



BCM2 Series Power Meter

User Guide
Release 3.2.1

Copyright © 2015 Raritan, Inc.

BCM2-0A-v3.2.1-E

December 2015

255-64-0003-00

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2015 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.



Safety Information

DANGER!

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Follow safe electrical work practices. See NFPA 70E in the USA, or applicable local codes.
- This equipment must only be installed and serviced by qualified electrical personnel.
- Read, understand and follow the instructions before installing this product.
- Turn off all power supplying equipment before working on or inside the equipment.
- Any covers that may be displaced during the installation must be reinstalled before powering the unit.
- Use a properly rated voltage sensing device to confirm power is off.
- **DO NOT DEPEND ON THIS PRODUCT FOR VOLTAGE INDICATION**
- **Failure to follow these instructions will result in death or serious injury.**

NOTICE

- This product is not intended for life or safety applications.
- Do not install this product in hazardous or classified locations.
- The installer is responsible for conformance to all applicable codes.
- Mount this product inside a suitable fire and electrical enclosure.

CAUTION

RISK OF EQUIPMENT DAMAGE

- This product is designed only for use with 0.33V output current transducers (CTs).
- DO NOT USE CURRENT OUTPUT (e.g. 5A) CTs ON THIS PRODUCT.
- Failure to follow these instructions can result in overheating and permanent equipment damage.

For use in a Pollution Degree 2 or better environment only. A Pollution Degree 2 environment must control conductive pollution and the possibility of condensation or high humidity. Consider the enclosure, the correct use of ventilation, thermal properties of the equipment, and the relationship with the environment. Installation category: CAT II or CAT III

Provide a disconnect device to disconnect the meter from the supply source. Place this device in close proximity to the equipment and within easy reach of the operator, and mark it as the disconnecting device. The disconnecting device shall meet the relevant requirements of IEC 60947-1 and IEC 60947-3 and shall be suitable for the application. Disconnecting fuse holders can be used in the USA and Canada. Provide overcurrent protection and disconnecting device for supply conductors with approved current limiting devices suitable for protecting the wiring.

If the equipment is used in a manner not specified by the manufacturer, the protection provided by the device may be impaired.



This symbol indicates an electrical shock hazard exists.



Documentation must be consulted where this symbol is used on the product.

Contents

Safety Information	iii
---------------------------	------------

Chapter 1 Introduction	1
-------------------------------	----------

Product Models	1
Product Overview - PM Series Power Meters	2
Product Overview - BCM2 Series	3

Chapter 2 Installation and Initial Configuration	4
---	----------

Hardware Installation	4
Login and Configuration.....	4
Configuring Power Meters and Branch Circuit Monitors	5
Using the BCM2's Display	11
Alerts.....	11
Power Meters.....	13
Device Info.....	14
Peripherals.....	18

Chapter 3 Connecting External Equipment (Optional)	22
---	-----------

Connecting Environmental Sensor Packages	22
DPX Sensor Packages	23
DPX2 Sensor Packages	26
DX Sensor Packages	28
Connecting Asset Management Sensors	31
Combining Regular Asset Sensors.....	31
Connecting Regular Asset Sensors to the BCM2	33
Connecting Blade Extension Strips	34
Connecting Composite Asset Sensors to the BCM2.....	37
Connecting a Logitech Webcam.....	39
Connecting a GSM Modem	40
Connecting an Analog Modem	41
Connecting an External Beeper.....	41
Cascading the BCM2 via USB.....	42
Wireless Network Connection.....	44
USB Wireless LAN Adapters.....	44
Supported Wireless LAN Configuration.....	45

Chapter 4 Using the Web Interface 46

Supported Web Browsers	47
Changing Your Password	47
Introduction to the Web Interface	48
Status Bar	49
Add a Page Icon	50
The Yellow- or Red-Highlighted Sensors	50
Viewing the Dashboard	52
Alerted Sensors	53
Alarms List	53
Device Management	54
Displaying the Device Information	55
Naming the BCM2	59
Modifying the Network Configuration	59
Modifying Network Service Settings	69
Setting the Date and Time	80
Setting Default Measurement Units	82
Configuring the Feature Port	82
Front Panel Settings	83
Configuring the Serial Port	84
Setting the Cascading Mode	85
Specifying the Device Altitude	90
Setting Data Logging	91
Configuring SMTP Settings	92
Configuring Data Push Settings	93
Resetting All Active Energy	94
Checking the Internal Beeper State	95
User Management	95
Creating a User Profile	96
Modifying a User Profile	99
Deleting a User Profile	99
Setting Up Your Preferred Measurement Units	100
Setting Up Roles	101
Permissions	101
Creating a Role	101
Modifying a Role	102
Deleting a Role	103
Meter, Panel, and Branch Circuit Monitoring and Management	104
Viewing the Panel Data	104
Panel Mains Circuit Management	106
Panel Branch Circuits Operations	109
Viewing the Power Meter Data	111
Power Meter Management	112
Setting Power Thresholds	114
Access Security Control	123
Forcing HTTPS Encryption	123
Configuring the Firewall	123
Setting Up User Login Controls	130

Setting Up Role-Based Access Control Rules	134
Setting Up a TLS Certificate	138
Certificate Signing Request	139
Creating a Self-Signed Certificate	141
Installing Existing Key and Certificate Files.....	143
Downloading Key and Certificate Files.....	143
Setting Up External Authentication	144
Gathering the External Authentication Information.....	144
Adding Authentication Servers	146
Sorting the Access Order	150
Testing the Server Connection	150
Editing Authentication Server Settings	151
Deleting Authentication Server Settings.....	151
Disabling External Authentication.....	151
Enabling External and Local Authentication Services	152
Event Rules and Actions.....	153
Components of an Event Rule.....	153
Creating an Event Rule	153
Sample Event Rules	190
A Note about Infinite Loop	191
Modifying an Event Rule.....	192
Modifying an Action	193
Deleting an Event Rule or Action.....	194
A Note about Untriggered Rules.....	194
Viewing Connected Users	195
Monitoring Server Accessibility.....	196
Adding IT Devices for Ping Monitoring.....	196
Editing Ping Monitoring Settings.....	199
Deleting Ping Monitoring Settings	199
Checking Server Monitoring States	200
Managing Event Logging	200
Viewing the Local Event Log	200
Clearing Event Entries.....	201
Viewing the Wireless LAN Diagnostic Log	201
Environmental Sensors and Actuators	202
Identifying Environmental Sensors and Actuators.....	203
Managing Environmental Sensors or Actuators	207
Configuring Environmental Sensors or Actuators	208
Viewing Sensor or Actuator Data	213
Unmanaging Environmental Sensors or Actuators	217
Disabling the Automatic Management Function.....	218
Enabling the Front Panel Actuator Control.....	219
Controlling Actuators	219
Asset Management.....	219
Configuring the Asset Sensor.....	220
Setting Asset Sensor LED Colors.....	221
Configuring a Specific Rack Unit.....	222
Expanding a Blade Extension Strip	223
Displaying the Asset Sensor Information	224
Webcam Management.....	225
Configuring Webcams	225
Configuring Webcam Storage	226

Adjusting Image Properties	227
Viewing Webcam Snapshots or Videos	228
Saving Snapshots.....	229
Sending Snapshots or Videos in an Email or Instant Message	230
Managing the Snapshots Saved to BCM2	231
Firmware Upgrade	232
Updating the BCM2 Firmware	233
Viewing Firmware Update History	234
Full Disaster Recovery	234
Updating the Asset Sensor Firmware.....	235
Network Diagnostics	235
Pinging a Host	235
Tracing the Network Route.....	236
Listing TCP Connections	236
Downloading Diagnostic Information	236
Bulk Configuration.....	237
Saving a BCM2 Configuration	238
Copying the BCM2 Configuration.....	239
Backup and Restore of BCM2 Device Settings	240
Rebooting the BCM2.....	241
Accessing the Help	241
Retrieving Software Packages Information	241
Browsing through the Online Help.....	242

Chapter 5 Using SNMP 244

Enabling SNMP.....	244
Configuring Users for Encrypted SNMP v3	245
Configuring SNMP Notifications	246
SNMPv2c Notifications	247
SNMPv3 Notifications.....	249
SNMP Gets and Sets.....	251
The BCM2 MIB	252
A Note about Enabling Thresholds.....	254

Chapter 6 Using the Command Line Interface 255

About the Interface.....	255
Logging in to CLI.....	256
With HyperTerminal	256
With SSH or Telnet.....	259
With an Analog Modem	260
Different CLI Modes and Prompts	261
Closing a Local Connection.....	261
Help Command	262
Querying Available Parameters for a Command	263
Showing Information	263
Network Configuration	264
Date and Time Settings.....	266

Default Measurement Units	266
Environmental Sensor Information	267
Environmental Sensor Package Information	269
Actuator Information	270
Environmental Sensor Threshold Information	271
Environmental Sensor Default Thresholds	272
USB-Cascading Configuration Information	273
Security Settings.....	273
Existing User Profiles	274
Existing Roles	275
Serial Port Settings	275
Asset Sensor Settings	276
Rack Unit Settings of an Asset Sensor	276
Blade Extension Strip Settings	277
Event Log.....	278
Wireless LAN Diagnostic Log	279
Server Reachability Information	279
Reliability Data.....	280
Reliability Error Log	281
Command History	281
History Buffer Length	281
Examples	281
Clearing Information.....	283
Clearing Event Log	283
Configuring the BCM2 Device and Network	283
Entering Configuration Mode.....	284
Quitting Configuration Mode.....	284
Network Configuration Commands.....	285
Time Configuration Commands.....	309
Checking the Accessibility of NTP Servers	313
Security Configuration Commands.....	314
User Configuration Commands	335
Role Configuration Commands	347
Server Reachability Configuration Commands	351
Serial Port Configuration Commands.....	355
Setting the History Buffer Length.....	355
Multi-Command Syntax	356
Configuring Environmental Sensors' Default Thresholds	357
Example - Default Upper Thresholds for Temperature	358
Environmental Sensor Configuration Commands	359
Changing the Sensor Name	359
Specifying the CC Sensor Type	360
Setting the X Coordinate	360
Setting the Y Coordinate	361
Setting the Z Coordinate.....	361
Changing the Sensor Description.....	362
Using Default Thresholds	362
Setting the Alarmed to Normal Delay for DX-PIR.....	363
Examples	363
Environmental Sensor Threshold Configuration Commands	363
Example 1 - Upper Critical Threshold for a Temperature Sensor	365

Appendix D	Integration	419
<hr/>		
	Power IQ	419
Appendix E	Additional BCM2 Information	420
<hr/>		
	Raritan Training Website	420
	Altitude Correction Factors	420
	Truncated Data in the Web Interface.....	421
	Reserving IP Addresses in Windows DHCP Servers	421
	Ways to Probe Existing User Profiles	423
	EnergyWise and LHX/SHX Not Supported.....	423
Index		425
<hr/>		

Chapter 1 Introduction

In This Chapter

Product Models.....	1
Product Overview - PM Series Power Meters	2
Product Overview - BCM2 Series.....	3

Product Models

BCM2 software applies to both the Power Meter Series modular power meter and branch circuit monitor products (PMM, PMB, and PMC), and the BCM2 power meter product.

Product Overview - PM Series Power Meters

Raritan PM series power meters is a modular power metering solution comprising three components.

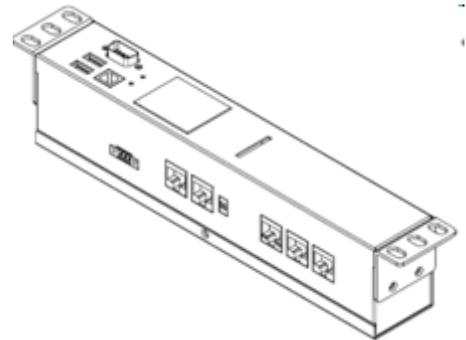
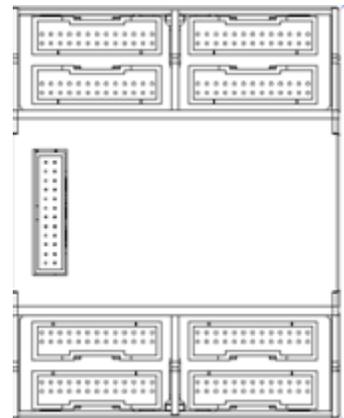
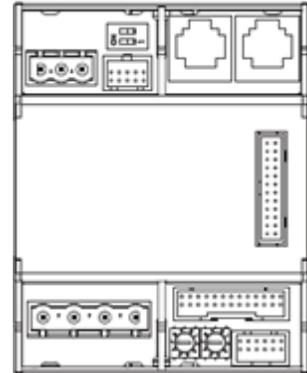
PMM: a 3-phase power meter with neutral and earth current monitoring.

PMB: a 96 channel branch circuit monitor that plugs into PMM. A PMM+PMB monitors a panel board mains and branch circuit.

PMC: power meter controller. One PMC controls up to 70 PMM or 8 PMM+PMB. Interconnection uses standard shielded CAT-5 cable. All modules receive redundant power and continue to function as long as one or more PMM remain powered.

Raritan PM series power meters are designed for ease of use:

- CTs are available in various ratings and contain built-in burden resistors so they can be snapped onto live wires without damage.
- CT orientation is not critical because meter auto-corrects polarity for any CT installed backwards.
- CT connections are made close to branch circuits using multi-conductor wiring harnesses with individual CT wire-pairs labeled and terminated with a keyed connector.



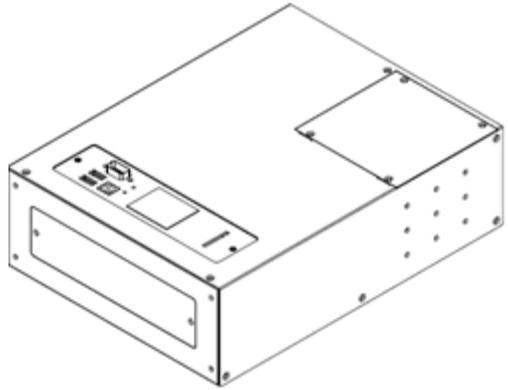
Product Overview - BCM2 Series

Raritan BCM2 is a 96 channel branch circuit monitor.

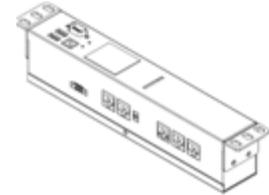
Models available with or without built-in meter controller, with power line cords or field wiring terminals.

One meter controller (built-in or external) interconnects one to eight BCM2. Built-in controller is top or front mountable. External controller rack mounts or attaches to PDU access door.

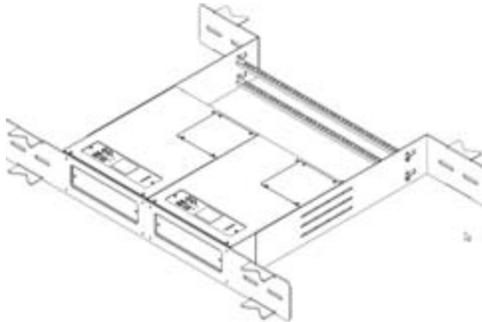
▶ **BCM2_96xx (with built-in controller)**



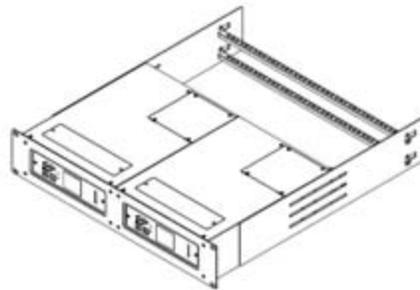
▶ **External meter controller**



Mounting kits are available for subfloor, rack or wall. Floor and rack mount kits hold one or two BCM2 meters.



BCM2_FLOOR_MOUNT_KIT



BCM2_RACK_MOUNT_KIT



BCM2_WALL_MOUNT_KIT

Chapter 2 Installation and Initial Configuration

- This equipment must only be installed and serviced by qualified electrical personnel.
- Read, understand and follow the instructions before installing this product.
- See **Safety Information** (on page iii).

In This Chapter

Hardware Installation.....	4
Login and Configuration	4
Using the BCM2's Display	11

Hardware Installation

Please refer to the Quick Setup Guide for your product. The printed guide is in your product box, or you can download from the BCM2 Support page on Raritan.com

BCM2 Series Branch Circuit Monitor Quick Setup Guide

Power Meter Series Quick Setup Guide

Login and Configuration

Connect your PC directly to the BCM2 to complete the initial configuration.

► **To access the web interface at the rack:**

1. Disable the wireless interface of the PC.
2. Connect a cat 5 cable between the PC and BCM2 network ports.
3. Open a browser. Enter the URL "https://pdu.local". The login page appears.

If the URL does not resolve, use the IP address of the PMC. Retrieve the direct IP address using the LCD display: Menu > Device Information, scroll to the IPV4 settings. Enter the IP address in the web browser: "https://IP address/"

4. Login with the default username and password. Allow 30 seconds for first connection.
 - Username: admin
 - Password: raritan

Configuring Power Meters and Branch Circuit Monitors

You can configure your product with a spreadsheet, or in the product's web interface.

► To configure with a spreadsheet:

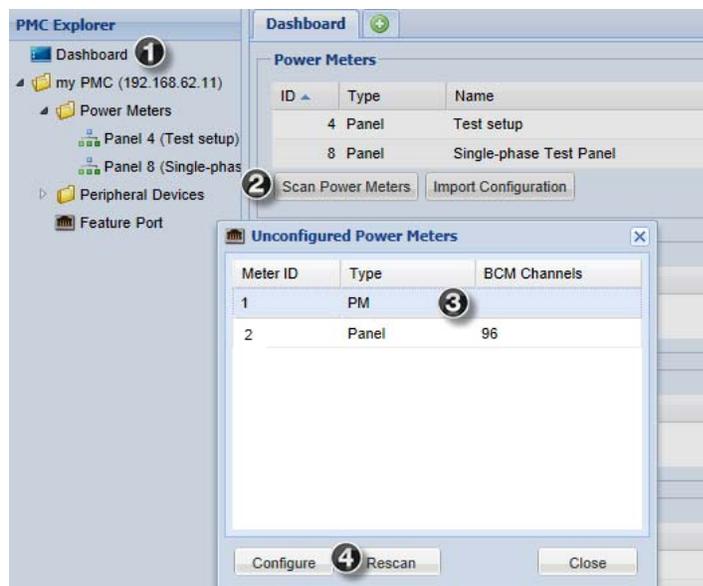
Go to Raritan.com and download the configuration spreadsheet from the BCM2 Support page. Follow the instructions in the spreadsheet.

► To configure with the product web interface:

Make a network connection to the product. See **Login and Configuration** (on page 4). Follow the instructions in this guide, starting with Configure Using the Web Interface.

Scan Power Meters

- 1 Go to the Dashboard.
- 2 Click Scan Power Meters.
Click the power meter or panel in the discovered list.
- 3 Types:
Power Meter: 3-phase
Branch Circuit Monitor: BCM
- 4 Click Configure.



Configure Power Meter

- 1 Enter a name.
 - 2 Select the circuit type:
 - Single Phase
 - Split Phase
 - 3-phase
 - 3 Enter the mains circuit breaker rating.
 - 4 Select the checkbox for each CT installed.
Enter the CT rating. Ratings are marked on the CT.
 - 5 Click OK.
- The configured power meter displays in the dashboard.
- If there are more unconfigured power meters, the scan results stay open.

Configure Power Meter

Settings

Name: PMM-1

Type: 3-Phase

Main Circuit

Circuit Rating (A): 200

Phase CT Present

Phase CT Rating (A): 60

Neutral CT Present

Neutral CT Rating (A): 60

Earth CT Present

Earth CT Rating (A): 60

Modbus

Enable Modbus Access

Modbus Address:

OK Cancel

Configure Panel Mains Circuit

- 1 Enter a name.
- 2 Select the circuit type:
 - Single Phase
 - Split Phase
 - 3-phase

Enter the number of circuit positions in the panel.
- 3 Select the panel layout: one or two columns.
 Select the circuit position numbering style: sequential or odd/even.
- 4 Enter the current rating (circuit breaker rating) of the circuit.
- 5 Select the checkbox for each CT installed.
 Enter the CT rating. Ratings are marked on the CT.
- 6 Click OK.

The screenshot shows the 'Configure Panel' dialog box with the following fields and callouts:

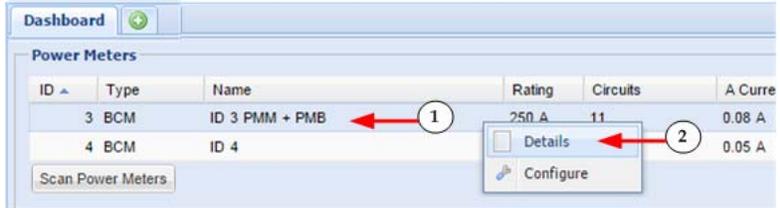
- Settings:**
 - Name: Panel Mains 1 (Callout 1)
 - Type: 3-Phase (Callout 2)
- Panel Layout:**
 - Number of Circuit Positions: 96
 - Panel Layout: Two Columns (Callout 3)
 - Circuit Position Numbering: Odd/Even
- Main Circuit:**
 - Circuit Rating (A): 250 (Callout 4)
 - Phase CT Present
 - Phase CT Rating (A): 60
 - Neutral CT Present (Callout 5)
 - Neutral CT Rating (A): 60
 - Earth CT Present
 - Earth CT Rating (A): 60
- Modbus:**
 - Enable Modbus Access
 - Modbus Address: (empty field)

Buttons: OK (Callout 6), Cancel

The configured branch circuit monitor displays in the dashboard .

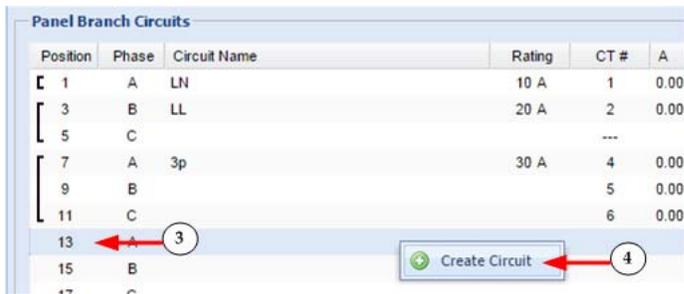
Configure Panel Branch Circuits

- 1 In the dashboard, click the BCM to open the pop-up menu.

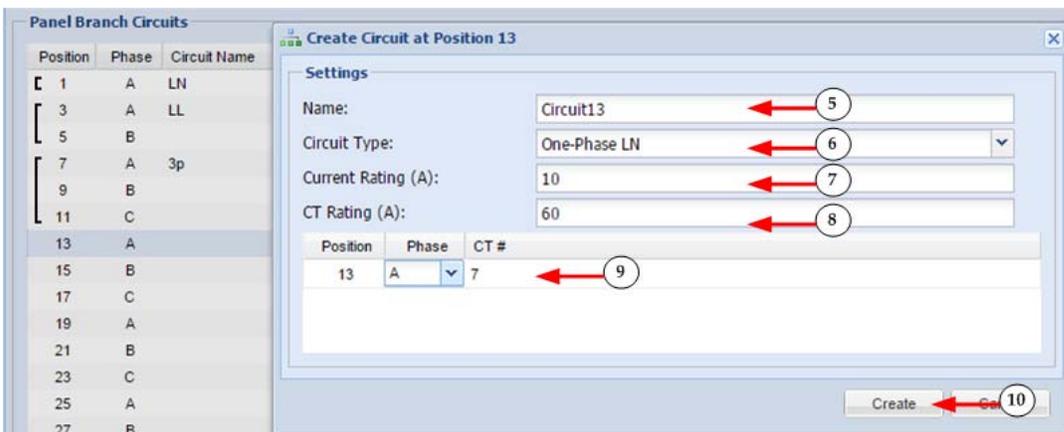


- 2 Click Details. The Panel details open in a new tab.

- 3 In the Panel Branch Circuits section, click the circuit position to open the pop-up menu.



- 4 Click Create Circuit. The Create Circuit dialog opens.



- 5 Enter a name for the circuit.
- 6 Select the circuit type: One-Phase LN, One-Phase LL, One-Phase LLN, or Three-Phase. Circuit type cannot be changed later.

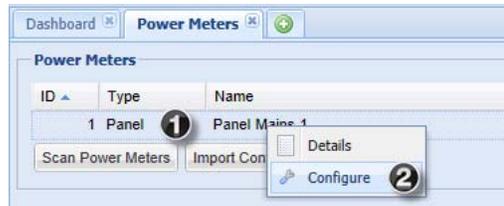
- 7 Enter the current rating of the circuit in Amps.
- 8 Enter the rating of the CT connected at this circuit position in Amps.
- 9 Click the Phase or CT# to edit the automatic labels.
- 10 Click Create.

- 11 Circuits appear in the list with a black bracket around the circuit positions.

Panel Branch Circuits			
Position	Phase	Circuit Name	
[1	A	LN	
[3	A	LL	
[5	B	←	
[7	A	3p	
[9	B		
[11	C		

Configure Thresholds

- 1 In the dashboard, click the power meter or panel to open the pop-up menu.
- 2 Click Configure. A new dialog opens.



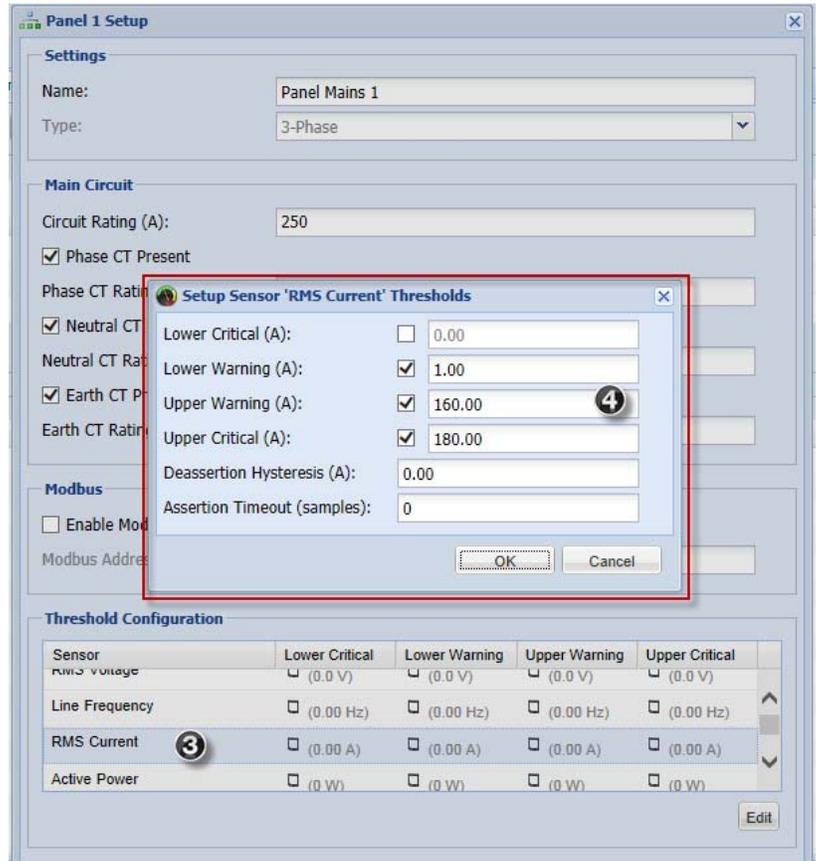
3

Double-click the reading you want to set thresholds for. A new dialog opens on top.

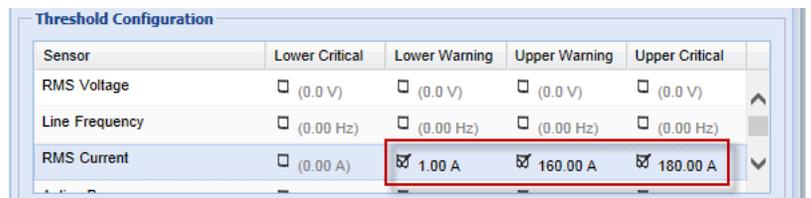
4

Select the checkbox for the level, and enter the threshold current in amps. Click OK.

This example shows RMS Current thresholds set for upper warning and critical levels for the circuit max current rating, and a lower warning set for 1 amp.



Thresholds display in the configuration dialog.



Using the BCM2's Display

▶ Automatic Mode:

The BCM2 has a display with automatic and manual modes. In automatic mode, the display scrolls through readings.



▶ Manual Mode:

In manual mode, you can select readings and settings to view.

Press  or  to view the Main Menu.

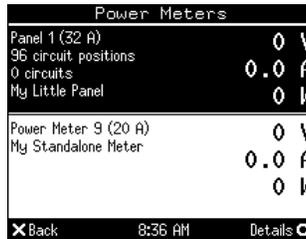


To return to automatic mode, press  once or several times.

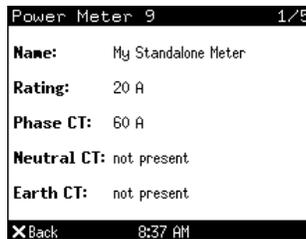
Press   to choose a menu item.

Press  to select.

▶ Power Meters list



▶ Power Meter details



Alerts

The "Alerts" menu command shows a list of the following alerted sensors, including both internal and external sensors.

- Any sensor that enters the warning or critical range if the thresholds have been enabled

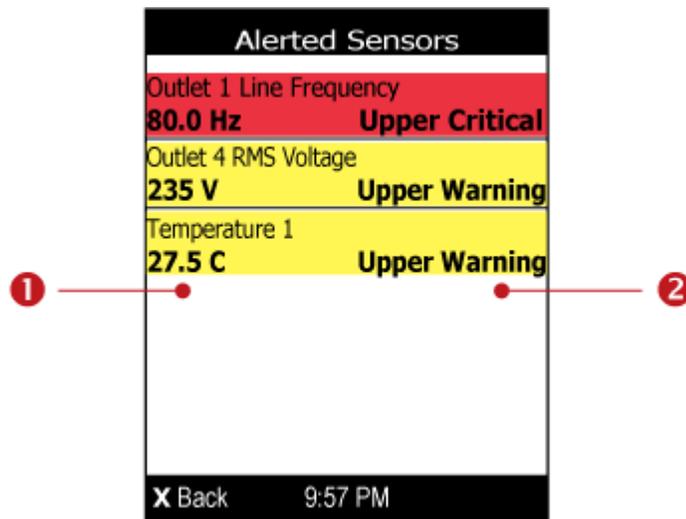
- Discrete (on/off) sensors that enter the alarmed state
- Any tripped circuit breakers or blown fuses

*Tip: The same information is available in the BCM2 web interface's Dashboard. See **Alerted Sensors** (on page 53).*

If there are no alerted sensors, the LCD display shows the message "No alerts."

► **To view alerted sensors:**

1. Press  or  to select "Alerts" in the Main Menu, and press .
2. Alerted sensors are highlighted in either red or yellow. See **The Yellow- or Red-Highlighted Sensors** (on page 50) for color meanings.



Number	Description
1	Sensor names. For a numeric sensor, its reading is displayed right below the sensor name. For a discrete sensor, no reading is displayed.

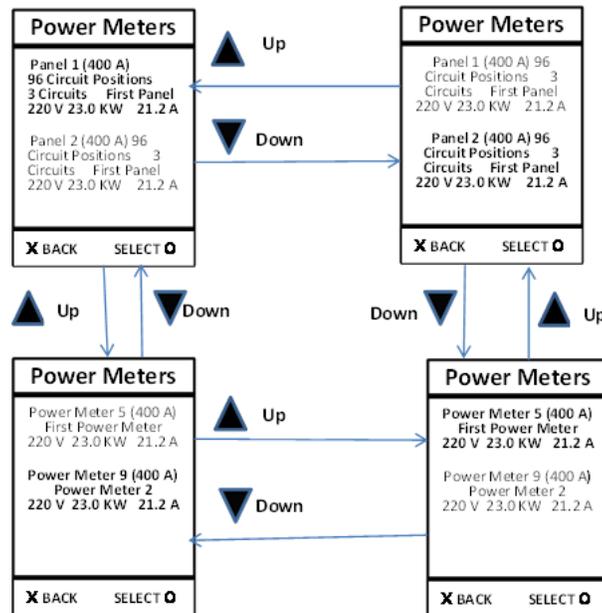
Number	Description
2	<p>Sensor states as listed below. For further information, see States of Managed Sensors (on page 214).</p> <ul style="list-style-type: none"> ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ Open (for overcurrent protectors)

3. Press  or  to view additional pages. When there are multiple pages, page numbers show in the top-right corner of the display.

Power Meters

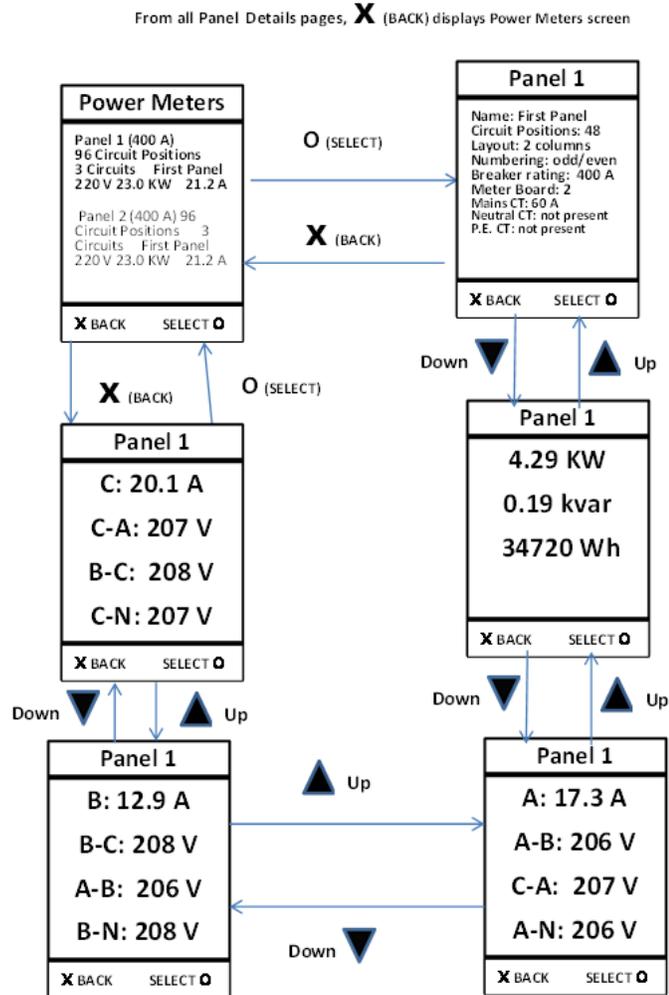
The Power Meters menu option displays information and readings for each power meter. Use the arrow buttons to navigate through all power meters.

From all Power Meters pages, **X** (BACK) displays the Main Menu



Panels

Navigate to a panel from the power meter details and press O (select) to display the panel details and readings.



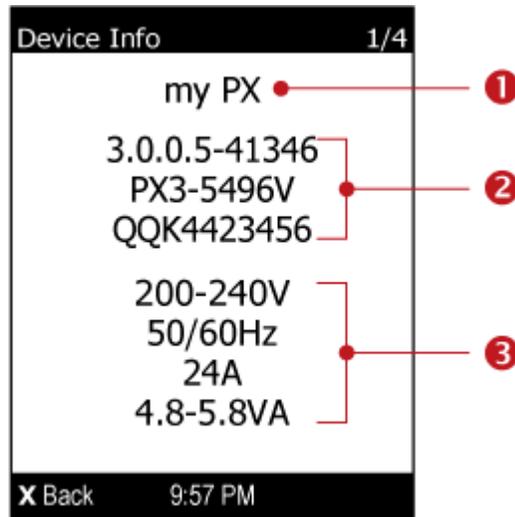
Device Info

The display shows the BCM2 device's information, network and IPv4 settings through various pages. Page numbers are indicated in the top-right corner of the LCD display.

► To show the device information:

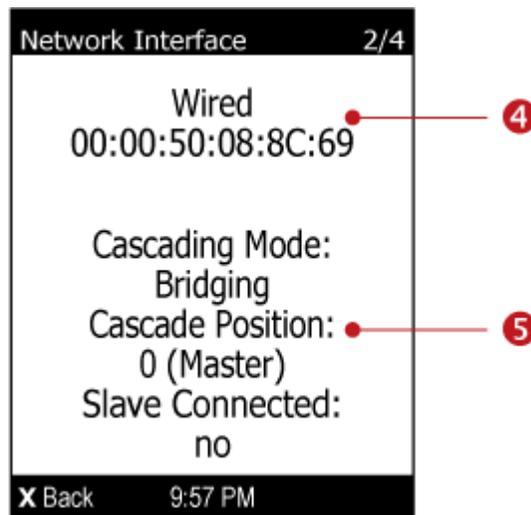
1. Press or to select "Device Info" in the Main Menu, and press .

- The display shows device information similar to the following diagram.



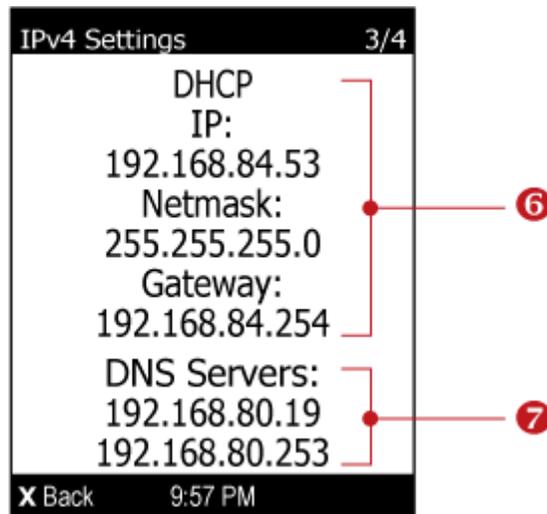
Number	Description
1	The BCM2 device's name.
2	Firmware version, model name and serial number.
3	Device ratings, including rated voltage, frequency, current and power.

- To go to the next page which shows the networking mode and USB-cascading status, press .



Number	Description
4	<p>Networking information, including:</p> <ul style="list-style-type: none"> ▪ Network mode: Wired or Wireless. ▪ MAC address of the BCM2. ▪ If the networking mode is wireless, the following additional information is available: <ul style="list-style-type: none"> - SSID - MAC address of the access point being used
5	<p>USB-cascading status, including:</p> <ul style="list-style-type: none"> ▪ Cascading mode: Bridging or Port Forwarding. See Setting the Cascading Mode (on page 85). ▪ Cascade position: The position information is available only when the BCM2 is in a USB-cascading configuration. The information comprises a number and a noun enclosed in parentheses: <ul style="list-style-type: none"> - The number represents the device's position. For example, 0 represents the master device, 1 represents Slave 1, 2 represents Slave 2, and so on. - The noun in parentheses indicates whether it is a master or slave device. ▪ Slave connected: Indicates whether the presence of a slave device is detected on the USB-A port - <i>yes</i> or <i>no</i>.

4. To go to the next page which shows IPv4 settings, press .

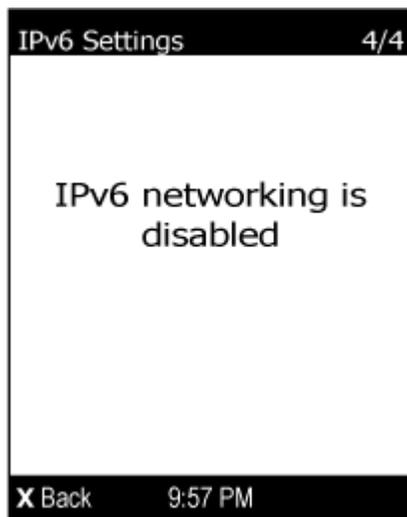


Number	Description
6	IPv4 network information, including: <ul style="list-style-type: none"> ▪ Network configuration: DHCP or Static. Static represents Static IP. ▪ IP address. ▪ Netmask. ▪ Gateway.
7	DNS server addresses, including the primary and secondary ones.

If you do not enable IPv4 settings, a message is displayed to indicate IPv4 is disabled.

5. To show IPv6 settings, press . If IPv6 settings have been enabled, the following IPv6 information is available:
- Network configuration: Automatic or Static.
 - IP address(es).
 - DNS server address(es).

If you do not enable IPv6 settings, the following message is displayed instead.



6. To return to the Main Menu, press .

Peripherals

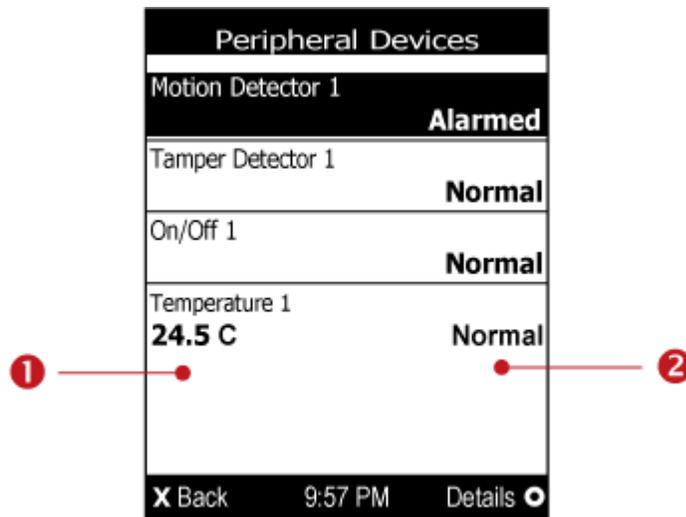
If there are no Raritan environmental sensor packages connected to your BCM2, the LCD display shows the message "No managed devices" for the "Peripherals" menu command.

If any connected sensor is highlighted in red or yellow, that sensor has entered an alarmed, warning or critical state. See **The Yellow- or Red-Highlighted Sensors** (on page 50) for color meanings.

If you have enabled the front panel actuator control function, you can switch on or off a connected actuator using the LCD display. See **Enabling the Front Panel Actuator Control** (on page 219).

► To show environmental sensor or actuator information:

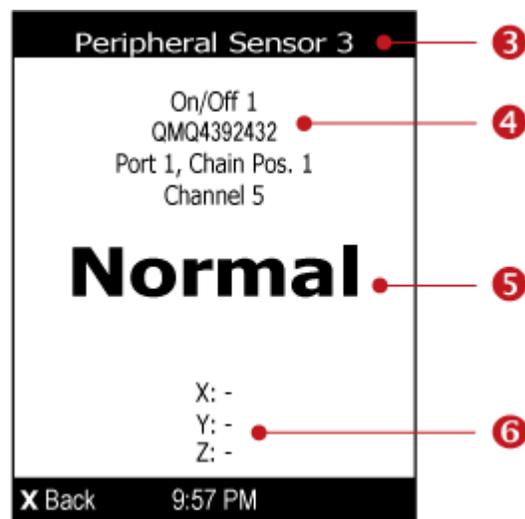
1. Press  or  to select "Peripherals" in the Main Menu, and press .
2. The display shows a list of environmental sensors similar to the following diagram.
 - If the desired sensor or actuator is not visible, press  or  to scroll up or down. Page numbers are indicated in the top-right corner of the LCD display.



Number	Description
1	Sensor or actuator names. For a numeric sensor, its reading is displayed right below the sensor name. For a discrete sensor, no reading is displayed.

Number	Description
2	<p>Sensor or actuator states as listed below. For further information, see States of Managed Sensors (on page 214) and States of Managed Actuators (on page 217).</p> <ul style="list-style-type: none"> ▪ n/a = unavailable ▪ Normal ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ On ▪ Off

3. To view an environmental sensor or actuator's detailed information, press  or  to select that sensor or actuator, and press . A screen similar to the following is shown.

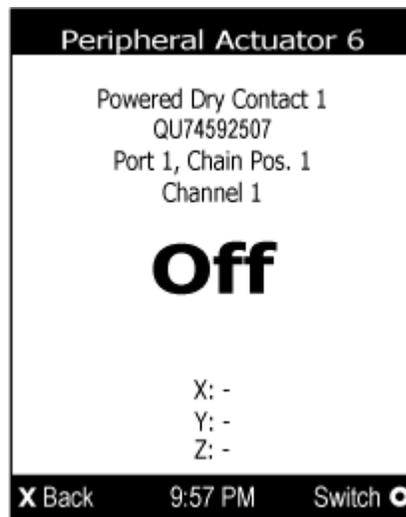


Number	Description
3	<p>The ID number assigned to this sensor or actuator.</p> <ul style="list-style-type: none"> ▪ A sensor is shown as "Peripheral Sensor x," where x is the ID number. ▪ An actuator is shown as "Peripheral Actuator x," where x is the ID number.

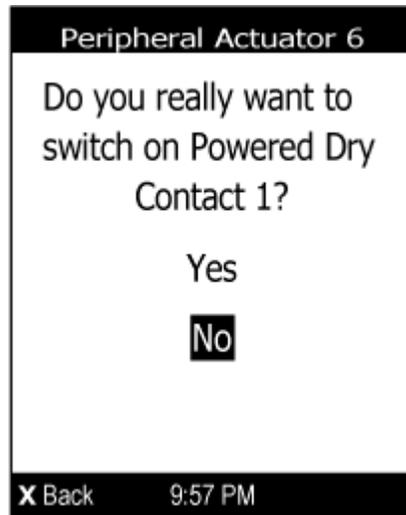
Number	Description
4	<p>Three pieces of sensor or actuator information are listed from top to down.</p> <ul style="list-style-type: none"> ▪ Sensor or actuator name ▪ Serial number ▪ Chain position, which involves the following information: Port <N>: <N> is the number of the sensor port where this sensor or actuator is connected. Chain Pos. <n>: <n> is the sensor or actuator's position in a sensor daisy chain. <hr/> <p><i>Note: Only DX and DPX2 sensor packages provide the chain position information.</i></p> <hr/> <ul style="list-style-type: none"> ▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX-D2C6, its channel number is indicated as "Channel x", where x is a number.
5	<p>Depending on the sensor type, any of the following information is displayed:</p> <ul style="list-style-type: none"> ▪ State of a discrete (on/off) sensor: Normal or Alarmed. ▪ State of an actuator: On or Off. ▪ Reading of a numeric sensor.
6	<p>X, Y, and Z coordinates which you specify for this sensor or actuator. See Configuring Environmental Sensors or Actuators (on page 208).</p>

► **To switch on or off an actuator:**

1. Follow the above steps 1 to 3 to select the actuator.



2. Press  to turn on or off the actuator. A confirmation message similar to the following is shown.



3. Press  or  to select Yes or No, and then press .
4. Verify that the actuator status shown on the LCD display has been changed.

Chapter 3 Connecting External Equipment (Optional)

More features are available if you connect Raritan's or third-party external equipment to your BCM2.

In This Chapter

Connecting Environmental Sensor Packages	22
Connecting Asset Management Sensors	31
Connecting a Logitech Webcam	39
Connecting a GSM Modem	40
Connecting an Analog Modem	41
Connecting an External Beeper	41
Cascading the BCM2 via USB	42
Wireless Network Connection	44

Connecting Environmental Sensor Packages

The BCM2 supports all types of Raritan environmental sensor packages, including DPX, DPX2 and DX sensor packages. For detailed information on each sensor package, refer to the Environmental Sensors Guide or Online Help on Raritan website's **Support page** (<http://www.raritan.com/support/>).

An environmental sensor package may comprise sensors only or a combination of sensors and actuators.

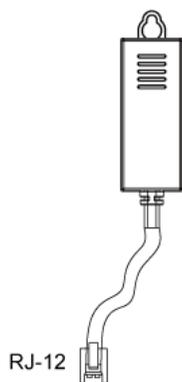
The BCM2 can manage a maximum of 32 sensors and/or actuators. The supported maximum distance is 98 feet (30 m).

For information on connecting different types of sensor packages, see:

- **DPX Sensor Packages** (on page 23)
- **DPX2 Sensor Packages** (on page 26)
- **DX Sensor Packages** (on page 28)

DPX Sensor Packages

Most DPX sensor packages come with a factory-installed sensor cable, whose sensor connector is RJ-12.



The supported maximum distance is 98 feet (30 m). See **Supported Maximum DPX Sensor Distances** (on page 25) for further illustrations.

Warning: For proper operation, wait for 15-30 seconds between each connection operation or each disconnection operation of environmental sensor packages.

► **To directly connect a DPX with a factory-installed sensor cable:**

An RJ-12 to RJ-45 adapter is required to connect a DPX sensor package to the BCM2.

- a. Connect the adapter's RJ-12 connector to the DPX sensor cable.
- b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the BCM2.

► **To directly connect a differential air pressure sensor:**

1. Connect a Raritan-provided phone cable to the IN port of a differential air pressure sensor.
2. Get an RJ-12 to RJ-45 adapter. Connect the adapter's RJ-12 connector to the other end of the phone cable.
3. Connect this adapter's RJ-45 connector to the RJ-45 SENSOR port on the BCM2.

*Note: You can cascade multiple differential air pressure sensors using Raritan-provided phone cables. For details, refer to the Environmental Sensors Guide or Online Help on Raritan website's **Support page** (<http://www.raritan.com/support/>). When cascading sensors, remember that a SENSOR port supports a maximum of 32 sensors.*

Using an Optional DPX-ENVHUB4 Sensor Hub

Optionally, you can connect a Raritan DPX-ENVHUB4 sensor hub to the BCM2. This allows you to connect up to four DPX sensor packages to the BCM2 via the hub.

The DPX-ENVHUB4 sensor hub supports DPX sensor packages only. Do NOT connect DPX2 or DX sensor packages to this hub.

DPX-ENVHUB4 sensor hubs CANNOT be cascaded. You can only connect one hub to each SENSOR port on the BCM2.

► To connect DPX sensor packages via the DPX-ENVHUB4 hub:

1. Connect the DPX-ENVHUB4 sensor hub to the BCM2.
 - a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
 - b. Get an RJ-12 to RJ-45 adapter. Connect this adapter's RJ-12 connector to the other end of the phone cable.
 - c. Connect this adapter's RJ-45 connector to the BCM2's RJ-45 SENSOR port.
2. Connect DPX sensor packages to any of the four OUT ports on the hub.

This diagram illustrates a configuration with a sensor hub connected.

Using an Optional DPX-ENVHUB2 cable

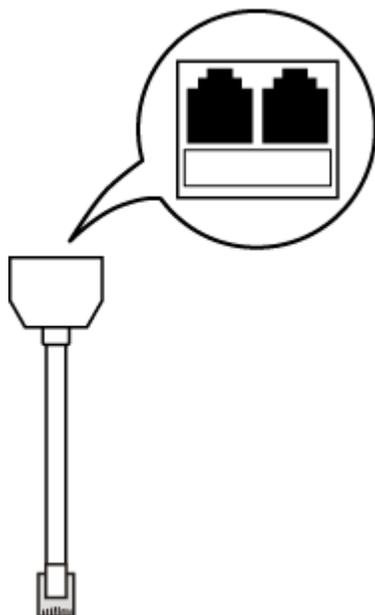
A Raritan *DPX-ENVHUB2* cable doubles the number of connected environmental sensors per SENSOR port.

This cable supports DPX sensor packages only. Do NOT connect DPX2 or DX sensor packages to it.

► To connect DPX sensor packages via the DPX-ENVHUB2 cable:

1. Use an RJ-12 to RJ-45 adapter to connect the DPX-ENVHUB2 cable to the BCM2.
 - a. Connect the adapter's RJ-12 connector to the cable.
 - b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port on the BCM2.

