CHAPTER 3

Configuration Workflows and Checklists

This chapter is divided into two major sections that define the processes to follow when configuring Cisco Broadband Access Center (Cisco BAC) components to support various technologies.

This chapter includes the following sections:

- Component Workflows, page 3-1
- Technology Workflows, page 3-3

Component Workflows

This section describes the workflows you must follow to configure each Cisco BAC component for the technologies supported by Cisco BAC. These configuration tasks are performed before configuring Cisco BAC to support specific technologies.

The component workflows described in this section are arranged in a checklist format and include:

- RDU Checklist
- DPE Checklist

RDU Checklist

Table 3-1 identifies the workflow to follow when configuring the RDU.

Table 3-1 RDU Workflow Checklist

Procedure	Refer to...
1. Configure the system syslog service for use with Cisco BAC.	*Installation Guide for Cisco Broadband Access Center 3.8*
2. Access the Cisco BAC administrator user interface.	Configuring the Administrator User Interface, page 15-1
3. Change the admin password.	Configuring the Administrator User Interface, page 15-1
4. Add the appropriate license keys.	Managing License Keys, page 17-20

Table 3-1 RDU Workflow Checklist (continued)

Procedure	Refer to...
5. Configure the RDU database backup procedure.	Backup and Recovery, page 10-4
6. Configure the RDU SNMP agent.	Using the snmpAgentCfgUtil.sh Tool, page 11-6

DPE Checklist

You must perform the tasks described in Table 3-2 after those described in Table 3-1.

Note Items marked with an asterisk (*) are mandatory tasks or procedures.

Table 3-2 DPE Configuration Checklist

Procedure	Refer to ...
1. Configure the system syslog service for use with Cisco BAC.	*Cisco Broadband Access Center 3.8 Installation Guide.*
2. Change the passwords.*	The **password** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
3. Configure the provisioning interface.	The **interface ethernet** [**intf0** | **intf1**] command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
4. Configure the Cisco BAC shared secret.*	The **dpe shared-secret** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
5. Configure the DPE to connect to the desired RDU.*	The **dpe rdu-server** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
6. Configure the network time protocol (NTP).	Solaris or Linux documentation for configuration information.
7. Configure the provisioning group name.*	The **dpe provisioning-group primary** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
8. Configure the required routes to the RDU as well as to the devices in the network.	Solaris or Linux documentation for configuration information.
9. Configure the DPE SNMP agent.	The SNMP agent commands in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*

Note You can configure the SNMP agent using either the DPE command line interface or the snmpAgentCfgUtil.sh tool. For more information, see Using the snmpAgentCfgUtil.sh Tool, page 11-6.

Table 3-2 DPE Configuration Checklist (continued)

Procedure	Refer to ...
10. Verify that the DPE successfully connected to the RDU and was registered.	Viewing Servers, page 16-22
11. Configure the home provisioning group redirection service on the DPE	The **interface ip** *x.x.x.x.* **pg-communication** and **service cwmp-redirect 1 enable** commands described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*

Technology Workflows

This section describes the tasks that you must perform when configuring Cisco BAC to support specific technologies; in this case, CWMP. These configuration tasks are performed after configuring Cisco BAC components.

The CWMP technology workflows described in this section are arranged in a checklist format and include:

- RDU Configuration Workflow, page 3-3
- DPE Configuration Workflow, page 3-5

RDU Configuration Workflow

Table 3-3 identifies the configuration tasks you must perform to configure the RDU for the CWMP technology.

Table 3-3 RDU Configuration Workflow

Procedure	Refer to ...
1. Create service profiles by using the Cisco BAC Class of Service. Define custom properties referenced in templates from the administrator user interface. The custom properties can be referenced in configuration and firmware rules templates. For each service, you must:	Configuring Custom Properties, page 17-5
a. Create a configuration template. Add the configuration template to the RDU from the administrator user interface.	Adding Files, page 17-17
b. Create a firmware rules template. – Add the firmware images to the RDU from the administrator user interface. – Add the firmware rules template to the RDU from the administrator user interface.	Adding Files, page 17-17

Table 3-3 RDU Configuration Workflow (continued)

Procedure	Refer to ...
c. Create a Class of Service from the administrator user interface. Remember to: – Specify the configuration template file. – Specify the firmware rules file. – Optionally, specify properties.	Configuring the Class of Service, page 17-1
2. Configure default settings for the CWMP technology from the administrator user interface. – Set the default Class of Service; for example, for unknown devices. – Set the Connection Request Service defaults from any of the following pages: **Configuration > Class of Service**; **Configuration > Defaults**; and **Devices.**	Configuring Defaults, page 17-6
3. Preregister the CWMP devices.	Preregistering Device Data in Cisco BAC, page 3-4

Preregistering Device Data in Cisco BAC

Preregistering adds the device record to the RDU before the device makes initial contact with the DPE. The DPE is also known as the autoconfiguration server (ACS). This task is typically executed from the provisioning API. However, you can preregister device data from the administrator user interface as well.

