and attempts to restart the process.

Using the Cisco BAC Process Watchdog from the Command Line

The Cisco BAC process watchdog automatically starts whenever the system boots up. Consequently, this watchdog also starts those Cisco BAC system components installed on the same system. You can 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 (CLI) commands available for use with the Cisco BAC process watchdog.

Table 9-1 Cisco BAC CLI Commands

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

- **rdu**—Specifies the RDU server.
- **dpe**—Specifies the DPE server.
- **kdc**—Specifies the KDC server.
- **snmpAgent**—Specifies the SNMP agent.
- **tomcat**—Specifies the administrator.
- **cli**—Specifies the DPE CLI.

**Note**

When the Solaris operating system 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, use the Solaris **shutdown** command. Remember, the Solaris **reboot** command does not execute application shutdown hooks and kills Cisco BAC processes rather than shutting them down. While this action is not harmful to Cisco BAC, it may delay server startup 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 the standard `local6` facility.

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 system to:

- Configure global defaults
- Define custom properties
- Add, modify, and delete Class of Service
- Add, modify, and delete DHCP Criteria
- Add, modify, and delete devices
- Add and edit device information
- Group devices
- View server status and server logs
- Manage users

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

- [Chapter 11, “Understanding the Administrator User Interface,”](#) describes how to access and configure the Cisco BAC administrator user interface.
- [Chapter 12, “Using the Administrator User Interface,”](#) provides instructions for performing administrative activities involving the monitoring of various Cisco BAC components.
- [Chapter 13, “Configuring Cisco Broadband Access Center,”](#) describes tasks that you perform to configure Cisco BAC.

Command-Line Interface

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

You can enable authentication of the CLI through a locally configured login and privileged 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 local_hostname 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 privileged passwords are **changeme**.

See the *Cisco Broadband Access Center DPE CLI Reference 4.1* for specific information on the CLI commands that a DPE supports.

SNMP Agent

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

For additional information on the SNMP configuration command-line tool, see [Using the snmpAgentCfgUtil.sh Tool, page 10-10](#). For additional information on the DPE CLI, see the *Cisco Broadband Access Center DPE CLI Reference 4.1*.

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 Cisco BAC Tools

Tool	Description	Refer...
Configuration File Utility	Used to test, validate, and view Cisco BAC template and configuration files.	Using the Configuration File Utility for Template, page 5-30
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.	Using the Cisco BAC Process Watchdog from the Command Line, page 9-2
RDU Log Level Tool	Sets the log level of the RDU, and enables or disables debugging log output.	Using the RDU Log Level Tool, page 10-4
PacketCable Certificates Tool	Installs, and manages, the KDC certificates that are required by the KDC for its operation.	Using the PKCert.sh Tool, page 14-2
KeyGen Tool	Generates PacketCable service keys.	Using the KeyGen Tool, page 14-8
Changing Network Registrar Properties Tool	Used to change key configuration properties used by Cisco BAC extensions that are incorporated into the Network Registrar DHCP server.	Using the changeNRProperties.sh Tool, page 14-11
SNMP Agent Configuration Tool	Manages the SNMP agent.	Using the snmpAgentCfgUtil.sh Tool, page 10-10
Diagnostics Tool	Collects server data related to system performance and troubleshooting.	Troubleshooting Using the Diagnostics Tool, page 16-5
BundleState.sh Tool	Bundles diagnostics data related to server state for support escalations.	Bundling Server State for Support, page 16-10
Disk Space Monitoring 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.	Using the disk_monitor.sh Tool, page 14-12