2. The cable has two RJ-12 sensor ports. Connect DPX sensor packages to the cable's sensor ports.



Supported Maximum DPX Sensor Distances

A maximum connection distance of 98' (30 m) is supported when connecting the following DPX sensor packages to the BCM2. This maximum includes the 16' (5 m) sensor cable length:

- DPX-CC2-TR
- DPX-T1
- DPX-T3H1
- DPX-AF1
- DPX-T1DP1

The following configurations were tested when connecting DPX sensor packages to a BCM2 via a Raritan DPX-ENVHUB4 sensor hub:

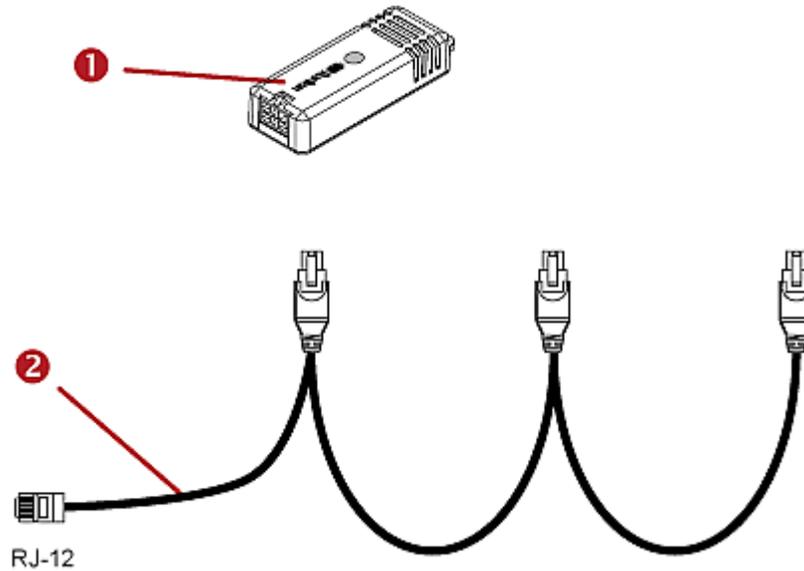
BCM2 → 16' (5 m) cable → 1 sensor hub → 16' (5 m) cable → Up to 4 DPX-T3H1 sensors

- BCM2 → 50' (15 m) cable → 1 sensor hub → 16' (5 m) cable → Up to 4 DPX-T3H1 sensors
- BCM2 → 82' (25 m) cable → 1 sensor hub → 16' (5 m) cable → Up to 4 DPX-T3H1 sensors

DPX2 Sensor Packages

A DPX2 sensor cable is shipped with a DPX2 sensor package. This cable is made up of one RJ-12 connector and one to three head connectors. You have to connect DPX2 sensor packages to the sensor cable.

For more information on DPX2 sensor packages, access the Environmental Sensors Guide or Online Help on Raritan website's **Support page** (<http://www.raritan.com/support/>).



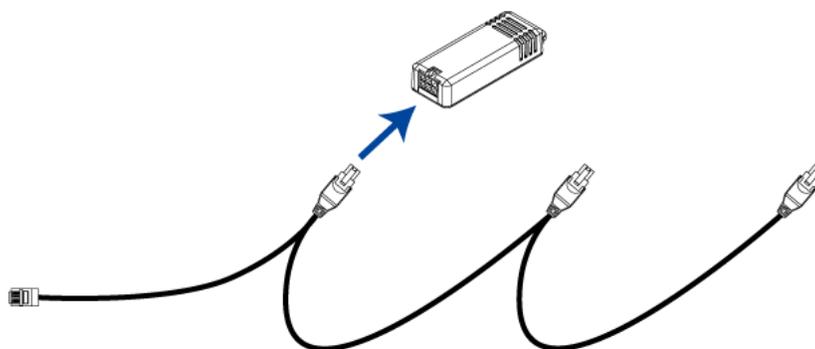
Item	
①	DPX2 sensor package
②	DPX2 sensor cable with one RJ-12 connector and three head connectors

The following procedure illustrates a DPX2 sensor cable with three head connectors. Your sensor cable may have fewer head connectors.

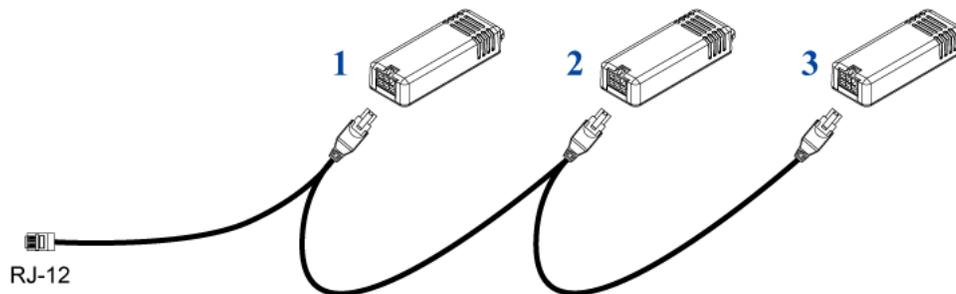
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor package with a DPX2 sensor package.

► **To connect DPX2 sensor packages to the BCM2:**

1. Connect a DPX2 sensor package to the first head connector of the DPX2 sensor cable.



2. Connect remaining DPX2 sensor packages to the second and then the third head connector.



Tip: If the number of sensors you are connecting is less than the number of head connectors on your sensor cable, connect them to the first one or first two head connectors to ensure that there are NO free head connectors prior to the final DPX2 sensor package attached.

3. Use an RJ-12 to RJ-45 adapter to connect a DPX2 sensor package to the BCM2.
 - a. Connect the adapter's RJ-12 connector to the DPX2 sensor cable.

- b. Connect the adapter's RJ-45 connector to the RJ-45 SENSOR port of the BCM2.

OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See **Connecting a DPX2 Sensor Package to DX** (on page 30).

DX Sensor Packages

Most DX sensor packages contain terminals for connecting detectors or actuators. For information on connecting actuators or detectors to DX terminals, refer to the Environmental Sensors Guide or Online Help on Raritan website's **Support page** (<http://www.raritan.com/support/>).

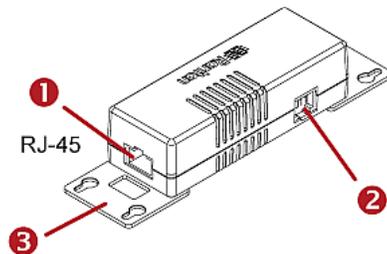
You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the BCM2 only supports a maximum of 32 sensors and/or actuators.

If there are more than 32 sensors and/or actuators connected, every sensor and/or actuator after the 32nd one is NOT managed by the BCM2.

For example, if you cascade 12 DX packages, and each package contains 3 functions (a function is a sensor or actuator), the BCM2 does NOT manage the last 4 functions because the total 36 ($12 \times 3 = 36$) exceeds 32 by 4.

*Tip: To manage the last 4 functions, you can release 4 sensors or actuators that have been under management, and then manually bring the last 4 functions into management. See **Unmanaging Environmental Sensors or Actuators** (on page 217) and **Managing Environmental Sensors or Actuators** (on page 207).*



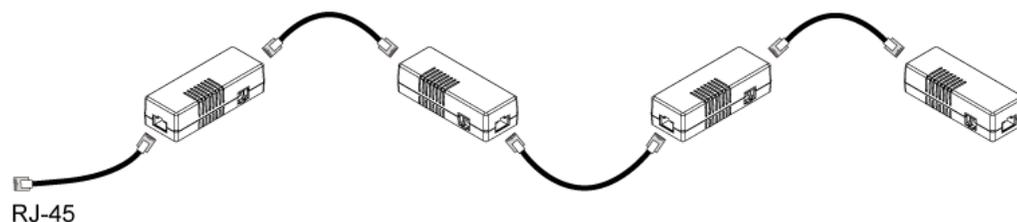
Numbers	Components
①	RJ-45 ports, each of which is located on either end of a DX sensor package.
②	RJ-12 port, which is reserved for future use and now blocked.
③	Removable rackmount brackets.

► **Connect DX sensor packages to the BCM2:**

1. Connect a standard network patch cable (CAT5e or higher) to either RJ-45 port on a DX sensor package.
2. If you want to cascade DX packages, get an additional standard network patch cable (CAT5e or higher) and then:
 - a. Plug one end of the cable into the remaining RJ-45 port on the prior DX package.
 - b. Plug the other end into either RJ-45 port on an additional DX package.

Repeat the same steps to cascade more DX packages.

Exception: You CANNOT cascade DX-PD2C5 sensor packages. A BCM2 device supports only one DX-PD2C5.



3. Connect the first DX sensor package to the BCM2 by plugging its cable's connector into the RJ-45 SENSOR port of the BCM2.
4. If needed, connect a DPX2 sensor package to the end of the DX chain. See **Connecting a DPX2 Sensor Package to DX** (on page 30).

Warning: The BCM2 does NOT support simultaneous connection of both DX-PD2C5 and asset management sensor(s) so do NOT connect both of them to the BCM2 device.

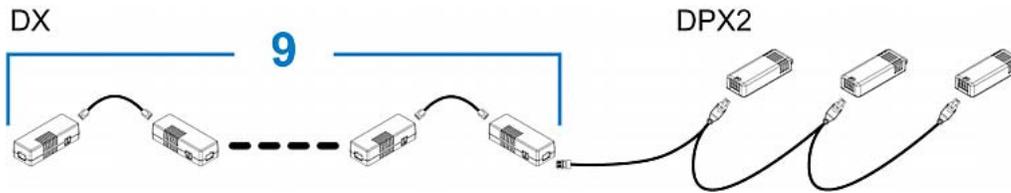
Connecting a DPX2 Sensor Package to DX

You can connect only one DPX2 sensor package to the "end" of a DX sensor chain. Simply plug the RJ-12 connector of the DPX2 sensor cable into the RJ-45 port of the final DX in the chain.

The maximum number of DX sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

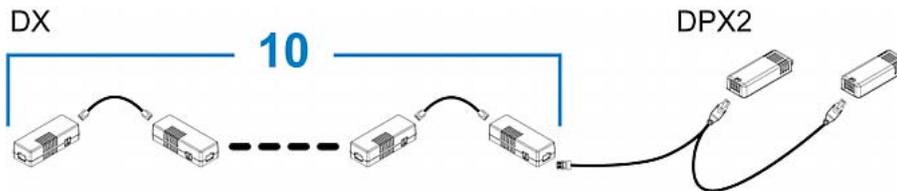
▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

A maximum of nine DX sensor packages can be cascaded because $12-3=9$.



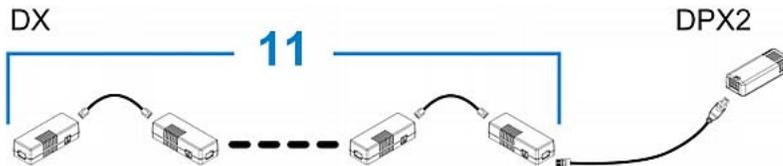
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

A maximum of ten DX sensor packages can be cascaded because $12-2=10$.



▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DX sensor packages can be cascaded because $12-1=11$.



Connecting Asset Management Sensors

Note that only the PMC models of the BCM2 series have the FEATURE port. Therefore, only PMC models support the asset management feature.

You can remotely track the locations of up to 64 IT devices in the rack by connecting an asset management sensor (asset sensor) to the BCM2 after IT devices are tagged electronically.

To use the asset management feature, you need the following items:

- *Raritan asset sensors*: An asset sensor transmits the asset management tag's ID and positioning information to the BCM2.
- *Raritan asset tags*: An asset tag is adhered to an IT device. The asset tag uses an electronic ID to identify and locate the IT device.

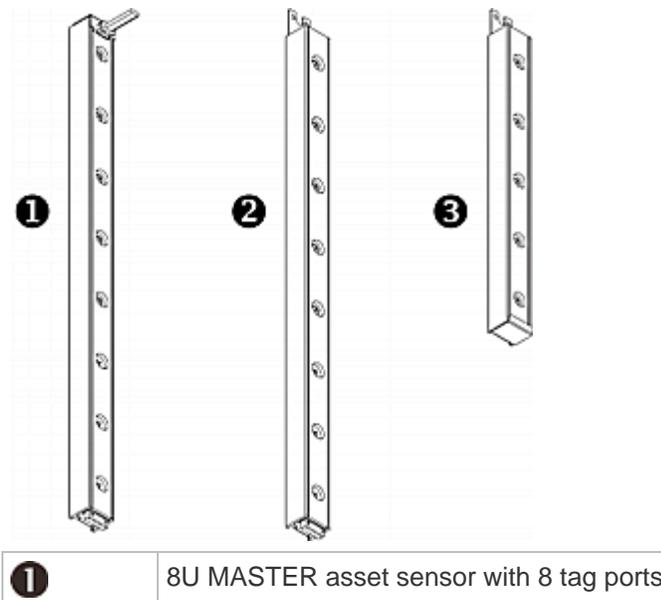
Combining Regular Asset Sensors

Each tag port on the regular asset sensor corresponds to a rack unit and can be used to locate IT devices in a specific rack (or cabinet).

For each rack, you can attach asset sensors up to 64U long, consisting of one MASTER and multiple SLAVE asset sensors.

The difference between the master and slave asset sensors is that the master asset sensor has an RJ-45 connector while the slave does not.

The following diagram illustrates some asset sensors. Note that Raritan provides more types of asset sensors than the diagram.

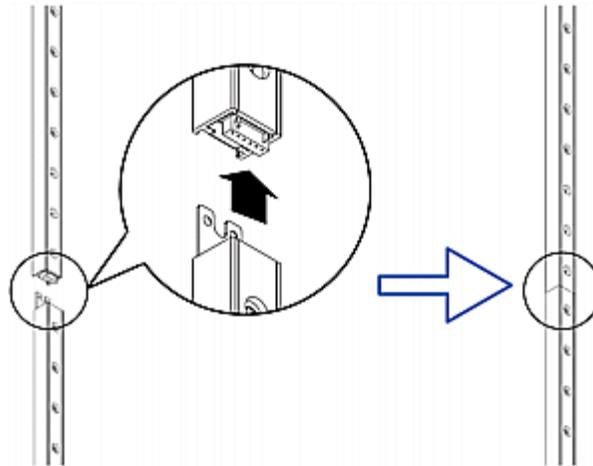


2	8U SLAVE asset sensor with 8 tag ports
3	5U "ending" SLAVE asset sensor with 5 tag ports

Note: Unlike general slave asset sensors, which have one DIN connector respectively on either end, the ending slave asset sensor has one DIN connector on only one end. An ending asset sensor is installed at the end of the asset sensor assembly.

► **To assemble asset sensors:**

1. Connect a MASTER asset sensor to an 8U SLAVE asset sensor.
 - Plug the white male DIN connector of the slave asset sensor into the white female DIN connector of the master asset sensor.
 - Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. Screw up the U-shaped sheet metal to reinforce the connection.



2. Connect another 8U slave asset sensor to the one being attached to the master asset sensor in the same manner as Step 1.
3. Repeat the above step to connect more slave asset sensors. The length of the asset sensor assembly can be up to 64U.
 - The final asset sensor can be 8U or 5U, depending on the actual height of your rack.
 - Connect the "ending" asset sensor as the final one in the assembly.
4. Vertically attach the asset sensor assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit.

- The asset sensors are automatically attracted to the rack because of magnetic stripes on the back.

Note: The asset sensor is implemented with a tilt sensor so it can be mounted upside down.

Connecting Regular Asset Sensors to the BCM2

Note that only the PMC models of the BCM2 series have the FEATURE port.

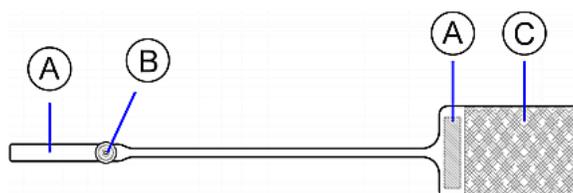
The cabling distance between an asset sensor assembly and the BCM2 can be up to 10 meters.

You need both asset sensors and asset tags for tracking IT devices.

Asset tags provide an ID number for each IT device. The asset tags are adhered to an IT device at one end and plugged in to an asset sensor at the other.

The asset sensor is connected to the BCM2, and the asset tag transmits the ID and positioning information to the asset sensor.

The following diagram illustrates an asset tag.



A	Barcode (ID number), which is available on either end of the asset tag
B	Tag connector
C	Adhesive area with the tape

Note: The barcode of each asset tag is unique and is displayed in the BCM2 device's web interface for identification.

► To connect regular asset sensors to the BCM2 device:

- Affix the adhesive end of an asset tag to each IT device through the tag's tape.
- Plug the connector of each asset tag into the corresponding tag port on the asset sensor.
- Connect the asset sensor assembly to the BCM2 device, using a network patch cable (CAT5e or higher).

- a. Connect one end of the cable to the RJ-45 connector on the MASTER asset sensor.
- b. Connect the other end of the cable to the FEATURE port on the BCM2 device.

The BCM2 device supplies power to the connected asset sensor assembly. All LEDs on the asset sensor assembly may cycle through different colors during the power-on process if the asset sensor's firmware is being upgraded by the BCM2 device. After the power-on or firmware upgrade process completes, the LEDs show solid colors. Note that the LED color of the tag ports with asset tags connected will be different from the LED color of the tag ports without asset tags connected.

*Note: The BCM2 cannot detect how many rack units the connected asset sensor(s) has. You must provide the information to it manually. See **Configuring the Asset Sensor** (on page 220).*

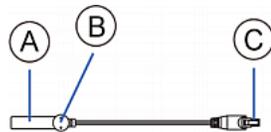
Connecting Blade Extension Strips

For blade servers, which are contained in a single chassis, you can use a blade extension strip to track individual blade servers.

Raritan's blade extension strip functions similar to a Raritan asset sensor but requires a tag connector cable for connecting it to a tag port on the regular or composite asset sensor. A blade extension strip contains 4 to 16 tag ports.

The following diagrams illustrate a tag connector cable and a blade extension strip with 16 tag ports.

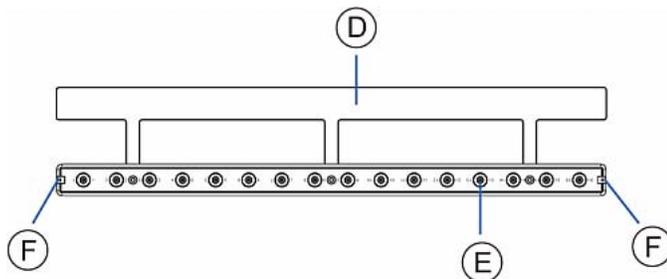
Tag connector cable



A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

Note: A tag connector cable has a unique barcode, which is displayed in the BCM2 device's web interface for identifying each blade extension strip where it is connected.

Blade extension strip with 16 tag ports

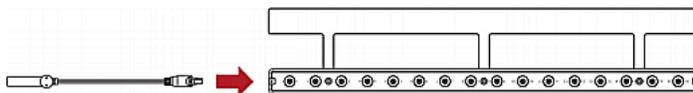


D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

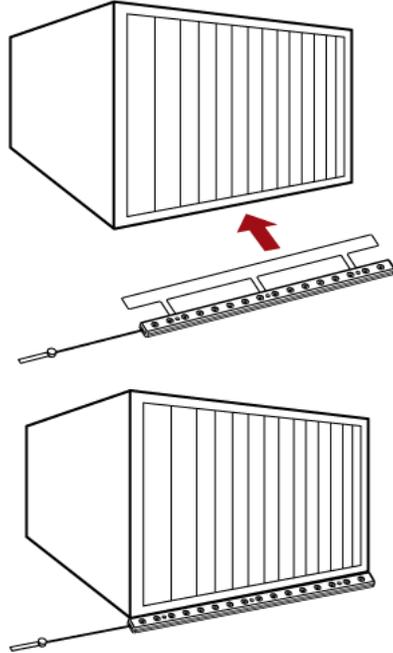
Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the BCM2 device's web interface.

► **To install a blade extension strip:**

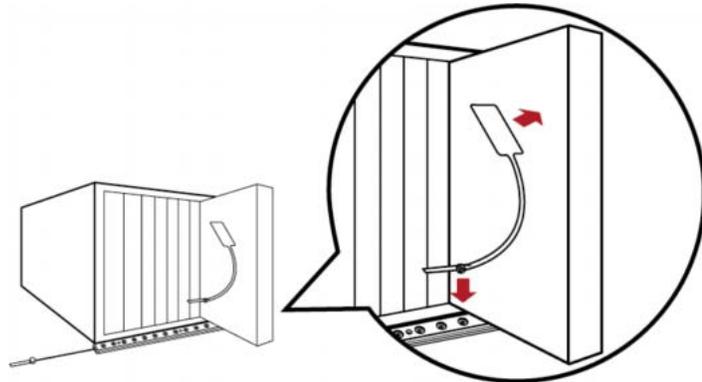
1. Connect the tag connector cable to the blade extension strip.
 - Plug the cable's connector into the socket at either end of the blade extension strip.



2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.

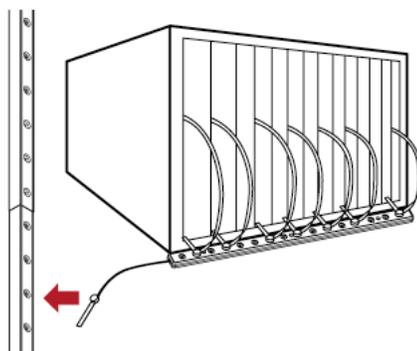


3. Connect one end of an asset tag to a blade server and the other end to the blade extension strip.
 - a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.
 - b. Plug the tag connector of the asset tag into a tag port on the blade extension strip.



4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

5. Plug the tag connector of the blade extension strip into the closest tag port of the regular or composite asset sensor on the rack.



6. Repeat the above steps to connect additional blade extension strips. Up to 128 asset tags on blade extension strips are supported per FEATURE port.

Note: If you need to temporarily disconnect the blade extension strip from the asset sensor, wait at least 1 second before re-connecting it back, or the BCM2 device may not detect it.

Connecting Composite Asset Sensors to the BCM2

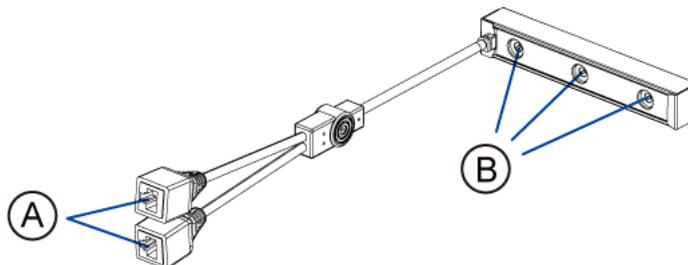
A composite asset sensor is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset sensor that functions the same as regular MASTER asset sensors except for the following differences:

- It has two RJ-45 connectors.
- Multiple composite asset sensors can be daisy chained.
- A composite asset sensor contains less tag ports than regular asset sensors.

For example, AMS-M2-Z contains two tag ports and AMS-M3-Z contains three tag ports only.

The composite asset sensor is especially useful for tracking large devices such as SAN boxes in the cabinet.

The following diagram illustrates AMS-M3-Z.



A	Two RJ-45 connectors
B	Tag ports

► **To connect composite asset sensors to the BCM2 device:**

1. Connect a composite asset sensor to the BCM2 device via a standard network patch cable (CAT5e or higher).
 - a. Connect one end of the cable to the RJ-45 port labeled "Input" on the composite asset sensor.
 - b. Connect the other end of the cable to the FEATURE port on the BCM2 device.
2. Affix an asset tag to the IT device. Then connect this asset tag to the composite asset sensor by plugging the tag connector into the tag port on the composite asset sensor. For details, see **Connecting Regular Asset Sensors to the BCM2** (on page 33).
3. If necessary, daisy chain *the same* type of composite asset sensors to track more IT devices.
 - a. Get a standard network patch cable that is within 2 meters.
 - b. Connect one end of the network cable to the RJ-45 connector labeled "Output" on the previous composite asset sensor.
 - c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on the subsequent composite asset sensor.
 - d. Repeat the above steps to connect more composite asset sensors. See **Daisy-Chain Limitations of Composite Asset Sensors** (on page 38) for the maximum number of composite asset sensors supported per chain.

It is highly recommended using the cable ties to help hold the weight of all connecting cables.

Daisy-Chain Limitations of Composite Asset Sensors

There are some limitations when daisy chaining composite asset sensors "AMS-Mx-Z," where x is a number.

- The maximum cable length between composite asset sensors is 2 meters, but the total cable length cannot exceed 10 meters.
- The maximum number of composite asset sensors that can be daisy chained vary according to the Raritan device.

Raritan devices	Maximum sensors per chain
EMX2-111, PX2 PDUs, BCM1 (NOT BCM2)	Up to 4 composite asset sensors are supported.
EMX2-888, PX3 PDUs, PX3TS transfer switches PMC	Up to 6 composite asset sensors are supported.

Important: Do NOT mix different types of composite asset sensors in a chain. For example, all in the chain are AMS-M2-Z or all are AMS-M3-Z.

Connecting a Logitech Webcam

Connect webcams to BCM2 in order to view videos or snapshots of the webcam's surrounding area.

The following UVC-compliant webcams are supported:

- Logitech® Webcam® Pro 9000, Model 960-000048
- Logitech QuickCam Deluxe for Notebooks, Model 960-000043
- Logitech QuickCam Communicate MP, Model 960-000240
- Logitech C200, C210, C270 and C920

Other UVC-compliant webcams may work. However, Raritan has neither tested them nor claimed that they will work properly. More information about the scores of UVC-compliant webcams can be found at <http://www.ideasonboard.org/uvc> (<http://www.ideasonboard.org/uvc>).

The BCM2 supports up to two webcams. After connecting a webcam, you can retrieve visual information from anywhere through the BCM2 web interface. If your webcam supports audio, audio is available with videos.

For more information on the Logitech webcam, see the user documentation accompanying it.

► **To connect a webcam:**

1. Connect the webcam to the USB-A port on the BCM2 device. The BCM2 automatically detects the webcam.
2. Position the webcam properly.

Important: If a USB hub is used to connect the webcam, make sure it is a

"powered" hub.

Snapshots or videos captured by the webcam are immediately displayed in the BCM2 web interface after the connection is complete. See **Viewing Webcam Snapshots or Videos** (on page 228).

Connecting a GSM Modem

A Cinterion® MC52iT or MC55iT GSM modem can be connected to the BCM2 in order to send SMS messages containing event information. See **Creating Actions** (on page 154) for more information on SMS messages.

Note: BCM2 cannot receive SMS messages.

► **To connect the GSM modem:**

1. Connect the GSM modem to the serial port labeled CONSOLE / MODEM on the BCM2.
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.
3. Configure the GSM modem settings in BCM2.
 - a. Click Device Settings > Serial Port Settings. The Serial Port Configuration dialog opens.
 - b. If needed, enter the GSM modem SIM PIN.

Connecting an Analog Modem

The BCM2 supports remote dial-in communications to access the CLI through an analog modem. This dial-in feature provides an additional alternative to access the BCM2 when the LAN access is not available. To dial in to the BCM2, the remote computer must have a modem connected and dial the correct phone number.

Below are the analog modems that the BCM2 supports for sure:

- NETCOMM IG6000 Industrial Grade SmartModem
- US Robotics 56K modem

The BCM2 may also support other analog modems which Raritan did not test.

Note that the BCM2 does NOT support dial-out or dial-back operations via the modem.

► **To connect an analog modem:**

1. Plug a telephone cord into the phone jack of the supported modem.
2. Plug the modem's RS-232 cable into the serial port labeled CONSOLE / MODEM on the BCM2.

You need to enable the modem dial-in support to take advantage of this feature, see **Configuring the Serial Port** (on page 84).

Connecting an External Beeper

Note that only the PMC models of the BCM2 series have the FEATURE port. Therefore, only PMC models support the external beeper feature.

The BCM2 supports the use of an external beeper for audio alarms.

External beepers that are supported include but may not be limited to the following:

- Mallory Sonalert MODEL SNP2R

After having an external beeper connected, you can create event rules for the BCM2 to switch on or off the external beeper when specific events occur. See **Creating an Event Rule** (on page 153).

► **To connect an external beeper:**

1. Connect a standard network patch cable to the FEATURE port of the BCM2.
2. Plug the other end of the cable into the external beeper's RJ-45 socket.

The beeper can be located at a distance up to 330 feet (100 m) away from the BCM2.

Cascading the BCM2 via USB

You can use USB cables to cascade up to eight Raritan devices. All devices in the USB-cascading chain share the Ethernet connectivity. Different Raritan models can be cascaded as long as they are running an appropriate firmware.

The first device in the chain is the master device and all the other are slave devices.

All devices in the chain are accessible over the network, with the bridging or port-forwarding cascading mode activated on the master device. See **Setting the Cascading Mode** (on page 85).

Only the master device is connected to the LAN. The LAN connection method varies based on the cascading mode.

- The bridging mode supports the *wired* networking only.
- The port forwarding mode supports both the *wired* and *wireless* networking.

For more information on the USB-cascading configuration, see the *USB-Cascading Solution Guide*, which is available from Raritan website's **Support page** (<http://www.raritan.com/support/>).

► To cascade the BCM2 devices via USB:

1. Select one of the devices as the master device.
 - When the port forwarding mode over wireless LAN is intended, the master device must be a Raritan product with two USB-A ports, such as BCM2, PX3, EMX2-888 or PX3TS.
2. Connect the master device to the LAN via:
 - A standard network patch cable (CAT5e or higher) if the bridging mode is intended.
 - A standard network patch cable or a Raritan USB WIFI wireless LAN adapter if the port forwarding mode is intended.

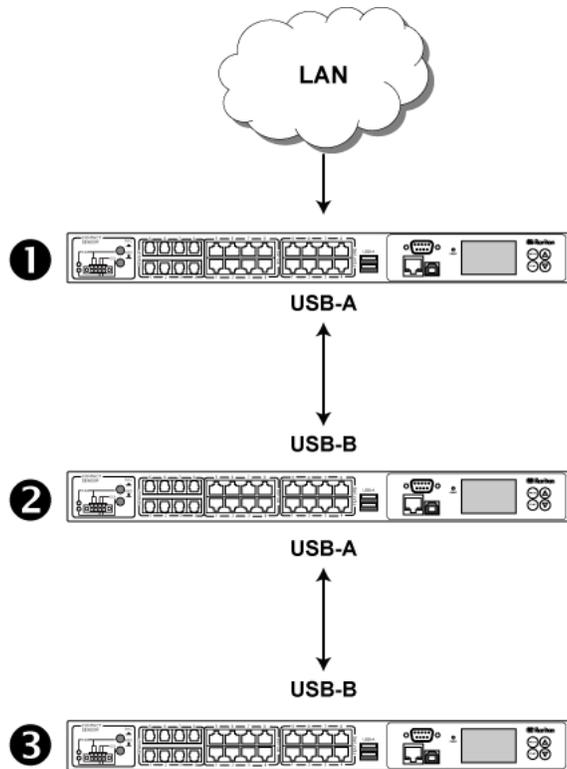
For information on the Raritan USB WIFI adapter, see **USB Wireless LAN Adapters** (on page 44).
3. Connect the USB-A port of the master device to the USB-B port of an additional BCM2 via a USB cable. This additional device is Slave 1.
4. Connect Slave 1's USB-A port to the USB-B port of an additional BCM2 via a USB cable. The second additional device is Slave 2.

5. Repeat the same step to connect more slave devices. You may connect up to 7 slave devices.

Do NOT connect any slave device to the LAN. That is, there is no connection of a standard network cable or USB wireless LAN adapter to the slave devices.

6. Log in to the master device to configure the cascading mode. See **Setting the Cascading Mode** (on page 85) or **Configuring the Cascading Mode** (on page 367).
7. Configure the master and/or each slave device's networking settings.
 - Bridging mode: You need to configure each cascaded device's network settings respectively.
 - Port forwarding mode: Only the mater device's network settings must be configured.

Note: The master/slave devices shown in the following diagram may not look the same as BCM2, but the USB-cascading connection method is the same.



Number	Device role
1	Master device
2	Slave 1

Number	Device role
3	Slave 2

Note: To remotely identify the master and slave devices and their positions in the USB-cascading configuration, see **Identifying Cascaded Devices** (on page 56).

Tip: The USB-cascading configuration can be a combination of diverse Raritan products that support the USB-cascading feature, including PX2, PX3, PX3TS, EMX and BCM. See the USB-Cascading Solution Guide on Raritan website's **Support page** (<http://www.raritan.com/support/>).

Wireless Network Connection

If intended, you can connect your BCM2 to a wireless network instead of a wired network.

► To make a wireless connection:

Do one of the following:

- Plug a supported USB wireless LAN adapter into the USB-A port on your BCM2.
- Connect a USB docking station to the USB-A port on the BCM2. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the docking station.

See **USB Wireless LAN Adapters** (on page 44) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The BCM2 supports the following USB Wi-Fi LAN adapters.

Wi-Fi LAN adapters	Supported 802.11 protocols
Proxim Orinoco 8494	A/B/G
Zyxel NWD271N	B/G
Edimax EW-7722UnD	A/B/G/N
TP-Link TL-WDN3200 v1	A/B/G/N
Raritan USB WIFI	A/B/G/N

Note: To use the Edimax EW-7722UnD or Raritan USB WIFI wireless LAN adapter to connect to an 802.11n wireless network, the handshake timeout setting must be changed to 500 or greater, or the wireless connection will fail.

Supported Wireless LAN Configuration

If wireless networking is preferred, ensure that the wireless LAN configuration of your BCM2 matches the access point. The following is the wireless LAN configuration that the BCM2 supports.

- Network type: 802.11 A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the BCM2. See *USB Wireless LAN Adapters* (on page 44).

Chapter 4 Using the Web Interface

Use the web interface of the BCM2 for configuration and administration.

The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

▶ **Default login:**

- Username: admin
- Password: raritan
- You are prompted to change the defaults at your first login.

▶ **To login to the web interface:**

1. In a supported browser, go to the IP address of the PMC (BCM2).
2. Login and accept security warnings.

In This Chapter

Supported Web Browsers	47
Changing Your Password	47
Introduction to the Web Interface.....	48
Viewing the Dashboard.....	52
Device Management	54
User Management.....	95
Setting Up Roles	101
Meter, Panel, and Branch Circuit Monitoring and Management.....	104
Access Security Control.....	123
Setting Up a TLS Certificate	138
Setting Up External Authentication	144
Event Rules and Actions	153
Viewing Connected Users.....	195
Monitoring Server Accessibility	196
Managing Event Logging	200
Environmental Sensors and Actuators	202
Asset Management	219
Webcam Management	225
Firmware Upgrade	232
Network Diagnostics	235
Downloading Diagnostic Information	236
Bulk Configuration.....	237
Backup and Restore of BCM2 Device Settings	240
Rebooting the BCM2.....	241
Accessing the Help	241

Supported Web Browsers

- Internet Explorer® 8, 9, 10 and 11
- Firefox® 25 and later
- Safari® 5.x (MacOS Lion)
- Google® Chrome® 32 and later
- Android 4.2 and later
- IOS 7.0
- Windows Edge

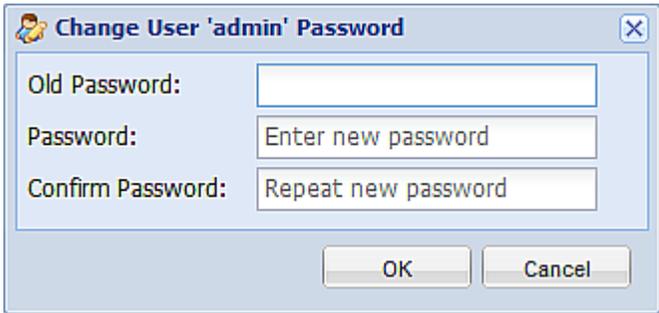
Changing Your Password

You must have the Change Own Password permission to change your own password. See **Setting Up Roles** (on page 101).

You must have Administrator Privileges to change other users' passwords. See **Modifying a User Profile** (on page 99).

► **To change your password:**

- Choose User Management > Change Password. The Change User Password dialog appears.
- Passwords are case sensitive.
- Password length: 4 to 64 characters.



The screenshot shows a dialog box titled "Change User 'admin' Password". It contains three input fields: "Old Password:", "Password:", and "Confirm Password:". The "Password:" field has the placeholder text "Enter new password" and the "Confirm Password:" field has the placeholder text "Repeat new password". At the bottom of the dialog are "OK" and "Cancel" buttons.

Introduction to the Web Interface

The screenshot displays the Raritan PMC web interface. At the top, there is a navigation bar with menus (1) and a logout button (5). On the left, a sidebar (2) lists various power meters. The main content area (4) shows the configuration for Power Meter 7, including a table of sensor data. The status bar (3) at the bottom provides user information and the current time.

Type	Total		Phase A		Phase B	
	Value	State	Value	State	Value	State
RMS Voltage (L-L)	0 V	normal	0 V	normal	0 V	normal
RMS Voltage (L-N)	0 V	normal	0 V	normal	0 V	normal
Line Frequency	0.0 Hz	normal				
RMS Current	0.0 A	normal	0.0 A	normal	0.0 A	normal
Phase Angle			0.0 °	normal	0.0 °	normal
Active Power	0 W	normal	0 W	normal	0 W	normal
Reactive Power	0 var	normal	0 var	normal	0 var	normal
Apparent Power	0 VA	normal	0 VA	normal	0 VA	normal
Power Factor			1.00	normal	1.00	normal
Displacement Po...			1.00	normal	1.00	normal
Active Energy	0 Wh	normal	0 Wh	normal	0 Wh	normal
Neutral Current		unavailable				
Earth Current		unavailable				

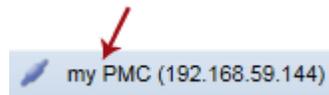
- ① Menus
- ② PMC Explorer pane
- ③ Status bar
- ④ Open power meter tabs and Add a Page icon
- ⑤ Logout and Help

Status Bar

The status bar shows five pieces of information from left to right.

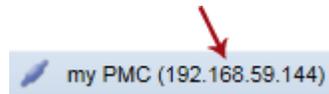
- **Device name:**

This is the name assigned to the BCM2 device. The default is "my PMC." See **Naming the BCM2** (on page 59).



- **IP address:**

The numbers enclosed in parentheses is the IP address assigned to the BCM2 device. See **Modifying Network Settings** (on page 63).



Tip: The presence of the device name and IP address in the status bar indicates the connection to the BCM2 device. If the connection is lost, it shows "  disconnected " instead.

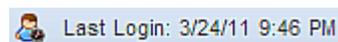
- **Login name:**

This is the user name you used to log in to the web interface.



- **Last login time:**

This shows the date and time this login name was used to log in to this BCM2 device last time.



When the mouse pointer hovers over the last login time, detailed information about the last login is displayed, including the access client and IP address.

For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.

There are different types of access clients:

- Web GUI: Refers to the BCM2 web interface.
- CLI: Refers to the command line interface (CLI).

The information in parentheses following "CLI" indicates how this user is connected to the CLI.

- *Serial*: Represents the local connection (serial RS-232 or USB).
- *SSH*: Represents the SSH connection.
- *Telnet*: Represents the Telnet connection.

- **System date and time:**

Current date, year, and time are displayed to the right of the bar. If positioning the mouse pointer over the system date and time, the time zone information is also displayed.



Add a Page Icon

Click the Add Page icon  to open multiple pages of information, such as in a browser with tabs.



The Yellow- or Red-Highlighted Sensors

When a numeric sensor's reading enters the warning or critical range, the background color of the sensor row turns to yellow or red for alerting you.

For a discrete (on/off) sensor, the row changes the background color when the sensor enters the abnormal state.

See the table for the meaning of each color:

Color	State
White	<p>The background is white in one of the following scenarios:</p> <ul style="list-style-type: none"> • For a numeric sensor, no thresholds have been enabled. • If any thresholds have been enabled for a numeric sensor, the sensor reading is within the normal range, which is between the lower and upper warning thresholds. • For a discrete (on/off) sensor, the sensor state is normal. • The sensor is unavailable or unmanaged.

Color	State
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.
Red	<p>The meaning of the red color varies depending on the sensor type:</p> <ul style="list-style-type: none"> • For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold. • For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state.

To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- below lower critical: The numeric sensor's reading drops below the lower critical threshold.
- below lower warning: The numeric sensor's reading drops below the lower warning threshold.
- above upper critical: The numeric sensor's reading reaches or exceeds the upper critical threshold.
- above upper warning: The numeric sensor's reading reaches or exceeds the upper warning threshold.
- alarmed: The discrete sensor is NOT in the normal state.

For information on the thresholds, see **Setting Power Thresholds** (on page 114).

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the BCM2 device's status.

The screenshot shows the PMC Explorer web interface. On the left is a navigation tree with 'my PMC (192.168.62.11)' selected. The main area is titled 'Dashboard' and contains several sections: 'Power Meters' (a table with columns for ID, Type, Name, Rating, Circuits, A Current, B Current, and C Current), 'Alerted Sensors' (a table with columns for Sensor, Reading, and State), 'Alarms' (a table with columns for Name, Reason, First Appearance, Last Appearance, Count, and More Alerts), and 'Peripheral Devices (2 managed, 1 unmanaged)' (a table with columns for Name, Position, Reading, and State). Red callouts with numbers 1 through 8 point to specific elements: 1 points to the PMC controller in the tree; 2 points to the Power Meters folder; 3 points to the Peripheral Devices folder; 4 points to the Power Meters table; 5 points to the 'Scan Power Meters' button; 6 points to a red alert row in the Alerted Sensors table; 7 points to the Alarms section; and 8 points to the Peripheral Devices table.

①	PMC controller
②	Configured power meters
③	External sensors
④	Configured power meters with basic details and current readings for each phase
⑤	Scan Power Meters to discover unconfigured meters
⑥	Enabled thresholds show alerts in red or yellow

7	Alarms.
8	External sensors with basic details and readings.

Alerted Sensors

One of the sections on the Dashboard page only displays critical or warning conditions detected by internal or external sensors so that you are alerted to take actions. This section is labeled Alerted Sensors.

The Alerted Sensors section lists any or all of the following:

- Any sensor that enters the warning or critical range if the thresholds have been enabled
- Discrete (on/off) sensors that enter the alarmed state



Sensor	Reading	State
Power Meter 5 (3Phase Power Meter-id5...	0.2 A	below lower warning
Power Meter 5 (3Phase Power Meter-id5...	244 V	above upper warning
Power Meter 5 (3Phase Power Meter-id5...	249 V	above upper critical
Power Meter 5 (3Phase Power Meter-id5...	246 V	above upper critical

For the background color meanings, see **The Yellow- or Red-Highlighted Sensors** (on page 50).

Alarms List

You can create event rules that request users to acknowledge certain alerts, and resend alert notifications if the acknowledgment action is not taken yet. See **Creating Actions** (on page 154).

If any of these alerts has not been acknowledged since its occurrence, the Alarms section on the dashboard shows this alert until it is acknowledged. All alerts on the Alarms section are highlighted in red.

Below is the illustration of the alarms list.



Name	Reason	First Appearance	Last Appearance	Count	More Alerts
New Action 1	Peripheral device 'On/Off 1' in slot 1 is unavailable.	1/8/15 11:24 AM	1/8/15 1:56 PM	2	1 more reasons Details

The following table explains each column of the alarms list.

Column	Description
Name	The customized name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	The date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	The date and time when the event indicated in the Reason column occurred for the last time.
Count	The number of times the event indicated in the Reason column has occurred.
More Alerts	<ul style="list-style-type: none"> ▪ A dash is displayed when there is only one event triggering this alert. ▪ If there are other types of events triggering the same alert, the total number of these additional reasons is displayed. You can double click that alarm to view a list of all events that have occurred.
Details	Click "Details" to trigger a dialog showing both the alarm details and the acknowledgment button.

Only users who have the Acknowledge Alarms permission can manually acknowledge an alarm.

► **To acknowledge an alarm:**

1. Double-click the alarm that you want to acknowledge, or click Details in the final column. A dialog appears.
2. Click Acknowledge Alarm to acknowledge it. That alarm then disappears from the Alarms section.

Device Management

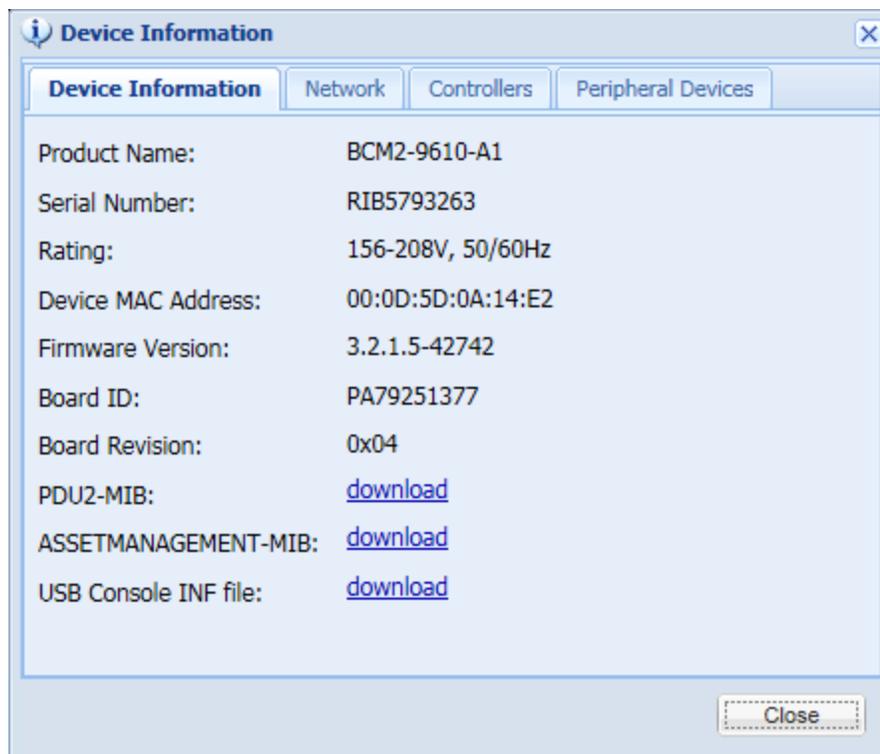
Using the web interface, you can retrieve basic hardware and software information, give the BCM2 a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying the Device Information

The Device Information dialog contains the serial number, model name and rating.

► To display the device information:

1. Choose Maintenance > Device Information.



Tab	Information shown
Device Information	General device information, such as model name, serial number, firmware version, hardware revision, and so on.
Network	The device specific network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether this BCM2 is part of an USB-cascading configuration. See Identifying Cascaded Devices (on page 56).
Controllers	The device controller's information, including its serial number, firmware version, and hardware revision.

Tab	Information shown
Peripheral Devices	Serial numbers, model names and firmware-related information of connected external devices, such as environmental sensor packages.

Identifying Cascaded Devices

This section explains how to identify a cascaded BCM2 in the Device Information dialog.

For information on how to cascade devices using USB cables, see **Cascading the BCM2 via USB** (on page 42).

*Note: For more information on the USB-cascading configuration, see the USB-Cascading Solution Guide, which is available from Raritan website's **Support page** (<http://www.raritan.com/support/>).*

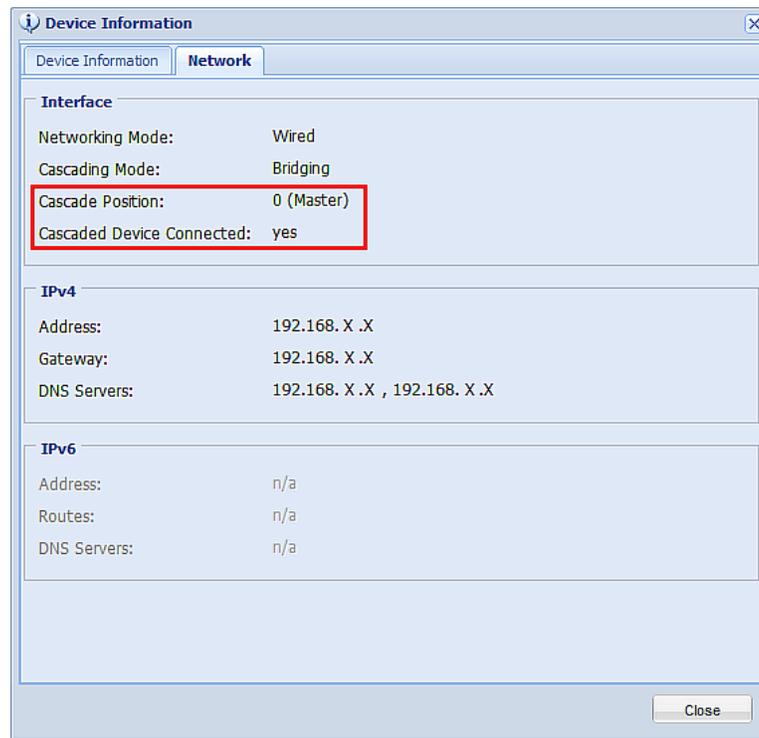
► **To identify the USB-cascading status of a BCM2 device:**

1. Choose Maintenance > Device Information.
2. Select the Network tab and locate the Interface section. The Interface section contains four read-only fields as listed below.

Fields	Description
Networking Mode	Indicates how the BCM2 is connected to the LAN. <ul style="list-style-type: none"> ▪ Wired: The device is connected to the LAN through a standard network cable. ▪ Wireless: The device is connected to the LAN through a supported USB wireless LAN adapter. See USB Wireless LAN Adapters (on page 44). ▪ XXX (USB): XXX represents Wired or Wireless. The device is connected to the LAN through a USB-cascading configuration. That is, it is a slave device.
Cascading Mode	Shows the cascading mode applied. See Setting the Cascading Mode (on page 85).

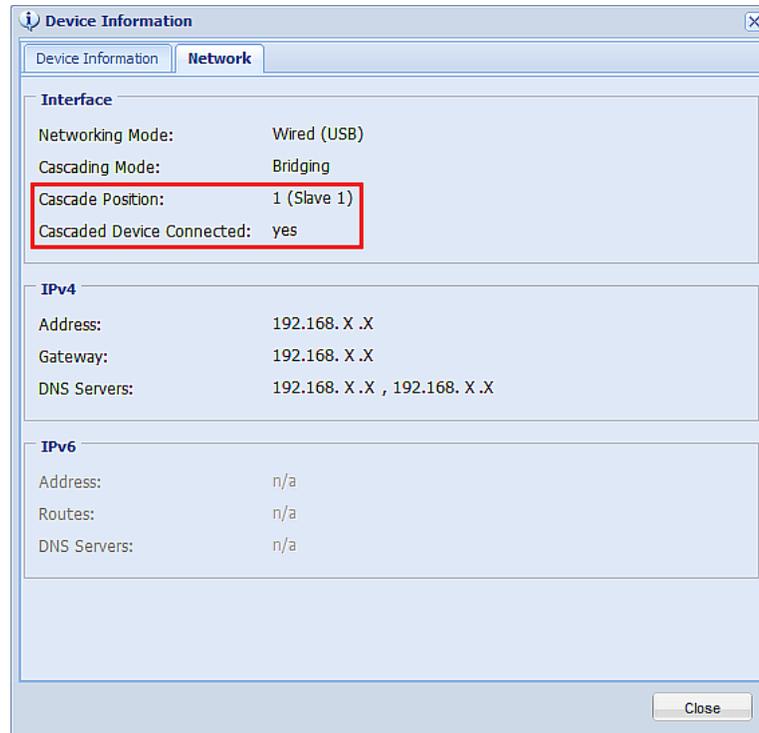
Fields	Description
Cascade Position	<p>Indicates the position of the BCM2 in the USB-cascading configuration.</p> <ul style="list-style-type: none"> 0 (zero) represents the master device. A non-zero number represents a slave device. 1 is Slave 1, 2 is Slave 2, 3 is Slave 3 and so on. <p>This field is NOT available on a standalone BCM2.</p>
Cascaded Device Connected	<p>Indicates whether the presence of a slave device is detected on the USB-A port.</p> <ul style="list-style-type: none"> yes: Connection to a slave device is detected. no: NO connection to a slave device is detected.

- A master device shows 0 (zero) in the Cascade Position field and yes in the Cascaded Device Connected field.



- A slave device in the middle position shows a non-zero number which indicates its exact position in the Cascade Position field and yes in the Cascaded Device Connected field.

The following diagram shows 1, indicating it is the first slave - Slave 1.



- The final slave device shows a non-zero number which indicates its position in the Cascade Position field and *no* in the Cascaded Device Connected field.

The following diagram shows 2, indicating it is the second slave - Slave 2. The Cascaded Device Connected field shows *no*, indicating that it is the final one in the chain.

The screenshot shows a web interface window titled "Device Information" with a "Network" tab selected. The "Interface" section contains the following settings:

Networking Mode:	Wired (USB)
Cascading Mode:	Bridging
Cascade Position:	2 (Slave 2)
Cascaded Device Connected:	no

The "IPv4" section shows:

Address:	192.168. X .X
Gateway:	192.168. X .X
DNS Servers:	192.168. X .X , 192.168. X .X

The "IPv6" section shows:

Address:	n/a
Routes:	n/a
DNS Servers:	n/a

A "Close" button is located at the bottom right of the window.

Naming the BCM2

The default name for BCM2 is *my PMC*. You may give it a unique device name.

► To change the device name:

1. Click the PMC folder.

*Note: The PMC folder is named "my PMC" by default. The name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Setup in the Settings section. The setup dialog appears.
3. Type a new name in the Device Name field.
4. Click OK.

Modifying the Network Configuration

The network settings you can change via the web interface include wired, wireless, IPv4 and/or IPv6 settings.

Modifying Network Interface Settings

The BCM2 supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies.

Wired Network Settings

The LAN interface speed and duplex mode were set during the initial configuration process.

By default, the LAN speed and duplex mode are set to "Auto" (automatic), which works in nearly all scenarios. You can change them if there are special local requirements.