To preregister device data in Cisco BAC:

Step 1 Add the device record to the RDU database by using the API or the administrator user interface.

To add a device record from the administrator user interface:

a. Choose **Devices > Manage Devices**.

b. On the Manage Devices page, click **Add.**

The Add Device page appears.

c. Enter values in the appropriate fields. The required and recommended provisioning attributes for a preregistered device are:

Required
• Device identifier
• Registered Class of Service
• Home provisioning group
Additional Typical Attributes Additional attributes may be required depending on customer premises equipment (CPE) authentication methods.

• Owner identifier
• CPE password, if client authentication using unique client certificates is not enabled.
• Connection Request username. This step is optional.
• Connection Request password. This step is optional.
Optional
Connection Request Methods on the Class of Service. This step is optional. Configuring the connection request method enables device authentication of the autoconfiguration server. Choose from: • Discovered • Use FQDN • Use IP

Step 2 Verify whether the device record is preregistered. To do this:

- Examine the Device Details. To do this:

  From the **Devices > Manage Devices** page, click the **View Details** icon ( ) corresponding to the device. From the Device Details page:

  – Check if the device settings are correct.

  – Look for discovered parameters; these parameters are not displayed if the device is yet to initiate its first contact with the DPE.

  – Check the Device History log.

- Examine the RDU and the DPE log files (see Logging, page 21-2).

Step 3 Configure the device to send periodic informs to the DPE. To do this, set the *PeriodicInformEnable* and the *PeriodicInformInterval* variables in a configuration template.

Step 4 Initiate device contact with Cisco BAC for the first time. To initiate device contact, do one of the following:

- Initiate a connection request from the API.
- Wait for the next periodic contact from the device.
- Reboot.

Step 5 Verify the first device contact with Cisco BAC. From **Device > Manage Devices > Device Details**, check if discovered properties are visible. Also, check the history log for details.

DPE Configuration Workflow

This section describes how you can provide CWMP support at the DPE, by configuring:

- CWMP services for CWMP management on the DPE.

  See Configuring CWMP Service on the DPE, page 3-6.

- HTTP file services for firmware management on the DPE.

  See Configuring HTTP File Service on the DPE, page 3-7.

- Configuring HTTP auth service on DPE.

Configuring CWMP Service on the DPE

Table 3-4 identifies the configuration tasks that you must perform to configure the CWMP services on the DPE.

Table 3-4 DPE Configuration Workflow - CWMP Management

Procedure	Refer to ...
Configure the CWMP services that run on the DPE. Configuring the CWMP technology on the DPE requires that you enable at least one CWMP service. To enable a CWMP service, enter: **`service cwmp`** *num* **`enable true`** where *num* identifies the CWMP service, which could be 1 or 2. By default, the CWMP service is: – Enabled on service 1. – Disabled on service 2.	The CWMP Technology Commands described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.
1. Configure the port on which the CWMP service communicates with the CPE. By default, the CWMP service is configured to listen on: – Port 7547 for service 1. – Port 7548 for service 2.	The **service cwmp** *num* **port** *port* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
2. Configure client authentication for the CWMP service. To limit security risks during client authentication, we recommend using the Digest mode (the default configuration). You should not allow client authentication in the Basic mode, or altogether disable Basic and Digest authentication.	The **service cwmp** *num* **client-auth** *mode* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.
3. Configure client authentication using certificates through SSL for the CWMP service.	The **service cwmp** *num* **ssl client-auth** *mode* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.
4. Configure the DPE to request configuration from the RDU for devices unknown to the DPE. Enabling this feature may allow a Denial of Service attack on the RDU.	The **service cwmp** *num* **allow-unknown-cpe** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.

Configuring HTTP File Service on the DPE

Table 3-5 identifies the configuration tasks that you must perform to configure the HTTP file services running on the DPE.