► **To modify the network interface settings:**

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.
 - Auto: System determines the optimum LAN speed through auto-negotiation.
 - 10 Mbit/s: The LAN speed is always 10 Mbps.
 - 100 Mbit/s: The LAN speed is always 100 Mbps.
5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.
 - Auto: The BCM2 selects the optimum transmission mode through auto-negotiation.
 - Full: Data is transmitted in both directions simultaneously.
 - Half: Data is transmitted in one direction (to or from the BCM2 device) at a time.
6. Click OK.

Tip: You can check the LAN status in the Current State field, including the speed and duplex mode.

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. You can change them later.

*Note for USB-cascading configuration: "Port forwarding" mode over wireless LAN is supported. See **Cascading the BCM2 via USB** (on page 42).*

► **To modify the wireless interface settings:**

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the BCM2 device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See **Wireless Network Connection** (on page 44).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

Note: BSSID refers to the MAC address of an access point in the wireless network.

7. In the Authentication field, select an appropriate option from the drop-down list.

Options	Description
No Authentication	Select this option when no authentication data is required.
PSK	A Pre-Shared Key is required for this option. <ul style="list-style-type: none"> ▪ In the Pre-Shared Key field, type the PSK string.

Options	Description
EAP - PEAP	<p>PEAP stands for Protected Extensible Authentication Protocol.</p> <p>Enter the following authentication data:</p> <ul style="list-style-type: none"> ▪ Inner Authentication: Only Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) is supported, allowing authentication to databases that support MSCHAPv2. ▪ Identity: Type your user name. ▪ Password: Type your password. ▪ CA Certificate: A third-party CA certificate may or may not be needed. If needed, follow the step below.

8. When the PEAP authentication requires a CA certificate, do the following:
 - a. Select the "Enable Verification of TLS Certificate Chain" checkbox for the BCM2 to verify the validity of the TLS certificate that will be installed. For example, the BCM2 will check the certificate's validity period against the system time.
 - b. Click Browse to select a TLS certificate file. Then you can:
 - Click Show to view the certificate's contents.
 - Click Remove to delete the installed certificate if it is inappropriate.
 - c. Select the "Allow expired and not yet valid certificates" checkbox if intending to make the wireless network connection successful even though the installed TLS certificate chain contains any certificate that is outdated or not valid yet.
 - d. Select the "Allow wireless connection if system clock is incorrect" checkbox to make the wireless network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with any NTP server. If the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail while this checkbox is not selected.

The incorrect system time issue may occur when the BCM2 has once been powered off for a long time.
9. Click OK.

Modifying Network Settings

The BCM2 was configured for network connectivity during the installation and configuration process. If necessary, you can modify any network settings later.

Selecting the Internet Protocol

The BCM2 device supports two types of Internet protocols -- IPv4 and IPv6. You can enable either or both protocols. After enabling the desired Internet protocol(s), all but not limited to the following protocols will be compliant with the enabled Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL/TLS
- SNMP
- SysLog

► To select the appropriate Internet Protocol:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IP Protocol tab.
3. Select one checkbox according to the Internet protocol(s) you want to enable:
 - IPv4 only: Enables IPv4 only on all interfaces. This is the default.
 - IPv6 only: Enables IPv6 only on all interfaces.
 - IPv4 and IPv6: Enables both IPv4 and IPv6 on all interfaces.
4. If you selected the "IPv4 and IPv6" checkbox in the previous step, you must determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses.
 - IPv4 Address: Use the IPv4 addresses returned by the DNS server.
 - IPv6 Address: Use the IPv6 addresses returned by the DNS server.
5. Click OK.

Modifying IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See **Selecting the Internet Protocol** (on page 63).

► **To modify IPv4 settings:**

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IPv4 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
DHCP	<p>To auto-configure the BCM2, select DHCP.</p> <p>With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field.</p> <p>The host name:</p> <ul style="list-style-type: none"> ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols <p>Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.</p>
Static	<p>To manually assign an IP address, select Static, and enter the following information in the corresponding fields:</p> <ul style="list-style-type: none"> ▪ IP address ▪ Netmask ▪ Default gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional) <p>If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your BCM2 can communicate with the other subnet. Each static route requires:</p>

Option	Description
	<ul style="list-style-type: none"> ▪ Destination: IP address of the other subnet and subnet mask using the format "IP address/subnet mask." ▪ Next Hop: IP address of the next hop router. <p>See Static Route Examples (on page 67) for illustrations.</p>

4. Click OK.

Note: The BCM2 supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the BCM2 only uses the primary IPv4 and IPv6 DNS servers.

Modifying IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See **Selecting the Internet Protocol** (on page 63).

► To modify IPv6 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IPv6 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
Automatic	<p>To auto-configure the BCM2, select Automatic.</p> <p>With this option selected, you can enter a preferred host name, which is optional. Type the host name in the Preferred Hostname field.</p> <p>The host name:</p> <ul style="list-style-type: none"> ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols <p>Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.</p>
Static	<p>To manually assign an IP address, select Static, and enter the following information in the corresponding fields:</p>

Option	Description
	<ul style="list-style-type: none"> ▪ IP address ▪ Default gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional) <p>If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your BCM2 can communicate with the other subnet. Each static route requires:</p> <ul style="list-style-type: none"> ▪ Destination: IP address of the current subnet and prefix length using the format "IP address/prefix." ▪ Next Hop: IP address of the next hop router. <p>See Static Route Examples (on page 67) for illustrations.</p>

4. Click OK.

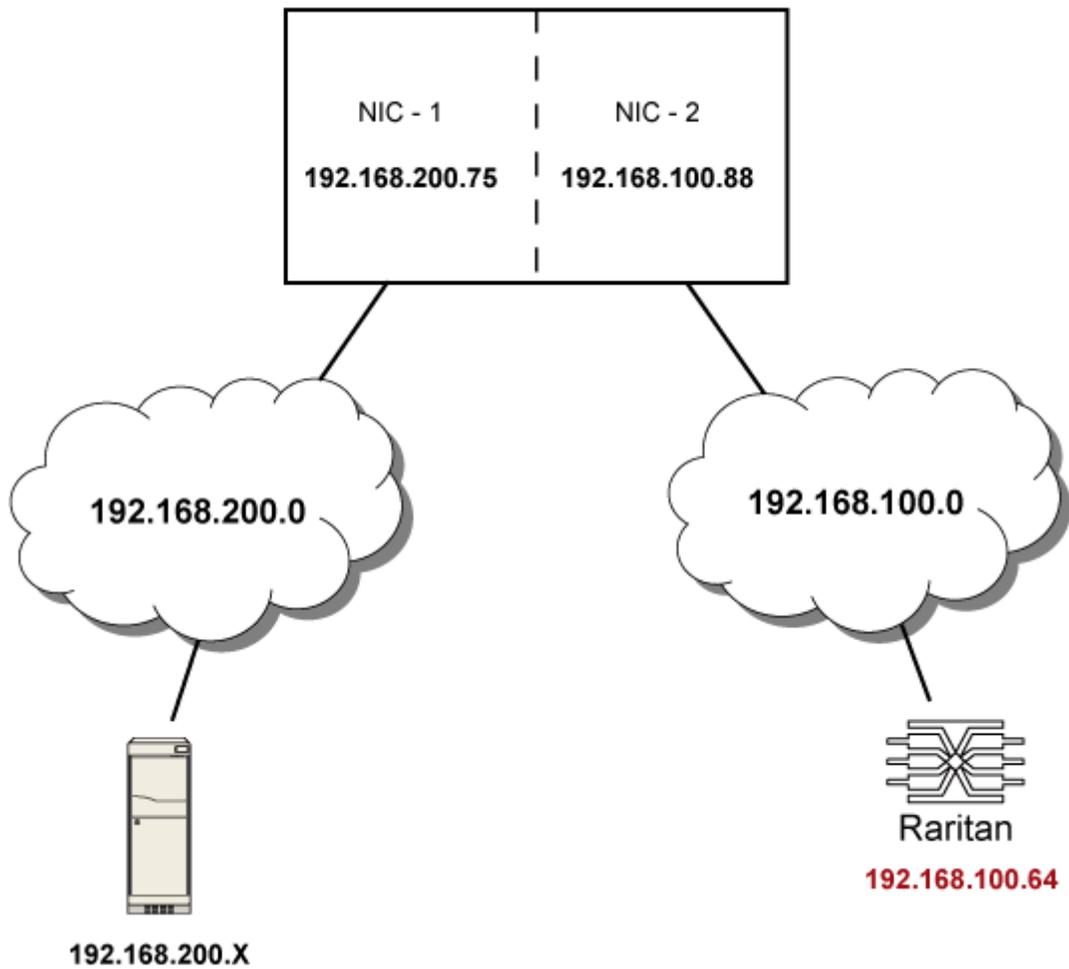
Note: The BCM2 supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the BCM2 only uses the primary IPv4 and IPv6 DNS servers.

Static Route Examples

This section has two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and BCM2 devices in the examples use static IP addresses.

► **IPv4 example:**

- Your BCM2: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Subnet mask: *24*

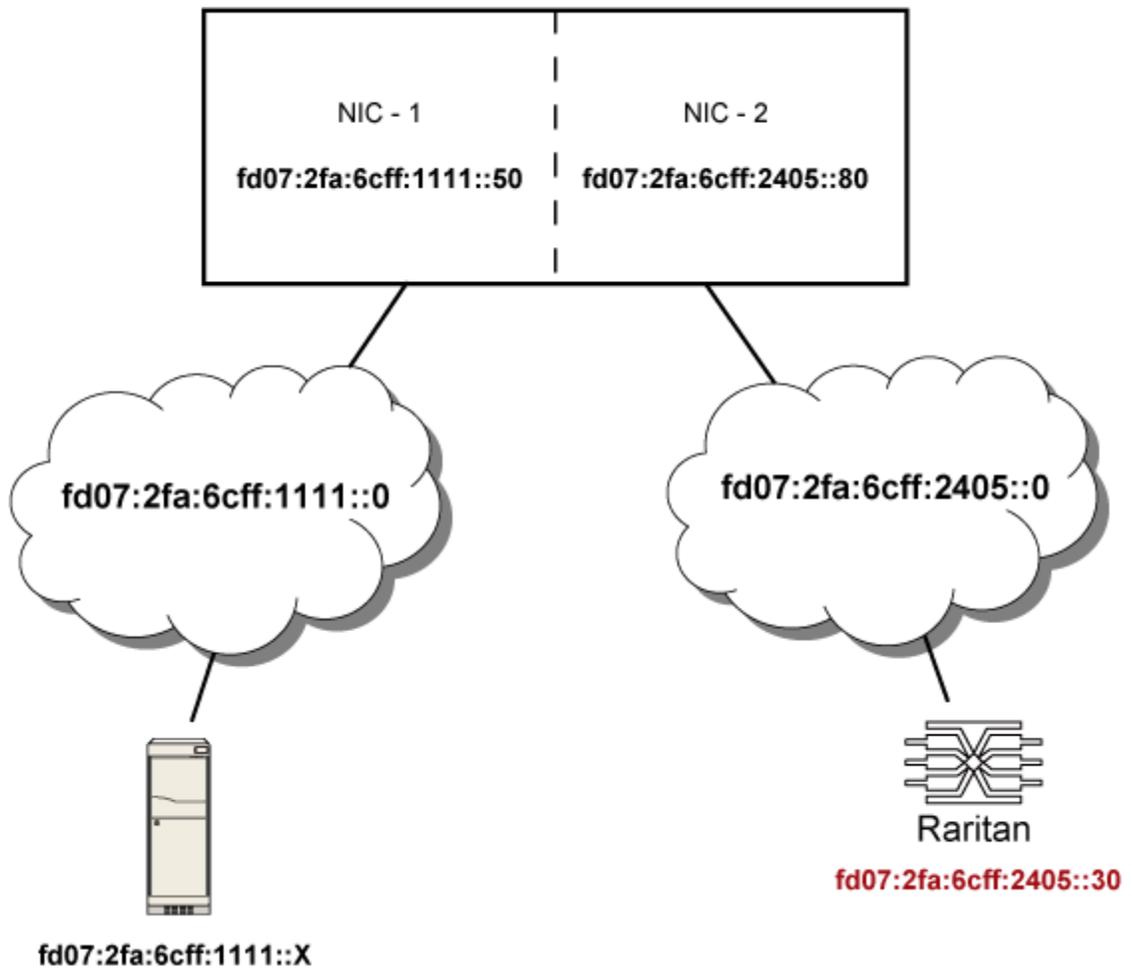


In this example, NIC-2 (192.168.100.88) is the next hop router for your BCM2 to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Append new Route" dialog, you should specify:

- Destination: 192.168.200.0/24
- Next Hop: 192.168.100.88

► **IPv6 example:**

- Your BCM2: *fd07:2fa:6cff:2405::30*
- Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*
- Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*
- Prefix length: 64



In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your BCM2 to communicate with any device in the other subnet fd07:2fa:6cff:1111::0. In the IPv6 'Append new Route' dialog, you should specify:

- Destination: fd07:2fa:6cff:2405::0/64
- Next Hop: fd07:2fa:6cff:2405::80

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the BCM2 may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the BCM2 can resolve the external authentication server's name to an IP address for establishing a connection. If the *SSL/TLS encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on external authentication, see **Setting Up External Authentication** (on page 144).

Modifying Network Service Settings

The BCM2 supports these network communication services: HTTPS, HTTP, Telnet and SSH.

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the command line interface. See **Using the Command Line Interface** (on page 255).

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

In addition, the BCM2 also supports the SNMP and Modbus/TCP protocols.

Changing HTTP(S) Settings

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the BCM2 device so it is a more secure protocol than HTTP.

By default, any access to the BCM2 device via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

► **To change HTTP or HTTPS port settings:**

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.
2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

Warning: Different network services cannot share the same TCP port.

3. Enable or disable either or both ports.
 - To enable or disable the HTTP port, select or deselect the "HTTP access" checkbox.
 - To enable or disable the HTTPS port, select or deselect the "HTTPS access" checkbox.

► **To enable or disable HTTPS redirection:**

In the HTTP Settings dialog, the "Enforce use of HTTPS (redirect to HTTPS)" checkbox determines whether the HTTP access to the BCM2 is redirected to HTTPS.

- To enable the redirection, select the checkbox.
- To disable the redirection, deselect the checkbox.

Note: The redirection checkbox is configurable only when both HTTP and HTTPS ports have been enabled.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, or change the default TCP port for the SSH service. In addition, you can decide to log in using either the password or the public key over the SSH connection.

► **To change SSH service settings:**

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the port field. Valid range is 1 to 65535.

3. To enable the SSH application, select the Enable SSH Access checkbox. To disable it, deselect the checkbox.
4. To select a different authentication method, select one of the checkboxes.
 - Password authentication only: Enables the password-based login only.
 - Public key authentication only: Enables the public key-based login only.
 - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click OK.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 96).

Changing Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the default TCP port for the Telnet service.

► To change Telnet service settings:

1. Choose Device Settings > Network Services > Telnet. The Telnet Settings dialog appears.
2. To use a different port, type a new port number in the port field. Valid range is 1 to 65535.
3. To enable the Telnet application, select the Enable Telnet Access checkbox. To disable it, deselect the checkbox.
4. Click OK.

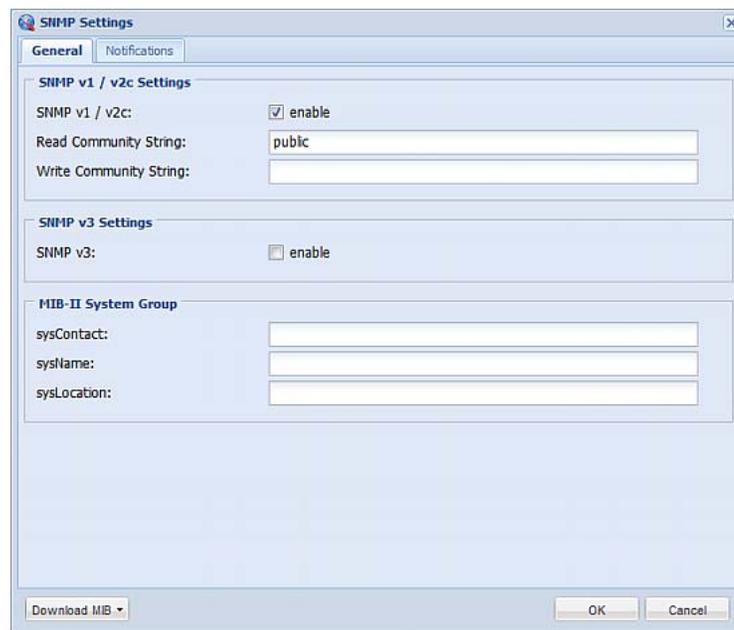
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the BCM2 device. Enabling SNMP communication allows the manager to retrieve the status of the BCM2 device.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See **Event Rules and Actions** (on page 153).

► **To configure the SNMP communication:**

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
 - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
 - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

*Tip: You can permit or disallow a user to access the BCM2 via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** (on page 245).*

4. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system
 - b. sysName - the name assigned to the system
 - c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your BCM2 is used by the SNMP manager.

*Important: You must download the SNMP MIB for your BCM2 to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** (on page 252).*

6. Click OK.

► **To configure SNMP notification destinations:**

1. Click the Notifications tab in the same dialog.
2. Select the Enabled checkbox.
3. Select an SNMP notification type - SNMP v2c Trap, SNMP v2c Inform, SNMP v3 Trap, and SNMP v3 Inform.
4. Specify the SNMP notification destinations by doing the following:
 - a. Specify the SNMP notification destinations in the Host field(s).
 - b. Specify a port number for the destination in the Port field(s).
 - c. Enter necessary information in other fields, such as the community string for SNMP Trap or authentication pass phrase for SNMP Inform. See **Configuring SNMP Notifications** (on page 246) for details.
5. Click OK.

*Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** (on page 193).*

Configuring Modbus TCP and/or RTU

If enabling the Modbus/TCP feature, the Modbus clients on your network can access the BCM2.

If enabling the Modbus/RTU feature, the Modbus RTU clients connected to the BCM2 can access the BCM2.

After enabling any Modbus access, you have to determine whether the Modbus access to the following devices connected to the BCM2 is enabled or not:

- Panels. See **Panel Mains Circuit Management** (on page 106).
- Power Meters. See **Power Meter Management** (on page 112).
- Environmental sensor packages, including actuators. See **Enabling Main Controller Access** (on page 77).

This table lists the capabilities available after enabling either Modbus feature.

Capability	Required Modbus settings
Configure the thresholds of panel mains circuits and panel branch circuits	<ul style="list-style-type: none"> ▪ Modbus TCP and/or RTU is enabled. ▪ Read-only mode is DISABLED.
Retrieve the data of environmental sensor packages connected to the BCM2	<ul style="list-style-type: none"> ▪ Modbus TCP and/or RTU is enabled. ▪ Main Controller Access is enabled.
Switch on/off the actuators connected to the BCM2	<ul style="list-style-type: none"> ▪ Modbus TCP and/or RTU is enabled. ▪ Read-only mode is DISABLED. ▪ Main Controller Access is enabled.

Changing Modbus/TCP Settings

Modbus Settings

Enable Modbus/TCP Access

Modbus/TCP Port:

Enable read-only mode

Enable Modbus/RTU Access

Baud rate: ▼

Parity: ▼

Stop Bits: ▼

Enable read-only mode

Enable Main Controller Access

Modbus Address:

OK Cancel

You can enable or disable the Modbus/TCP access to the BCM2 or the read-only mode, or change the default TCP port for the Modbus service.

► **To change the Modbus service settings:**

1. Choose Device Settings > Network Services > Modbus. The Modbus Settings dialog appears.
2. To enable the Modbus/TCP access, select the Enable Modbus/TCP Access checkbox. To disable it, deselect the checkbox.
3. To use a different port, type a new port number in the port field. Valid range is 1 to 65535.
4. To enable the Modbus read-only mode, select the "Enable read-only mode" checkbox. To disable it, deselect the checkbox.

For the capabilities available when disabling the read-only mode, see **Configuring Modbus TCP and/or RTU** (on page 74).

Enabling the Modbus/RTU Feature

With the Modbus/RTU feature enabled, the BCM2 allows the Modbus RTU device(s) connected to the BCM2 to access the BCM2.

The BCM2 supports communications to multiple Modbus RTU devices. Note that the connected Modbus RTU devices are invisible to the BCM2.

► To use the Modbus/RTU feature:

1. Attach a Modbus RTU device, or a Modbus bus with multiple RTU devices connected, to the green connector labeled MODBUS on the BCM2.
2. On the BCM2, enable and properly configure the Modbus/RTU feature. See **Configuring Modbus/RTU Settings** (on page 76).

Configuring Modbus/RTU Settings

1. Choose Device Settings > Network Services > Modbus.
2. Select the Enable Modbus/RTU Access checkbox.

The screenshot shows a 'Modbus Settings' dialog box with the following configuration:

- Enable Modbus/TCP Access
 - Modbus/TCP Port: 502
 - Enable read-only mode
- Enable Modbus/RTU Access (highlighted with a red border)
 - Baud rate: 19200 bit/s
 - Parity: Even
 - Stop Bits: 1
 - Enable read-only mode
- Enable Main Controller Access
 - Modbus Address: 2

Buttons: OK, Cancel

Settings	Description
Baud rate, Parity and Stop Bits Required	Update these parameters if your Modbus/RTU master device controlling the bus is using different communication parameters.
Enable read-only mode Optional	Enable the read-only mode only when intending to prevent any changes made by Modbus/RTU clients on the same bus. For the capabilities available when disabling the read-only mode, see Configuring Modbus TCP and/or RTU (on page 74).

Enabling Main Controller Access

After enabling the Modbus TCP and/or RTU access, you can determine whether to allow the Modbus clients to access environmental sensor packages or even control the actuators connected to the BCM2. If yes, a unique Modbus address is required.

The Modbus address MUST NOT collide with those of connected panels, power meter modules and, if Modbus/RTU is enabled, other Modbus RTU devices on the same bus. Otherwise, the communication between the Modbus clients and the BCM2's environmental sensor packages fails.

*Note: To control the actuators, make sure the Modbus "read-only mode" is disabled. See **Configuring Modbus TCP and/or RTU** (on page 74).*

► **To configure Main Controller Access and Modbus Address:**

1. Choose Device Settings > Network Services > Modbus.
2. Enable either or both of the Modbus access methods.
 - To enable the Modbus/TCP access, see **Changing Modbus/TCP Settings** (on page 75).
 - To enable the Modbus/RTU access, see **Enabling the Modbus/RTU Feature** (on page 76).

3. Select the Enable Main Controller Access checkbox.

The screenshot shows a 'Modbus Settings' dialog box with the following configuration:

- Enable Modbus/TCP Access**
 - Modbus/TCP Port: 502
 - Enable read-only mode
- Enable Modbus/RTU Access**
 - Baud rate: 19200 bit/s
 - Parity: Even
 - Stop Bits: 1
 - Enable read-only mode
- Enable Main Controller Access**
 - Modbus Address: 2

Buttons: OK, Cancel

4. In the Modbus Address field, assign a unique Modbus address to the BCM2 main controller.
 - This address CANNOT be identical to that of any panel or power meter module connected to this BCM2, or you cannot save the dialog. See **Panel Mains Circuit Management** (on page 106) and **Power Meter Management** (on page 112).
 - If enabling the Modbus/RTU feature, make sure this address is NOT identical to that of any other device on the same Modbus RTU bus.

Enabling Service Advertisement

The BCM2 advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicastDNS). The advertised services are discovered by clients that have implemented DNS-SD and mDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

By default, this feature is enabled.

The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where *<preferred_host_name>* is the preferred host name you have specified for BCM2. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

*Note: For information on configuring IPv4 and/or IPv6 network settings, see **Modifying Network Settings** (on page 63).*

► To enable service advertisement:

1. Choose Device Settings > Network Services to select the Service Advertisement checkbox.
2. Click Yes on the confirmation message to switch to zero configuration advertising. The feature is enabled and the Service Advertisement checkbox is selected in the submenu.

► To disable service advertisement:

1. Choose Device Settings > Network Services to deselect the Service Advertisement checkbox.
2. Click Yes on the confirmation message to switch off the zero configuration advertising. The feature is disabled and the Service Advertisement checkbox is deselected in the submenu.

Setting the Date and Time

Set the internal clock on the BCM2 device manually, or link to a Network Time Protocol (NTP) server.

► **To set the date and time:**

1. Choose Device Settings > Date/Time.
2. In the Time Zone field, select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.
If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

4. Choose one of the methods to set the date and time:
 - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
 - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on.
 - To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.
 - To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
 - To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.
Click Check NTP Servers to verify the validity and accessibility of the specified NTP servers.

Note: If the BCM2 device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.

5. Click OK.

The BCM2 follows the NTP server sanity check per the IETF RFC. If your BCM2 has problems synchronizing with a Windows NTP server, see **Windows NTP Server Synchronization Solution** (on page 81).

Note: If you are using Sunbird's Power IQ to manage the BCM2, you must configure Power IQ and the BCM2 to have the same date/time or NTP settings.

Windows NTP Server Synchronization Solution

The NTP client on the BCM2 follows the NTP RFC so the BCM2 rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the BCM2.

Note: For information on NTP RFC, visit <http://tools.ietf.org/html/rfc4330> <http://tools.ietf.org/html/rfc4330> to refer to the section 5.

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the BCM2. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

► **To change the Windows NTP's root dispersion settings:**

1. Access the registry settings associated with the root dispersion on the Windows NTP server.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.
 - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
 - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.

3. *LocalClockDispersion* must be set to 0.

Setting Default Measurement Units

Default measurement units are applied to the BCM2 web and CLI interfaces across all users, including users accessing the device via external authentication servers. Default units apply before users set their own preferred measurement units or the administrator changes preferred units for any user.

*Note: To set preferred measurement units for your own, see **Setting Up Your Preferred Measurement Units** (on page 100). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to the BCM2 user interfaces after you log in.*

► **To set up default user preferences:**

1. Choose User Management > Default User Preferences.
2. Update any of the following as needed:
 - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
 - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
 - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.
3. Click OK.

Configuring the Feature Port

The FEATURE port supports Raritan asset management sensors and an external beeper. See **Connecting Asset Management Sensors** (on page 31) and **Connecting an External Beeper** (on page 41).

Note that only the PMC models of the BCM2 series have the FEATURE port.

► **To configure the FEATURE port:**

1. Click the Feature Port folder. The Feature Port page opens in the right pane.
2. Select the Port# 1 device on the Feature Port page, and click Setup. The Feature Port Setup dialog appears.
3. Select the desired mode in the Detection Mode field.
 - Auto: The BCM2 automatically detects and displays the device connected to the FEATURE port. This is the default.
 - Disabled: The FEATURE port is disabled so the BCM2 does not detect and display the connected device.

- A specific device type: The BCM2 always displays the selected device type no matter which device is connected or whether the selected device is detected or not. After selecting a device type, the Mode column shows "Pinned." Available device types are listed below.

Device type	Description
Asset Strip	Raritan asset sensors.
External Beeper	An external beeper with the RJ-45 socket.

Front Panel Settings

You can choose the default front panel view of the PMC.

Automatic mode: The PMC scrolls through readings for each power meter.

Power meter overview: The PMC shows a list of configured power meters as well as their readings. See the illustration shown below.

Power Meters	
Panel 2 (200 A)	397.5 V
96 circuit positions	0.00 A
0 circuits	0 W
Power Meter 9 (32 A)	229.0 V
	19.20 A
	4,140 W

✕ Menu
9:42 AM
Details ○

► **To configure front panel settings:**

1. Choose Device Settings > Front Panel Settings.
2. Select Automatic mode or Power Meter Overview and click OK.

Configuring the Serial Port

You can change the bit-rate of the serial port labeled CONSOLE / MODEM on the BCM2 device. The default bit-rate for both console and modem operation is 115200 bps.

The BCM2 supports the use of one of the following devices via the serial interface:

- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit-rate before connecting the supported device to the BCM2 through the serial port, or there are communication problems.

You can set diverse bit-rate settings for console and modem operations. Usually the BCM2 can detect the device type, and automatically apply the preset bit-rate.

► **To change the serial port baud rate settings:**

1. Choose Device Settings > Serial Port Settings. The Serial Port Configuration dialog appears.
2. In the "Connected device" field, select an appropriate option to force the serial port to enter the correct state.

Options	Description
Automatic detection	The BCM2 automatically detects the device type on the serial port. Select this option unless your BCM2 cannot correctly detect it.
Force console	The port enters the local console state.
Force analog modem	The port enters the analog modem state.
Force GSM modem	The port enters the GSM modem state.

3. In the Console Baud Rate field, select the baud rate intended for console management.

Note: For a serial RS-232 or USB connection between a computer and the BCM2, leave it at the default (115200 bps).

4. In the Modem Baud Rate field, select the baud rate used for the modem connected to the BCM2.

► **To configure the analog modem settings:**

1. Click the Analog Modem tab.

2. Select the "Answer incoming calls" checkbox to enable the remote access via a modem. Otherwise, deselect this checkbox.
3. Specify the number of rings the BCM2 must wait before answering the call. You can either type a value or click the Up/Down arrow keys to adjust the value in the "Number of rings until answering" field.

► **To configure the GSM modem settings:**

1. Click the GSM Modem tab.
2. Enter the SIM PIN.
3. Select 'Use custom SMS center number' if a custom SMS will be used.
4. Enter the SMS center number in the SMS Center field.
5. Click Advanced Information to show information.
6. Enter the number of the recipient's phone in the Recipients Phone field, then click Send SMS Test to send a test SMS message.

Setting the Cascading Mode

A maximum of eight BCM2 devices can be cascaded using USB cables and therefore share only one Ethernet connection. See **Cascading the BCM2 via USB** (on page 42).

The Ethernet sharing mode applied to the USB-cascading configuration is either network bridging or port forwarding. This mode is determined by the master device.

Only the Admin user or a user who has the Administrator Privileges permission can configure the cascading mode.

Note: The BCM2 in the "port-forwarding" mode does not support APIPA.

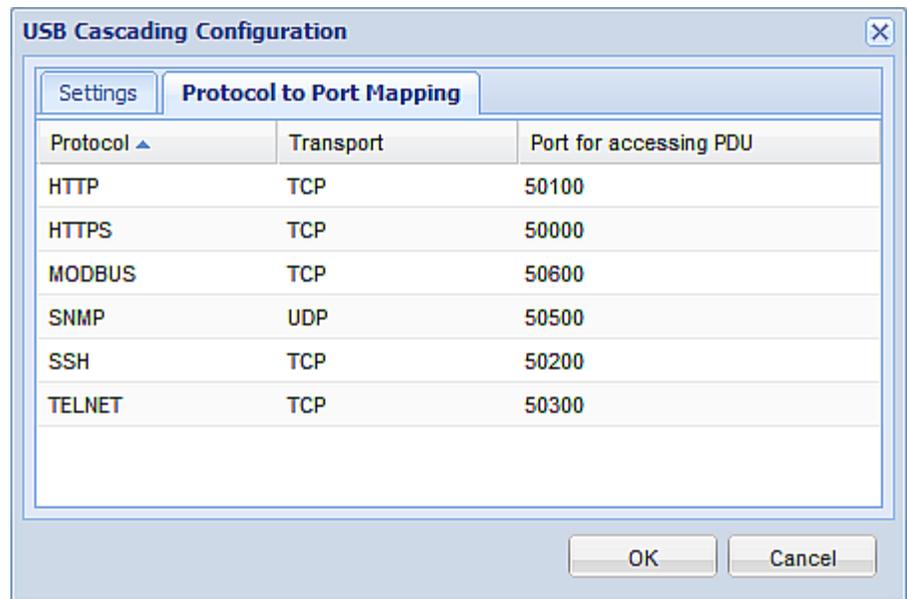
► **To configure the cascading mode:**

1. Log in to the master device's web interface.
2. Choose Device Settings > USB Cascading. The USB Cascading Configuration dialog appears.
3. Verify that the "Position in cascaded chain" field shows 0 (Master), indicating that this BCM2 is the master device.
4. Select the preferred cascading mode in the "Cascading mode" field.
 - Bridging: Each device in the USB-cascading configuration is accessed with a different IP address. This is the default.
 - Port Forwarding: Each device in the USB-cascading configuration is accessed with the same IP address with a different port number assigned. The port numbers vary based on the networking protocol and device position in the chain. See **Port Number Syntax** (on page 87).

Note: If reversing or disconnecting the USB cable from a slave device, causing the slave device to become a master or standalone device, you must plug an Ethernet cable to it to update its USB-cascading status.

5. Click OK.
6. If selecting Port Forwarding, a list of port numbers for diverse networking protocols will be available on the "Protocol to Port Mapping" tab of each cascaded device.

Return to the same dialog and click the "Protocol to Port Mapping" tab to view the master device's port numbers.



For information on accessing each cascaded device in the Port Forwarding mode, see **Port Forwarding Examples** (on page 88).

Port Number Syntax

In the Port Forwarding mode, all devices in the USB-cascading configuration share the same IP address. To access any cascaded device, you must assign an appropriate port number to it.

- Master device: The port number is either *5NNXX* or the standard TCP/UDP port.
- Slave device: The port number is *5NNXX*.

► **5NNXX port number syntax:**

- NN is a two-digit number representing the network protocol as shown below:

Protocols	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

- XX is a two-digit number representing the device position as shown below:

Position	XX
Master device	00
Slave 1	01
Slave 2	02
Slave 3	03
Slave 4	04
Slave 5	05
Slave 6	06
Slave 7	07

For example, to access the Slave 4 device via Modbus/TCP, the port number is 50604. See **Port Forwarding Examples** (on page 88) for further illustrations.

*Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. See **Setting the Cascading Mode** (on page 85).*

► **Standard TCP/UDP ports:**

The master device can be also accessed through standard TCP/UDP ports as listed in the following table.

Protocols	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

In the Port Forwarding mode, the BCM2 does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet, SNMP and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

- Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports. See **Port Number Syntax** (on page 87) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a USB-cascading configuration comprising three Raritan products. The IP address is 192.168.84.77.*

► **Master device:**

Position code for the master device is 00 so each port number is 5NN00 as shown below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100

Protocols	Port numbers
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

- To access the master device via HTTPS, the IP address is:
https://192.168.84.77:50000/
- To access the master device via HTTP, the IP address is:
http://192.168.84.77:50100/
- To access the master device via SSH, the command is:
ssh -p 50200 192.168.84.77

Examples using standard TCP/UDP ports:

- To access the master device via HTTPS, the IP address is:
https://192.168.84.77:443/
- To access the master device via HTTP, the IP address is:
http://192.168.84.77:80/
- To access the master device via SSH, the command is:
ssh -p 22 192.168.84.77

▶ Slave 1 device:

Position code for Slave 1 is 01 so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

Examples:

- To access Slave 1 via HTTPS, the IP address is:
https://192.168.84.77:50001/

- To access Slave 1 via HTTP, the IP address is:
`http://192.168.84.77:50101/`
- To access Slave 1 via SSH, the command is:
`ssh -p 50201 192.168.84.77`

► **Slave 2 device:**

Position code for Slave 2 is 02 so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

Examples:

- To access Slave 2 via HTTPS, the IP address is:
`https://192.168.84.77:50002/`
- To access Slave 2 via HTTP, the IP address is:
`http://192.168.84.77:50102/`
- To access Slave 2 via SSH, the command is:
`ssh -p 50202 192.168.84.77`

Specifying the Device Altitude

You must specify the BCM2 device's altitude above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See **Altitude Correction Factors** (on page 420).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See **Setting Default Measurement Units** (on page 82).

► **To specify the altitude of the BCM2 device:**

1. Click the PMC folder.

*Note: The PMC folder is named "my PMC" by default. The name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Setup in the Settings section. The setup dialog appears.
3. Type an integer number in the Altitude field. Depending on the measurement unit displayed, the range of valid numbers differs.
 - For meters (m), the value ranges between 0 and 3000.
 - For feet (ft), the value ranges between 0 and 9842.
4. Click OK.

Setting Data Logging

The BCM2 can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the BCM2 internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in the log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

*Note: The BCM2 device's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** (on page 244). In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is enabled. You must have "Administrator" or "Change PMC, PMB & PMM Configuration" permissions to change the setting.

► **To configure the data logging feature:**

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All to have all sensors selected.
5. Click OK.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the BCM2 in Step 4, it is NOT recommended.

Configuring SMTP Settings

The BCM2 can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See **Viewing the Local Event Log** (on page 200).

Note: See **Event Rules and Actions** (on page 153) for information on creating event rules to send email notifications.

► **To set SMTP server settings:**

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the "Number of Sending Retries" field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
 - a. Select the Server Requires Authentication checkbox.
 - b. Type a user name in the User Name field.
 - c. Type a password in the Password field.
8. If your SMTP server supports the Transport Layer Security (TLS), select the "Enable SMTP over TLS (StartTLS)" checkbox. Then do the following:
 - a. Click Browse to select the TLS CA certificate file. Then you may:

- Click Show to view the installed certificate's contents.
 - Click Remove to delete the installed certificate if it is inappropriate.
- b. Select or deselect the "Allow expired and not yet valid certificates" checkbox.
 - To always send the email messages even though the installed certificate chain contains a certificate that is outdated or not valid yet, select this checkbox.
 - To prevent the email messages from being sent when any certificate in the installed certificate chain is outdated or not valid yet, deselect this checkbox.
9. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:
 - a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
 - b. Click Send Test Email.
 - c. Check if the recipient(s) receives the email successfully.
 10. Click OK.

Configuring Data Push Settings

If any Raritan asset sensors have been connected to BCM2, you can push the asset sensor data to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the BCM2.

For instructions on connecting asset sensors, see **Connecting Asset Management Sensors** (on page 31).

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule. See **Push Out Sensor Readings** (on page 160).
- To push the data at a regular interval, schedule the data push action. See **Scheduling an Action** (on page 175).

► **To configure data push settings:**

1. Choose Device Settings > Data Push. The Data Push dialog appears.
2. Click New. The Add New Destination dialog appears.
3. In the URL field, determine the following information.

- Click the arrow to select http or https.
 - Type the URL or host name in the accompanying text box.
4. If the destination server requires authentication, select the "Use authentication" checkbox, and provide the authentication information:
 - In the "User name" field, type the login name.
 - In the Password field, type the login password.
 5. In the "Entry type" field, determine the data that will be transmitted.
 - Asset management information: Transmit the information of the specified asset sensor(s), including the general status of the specified sensor(s) and a list of asset tags on blade extension strips if any.
 - Asset management log: Transmit the log of all asset sensors, which is generated when there are changes made to asset tags and asset sensors, including asset tag connection or disconnection events.
 6. If "Asset management information" is selected in the above step, specify the asset sensor(s) whose log to send. The BCM2 has only one FEATURE port so only one asset sensor is available.
 - To specify the asset sensor, select it in the Available list box and click  (Add) or  (Add All).
 - To remove the asset sensor, select it in the Selected list box and click  (Remove) or  (Remove All).
 7. Click OK.

Resetting All Active Energy

You can reset the active energy readings of all connected panels and power meters at a time.

Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

► **To reset active energy readings of all panels:**

1. Click the PMC folder to to open the PMC page.

*Note: This folder's name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Reset All Active Energy Counters.
3. Click Yes on the confirmation message. The "Active Energy" readings of all panels are now reset to 0 (zero) Wh.

*Tip: To reset a power meter's active energy, see **Power Meter Management** (on page 112). To reset a branch circuit's active energy, see **Panel Branch Circuits Operations** (on page 109). To reset a panel's active energy, see **Panel Mains Circuit Management** (on page 106).*

Checking the Internal Beeper State

The internal beeper of the BCM2 always turns OFF if there are no event rules that involve this beeper.

If intended, you can set an event rule to turn on the internal beeper when a specific event occurs. See **Event Rules and Actions** (on page 153).

You can remotely check this beeper's state.

► **To check the internal beeper's state:**

1. Click the PMC folder in the left pane.

*Note: This folder's name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Locate the "Internal Beeper" section in the right pane. Either of the following states is displayed.
 - Off: The beeper is turned off.
 - Active: The beeper is turned on. A field titled "Activation reason" appears below the beeper state, indicating why the beeper sounds an alarm.

For example, if the internal beeper is turned on because of a specific event rule "BBB," the BCM2 shows the following "Activation reason:"

```
Event Action triggered by rule: BBB
```

User Management

The BCM2 is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's permissions. See **Setting Up Roles** (on page 101).

Tip: By default, multiple users can log in simultaneously using the same login name.

Creating a User Profile

► **To create a user profile:**

1. Choose User Management > Users. The Manage Users dialog appears.
2. Click New. The Create New User dialog appears.
3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to the BCM2. <ul style="list-style-type: none"> ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	<ul style="list-style-type: none"> ▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address <ul style="list-style-type: none"> ▪ Up to 64 characters ▪ Case sensitive

4. Select the Enabled checkbox. Enabled users can log in to the BCM2 device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.
6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
 - a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

*Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring SNMP Settings** (on page 72).*

- b. Set up SNMPv3 parameters if enabling the SNMPv3 access permission.

Field	Description
Security Level	<p>Click the drop-down arrow to select a preferred security level from the list:</p> <ul style="list-style-type: none"> ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	<p><i>This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.</i></p> <p>When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.</p>
Authentication Pass Phrase	<p>Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled.</p> <p>The pass phrase must consist of 8 to 32 ASCII printable characters.</p>
Confirm Authentication Pass Phrase	<p>Re-type the same authentication pass phrase for confirmation.</p>
Use Authentication Pass Phrase as Privacy Pass Phrase	<p><i>This checkbox is configurable only if AuthPriv is selected.</i></p> <p>When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.</p>
Privacy Pass Phrase	<p>Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled.</p> <p>The pass phrase must consist of 8 to 32 ASCII printable characters.</p>
Confirm Privacy Pass Phrase	<p>Re-type the same privacy pass phrase for confirmation.</p>
Authentication Protocol	<p>Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available:</p> <ul style="list-style-type: none"> ▪ MD5 ▪ SHA-1 (default)

Field	Description
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: <ul style="list-style-type: none"> ▪ DES (default) ▪ AES-128

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See **Changing SSH Settings** (on page 70).
 - a. Open the SSH public key with a text editor.
 - b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.
8. Click the Roles tab to determine the permissions of the user.
9. Select one or multiple roles by selecting corresponding checkboxes.
 - The Admin role provides full permissions.
 - The Operator role provides limited permissions for frequently-used functions. See **Setting Up Roles** (on page 101) for the scope of permissions. This role is selected by default.
 - If no roles meet your needs, you can:
 - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See **Modifying a Role** (on page 102).
 - *Create a new role by clicking the Manage Roles button:* See **Creating a Role** (on page 101).

Note: With multiple roles selected, a user has the union of all roles' permissions.

10. To change any measurement units displayed in the web interface and command line interface for this new user, click the Preferences tab, and do any of the following:
 - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
 - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
 - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

A Pascal is equal to one newton per square meter. Psi stands for pounds per square inch.

*Note: The measurement unit change only applies to the web interface and command line interface. Users can change the measurement units at any time by setting up their own user preferences. See **Setting Up Your Preferred Measurement Units** (on page 100).*

Modifying a User Profile

You can change any user profile's information except for the user name.

► **To modify a user profile:**

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Make all necessary changes to the information shown.

To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.

5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of **Creating a User Profile** (on page 96).
6. To change the permissions, click the Roles tab and do one of these:
 - Select or deselect any role's checkbox.
 - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See **Modifying a Role** (on page 102).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

Note: The measurement unit change only applies to the web interface and command line interface.

8. Click OK.

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

► **To delete user profiles:**

1. Choose User Management > Users. The Manage Users dialog appears.

2. Select the user you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Setting Up Your Preferred Measurement Units

The measurement units used in your BCM2 user interfaces can be changed according to your own preferences regardless of the permissions you have.

*Tip: Preferences can also be changed by administrators for specific users from the Preferences tab of the Manage Users dialog. See **Creating a User Profile** (on page 96).*

*Note: The measurement unit change only applies to the web interface and command line interface. Setting your preferences does not change the default measurement units, which apply to all users before any individual user or the administrator sets preferred measurement units on a per-user basis. See **Setting Default Measurement Units** (on page 82) for information on changing default measurement units.*

► **To change the measurement units applied to your BCM2 user interfaces:**

1. Choose User Management > User Preferences. The Setup User Preferences dialog opens.
2. Update any of the following as needed:
 - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
 - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
 - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.
3. Click OK.

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

The BCM2 is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:
 - Change PMC, PMB, & PMM Configuration
 - Acknowledge Alarms
 - View Event Settings
 - View Local Event Log
 - Change Own Password

The Operator role is assigned to a newly created user profile by default. See **Creating a User Profile** (on page 96).

Permissions

- Change PMC, PMB, & PMM Configuration
 - Configuring, editing, and deleting a power meter
 - Configuring, editing, and deleting a panel (BCM)
 - Creating, editing and deleting a circuit
 - Reset active energy counters
- Acknowledge Alarms
- View Event Settings
- View Local Event Log
- Change Own Password

Creating a Role

Create a new role when you need a new combination of permissions.

► **To create a role:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.

3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
 - a. Click Add. The "Add Privileges to new Role" dialog appears.
 - b. Select the permission you want from the Privileges list.
 - c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.
 - d. Click Add to add the selected permission (and arguments if any).
 - e. Repeat Steps a to d until you add all necessary permissions.
6. Click OK.

Now you can assign the new role to any users. See **Creating a User Profile** (on page 96) or **Modifying a User Profile** (on page 99).

Modifying a Role

You can change an existing role's settings except for the name.

► **To modify a role:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to modify by clicking it.
3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.

4. Modify the text shown in the Description field if necessary.
5. To change the permissions, click the Privileges tab.

Note: You cannot change the Admin role's permissions.

6. To delete any permissions, do this:
 - a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - b. Click Delete.
7. To add any permissions, do this:

- a. Click Add. The "Add Privileges to Role XXX" dialog appears, where XXX is the role name.
 - b. Select the permission you want from the Privileges list.
 - c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.
 - d. Click Add to add the selected permission (and arguments if any).
 - e. Repeat Steps a to d until you add all necessary permissions.
8. To change a specific permission's arguments, do this:
 - a. Select the permission by clicking it.
 - b. Click Edit. The "Edit arguments of privilege XXX" dialog appears, where XXX is the privilege name.

Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

- c. Select the argument you want. You can make multiple selections.
 - d. Click OK.
9. Click OK.

Deleting a Role

You can delete any role other than the Admin role.

► **To delete a role:**

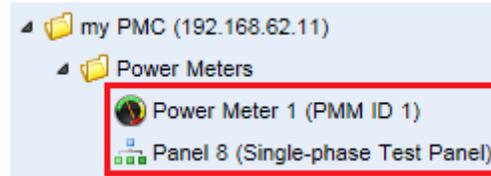
1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Meter, Panel, and Branch Circuit Monitoring and Management

To view or manage the connected panels and power meters, click the desired one under the Power Meters folder in the PMC Explorer pane.



*Note: For information on creating panels and/or power meters, see **Configuring Power Meters and Branch Circuit Monitors** (on page 5).*

Viewing the Panel Data

After selecting a panel in the PMC Explorer pane, the panel page opens. This page comprises two sections - Panel Mains Circuit and Panel Branch Circuits.

*Note: To make changes to mains and branch circuits settings, or reset active energy, see **Panel Mains Circuit Management** (on page 106) and **Panel Branch Circuits Operations** (on page 109).*

► Panel Mains Circuit:

The Panel Mains Circuit section shows the readings of each phase, such as each phase's RMS voltage readings of Line-Line and/or Line-Neutral.

Type	Total		Phase A		Phase B		Phase C	
	Value	State	Value	State	Value	State	Value	State
RMS Voltage (L-L)	213.3 V	normal	214.5 V	normal	216.4 V	normal	213.3 V	normal
RMS Current	0.00 A	normal						
Phase Angle			0.0 °	normal	0.0 °	normal	0.0 °	normal

Reset Active Energy

Panel Mains Circuit columns

①	Sensor type.
---	--------------

Panel Mains Circuit columns	
②	Sensor data summary, including: <ul style="list-style-type: none"> Total of all phases' readings, or the minimum or maximum value of specific sensors Sensor state
③	This sensor's data for phase A, including: <ul style="list-style-type: none"> Phase A reading Phase A state
④	This sensor's data for phase B, including: <ul style="list-style-type: none"> Phase B reading Phase B state
⑤	This sensor's data for phase C, including: <ul style="list-style-type: none"> Phase C reading Phase C state

► **Panel Branch Circuits:**

The Panel Branch Circuits section shows a list of branch circuits and their sensor data. Unlike the Panel Mains Circuit section, the branch circuit section does NOT show each phase's readings or state.

①	②	③	④	⑤	⑥	⑦	⑧
Position	Phase	Circuit Name	Rating	CT #	V	A	Φ
1	A	LLN	20 A	1	205.2 V	0.00 A	0.0 °
3	B					0.00 A	0.0 °
5	C	LLN	20 A	5	205.4 V	0.00 A	0.0 °
7	A					0.00 A	0.0 °
9	B	LLN	20 A	9	207.8 V	0.00 A	0.0 °
11	C					0.00 A	0.0 °

Panel Branch Circuits columns	
①	Branch circuit position.
②	Phase A, B or C of the branch circuit.

Panel Branch Circuits columns	
③	Branch circuit name.
④	Branch circuit rating.
⑤	CT ID number.
⑥	Branch circuit RMS voltage, which is the <i>minimum</i> of Line-Line or Line-Neutral RMS voltage readings. NO alerts will be available for a branch circuit's RMS voltage even though you have set the voltage thresholds for it.
⑦	Branch circuit RMS current.
⑧	Branch circuit phase angle.

*Note: Displayed columns of the Panel Branch Circuits section may be impacted by the "Select Readings" settings in the Panel Mains Circuit section. See **Panel Mains Circuit Management** (on page 106).*

Panel Mains Circuit Management

This section introduces the operations for the Panel Mains Circuit section. For information on the Panel Mains Circuit section's sensor data, see **Viewing the Panel Data** (on page 104).

Panel Configuration Delete Panel Select Readings ▾ Alarms Close								
Panel Mains Circuit								
Type	Total		Phase A		Phase B		Phase C	
	Value	State	Value	State	Value	State	Value	State
RMS Voltage (L-L)	213.3 V	normal	214.5 V	normal	216.4 V	normal	213.3 V	normal
RMS Current	0.00 A	normal						
Phase Angle			0.0 °	normal	0.0 °	normal	0.0 °	normal

Reset Active Energy

► Panel Configuration:

This button triggers the panel setup dialog.

Panel 1 Setup

Settings

Name:

Type:

Main Circuit

Circuit Rating (A):

Phase CT Present

Phase CT Rating (A):

Neutral CT Present

Neutral CT Rating (A):

Earth CT Present

Earth CT Rating (A):

Modbus

Enable Modbus Access

Modbus Address:

Threshold Configuration

Sensor	Lower Critical	Lower Warning	Upper Warning	Upper Critical
RMS Voltage	<input type="checkbox"/> (0.0 V)			
Line Frequency	<input type="checkbox"/> (0.00 Hz)			
RMS Current	<input type="checkbox"/> (0.00 A)			
Active Power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- You can change the panel's settings. For details of each field, see **Configure Panel Mains Circuit** (on page 7).
- To enable the Modbus access to this panel, select the Enable Modbus Access checkbox, and assign a "unique" Modbus address to the panel.

This Modbus address must be different from that of the main controller, any panel or power meter module connected to this BCM2, or the BCM2 does NOT allow you to save this dialog.

If Modbus/RTU is enabled, make sure this Modbus address is also different from those of other devices on the same Modbus RTU bus.

For details on Modbus, see **Configuring Modbus TCP and/or RTU** (on page 74).

- You can configure power thresholds for this panel. For details, see **Setting Power Thresholds** (on page 114).

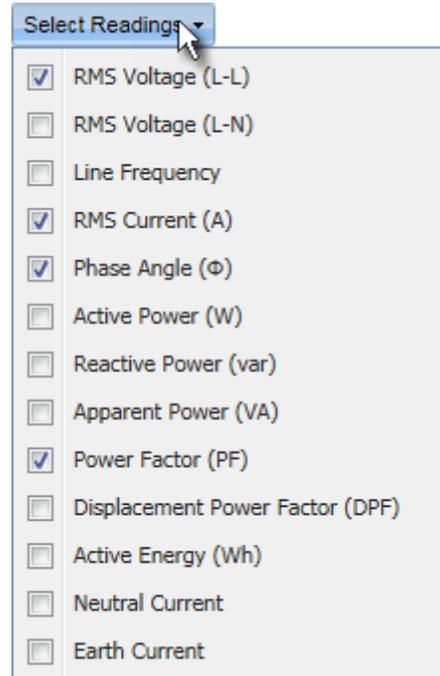
► **Delete Panel:**

The button deletes this panel.

► **Select Readings:**

If you want to view more readings of the selected panel's mains circuit, click the Select Readings button to select additional power readings, such as line frequency, active power and active energy.

Note that the changes made to the selected readings may also result in the display or hiding of some readings on the Panel Branch Circuits section if branch circuits support the selected/deselected readings.



► **Alarms:**

The button configures the power thresholds for multiple or all branch circuits at a time. See **Bulk Configuration for Branch Circuit Thresholds** (on page 121).

► **Reset Active Energy:**

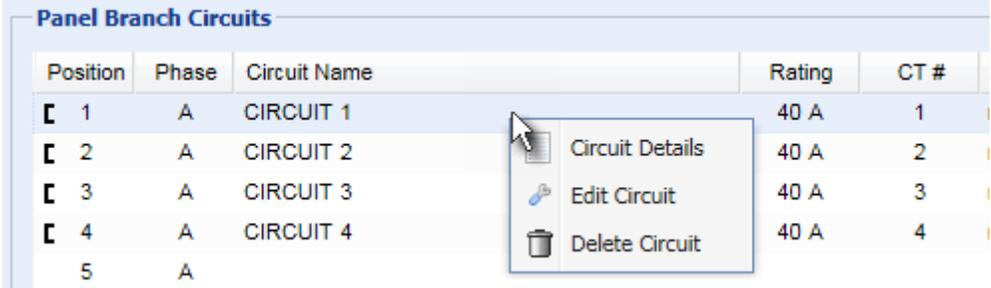
The button resets this panel's active energy reading to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

*Tip: To reset all active energy readings simultaneously, see **Resetting All Active Energy** (on page 94). To reset a branch circuit's active energy, see **Panel Branch Circuits Operations** (on page 109). To reset a Power Meter's active energy, see **Power Meter Management** (on page 112).*

Panel Branch Circuits Operations

This section introduces the operations for the Panel Branch Circuits section.

To manage existing branch circuits, simply click the desired branch circuit. Three commands as shown below appear.



The screenshot shows a table titled "Panel Branch Circuits" with the following columns: Position, Phase, Circuit Name, Rating, and CT #. The table contains five rows of data. A context menu is open over the first row (Circuit 1), showing three options: "Circuit Details", "Edit Circuit", and "Delete Circuit".

Position	Phase	Circuit Name	Rating	CT #
1	A	CIRCUIT 1	40 A	1
2	A	CIRCUIT 2	40 A	2
3	A	CIRCUIT 3	40 A	3
4	A	CIRCUIT 4	40 A	4
5	A			

*Note: For information on creating panel branch circuits, see **Configure Panel Branch Circuits** (on page 8). For information on the Panel Branch Circuits section's sensor data, see **Viewing the Panel Data** (on page 104).*

► **Circuit Details:**

A circuit page showing the circuit readings and detailed information opens. You can click one of the following buttons on the circuit page.

- Setup: This button triggers the circuit's setup dialog. See the following description for the Edit Circuit command.
- Delete Circuit: This button removes this circuit.

- **Reset Active Energy:** This button resets this circuit's active energy to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

*Tip: To reset all active energy readings simultaneously, see **Resetting All Active Energy** (on page 94). To reset a panel's active energy, see **Panel Mains Circuit Management** (on page 106). To reset a power meter's active energy, see **Power Meter Management** (on page 112).*

► **Edit Circuit:**

A circuit setup dialog appears.

You can change the circuit's settings. For details of each field, see **Configure Panel Branch Circuits** (on page 8).

Besides, you can configure power thresholds for this circuit. For details, see **Setting Power Thresholds** (on page 114).

Note: NO alerts will be available for a branch circuit's RMS voltage even though you have set the voltage thresholds for it.

► **Delete Circuit:**

Select Delete Circuit to remove this circuit.

Viewing the Power Meter Data

Separate power meter modules managed by your PMC are listed in the Power Meters folder. In the PMC Explorer pane, select a power meter shown under the Power Meters folder. The Power Meter page opens with a list of sensor data and readings.

This page shows the readings of each phase, such as each phase's RMS voltage readings of Line-Line and/or Line-Neutral.

*Note: To make changes to settings, or reset active energy, see **Power Meter Management** (on page 112).*

Type ①	② Total		③ Phase A		④ Phase B		⑤ Phase C	
	Value	State	Value	State	Value	State	Value	State
RMS Voltage (L-L)	211.3 V	normal	212.1 V	normal	212.6 V	normal	211.3 V	normal
RMS Voltage (L-N)			122.0 V	normal	122.8 V	normal	122.4 V	normal
Line Frequency	59.99 Hz	normal						
RMS Current	0.48 A	normal	0.26 A	normal	0.26 A	normal	0.48 A	normal

Power Meter columns

①	Sensor type.
②	Sensor data summary, including: <ul style="list-style-type: none"> Total of all phases' readings, or the minimum or maximum value of specific sensors Sensor state
③	This sensor's data for phase A, including: <ul style="list-style-type: none"> Phase A reading Phase A state
④	This sensor's data for phase B, including: <ul style="list-style-type: none"> Phase B reading Phase B state
⑤	This sensor's data for phase C, including: <ul style="list-style-type: none"> Phase C reading Phase C state

Power Meter Management

This section introduces the operations for a power meter module. For information on the power meter's sensor data, see **Viewing the Power Meter Data** (on page 111).

Power Meter Configuration Delete Power Meter Close

Sensors

Type	Total		Phase A		Phase B		Phase C	
	Value	State	Value	State	Value	State	Value	State
RMS Voltage (L-L)	209.6 V	normal	209.9 V	normal	210.7 V	normal	209.6 V	normal
RMS Voltage (L-N)			120.9 V	normal	121.5 V	normal	121.4 V	normal
Line Frequency	59.98 Hz	normal						
RMS Current	0.26 A	normal	0.24 A	normal	0.00 A	normal	0.20 A	normal
Phase Angle			0.0 °	normal	0.0 °	normal	-18.4 °	normal
Active Power	18 W	normal	12 W	normal	0 W	normal	6 W	normal
Reactive Power	-2 var	normal	0 var	normal	0 var	normal	-2 var	normal
Apparent Power			31 VA	normal	0 VA	normal	24 VA	normal
Power Factor			0.38	normal	1.00	normal	0.25	normal
Displacement Power...			1.00	normal	1.00	normal	0.95	normal
Active Energy	1266 Wh	normal	1240 Wh	normal	0 Wh	normal	26 Wh	normal
Neutral Current		unavailable						
Earth Current		unavailable						

Reset Active Energy

► Power Meter Configuration:

This button triggers the Power Meter setup dialog.

Power Meter 1 Setup

Settings

Name:

Type:

Main Circuit

Circuit Rating (A):

Phase CT Present

Phase CT Rating (A):

Neutral CT Present

Neutral CT Rating (A):

Earth CT Present

Earth CT Rating (A):

Modbus

Enable Modbus Access

Modbus Address:

Threshold Configuration

Sensor	Lower Critical	Lower Warning	Upper Warning	Upper Critical
RMS Voltage	<input type="checkbox"/> (0.0 V)			
Line Frequency	<input type="checkbox"/> (0.00 Hz)			
RMS Current	<input type="checkbox"/> (0.00 A)			
Active Power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- You can change a power meter's settings. For details of each field, see **Configure Power Meter** (on page 6).
- To enable the Modbus access to this power meter, select the Enable Modbus Access checkbox, and assign a "unique" Modbus address to the power meter.

This Modbus address must be different from that of the main controller, any panel or power meter module connected to this BCM2, or the BCM2 does NOT allow you to save this dialog.

If Modbus/RTU is enabled, make sure this Modbus address is also different from those of other devices on the same Modbus RTU bus.

For details on Modbus, see **Configuring Modbus TCP and/or RTU** (on page 74).

- You can configure power thresholds for this power meter. For details, see **Setting Power Thresholds** (on page 114).

▶ **Delete Power Meter:**

The button deletes this power meter.

▶ **Reset Active Energy:**

The button resets the power meter's active energy to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

*Tip: To reset all active energy readings simultaneously, see **Resetting All Active Energy** (on page 94). To reset a branch circuit's active energy, see **Panel Branch Circuits Operations** (on page 109). To reset a panel's active energy, see **Panel Mains Circuit Management** (on page 106).*

Setting Power Thresholds

Setting and enabling the thresholds causes the BCM2 to generate alert notifications when it detects that any component's power state crosses the thresholds. See **The Yellow- or Red-Highlighted Sensors** (on page 50).

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning level.
- Upper and Lower Critical thresholds indicate the sensor reading enters the critical level.

To avoid generating a large amount of alert events, you can set the assertion timeout and deassertion hysteresis.

*Note: After setting the thresholds, remember to configure event rules. See **Event Rules and Actions** (on page 153).*

Setting a Sensor's Thresholds

You can set the thresholds for a branch circuit sensor or a mains circuit sensor so that the alerts are generated when the sensor's reading crosses the thresholds. See **The Yellow- or Red-Highlighted Sensors** (on page 50).

Threshold Configuration					
Sensor	Lower Critical	Lower Warning	Upper Warning	Upper Critical	
RMS Voltage	<input type="checkbox"/> (0.0 V)	▲			
Line Frequency	<input type="checkbox"/> (0.00 Hz)				
RMS Current	<input type="checkbox"/> (0.00 A)	▼			
Active Power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

► To set power thresholds for a sensor:

1. Trigger the panel or circuit setup dialog. See **Panel Mains Circuit Management** (on page 106) or **Panel Branch Circuits Operations** (on page 109).
2. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
3. Click Edit or double-click the desired sensor. A threshold setup dialog appears.
4. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
 - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
 - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
5. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See **"To De-assert" and Deassertion Hysteresis** (on page 119).
6. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 117).
7. Click OK in the threshold setup dialog to retain the changes.
8. To set the thresholds for other sensors, repeat Steps 2 to 7.
9. Click OK.

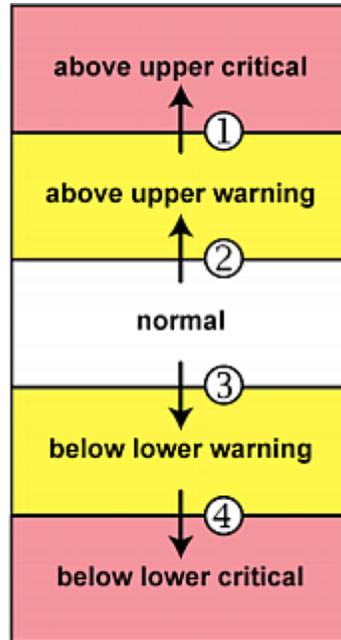
Important: The final step is required or the threshold changes are not saved.

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the BCM2 asserts a state for it whenever a bad state change occurs.

► **Assert a state:**

To assert a state is to announce a "worse" new state. Below are bad state changes that cause the BCM2 to assert.



1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

► **Assertion Timeout:**

In the threshold setup dialog, the Assertion Timeout field impacts the "assertion" action. It determines how long a sensor must be in the "worse" new state before the BCM2 turns on the "assertion" action. If that sensor changes its state again within the specified wait time, the BCM2 does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).

Setup Sensor XXX

Lower Critical :

Lower Warning :

Upper Warning :

Upper Critical :

Deassertion Hysteresis :

Assertion Timeout :

OK Cancel

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Because the BCM2 measures each sensor every second, timing of a sample is equal to a second.

► **How "Assertion Timeout" is helpful:**

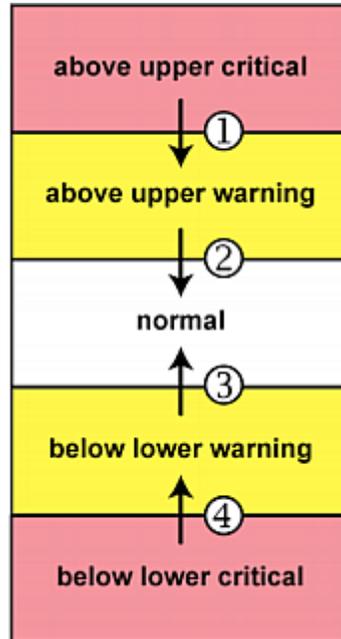
If you have created an event rule that instructs the BCM2 to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's reading fluctuates around a certain threshold.

"To De-assert" and Deassertion Hysteresis

After the BCM2 asserts a worse state for a sensor, it may de-assert the same state later on.

► **To de-assert a state:**

To de-assert a state is to announce the end of the previously asserted worse state. Below are good state changes that cause the BCM2 to de-assert the previous state.



1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

► **Deassertion Hysteresis:**

In the threshold settings dialog, the Deassertion Hysteresis field determines a new level to turn on the "deassertion" action.

Lower Critical :	<input checked="" type="checkbox"/>	<input type="text"/>
Lower Warning :	<input checked="" type="checkbox"/>	<input type="text"/>
Upper Warning :	<input checked="" type="checkbox"/>	<input type="text"/>
Upper Critical :	<input checked="" type="checkbox"/>	<input type="text"/>
Deassertion Hysteresis :	<input type="checkbox"/>	<input type="text"/>
Assertion Timeout :	<input type="checkbox"/>	<input type="text"/>

OK Cancel

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the BCM2 to de-assert the worse state for a sensor only when that sensor's reading hits the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The value of the decrease or increase is exactly the hysteresis value.

For example:

If Deassertion Hysteresis = 2,

- Upper Critical = 33, so its "deassertion" level = $33 - 2 = 31$.
- Upper Warning = 25, so its "deassertion" level = $25 - 2 = 23$.
- Lower Critical = 10, so its "deassertion" level = $10 + 2 = 12$.
- Lower Warning = 18, so its "deassertion" level = $18 + 2 = 20$.

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

► **How "Deassertion Hysteresis" is helpful:**

If you have created an event rule that instructs the BCM2 to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's reading fluctuates around a certain threshold.

Bulk Configuration for Branch Circuit Thresholds

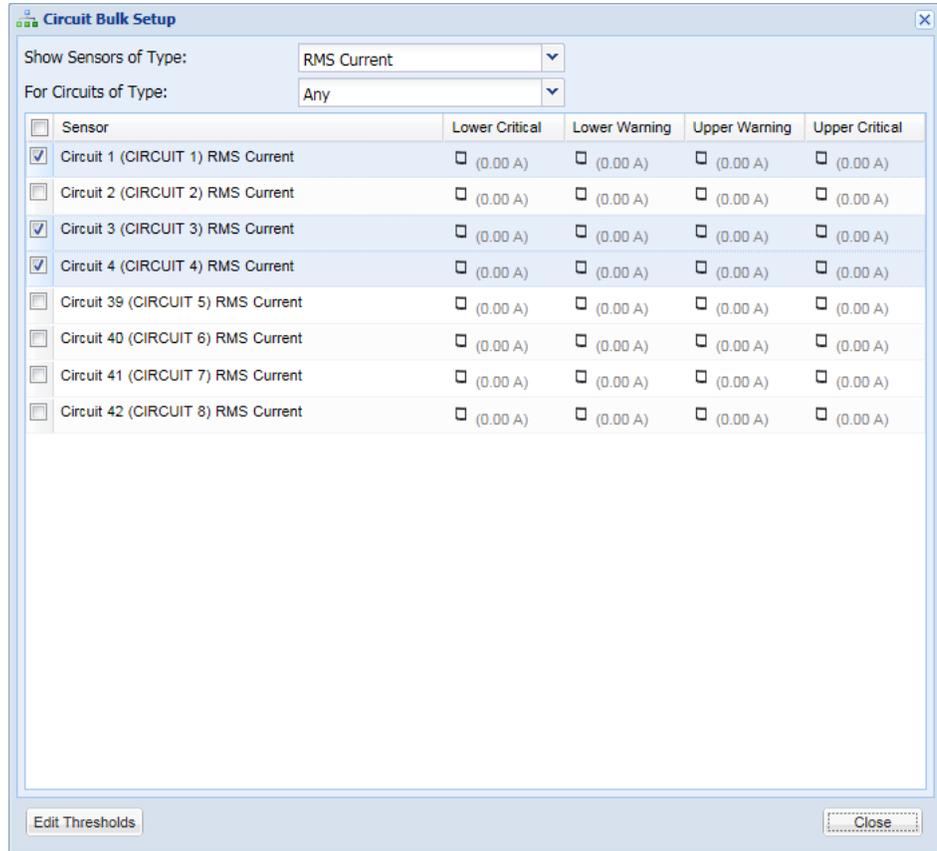
The BCM2 allows you to set power thresholds for multiple branch circuits at a time to save your time.

*Note: To set the power thresholds for a branch circuit, see **Setting a Sensor's Thresholds** (on page 115).*

► **To configure thresholds, deassertion hysteresis and assertion timeout for multiple branch circuits:**

1. Select a panel to open a panel page, and then click Alarms. See **Panel Mains Circuit Management** (on page 106).
2. The Circuit Bulk Setup dialog appears, with a list of available branch circuits.
3. Select the desired branch circuits by having their corresponding checkboxes selected.
 - To select all, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.

- To select partial branch circuits, click the corresponding checkboxes of those branch circuits.



- To deselect any branch circuit, just click their checkboxes once again.
4. Click Edit Thresholds. The threshold bulk setup dialog appears.
 5. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
 - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
 - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
 6. To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See **"To De-assert" and Deassertion Hysteresis** (on page 119).
 7. To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 117).
 8. Click OK.

Access Security Control

The BCM2 provides tools to control access. You can enable the internal firewall, create firewall rules, and create login limitations.

*Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up a TLS Certificate** (on page 138) and **Setting Up External Authentication** (on page 144).*

Forcing HTTPS Encryption

You can force all accesses to the BCM2 via HTTP to be redirected to HTTPS. See **Changing HTTP(S) Settings** (on page 69).

Configuring the Firewall

The BCM2 has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the BCM2 device or to prevent them from receiving any data from the BCM2.

The BCM2 allows you to configure the firewall rules for inbound and outbound traffic respectively. Inbound rules control the data sent to the BCM2, and outbound rules control the data sent from the BCM2.

By default the firewall is disabled.

► **To configure the firewall:**

1. Enable the firewall. See **Enabling the Firewall** (on page 123).
2. Set the default policy. See **Changing the Default Policy** (on page 124).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See **Creating Firewall Rules** (on page 125).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device.

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

► **To enable the BCM2 firewall:**

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.

2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable IPv4 Access Control checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable IPv6 Access Control checkbox.
4. Click OK.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from/to all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access the BCM2 or receive any data from the BCM2.

You can change the default policy to Drop or Reject, in which case traffic to/from all IP addresses is discarded except the IP addresses accepted by a specific rule.

Default policies for inbound and outbound traffic can be different.

► To change the default policy for inbound traffic:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
 - a. Click the IPv4 tab if necessary.
 - b. Ensure the Enable IPv4 Access Control checkbox is selected.
 - c. Locate the Default Policy field in the Inbound Rules section.
 - d. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
 - Accept: Accepts traffic from all IPv4 addresses.
 - Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
 - Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.
3. To determine the default policy for IPv6 addresses:
 - a. Click the IPv6 tab.
 - b. Ensure the Enable IPv6 Access Control checkbox is selected.
 - c. Locate the Default Policy field in the Inbound Rules section.
 - d. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.

- Accept: Accepts traffic from all IPv6 addresses.
 - Drop: Discards traffic from all IPv6 addresses, without sending any failure notification to the source host.
 - Reject: Discards traffic from all IPv6 addresses, and an ICMP message is sent to the source host for failure notification.
4. Click OK. The new default policy is applied.

► **To change the default policy for outbound traffic:**

Locate the Outbound Rules section on the IPv4 or IPv6 tab and then follow the above procedure to set up its Default Policy field by selecting one of the following options.

- Accept: Permits traffic sent from the BCM2 to all IP addresses.
- Drop: Discards traffic sent from the BCM2 to all IP addresses, without sending any failure notification to the destination host.
- Reject: Discards traffic sent from the BCM2 to all IP addresses, and an ICMP message is sent to the destination host for failure notification.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic to/from the BCM2, based on the IP address of the host sending or receiving the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

When traffic reaches or is sent from the BCM2 device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the BCM2.

- **Subnet mask is required.**

When typing the IP address, you must specify BOTH the address and a subnet mask. For example, to specify a single address in a Class C network, use this format:

x.x.x.x/24

where /24 = a subnet mask of 255.255.255.0.

To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IPv4 addresses entered are within the scope.

► **To create firewall rules:**

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Click the IPv4 tab for creating IPv4 firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. To set rules for inbound traffic, go to the Inbound Rules section. To set rules for outbound traffic, go to the Outbound Rules section.
5. Create specific rules. See the table for different operations.

Action	Procedure
Add a rule to the end of the rules list	<ul style="list-style-type: none"> ▪ Click Append. The "Append new Rule" dialog appears. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. <ul style="list-style-type: none"> ▪ Accept: Accepts traffic from/to the specified IP address(es). ▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host. ▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification. ▪ Click OK. <p>The system automatically numbers the rule.</p>

Action	Procedure
Insert a rule between two existing rules	<ul style="list-style-type: none">▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.▪ Click Insert. The "Insert new Rule" dialog appears.▪ Type an IP address and subnet mask in the IP/Mask field.▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.<ul style="list-style-type: none">▪ Accept: Accepts traffic from/to the specified IP address(es).▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.▪ Click OK. <p>The system inserts the rule and automatically renumbers the following rules.</p>

- When finished, the rules appear in the Configure IP Access Control Settings dialog.

Configure IP Access Control Settings

IPv4 | IPv6

Enable IPv4 Access Control:

Inbound Rules

Default Policy:

#	IP/Mask	Policy
1	192.168.80.80/32	ACCEPT
2	192.255.255.255/24	ACCEPT
3	192.155.123.123/32	DROP

Append Insert Edit Delete

Outbound Rules

Default Policy:

#	IP/Mask	Policy
1	192.168.88.88/24	REJECT

Append Insert Edit Delete

OK Cancel

- Click OK. The rules are applied.

Editing Firewall Rules

When an existing firewall rule requires updates of IP address range and/or policy, modify them accordingly.

► **To modify a firewall rule:**

- Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.

2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK.
8. Click OK to quit the Configure IP Access Control Settings dialog, or the changes are lost.

Sorting Firewall Rules

The rule order determines which one of the rules matching the same IP address is performed.

► To sort the firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click  or  to move the selected rule up or down until it reaches the desired location.
6. Click OK.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

► To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.

3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
7. Click OK.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the BCM2 and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to the BCM2 and fail authentication before the user is blocked.

Note that this function applies only to local authentication instead of authentication through external AA servers.

*Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a local connection. See **Unblocking a User** (on page 376).*

► To enable user blocking:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.
3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user is blocked from accessing the BCM2 device.
5. To determine how long the user's login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
 - Infinite: This option sets no time limit on blocking the login.

- X min: This type of option sets the time limit to X minutes, where X is a number.
- X h: This type of option sets the time limit to X hours, where X is a number.
- 1 d: This option sets the time limit to 1 day.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.

6. Click OK.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and how long users are permitted to stay idle before being forced to log out.

► To enable login limitations:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the Login Limitations section.
3. To prevent more than one person from using the same login at the same time, select the "Prevent concurrent login with same username" checkbox.
4. To adjust how long users can remain idle before they are forcibly logged out by the BCM2, select a time option in the Idle Timeout Period field. The default is 10 minutes.
 - X min: This type of option sets the time limit to X minutes, where X is a number.
 - X h: This type of option sets the time limit to X hours, where X is a number.
 - 1 d: This option sets the time limit to 1 day.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.

5. Click OK.

Tip: Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the BCM2.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the BCM2 device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

► **To force users to create strong passwords:**

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of restricted passwords in history	= 5

Note: The maximum password length accepted by the BCM2 is 64 characters.

3. Make necessary changes to the default settings.
4. Click OK.

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default is to disable this feature.

► **To force users to change passwords regularly:**

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Password Aging checkbox to enable the password aging feature.
3. To determine how often users are requested to change their passwords, select a number of days in the Password Aging Interval field. Users are required to change their password every time when that number of days has passed.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "9 d" to set the password aging time to 9 days.

4. Click OK.

Enabling and Editing the Security Banner

Use the BCM2 restricted service agreement (security banner) if you want to require users to read and accept a security agreement when they log in to the BCM2.

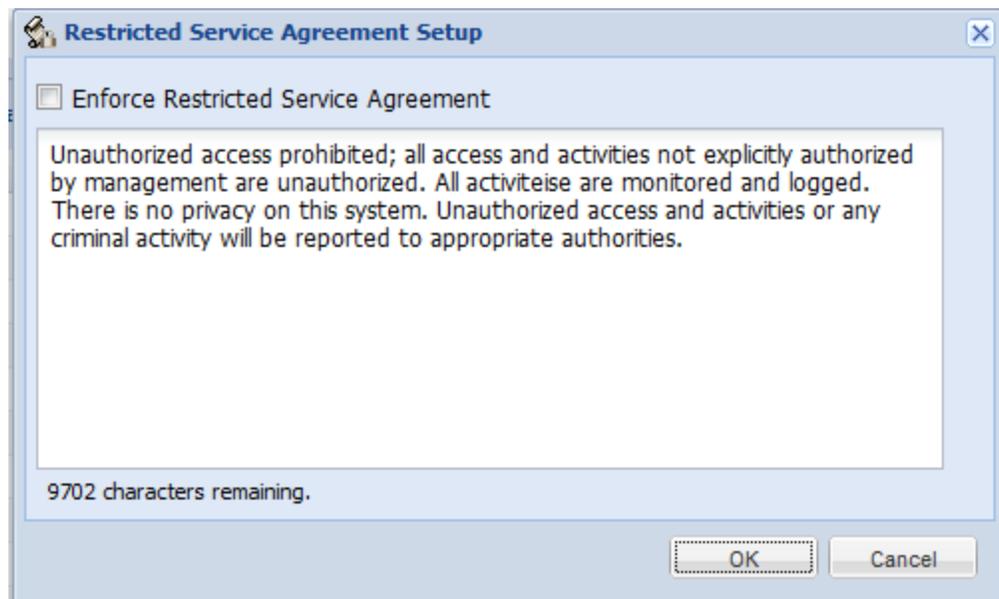
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

A maximum of 10,000 characters can be entered or pasted into the security banner.

If a user declines the agreement, they cannot log in. An event notifying you if a user has accepted or declined the agreement can be created. See **Default Log Messages** (on page 180)

► To enable the service agreement:

1. Click Device Services > Security > Restricted Service Agreement Banner. The Restricted Service Agreement Setup dialog opens.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit the text or replace it as needed.
4. Click OK.



If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the BCM2. Do either of the following, or you cannot successfully log in to the BCM2:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

Tip: To select the agreement checkbox using the keyboard, press the Space bar.

- In the CLI, type `y` when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting Up Role-Based Access Control Rules

Role-based access control rules are similar to firewall rules, except they are applied to members sharing a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

► **To set up role-based access control rules:**

1. Enable the feature. See **Enabling the Feature** (on page 134).
2. Set the default policy. See **Changing the Default Policy** (on page 135).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See **Creating Role-Based Access Control Rules** (on page 135).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

► **To enable role-based access control rules:**

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To enable the IPv4 firewall, click the IPv4 tab, and select the "Enable Role Based Access Control for IPv4" checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the "Enable Role Based Access Control for IPv6" checkbox.
4. Click OK.

Changing the Default Policy

The default policy is to accept all traffic from all IP addresses regardless of the role applied to the user.

► **To change the default policy:**

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
 - a. Click the IPv4 tab if necessary.
 - b. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected.
 - c. Select the action you want from the Default Policy drop-down list.
 - Allow: Accepts traffic from all IPv4 addresses regardless of the user's role.
 - Deny: Drops traffic from all IPv4 addresses regardless of the user's role.
3. To determine the default policy for IPv6 addresses:
 - a. Click the IPv6 tab.
 - b. Ensure the "Enable Role Based Access Control for IPv6" checkbox is selected.
 - c. Select the action you want from the Default Policy drop-down list.
 - Allow: Accepts traffic from all IPv6 addresses regardless of the user's role.
 - Deny: Drops traffic from all IPv6 addresses regardless of the user's role.
4. Click OK.

Creating Role-Based Access Control Rules

Role-based access control rules accept or drop traffic, based on the user's role and IP address. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

► **To create role-based access control rules:**

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Click the IPv4 tab for creating IPv4 firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.

3. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected on the IPv4 tab, or the "Enable Role Based Access Control for IPv6" checkbox is selected on the IPv6 tab.
4. Create specific rules:

Action	Do this...
Add a rule to the end of the rules list	<ul style="list-style-type: none"> ▪ Click Append. The "Append new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. <ul style="list-style-type: none"> ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role ▪ Click OK. <p>The system automatically numbers the rule.</p>
Insert a rule between two existing rules	<ul style="list-style-type: none"> ▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. <ul style="list-style-type: none"> ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified

Action	Do this...
	<p style="text-align: center;">role</p> <ul style="list-style-type: none"> ▪ Click OK. <p>The system inserts the rule and automatically renumbers the following rules.</p>

5. Click OK.

Editing Role-Based Access Control Rules

You can modify existing rules when these rules do not meet your needs.

► To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected on the IPv4 tab, or the "Enable Role Based Access Control for IPv6" checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK.

Sorting Role-Based Access Control Rules

Similar to firewall rules, the order of role-based access control rules determines which one of the rules matching the IP address and role is performed.

► To sort role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected on the IPv4 tab, or the "Enable Role Based Access Control for IPv6" checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click  or  to move the selected rule up or down until it reaches the desired location.

6. Click OK.

Deleting Role-Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

► **To delete a role-based access control rule:**

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected on the IPv4 tab, or the "Enable Role Based Access Control for IPv6" checkbox is selected on the IPv6 tab.
4. Select the rule to be deleted in the rules list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
7. Click OK.

Setting Up a TLS Certificate

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Having an X.509 digital certificate ensures that both parties in an TLS connection are who they say they are.

To obtain a certificate for the BCM2, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate, which you must install on the BCM2 device.

Note 1: If you are using a TLS certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

*Note 2: See **Forcing HTTPS Encryption** (on page 123) for instructions on forcing users to employ TLS when connecting to the BCM2.*

A CSR is not required in either of the following scenarios:

- You decide to generate and use a *self-signed* certificate on the BCM2 device.
- Appropriate, valid certificate and key files are already available.

Certificate Signing Request

When appropriate certificate and key files for the BCM2 are NOT available, one of the alternatives is to create a CSR and private key on the BCM2 device, and send the CSR to a CA for signing the certificate.

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your BCM2 device.

► **To create a CSR:**

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.
 - In the Subject section:

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ISO website (http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.

Field	Type this information
Common Name	The fully qualified domain name (FQDN) of your BCM2 device.
Email Address	An email address where you or another administrative user can be reached.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields. If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

- In the Key Creation Parameters section:

Field	Do this
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the BCM2 device's response.
Self Sign	For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.
Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional, and the value should be 4 to 64 characters long. The password is case sensitive, so ensure you capitalize the letters correctly.
Confirm Challenge	Type the same password again for confirmation.

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
 - a. You are prompted to open or save the file. Click Save to save it onto your computer.
 - b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
 - c. If intended, click Delete Certificate Signing Request to remove the CSR file permanently from the BCM2 device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it onto your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the BCM2 device.

► **To install the certificate:**

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. In the Certificate File field, click Browse to select the certificate file provided by the CA.
4. Click Upload. The certificate is installed on the BCM2 device.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab.

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the BCM2 device are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

► **To create and install a self-signed certificate:**

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ISO website (http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your BCM2 device.
Email Address	An email address where you or another administrative user can be reached.

Field	Type this information
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the BCM2 device's response.
Self Sign	Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear after the Self Sign checkbox is selected.

4. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.
5. You can also do any of the following:
 - Click "Install Key and Certificate" to immediately install the self-signed certificate and private key. When any confirmation and security messages appear, click Yes to continue.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab.

- To download the self-signed certificate or private key, click Download Certificate or Download Key. You are prompted to open or save the file. Click Save to save it onto your computer.
 - To remove the self-signed certificate and private key permanently from the BCM2 device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the BCM2 device resets and the login page re-opens.

Installing Existing Key and Certificate Files

If the TLS certificate and private key files are already available, you can install them directly without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a TLS certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

► **To install existing key and certificate files:**

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the BCM2 device.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab.

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

You can download the key and certificate files currently installed on the BCM2 device for backup or other operations. For example, you can install the files on a replacement BCM2 device, add the certificate to your browser and so on.

► **To download the certificate and key files from the BCM2 device:**

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. The Active SSL Certificate tab should open. If not, click it.
3. Click Download Key to download the private key file installed on the BCM2 device. You are prompted to open or save the file. Click Save to save it onto your computer.
4. Click Download Certificate to download the certificate file installed on the BCM2 device. You are prompted to open or save the file. Click Save to save it onto your computer.
5. Click Close to quit the dialog.

Setting Up External Authentication

For security purposes, users attempting to log in to the BCM2 must be authenticated. The BCM2 supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the BCM2 device
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (RADIUS) protocol

By default, the BCM2 is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user.

If you prefer external authentication, you must provide the BCM2 with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user profiles on the BCM2 in addition to providing the external AA server's data.

When configured for external authentication, all BCM2 users must have an account on the external AA server. Local-authentication-only users will have no access to the BCM2 except for the admin, who always can access the BCM2.

Only users who have the "Change Authentication Settings" permission can set up or modify the authentication settings.

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Gathering the External Authentication Information

No matter which type of external authentication is preferred, the first step is to gather the data of all external AA servers that you want to use.

Gathering the LDAP Information

It requires knowledge of your LDAP server and directory settings to configure the BCM2 for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
 - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
 - *OpenLDAP*
 - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
 - *Microsoft Active Directory® (AD)*
 - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Gathering the RADIUS Information

To configure RADIUS authentication, you need to collect the RADIUS information. If you are not familiar with the remote RADIUS information, consult your RADIUS administrator for help.

Below is the RADIUS information to gather:

- The IP address or host name of the RADIUS server
- Authentication protocol used by the RADIUS server
- Shared secret for a secure communication
- UDP authentication port used by the RADIUS server
- UDP accounting port used by the RADIUS server

Adding Authentication Servers

Add all external AA servers that you want to use to the BCM2. Later you can use the sequence of the server list to control the AA servers' access priority.

Adding LDAP Server Settings

To activate and use external LDAP/LDAPS server authentication, enable LDAP authentication and enter the information you have gathered for any LDAP/LDAPS server.

If the external LDAP/LDAPS server authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See **Viewing the Local Event Log** (on page 200).

Note: An LDAPS server refers to a TLS-secured LDAP server.

► **To add new LDAP/LDAPS server settings:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate the LDAP/LDAPS authentication.
3. Click New to add an LDAP/LDAPS AA server. The "Create new LDAP Server Configuration" dialog appears.
4. IP Address / Hostname - Type the IP address or hostname of your LDAP/LDAPS authentication server.

Important: Without the TLS encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the TLS encryption is enabled.

5. Type of LDAP Server - Choose one of the following options:
 - OpenLDAP
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
6. Security - Determine whether you would like to use Transport Layer Security (TLS) encryption, which is a cryptographic protocol that allows the BCM2 to communicate securely with the LDAPS server.

Three security options are available:

- StartTLS
- TLS

- None
7. Port (None/StartTLS) - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
 8. Port (TLS) - The default is 636. Either use the default port or specify another port. This field is enabled only when "TLS" is selected in the Security field.
 9. Enable verification of LDAP Server Certificate - Select this checkbox if you would like the BCM2 to verify the validity of the selected LDAP server certificate. For example, the BCM2 will check the certificate's validity period against the system time.
 10. CA Certificate - Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse to select the TLS CA certificate file.
 - Click Show to view the installed certificate's contents.
 - Click Remove to delete the installed certificate if it is inappropriate.
 11. Allow expired and not yet valid certificates - If a certificate has been installed, use this checkbox to determine whether the validity period of the certificate affects the authentication.
 - To always make the authentication succeed regardless of the validity period, select this checkbox.
 - To make the authentication fail when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect the checkbox.
 12. Anonymous Bind - For "OpenLDAP," use this checkbox to enable or disable anonymous bind.
 - To use anonymous bind, select this checkbox.
 - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
 13. Use Bind Credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
 - To use anonymous bind, deselect this checkbox. By default it is deselected.
 - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.
 14. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base. This information is required only when the Use Bind Credentials checkbox is selected.
 15. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required only when the Use Bind Credentials checkbox is selected.

16. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your AA server administrator for the appropriate values to enter into these fields.
17. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
 - Login name attribute (also called AuthorizationString)
 - User entry object class
 - User search subfilter (also called BaseSearch)

Note: The BCM2 will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.

18. Active Directory Domain - Type the name of the Active Directory Domain. For example, `testradius.com`. Consult with your Active Directory Administrator for a specific domain name.
19. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the BCM2 can connect to the remote authentication server successfully.

Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.

20. Click OK. The new LDAP server is listed in the Authentication Settings dialog.
21. To add additional LDAP/LDAPS servers, repeat Steps 3 to 20.
22. Click OK. The LDAP authentication is now in place.

► **To duplicate LDAP/LDAPS server settings:**

If you have added any LDAP/LDAPS server information to the BCM2, and the server you are adding shares identical or similar settings with an existing server, the most convenient way is to duplicate that LDAP/LDAPS server's data.

1. Repeat Steps 1 to 4 in the above procedure to add the LDAP/LDAPS server you want.
2. Select the "Use settings from LDAP Server" checkbox.
3. Click the drop-down arrow below the checkbox to select the LDAP/LDAPS server whose settings you want to copy.
4. Make necessary changes to the information shown.
5. Click OK.

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

More Information about AD or RADIUS Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see **LDAP Configuration Illustration** (on page 384).

For more information on RADIUS configuration, see **RADIUS Configuration Illustration** (on page 392).

Adding RADIUS Server Settings

To activate and use external RADIUS server authentication, enable RADIUS authentication and enter the information you have gathered for any RADIUS server.

► To set up RADIUS authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Radius radio button to enable the RADIUS authentication.
3. Click New to add a RADIUS AA server. The "Create new RADIUS Server Configuration" dialog appears.
4. Type the IP address or host name of the RADIUS server in the IP Address / Hostname field.
5. Select an authentication protocol in the "Type of RADIUS Authentication" field. Your choices include:
 - PAP (Password Authentication Protocol)
 - CHAP (Challenge Handshake Authentication Protocol)

CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.

6. By default, the BCM2 uses the standard RADIUS port 1812 (authentication) and 1813 (accounting). If you prefer to use non-standard ports, change the ports.
7. Type the timeout period in seconds in the Timeout field. This sets the maximum amount of time to establish contact with the RADIUS server before timing out. Default is 1 second.
8. Type the number of retries permitted in the Retries field. Default is 3.
9. Type the shared secret in the Shared Secret and Confirm Shared Secret fields. The shared secret is necessary to protect communication with the RADIUS server.

10. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the BCM2 can connect to the remote authentication server successfully.

Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.

11. Click OK. The new RADIUS server is listed in the Authentication Settings dialog.
12. To add additional RADIUS servers, repeat Steps 3 to 11.
13. Click OK. RADIUS authentication is now in place.

Sorting the Access Order

The order of the authentication server list determines the access priority of remote authentication servers. The BCM2 first tries to access the top server in the list for authentication, then the next one if the access to the first one fails, and so on until the BCM2 device successfully connects to one of the listed servers.

Note: After successfully connecting to one external authentication server, the BCM2 STOPS trying to access the remaining authentication servers in the list regardless of the user authentication result.

► **To re-sort the authentication server access list:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server whose priority you want to change.
3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK.

Testing the Server Connection

You can test the connection to any external authentication server to verify the server accessibility or the validity of the authentication settings.

► **To test the connection to an authentication server:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to test.
3. Click Test Connection to start the connection test.

Editing Authentication Server Settings

If the configuration of any external authentication server has been changed, such as the port number, you must modify the authentication settings on the BCM2 device accordingly, or the authentication fails.

▶ **To modify the external authentication configuration:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to edit.
3. Click Edit or double-click that server.
4. Make necessary changes to the information shown.
5. Click OK.

Deleting Authentication Server Settings

You can delete the settings of a specific authentication server when that server is no longer available or used for remote authentication.

▶ **To remove one or multiple authentication servers:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK.

Disabling External Authentication

When the remote authentication service is disabled, the BCM2 authenticates users against the local database stored on the BCM2 device.

▶ **To disable the external authentication service:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Local Authentication radio button.
3. Click OK.

Enabling External and Local Authentication Services

To make authentication function properly all the time - even when external authentication is not available, you can enable both the local and remote authentication services.

When both authentication services are enabled, the BCM2 follows these rules for authentication:

- When any of the remote authentication servers in the access list is accessible, the BCM2 authenticates against the connected authentication server only.
- When the connection to all remote authentication servers fails, the BCM2 allows authentication against the local database.

► **To enable both authentication services:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Make sure you have selected one external authentication radio button, such as the LDAP radio button.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of and react to a change in conditions. This event notification or reaction is an "event rule."

The BCM2 is shipped with four built-in event rules, which cannot be deleted.

- System Event Log Rule: This causes ANY event occurred to the BCM2 to be recorded in the internal log. It is enabled by default.
- System SNMP Notification Rule: This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the BCM2. It is disabled by default.
- System Tamper Detection Alarmed: This causes the BCM2 to send alarm notifications if a DX tamper sensor has been connected and the BCM2 detects that the tamper sensor enters the alarmed state.
- System Tamper Detection Unavailable: This causes the BCM2 to send alarm notifications if a DX tamper sensor has been connected and the BCM2 detects that the communication with the connected tamper sensor is lost.

If these do not satisfy your needs, you can create additional rules to respond to different events. You need the Administrator Privileges to configure event rules.

Note: Internet Explorer® 8 (IE8) does not use compiled JAVA script. When using IE8 to create or change event rules, the CPU performance may be degraded, resulting in the appearance of the connection time out message. When this occurs, click Ignore to continue.

Components of an Event Rule

An event rule defines what the BCM2 does in certain situations and is composed of two parts:

- Event: This is the situation where the BCM2 or part of it meets a certain condition. For example, the inlet's voltage exceeds the warning threshold.
- Action: This is the response to the event. For example, the BCM2 notifies the system administrator of the event and records the event in the log.

Creating an Event Rule

The best way to create a new set of event rules in sequence is to:

- Create actions for responding to one or multiple events
- Create rules to determine what actions are taken when these events occur

Creating Actions

The BCM2 comes with three built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Notification Action: This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.
- System Tamper Alarm: This action causes the BCM2 to show the alarm for the DX tamper sensor in the Alarms section of the Dashboard until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see **Alarms List** (on page 53).

Note: No IP addresses are specified in the "System SNMP Notification Action" by default so you must specify IP addresses before applying this action to any event rule.

The built-in actions cannot be deleted.

► **To create new actions:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action:

Action	Function
Execute an action group	Creates a group of actions comprising existing actions. See Action Group (on page 156).
Alarm	Requires the user to acknowledge the alert when it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See Alarm (on page 157).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See External Beeper (on page 158).

Action	Function
Log event message	Records the selected events in the internal log. See Log an Event Message (on page 159).
Push out sensor readings	Sends asset management sensor data to a remote server using HTTP POST requests. See Push Out Sensor Readings (on page 160).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See Send a Snapshot via Email (on page 160).
Send email	Emails a textual message. See Send EMail (on page 162).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See Send an SNMP Notification (on page 163).
Syslog message	Makes the BCM2 automatically forward event messages to the specified syslog server. See Syslog Message (on page 165).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See Send Sensor Report (on page 166).
Send SMS message	Sends a message to a mobile phone. See Send SMS Message (on page 168).
Internal beeper	Turns on or off the internal beeper. See Internal Beeper (on page 169).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See Record Snapshots to Webcam Storage (on page 170).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See Switch Peripheral Actuator (on page 169).

- Click OK to save the new action.

Note: If you do not click OK before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

- To create additional actions, repeat the above steps.
- Click Close to quit the dialog.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to an event rule rather than selecting all needed actions one by one per rule.

► **To create an action group:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Execute an action group.
6. To mark an action as part of the action group, select it from the Available Actions list box, and click  to move it to the Used Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To move all actions to the Used Actions list box, click . A maximum of 32 actions can be grouped.

7. To remove an action from the action group, select it from the Used Actions list box, and click  to move it to the Available Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To remove all actions, click .

8. Click OK.
9. To create additional action groups, repeat Steps 3 to 8.

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the BCM2 resends or regenerates an alert notification regularly until the alert is acknowledged or it reaches the maximum number of alert notifications.

For information on acknowledging an alarm, see **Alarms List** (on page 53).

► **To create an Alarm action:**

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Alarm.
5. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications.

- a. In the Available Actions field, select the method to send alert notifications. Available methods vary, depending on how many notification-based actions have been created.

Notification-based action types include:

- External beeper
- Syslog message
- Send email
- Send SMS message
- Internal beeper

If no appropriate actions are available, click Create New Notification Action to immediately create them.

- b. Click  to add the selected method to the Alarm Notifications list box.
- c. Repeat the above steps to add more methods if needed.
 - To remove any method from the Alarm Notifications list box, select that method and click .
6. In the Notification Options section, configure the notification-resending or -regenerating feature.

- a. To enable the notification-resending feature, select the "Enable re-scheduling of alarm notifications" checkbox. To disable this feature, deselect the checkbox.
 - b. In the "Period in Minutes" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly. You can either directly type a numeric value or click the Up/Down arrow keys to adjust the time.
 - c. In the "Max. numbers" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. If needed, you can instruct the BCM2 to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications list box. **(Optional)**
- a. In the Available Actions field, select the method to send the acknowledge notification. Available methods are identical to those for generating alarm notifications.
 - b. Click  to add the selected method to the Acknowledgment Notifications list box.
 - c. Repeat the above steps to add more methods if needed.
 - To remove any method from the Acknowledgment Notifications list box, select that method and click .
8. Click OK.

External Beeper

If an external beeper is connected to the BCM2, the BCM2 can change the beeper's behavior or status to respond to a certain event.

► To control the connected external beeper:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: External beeper.
5. From the Beeper Port drop-down list, select the port where the external beeper is connected. This port is the FEATURE port.
6. From the Beeper Action drop-down list, select an action for the external beeper to carry out.

- Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.
 - On: Turns on the external beeper so that it buzzes continuously.
 - Off: Turns off the external beeper so that it stops buzzing.
7. Click OK.

Note: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Log an Event Message

This option records the selected events in the internal log.

► To create a log event message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Log event message.
6. Click OK.

Push Out Sensor Readings

If you have connected Raritan's asset sensors to the BCM2, you can configure the BCM2 to push asset sensor data to a remote server after a certain event occurs.

Before creating this action, make sure that you have properly defined the destination servers and the sensor data type in the Data Push dialog. See **Configuring Data Push Settings** (on page 93).

*Tip: To send the asset sensor data at a regular interval, schedule this action. See **Scheduling an Action** (on page 175). Note that the "Asset management log" is generated only when there are changes made to any asset sensors or asset tags, such as connection or disconnection events.*

► To push out the sensor data:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Push out sensor readings.
6. Select a server or host which receives the asset sensor data in the Destination field.
 - If the desired destination is not available yet, go to the Data Push dialog to enter it. See **Configuring Data Push Settings** (on page 93).
7. Click OK.

Send a Snapshot via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

► To create a send snapshot via email action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.

4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send snapshots via email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

If the SMTP server settings are not configured yet, click Configure. See **Configuring SMTP Settings** (on page 92) for the information of each field.

8. Select the webcam that is capturing the images you want sent in the email.
9. Use the slide bars to increase or decrease the following:
 - Number of Snapshots - the number of snapshots to be included in the sequence of images that are taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
 - Snapshots/Mail field - the number of snapshots from the sequence to be sent at one time in the email.
 - "Time before first Snapshot (s):" - the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
 - "Time between Snapshots (s):" - the amount of time between when each snapshot is taken.
10. Click OK.

Send Email

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and BCM2 placeholders. The placeholders represent information is pulled from the BCM2 and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See **Email and SMS Message Placeholders** (on page 187) for a list and definition of available variables.

► **To configure sending emails:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

If the SMTP server settings are not configured yet, click Configure. See **Configuring SMTP Settings** (on page 92) for the information of each field. Default messages are sent based on the event. See **Default Log Messages** (on page 180) for a list of default log messages and events that trigger them.

8. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.
 - To start a new line in the text box, press Enter.

- Click the Information icon  to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See **Email and SMS Message Placeholders** (on page 187) for more details.
9. Click OK.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

► **To configure sending an SNMP notification:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send SNMP notification.
6. Select the type of SNMP notification. See either procedure below according to your selection.

► **To send SNMP v2c notifications:**

1. From the Notification Type drop-down, select SNMPv2c Trap or SNMPv2c Inform.
2. For SNMP INFORM communications, leave the resend settings at their default or:
 - a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
 - b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.

4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.

Tip: An SNMP v2c notification action only permits entering a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

► **To send SNMP v3 notifications:**

1. From the Notification Type drop-down, select SNMPv3 Trap or SNMPv3 Inform.
2. For SNMP TRAPS, the engine ID is prepopulated.
3. For SNMP INFORM communications, leave the resend settings at their default or:
 - a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
 - b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
 - a. Host name
 - b. Port number
 - c. User ID needed to access the host
 - d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. <ul style="list-style-type: none"> • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. <ul style="list-style-type: none"> • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

The BCM2 may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See **Viewing the Local Event Log** (on page 200).

► **To configure a syslog message action:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Syslog message.

6. In the "Syslog server" field, specify the IP address to which the syslog is forwarded.
7. In the Transport Protocol field, select one of the syslog protocols: TCP or UDP. The default is UDP.

Transport protocol types	Next steps
UDP	<ul style="list-style-type: none"> ▪ In the UDP Port field, specify an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol (UDP only)" checkbox if applicable.
TCP	<p>If NO TLS certificate is required, type an appropriate port number in the TCP Port field.</p> <p>If a TLS certificate is required, select the "Enable Secure Syslog over TLS" checkbox, and then do the following:</p> <ol style="list-style-type: none"> a. Specify an appropriate port number in the "TCP Port (TLS)" field. Default is 6514. b. In the CA Certificate field, click Browse to select a TLS certificate. After installing the certificate, you may: <ul style="list-style-type: none"> ▪ Click Show to view its contents. ▪ Click Remove to delete it if it is inappropriate. c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox. <ul style="list-style-type: none"> ▪ To always send the event message to the specified syslog server after a TLS certificate has been installed, select this checkbox. ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

8. Click OK.

Send Sensor Report

You may set the BCM2 so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors as listed below.

- Panel sensors, including RMS current, RMS voltage, active power, apparent power, and so on.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the BCM2, such as temperature or humidity sensors.

► **To configure a sensor report action:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.

2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send sensor report.
6. In the Destination Actions field, select the method(s) to report sensor readings or states. The number of available methods vary, depending on how many messaging actions have been created.

The messaging action types include:

- Log event message
 - Syslog message
 - Send email
 - Send SMS message
- a. If no messaging actions are available, click Create New Destination Action to immediately create them.
 - b. To select any method, select it in the right list box, and click  to move it to the left list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To select all methods, simply click .
 - c. To delete any method, select it in the left list box, and click  to move it back to the right list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To remove all methods, simply click .
7. In the Available Sensors field, select the desired sensor.
 - a. Select the sensor type from the field to the left.
 - b. Select the specific sensor from the field to the right.
 - c. Click  to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

8. To report additional sensors simultaneously, repeat the above step to add more sensors.
 - To remove any sensor from the Report Sensors list box, select it and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

9. To immediately send out the sensor report, click Send Report Now. A message appears, indicating whether the sensor report is sent successfully.
10. To save this action, click OK.

*Note: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** (on page 187).*

Send SMS Message

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and BCM2 placeholders. The placeholders represent information which is pulled from the BCM2 and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the BCM2 in order to send SMS messages.

Note: The BCM2 cannot receive SMS messages.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See **Email and SMS Message Placeholders** (on page 187) for a list and definition of available variables.

► **To configure SMS message:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send SMS message.
6. In the Recipient Phone Number field, specify the phone number of the recipient.
7. Select the Use Custom Log Message checkbox, then create a custom message in the provided field.

Click the Information icon  to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See **Email and SMS Message Placeholders** (on page 187) for more details.

Note: Only the 7-bit ASCII charset is supported for SMS messages.

8. Click OK.

Internal Beeper

You can have the built-in beeper of the BCM2 turned on or off when a certain event occurs.

► **To switch the internal beeper:**

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Internal beeper.
5. Select an option from the Operation field.
 - Turn Beeper On: Turns on the internal beeper to make it buzz.
 - Turn Beeper Off: Turns off the internal beeper to make it stop buzzing.
6. Click OK.