Table 3-5 DPE Configuration Workflow - Firmware Management

Procedure	Refer to ...
Configure the HTTP file service that runs on the DPE. Configuring firmware management on the DPE requires that you enable at least one HTTP file service. To enable a HTTP file service, enter: `service http num enable true` where *num* identifies the HTTP file service, which could be 1 or 2. By default, the HTTP service is: – Enabled on service 1. – Disabled on service 2.	The CWMP Technology Commands described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
1. Configure the port on which the HTTP file service communicates with the CPE. By default, the HTTP file service is configured to listen on: – Port 7549 for service 1. – Port 7550 for service 2.	The **service http** *num* **port** *port* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
2. Configure client authentication for the HTTP file service. To limit security risks during client authentication, we recommend that you use the Digest mode (the default configuration). You should not allow client authentication in the Basic mode, or altogether disable Basic and Digest authentication.	The **service http** *num* **client-auth** *mode* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
3. Configure client authentication by using certificates through SSL for the HTTP file service.	The **service http** *num* **ssl client-auth** *mode* described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*

Configuring HTTP Auth Service on the DPE

Table 3-6 below identifies the configuration tasks that you must perform to configure the AUTH services on the DPE.

Table 3-6 DPE Configuration Workflow - AUTH Management

Procedure	Refer to ...
Configure the Auth service that run on the DPE. To enable a Auth service, enter: `service auth 1 enabled true` By default, the Auth service is enabled.	The CWMP Technology Commands described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
Configure the http interface on which the Auth service is running on. To configure the Auth service interface, enter: `service auth 1 address (host_fqdn)` By default, the Auth service is configured to listen on `localhost`.	The **service http** *num* **port** *port* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
Configure the port on which the Auth service communicates with the CAR-EP. To configure the Auth service port, enter: `service auth 1 port port_num` By default, the Auth service is configured to listen on `7551`.	The **service http** *num* **client-auth** *mode* command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
Enables or disables use of HTTP over SSL/TLS for the Auth service. To enable SSL/TLS for the Auth Service interface, enter: `service auth 1 ssl enabled true`	The **service http** *num* **ssl client-auth** *mode* described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*

Provisioning Group Configuration Workflow

Provisioning groups are automatically created when the DPE is first configured to be in a particular provisioning group (see Adding DPE to a Provisioning Group, page 12-18), and then it registers with the RDU. After the provisioning group is created, you can configure it by assigning the URL of the Cisco BAC server from the administrator user interface.

Before configuring the provisioning group URL, familiarize yourself with Cisco BAC concepts regarding local and regional redundancy. These concepts are described in Provisioning Group Scalability and Failover, page 12-16.

Note We recommend that you assign a URL to the provisioning group right when you create the provisioning group. Assigning the URL enables CPE redirection between provisioning groups. If you are using a load balancer, ensure that the address of the load balancer is used as the ACS URL.

To configure the ACS URL of a provisioning group from the administrator user interface:

Step 1 On the primary navigation bar, click **Servers > Provisioning Groups**.

The Manage Provisioning Groups page appears.

Step 2 Click the identifier link of the correct provisioning group.

The View Provisioning Group Details page appears.

Step 3 In the Provisioning Group Properties area, enter the URL in the ACS URL field.

Note Remember that the URL that you configure overrides the discovered ACS URL.

Step 4 Click **Submit**.

The provisioning group now contacts Cisco BAC at the URL that you configured.

Configuring Home Provisioning Group Redirection Service on the DPE

Cisco BAC provides redirection to the home provisioning group of a device by having the provisioning groups communicate among themselves (see Redirecting CPE to Home Provisioning Group, page 14-7).

To enable the home provisioning group redirection feature, you must configure the home provisioning group redirection service on the DPE.

Table 3-7 identifies the configuration tasks that you must perform to configure the home provisioning group redirection service on the DPE.

Table 3-7 Home Provisioning Group Redirection Configuration

Procedure	Refer to...
1. Configure the DPE to use the interface identified by the IP address for communication with other provisioning groups. If you do not configure the DPE to use this interface, the DPE always binds to the localhost.	The **interface ip** *x.x.x.x.* **pg-communication** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*
2. Configure the cwmp-redirect service on the DPE. To enable the cwmp-redirect service, enter: `service cwmp-redirect 1 enable true`	The **service cwmp-redirect 1 enable** command described in the *Cisco Broadband Access Center 3.8 DPE CLI Reference*

For information on CLI commands used for the cwmp-redirect service, see the *Cisco Broadband Access Center 3.8 DPE CLI Reference.*