Switch Peripheral Actuator

If you have any actuator connected to the BCM2, you can set up the BCM2 so it automatically turns on or off the system controlled by this actuator when a specific event occurs.

*Note: For information on connecting actuators to the BCM2, see **DX Sensor Packages** (on page 28).*

► **To switch on or off the system connected to an actuator:**

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.

4. In the Action field, click the drop-down arrow and select the desired action: Switch peripheral actuator.
5. From the Operation drop-down list, select an operation for the selected actuator.
 - Turn On: Turns on the selected actuator.
 - Turn Off: Turns off the selected actuator.
6. To select the actuator where this action will be applied, select it from the Available Actuators list and click  to add it to the Switched Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To add all actuators to the Switched Actuators list box, click .
7. To remove any actuator from the Switched Actuators list, select it and click  to move it back to the Available Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To remove all actuators, click .
8. Click OK.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

► To configure a record snapshot to webcam storage action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Record snapshots to webcam storage.
6. Select a webcam from the Webcam drop-down.
7. Selecting the action to perform - Start recording or Stop recording. If "Start recording" is selected, do the following:

- a. Use the slide bar to specify the total number of snapshots to be taken when the event occurs. The maximum amount of snapshots that can be stored on the BCM2 is ten (10). If you set it for a number greater than ten and the storage location is on the BCM2, after the tenth snapshot is taken and stored, the oldest snapshots are overwritten.

*Tip: By default, the storage location is on the BCM2. You can specify a remote server to store the snapshots. See **Configuring Webcam Storage** (on page 226).*

- b. In the "Time before first Snapshot (s):" field, use the slide bar to specify the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
 - c. In the "Time between Snapshots (s):" field, use the slide bar to specify the amount of time between each snapshot being taken.
8. Click OK.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, the BCM2 provides the following built-in event rules:

- System Event Log Rule
- System SNMP Notification Rule
- System Tamper Detection Alarmed
- System Tamper Detection Unavailable

If the built-in rules do not satisfy your needs, create new ones.

► To create event rules:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, click New.
3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enabled checkbox to activate this event rule.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing various types of events appears.
 - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

Note: To select all items or events listed on the same submenu, select the option enclosed in brackets, such as <Any sub-event>, <Any Server> and <Any user>. <Any Power Meter> refers to all panels and/or power meter modules.

6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." <ul style="list-style-type: none"> ▪ Asserted: The BCM2 takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The BCM2 takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The BCM2 takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts). ▪ For connection state for USB cascading and auxiliary/RS-485 devices, assertion is displayed as "connected" and deassertion as "disconnected"
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed," "No longer alarmed" and "Both." <ul style="list-style-type: none"> ▪ Alarmed: The BCM2 takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The BCM2 takes the action only when the chosen sensor returns to normal. ▪ Both: The BCM2 takes the action both when the chosen sensor enters or quits the alarmed state.

Event types	Radio buttons
Sensor availability	<p>Available radio buttons include "Unavailable," "Available" and "Both."</p> <ul style="list-style-type: none"> ▪ Unavailable: The BCM2 takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The BCM2 takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The BCM2 takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	<p>Available radio buttons include "Link state is up," "Link state is down" and "Both."</p> <ul style="list-style-type: none"> ▪ Link state is up: The BCM2 takes the action only when the network link state changes from down to up. ▪ Link state is down: The BCM2 takes the action only when the network link state changes from up to down. ▪ Both: The BCM2 takes the action whenever the network link state changes.
Function enabled or disabled	<p>Available radio buttons include "Enabled," "Disabled" and "Both."</p> <ul style="list-style-type: none"> ▪ Enabled: The BCM2 takes the action only when the chosen function is enabled. ▪ Disabled: The BCM2 takes the action only when the chosen function is disabled. ▪ Both: The BCM2 takes the action when the chosen function is either enabled or disabled.
User logon state	<p>Available radio buttons include "Logged in," "Logged out," and "Both."</p> <ul style="list-style-type: none"> ▪ Logged in: The BCM2 takes the action only when the selected user logs in. ▪ Logged out: The BCM2 takes the action only when the selected user logs out. ▪ Both: The BCM2 takes the action both when the selected user logs in and logs out.

Event types	Radio buttons
Restricted service agreement	<p>Available radio buttons include "Accepted," "Declined," and "Both."</p> <ul style="list-style-type: none"> ▪ Accepted: The BCM2 takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: The BCM2 takes the action only when the specified user rejects the restricted service agreement. ▪ Both: The BCM2 takes the action both when the specified user accepts or rejects the restricted service agreement
Server monitoring event	<p>Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both."</p> <ul style="list-style-type: none"> ▪ Monitoring started: The BCM2 takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The BCM2 takes the action only when the monitoring of any specified server stops. ▪ Both: The BCM2 takes the action when the monitoring of any specified server starts or stops.
Server reachability	<p>Available radio buttons include "Unreachable," "Reachable," and "Both."</p> <ul style="list-style-type: none"> ▪ Unreachable: The BCM2 takes the action only when any specified server becomes inaccessible. ▪ Reachable: The BCM2 takes the action only when any specified server becomes accessible. ▪ Both: The BCM2 takes the action when any specified server becomes either inaccessible or accessible.

7. In the Actions field, select the desired action from the "Available actions" list box, and click  to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - To add all actions, simply click .
 - If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box.
8. To add additional actions, repeat Step 7.

9. To remove any action, select it from the "Selected actions" list box, and click  to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - To remove all actions, click .
10. Click OK to save the new event rule.

Note: If you do not click OK before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

11. Repeat the same steps to create additional event rules.
12. Click Close to quit the dialog.

Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the BCM2 report the reading or state of a specific environmental sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer time between this action's execution time and creation time. Otherwise, the scheduled action will NOT be performed at the specified time if the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling this action at 10:59 am or earlier.

► To schedule any action(s):

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Scheduled Actions tab.
3. Click New.
4. In the "Timer name" field, type a name for this scheduled action. The default name is New Timer <n>, where <n> is the sequential number starting at 1.
5. Make sure the Enabled checkbox is selected, or the BCM2 will not carry out this scheduled action.
6. Select the desired time frequency from the Execution Time field and then specify the time interval or a specific date and time in the Time field.

Time options	Frequency settings
Minutes	The frequency in minutes ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	The hourly option sets the timing to either of the following: <ul style="list-style-type: none"> ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	You need to specify the time for this daily option. For example, if you specify 13:30 in the Time field, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. Days range from Sunday to Monday.
Monthly	Both the date and time must be specified for the monthly option. The dates range from 1 to 31, and the time is specified in 24-hour format. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: <ul style="list-style-type: none"> ▪ Month - January through December. ▪ Date - 1 to 31. ▪ Time - the value is specified in 24-hour format.

7. In the Actions field, select the desired action from the "Available actions" list box, and click  to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To add all actions, simply click .
- If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box. See **Creating Actions** (on page 154).

When creating new actions from the Scheduled Actions tab, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

8. To remove any action, select it from the "Selected actions" list box, and click  to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To remove all actions, click .
9. Click OK.

Send Sensor Report Example

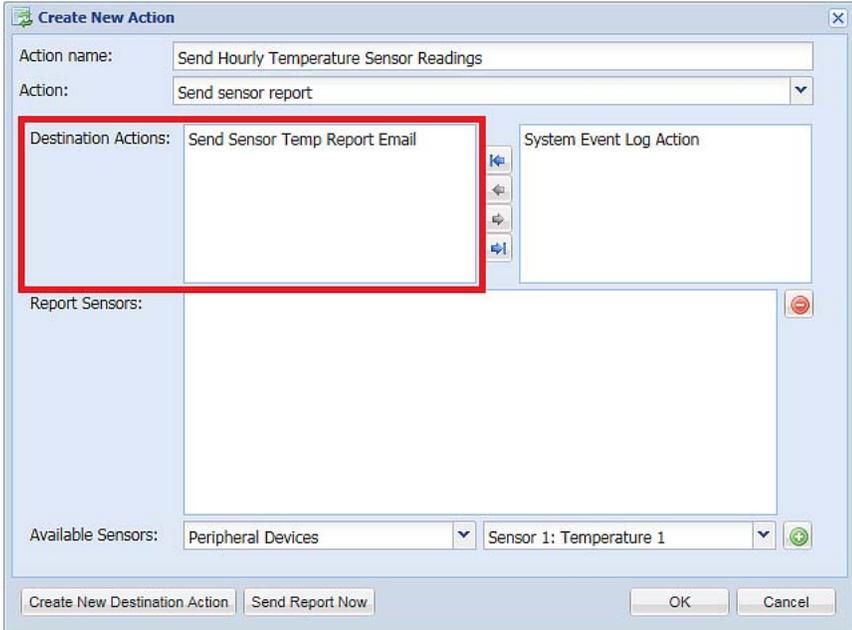
Below is an example of a scheduled action set to send a temperature sensor report via email hourly.

In this example,

- a. Define a 'Send email' destination action that is name *Send Sensor Temp Report Email*.
 - This destination action sends an email to the specified recipient(s).
- b. Define a 'Send sensor report' action that is named *Send Hourly Temperature Sensor Readings*.
 - This action reports temperature sensor readings via the selected destination action -- Send Sensor Temp Report Email.
- c. Define a timer that is named *Hourly Sensor Temperature Readings*.
 - This timer determines that the 'Send Hourly Temperature Sensor Readings' action shall take place on an hourly basis.

► Detailed steps:

1. If you have not already done so, create the destination action 'Send Sensor Temp Report Email', which is performed when the 'Send Hourly Temperature Sensor Readings' action occurs.



The screenshot shows the 'Create New Action' dialog box. The 'Action name' field is filled with 'Send Hourly Temperature Sensor Readings'. The 'Action' dropdown menu is set to 'Send sensor report'. Below this, there are two lists of actions. The first list, 'Destination Actions', contains 'Send Sensor Temp Report Email' and is highlighted with a red rectangular box. The second list, 'System Event Log Action', is currently empty. Below the action lists is a 'Report Sensors' field, which is empty. At the bottom, the 'Available Sensors' dropdown is set to 'Peripheral Devices', and 'Sensor 1: Temperature 1' is selected. The dialog box has buttons for 'Create New Destination Action', 'Send Report Now', 'OK', and 'Cancel'.

- You must create the destination action as illustrated below prior to creating the 'Send Hourly Temperature Sensor Readings' action. For details, see **Send Email** (on page 162).

The screenshot shows a web-based dialog box titled "Create New Action". It has the following fields and options:

- Action name:** A text input field containing "Send Sensor Temp Report Email".
- Action:** A dropdown menu with "Send Email" selected.
- Recipients email addresses:** A text input field containing "sensor_reporting@raritan.com".
- SMTP Settings:**
 - Use Default SMTP Server**
 - Server Name: mail.raritan.info
 - Sender Email Address: test-mkr@peppercon.de
 - Configure button
 - Use Custom SMTP Settings**
- Use Custom Log Message**
 - Hourly sensor report

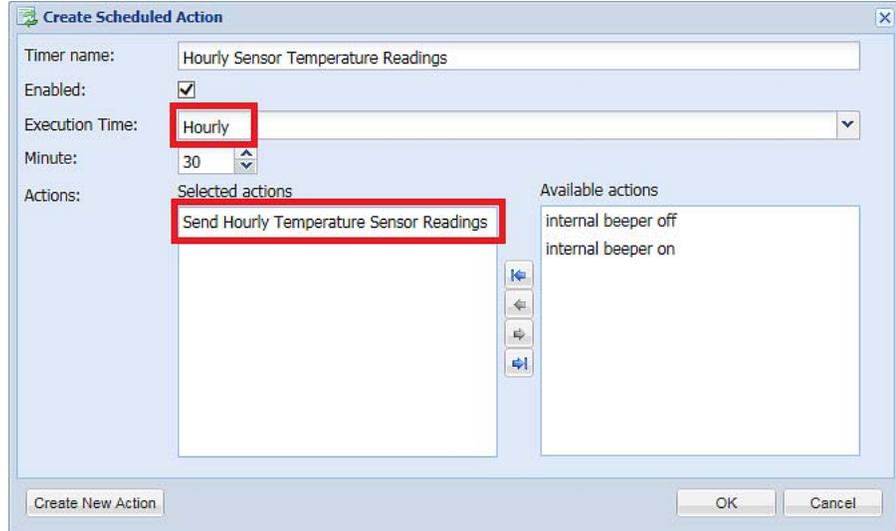
At the bottom right, there are "OK" and "Cancel" buttons.

2. Create the 'Send sensor report' action -- *Send Hourly Temperature Sensor Readings*.
 - a. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
 - b. Click the Actions tab > New.
 - c. Enter the following information.

- Type the action's name -- *Send Hourly Temperature Sensor Readings*.
- Select the 'Send sensor report' action.
- Select the destination action 'Send Sensor Temp Report Email'.
- Add the desired temperature sensor(s) from the Available Sensors list to the Report Sensors box.

- d. Click OK. For details, see **Send Sensor Report** (on page 166).
3. Create a timer for this newly-created action in the same Event Rule Settings dialog.
 - a. Click the Scheduled Actions tab > New.
 - b. Enter the following information.

- Type the timer name -- *Hourly Sensor Temperature Readings*.
- Select the Enabled checkbox.
- Select Hourly, and set the Minute to 30.
- Select the 'Send Hourly Temperature Sensor Readings' action.



c. Click OK. For details, see **Scheduling an Action** (on page 175).

Then the BCM2 will regularly send out an email containing the specified temperature sensor readings at 0:30 am, 1:30 am, 2:30 am, 3:30 am, 4:30 am, and so on until 23:30 pm every day.

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when BCM2 events occur (are TRUE) or, in some cases, do not occur (are FALSE). See **Send Email** (on page 162) for information configuring email messages to be sent when specified events occur.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	
Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [STRIPID] ('[STRIPNAME]').	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]').	
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	
Card Reader Management > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved from host '[USERIP]'.	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGER PORT] failed or no response. [ERRORDESC].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrect system clock.	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > Features > Schroff LHX / SHX Support	Schroff LHX / SHX support enabled.	Schroff LHX / SHX support disabled.
Energywise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Peripheral Device Slot > * > Numeric Sensor > Below lower warning	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical' at [READING].
Peripheral Device Slot > * > State Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor > Alarmed / Open / On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Modem > Dial-in link established	An incoming call from caller '[CALLERID]' was received.	The incoming call from caller '[CALLERID]' was disconnected: [CALLENDREASON].
Modem > Modem attached	A [MODEMTYPE] modem was attached.	
Modem > Modem detached	A [MODEMTYPE] modem was removed.	
Power Metering Controller > Power Meter Created	Power meter '[POWERMETER]' was created.	
Power Metering Controller > Power Meter Deleted	Power meter '[POWERMETER]' was deleted.	
Power Metering Controller > Power Meter Modified	Power meter '[POWERMETER]' was modified.	
Power Metering Controller > * > Circuit Created	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was created.	
Power Metering Controller > * > Circuit Deleted	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was deleted.	
Power Metering Controller > * > Circuit Modified	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was modified.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Power Metering Controller > * > Sensor > * > Unavailable	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' unavailable.	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' available.
Power Metering Controller > * > Sensor > * > Above upper critical	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
Power Metering Controller > * > Sensor > * > Above upper warning	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
Power Metering Controller > * > Sensor > * > Below lower warning	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Power Metering Controller > * > Sensor > * > Below lower critical	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Power Metering Controller > * > Sensor > * > Reset	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Server Monitoring > * > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]	
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	

User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]' accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]' declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	

The asterisk symbol () represents anything you select for the 'trigger' events.*

Email and SMS Message Placeholders

Following are placeholders that can be used in custom event email messages.

Note: Click the Information icon  to open the Event Context Information dialog, which contains a list of placeholders and their definitions. Then select the desired placeholder, and either double-click it or click the "Paste into Message" button to insert it into the customized message.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule

Placeholder	Definition
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSOR SLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[RADIUSERRORDESC]	A Radius error occurred

Placeholder	Definition
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to

Sample Event Rules

Sample Device-Level Event Rule

In this example, we want the BCM2 to record the firmware upgrade failure in the internal log when it happens. The sample event rule looks like this:

- Event: Device > Firmware update failed
- Actions: System Event Log Action

▶ **To create the above event rule:**

1. Select Event > Device to indicate we are specifying an event at the device level.
2. Select "Firmware update failed" in the submenu because we want the BCM2 to respond to the event related to firmware upgrade failure.
3. Select System Event Log Action as we intend to record the firmware update failure event in the internal log.

Sample Mains-Level Event Rule

In this example, we want the BCM2 to send SNMP notifications to the SNMP manager for any sensor change event of the mains.

*Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps or informs, depending on the settings for the System SNMP Notification Action. See **Configuring SNMP Notifications** (on page 246).*

The event rule is set like this:

- Event: Mains > Mains M > Sensor > Any sub-event
- Actions: System SNMP Notification Action

▶ **To create the above event rule:**

1. Select Event > Mains to indicate we are specifying an event at the mains level.
2. Select "Mains M" from the submenu because that is the target.
3. Select "Sensor" to refer to sensor readings.
4. Select "Any sub-event" because we want to specify all events related to all types of Mains sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Notification Action" to send SNMP notifications to respond to the specified event.

Then the SNMP notifications are sent when:

- Any numeric sensor's reading moves past any threshold into the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.

For example, when the mains' voltage crosses into the upper warning range, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the BCM2 keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one event again.

Example 1

This example illustrates an event rule which continuously causes the BCM2 to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

Example 2

This example illustrates an event rule which continuously causes the BCM2 to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

Modifying an Event Rule

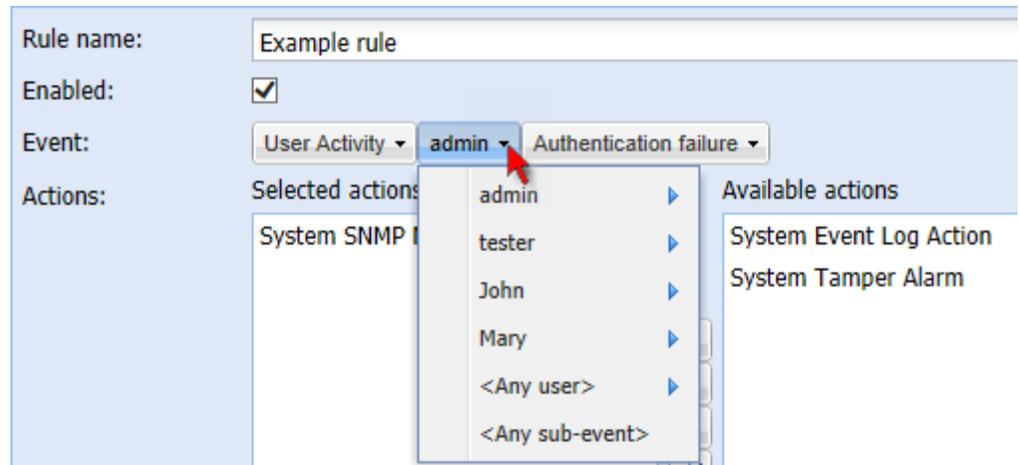
You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule, System SNMP Notification Rule, System Tamper Detection Alarmed, and System Tamper Detection Unavailable.

► **To modify an event rule:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify and click Edit, or simply double-click that rule.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all users (shown as <Any user>).



5. If the "Trigger condition" field is available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
 - To add any action, select it from the "Available actions" list box, and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To add all actions, click .
 - To remove any action, select it from the "Selected actions" list box, and click  to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - To remove all actions, click .
 - To create a new action, click Create New Action. The newly created action will be moved to the "Selected actions" list box once it is created. See **Creating Actions** (on page 154) for information on creating an action.
7. Click OK to save the changes.

Note: If you do not click OK before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in actions "System Event Log Action" and "System Tamper Alarm" are not user-configurable.

► **To modify an action:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify and click Edit, or simply double-click that action.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

Note: If you do not click OK before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

► **To delete an event rule or action:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
 - a. Ensure the Rules tab is selected. If not, click the Rules tab.
 - b. Select the desired rule from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - c. Click Delete.
 - d. Click Yes on the confirmation message.
3. To delete an action:
 - a. Click the Actions tab.
 - b. Select the desired action from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
 - c. Click Delete.
 - d. Click Yes on the confirmation message.
4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the BCM2 to generate an alert. The measurement then returns to a value within the threshold, but the BCM2 does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the BCM2 uses. See **"To De-assert" and Deassertion Hysteresis** (on page 119).

Viewing Connected Users

You can see which users are connected to the BCM2 device and their status. If you have administrator privileges, you can terminate any user's connection to the BCM2 device.

► **To view connected users:**

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the BCM2. <ul style="list-style-type: none"> ▪ Web GUI: Refers to the BCM2 web interface. ▪ CLI: Refers to the command line interface (CLI). <p>The information in parentheses following "CLI" indicates how this user is connected to the CLI.</p> <ul style="list-style-type: none"> - <i>Serial</i>: Represents the local connection (serial RS-232 or USB). - <i>SSH</i>: Represents the SSH connection. - <i>Telnet</i>: Represents the Telnet connection.
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
 - a. A dialog appears, prompting you to confirm the operation.
 - b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out..
3. Click Close to quit the dialog.

*Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** (on page 230).*

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the BCM2 device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

Adding IT Devices for Ping Monitoring

BCM2 can monitor the accessibility of any type of IT equipment, such as database servers, remote authentication servers, power distribution units (PDUs), and so on.

BCM2 supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings to meet your own needs.

*Tip: To make the BCM2 automatically log, send notifications or perform other actions for any server accessibility or inaccessibility events, you can create event rules associated with server monitoring. See **Event Rules and Actions** (on page 153).*

► **To add IT equipment for ping monitoring:**

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Provide the information required.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.

Field	Description
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time (in seconds) after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time (in seconds) after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time (in seconds) before resuming pinging after failure	The wait time before the BCM2 resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the BCM2 disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click OK.
6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

In the beginning, the status of the monitored equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the BCM2 can declare that the monitored device is reachable or unreachable.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your BCM2 to make sure that PDU is properly operating all the time, and the BCM2 must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power source for your BCM2 is different from the power source for that PDU.

This requires two steps: set up the PDU monitoring and create an event rule.

► Step 1: Set up the ping monitoring for the target PDU

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New.
3. Type 192.168.84.95 in the "IP address/hostname" field.
4. Ensure the "Enable ping monitoring for this server" checkbox is selected.
5. To make the BCM2 declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, do the following:
 - a. In the "Number of successful pings to enable feature" field, type 3.
 - b. In the "Wait time (in seconds) after successful ping" field, type 5.
6. To make the BCM2 declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 pings * 3 seconds), do the following:
 - a. In the "Number of consecutive unsuccessful pings for failure" field, type 4.
 - b. In the "Wait time (in seconds) after unsuccessful ping" field, type 3.
7. In the "Wait time (in seconds) before resuming pinging" field, type 60 to make the BCM2 stops pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the BCM2 will re-ping the target PDU.

► Step 2: Create an event rule to send SNMP notifications for this PDU

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click New.

3. In the "Rule name" field, type "Send SNMP notifications for PDU (192.168.84.95) inaccessibility."
4. Select the Enabled checkbox to enable this new rule.
5. In the Event field, choose Server Monitoring > 192.168.84.95 > Unreachable.
6. In the "Trigger condition" field, select the Unreachable radio button. This makes the BCM2 react only when the target PDU becomes inaccessible.
7. Select the System SNMP Notification Action from the "Available actions" list box, and click  to add it to the "Selected actions" list box.

*Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Configuring SNMP Notifications** (on page 246).*

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever needed.

► **To modify the ping monitoring settings for an IT device:**

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify.
3. Click Edit or double-click that IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

► **To delete ping monitoring settings for an IT device:**

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. Click Yes on the confirmation message.

5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying IT devices for the BCM2 device to monitor their network accessibility.

► **To check the server monitoring states and results:**

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
 -  : This icon denotes that the monitoring for the corresponding device is enabled.
 -  : This icon denotes that the monitoring for the corresponding device is disabled.
3. The column labeled "Status" indicates the accessibility of each monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the BCM2 device and the monitored equipment is not reliably established yet.

4. Click Close to quit the dialog.

Managing Event Logging

By default, the BCM2 captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view over 2000 historical events that occurred to the BCM2 device in the local event log.

When the log size exceeds 256KB, each new entry overwrites the oldest entry.

► **To display the local log:**

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

Each event entry in the local log consists of:

- Date and time of the event
 - Type of the event
 - A description of the event
 - ID number of the event
2. The dialog shows the final page by default. You can:
- Switch between different pages by doing one of the following:
 - Click  or  to go to the first or final page.
 - Click  or  to go to the prior or next page.
 - Type a number in the Page text box and press Enter to go to a specific page.
 - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

Note: Sometimes when the dialog is too narrow, the icon  takes the place of the Show Details button. In that case, click  and select Show Details to view details.

- Click  to view the latest events.
- View a specific type of events only by selecting an event type in the Filter Event Class field.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

► **To delete all event entries:**

1. Choose Maintenance > View Event Log. The Event Log dialog appears.
2. Click Clear Event Log.
3. Click Yes on the confirmation message.

Viewing the Wireless LAN Diagnostic Log

The BCM2 provides a diagnostic log for inspecting connection errors that occurred over the wireless network interface. The information is useful for technical support engineers.

► **To display the wireless LAN diagnostic log:**

1. Choose Device Settings > Network. The Network Configuration dialog appears.

2. Click Show WLAN Diagnostic Log. The WLAN Diagnostic Log dialog appears.

Each entry in the log consists of the event's:

- ID number
- Date and time
- Description

Note: The Show WLAN Diagnostic Log button is available only when the Network Interface is set to Wireless.

3. The dialog shows the final page by default. You can:
 - Switch between different pages by doing one of the following:
 - Click  or  to go to the first or final page.
 - Click  or  to go to the prior or next page.
 - Type a number in the Page text box and press Enter to go to a specific page.
 - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

Note: Sometimes when the dialog is too narrow, the icon  takes the place of the Show Details button. In that case, click  and select Show Details to view details.

- Click  to view the latest events.

▶ **To clear the diagnostic log:**

1. Click Clear WLAN Diagnostic Log.
2. Click Yes on the confirmation message.

Environmental Sensors and Actuators

The BCM2 can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed. If an actuator is connected to the BCM2, you can use it to control a system or mechanism.

▶ **To add environmental sensors and actuators:**

1. Physically connect environmental sensor packages to the BCM2 device. See **Connecting Environmental Sensor Packages** (on page 22).
2. Log in to the BCM2 web interface. The BCM2 should have detected the connected sensors and actuators, and display them in the web interface.

3. Identify each sensor and actuator. See **Identifying Environmental Sensors and Actuators** (on page 203).
4. The BCM2 should automatically manage the detected sensors and actuators. Verify whether detected sensors and actuators are managed. If not, have them managed. See **Managing Environmental Sensors or Actuators** (on page 207).
5. Configure the sensors and actuators. See **Configuring Environmental Sensors or Actuators** (on page 208). The steps include:
 - a. Name the sensor or actuator.
 - b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
 - c. Mark the sensor or actuator's physical location on the rack or in the room.
 - d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes. Only numeric sensors have threshold settings. As for actuators, they are used to control a device or system so they show state changes only.

Identifying Environmental Sensors and Actuators

A DPX environmental sensor package includes a serial number tag on the sensor cable.



A DPX2, DPX3 or DX sensor has a serial number tag attached to its rear side.



The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the BCM2.

► **To identify each detected environmental sensor:**

1. Click Peripheral Devices in the left pane.

Peripheral Devices									
ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State	
1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal	
2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal	
3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal	
4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal	
5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal	
6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal	

2. Match the serial number from the tag to those listed in the sensor table.

Matching the Serial Number

A DPX environmental sensor package includes a serial number tag on the sensor cable.



A DPX2, DPX3 or DX sensor has a serial number tag attached to its rear side.



The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the BCM2.

► **To identify each detected environmental sensor or actuator via serial numbers:**

1. Click Peripheral Devices in the left pane.

- Match the serial number from the tag to those listed in the sensor table.

Peripheral Devices								
ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

Matching the Position

DPX2, DPX3 and DX sensor packages can be daisy chained. The BCM2 can indicate each sensor or actuator's position by showing the sensor port where the environmental sensor package is connected as well as its sequence in a sensor daisy chain.

► To identify an environmental sensor or actuator through its position:

- Click Peripheral Devices in the left pane.
- Locate the Position column, which shows one or two pieces of position information.
 - The sensor port number, such as Port 1, Port 2, Port 3 and so on.
 - The sensor or actuator's location in the sensor chain, such as Chain Position 1, Chain Position 2, and so on.

Peripheral Devices								
ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	Temperature 1	Port 1, Chain Position 4	REB5893292	Temperature			23.7 °C	normal
2	Relative Humidity 1	Port 1, Chain Position 4	REB5893292	Relative Humidity			63 %	normal
3	Temperature 2	Port 1, Chain Position 3	REB5893291	Temperature			23.8 °C	normal
4	Relative Humidity 2	Port 1, Chain Position 3	REB5893291	Relative Humidity			62 %	normal
5	Temperature 3	Port 1, Chain Position 2	REB5893290	Temperature			22.7 °C	normal
6	Relative Humidity 3	Port 1, Chain Position 2	REB5893290	Relative Humidity			66 %	normal
7	Temperature 4	Port 1, Chain Position 1	REB5893289	Temperature			23.8 °C	normal
8	Relative Humidity 4	Port 1, Chain Position 1	REB5893289	Relative Humidity			63 %	normal

► DPX sensor position information:

The BCM2 only displays the sensor port where the DPX sensor package is physically connected. No chain position information is displayed.

For example, if a DPX sensor package is connected to the SENSOR port numbered 1, its Position column shows "Port 1" only.

Note: For the BCM2 devices with only one SENSOR port, it always shows "Port 1."

► **DPX2, DPX3 and DX sensor position information:**

The BCM2 displays the sensor package's position in the chain in addition to the sensor port number for DPX2, DPX3 and DX sensor packages.

For example, if such sensor or actuator is located on the second sensor package in the sensor chain connected to the SENSOR port 1, its Position column shows "Port 1, Chain Position 2."

Identifying Sensor or Actuator Channels

A sensor package may have multiple contact closure (CC) or dry contact (DC) channels, such as DX-D2C6 or DX-PD2C5.

When the BCM2 initially detects and automatically manages a sensor package with multiple channels, all channels are assigned with ID numbers in sequence.

If you manually manage these channels by selecting "Automatically assign a sensor number," the BCM2 assigns ID numbers randomly because this option assumes that users do not care about the sequence. In this case, see the Channel column to identify each channel correctly. For example, CC1 or DC1 is Channel 1, CC2 or DC2 is Channel 2, and so on.

ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
1	On/Off 1	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	5			normal
2	On/Off 2	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	4			normal
3	On/Off 3	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	3			normal
4	On/Off 4	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	2			normal
5	On/Off 5	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	1			normal
6	Powered Dry Contact 1	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	2	✓		off
7	Powered Dry Contact 2	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	1	✓		off

Managing Environmental Sensors or Actuators

The BCM2 starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed. To control an actuator, you also need to have it managed.

The BCM2 device can manage a maximum of 32 environmental sensors or actuators.

When there are less than 32 managed sensors or actuators, the BCM2 automatically brings detected environmental sensors or actuators under management by default. You have to manually manage a sensor or actuator only when it is not under management.

*Tip: You can disable the automatic management feature so that newly connected environmental sensors or actuators are NOT brought under management automatically. See **Disabling the Automatic Management Function** (on page 218).*

► To manually manage an environmental sensor or actuator:

1. If the BCM2 folder is not expanded, expand it to show all components and component groups. See Expanding the Tree.

*Note: The PMC folder is named "my PMC" by default. The name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Peripheral Devices in the left pane.
3. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To manage multiple ones, select multiple checkboxes.

*Note: To identify all detected sensors or actuators, see **Identifying Environmental Sensors and Actuators** (on page 203).*

4. Click Manage. If you selected only one sensor or actuator, the "Manage peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor or actuator's serial number and <sensor type> is its type.

Note: For a sensor package with contact closure (CC) or dry contact (DC) channels, a channel number is added to the end of the <sensor type>.

5. There are two ways to manage a sensor or actuator:
 - To manage it by letting the BCM2 assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors or actuators.

- To manage it by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

If the number you selected was already assigned to a sensor or actuator, that sensor or actuator becomes released after losing this ID number.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to any sensor or actuator. If it has been assigned to a sensor or actuator, it shows its serial number. Otherwise, it shows the word "unused."

The manual assignment method is unavailable if you selected multiple sensors or actuators in Step 2.

6. Click OK. The BCM2 starts to display the managed sensor or actuator's reading and state.
7. To manage additional ones, repeat Steps 2 to 5.

*Note: When the total number of managed sensors and actuators reaches the maximum, you CANNOT manage additional sensors or actuators unless you remove or replace any managed ones. To remove a sensor or actuator, see **Unmanaging Environmental Sensors or Actuators** (on page 217).*

Configuring Environmental Sensors or Actuators

You can change the default name to easily identify the managed sensor or actuator, and describe its location with X, Y and Z coordinates.

► **To configure environmental sensors or actuators:**

1. Click Peripheral Devices in the left pane.
2. Select the sensor or actuator that you want to configure.
3. Click Setup in the right pane. The "Setup of peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is its serial number and <sensor type> is its type.

For example, *Setup of peripheral device AEI7A00022 (Temperature)*.

4. Configure available fields properly.

Fields	Description
Name	Assign a name for identification.
Description	Type any descriptive text as needed.

Fields	Description
Location (X, Y and Z)	<p>Describe the sensor's or actuator's location by assigning alphanumeric values to the X, Y and Z coordinates. See <i>Describing the Sensor's or Actuator's Location</i> (on page 211).</p> <p>When the term "Rack Units" appears inside the parentheses in the Z location field, indicating that the Z coordinate format is set to Rack Units, you must type an integer number. See Setting the Z Coordinate Format.</p>
Binary Sensor Subtype	<p>This field is available only when the selected sensor is a contact closure sensor. Select one of the following sensor types:</p> <ul style="list-style-type: none"> ▪ Contact: The detector/switch is designed to detect the door lock or door open/closed status. ▪ Smoke Detection: The detector/switch is designed to detect the appearance of smoke. ▪ Water Detection: The detector/switch is designed to detect the appearance of water on the floor. ▪ Vibration: The detector/switch is designed to detect the vibration in the floor.
Alarmed to Normal Delay	<p>This field is available only when the selected sensor is the DX-PIR presence detector.</p> <p>It determines the wait time before the PX announces that the presence detector returns to the normal state after it is back to normal.</p> <p>Type both the time and measurement units in this field. For example, type '30 s' for 30 seconds, or '2 min' for 2 minutes.</p>

5. If the selected sensor is a numeric sensor, its threshold settings are displayed in the dialog. See Sensor Threshold Settings for detailed information.

There are two types of thresholds: sensor-specific thresholds and default thresholds.

To use the sensor-specific threshold settings, select the Use Sensor Specific Thresholds radio button.

- Click Edit or double-click the threshold setting row to open the threshold setup dialog.
- To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
- After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
- To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 119).

- To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 117).

To use the default threshold settings, select the Use Default Thresholds radio button. To modify the default threshold settings, see **Changing Default Thresholds** (on page 211).

Note: The Upper Critical and Lower Critical values are points at which the PX considers the operating environment critical and outside the range of the acceptable threshold.

6. Click OK.
7. Repeat the same steps to configure additional ones.

*Tip: You can configure thresholds of multiple sensors at a time as long as these sensors belong to the same type. See **Setting Thresholds for Multiple Sensors** (on page 212).*

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors and actuators.

► To determine the Z coordinate format:

1. Click the PMC folder.

*Note: The PMC folder is named "my PMC" by default. The name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Setup in the Settings section. The setup dialog appears.
3. In the Peripheral Device Z Coordinate Format field, click the drop-down arrow and select an option from the list.
 - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
 - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK.

Describing the Sensor's or Actuator's Location

Use the X, Y and Z coordinates to describe each sensor or actuator's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = Brown Cabinet Row

Y = Third Rack

Z = Top of Cabinet

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 24 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 24 characters.

*Tip: To configure and retrieve these coordinate values over SNMP, see the BCM2 MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** (on page 255).*

Changing Default Thresholds

The default thresholds are the initial threshold values that automatically apply to numeric environmental sensors. These values are configured on a sensor type basis, which include:

- Temperature sensors
- Humidity sensors (both relative and absolute humidity)
- Air pressure sensors
- Air flow sensors
- Vibration sensors

Note that changing the default thresholds re-determine the initial thresholds applying to the environmental sensors that are added or detected later on.

In addition, changing the default thresholds also change the thresholds of those environmental sensors where the default thresholds have been selected as their threshold option. See **Configuring Environmental Sensors or Actuators** (on page 208).

► To change the default threshold settings:

1. Click Peripheral Devices in the left pane.

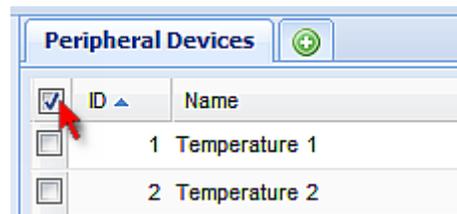
2. Click Default Thresholds Setup on the Peripheral Devices page. A dialog appears, showing a list of all numeric environmental sensor types.
3. Select the desired sensor type.
4. Click Edit or double-click that sensor type to adjust its threshold settings, deassertion hysteresis or assertion timeout.
 - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
 - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
 - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See **"To De-assert" and Deassertion Hysteresis** (on page 119).
 - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See **"To Assert" and Assertion Timeout** (on page 117).
5. Repeat the above step to modify the threshold settings of other numeric sensor types.
6. Click OK.

Setting Thresholds for Multiple Sensors

You can configure thresholds for multiple environmental sensors of *the same type* at a time. For example, if you want all temperature sensors to have identical upper and lower thresholds, follow the procedure below to set up all temperature sensors together.

► **To configure thresholds of multiple environmental sensors:**

1. Click Peripheral Devices in the left pane.
2. Select the checkboxes of those environmental sensors whose threshold settings should be the same. Make sure the selected sensors belong to the same type.
 - To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.



3. Click Setup. Note that the Setup button is disabled if any of the selected sensors belongs to a different type.

4. Configure the thresholds as described in **Configuring Environmental Sensors or Actuators** (on page 208).
5. Click OK.

Viewing Sensor or Actuator Data

Readings and states of the environmental sensors or actuators will display in the web interface after the sensors and actuators are properly connected and managed.

The Dashboard page shows the information of managed environmental sensors and actuators only, while the Peripheral Devices page shows the information of both managed and unmanaged ones.

Both pages indicate an environmental sensor or actuator's position in either of the following manners:

- **Port <n>**, where <n> is the number of the SENSOR port on the BCM2 where a specific environmental sensor package is connected. DPX sensor packages show this information only.
- **Port <n>, Chain Position <pos_num>**, where <pos_num> is the sensor package's sequential position in a sensor daisy chain. DPX2 and DX sensor packages show this information.

If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Sensors** (on page 50).

► To view managed environmental sensors and actuators only:

1. Click the Dashboard icon in the PMC Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Peripheral Devices section on the Dashboard page. The section shows:
 - Total number of managed sensors and actuators
 - Total number of unmanaged sensors and actuators
 - Information of each managed sensor and actuator, including:
 - Name
 - Position
 - Reading (for numeric sensors)
 - State

► To view both managed and unmanaged ones:

Click Peripheral Devices in the left pane.

Detailed information for each connected sensor or actuator is displayed, including:

- ID number
- Name
- Position
- Serial number
- Type
- Channel (for a sensor package with contact closure or dry contact channels)
- Whether the sensor is an 'Actuator' or not (if yes, this icon  appears in the Actuator column)
- Reading
- State

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete sensors. For example, a contact closure sensor is a discrete (on/off) sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity or communications with the sensor is lost.

The BCM2 pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor package show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The BCM2 continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

For DPX2 or DX sensor packages, all of the connected sensor packages also enter the *unavailable* states if any of them is upgrading its sensor firmware.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, usually this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

For a Raritan's DPX floor water sensor, the normal state must be set to Normally Closed, which means no water is detected.

*Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** (<http://www.raritan.com/support/>).*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

$$\text{Lower Warning threshold} \leq \text{Reading} < \text{Upper Warning threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

Usually for a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

For Raritan's floor water sensor, the normal state must be set to Normally Closed, which means no water is detected. The *alarmed* state indicates that the presence of water is detected.

*Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** (<http://www.raritan.com/support/>).*

Tip: A contact closure sensor's LED is lit after entering the alarmed state. Determine which contact closure switch is in the "abnormal" status according to the corresponding LED.

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

$$\text{Reading} < \text{Lower Critical Threshold}$$

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

$$\text{Lower Critical Threshold} \leq \text{Reading} < \text{Lower Warning Threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

$$\text{Upper Warning Threshold} \leq \text{Reading} < \text{Upper Critical Threshold}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

$$\text{Upper Critical Threshold} \leq \text{Reading}$$

Note: The symbol \leq means smaller than ($<$) or equal to ($=$).

States of Managed Actuators

DX sensor packages with dry contact channels allow you to connect actuators. An actuator has only three states described below. Note that an actuator is never highlighted in red or yellow regardless of the actuator states.

- unavailable: The communication with the actuator is lost.
- On: The actuator has been turned on.
- Off: The actuator has been turned off.

States of Unmanaged Sensors or Actuators

All sensors or actuators that are physically connected to the BCM2 but NOT under management always show the following state:

- unmanaged

Note: For firmware versions prior to 3.2.1, unmanaged sensors or actuators show the state "unavailable."

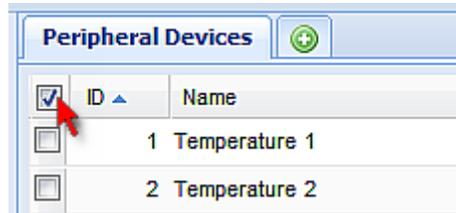
Unmanaging Environmental Sensors or Actuators

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the BCM2 device stops retrieving the sensor's reading and/or state. This procedure also applies if you want to unmanage an actuator.

► To release a managed sensor or actuator:

1. Click Peripheral Devices in the left pane.
2. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To release multiple ones, select multiple checkboxes.

- To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.



3. Click Release.

► **After a sensor or actuator is removed from management:**

- The ID number assigned to it is released and can be automatically assigned to any newly-detected sensor or actuator.
- If it is no longer connected to the BCM2, it disappears from the sensor list on the Peripheral Devices page.
- If it remains connected, it continues to be listed on the Peripheral Devices page but its state is changed to *unmanaged*. See **States of Unmanaged Sensors or Actuators** (on page 217).

Disabling the Automatic Management Function

The factory default is to enable the automatic management feature for environmental sensors and actuators. Therefore, when the total number of managed sensors and actuators has not reached 32 yet, the BCM2 automatically brings newly-connected environmental sensors and actuators under management after detecting them.

When this feature is disabled, the BCM2 no longer automatically manages any newly-detected environmental sensors and actuators, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly-added ones.

► **To disable the automatic management feature:**

1. Click the PMC folder.

*Note: The PMC folder is named "my PMC" by default. The name changes after customizing the device name. See **Naming the BCM2** (on page 59).*

2. Click Setup in the Settings section. The setup dialog appears.
3. Deselect the Peripheral Device Auto Management checkbox.
4. Click OK.

Enabling the Front Panel Actuator Control

You can operate the front panel buttons to turn on or off a connected actuator. By default, this function is disabled.

For information on controlling the actuators via the front panel display, see **Peripherals** (on page 18).

► **To enable the front panel actuator control feature:**

1. Choose Device Settings > Security > Front Panel Permissions. The Front Panel Permissions dialog appears.
2. Select the "Peripheral actuator control" checkbox.
3. Click OK.

Controlling Actuators

If you have any DX sensor packages with actuators connected, which can move or control a mechanism or system, you can remotely turn on or off the actuators to control the connected mechanism or system.

► **To turn on or off an individual actuator:**

1. Expand the Peripheral Devices folder in the left pane to show a list of environmental sensors and/or actuators.
2. Click the desired actuator from the navigation tree. That actuator's page opens in the right pane.
3. Click "Switch on" to turn on the actuator, or "Switch off" to turn it off.

► **To turn on or off multiple actuators:**

1. Click Peripheral Devices in the left pane.
2. Select the checkboxes of the desired actuators on the Peripheral Devices page.

Tip: An actuator is indicated with the icon  displayed in the 'Actuator' column.

3. Click "Switch on" or "Switch off" to turn on or off the selected actuators. Confirm you want to switch when prompted.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the BCM2 device.

*Note: To set up an asset management system, see **Connecting Asset Management Sensors** (on page 31).*

Configuring the Asset Sensor

The BCM2 cannot detect how many rack units (tag ports) a connected asset management sensor supports, so you must provide this information manually.

When you add an asset management sensor, you name it.

► **To configure an asset sensor (asset strip):**

1. Expand the Feature Port folder as needed.
2. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

Tip: The same asset sensor's page can be also opened by clicking Feature Port in the left pane, and then double-clicking the asset sensor in the right pane.

3. Click Setup. The setup dialog for the asset sensor appears.

Tip: You can also trigger the same dialog by clicking Asset Management in the left pane, and then clicking Asset Strip Setup or double-clicking the asset sensor in the right pane.

4. To rename the asset sensor, type a new name in the Name field.
5. In the "Number of Rack Units" field, type the total number of rack units supported by the AMS. Default is 48.
6. Here, rack units are the number of asset management tag ports on the asset management strip. For example, if the AMS has 48 asset management tag ports, it supports up to 48 rack units on a cabinet.
7. Determine how to number all rack units on the asset sensor by selecting an option in the Numbering Mode.
 - Top-Down: The rack units are numbered in the ascending order from the highest to the lowest rack unit.
 - Bottom-Up: The rack units are numbered in the descending order from the highest to the lowest rack unit.
8. In the Numbering Offset field, select the starting number. For example, if you select 3, the first rack unit is numbered 3, the second is numbered 4, the third is numbered 5, and so on until the final number.
9. Indicate how the asset sensor is mounted on the rack in the Orientation field. The rack unit that is most close to the RJ-45 connector of the asset sensor will be marked with the index number 1 in the web interface.

For the latest version of asset sensors with a built-in tilt sensor, it is NOT necessary to configure the orientation setting manually. The BCM2 device can detect the orientation of the asset sensors and automatically configure it.

- Top Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
- Bottom Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom. Click OK.

10. Change the LED color settings as needed. See **Setting Asset Sensor LED Colors** (on page 221).

11. Click OK.

Setting Asset Sensor LED Colors

Each LED on the asset sensor indicates the presence and absence of a connected asset tag by changing its color.

By default the LED color of the tag ports with tags connected is green, and the color of the tag ports without tags connected is red. You can change the default LED color settings for all tag ports on an asset sensor assembly.

This feature is accessible only by users with Administrative Privileges.

► To configure all LED colors:

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

3. Click Setup on the asset sensor page. The setup dialog for that asset sensor appears.
4. To change the LED color denoting the presence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color with connected Tag" field.
5. To change the LED color denoting the absence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color without connected Tag" field.
6. Click OK.

*Tip: To make a specific LED's color settings different from other LEDs, see **Configuring a Specific Rack Unit** (on page 222).*

Configuring a Specific Rack Unit

In the BCM2 web interface, a rack unit refers to a tag port on the asset sensor. You can name a specific rack unit, or change its LED color settings so that this LED behaves differently from others on the same asset sensor.

► **To change an LED's settings:**

1. Connect the asset sensor to the EMX if it is not already.
2. Expand the Feature Ports folder in the navigation tree.
3. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

4. Select the rack unit whose LED settings you want to change.
5. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.
6. In the Name field, type a name for identifying this rack unit.
7. Select either Auto or Manual Override as this rack unit's LED mode.
 - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings.
 - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or an LED color for the selected rack unit.
 - LED Mode: Select On to have the LED stay lit, Off to have it stay off, "Slow blinking" to have it blink slowly, or "Fast blinking" to have it blink quickly.
 - LED Color: If you select On, "Slow blinking" or "Fast blinking" in the LED Mode field, select an LED color by either clicking a color in the color palette or typing the hexadecimal RGB value of a color in the accompanying text box.
8. Click OK.

Expanding a Blade Extension Strip

A blade extension strip, like an asset sensor, has multiple tag ports. After connecting it to a specific asset sensor, it is displayed as a folder on that asset sensor's page.

Note: If you need to temporarily disconnect the blade extension strip from the asset sensor, wait at least 1 second before re-connecting it back, or the BCM2 device may not detect it.

► To expand a blade extension strip folder:

1. Click the desired asset sensor in the left pane. The selected asset sensor's page opens in the right pane.
2. Locate the rack unit (tag port) where the blade extension strip is connected.

Rack Units					
	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
▶	2	2			00000007CACB
	3	3			
	4	4			

3. Double-click that rack unit or click the white arrow ▶ prior to the folder icon. The arrow then turns into a black, gradient arrow ▲, and all tag ports of the blade extension strip appear below the folder.

Rack Units					
	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
▲	2	2			00000007CACB
			1		
			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
			10		
			11		
			12		
			13		
			14		
			15		
			16		
	3	3			
	4	4			

► **To collapse a blade extension strip:**

- Double-click the blade extension strip folder, or click the black, gradient arrow ▲ prior to the folder icon. All tag ports under the folder are hidden.

Displaying the Asset Sensor Information

The hardware and software information of the connected asset sensor is available through the web interface.

► **To display the asset sensor information:**

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

3. Click Extended Device Info, where the asset sensor data is displayed.
4. Click Close to quit the dialog.

Webcam Management

With a Logitech® webcam connected to the BCM2 device, you can visually monitor the environment around the BCM2 via snapshots or videos captured by the webcam.

- To view snapshots and videos, you need the permission of either "Change Webcam Configuration" or "View Webcam Sanpshots and Configuration."
- To configure webcam settings, you need the "Change Webcam Configuration" permission.

For more information on the Logitech webcam, see the user documentation accompanying it. For information on connecting a webcam to the BCM2, see **Connecting a Logitech Webcam** (on page 39).

You can manually store snapshots taken from the webcam onto the BCM2 or a remote server. See **Saving Snapshots** (on page 229) or **Configuring Webcam Storage** (on page 226).

Links to snapshots or videos being captured by a webcam can be sent via email or instant message. See **Sending Snapshots or Videos in an Email or Instant Message** (on page 230).

Events that trigger emails containing snapshots from a webcam can be created. See **Creating Actions** (on page 154).

Configuring Webcams

Before you can configure a webcam, it must be connected to the BCM2. See **Connecting a Logitech Webcam** (on page 39).

► To configure a webcam:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Click on the webcam you want to configure and then click Setup at the bottom right of page. The Webcam Setup dialog opens.
3. Enter a name for the webcam. Up to 64 characters are supported.
4. Type the location information in each location field if needed. Up to 63 characters are supported.
5. Select a resolution for the webcam.
 - If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.
6. Select the webcam mode. This can be changed as needed once the webcam is configured.

- a. Video - the webcam is in video mode. Set the Framerate (frames per second) rate.
 - b. Snapshot - the webcam displays images from the webcam. Set the "Time between Snapshots" rate as measured in seconds.
7. Click OK. The image or video from the webcam is now available in the BCM2 once you click on the webcam in the navigation tree.

► **To edit a webcam configuration:**

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Double-click on the webcam you want to edit. The webcam image or video opens in a new tab.
3. Click Setup .
4. Edit the information as needed. Changes to the resolution do not apply to existing, stored images - it applies only to images and videos taken after the resolution is changed.
5. Click OK.

Configuring Webcam Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the BCM2 by default. Up to ten (10) images can be stored on the BCM2 at once.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.

Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten. Rebooting the BCM2 deletes all webcam snapshots that are saved on the device.

► **To configure another storage location for images:**

1. In the navigation tree, click Snapshots under the Webcam Management folder. The Snapshots page opens.
2. Click on the Setup Storage icon . The Storage Setup dialog opens.

3. By default, Local, meaning the BCM2, is the designated default storage.
4. Select CIFS/Samba as the storage location.
5. Enter the server where to store the images.
6. If needed, enter the share drive/folder to store the images in.
7. Enter the username and password needed to access the server where the images are stored.
8. Enter or use the slide bar to set the number of images that can be saved to the storage location.
9. Click OK.

Adjusting Image Properties

If any snapshot or video properties, such as the brightness, contrast, saturation, and gain settings, do not satisfy your needs, adjust them.

► **To adjust the image or video properties:**

1. Select the webcam shown on the Webcam Management page or in the navigation tree. See **Configuring Webcams** (on page 225).
2. Click Setup or .
3. Click the Controls tab.
4. Adjust the desired property by adjusting the corresponding slide bar.
Or click "Set to webcam defaults" to restore all settings to this webcam's factory defaults.
5. Click OK.

Viewing Webcam Snapshots or Videos

You can switch between snapshots or live videos being captured by a webcam.

The snapshot or video is displayed either in the BCM2 web interface or in a Primary Standalone Live Preview window that you open.

You can open a maximum of five Primary Standalone Live Preview windows.

*Note: For remote Live Preview sessions, such as those accessed via a link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the BCM2 interface, and up to two (2) remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** (on page 230).*

► To switch between snapshot and video modes:

1. Click the desired webcam's icon in the navigation tree.

Snapshots or videos captured by the webcam are displayed in the right pane of the BCM2 web interface once a webcam is selected in the navigation tree.

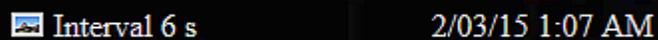
Snapshots and videos can also be displayed in Live Preview mode in the Primary Standalone Live Preview window by clicking on the Live Preview icon .

*Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** (on page 195).*

2. By default the BCM2 enters the snapshot mode. Wait around one minute for the snapshot to appear.

In the snapshot mode, three pieces of information are displayed on the top of the image:

- A snapshot mode icon .
- The interval time between snapshots (in seconds).
- A time stamp.



 Interval 6 s 2/03/15 1:07 AM

The webcam's location information, if available, is displayed in the Location pane of the BCM2 web interface.

- To change any image settings, click Setup . See **Configuring Webcams** (on page 225) or **Adjusting Image Properties** (on page 227).
 - To save the snapshot being displayed, click the "Store Snapshot to Webcam Storage" icon . See **Saving Snapshots** (on page 229).
3. To switch to the video mode, click Setup  and select Video in the Webcam Mode field.

In the video mode, two pieces of information are displayed on the top of the image:

- A video mode icon .
- The number of frames to take per second (fps).



To change any video settings, click Setup .

4. To return to the snapshot mode, repeat the above step and select Snapshot.

Saving Snapshots

If it is intended to keep the snapshot being displayed on the webcam, you can manually save it onto the BCM2. A snapshot is saved as a JPEG file and stored on the Snapshots page.

Warning: The snapshots stored on the BCM2 are cleared when rebooting the BCM2. Check the importance of the snapshots before performing the reset.

► To save the snapshot being displayed:

1. In the navigation tree, click on the webcam you want to take a snapshot with. The webcam image is displayed in the right pane.
The webcam must be in snapshot mode in order to take snapshots. If the webcam is in video mode, click Setup in the right pane above the video image to open the Webcam Setup dialog, then select the Snapshot radio button.
2. Once the snapshot image being taken by the selected webcam is displayed in the right pane, click the Store Snapshot to Webcam Storage  icon above the image to take a snapshot. Up to ten (10) snapshots can be stored at once on the device.

3. Click on the Snapshots icon in the navigation tree to verify that those snapshots are successfully saved and listed on the Snapshots page.

*Tip: To store snapshots on a remote server rather than the BCM2, see **Configuring Webcam Storage** (on page 226).*

Sending Snapshots or Videos in an Email or Instant Message

Whenever you open a Primary Standalone Live Preview window, a unique URL is generated for this window session, which permits a link to the snapshot or video being captured.

You are able to email or instant message up to two (2) recipients a link to webcams attached to the BCM2. Users can then click on the links and view snapshots or videos.

A total of three sessions based on the same URL are supported, including a Primary Standalone Live Preview window of the sender and two remote sessions of the recipients.

*Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** (on page 195).*

For explanation of this topic, the message sender is User A and the recipient is User B.

The recipient is able to access the snapshot or video image via the link in any of the following scenarios:

- The snapshot or video remains open in the Primary Standalone Live Preview window in User A's side. If so, even though User A logs out of the BCM2 interface or the login session times out, the link is available.

Or

- At least a remote session based on the same URL remains open. If so, even though User A has closed the Primary Standalone Live Preview window, the link is available.

Or

- Neither the Primary Standalone Live Preview window nor any remote session based on the same URL remains open, but the idle timeout period has not expired yet since the last Live Preview window session was closed. For information on idle timeout, see **Enabling Login Limitations** (on page 131).

Tip: If the idle timeout has not expired, the <webcam> user for that Live Preview URL remains shown in the Connected Users dialog.

Best Practice

As a best practice, User A should open the snapshot or video using a Primary Standalone Live Preview window and leave that window open at least until User B opens the snapshot or video via the link.

Once User B opens the snapshot or video via the link, User A can close the Primary Standalone Live Preview window.

User B should let User A know that the link has been opened.

► To send a snapshot or video link via email or instant message:

1. In the navigation tree, click on the webcam that is capturing the snapshot or video you want to provide a link to other people. The snapshot or video is displayed in Live Preview mode in the right pane.
2. Click on the Live Preview icon  located above the snapshot or video. The snapshot or video opens in a standalone Live Preview window.
3. Copy the URL from the Live Preview window, paste it into the email or instant message application. Leave the Live Preview window open at least until the recipient opens the snapshot or video via the link.

Managing the Snapshots Saved to BCM2

A maximum of 10 saved snapshots can be stored and displayed on the Snapshots page of the BCM2.

See **Saving Snapshots** (on page 229) for instructions on storing snapshots on the BCM2.

The Snapshots page is categorized into three sections: Storage, Snapshot and Details.

- Storage: shows a list of all saved snapshots.
On the top of the Storage section, the number following "Used" indicates the total of saved snapshots and the number following "Size" indicates maximum number of snapshots allowed in storage.

- Snapshot: displays the image of the snapshot being selected.
- Details: shows the information which had been entered when the snapshot was saved, including resolution and location settings.

*Tip: To save more than 10 snapshots, save snapshots onto a remote server. See **Configuring Webcam Storage** (on page 226).*

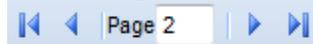
▶ **To view the saved snapshots:**

1. In the navigation tree, click Snapshots under the Webcam Management folder. The snapshots are displayed in the right pane in the Storage section of the page.
2. View an individual snapshot by clicking on a snapshot file in the Storage section of the page.

The size of each snapshot file, the date and time each snapshot was taken, and the webcam that took each snapshot, is displayed when viewing snapshots.

Details, such as the webcam location and/or labels, if any, are displayed in the Details section below the snapshot in the right pane. This information is defined when the webcam is initially configured. See **Configuring Webcams** (on page 225).

3. Use the navigation icons to move through each snapshot, or enter a specific page number to jump to that snapshot page.



4. Click the Refresh icon  to refresh the page. New snapshots are displayed if they are available.

▶ **To delete any snapshot from the storage:**

- Delete snapshots by selecting the checkbox next to the snapshot you want to delete, then clicking the Delete icon  at the top of the section. To select and delete all snapshots at once, click the checkbox in the checkbox column header, then click the Delete icon.

Firmware Upgrade

You may upgrade your BCM2 device to benefit from the latest enhancements, improvements and features.

Firmware files are available on Raritan website's **Support page** (<http://www.raritan.com/support/>).

Updating the BCM2 Firmware

► **To update the firmware:**

1. Choose Maintenance > Update Firmware. The Update Firmware dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

Warning: Do NOT power off the BCM2 during the update.

During the firmware update:

- A progress bar appears in the web interface, indicating the update status.
 - The front panel display on the BCM2 shows three digits: 'FuP' or 'FUP.'
 - No users can successfully log in to the BCM2.
 - The user management operation, if any, is forced to suspend.
7. When the update is complete, a message appears, indicating the update is successful.
 8. The BCM2 resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

*Note 2: If you are using the BCM2 with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using. See **Using SNMP** (on page 244) in the User Guide.*

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the BCM2 device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

► **To view the firmware update history:**

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.
 - Date and time of the firmware upgrade event
 - Previous firmware version
 - Update firmware version
 - Firmware upgrade result
2. You may change the number of displayed columns or re-sort the list for better viewing the data.
3. To view the details of any firmware upgrade event, select it and click Details, or simply double-click the event. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the BCM2 device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate BCM2 firmware file is required in the recovery procedure.

Updating the Asset Sensor Firmware

After connecting the asset sensor to the BCM2 device, it automatically checks its own firmware version against the version of the asset sensor firmware stored in the BCM2 firmware. If two versions are different, the asset sensor automatically starts downloading the new firmware from the BCM2 device to upgrade its own firmware.

During the firmware upgrade, the following events take place:

- The asset sensor is completely lit up, with the blinking LEDs changing the color from red to green.
- A firmware upgrade process is indicated in the BCM2 web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

Network Diagnostics

The BCM2 provides the following tools in the web interface for diagnosing potential networking issues.

- Ping
- Trace Route
- List TCP Connections

*Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** (on page 377).*

Pinging a Host

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

► **To ping a host:**

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 20 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

► **To trace the route for a host:**

1. Choose Maintenance > Network Diagnostics > Trace Route. The "Trace Route to Host" dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. In the Timeout (s) field, type a timeout value in seconds to end the trace route operation. Note that if the timeout value is too small, the trace route results may be incomplete.
4. To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select the Use ICMP Packets checkbox.
5. Click Run. A dialog appears, displaying the Trace Route results.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

► **To list TCP connections:**

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP Connections window appears.
2. Click Close to quit the dialog.

Downloading Diagnostic Information

Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the BCM2 device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges.

► **To retrieve a diagnostic file:**

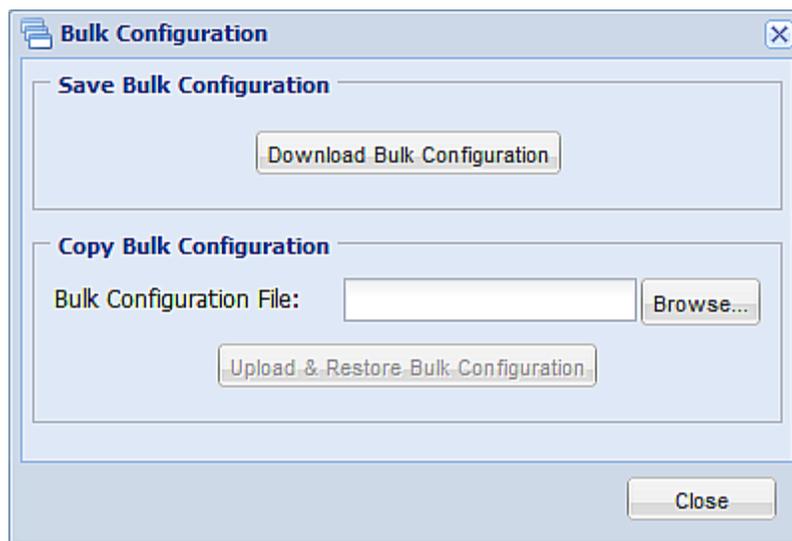
1. Choose Maintenance > Download Diagnostic Information. You are then prompted to save or open the file.
2. Click Save to save the file.

3. E-mail this file as instructed by Raritan Technical Support.

Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured BCM2 device to your PC. You can use this configuration file to copy that configuration to other BCM2 devices of the same model and firmware version.

You must have the administrator privileges to save and copy the BCM2 configurations.



*Note: No device-specific data is saved to the Bulk Configuration file, such as environmental sensor or certain network settings. To back up or restore a specific BCM2 device's all settings, use the Backup/Restore feature instead. See **Backup and Restore of BCM2 Device Settings** (on page 240).*

Saving a BCM2 Configuration

A source device is an already configured BCM2 device that is used to create a configuration file containing the settings that can be shared between BCM2 devices. These settings include user and role configurations, thresholds, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Panel and power meter data
- Branch circuit data
- Environmental sensor and actuator names
- States and values of environmental sensors and actuators
- TLS certificate

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the BCM2 devices in a different time zone than the source device.

▶ **To save a configuration file:**

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Copying the BCM2 Configuration

A target device is the BCM2 device that loads another BCM2 device's configuration file.

Copying a source BCM2 device's configuration to a target device adjusts the target BCM2 device's settings to match those of the source BCM2 device. In order to successfully copy a source BCM2 device's configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target BCM2 device must be running the same firmware version as the source BCM2 device.
- The target BCM2 device must be of the same model type as the source BCM2 device.

► **To copy a BCM2 configuration:**

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See **Firmware Upgrade** (on page 232).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse to select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.
A message appears, prompting you to confirm the operation and enter the admin password.
6. Enter the admin password, then click Yes to confirm the operation.
7. Wait until the BCM2 device resets and the Login page re-appears, indicating that the configuration copy is complete.

Note: On startup, the BCM2 performs all of its functions, including event rules and logs, based on the new configuration file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

Backup and Restore of BCM2 Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore BCM2 device settings, you should perform the Backup/Restore feature.

All BCM2 information is captured in the XML backup file except for the device logs and TLS certificate.

*Note: To perform the bulk configuration among multiple BCM2 devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** (on page 237).*

► **To download a backup BCM2 XML file:**

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Save Device Settings section, click Download Device Settings. Save the file to your computer.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

► **To restore the BCM2 using a backup XML file:**

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Copy Device Settings section, click Browse to locate the file.
3. Click Upload & Restore Device Settings to upload the file.

A message appears, prompting you to confirm the operation and enter the admin password.

4. Enter the admin password, then click Yes to confirm the operation.
5. Wait until the BCM2 device resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the BCM2 performs all of its functions, including event rules and logs, based on the new configuration file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

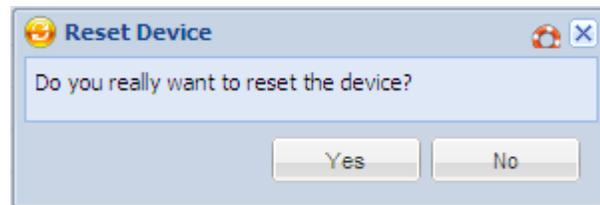
Rebooting the BCM2

You can remotely reboot the BCM2 device via the web interface. Rebooting the BCM2 does not reset the configuration of the device as is done during a factory reset.

Note: Rebooting the BCM2 deletes all webcam snapshots that are saved on the device.

► **To reboot the device:**

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the BCM2.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the BCM2 device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the BCM2 help

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the BCM2 device through the web interface.

► **To retrieve the embedded software packages information:**

1. Choose Help > About PX iPDU. The About PX iPDU dialog appears, with a list of open source packages displayed.

2. You can click any link in the dialog to access related information or download any software package.

Browsing through the Online Help

The BCM2 Online Help is accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriptlets. Consult your browser help for information on enabling these features.

► To use the BCM2 online help:

1. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:
 - To view the next topic, click the Next icon  in the toolbar.
 - To view the previous topic, click the Previous icon .
 - To view the first topic, click the Home icon .
4. To expand or collapse a topic that contains sub-topics, do the following:
 - To expand any topic, click the white arrow  prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow , and sub-topics appear below the topic.
 - To collapse any expanded topic, click the black, gradient arrow  prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow , and all sub-topics below that topic disappear.
5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon  to start the search.
 - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

The search results are displayed in the left pane.

6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon  in the toolbar.

9. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon .
10. To print the currently selected topic, click the "Print this page" icon .

Chapter 5 Using SNMP

This SNMP section helps you set up the BCM2 for use with an SNMP manager. The BCM2 can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling SNMP	244
Configuring Users for Encrypted SNMP v3	245
Configuring SNMP Notifications	246
SNMP Gets and Sets	251

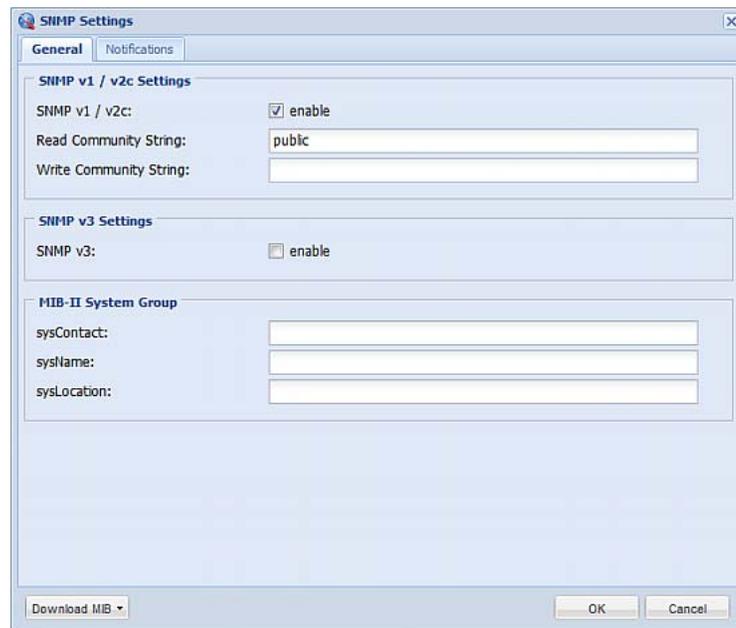
Enabling SNMP

By default, SNMP v1/v2c is enabled on the BCM2 so the BCM2 can communicate with an SNMP manager. If you have disabled the SNMP, it must be enabled to communicate with an SNMP manager.

Note that read-only access is enabled and the community string is public.

► To enable SNMP:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
 - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
 - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

*Tip: You can permit or disallow a user to access the BCM2 via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** (on page 245).*

4. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system
 - b. sysName - the name assigned to the system
 - c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your BCM2 is used by the SNMP manager.

*Important: You must download the SNMP MIB for your BCM2 to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** (on page 252).*

6. Click OK.

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the BCM2.

► **To configure users for SNMP v3 encrypted communication:**

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of **Creating a User Profile** (on page 96).

5. Click OK. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Notifications

The BCM2 automatically keeps an internal log of events that occur. See **Event Rules and Actions** (on page 153). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The BCM2 provides you with the ability to create SNMPv2c and SNMPv3 TRAP communications, or SNMPv2c and SNMPv3 INFORM communications.

SNMP TRAP communications capture and send information via SNMP, but no confirmation that the communication between the devices has succeeded is provided by the receiving device.

SNMP INFORM communications capture and send information via SNMP, and an acknowledgment that the communication was received by the receiving device is provided. If the inform communication fails, it is resent. You can define the number of times and the intervals to resend the inform communication, or leave the defaults of five resends in three second intervals.

Note: SNMP INFORM communications may take up slightly more network resources than SNMP TRAP communications since there are additional communications between the devices, and due to additional network traffic created should the initial communication fail and another is sent.

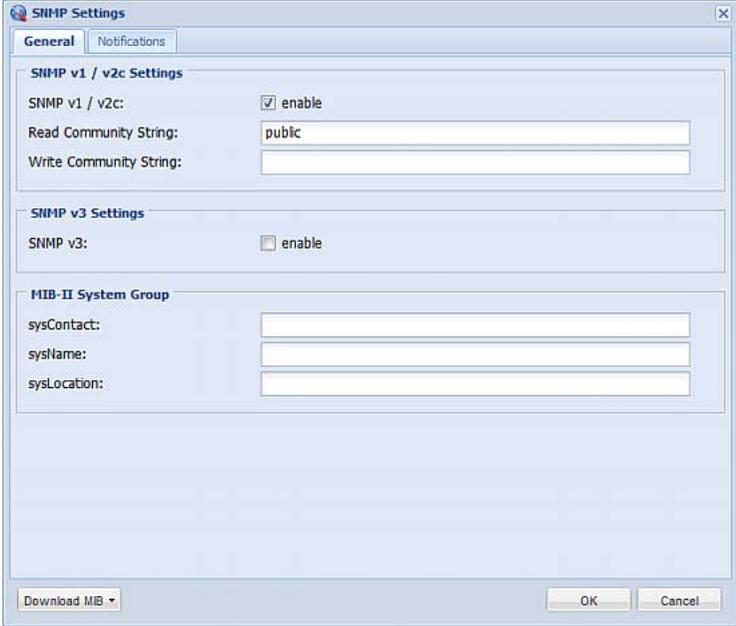
Use SNMP TRAP rules if you do not need confirmation that the communication has succeeded, and if you need to conserve network resources. Use SNMP INFORM communications to ensure more reliable communications, and if network resources can be managed with the potential additional network traffic.

*Note: You should update the MIB used by your SNMP manager when updating to a new BCM2 release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** (on page 252).*

SNMPv2c Notifications

► **To configure the BCM2 to send SNMP notifications:**

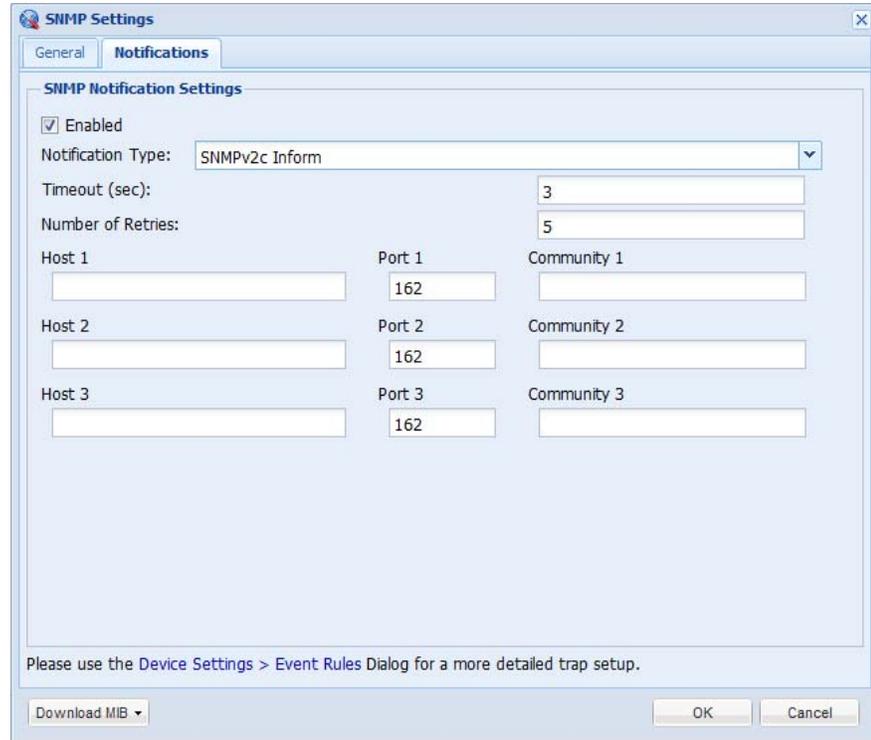
1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. The dialog is divided into three sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the 'SNMP v1 / v2c Settings' section, the 'SNMP v1 / v2c:' checkbox is checked and labeled 'enable'. The 'Read Community String:' field contains the text 'public', and the 'Write Community String:' field is empty. In the 'SNMP v3 Settings' section, the 'SNMP v3:' checkbox is unchecked. In the 'MIB-II System Group' section, the 'sysContact:', 'sysName:', and 'sysLocation:' fields are all empty. At the bottom of the dialog, there is a 'Download MIB' button with a dropdown arrow, and 'OK' and 'Cancel' buttons.

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

- From the Notification Type drop-down, select the type of SNMP notification.

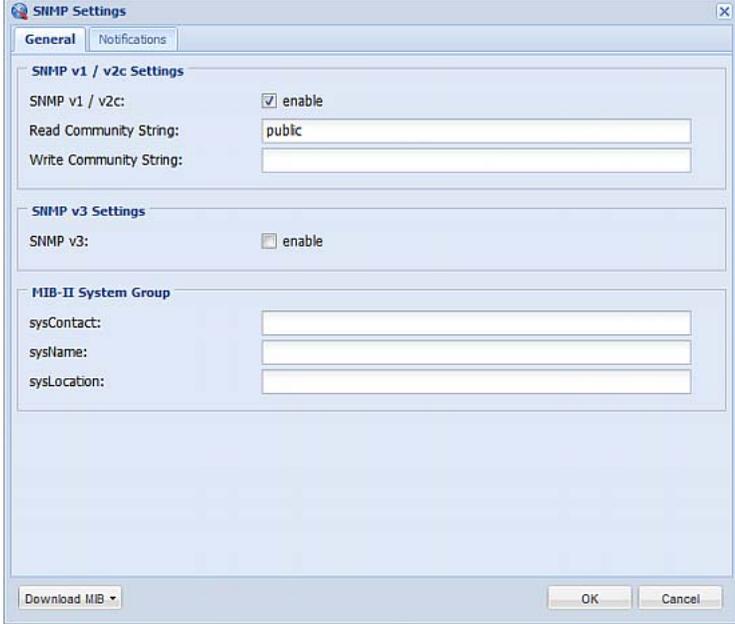


- For SNMP INFORM communications, leave the resend settings at their default or:
 - In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
 - In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
- In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent. You can specify up to 3 SNMP destinations.
- In the Port fields, enter the port number used to access the device(s).
- In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.
- Click OK.

SNMPv3 Notifications

► **To configure the BCM2 to send SNMPv3 notifications:**

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. The dialog is divided into three sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the 'SNMP v1 / v2c Settings' section, the 'SNMP v1 / v2c:' checkbox is checked and labeled 'enable'. The 'Read Community String:' field contains the text 'public', and the 'Write Community String:' field is empty. In the 'SNMP v3 Settings' section, the 'SNMP v3:' checkbox is unchecked. In the 'MIB-II System Group' section, the 'sysContact:', 'sysName:', and 'sysLocation:' fields are empty. At the bottom of the dialog, there is a 'Download MIB' button with a dropdown arrow, and 'OK' and 'Cancel' buttons.

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.

The screenshot shows the 'SNMP Settings' dialog box with the 'Notifications' tab selected. The 'SNMP Notification Settings' section is expanded, showing a list of configuration options. The 'Enabled' checkbox is checked. The 'Notification Type' is set to 'SNMPv3 Trap'. The 'EngineID' field is populated with a long hexadecimal string. The 'Port' field is set to '162'. The 'Timeout (sec)' field is set to '3', and the 'Number of Retries' field is set to '5'. The 'Security Level' is set to 'authPriv', and the 'Authentication Protocol' is set to 'SHA'. The 'Privacy Protocol' is set to 'AES'. There are also fields for 'Host', 'UserID', 'Authentication Passphrase', 'Confirm Authentication Passphrase', 'Privacy Passphrase', and 'Confirm Privacy Passphrase', which are currently empty. At the bottom of the dialog, there is a 'Download MIB' button and 'OK' and 'Cancel' buttons. A note at the bottom of the dialog reads: 'Please use the Device Settings > Event Rules Dialog for a more detailed trap setup.'

4. For SNMP TRAPS, the engine ID is prepopulated.
5. For SNMP INFORM communications, leave the resend settings at their default or:
 - a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
 - b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
6. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
 - a. Host name
 - b. Port number
 - c. User ID needed to access the host
 - d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. <ul style="list-style-type: none"> • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. <ul style="list-style-type: none"> • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

SNMP Gets and Sets

In addition to sending notifications, the BCM2 is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the BCM2, such as the system location, and the current on a specific branch circuit.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the BCM2 device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The BCM2 does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom BCM2 MIB.

The BCM2 MIB

The SNMP MIB file is required for using your BCM2 device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the BCM2 can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

▶ **To download the file from the SNMP Settings dialog:**

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appears.
3. Select the desired MIB file to download.
 - PDU2-MIB: The SNMP MIB file for BCM2 power management.
 - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
4. Click Save to save the file onto your computer.

▶ **To download the file from the Device Information dialog:**

1. Choose Maintenance > Device Information.
2. Click the "download" link in the PDU-MIB field to download the desired SNMP MIB file.
 - PDU2-MIB: The SNMP MIB file for BCM2 power management.
 - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.

The "USB Console INF file" link lets you download the USB-to-serial driver that may be required only when the BCM2 is connected to a computer via a USB cable. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 258) for details.

3. Click Save to save the file onto your computer.

Layout

Opening the MIB reveals the custom objects that describe the BCM2 system at the unit level as well as at the individual branch circuit level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



```

BCM2-MIB - Notepad
File Edit Format View Help

measurementsGroup      OBJECT-GROUP
                        OBJECTS {
                            measurementsUnitSensorIsAvailable,
                            measurementsUnitSensorState,
                            measurementsUnitSensorValue,
                            measurementsUnitSensorTimeStamp,
                            measurementsUnitSensorSignedValue,
                            measurementsInletSensorIsAvailable,
                            measurementsInletSensorState,
                            measurementsInletSensorValue,
                            measurementsInletSensorTimeStamp,
                            measurementsInletSensorSignedValue,
                            .
                            .
                            .
                            measurementsExternalSensorIsAvailable,
                            measurementsExternalSensorState,
                            measurementsExternalSensorValue,
                            measurementsExternalSensorTimeStamp,
                            measurementsTransferSwitchSensorIsAvailable,
                            measurementsTransferSwitchSensorState,
                            measurementsTransferSwitchSensorValue,
                            measurementsTransferSwitchSensorTimeStamp,
                            measurementsTransferSwitchSensorSignedValue,
                            measurementsCircuitSensorIsAvailable,
                            measurementsCircuitSensorState,
                            measurementsCircuitSensorValue,
                            measurementsCircuitSensorTimeStamp,
                            measurementsCircuitSensorSignedValue,
                            measurementsCircuitPoleSensorIsAvailable,
                            measurementsCircuitPoleSensorState,
                            measurementsCircuitPoleSensorValue,
                            measurementsCircuitPoleSensorTimeStamp,
                            measurementsCircuitPoleSensorSignedValue
                        }
                        STATUS current
                        DESCRIPTION
                            "A collection of objects providing measurements (most recent data)
capabilities.
                            about the PDU."
                        ::= { groups 3 }

```

For example, the measurementsGroup group contains objects for sensor readings of BCM2 as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor reading as an unsigned integer. The value of this OID variable should be scaled by unitSensorDecimalDigits...". pduRatedCurrent, part of the configGroup group, describes the current ratings of all panels, power meter modules and the main controller attached to the BCM2.

Note that the MIB file uses the following terms to refer to the device or its components:

- power meter: Panels or power meter modules
- panel or power meter panel: Panels
- circuit: Panel branch circuits
- px: The BCM2 device
- pdu or unit: The BCM2 device's main controller, panels and power meter modules

Example: "pduld" refers to the ID numbers of the BCM2's main controller, panels and power meter modules. The main controller's ID is always 0.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the BCM2 to generate a warning and send an SNMP notification when certain parameters are exceeded. See **Setting Power Thresholds** (on page 114) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 6 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a BCM2 device.

In This Chapter

About the Interface	255
Logging in to CLI	256
Help Command.....	262
Querying Available Parameters for a Command.....	263
Showing Information.....	263
Clearing Information	283
Configuring the BCM2 Device and Network.....	283
Configuring Environmental Sensors' Default Thresholds.....	357
Environmental Sensor Configuration Commands	359
Environmental Sensor Threshold Configuration Commands	363
Actuator Configuration Commands	366
USB-Cascading Configuration Commands	367
Asset Management Commands	367
Actuator Control Operations	374
Unblocking a User	376
Resetting the BCM2	376
Network Troubleshooting.....	377
Retrieving Previous Commands.....	380
Automatically Completing a Command	381
Logging out of CLI	381

About the Interface

The BCM2 provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the BCM2 device
- Display the BCM2 and network information, such as the device name, firmware version, IP address, and so on
- Configure the BCM2 and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

*Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying Network Service Settings** (on page 69).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

If a security login agreement has been enabled, you must accept the agreement in order to complete the login. Users are authenticated first and the security banner is checked afterwards.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

For information on how to make a local connection, see **Making an RS-232 or USB Connection** (on page 257).

► **To log in using HyperTerminal:**

1. Connect your computer to the BCM2 via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

Make sure the COM port settings use this configuration:

- Bits per second = 115200 (115.2Kbps)
- Data bits = 8
- Stop bits = 1
- Parity = None
- Flow control = None

Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the BCM2. The Username prompt appears.

Username: _

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

```
Username: admin
Password: _
```

5. Type a password and press Enter. The password is case sensitive. After properly entering the password, the # or > system prompt appears. See **Different CLI Modes and Prompts** (on page 261) in the User Guide for more information.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the BCM2.

Making an RS-232 or USB Connection

To access the CLI locally, you must connect the BCM2 to a computer via RS-232 or USB.

Establish one of the following connections to a computer.

▶ Serial RS-232 connection:

1. Connect one end of the null-modem cable to the male RS-232 port labeled CONSOLE / MODEM on the BCM2.
2. Connect the other end to your computer's RS-232 port (COM).

▶ USB connection:

1. A USB-to-serial driver is required in Windows®. Install this driver before connecting the USB cable. See **Installing the USB-to-Serial Driver (Optional)** (on page 258).
2. Connect a USB cable between the BCM2 device's USB-B port and a computer's USB-A port.

Note: Not all serial-to-USB converters work properly with the BCM2 so Raritan does not introduce the use of such converters.

Installing the USB-to-Serial Driver (Optional)

The BCM2 can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Serial Console" is required for Microsoft® Windows® operating systems.

Download the USB Driver file from the Raritan website's **Support page** (<http://www.raritan.com/support/>). The driver contains the *dominion-serial.inf*, *dominion-serial.cat* and *dominion-serial-setup-<n>.exe* files.

Note: <n> in the filename of "dominion-serial-setup-<n>.exe" represents the file's version number.

There are two ways to install this driver: automatic and manual installation. Automatic driver installation is highly recommended.

► Automatic driver installation in Windows®:

1. Make sure the BCM2 is NOT connected to the computer via a USB cable.
2. Run *dominion-serial-setup-<n>.exe* on the computer and follow online instructions to install the driver.

Note: If any Windows security warning appears, accept it to continue the installation.

3. Connect the BCM2 to the computer via a USB cable. The driver is automatically installed.

► Manual driver installation in Windows®:

1. Make sure the BCM2 has been connected to the computer via a USB cable.
2. The computer detects the new device and the "Found New Hardware Wizard" dialog appears. If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the *Serial Console*, and choose Update Driver.
3. Select the option of driver installation from a specific location, and then specify the location where both *dominion-serial.inf* and *dominion-serial.cat* are stored.

Note: If any Windows security warning appears, accept it to continue the installation.

4. Wait until the installation is complete.

Note: If the BCM2 enters the disaster recovery mode when the USB serial driver is not installed yet, it may be shown as a 'GPS camera' in the Device Manager on the computer connected to it.

► **In Linux:**

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the BCM2 to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

```
> set line /dev/ttyACM0
> Connect
```

With SSH or Telnet

You can remotely log in to the command line interface (CLI) using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

► **To log in using SSH or Telnet:**

1. Ensure SSH or Telnet has been enabled. See **Modifying Network Service Settings** (on page 69) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as: █
```

3. Type a name and press Enter. The name is case sensitive.

Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password: █
```

4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the # or > system prompt appears. See **Different CLI Modes and Prompts** (on page 261) in the User Guide for more information.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the BCM2.

With an Analog Modem

The BCM2 supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

▶ **To connect to the BCM2 via the modem:**

1. Make sure the BCM2 has an analog modem connected. See **Connecting an Analog Modem** (on page 41).
2. Make sure the computer you are using has an appropriate modem connected.
3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the BCM2. See **Configuring the Serial Port** (on page 84).
4. Type the following AT command to make a connection with the BCM2.

`ATD<modem phone number>`
5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

▶ **To disconnect from the BCM2:**

1. Return to the modem's command mode using the escape code +++.
2. After the OK prompt appears, type the following AT command to disconnect from the BCM2.

`ATH`

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- **User Mode:** When you log in as a normal user, who may not have full permissions to configure the BCM2 device, the **>** prompt appears.
- **Administrator Mode:** When you log in as an administrator, who has full permissions to configure the BCM2 device, the **#** prompt appears.
- **Configuration Mode:** You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change BCM2 device and network configurations. See *Entering Configuration Mode* (on page 284).
- **Diagnostic Mode:** You can enter the diagnostic mode from the administrator or user mode. In this mode, the prompt changes to **diag:#** or **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See *Entering Diagnostic Mode* (on page 378).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a BCM2 device over the local connection.

When accessing or upgrading multiple BCM2 devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

Help Command

The help (?) command shows a list of main CLI commands available for the current mode. This is helpful when you are not familiar with CLI commands.

▶ **Help command under the administrator mode:**

```
#          ?
```

▶ **Help command under the configuration mode:**

```
config:#   ?
```

▶ **Help command under the diagnostic mode:**

```
diag:#     ?
```

Press Enter after typing the help command, and a list of main commands for the current mode is displayed.

*Tip: You can check what parameters are available for a specific CLI command by adding the help command to the end of the queried command. See **Querying Available Parameters for a Command** (on page 263).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

▶ **To query available parameters for the "show" command:**

```
#          show ?
```

▶ **To query available parameters for the "show user" command:**

```
#          show user ?
```

▶ **To query available network configuration parameters:**

```
config:#   network ?
```

▶ **To query available role configuration parameters:**

```
config:#   role ?
```

▶ **To query available parameters for the "role create" command:**

```
config:#   role create ?
```

Showing Information

You can use the show commands to view current settings or the status of the BCM2 device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

*Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** (on page 261).*

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
# show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
# show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both IPv4 and IPv6 settings. <hr/> <i>Tip: You can also type the command without adding this option "all" to get the same data.</i> <hr/>
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, including LAN interface speed, duplex mode, current LAN interface status and LAN interface MAC address.

```
# show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
# show network mode
```

Note: If the BCM2 is a slave device connected to the LAN via the master BCM2 device, the `show network mode` command displays wired(USB) instead of wired.

Wireless Configuration

This command only shows the wireless configuration of the BCM2 device, such as the SSID parameter.

```
# show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
# show network services <option>
```

Variables:

- <option> is one of the options: *all, http, https, telnet, ssh, snmp, modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
http	Only displays the TCP port for the HTTP service.

Option	Description
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

Date and Time Settings

This command shows the current date and time settings on the BCM2 device.

```
# show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show time details
```

Default Measurement Units

This command shows the default measurement units applied to the BCM2 web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
# show user defaultPreferences
```

*Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the BCM2. See **Existing User Profiles** (on page 274) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
# show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show externalsensors <n> details
```

```
External sensor 3 ('Temperature 1')
```

```
Sensor type: Temperature
```

```
Reading: 31.8 deg C (normal)
```

```
Serial number: AEI0950133
```

```
Description: Not configured
```

```
Location: X Not configured
```

```
Y Not configured
```

```
Z Not configured
```

```
Position: Port 1
```

```
Using default thresholds: yes
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripheral Devices page of the BCM2 web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

Note: A discrete (on/off) sensor displays the sensor state instead of the numeric reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information..

Environmental Sensor Package Information

Different from the "show externalsensors" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
# show peripheralDevicePackages
```

Information similar to the following is displayed. An environmental sensor package is a peripheral device package.

```
Peripheral Device Package 1
Serial Number:    AEI7A00022
Package Type:    DPX-T1H1
Position:        Port 1
Package State:   operational
Firmware Version: Not available
```

```
Peripheral Device Package 2
Serial Number:    AEI7A00021
Package Type:    DPX-T3H1
Position:        Port 1
Package State:   operational
Firmware Version: Not available
```

Actuator Information

This command syntax shows an actuator's information.

```
# show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show actuators <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the BCM2 web interface or CLI. It is an integer starting at 1.

Displayed information:

- Without the parameter "details," only the actuator ID, type and state are displayed.
- With the parameter "details," more information is displayed in addition to the ID number and actuator state, such as the serial number and X, Y, and Z coordinates.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
# show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor externalsensor <n> details
```

```
External sensor 3 (Temperature):
```

```
Reading: 31.8 deg C
```

```
State: normal
```

```
Active Thresholds: Sensor specific thresholds
```

```
Default Thresholds for Temperature sensors:
```

```
Lower critical threshold: 10.0 deg C
```

```
Lower warning threshold: 15.0 deg C
```

```
Upper warning threshold: 30.0 deg C
```

```
Upper critical threshold: 35.0 deg C
```

```
Deassertion hysteresis: 1.0 deg C
```

```
Assertion timeout: 0 samples
```

```
Sensor Specific Thresholds:
```

```
Lower critical threshold: 8.0 deg C
```

```
Lower warning threshold: 13.0 deg C
```

```
Upper warning threshold: 28.0 deg C
```

```
Upper critical threshold: 33.0 deg C
```

```
Deassertion hysteresis: 1.0 deg C
```

```
Assertion timeout: 0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripheral Devices page of the BCM2 web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
# show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors
	<i>Tip: You can also type the command without adding this option "all" to get the same data.</i>

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

USB-Cascading Configuration Information

This command shows the USB-cascading configuration, such as the cascading mode and device position.

```
#          show cascading
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show cascading details
```

Security Settings

This command shows the security settings of the BCM2.

```
#          show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
# show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
# show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the BCM2 device.

```
# show serial
```

Asset Sensor Settings

This command shows the asset sensor settings, such as the total number of rack units (tag ports), asset sensor state, numbering mode, orientation, available tags and LED color settings.

```
# show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset sensor information. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific asset sensor number	Displays the settings of the asset sensor connected to the specified FEATURE port number. For the BCM2 device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Sensor

For the Raritan asset sensor, a rack unit refers to a tag port. This command shows the settings of a specific rack unit or all rack units on an asset sensor, such as a rack unit's LED color and LED mode.

```
# show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset sensor. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>

Option	Description
A specific number	Displays the settings of the specified rack unit on the specified asset sensor. Use the index number to specify the rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#          show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset sensor. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <blade_slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit. The number of each tag port on the blade extension strip is available on the Asset Strip page.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

▶ **Show the last 30 entries:**

```
# show eventlog
```

▶ **Show a specific number of last entries in the event log:**

```
# show eventlog limit <n>
```

▶ **Show a specific type of events only:**

```
# show eventlog class <event_type>
```

▶ **Show a specific number of last entries associated with a specific type of events only:**

```
# show eventlog limit <n> class <event_type>
```

Variables:

- <n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.

Event type	Description
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
lhx	Schroff® LHX/SHX heat exchanger events.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.

Wireless LAN Diagnostic Log

This command shows the diagnostic log for the wireless LAN connection.

```
# show wlanlog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
# show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
# show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show serverReachability server <n> details
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

#	IP address	Enabled	Status
1	192.168.84.126	Yes	Waiting for reliable connection
2	www.raritan.com	Yes	Waiting for reliable connection

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Reliability Data

This command shows the reliability data.

```
# show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
# show reliability errorlog <n>
```

Variables:

- <n> is one of the options: 0 (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. <i>Tip: You can also type the command without adding this option "0" to get all data.</i>
A specific integer number	Displays the specified number of last entries in the reliability error log.

Command History

This command syntax shows the command history for current connection session.

```
# show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing history commands.

```
# show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled
IPv6 access control: Disabled
Role based access control for IPv4: Disabled
Role based access control for IPv6: Disabled
Password aging: Disabled
Prevent concurrent user login: No
Strong passwords: Disabled
Enforce HTTPS for web access: Yes
Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled
IPv6 access control: Disabled

Role based access control for IPv4: Disabled
Role based access control for IPv6: Disabled
Password aging: Disabled
Prevent concurrent user login: No
Maximum number of failed logins: 3
User block time: 10 minutes

User idle timeout: 1440 minutes
Strong passwords: Disabled
Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Clearing Information

You can use the clear commands to remove unnecessary data from the BCM2.

After typing a "clear" command, press Enter to execute it.

*Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** (on page 261).*

Clearing Information

You can use the clear commands to remove unnecessary data from the BCM2.

After typing a "clear" command, press Enter to execute it.

*Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** (on page 261).*

Clearing Event Log

This command removes all data from the event log.

```
#          clear eventlog
          -- OR --
#          clear eventlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type *y* to clear the event log or *n* to abort the operation.

If you type *y*, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Configuring the BCM2 Device and Network

To configure the BCM2 device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive so ensure you capitalize them correctly.

Entering Configuration Mode

Configuration commands function in configuration mode only.

► **To enter configuration mode:**

1. Ensure you have entered administrator mode and the # prompt is displayed.

*Note: If you enter configuration mode from user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** (on page 261).*

2. Type `config` and press Enter.
3. The `config:#` prompt appears, indicating that you have entered configuration mode.

```
config:# _
```

4. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes. See *Quitting Configuration Mode* (on page 284).

Quitting Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

► **To quit the configuration mode, use either command:**

```
config:#    apply
           -- OR --
config:#    cancel
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See **Different CLI Modes and Prompts** (on page 261).

Network Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Setting the Networking Mode

If your BCM2 device is implemented with both wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command enables the wired or wireless networking mode.

```
config:# network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the BCM2 does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your BCM2 device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command determines which IP protocol is enabled on the BCM2.

```
config:# network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Selecting IPv4 or IPv6 Addresses

This command determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both IPv4 and IPv6 protocols are enabled on the BCM2.

```
config:# network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6*.

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

```
config:# network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
 - Up to 32 ASCII characters
 - No spaces
 - ASCII codes 0x20 ~ 0x7E

Setting the Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:# network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:# network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
 - 8 to 63 characters
 - No spaces
 - ASCII codes 0x20 ~ 0x7E

Setting EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

▶ **Determine the outer authentication protocol:**

```
config:# network wireless eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol:**

```
config:# network wireless eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:# network wireless eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:# network wireless eapPassword
```

After performing the above command, the BCM2 prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a CA TLS certificate:**

```
config:# network wireless eapCACertificate
```

After performing the above command, the system prompts you to enter the CA certificate's contents. For details, see **EAP CA Certificate Example** (on page 291).

▶ **Enable or disable verification of the TLS certificate chain:**

```
config:# network wireless enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
config:# network wireless allowOffTimeRangeCerts <option2>
```

▶ **Allow wireless network connection with incorrect system time:**

```
config:# network wireless allowConnectionWithIncorrectClock <option3>
```

Variables:

- The value of <outer_auth> is *PEAP* because BCM2 only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because BCM2 only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.
- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the wireless network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The wireless network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the wireless network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The wireless network connection is NOT successfully established when the BCM2 finds that the TLS certificate is not valid due to incorrect system time.

EAP CA Certificate Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

► **To provide a CA certificate:**

1. Make sure you have entered the configuration mode. See **Entering Configuration Mode** (on page 284).

2. Type the following command and press Enter.

```
config:# network wireless eapCACertificate
```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxmzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwXTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlyDTL2ftgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMMFQxCzAJBgNVBAYTAIVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBBZxJvbmF1dGljcyBhbmQGU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVROBAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVROKBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLcGiTkCKp0F5EWIrVDwh54NNeVkcQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICjTCCAf igAwIBAgIEMaYgRzALBqkqhkiG9w0BAQQwRTELMak
GA1UEBhMCMVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgXM
zQ5MDUyMDgwMBCROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCMVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEWxTdGV2ZSBTY2hvY2gwWDALBqkqhkiG9w0BAQEDSQAAR
gJBALrAwYydgxmzNP / ts0Uyf6BpmiJYktU / w4NG67ULa4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlyDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH / BFowWDBWFMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dG1jcyBhbmQGU3BhY2UgQWRta
W5pc3RyYXRpb24xDALBgNVBAMTBENSTDEwFwYDVR0BAQH / BA0w
C4AJODMyOTcwODEwMBCGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw /
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd / 0JtG0glT9usFFBDvYK800ebgz / P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNEvkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

```
config:#
```

Setting the BSSID

This command specifies the BSSID.

```
config:# network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:# network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:# network ipv4 preferredHostName <name>
```

Variables:

- <name> is a host name which:
 - Consists of alphanumeric characters and/or hyphens
 - Cannot begin or end with a hyphen
 - Cannot contain more than 63 characters
 - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2 device.

```
config:# network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your BCM2 device. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command to define the subnet mask.

```
config:# network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See **Overriding the IPv4 DHCP-Assigned DNS Server** (on page 295).

```
config:# network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See **Overriding the IPv4 DHCP-Assigned DNS Server** (on page 295).

```
config:# network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Note: The BCM2 supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the BCM2 only uses the primary IPv4 and IPv6 DNS servers.

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:# network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

▶ **Add a static route:**

```
config:# network ipv4 staticRoutes add <dest-1> <hop>
```

▶ **Delete an existing static route:**

```
config:# network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:# network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:# network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:# network ipv6 preferredHostName <name>
```

Variables:

- <name> is a host name which:
 - Consists of alphanumeric characters and/or hyphens
 - Cannot begin or end with a hyphen
 - Cannot contain more than 63 characters
 - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2 device.

```
config:# network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your BCM2 device. This value uses the IPv6 address format. Note that you must add /xx, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting the IPv6 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See **Overriding the IPv6 DHCP-Assigned DNS Server** (on page 299).

```
config:# network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See **Overriding the IPv6 DHCP-Assigned DNS Server** (on page 299).

```
config:# network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

Note: The BCM2 supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the BCM2 only uses the primary IPv4 and IPv6 DNS servers.

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:# network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

▶ **Add a static route:**

```
config:# network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Delete a static route**

```
config:# network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:# network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the BCM2 belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:# network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:# network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The BCM2 selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the BCM2 device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

► **Change the HTTP port:**

```
config:# network services http port <n>
```

► **Enable or disable the HTTP port:**

```
config:# network services http enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The HTTP port is enabled.
false	The HTTP port is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

► **Change the HTTPS port:**

```
config:# network services https port <n>
```

► **Enable or disable the HTTPS access:**

```
config:# network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the BCM2 via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:# network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:# network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:# network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:# network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:# network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Specifying the SSH Public Key*** (on page 343).

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:# network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:# network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:# network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:# network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:# network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:# network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:# network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:# network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:# network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:# network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling the Service Advertisement

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See **Enabling Service Advertisement** (on page 79) for details.

```
config:# network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Networking Mode

The following command enables the wired networking mode.

```
config:# network mode wired
```

Example 2 - Enabling Both IP Protocols

The following command determines that both IPv4 and IPv6 protocols are enabled.

```
config:# network ip proto both
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:# network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IP configuration mode.

```
config:# network ipv4 ipConfigurationMode static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:# time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.

Mode	Description
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command that is used to set the NTP parameters begins with *time ntp*.

Specifying the Primary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#    time ntp firstServer <first_server>
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.

Specifying the Secondary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#    time ntp secondServer <second_server>
```

Variables:

- The <second_server> is the IP address or host name of the secondary NTP server.

Overriding DHCP-Assigned NTP Servers

This command determines whether the customized NTP server settings override the DHCP-specified NTP servers.

```
config:#    time ntp overrideDHCPProvidedServer <option>
```

Variables:

- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for the BCM2.

```
config:#    time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

Customizing the Date and Time

If intending to manually configure the date and time, use the following CLI commands to specify them.

*Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** (on page 309).*

► **Assign the date:**

```
config:# time set date <yyyy-mm-dd>
```

► **Assign the time:**

```
config:# time set time <hh:mm:ss>
```

Variables:

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type 2015-11-30 for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type 13:50:20 for 1:50:20 pm.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight savings time is applied to the time settings.

```
config:# time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#    time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#    time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your BCM2 and then shows the result. For instructions on specifying NTP servers via CLI, see **Setting NTP Parameters** (on page 310).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See **Setting NTP Parameters** (on page 310).
- Make the customized NTP servers override the DHCP-assigned ones. See **Overriding DHCP-Assigned NTP Servers** (on page 311).

This command is available either in the administrator/user mode or in the configuration mode. See **Different CLI Modes and Prompts** (on page 261).

▶ In the administrator/user mode:

```
#          check ntp
```

▶ In the configuration mode:

```
config#    check ntp
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the BCM2 device from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 firewall control feature:**

```
config:# security ipAccessControl ipv4 enabled <option>
```

▶ **Determine the default IPv4 firewall control policy for inbound traffic:**

```
config:# security ipAccessControl ipv4 defaultPolicyIn <policy>
```

▶ **Determine the default IPv4 firewall control policy for outbound traffic:**

```
config:# security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 firewall control feature:**

```
config:# security ipAccessControl ipv6 enabled <option>
```

▶ **Determine the default IPv6 firewall control policy for inbound traffic:**

```
config:# security ipAccessControl ipv6 defaultPolicyIn <policy>
```

- ▶ **Determine the default IPv6 firewall control policy for outbound traffic:**

```
config:# security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** (on page 356).

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

- ▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:# security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

- ▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:# security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert>  
<rule_number>
```

-- OR --

```
config:# security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>  
<ip_mask> <policy>
```

- *IPv6 commands*

- ▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:# security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

- ▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:# security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>  
<rule_number>
```

-- OR --

```
config:# security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>  
<ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- `<ip_mask>` is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: `192.168.94.222/24`.
- `<policy>` is one of the options: `accept`, `drop` or `reject`.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- `<insert>` is one of the options: `insertAbove` or `insertBelow`.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

- `<rule_number>` is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

► Modify an IPv4 rule's IP address and/or subnet mask:

```
config:# security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask <ip_mask>
```

► Modify an IPv4 rule's policy:

```
config:# security ipAccessControl ipv4 rule modify <direction> <rule_number> policy <policy>
```

► Modify all contents of an existing IPv4 rule:

```
config:# security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask <ip_mask> policy <policy>
```

- IPv6 commands

▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
config:# security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask <ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

```
config:# security ipAccessControl ipv6 rule modify <direction> <rule_number> policy <policy>
```

▶ **Modify all contents of an IPv6 existing rule:**

```
config:# security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.

Option	Description
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
config:# security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:# security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:# security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the BCM2. Do either of the following, or you cannot successfully log in to the BCM2:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

Tip: To select the agreement checkbox using the keyboard, press the Space bar.

- In the CLI, type *y* when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:# security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
 - a. Press Enter.
 - b. Type `--END--` to indicate the end of the content.
 - c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

*Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting Configuration Mode** (on page 284).*

Example

```
Welcome to BCM2 CLI!

Last login: 2015-08-06 04:58:42 EDT [CLI (Telnet) from ]

# show security details

[...]

Restricted Service Agreement: disabled

Restricted Service Agreement Banner Content:

Unauthorized access prohibited; all access and activities
not explicitly authorized by management are unauthorized.
All activities are monitored and logged. There is no privacy
on this system. Unauthorized access and activities or any
criminal activity will be reported to appropriate
authorities.

# config

config:# security restrictedServiceAgreement
enabled          bannerContent

config:# security restrictedServiceAgreement enabled
true            false

config:# security restrictedServiceAgreement enabled
true

config:# security restrictedServiceAgreement
bannerContent

Please input the Restricted Service Agreement banner
content.

Maximum content length is 10000 characters, no special
characters allowed.

Terminate the input with '<Enter>--END--<Enter>'.

This is my
new restricted service agreement.

--END--

Successfully entered Restricted Service Agreement (44
characters)

config:# apply

# show security details

[...]
```

```
Restricted Service Agreement: enforced
Restricted Service Agreement Banner Content:
This is my
new restricted service agreement.
#
```

-> on login (with newly configured banner)

```
Login for BCM2 CLI
Username: admin
Password:
```

```
RESTRICTED SERVICE AGREEMENT
=====
```

```
This is my
new restricted service agreement.
```

```
I understand and accept the Restricted Service Agreement
[y/n] y
```

Welcome to BCM2 CLI!

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before forcing a user to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify various login limitation parameters at a time. See **Multi-Command Syntax** (on page 356).

Single Login Limitation

This command enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:# security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Password Aging

This command enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:# security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Password Aging Interval

This command determines how often the password should be changed.

```
config:# security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the BCM2 web interface or CLI.

```
config:# security loginLimits idleTimeout <value>
```

Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

You can combine multiple commands to modify the user blocking parameters at a time. See **Multi-Command Syntax** (on page 356).

▶ **Determine the maximum number of failed logins before blocking a user:**

```
config:# security userBlocking maximumNumberOfFailedLogins <value1>
```

▶ **Determine how long a user is blocked:**

```
config:# security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value ranging from 1 to 1440 minutes (one day), or *infinite*, which blocks the user all the time until the user is unblocked manually.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See **Multi-Command Syntax** (on page 356).

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:# security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:# security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:# security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:# security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:# security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:# security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.

Option	Description
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:# security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:# security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:# security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:# security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:# security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
config:# security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** (on page 356).

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- *IPv4 commands*

▶ Add a new rule to the bottom of the IPv4 rules list:

```
config:# security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ Add a new IPv4 rule by inserting it above or below a specific rule:

```
config:# security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy> <insert> <rule_number>
```

- *IPv6 commands*

▶ Add a new rule to the bottom of the IPv6 rules list:

```
config:# security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

▶ Add a new IPv6 rule by inserting it above or below a specific rule:

```
config:# security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
<policy> <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- *IPv4 commands*

► **Modify a rule's IPv4 address range:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip>
```

► **Modify an IPv4 rule's role:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

▶ **Modify an IPv4 rule's policy:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number> policy  
<policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>  
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- *IPv6 commands*

▶ **Modify a rule's IPv6 address range:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>  
startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv6 rule's role:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

▶ **Modify an IPv6 rule's policy:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number> policy  
<policy>
```

▶ **Modify all contents of an existing IPv6 rule:**

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

▶ IPv4 commands

```
config:# security roleBasedAccessControl ipv4 rule delete <rule_number>
```

▶ IPv6 commands

```
config:# security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
config:# security ipAccessControl ipv4 enabled true defaultPolicyIn accept
defaultPolicyOut accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:# security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
config:# security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Example 4 - Adding an IPv4 Role-based Access Control Rule

The following command creates a new IPv4 role-based access control rule and specifies its location in the list.

```
config:# security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command creates a new user profile.

```
config:# user create <name> <option> <roles>
```

After performing the user creation command, the BCM2 prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

*Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** (on page 356).*

Changing a User's Password

This command allows you to change an existing user's password if you have the Administrator Privileges.

```
config:# user modify <name> password
```

After performing the above command, BCM2 prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

Variables:

- <name> is the name of the user whose settings you want to change.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

Various commands can be combined to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** (on page 356).

► Change a user's full name:

```
config:# user modify <name> fullName "<full_name>"
```

► Change a user's telephone number:

```
config:# user modify <name> telephoneNumber "<phone_number>"
```

► Change a user's email address:

```
config:# user modify <name> emailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Enabling or Disabling a User Profile

This command enables or disables a user profile. A user can log in to the BCM2 device only after that user's user profile is enabled.

```
config:# user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Forcing a Password Change

This command determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:# user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Modifying SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See **Multi-Command Syntax** (on page 356).

- ▶ **Enable or disable the SNMP v3 access to BCM2 for the specified user:**

```
config:# user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

- ▶ **Determine the security level:**

```
config:# user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

- ▶ **Determine whether the authentication passphrase is identical to the password:**

```
config:# user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

► **Determine the authentication passphrase:**

```
config:# user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising 8 to 32 ASCII printable characters.

► **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
config:# user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

► **Determine the privacy passphrase:**

```
config:# user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising 8 to 32 ASCII printable characters.

► **Determine the authentication protocol:**

```
config:# user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

► **Determine the privacy protocol:**

```
config:# user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:# user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile. See **All Privileges** (on page 347).

Changing Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time. To combine all commands, see **Multi-Command Syntax** (on page 356).

Note: The measurement unit change only applies to the web interface and command line interface.

*Tip: To set the default measurement units applied to the BCM2 user interfaces for all users via CLI, see **Setting Default Measurement Units** (on page 344).*

► Set the preferred temperature unit:

```
config:# user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

► **Set the preferred length unit:**

```
config:# user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

► **Set the preferred pressure unit:**

```
config:# user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

► **To specify the SSH public key for a specific user:**

1. Type the SSH public key command as shown below and press Enter.

```
config:# user modify <name> sshPublicKey
```

2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:
 - a. Open your SSH public key with a text editor.
 - b. Copy all contents in the text editor.

- c. Paste the contents into the terminal.
- d. Press Enter.

Tip: To remove an existing SSH public key, simply press Enter without typing or pasting anything when the system prompts you to input the contents.

Deleting a User Profile

This command deletes an existing user profile.

```
config:# user delete <name>
```

Changing Your Own Password

Every user can change their own password via this command if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:# password
```

After performing this command, the BCM2 prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the BCM2 user interfaces across all users except for those whose preferred measurement units are set differently by themselves or the administrator. Diverse measurement unit commands can be combined so that you can set all default measurement units at a time. To combine all commands, see **Multi-Command Syntax** (on page 356).

Note: The measurement unit change only applies to the web interface and command line interface.

*Tip: To change the preferred measurement units displayed in the BCM2 user interfaces for a specific user via CLI, see **Changing Measurement Units** (on page 342).*

- ▶ **Set the default temperature unit:**

```
config:# user defaultpreferences preferredTemperatureUnit <option1>
```

Variables:

- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

▶ **Set the default length unit:**

```
config:# user defaultpreferences preferredLengthUnit <option2>
```

Variables:

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

▶ **Set the default pressure unit:**

```
config:# user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:# user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "May."

```
config:# user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:# user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet  
preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:# role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:# role create <name> <privilege1>:<argument1>,<argument2>...;
<privilege2>:<argument1>,<argument2>...;
<privilege3>:<argument1>,<argument2>...;
...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See **All Privileges** (on page 347).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

All Privileges

This table lists all privileges.

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDateTimeSettings	Change Date/Time Settings

Privilege	Description
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change PMC, PMB & PMM Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator**	Switch Actuator
switchTransferSwitch	Switch Transfer Switch
viewEventSetup	View Event Settings
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

**The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,
`switchActuator:all`

- An actuator's ID number. For example:

```
switchActuator:1
switchActuator:2
switchActuator:3
```
- A list of comma-separated ID numbers of different actuators. For example:

```
switchActuator:1,3,6
```

Note: The ID number of each actuator is shown in the BCM2 web interface. It is an integer between 1 and 32.

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

► Modify a role's description:

```
config:#    role modify <name> description "<description>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

► Add more privileges to a specific role:

```
config:#    role modify <name> addPrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#  role modify <name> addPrivileges
          <privilege1>:<argument1>,<argument2>...;
          <privilege2>:<argument1>,<argument2>...;
          <privilege3>:<argument1>,<argument2>...;
          ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See **All Privileges** (on page 347).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

► **Remove specific privileges from a role:**

```
config:#  role modify <name> removePrivileges
          <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#  role modify <name> removePrivileges
          <privilege1>:<argument1>,<argument2>...;
          <privilege2>:<argument1>,<argument2>...;
          <privilege3>:<argument1>,<argument2>...;
          ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See **All Privileges** (on page 347).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:# role delete <name>
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:# serverReachability add <IP_host> <enable> <succ_ping>
<fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

- <succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the BCM2 resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the BCM2 disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Deleting a Monitored Device

This command removes a monitored IT device from the server reachability list.

```
config:# serverReachability delete <n>
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

#	IP address	Enabled	Status
1	192.168.84.126	Yes	Waiting for reliable connection
2	www.raritan.com	Yes	Waiting for reliable connection

Modifying a Monitored Device's Settings

The command to modify a monitored IT device's settings begins with `serverReachability modify`.

You can modify various settings for a monitored device at a time. See **Multi-Command Syntax** (on page 356).

- ▶ **Modify a device's IP address or host name:**

```
config:# serverReachability modify <n> ipAddress <IP_host>
```

- ▶ **Enable or disable the ping monitoring feature for the device:**

```
config:# serverReachability modify <n> pingMonitoringEnabled <option>
```

- ▶ **Modify the number of successful pings for declaring "Reachable":**

```
config:# serverReachability modify <n> numberOfSuccessfulPingsToEnable  
<succ_number>
```

- ▶ **Modify the number of unsuccessful pings for declaring "Unreachable":**

```
config:# serverReachability modify <n> numberOfUnsuccessfulPingsForFailure  
<fail_number>
```

- ▶ **Modify the wait time after a successful ping:**

```
config:# serverReachability modify <n> waitTimeAfterSuccessfulPing  
<succ_wait>
```

- ▶ **Modify the wait time after a unsuccessful ping:**

```
config:# serverReachability modify <n> waitTimeAfterUnsuccessfulPing  
<fail_wait>
```

- ▶ **Modify the wait time before resuming pinging after declaring "Unreachable":**

```
config:# serverReachability modify <n> waitTimeBeforeResumingPinging  
<resume>
```

- ▶ **Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:**

```
config:# serverReachability modify <n> numberOfFailuresToDisable
        <disable_count>
```

Variables:

- <n> is a number representing the sequence of the IT device in the server monitoring list.
- <IP_host> is the IP address or host name of the IT device whose settings you want to modify.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

- <succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the BCM2 resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the BCM2 disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Example - Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
config:# serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
        numberOfUnsuccessfulPingsForFailure 8
        waitTimeAfterSuccessfulPing 30
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Serial Port Baud Rate

The following command syntax sets the CONSOLE baud rate (bps) of the serial port labeled CONSOLE / MODEM on the BCM2 device. Change the CONSOLE baud rate before connecting it to any Raritan device, such as Raritan's P2CIM-SER, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the BCM2 or power cycle the connected Raritan device for proper communications.

```
config:#    serial baudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the CONSOLE baud rate options: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Note: The serial port bit-rate change is needed when the BCM2 works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

Setting the History Buffer Length

This command syntax sets the history buffer length, which determines the amount of history commands that can be retained in the buffer. The default length is 25.

```
config:#    history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2>  
<value 2> <setting 3> <value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:# network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0  
gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of SSID and PSK Parameters

This multi-command syntax configures both SSID and PSK parameters simultaneously for the wireless feature.

```
config:# network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands. See **Multi-Command Syntax** (on page 356).

- ▶ **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:# defaultThresholds <sensor type> upperCritical <value>
```

- ▶ **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:# defaultThresholds <sensor type> upperWarning <value>
```

- ▶ **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:# defaultThresholds <sensor type> lowerCritical <value>
```

- ▶ **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:# defaultThresholds <sensor type> lowerWarning <value>
```

- ▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:# defaultThresholds <sensor type> hysteresis <hy_value>
```

- ▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
config:# defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m ³ (that is, g/m ³)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

- <hy_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20°C and Upper Critical threshold to 24°C for all temperature sensors.

```
config:# defaultThresholds temperature upperWarning 20
        upperCritical 24
```

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

*Note: To configure an actuator, see **Actuator Configuration Commands** (on page 366).*

Changing the Sensor Name

This command names an environmental sensor.

```
config:# externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

*Note: To name an actuator, see **Actuator Configuration Commands** (on page 366).*

Specifying the CC Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#    externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command specifies the X coordinate of an environmental sensor.

```
config:#    externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#  externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#  externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format** (on page 210).

Changing the Sensor Description

This command provides a description for a specific environmental sensor.

```
config:#    externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#    externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a DX-PIR presence detector.

```
config:#    externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#    externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#    externalsensor 1 useDefaultThresholds true
```

Environmental Sensor Threshold Configuration Commands

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

You can configure various environmental sensor threshold settings at a time by combining multiple commands. See **Multi-Command Syntax** (on page 356).

- ▶ **Set the Upper Critical threshold for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an environmental sensor:**

```
config:# sensor externalsensor <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <sensor type> is one of these sensor types: *temperature*, *absoluteHumidity*, *relativeHumidity*, *airPressure*, *airFlow* or *vibration*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See **"To De-assert" and Deassertion Hysteresis** (on page 119).

<as_value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. It ranges between 1 and 100. See **"To Assert" and Assertion Timeout** (on page 117).

Example 1 - Upper Critical Threshold for a Temperature Sensor

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:# sensor externalsensor 2 temperature upperCritical 40
```

Actuator Configuration Commands

An actuator configuration command begins with *actuator*. You can configure the name and location parameters of an individual actuator.

You can configure various parameters for one actuator at a time. See **Multi-Command Syntax** (on page 356).

▶ **Change the name:**

```
config:# actuator <n> name "<name>"
```

▶ **Set the X coordinate:**

```
config:# actuator <n> xlabel "<coordinate>"
```

▶ **Set the Y coordinate:**

```
config:# actuator <n> ylabel "<coordinate>"
```

▶ **Set the Z coordinate:**

```
config:# actuator <n> zlabel "<z_label>"
```

▶ **Modify the actuator's description:**

```
config:# actuator <n> description "<description>"
```

Variables:

- <n> is the ID number assigned to the actuator. The ID number can be found using the BCM2 web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
- There are two types of values for the <z_label> variable, depending on the Z coordinate format you set:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

*Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format** (on page 210).*

- <description> is a sentence or paragraph comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example - Actuator Naming

The following command assigns the name "Door lock" to the actuator whose ID number is 9.

```
config:# actuator 9 name "Door lock"
```

USB-Cascading Configuration Commands

A USB-cascading configuration command begins with *cascading*. You can set the cascading mode on the master device.

Note: You CANNOT change the cascading mode on slave devices.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:# cascading mode <mode>
```

Variables:

- <mode> is one of the following cascading modes:

Mode	Description
bridging	The network bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The port forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset sensor (if any) or the settings of LEDs on the asset sensor.

Asset Sensor Management

An asset sensor management configuration command begins with `assetStrip`.

Naming an Asset Sensor

This command syntax names or changes the name of an asset sensor connected to the BCM2 device.

```
config:#  assetStrip <n> name "<name>"
```

Variables:

- `<n>` is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- `<name>` is a string comprising up to 32 ASCII printable characters. The `<name>` variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset sensor connected to the BCM2 device.

```
config:#  assetStrip <n> numberOfRackUnits <number>
```

Note: For the Raritan asset sensor, a rack unit refers to a tag port.

Variables:

- `<n>` is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- `<number>` is the total number of rack units available on the connected asset sensor. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset sensors connected to the BCM2 device. The numbering mode changes the rack unit numbers.

```
config:#  assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset sensors connected to the BCM2 device.

```
config:#  assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset sensor. This value is an integer number.

Specifying the Asset Sensor Orientation

This command syntax specifies the orientation of the asset sensors connected to the BCM2 device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the BCM2 unable to detect the asset sensors' orientation.

```
config:#    assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to indicate the presence of a connected asset tag.

```
config:#    assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset sensor(s) to indicate the absence of a connected asset tag.

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

For the Raritan asset sensor, a rack unit refers to a tag port. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset sensor.

```
config:#    rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset sensor follows the global LED color settings.

```
config:# rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See Setting LED Colors for Connected Tags (on page 370) and Setting LED Colors for Disconnected Tags (on page 371). This is the default.
manual	This option enables selection of a different LED color and LED mode for the specified rack unit. When this option is selected, see Setting an LED Color for a Rack Unit (on page 373) and Setting an LED Mode for a Rack Unit (on page 373) to set different LED settings.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

*Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** (on page 370) and **Setting LED Colors for Disconnected Tags** (on page 371).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.

Mode	Description
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Sensor LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#    assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#    rackUnit 1 25 name "Linux server"
```

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a DX sensor, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See ***Different CLI Modes and Prompts*** (on page 261).

Switching On an Actuator

This command syntax turns on one actuator.

```
# control actuator <n> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
# control actuator <n> on /y
```

Variables:

- <n> is an actuator's ID number.
The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type *y* to confirm the operation, OR
- Type *n* to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
# control actuator <n> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
# control actuator <n> off /y
```

Variables:

- <n> is an actuator's ID number.
The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without `/y`, a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
# control actuator 8 on
```

Unlocking a User

If any user is blocked from accessing the BCM2, you can unblock them at the local console.

► **To unblock a user:**

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 256).
2. When the Username prompt appears, type `unlock` and press Enter.

Username: `unlock`

3. When the "Username to unblock" prompt appears, type the name of the blocked user and press Enter.

Username to unblock:

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the BCM2

You can reset the BCM2 device to factory defaults or simply restart it using the CLI commands.

Restarting the Device

This command restarts the BCM2 device. It is not a factory default reset.

► **To restart the BCM2 device:**

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the BCM2 device.

```
# reset unit
-- OR --
# reset unit /y
```
3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.
5. Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

Resetting to Factory Defaults

The following commands restore all settings of the BCM2 device to factory defaults.

► **To reset BCM2 settings after login, use either command:**

```
# reset factorydefaults
-- OR --
# reset factorydefaults /y
```

► **To reset BCM2 settings before login:**

```
Username: factorydefaults
```

See **Using the CLI Command** (on page 383) for details.

Network Troubleshooting

The BCM2 provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

► **To enter the diagnostic mode:**

1. Enter either of the following modes:
 - Administrator mode: The # prompt is displayed.
 - User mode: The > prompt is displayed.
2. Type `diag` and press Enter. The `diag#` or `diag>` prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Quitting Diagnostic Mode

► **To quit the diagnostic mode, use this command:**

```
diag>      exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See ***Different CLI Modes and Prompts*** (on page 261).

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>      nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag> netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Testing the Network Connectivity

This ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag> ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.

Options	Description
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag> ping <host> count <number1> size <number2> timeout <number3>
```

Tracing the Route

This command syntax traces the network route between your BCM2 device and a network host.

```
diag> traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag> ping 192.168.84.222 count 5
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

► **To have a command completed automatically:**

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.
2. Press Tab or Ctrl+i until the complete command appears.

Example 1:

Type the first word and the first letter of the second word of the "reset factorydefaults" command, that is, `reset f`. Then press Tab or Ctrl+i to complete the second word.

Example 2:

Type the first word and initial letters of the second word of the "security enforceHttpsForWebAccess" command, that is, `security enf`. Then press Tab or Ctrl+i to complete the second word.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

► **To log out of the CLI:**

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Appendix A Resetting to Factory Defaults

You can use either the reset button or the command line interface (CLI) to reset the BCM2.

Important: Exercise caution before resetting the BCM2 to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

In This Chapter

Using the Reset Button.....	382
Using the CLI Command	383

Using the Reset Button

An RS-232 serial connection to a computer is required for using the reset button.

► **To reset to factory defaults using the reset button:**

1. Connect a computer to the BCM2 device via RS-232. See **Making an RS-232 or USB Connection** (on page 257).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the BCM2. For information on the serial port configuration, see step 2 of **With HyperTerminal** (on page 256).
3. Press (and release) the Reset button of the BCM2 device while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the BCM2 to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the BCM2 to factory defaults. For information on CLI, see ***Using the Command Line Interface*** (on page 255).

► **To reset to factory defaults after logging in to the CLI:**

1. Connect to the BCM2 device. See ***Logging in to CLI*** (on page 256) or ***Making an RS-232 or USB Connection*** (on page 257).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the BCM2. For information on the serial port configuration, see step 2 of ***With HyperTerminal*** (on page 256).
3. Log in to the CLI by typing the user name "admin" and its password.
4. After the # system prompt appears, type either of the following commands and press Enter.

```
# reset factorydefaults
```

-- OR --

```
# reset factorydefaults /y
```
5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.
6. Wait until the Username prompt appears, indicating the reset is complete.

► **To reset to factory defaults without logging in to the CLI:**

The BCM2 provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the BCM2 and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

```
Username: factorydefaults
```
3. Type y on a confirmation message to perform the reset.

Appendix B LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

- a. Determine user accounts and roles (groups) intended for the BCM2
- b. Create user groups for the BCM2 on the AD server
- c. Configure LDAP authentication on the BCM2 device
- d. Configure roles on the BCM2 device

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

In This Chapter

Step A. Determine User Accounts and Groups.....	384
Step B. Configure User Groups on the AD Server.....	385
Step C. Configure LDAP Authentication on the BCM2 Device	386
Step D. Configure Roles on the BCM2.....	388

Step A. Determine User Accounts and Groups

Determine the user accounts and roles (groups) that are authenticated for accessing the BCM2. In this example, we will create two user roles with different permissions. Each role (group) will consist of two user accounts available on the AD server.

User groups	User accounts (members)
BCM_User	usera
	bcmuser2
BCM_Admin	userb
	bcmuser

Group permissions:

- The BCM_User group will only have read-only permissions.
- The BCM_Admin group will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the BCM2 on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the BCM2 are named *BCM_Admin* and *BCM_User*.
- User accounts *bcmuser*, *bcmuser2*, *usera* and *userb* already exist on the AD server.

► To configure the user groups on the AD server:

1. On the AD server, create new groups -- *BCM_Admin* and *BCM_User*.

Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *bcmuser2* and *usera* accounts to the *BCM_User* group.
3. Add the *bcmuser* and *userb* accounts to the *BCM_Admin* group.
4. Verify whether each group comprises correct users.



Step C. Configure LDAP Authentication on the BCM2 Device

You must enable and set up LDAP authentication properly on the BCM2 device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Modifying Network Settings** (on page 63) and **Role of a DNS Server** (on page 69).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

► **To configure LDAP authentication:**

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate the LDAP/LDAPS authentication.
3. Click New to add an LDAP/LDAPS AA server. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the BCM2 with the information about the AD server.
 - IP Address / Hostname - Type the domain name *techadssl.com* or IP address *192.168.56.3*.

Important: Without the TLS encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the TLS encryption is enabled.

- Use settings from LDAP server - Leave the checkbox deselected.
- Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
- Security - Select "None" since the TLS encryption is not applied in this example.
- Port (None/StartTLS) - Ensure the field is set to *389*.
- Port (TLS) and CA Certificate - Skip the two fields since the TLS encryption is not enabled.
- Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
- Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.

Create new LDAP Server Configuration

IP Address / Hostname: 192.168.56.3

Use settings from LDAP Server

Select LDAP Server

Type of LDAP Server: Microsoft Active Directory

Security: None

Port (None/StartTLS): 389

Port (TLS): 636

Enable verification of LDAP Server Certificate

CA Certificate: not set

Allow expired and not yet valid certificates

Anonymous Bind

Use Bind Credentials

Bind DN:

Bind Password:

Confirm Bind Password:

Base DN for Search: dc=techadssl,dc=com

Login Name Attribute: sAMAccountName

User Entry Object Class: user

User Search Subfilter:

Active Directory Domain: techadssl.com

5. Click OK. The LDAP server is saved.

6. Click OK. The LDAP authentication is activated.

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the BCM2

A role on the BCM2 determines the system permissions. You must create the roles whose names are identical to the user groups created for the BCM2 on the AD server or authorization will fail. Therefore, we will create the roles named *BCM_User* and *BCM_Admin* on the BCM2.

In this illustration, we assume:

- Users assigned to the *BCM_User* role can only access the BCM2 and view settings.
- Users assigned to the *BCM_Admin* role can both access and configure the BCM2 because they have the Administrator permissions.

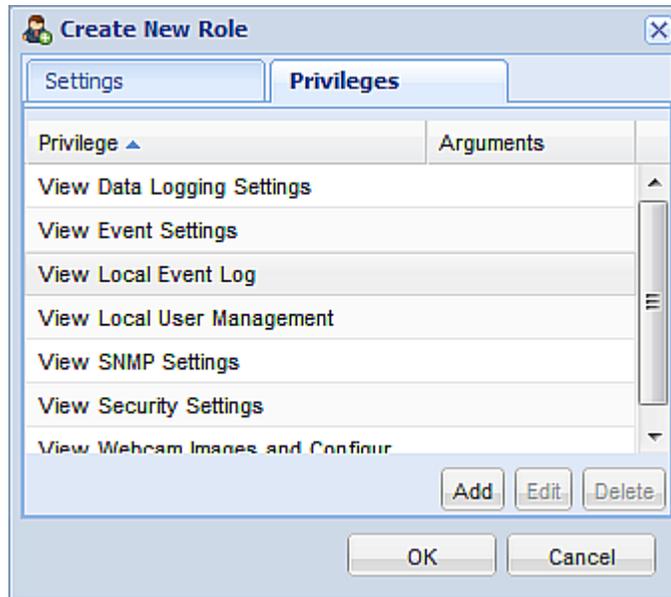
► **To create the *BCM_User* role with appropriate permissions assigned:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

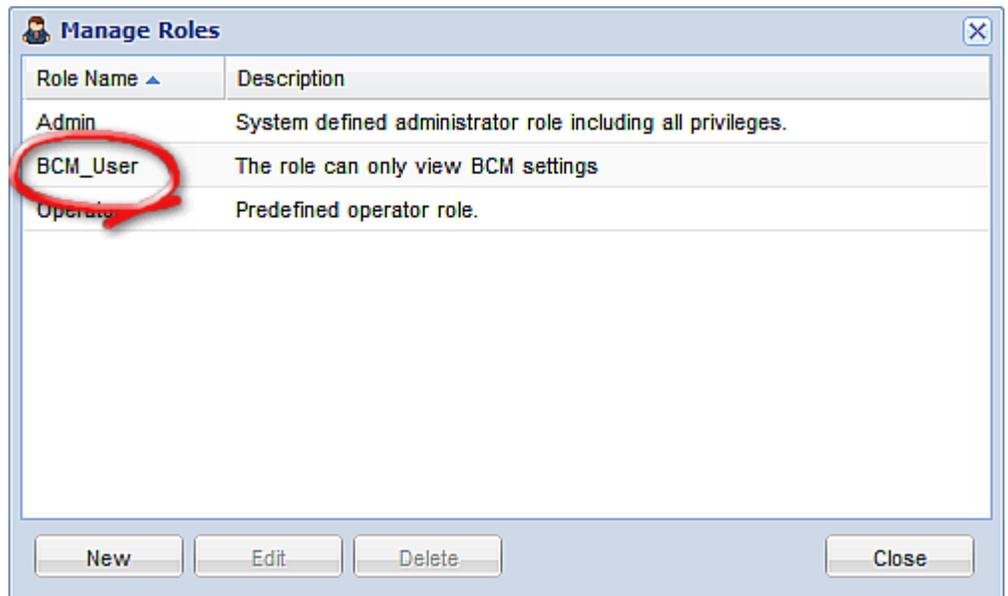
Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `BCM_User` in the Role Name field.
4. Type a description for the *BCM_User* role in the Description field. For example, "The role can only view BCM settings".
5. Click the Privileges tab to select all View permissions. A View permission lets users view the specified settings without the capability to configure or change them.
 - a. Click Add. The "Add Privileges to new Role" dialog appears.
 - b. Select a permission beginning with the word "View" from the Privileges list, such as View Event Settings.
 - c. Click Add.

- d. Repeat Steps a to c to add all permissions beginning with "View."



6. Click OK. The BCM_User role is created.

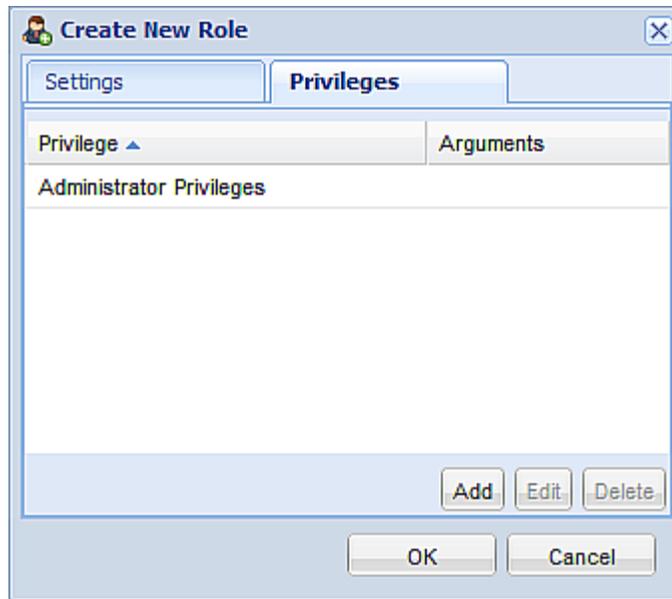


7. Keep the Manage Roles dialog opened to continue creating the BCM_Admin role.

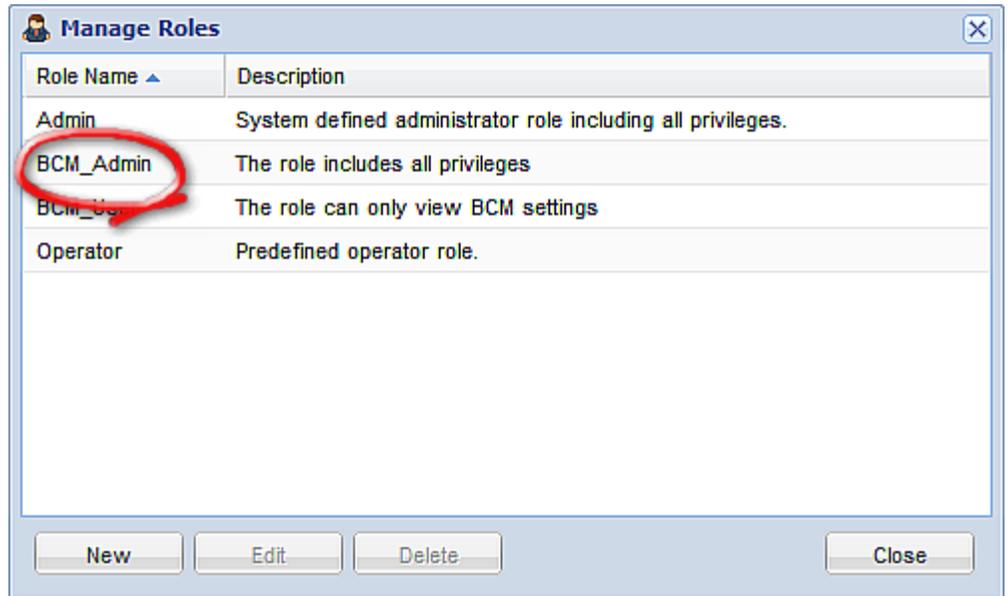
► **To create the BCM_Admin role with full permissions assigned:**

1. Click New. The Create New Role dialog appears.

2. Type `BCM_Admin` in the Role Name field.
3. Type a description for the `BCM_Admin` role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all BCM2 settings.
 - a. Click Add. The "Add Privileges to new Role" dialog appears.
 - b. Select the permission named Administrator Privileges from the Privileges list.
 - c. Click Add.



5. Click OK. The BCM_Admin role is created.



6. Click Close to quit the dialog.

Appendix C RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a non-Windows RADIUS server, such as FreeRADIUS.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the BCM2 device. See **Adding RADIUS Server Settings** (on page 149).
2. Configure roles on the BCM2 device. See **Creating a Role** (on page 101).
3. Configure your RADIUS server. See **Microsoft Network Policy Server** (on page 392) or **Non-Windows RADIUS Server** (on page 416).

In This Chapter

Microsoft Network Policy Server	392
Non-Windows RADIUS Server	416

Microsoft Network Policy Server

In this Microsoft NPS illustration, we assume that the NPS is running on the Windows 2008 system.

Three major steps are required for configuring Windows 2008 NPS:

- a. Add your BCM2 device to NPS as a RADIUS client
- b. Configure connection request policies on NPS
- c. Configure a vendor-specific attribute on NPS

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See **AD-Related Configuration** (on page 413).

Step A: Add Your BCM2 as a RADIUS Client

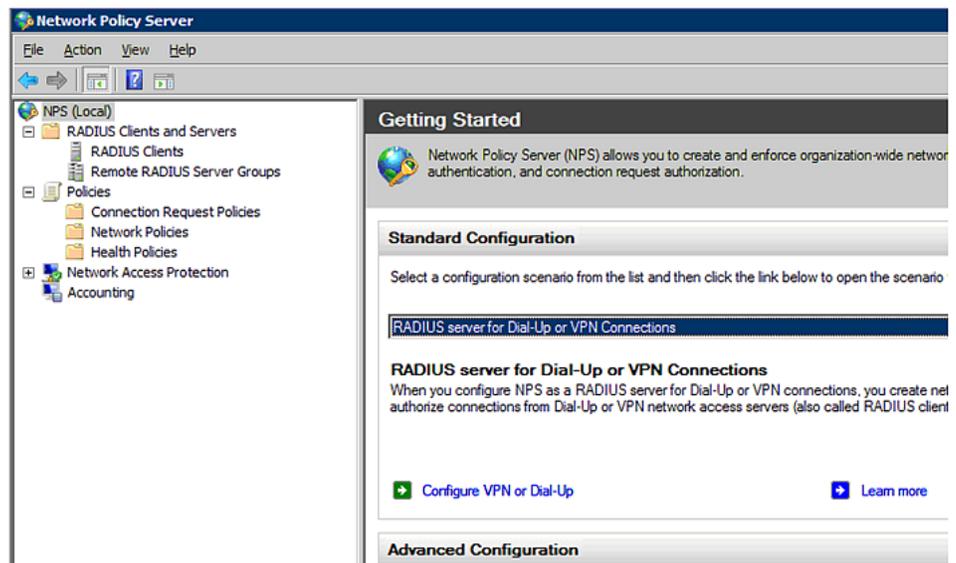
The RADIUS implementation on a BCM2 follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

In this illustration, we assume:

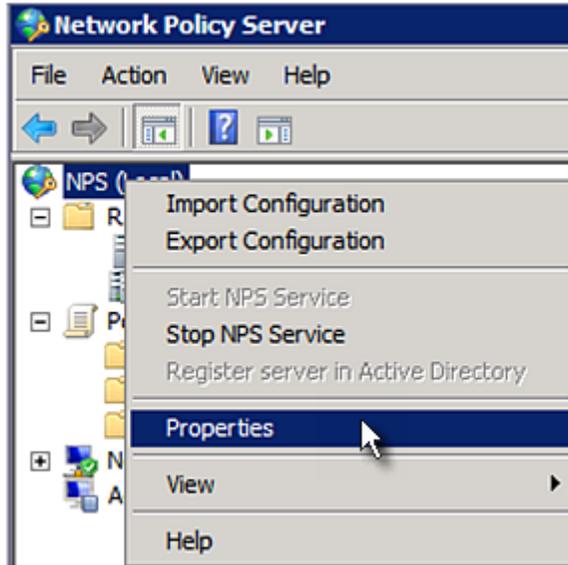
- IP address of your BCM2: 192.168.56.29
- RADIUS authentication port specified for BCM2: 1812
- RADIUS accounting port specified for BCM2: 1813

► To add your BCM2 to the RADIUS NPS:

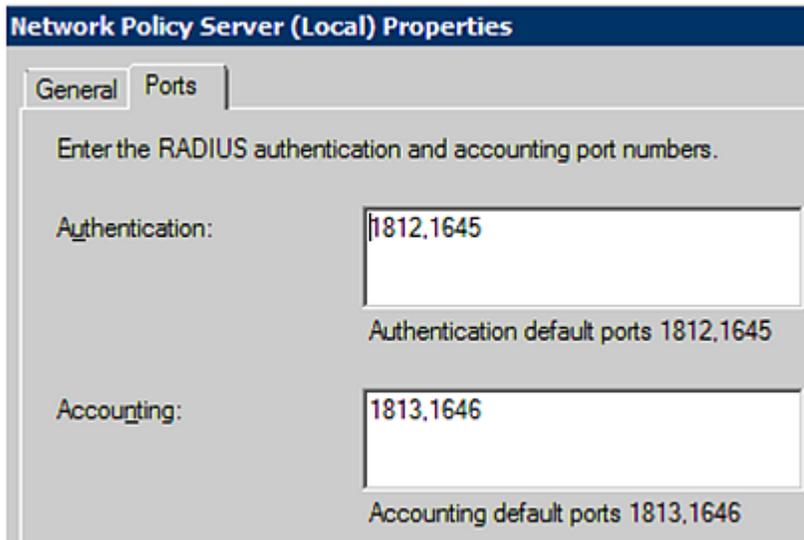
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



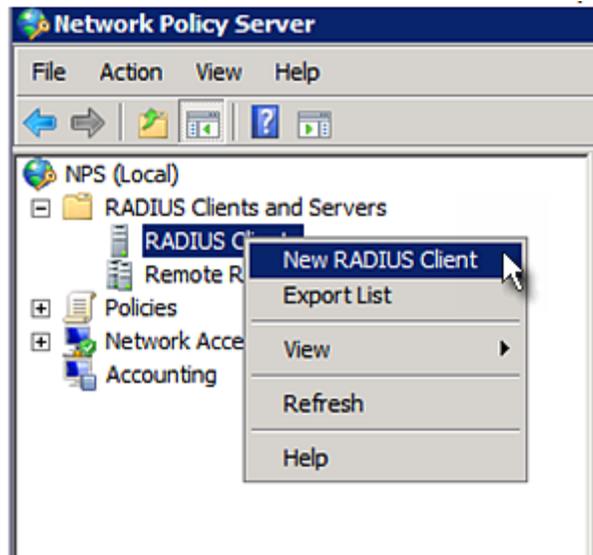
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your BCM2. In this example, they are 1812 and 1813. Then close this dialog.



3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



4. Do the following to add your BCM2 to NPS:
 - a. Verify the "Enable this RADIUS client" checkbox is selected.
 - b. Type a name for identifying your BCM2 in the "Friendly name" field.
 - c. Type *192.168.56.29* in the "Address (IP or DNS)" field.
 - d. Select *RADIUS Standard* in the "Vendor name" field.
 - e. Select the *Manual* radio button.

- f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your BCM2.

New RADIUS Client

Enable this RADIUS client

Name and Address

Friendly name:
RaritanDominion

Address (IP or DNS):
192.168.56.29 Verify...

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:
●●●●●●

Confirm shared secret:
●●●●●●

Additional Options

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

OK Cancel

- 5. Click OK.

Step B: Configure Connection Request Policies

You need to configure the following for connection request policies:

- a. IP address or host name of the BCM2

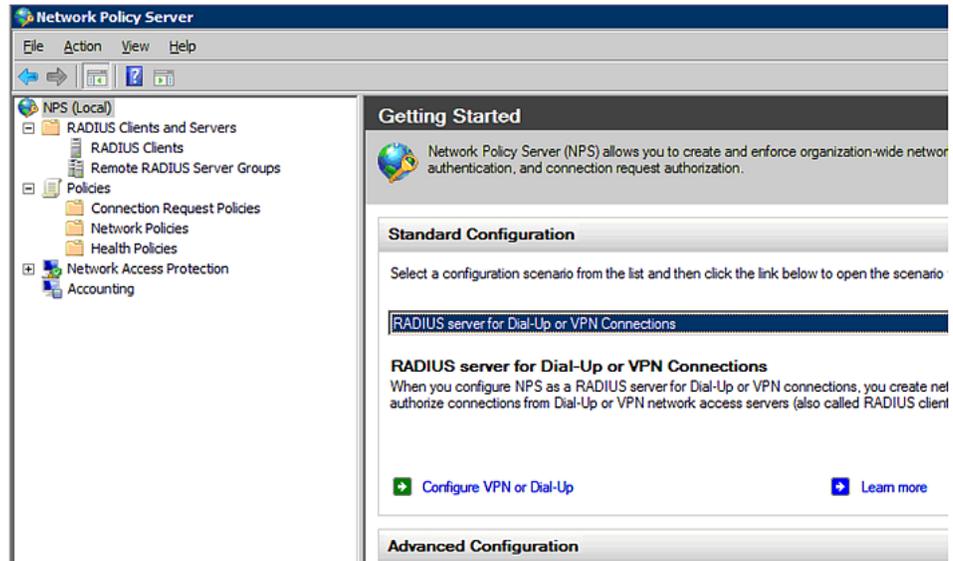
- b. Connection request forwarding method
- c. Authentication method(s)
- d. Standard RADIUS attributes

In the following illustration, we assume:

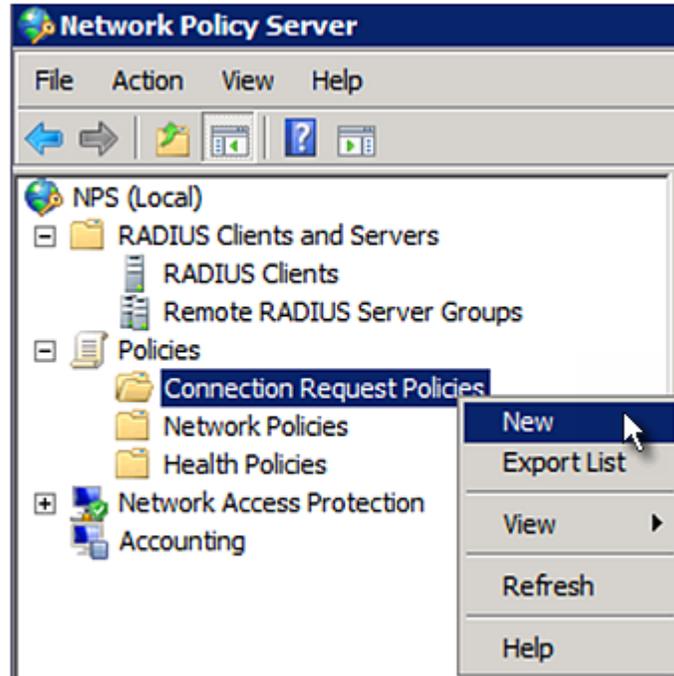
- *Local* NPS server is used
- IP address of your BCM2: *192.168.56.29*
- RADIUS protocol selected on your BCM2: *CHAP*
- Existing role of your BCM2: *Admin*

► **To configure connection request policies:**

1. Open the NPS console, and expand the Policies folder.



2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.



3. Type a descriptive name for identifying this policy in the "Policy name" field.

- You can leave the "Type of network access server" field to the default -- Unspecified.

New Connection Request Policy

 **Specify Connection Request Policy Name**

You can specify a name for your connection request policy and it will be applied.

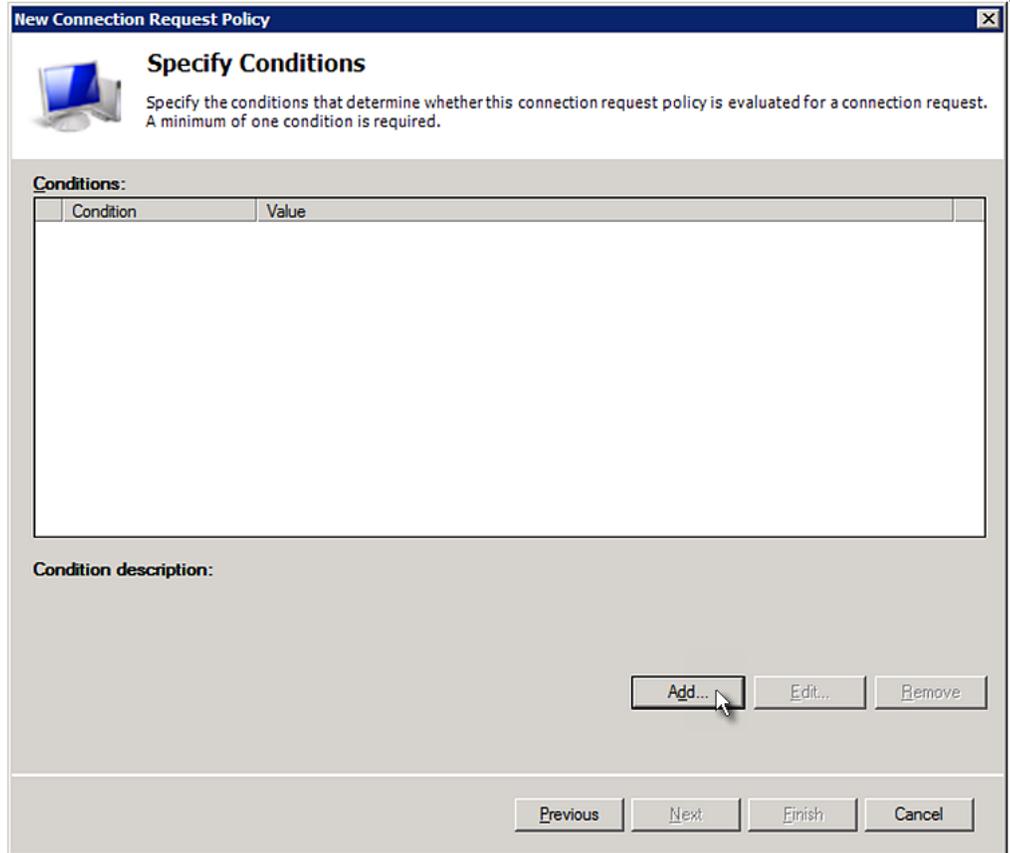
Policy name:
RaritanDominionPolicy

Network connection method
Select the type of network access server that sends the connection request to NPS. type or Vendor specific.

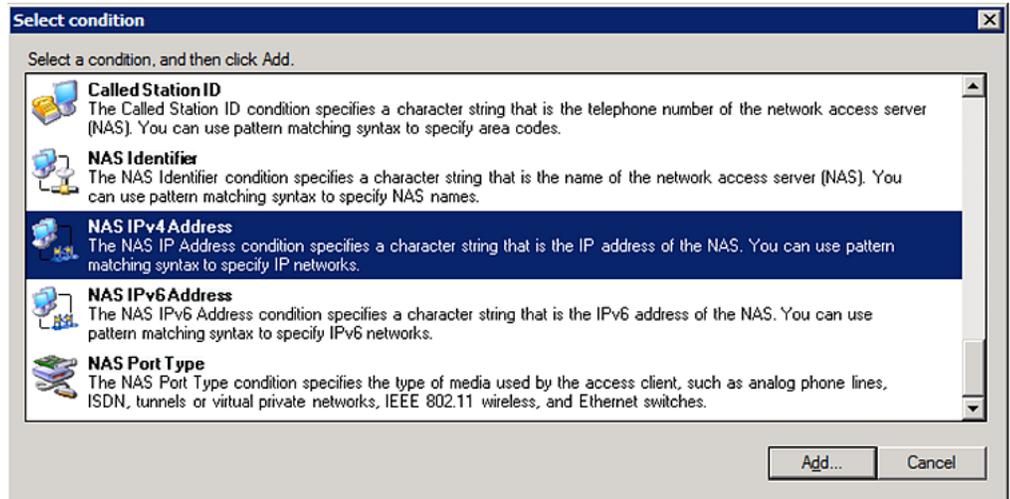
Type of network access server:
Unspecified

Vendor specific:
10

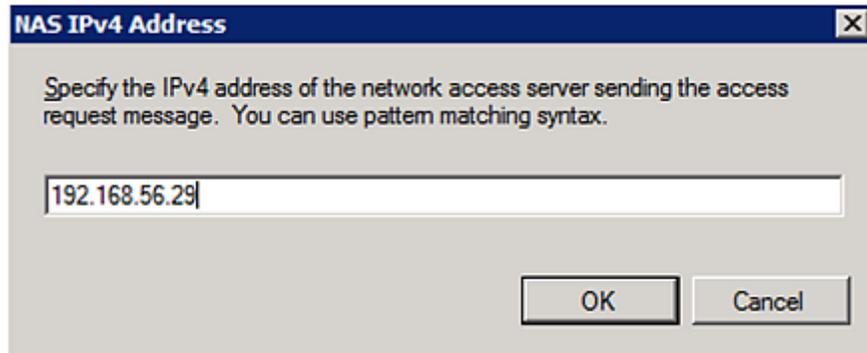
- Click Next to show the "Specify Conditions" screen. Click Add.



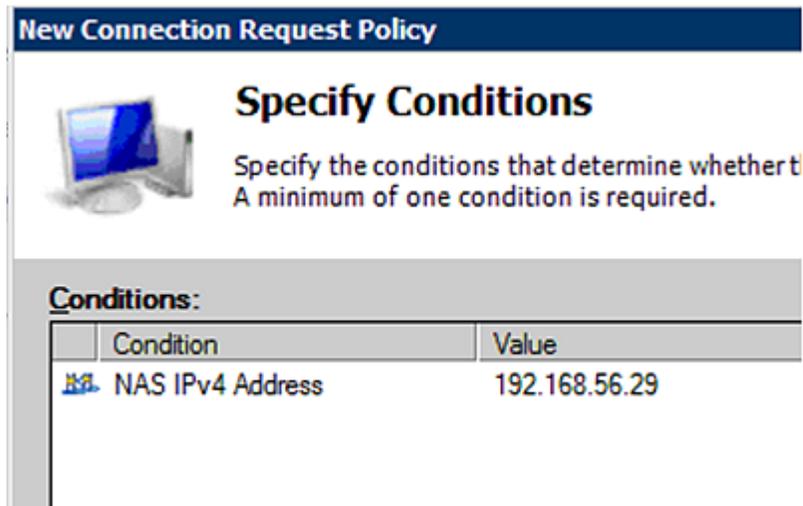
- The "Select condition" dialog appears. Click Add.



- The NAS IPv4 Address dialog appears. Type the BCM2 IP address -- 192.168.56.29, and click OK.

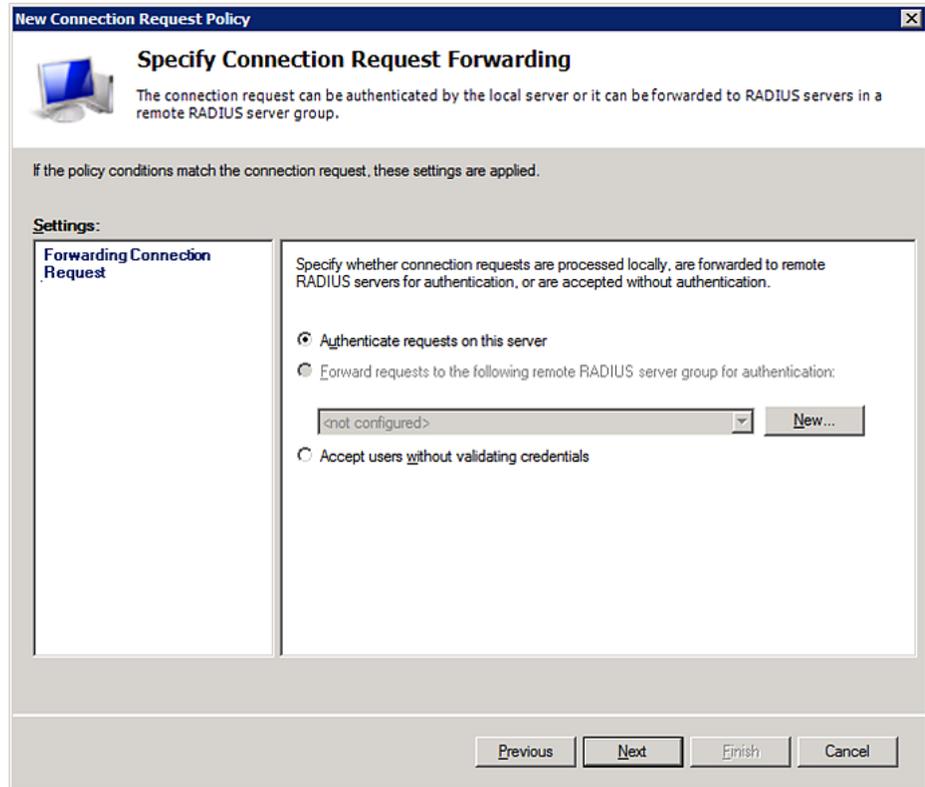


- Click Next in the New Connection Request Policy dialog.



- Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.



9. When the system prompts you to select the authentication method, select the following two options:
 - Override network policy authentication settings
 - CHAP -- the BCM2 uses "CHAP" in this example

Note: If your BCM2 uses PAP, then select "PAP."

New Connection Request Policy



Specify Authentication Methods

Configure one or more authentication methods required authentication, you must configure an EAP type. If you d Protected EAP.

Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which

EAP Types:

Less secure authentication methods:

Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

User can change password after it has expired

Microsoft Encrypted Authentication (MS-CHAP)

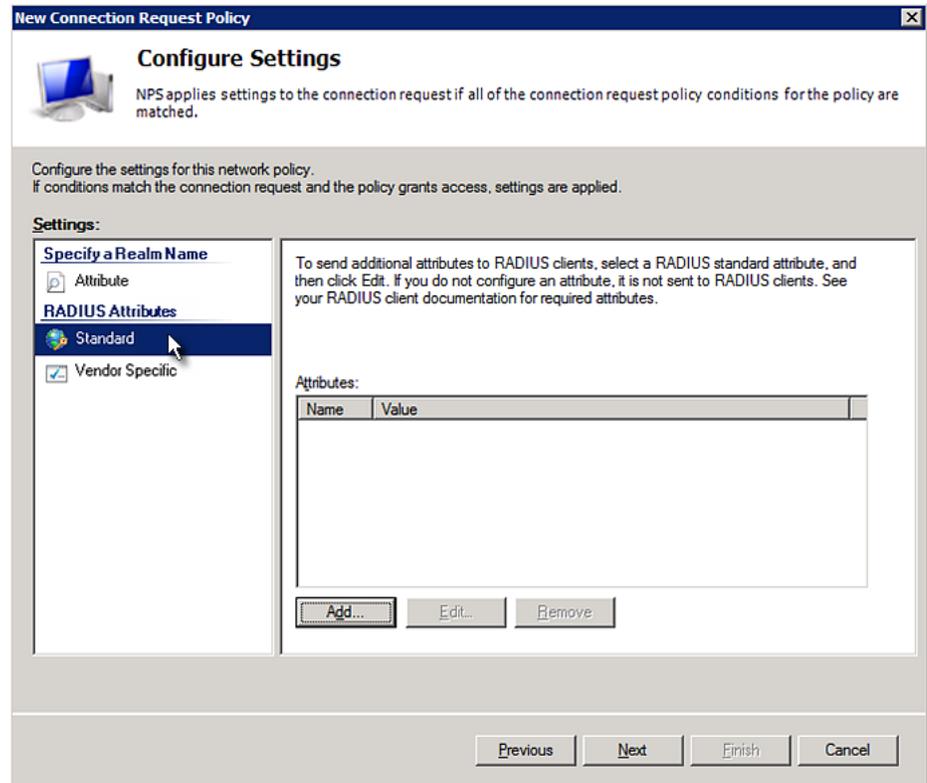
User can change password after it has expired

Encrypted authentication (CHAP)

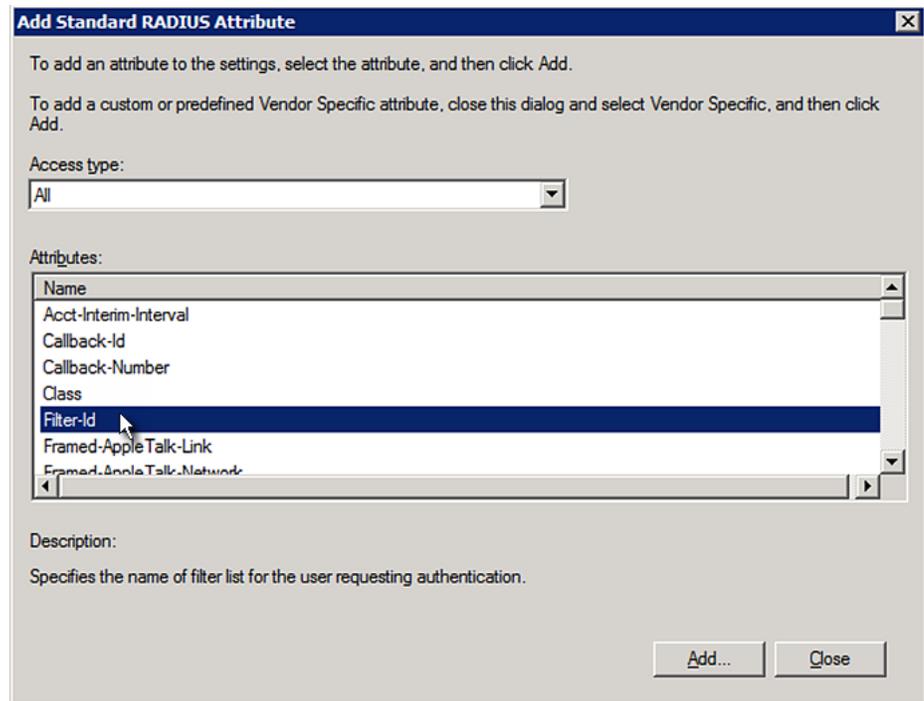
Unencrypted authentication (PAP, SPAP)

Allow clients to connect without negotiating an authentication method.

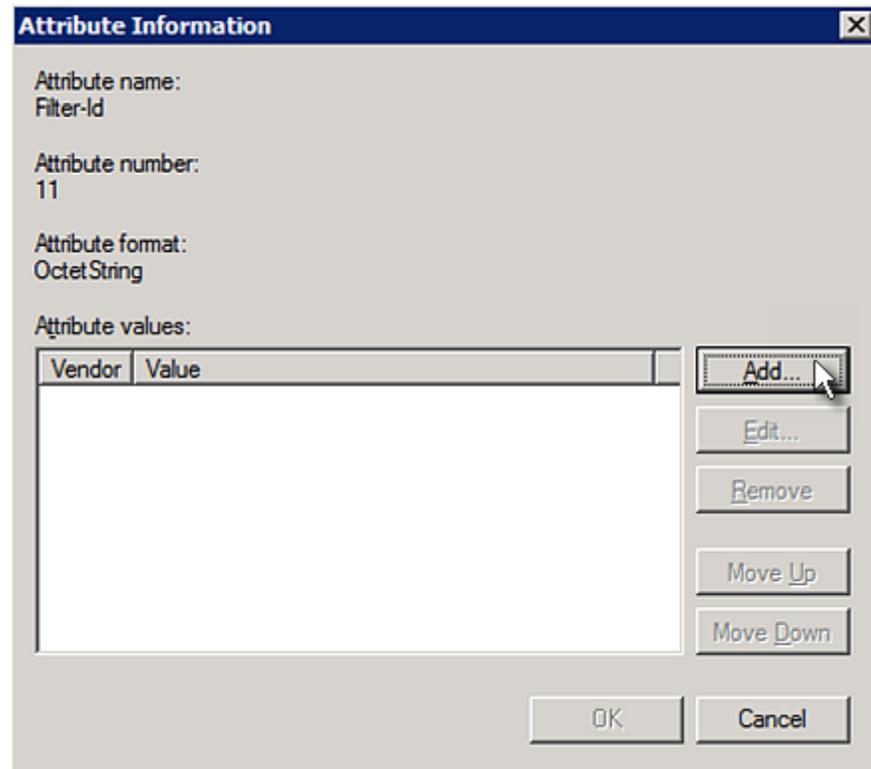
10. Select Standard to the left of the dialog and then click Add.



11. Select Filter-Id from the list of attributes and click Add.

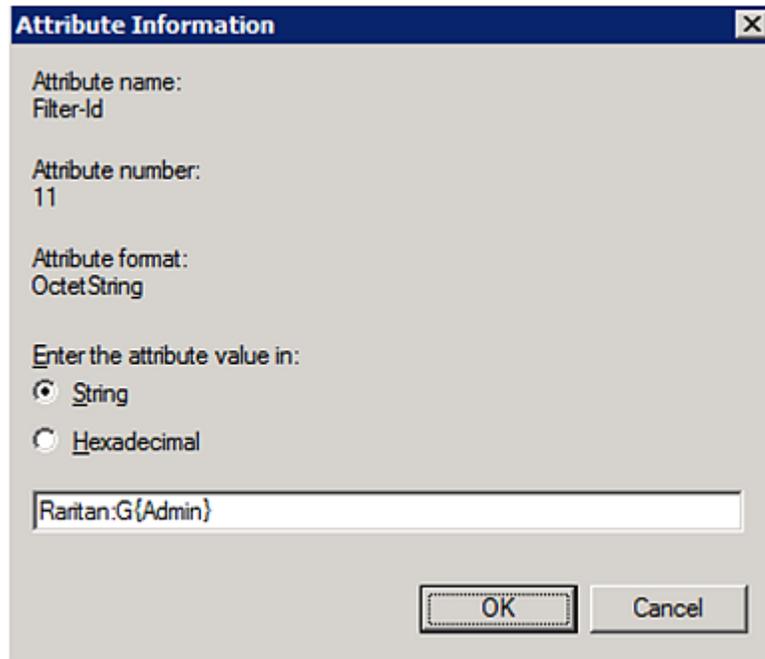


12. In the Attribute Information dialog, click Add.



13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

Admin inside the curved brackets {} is the existing role on the BCM2. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



The image shows a dialog box titled "Attribute Information" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Attribute name: Filter-Id
- Attribute number: 11
- Attribute format: OctetString
- Enter the attribute value in:
 - String
 - Hexadecimal
- Text input field containing: Raritan.G{Admin}
- Buttons: OK and Cancel

14. The new attribute is added. Click OK.

The dialog box, titled "Attribute Information", displays the following configuration:

- Attribute name: Filter-Id
- Attribute number: 11
- Attribute format: OctetString
- Attribute values: A table with one entry.

Vendor	Value
RADIUS Standard	Raritan:G{Admin}

Buttons on the right side of the table include: Add..., Edit..., Remove, Move Up, and Move Down. At the bottom right are OK and Cancel buttons. A mouse cursor is pointing at the OK button.

15. Click Next to continue.

New Connection Request Policy



Configure Settings

NPS applies settings to the connection request if all of the connect matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are a

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

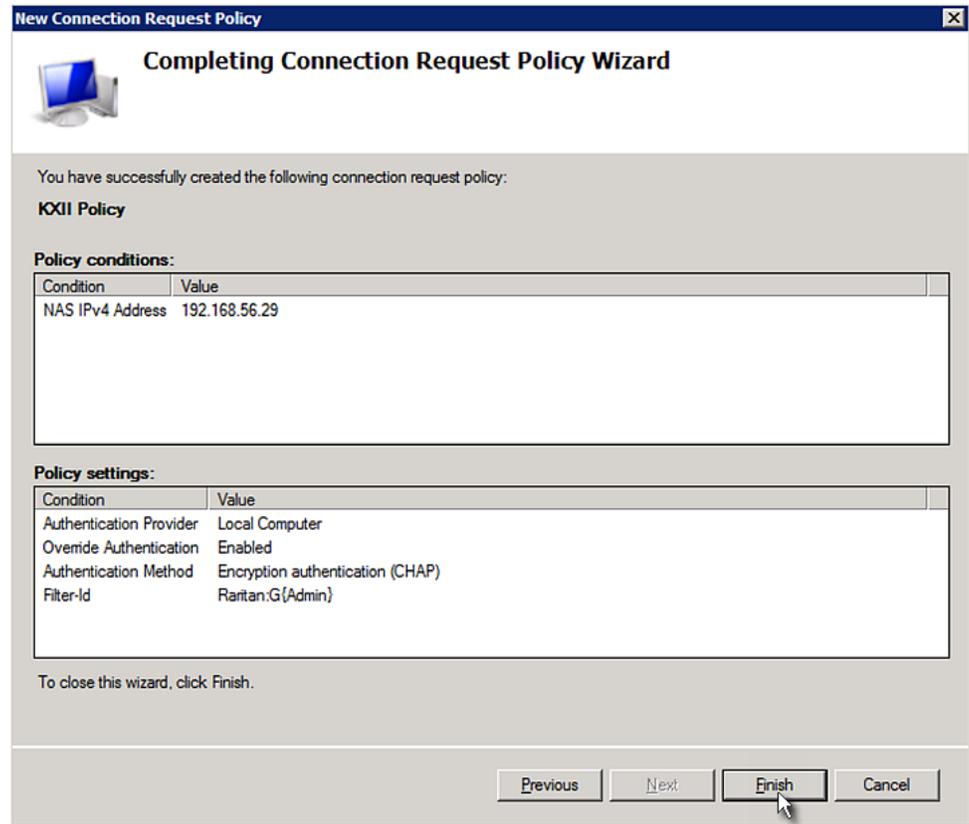
Vendor Specific

To send additional attributes to RADIUS client then click Edit. If you do not configure an attr your RADIUS client documentation for require

Attributes:

Name	Value
Filter-Id	Raritan.G{Admin}

16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.



Step C: Configure a Vendor-Specific Attribute

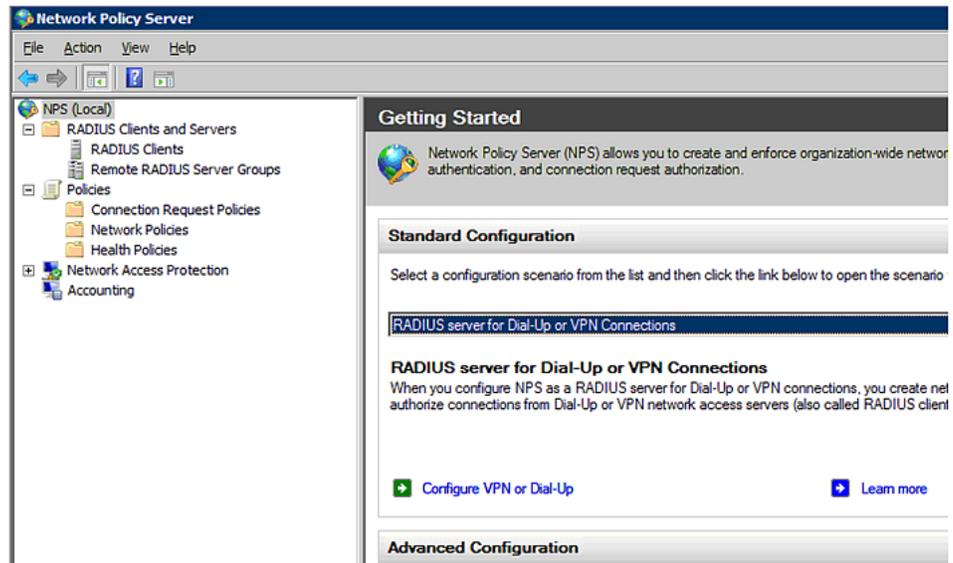
You must specify a vendor-specific attribute (VSA) for Raritan on Windows 2008 NPS. Raritan's vendor code is **13742**.

In the following illustration, we assume:

- There are three roles available on your BCM2: *Admin*, *User*, and *SystemTester*.

► To configure VSA:

1. Open the NPS console, and expand the Policies folder.

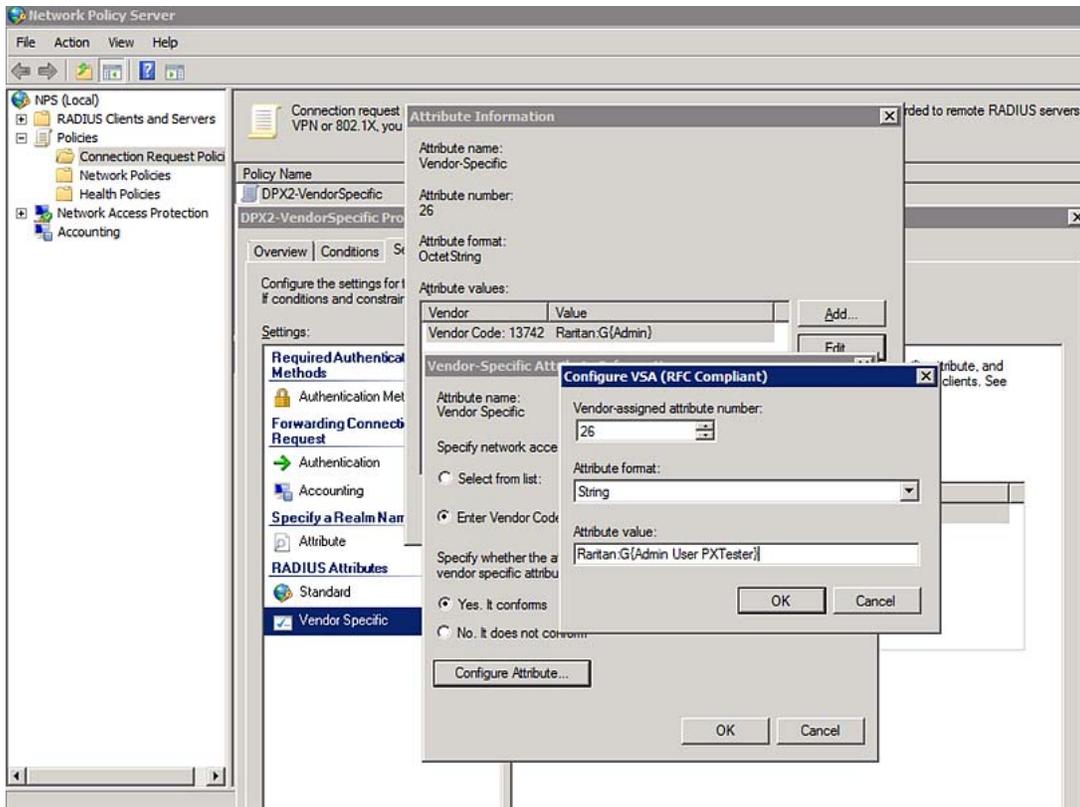


2. Select Connection Request Policies and double-click the policy where you want to add a custom VSA. The policy's properties dialog appears.
3. Click the Settings tab.
4. Select Vendor Specific, and click Add. The Add Vendor Specific Attribute dialog appears.
5. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
6. Click Add, and the Vendor-Specific Attribute Information dialog appears.
7. Click "Enter Vendor Code" and type *13742*.
8. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
9. Click Configure Attribute, and then:
 - a. Type 26 in the "Vendor-assigned attribute number" field.

- b. Select String in the "Attribute format" field.
- c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles are specified inside the curved brackets {} -- Admin, User and SystemTester.

Note that different roles must be separated with a space.

10. Click OK.



AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

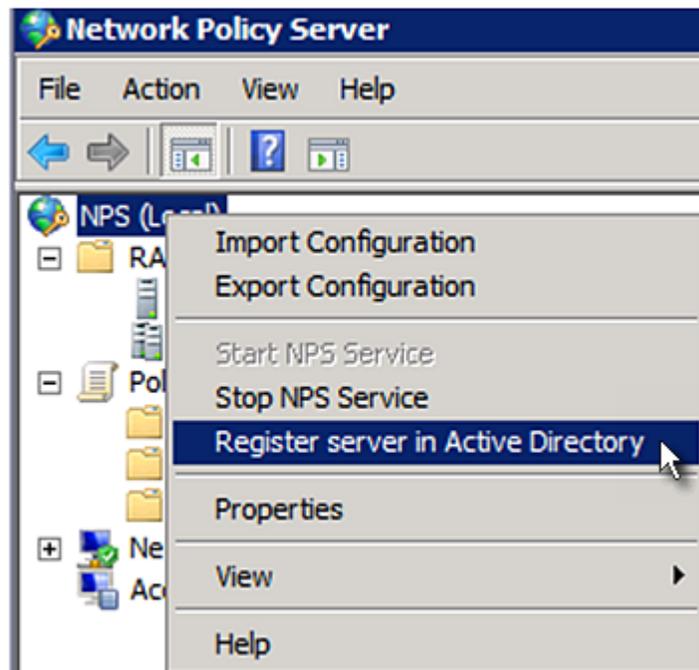
If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

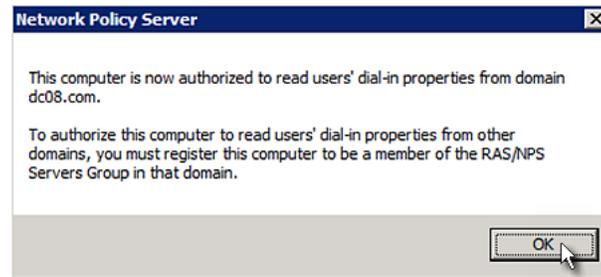
Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

► **To register NPS:**

1. Open the NPS console.
2. Right-click NPS (Local) and select "Register server in Active Directory."



3. Click OK, and then OK again.



► **To grant BCM2 users remote access permission:**

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user whom you want to grant the access permission.

- Click the Dial-in tab and select the "Allow access" checkbox.

The screenshot shows the 'Terminal Services Profile' dialog box with the 'Dial-in' tab selected. The 'Network Access Permission' section contains three radio buttons: 'Allow access' (selected), 'Deny access', and 'Control access through NPS Network Policy'. Below this is a 'Verify Caller-ID' checkbox and an empty text field. The 'Callback Options' section has three radio buttons: 'No Callback' (selected), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:' with an empty text field. The 'Assign Static IP Addresses' section is unchecked and includes a 'Static IP Addresses ...' button. The 'Apply Static Routes' section is also unchecked and includes a 'Static Routes ...' button. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

► **To enable reversible encryption for CHAP authentication:**

- Open Active Directory Users and Computers.
- Open the properties dialog of the user that you want to configure.

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.

The screenshot shows the 'Account' tab of a Windows NT User Manager dialog box. The 'Account options' section contains the following settings:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

The 'Account expires' section has the following settings:

- Never
- End of: Saturday, May 23, 2009

Other visible fields include 'User logon name' (empty), 'User logon name (pre-Windows 2000)' (DC08\ Administrator), and buttons for 'Logon Hours...', 'Log On To...', 'OK', 'Cancel', 'Apply', and 'Help'.

Non-Windows RADIUS Server

For a non-Windows RADIUS server, such as FreeRADIUS, a vendor-specific dictionary file is required.

Dictionary File

Create a vendor-specific dictionary file for Raritan and add the following information to it. Raritan's vendor code is **13742**.

```

# -*- text -*-
#
# dictionary.raritan
#
#
# Version:      $Id$
#
VENDOR          Raritan          13742
#
# Standard attribute
#
BEGIN-VENDOR    Raritan

ATTRIBUTE       Raritan-Vendor-Specific    26    string

END-VENDOR      Raritan

```

Note that "string" in the above contents must be replaced by `Raritan:G{roles}`, where "roles" are one or multiple roles to which the user belongs. For more details, see **Format of the "string"** (on page 417).

Format of the "string"

The format of `string` in the dictionary file is:

```
Raritan:G{roles}
```

"roles" inside the curved brackets {} are role names, which comprise one or multiple roles to which the user belongs.

Multiple role names are separated with a space.

► Example:

If the user has three roles -- *Admin*, *User* and *SystemTester*, then type:

```
Raritan:G{Admin User SystemTester}
```

Therefore, in Raritan's dictionary file, the attribute line is like the following:

Appendix C: RADIUS Configuration Illustration

```
ATTRIBUTE Raritan-Vendor-Specific 26 Raritan:G{Admin User SystemTester}
```

Appendix D Integration

The BCM2 device can work with certain Raritan's or Sunbird's products to provide diverse power solutions.

In This Chapter

Power IQ.....419

Power IQ

You can use Sunbird's Power IQ to collect the power measurement data of all Raritan BCM2 devices and remotely manage or monitor them.

In Power IQ, a Raritan BCM2 should be treated like a PDU and its branch circuit channels should be treated like a PDU's outlets.

Sunbird's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, refer to the Power IQ online help on the Sunbird website: <http://support.sunbirdcim.com>.

*Note: Power IQ supports the port forwarding mode comprising 2 PDUs as of release 4.3.0. For more information on the USB-cascading configuration, see the USB-Cascading Solution Guide, which is available from Raritan website's **Support page** (<http://www.raritan.com/support/>).*

Appendix E Additional BCM2 Information

In This Chapter

Raritan Training Website	420
Altitude Correction Factors	420
Truncated Data in the Web Interface	421
Reserving IP Addresses in Windows DHCP Servers.....	421
Ways to Probe Existing User Profiles.....	423
EnergyWise and LHX/SHX Not Supported	423

Raritan Training Website

Raritan offers free training materials for various Raritan products on the **Raritan training website** <http://www.raritantraining.com>. The Raritan products introduced on this website include the intelligent PDU, dcTrack®, Power IQ, KVM, EMX, BCM and CommandCenter Secure Gateway (CC-SG). Raritan would update the training materials irregularly according to the latest development of Raritan products.

To get access to these training materials or courses, you need to apply for a username and password through the Raritan training website. After you are verified, you can access the Raritan training website anytime.

Having access to the training website could be helpful for learning or getting some ideas regarding Raritan products and making correct decisions on purchasing them. For example, you can take the dcTrack video training before implementing or using it.

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04

Altitude (meters)	Altitude (feet)	Correction factor
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Truncated Data in the Web Interface

Some fields of the BCM2 web interface can accommodate data entry up to 256 characters. When the data entered is too long, it may be truncated due to some or all of the following factors:

- Screen resolution
- Font size
- Font type
- Size of different characters

Current web browser technology cannot break or wrap these fields with long inputs.

The solution for this issue includes:

- Increase of the screen resolution
- Application of smaller font size
- Use of other interfaces, such as the CLI or SNMP, to view the data in these fields

Reserving IP Addresses in Windows DHCP Servers

The BCM2 uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the BCM2 in a Windows® DHCP server, use the BCM2 device's serial number as the unique ID instead of the MAC address.

► IP address reservation procedure:

1. Convert the serial number of your BCM2 into hexadecimal ASCII codes.
 - For example, if the serial number is PEG1A00003, convert each digit to ASCII codes as shown below:

P=50

E=45

G=47

1=31

A=41

0=30

3=33

Below shows the complete converted ASCII codes:

PEG1A00003 = 50454731413030303033

- In your DHCP server, bring up the New Reservation dialog to reserve the IP address for your BCM2.

Field	Description
IP address	Enter the IP address you want to reserve.
MAC address	Enter the converted ASCII codes of the BCM2 serial number. Do NOT use spaces in the ASCII codes. <ul style="list-style-type: none"> In this example, enter 50454731413030303033
Other fields	Configure them according to your needs.

New Reservation ? X

Provide information for a reserved client.

Reservation name:

IP address:

MAC address:

Description:

Supported types

Both

DHCP only

BOOTP only

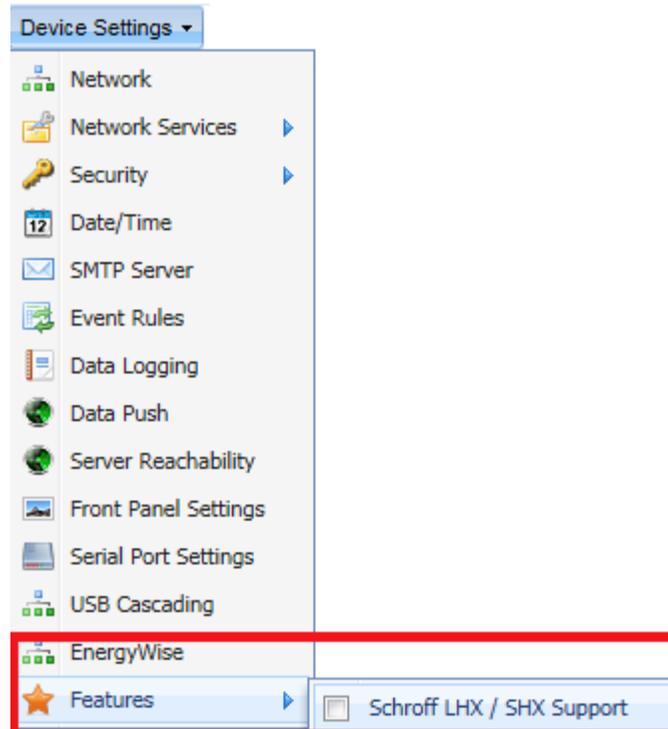
Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the BCM2.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

EnergyWise and LHX/SHX Not Supported

Note that EnergyWise and Schroff LHX/SHX appear as supported options under the Device Settings menu, but they are not supported at the time of writing.



Index

A

- A Note about Enabling Thresholds • 255
- A Note about Infinite Loop • 191
- A Note about Untriggered Rules • 194
- About the Interface • 257
- Access Security Control • 123
- Accessing the Help • 241
- Action Group • 154, 156
- Actuator Configuration Commands • 360, 367
- Actuator Control Operations • 375
- Actuator Information • 271
- Add a Page Icon • 50
- Adding a Firewall Rule • 316
- Adding a Monitored Device • 352
- Adding a Role-Based Access Control Rule • 331
- Adding Authentication Servers • 146
- Adding IT Devices for Ping Monitoring • 196
- Adding LDAP Server Settings • 146
- Adding RADIUS Server Settings • 149, 393
- Additional BCM2 Information • 421
- Adjusting Image Properties • 227, 229
- AD-Related Configuration • 393, 414
- Alarm • 154, 157
- Alarms List • 53, 154, 157
- Alerted Sensors • 12, 53
- Alerts • 11
- All Privileges • 343, 348, 351
- Altitude Correction Factors • 90, 421
- Asset Management • 219
- Asset Management Commands • 369
- Asset Sensor Management • 369
- Asset Sensor Settings • 277
- Automatically Completing a Command • 382

B

- Backup and Restore of BCM2 Device Settings • 237, 240
- Blade Extension Strip Settings • 278
- Browsing through the Online Help • 242
- Bulk Configuration • 237, 240
- Bulk Configuration for Branch Circuit Thresholds • 109, 121

C

- Cascading the BCM2 via USB • 42, 56, 61, 85
- Certificate Signing Request • 139
- Changing a User's Password • 337
- Changing Default Thresholds • 210, 211
- Changing HTTP(S) Settings • 69, 123
- Changing Measurement Units • 343, 346
- Changing Modbus/TCP Settings • 75, 77
- Changing SSH Settings • 70, 98
- Changing Telnet Settings • 71
- Changing the Default Policy • 123, 124, 134, 135
- Changing the LAN Duplex Mode • 302
- Changing the LAN Interface Speed • 302
- Changing the Modbus Configuration • 308
- Changing the Modbus Port • 309
- Changing the Role(s) • 343
- Changing the Sensor Description • 363
- Changing the Sensor Name • 360
- Changing the SSH Configuration • 305
- Changing the SSH Port • 305
- Changing the Telnet Configuration • 304
- Changing the Telnet Port • 305
- Changing Your Own Password • 345
- Changing Your Password • 47
- Checking Server Monitoring States • 200
- Checking the Accessibility of NTP Servers • 314
- Checking the Internal Beeper State • 95
- Clearing Event Entries • 201
- Clearing Event Log • 284
- Clearing Information • 284
- Closing a Local Connection • 262
- Combining Regular Asset Sensors • 31
- Command History • 282
- Components of an Event Rule • 153
- Configure Panel Branch Circuits • 8, 109, 110
- Configure Panel Mains Circuit • 7, 107
- Configure Power Meter • 6, 113
- Configure Thresholds • 9
- Configuring a Specific Rack Unit • 221, 222
- Configuring Data Push Settings • 93, 160
- Configuring Environmental Sensors' Default Thresholds • 358
- Configuring Environmental Sensors or Actuators • 20, 203, 208, 211, 213
- Configuring IP Protocol Settings • 286

- Configuring IPv4 Parameters • 293
 - Configuring IPv6 Parameters • 297
 - Configuring Modbus TCP and/or RTU • 74, 75, 77, 107, 113
 - Configuring Modbus/RTU Settings • 76
 - Configuring Power Meters and Branch Circuit Monitors • 5, 104
 - Configuring SMTP Settings • 92, 161, 162
 - Configuring SNMP Notifications • 73, 190, 199, 247
 - Configuring SNMP Settings • 72, 96
 - Configuring the Asset Sensor • 34, 220
 - Configuring the BCM2 Device and Network • 284
 - Configuring the Cascading Mode • 43, 368
 - Configuring the Feature Port • 82
 - Configuring the Firewall • 123
 - Configuring the Serial Port • 41, 84, 261
 - Configuring Users for Encrypted SNMP v3 • 73, 245, 246
 - Configuring Webcam Storage • 171, 225, 226, 230, 232
 - Configuring Webcams • 225, 227, 229, 232
 - Connecting a DPX2 Sensor Package to DX • 28, 29, 30
 - Connecting a GSM Modem • 40
 - Connecting a Logitech Webcam • 39, 225
 - Connecting an Analog Modem • 41, 261
 - Connecting an External Beeper • 41, 82
 - Connecting Asset Management Sensors • 31, 82, 93, 219
 - Connecting Blade Extension Strips • 34
 - Connecting Composite Asset Sensors to the BCM2 • 37
 - Connecting Environmental Sensor Packages • 22, 202
 - Connecting External Equipment (Optional) • 22
 - Connecting Regular Asset Sensors to the BCM2 • 33, 38
 - Controlling Actuators • 219
 - Copying the BCM2 Configuration • 239
 - Creating a Certificate Signing Request • 139
 - Creating a Role • 98, 101, 348, 393
 - Creating a Self-Signed Certificate • 141
 - Creating a User Profile • 71, 96, 99, 100, 101, 102, 246, 336
 - Creating Actions • 40, 53, 154, 176, 193, 225
 - Creating an Event Rule • 41, 153
 - Creating Firewall Rules • 123, 125
 - Creating Role-Based Access Control Rules • 134, 135
 - Creating Rules • 171
 - Customizing the Date and Time • 313
- ## D
- Daisy-Chain Limitations of Composite Asset Sensors • 38
 - Date and Time Settings • 267
 - Default Log Messages • 133, 162, 180
 - Default Measurement Units • 267
 - Deleting a Firewall Rule • 320
 - Deleting a Monitored Device • 353
 - Deleting a Role • 103, 352
 - Deleting a Role-Based Access Control Rule • 334
 - Deleting a User Profile • 99, 345
 - Deleting an Event Rule or Action • 194
 - Deleting Authentication Server Settings • 151
 - Deleting Firewall Rules • 129
 - Deleting Ping Monitoring Settings • 199
 - Deleting Role-Based Access Control Rules • 138
 - Describing the Sensor's or Actuator's Location • 209, 211
 - Determining the SSH Authentication Method • 306
 - Determining the Time Setup Method • 311, 313
 - Device Info • 14
 - Device Management • 54
 - Diagnostic Commands • 379
 - Dictionary File • 417
 - Different CLI Modes and Prompts • 258, 261, 262, 264, 284, 285, 314, 375, 379
 - Disabling External Authentication • 151
 - Disabling the Automatic Management Function • 207, 218
 - Displaying the Asset Sensor Information • 224
 - Displaying the Device Information • 55
 - Downloading Diagnostic Information • 236
 - Downloading Key and Certificate Files • 143
 - Downloading SNMP MIB • 73, 246, 247, 253
 - DPX Sensor Packages • 22, 23
 - DPX2 Sensor Packages • 22, 26
 - DX Sensor Packages • 22, 28, 169
- ## E
- EAP CA Certificate Example • 290, 292

- Editing Authentication Server Settings • 151
- Editing Firewall Rules • 128
- Editing Ping Monitoring Settings • 199
- Editing Role-Based Access Control Rules • 137
- Email and SMS Message Placeholders • 162, 163, 168, 169, 187
- Enabling and Editing the Security Banner • 133
- Enabling Data Logging • 91
- Enabling External and Local Authentication Services • 152
- Enabling IPv4 or IPv6 • 287
- Enabling Login Limitations • 131, 231
- Enabling Main Controller Access • 74, 77
- Enabling or Disabling a User Profile • 339
- Enabling or Disabling Modbus • 308
- Enabling or Disabling SNMP v1/v2c • 306
- Enabling or Disabling SNMP v3 • 307
- Enabling or Disabling SSH • 305
- Enabling or Disabling Strong Passwords • 327
- Enabling or Disabling Telnet • 304
- Enabling or Disabling the Read-Only Mode • 309
- Enabling or Disabling the Restricted Service Agreement • 321
- Enabling or Disabling the Service Advertisement • 309
- Enabling Password Aging • 132
- Enabling Service Advertisement • 79, 309
- Enabling SNMP • 91, 245
- Enabling Strong Passwords • 132
- Enabling the Feature • 134
- Enabling the Firewall • 123
- Enabling the Front Panel Actuator Control • 18, 219
- Enabling the Modbus/RTU Feature • 76, 77
- Enabling User Blocking • 130
- EnergyWise and LHX/SHX Not Supported • 424
- Entering Configuration Mode • 262, 285, 292
- Entering Diagnostic Mode • 262, 379
- Environmental Sensor Configuration Commands • 360
- Environmental Sensor Default Thresholds • 273
- Environmental Sensor Information • 268
- Environmental Sensor Package Information • 270
- Environmental Sensor Threshold Configuration Commands • 364
- Environmental Sensor Threshold Information • 272
- Environmental Sensors and Actuators • 202
- Event Log • 279
- Event Rules and Actions • 72, 92, 95, 114, 153, 196, 247
- Example • 323
 - Ping Monitoring and SNMP Notifications • 198
- Example - Actuator Naming • 368
- Example - Default Upper Thresholds for Temperature • 359
- Example - Ping Command • 381
- Example - Server Settings Changed • 355
- Example - Turning On a Specific Actuator • 377
- Example 1 • 191
 - Example 1 - Asset Sensor LED Colors for Disconnected Tags • 375
 - Example 1 - Basic Security Information • 283
 - Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 357
 - Example 1 - Creating a User Profile • 347
 - Example 1 - Environmental Sensor Naming • 364
 - Example 1 - IPv4 Firewall Control Configuration • 334
 - Example 1 - Networking Mode • 310
 - Example 1 - Time Setup Method • 314
 - Example 1 - Upper Critical Threshold for a Temperature Sensor • 366
- Example 2 • 191
 - Example 2 - Adding an IPv4 Firewall Rule • 335
 - Example 2 - Combination of SSID and PSK Parameters • 357
 - Example 2 - Enabling Both IP Protocols • 310
 - Example 2 - In-Depth Security Information • 283
 - Example 2 - Modifying a User's Roles • 347
 - Example 2 - Primary NTP Server • 314
 - Example 2 - Rack Unit Naming • 375
 - Example 2 - Sensor Threshold Selection • 364
- Example 3 - Default Measurement Units • 347
- Example 3 - User Blocking • 335
- Example 3 - Wireless Authentication Method • 310
- Example 4 - Adding an IPv4 Role-based Access Control Rule • 336
- Example 4 - Static IPv4 Configuration • 310
- Examples • 282, 310, 314, 334, 347, 364, 375
- Existing Roles • 276

Existing User Profiles • 267, 275
Expanding a Blade Extension Strip • 223
External Beeper • 154, 158

F

Firewall Control • 315
Firmware Upgrade • 232, 239
Forcing a Password Change • 339
Forcing HTTPS Encryption • 123, 139
Format of the • 418
Front Panel Settings • 83
Full Disaster Recovery • 234

G

Gathering the External Authentication Information • 144
Gathering the LDAP Information • 145
Gathering the RADIUS Information • 145

H

Hardware Installation • 4
Help Command • 263
History Buffer Length • 282

I

Identifying Cascaded Devices • 44, 55, 56
Identifying Environmental Sensors and Actuators • 203, 207
Identifying Sensor or Actuator Channels • 206
Idle Timeout • 326
Installation and Initial Configuration • 4
Installing a CA-Signed Certificate • 141
Installing Existing Key and Certificate Files • 143
Installing the USB-to-Serial Driver (Optional) • 253, 259
Integration • 420
Internal Beeper • 155, 169
Introduction • 1
Introduction to the Web Interface • 48
IP Configuration • 265

L

LAN Interface Settings • 265
Layout • 254
LDAP Configuration Illustration • 149, 385
Listing TCP Connections • 236

Log an Event Message • 155, 159
Logging in to CLI • 257, 384
Logging out of CLI • 382
Login and Configuration • 4, 5
Login Limitation • 324
Lowercase Character Requirement • 328

M

Making an RS-232 or USB Connection • 257, 258, 383, 384
Managing Environmental Sensors or Actuators • 28, 203, 207
Managing Event Logging • 200
Managing Firewall Rules • 316
Managing Role-Based Access Control Rules • 331
Managing the Snapshots Saved to BCM2 • 231
Matching the Position • 205
Matching the Serial Number • 204
Maximum Password History • 329
Maximum Password Length • 327
Meter, Panel, and Branch Circuit Monitoring and Management • 104
Microsoft Network Policy Server • 393
Minimum Password Length • 327
Modifying a Firewall Rule • 318
Modifying a Monitored Device's Settings • 353
Modifying a Role • 98, 99, 102, 350
Modifying a Role-Based Access Control Rule • 332
Modifying a User Profile • 47, 99, 102, 337
Modifying a User's Personal Data • 338
Modifying an Action • 73, 193
Modifying an Event Rule • 192
Modifying Firewall Control Parameters • 315
Modifying IPv4 Settings • 64
Modifying IPv6 Settings • 65
Modifying Network Interface Settings • 60
Modifying Network Service Settings • 69, 257, 260
Modifying Network Settings • 49, 63, 79, 387
Modifying Role-Based Access Control Parameters • 330
Modifying SNMPv3 Settings • 340
Modifying the Network Configuration • 59
Monitoring Server Accessibility • 196
More Information about AD or RADIUS Configuration • 149

Multi-Command Syntax • 316, 324, 326, 327, 331, 337, 338, 340, 343, 345, 353, 357, 358, 364, 367

N

Naming a Rack Unit • 372
 Naming an Asset Sensor • 369
 Naming the BCM2 • 49, 59, 90, 94, 95, 207, 210, 218
 Network Configuration • 265
 Network Configuration Commands • 286
 Network Diagnostics • 235
 Network Service Settings • 266
 Network Troubleshooting • 235, 378
 Networking Mode • 266
 Non-Windows RADIUS Server • 393, 417
 Numeric Character Requirement • 328

O

Overriding DHCP-Assigned NTP Servers • 312, 314
 Overriding the IPv4 DHCP-Assigned DNS Server • 295, 296
 Overriding the IPv6 DHCP-Assigned DNS Server • 299, 300

P

Panel Branch Circuits Operations • 95, 104, 109, 114, 115
 Panel Mains Circuit Management • 74, 78, 95, 104, 106, 110, 114, 115, 121
 Panels • 14
 Password Aging • 325
 Password Aging Interval • 325
 Peripherals • 18, 219
 Permissions • 101
 Pinging a Host • 235
 Port Forwarding Examples • 86, 88
 Port Number Syntax • 85, 87, 88
 Power IQ • 420
 Power Meter Management • 74, 78, 95, 109, 110, 111, 112
 Power Meters • 13
 Product Models • 1
 Product Overview - BCM2 Series • 3
 Product Overview - PM Series Power Meters • 2
 Push Out Sensor Readings • 93, 155, 160

Q

Querying Available Parameters for a Command • 263, 264
 Querying DNS Servers • 379
 Quitting Configuration Mode • 285, 322
 Quitting Diagnostic Mode • 379

R

Rack Unit Configuration • 372
 Rack Unit Settings of an Asset Sensor • 277
 RADIUS Configuration Illustration • 149, 393
 Raritan Training Website • 421
 Rebooting the BCM2 • 241
 Record Snapshots to Webcam Storage • 155, 170
 Reliability Data • 281
 Reliability Error Log • 282
 Reserving IP Addresses in Windows DHCP Servers • 422
 Resetting All Active Energy • 94, 109, 110, 114
 Resetting the BCM2 • 377
 Resetting to Factory Defaults • 378, 383
 Restarting the Device • 378
 Restricted Service Agreement • 320
 Retrieving Previous Commands • 381
 Retrieving Software Packages Information • 241
 Role Configuration Commands • 348
 Role of a DNS Server • 69, 387
 Role-Based Access Control • 329

S

Safety Information • iii, 4
 Sample Device-Level Event Rule • 190
 Sample Event Rules • 190
 Sample Mains-Level Event Rule • 190
 Saving a BCM2 Configuration • 238
 Saving Snapshots • 225, 229, 231
 Scan Power Meters • 5
 Scheduling an Action • 93, 160, 175, 180
 Security Configuration Commands • 315
 Security Settings • 274
 Selecting IPv4 or IPv6 Addresses • 287
 Selecting the Internet Protocol • 63, 64, 65
 Send a Snapshot via Email • 155, 160
 Send an SNMP Notification • 155, 163
 Send Email • 155, 162, 178, 180

- Send Sensor Report • 155, 166, 179
- Send Sensor Report Example • 177
- Send SMS Message • 155, 168
- Sending Snapshots or Videos in an Email or Instant Message • 196, 225, 228, 230
- Serial Port Configuration Commands • 356
- Serial Port Settings • 276
- Server Reachability Configuration Commands • 352
- Server Reachability Information • 280
- Server Reachability Information for a Specific Server • 281
- Setting a Sensor's Thresholds • 115, 121
- Setting an LED Color for a Rack Unit • 373, 374
- Setting an LED Mode for a Rack Unit • 373, 374
- Setting Asset Sensor LED Colors • 221
- Setting Data Logging • 91
- Setting Default Measurement Units • 82, 90, 100, 343, 345
- Setting EAP Parameters • 290
- Setting IPv4 Static Routes • 297
- Setting IPv6 Static Routes • 301
- Setting LAN Interface Parameters • 301
- Setting LED Colors for Connected Tags • 371, 373, 374
- Setting LED Colors for Disconnected Tags • 372, 373, 374
- Setting Network Service Parameters • 302
- Setting NTP Parameters • 311, 314
- Setting Power Thresholds • 51, 108, 110, 114, 255
- Setting the Alarmed to Normal Delay for DX-PIR • 364
- Setting the Authentication Method • 288
- Setting the Automatic Daylight Savings Time • 313
- Setting the BSSID • 293
- Setting the Cascading Mode • 16, 42, 43, 56, 85, 88
- Setting the Date and Time • 80
- Setting the History Buffer Length • 356
- Setting the HTTP Port • 303
- Setting the HTTPS Port • 304
- Setting the IPv4 Address • 294
- Setting the IPv4 Configuration Mode • 294
- Setting the IPv4 Gateway • 295
- Setting the IPv4 Preferred Host Name • 294
- Setting the IPv4 Primary DNS Server • 295
- Setting the IPv4 Secondary DNS Server • 296
- Setting the IPv4 Subnet Mask • 295
- Setting the IPv6 Address • 299
- Setting the IPv6 Configuration Mode • 298
- Setting the IPv6 Gateway • 299
- Setting the IPv6 Preferred Host Name • 298
- Setting the IPv6 Primary DNS Server • 299
- Setting the IPv6 Secondary DNS Server • 300
- Setting the LED Operation Mode • 373
- Setting the Networking Mode • 286
- Setting the PSK • 289
- Setting the Serial Port Baud Rate • 356
- Setting the SNMP Configuration • 306
- Setting the SNMP Read Community • 307
- Setting the SNMP Write Community • 307
- Setting the SSID • 288
- Setting the sysContact Value • 307
- Setting the sysLocation Value • 308
- Setting the sysName Value • 308
- Setting the Time Zone • 312
- Setting the X Coordinate • 361
- Setting the Y Coordinate • 362
- Setting the Z Coordinate • 362
- Setting the Z Coordinate Format • 210, 362, 368
- Setting Thresholds for Multiple Sensors • 210, 212
- Setting Up a TLS Certificate • 123, 138
- Setting Up External Authentication • 69, 123, 144
- Setting Up Role-Based Access Control Rules • 134
- Setting Up Roles • 47, 95, 98, 101
- Setting Up User Login Controls • 130
- Setting Up Your Preferred Measurement Units • 82, 99, 100
- Setting Wireless Parameters • 288
- Showing Information • 264
- Showing Network Connections • 380
- Single Login Limitation • 325
- SNMP Gets and Sets • 252
- SNMP Sets and Thresholds • 255
- SNMPv2c Notifications • 248
- SNMPv3 Notifications • 250
- Sorting Firewall Rules • 129
- Sorting Role-Based Access Control Rules • 137
- Sorting the Access Order • 150
- Special Character Requirement • 329
- Specifying the Agreement Contents • 321
- Specifying the Asset Sensor Orientation • 371
- Specifying the CC Sensor Type • 361

- Specifying the Device Altitude • 90
- Specifying the Number of Rack Units • 369
- Specifying the Primary NTP Server • 311
- Specifying the Rack Unit Numbering Mode • 370
- Specifying the Rack Unit Numbering Offset • 370
- Specifying the Secondary NTP Server • 311
- Specifying the SSH Public Key • 306, 344
- States of Managed Actuators • 19, 217
- States of Managed Sensors • 13, 19, 214
- States of Unmanaged Sensors or Actuators • 217, 218
- Static Route Examples • 64, 65, 67
- Status Bar • 49
- Step A
 - Add Your BCM2 as a RADIUS Client • 394
- Step A. Determine User Accounts and Groups • 385
- Step B
 - Configure Connection Request Policies • 397
- Step B. Configure User Groups on the AD Server • 386
- Step C
 - Configure a Vendor-Specific Attribute • 412
- Step C. Configure LDAP Authentication on the BCM2 Device • 387
- Step D. Configure Roles on the BCM2 • 389
- Strong Passwords • 327
- Supported Maximum DPX Sensor Distances • 23, 25
- Supported Web Browsers • 47
- Supported Wireless LAN Configuration • 45
- Switch Peripheral Actuator • 155, 169
- Switching Off an Actuator • 376
- Switching On an Actuator • 376
- Syslog Message • 155, 165

T

- Testing the Network Connectivity • 380
- Testing the Server Connection • 150
- The BCM2 MIB • 253
- The Yellow- or Red-Highlighted Sensors • 12, 18, 50, 53, 114, 115, 213
- Time Configuration Commands • 310
- Tracing the Network Route • 236
- Tracing the Route • 381
- Truncated Data in the Web Interface • 422

U

- Unblocking a User • 130, 377
- Unmanaging Environmental Sensors or Actuators • 28, 208, 217
- Updating the Asset Sensor Firmware • 235
- Updating the BCM2 Firmware • 233
- Uppercase Character Requirement • 328
- USB Wireless LAN Adapters • 42, 44, 45, 56
- USB-Cascading Configuration Commands • 368
- USB-Cascading Configuration Information • 274
- User Blocking • 326
- User Configuration Commands • 336
- User Management • 95
- Using an Optional DPX-ENVHUB2 cable • 24
- Using an Optional DPX-ENVHUB4 Sensor Hub • 24
- Using Default Thresholds • 363
- Using SNMP • 233, 244
- Using the BCM2's Display • 11
- Using the CLI Command • 378, 384
- Using the Command Line Interface • 69, 211, 256, 384
- Using the Reset Button • 383
- Using the Web Interface • 46

V

- Viewing Connected Users • 195, 228, 230
- Viewing Firmware Update History • 234
- Viewing Sensor or Actuator Data • 213
- Viewing the Dashboard • 52
- Viewing the Local Event Log • 92, 146, 165, 200
- Viewing the Panel Data • 104, 106, 109
- Viewing the Power Meter Data • 111, 112
- Viewing the Wireless LAN Diagnostic Log • 201
- Viewing Webcam Snapshots or Videos • 40, 228

W

- Ways to Probe Existing User Profiles • 424
- Webcam Management • 225
- Windows NTP Server Synchronization Solution • 80, 81
- Wired Network Settings • 60
- Wireless Configuration • 266

Index

Wireless LAN Diagnostic Log • 280
Wireless Network Connection • 44, 61
Wireless Network Settings • 61
With an Analog Modem • 261
With HyperTerminal • 257, 377, 383, 384
With SSH or Telnet • 260

▶ **U.S./Canada/Latin America**

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

▶ **China**

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

▶ **India**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

▶ **Japan**

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-5795-3170
Email: support.japan@raritan.com

▶ **Europe**

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

▶ **Melbourne, Australia**

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

▶ **Taiwan**

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com